# Extreme SLX-OS
# Software Upgrade Guide, 20.7.3

## Supporting ExtremeRouting and ExtremeSwitching
## SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150,
## Extreme 8820, Extreme 8720, and Extreme 8520

9039537-00 Rev AB
February 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

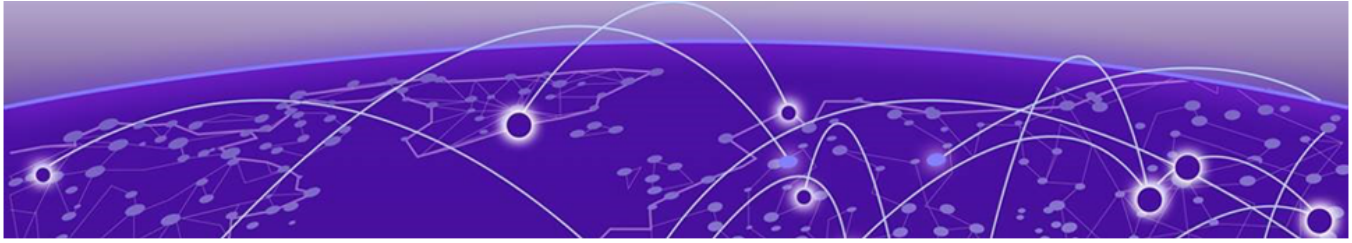
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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


**Preface** ..... **5**
- Text Conventions ..... 5
- Documentation and Training ..... 6
  - Open Source Declarations ..... 7
  - Training ..... 7
- Help and Support ..... 7
  - Subscribe to Product Announcements ..... 8
- Send Feedback ..... 8

**About This Document** ..... **9**
- What's New in this Document ..... 9
- Supported Hardware ..... 9

**Upgrading and Maintaining SLX-OS Software** ..... **11**
- Overview of Upgrading SLX-OS Software ..... 11
- Prepare to Upgrade the SLX-OS Software ..... 12
- Determining the Software Version ..... 13
- Enter Maintenance Mode Before Upgrading Software ..... 13
- Considerations for Obtaining, Decompressing, and Installing Software ..... 14
  - Error messages during firmware update ..... 15
  - Errors displayed on Console during firmware upgrade ..... 15
- Download Software for a Standard Upgrade ..... 21
- Download Software for a Delayed Upgrade ..... 22
- Download Software with the default-config Option ..... 23
- Download Software with the fullinstall Option ..... 24
- Download Software from a USB 3.0 Device ..... 25
- Intel Microcode Update ..... 26
- Upgrade the SLX 9540 FPGA Image ..... 26
- Upgrade the SLX 9540 CPLD Image ..... 27
- Upgrading MCT Clusters to SLX-OS 20.1.1 and Later ..... 27
  - Upgrade MCT Clusters from SLX-OS 18r.2.00b ..... 28
  - Upgrade MCT Clusters from the SLX-OS 20.1.1 Controlled Release ..... 30
- Guidelines for Upgrading TCAM Profiles ..... 31
  - TCAM Profile Changes ..... 31
  - Upgrade Considerations ..... 31
  - Sample Warning Message to Remain in the Current Profile ..... 32
  - Sample Warning Message with a Recommended Profile ..... 32
  - Sample Warning Message for a Deprecated Profile ..... 33
  - Sample Warning Message for a Merged Profile ..... 34
- SLX-OS Software Downgrade Considerations ..... 35
- SLX-OS Software Licenses ..... 35

**Upgrading SLX-OS Software with ONIE** ..... **37**

ONIE Overview....37
Upgrade the SLX-OS Software with ONIE....37
Update ONIE....43

**Installing the SLX-OS TPVM Package....44**
TPVM Installation Overview....44
Using tpvm deploy....45
Prepare to Upgrade the SLX-OS TPVM Package....47
Install the SLX-OS TPVM Package....48
Installing TPVM Using tpvm deploy....49
Upgrading TPVM....50

# 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.<br>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.

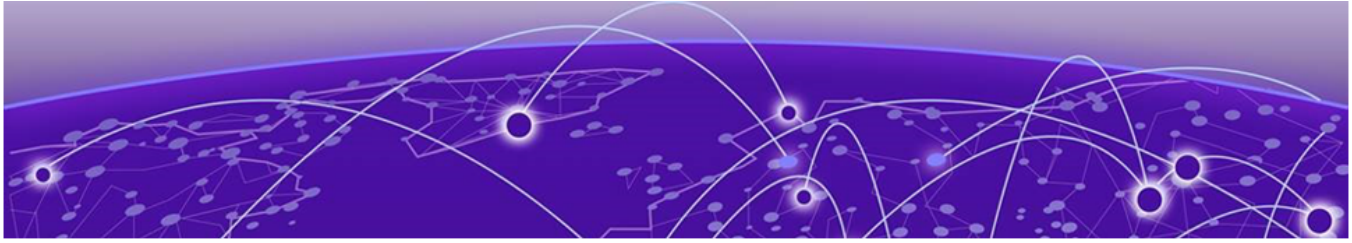
# Send Feedback

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.



# About This Document

What's New in this Document on page 9
Supported Hardware on page 9

## What's New in this Document

This document is released with the SLX-OS 20.7.3 software release.

The following table includes descriptions of changes made to this document for the SLX-OS 20.7.3 software release.

**Table 4: Changes made in Rev AB of this document.**

| Feature | Description | Described in |
|---|---|---|
| Upgrading and maintaining SLX-OS software | In section *User name and password errors*, added that SLX-OS does not support some special characters in firmware download passwords.<br>In the same section, added that *TFTP*, *USB*, and *HTTP* do not require credentials. | Username and Password Errors on page 16 |

**Table 5: Changes made in Rev AA of this document.**

| Feature | Description | Described in |
|---|---|---|
| Upgrading and Maintaining SLX-OS Software | Updated a note in the topic *Download Software from a USB 3.0 device*. Changed the format from *VFAT* to *FAT32* in this note. | Download Software from a USB 3.0 Device on page 25 |
| App Telemetry | | App Telemetry is deprecated from SLX-OS 20.7.3 |

For additional information, refer to the *Extreme SLX-OS Release Notes* for this version.

## Supported Hardware

SLX-OS 20.7.3 supports the following hardware platforms.

- Extreme 8820
- Extreme 8720

- Extreme 8520
- ExtremeSwitching SLX 9540
- ExtremeSwitching SLX 9250
- ExtremeSwitching SLX 9150
- ExtremeRouting SLX 9740
- ExtremeRouting SLX 9640

**Note**

All configurations and software features that are applicable to SLX 9150 and SLX 9250 devices are also applicable for the Extreme 8520 and Extreme 8720 devices respectively.

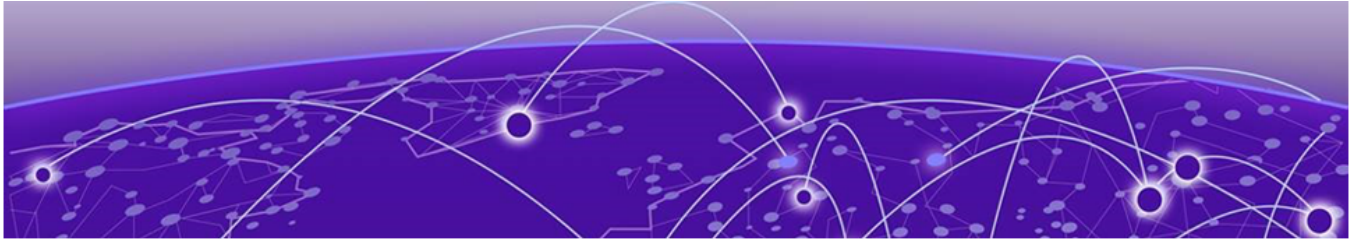
All configurations and software features that are applicable to SLX 9740 devices are also applicable for the Extreme 8820 devices.

The "Measured Boot with Remote Attestation" feature is only applicable to the Extreme 8520, Extreme 8720, and Extreme 8820 devices. It is not supported on the SLX 9150 and SLX 9250 devices.

**Note**

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

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



# Upgrading and Maintaining SLX-OS Software


Overview of Upgrading SLX-OS Software on page 11
Prepare to Upgrade the SLX-OS Software on page 12
Determining the Software Version on page 13
Enter Maintenance Mode Before Upgrading Software on page 13
Considerations for Obtaining, Decompressing, and Installing Software on page 14
Download Software for a Standard Upgrade on page 21
Download Software for a Delayed Upgrade on page 22
Download Software with the default-config Option on page 23
Download Software with the fullinstall Option on page 24
Download Software from a USB 3.0 Device on page 25
Intel Microcode Update on page 26
Upgrade the SLX 9540 FPGA Image on page 26
Upgrade the SLX 9540 CPLD Image on page 27
Upgrading MCT Clusters to SLX-OS 20.1.1 and Later on page 27
Guidelines for Upgrading TCAM Profiles on page 31
SLX-OS Software Downgrade Considerations on page 35
SLX-OS Software Licenses on page 35


## Overview of Upgrading SLX-OS Software

The SLX-OS software (firmware) download is performed incrementally, unless otherwise specified. The **`firmware download`** command compares the new software packages against the current installation and only downloads the packages that contain new features or have been modified.

You can download the software from a remote server by means of any of the following methods.

- HyperText Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- SSH File Transfer Protocol (SFTP)
- Trivial File Transfer Protocol (TFTP)

- Secure Copy Protocol (SCP)
- Prepared USB 3.0 device

If a software download session is interrupted by an unexpected reboot, SLX-OS attempts to recover the previously installed software. Success depends on the state of the software download. You must wait for the recovery to complete before starting another software download.



**Important**

Before upgrading or downgrading the device's firmware, it is recommended that you execute the **`copy running-config startup-config`** command. This will ensure that the *startup-config* data store and the *startup-config* file are updated with the changes stored in the *running-config* data store.

## Prepare to Upgrade the SLX-OS Software

Perform the following tasks so that in the unlikely event of a failure or timeout, you can provide your router support provider the information needed to troubleshoot the problem.

1. Verify the current software version.

   For more information, see Prepare to Upgrade the SLX-OS TPVM Package on page 47.
2. Download the software package from the Extreme Networks website to a server that is running the service for your chosen upgrade method.
3. Decompress the software archive.

   For more information, see Considerations for Obtaining, Decompressing, and Installing Software on page 14.
4. Decide on a migration path if you are crossing a known boundary, such as 32-bit to 64-bit, or kernel version 2.6 to 4.14.
   - Check the connected devices to ensure software compatibility.
   - See the "SLX-OS Compatibility" section of the *SLX-OS Release Notes* for the recommended software version.
5. If you will download software from a file server, verify that the file server is reachable from the SLX device and that you can transfer files from the server to the SLX device.
6. Back up your router configuration to a remote server or a prepared USB device that is attached to the SLX device.

   ```
   copy running-config destination
   ```
7. Connect the SLX device to a computer with a serial console cable.

   Ensure that all serial consoles and any open network connection sessions, such as Telnet, are logged and included with any trouble reports.
8. Run the **`copy support`** command to collect all current core files to a remote server or USB 3.0 device before downloading the software.

   The collected information can help you troubleshoot the software download process in the event of a problem. After you troubleshoot the problem, you can use the **`clear support`** command to remove the collected files.

9. Erase all existing messages and internal messages.

```
device# clear logging raslog
```

10. Configure maintenance mode to prevent traffic loss during the upgrade.

    For more information, see Enter Maintenance Mode Before Upgrading Software on page 13.

## Determining the Software Version

You use the **show version** command to determine the software (firmware) version for both primary and secondary partitions of each installed module of the SLX device or of the SLX device itself.

For example, here is the output for SLX-OS 20.1.1.

```
device# show version

SLX-OS Operating System Version: 20.1.1
Copyright (c) 1995-2019 Extreme Networks, Inc.
Firmware name:      20.1.1
Build Time:         21:34:29 Nov  2, 2019
Install Time:       20:29:12 Nov  8, 2019
Kernel:             4.14.67
Control Processor:  Intel(R) Atom(TM) CPU C3758 @ 2.20GHz,  8 cores
Microcode Version:  0x24
Memory Size:        System Total: 15632 MB
System Uptime:      1days 1hrs 29mins 27secs

Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   20.1.1
         20.1.1

device#
```

## Enter Maintenance Mode Before Upgrading Software

Planned maintenance operations may require the device to be shut down or restarted, resulting in traffic disruption even if alternative paths are available. Maintenance mode provides graceful traffic diversion to alternative traffic paths, helping to minimize traffic loss during such planned operations.

When an alternative path is available, the BGP and MCT protocols redirect traffic away from the node that is going into maintenance mode. When maintenance mode is enabled, all protocols that are running on the maintenance mode node are notified and redirection of traffic (convergence) begins in stages.

**Note**
Maintenance mode is not supported for the following features: BGP address-family, Flowspec, Layer 3 VPN, VPLS, and VLL (virtual leased line).

1. Access configuration mode.

```
device# configure terminal
```

2. Access system mode.

```
device(config)# system
```

3. Access system maintenance mode.

```
device(config-system)# maintenance
```

4. Enable maintenance mode.

```
device(config-system-maintenance)# enable
```

5. Specify the number of seconds allowed per stage of the convergence of traffic to the maintenance mode node.

```
device(config-system-maintenance)# convergence-time 125
```

   This example sets the convergence time to 125 seconds.

The following example summarizes the commands in this procedure.

```
device# configure terminal
device(config)# system
device(config-system)# maintenance
device(config-system-maintenance)# enable
device(config-system-maintenance)# convergence-time 125
```

## Considerations for Obtaining, Decompressing, and Installing Software

- You must download the software package and transfer it to the server and location (such as the FTP server root directory) that you will use for the software upgrade.
- You may also download the software package from a USB drive using the **`firmware download usb`** command.
- You must decompress the software package *before* using the **`firmware download`** command to upgrade the software.

  **Note**
  As a best practice, use 7zip to decompress the software tarball when you use a Microsoft Windows platform for software upgrade.

- The decompressed software package expands into a directory that is named according to the software version. When issued with the path to the directory where the software is stored, the **`firmware download`** command performs an automatic search for the package file type that is associated with the device.
- The following **`firmware download`** command options are available. See the *Extreme SLX-OS Command Reference* for more information about the options.
  - **`default-config`**: Downloads new software and, after a forced cold reboot, cleans up the in-band configuration.
  - **`fullinstall`**: Downloads a larger file selection to cover the differences between 32-bit and 64-bit software or between 2.6 and 4.14 kernel software when upgrading or downgrading the device.
  - **`noactivate`**: Downloads the software to the system without activating it, so the device is not automatically rebooted.
  - **`nocommit`**: Disables auto-commit mode so that software is downloaded only to the primary partition.

  - **noreboot**: Disables auto-reboot mode.
  - **use-vrf**: Specifies the name of the VRF where the host is located. If this option is not set, mgmt-vrf is used by default.
- So that you can address the FTP or SCP server by its name, ensure that a Domain Name System (DNS) entry is established for the server.
- SLX-OS does not support the use of special characters (such as &, !, %, or #) in FTP, TFTP, SFTP, or SCP passwords. The software download fails if your password contains special characters.



**Caution**

Extreme recommends that you do not interact with the device when a reboot is being performed after firmware update. During the upgrade process, SLX-OS might perform more than one reboot of the device being upgraded. Interacting or interfering with the device during this reboot cycle can cause the device not to come up and the installation will be in an inconsistent state.

## Error messages during firmware update

The following error messages are generated and displayed on the console when updating SLX-OS firmware using SCP.

- When the host device is not reachable:

  ```
  [FWDL_ERROR]: ssh: Could not resolve hostname
  ```

- When the username or password is incorrect. This message is also generated when the user account's password has expired:

  ```
  [FWDL_ERROR]: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
  ```

- When the destination directory on the host device is not accessible:

  ```
  [FWDL_ERROR]: No such file or directory
  ```

- When an attempt to install an build not supported on a host device is made.

  ```
  [FWDL_ERROR]: Cannot find firmware. Firmware path is invalid.
  ```



**Note**

These error are also applicable when updating TPVM using SCP.

## Errors displayed on Console during firmware upgrade

When upgrading the firmware using the Console, you might encounter various errors. These errors are displayed on the console during the upgrade process.

These errors can be broadly classified as:

- Username and Password Errors
- Connection Errors
- Host Not Reachable Errors
- Invalid Directory or Filename Errors

- Installing Same Build Errors
- Invalid Firmware Errors
- Invalid File Permission Errors
- Protocol Errors

*Username and Password Errors*

The following table lists the various username and password errors and their possible mitigations:

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:fvtt@10.6.46.52: Permission denied (publickey,gssapi-keyex, gssapi-with-mic,password).<br>Hint: Incorrect credentials. Provide correct credentials | • SCP<br>• SFTP | Incorrect Username or password is entered. | Provide correct username and/or password. |
| [FWDL_ERROR]:Login incorrect.<br>Hint: Incorrect credentials. Provide correct credentials | • FTP | Incorrect Username or password is entered. | Provide correct username and/or password.<br>For firmware download passwords, SLX-OS does not support the use of apostrophe/ single quote (') and double quotes ("). If used, firmware download will fail. |
| | • TFTP<br>• USB<br>• HTTP | None<br>**Note:** No credentials are required for these protocols. | Not Applicable |

*Connection Errors*

The following table lists the various connections errors and their possible mitigations:

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:ssh: Could not resolve hostname {host-name}: Name or service not known.<br>Hint: Unable to resolve host. Verify if host exists and is reachable. | • SCP<br>• SFTP | Connection error for the host identified as *{host-name}*. | Check if the identified host is available and is reachable. |
| [FWDL_ERROR]:wget: unable to resolve host address *{host-name}*<br>Hint: Unable to resolve host. Verify if host exists and is reachable. | • FTP<br>• HTTP | Connection error for the host identified as *{host-name}*. | Check if the identified host is available and is reachable. |
| [FWDL_ERROR]:Connection timed out.<br>Hint: Verify if host exists and is reachable. | • TFTP | Connection error when connecting to the TFTP server. | Check if the TFTP server is available and is reachable. |
| | • USB | None | Not Applicable |

*Host Not Reachable Errors*

The following table lists the various Host Not Reachable errors and their possible mitigations:

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:ssh: connect to host {host-name} port {port-number}: No route to host<br>Hint: Invalid Host address or the host is unreachable. | • SCP<br>• SFTP | Cannot connect to the host identified as {host-name} on port {port-number}. Host is not reachable or the host name is incorrect. | Verify if the host name is correct and is reachable over the network. |
| [FWDL_ERROR]:failed: No route to host.<br>Hint: Invalid Host address or the host is unreachable. | • FTP<br>• HTTP | Cannot connect to the FTP or HTTP server. Server is not reachable or the server host-name/IP is invalid. | Verify if the server host-name/IP is correct and is reachable over the network. |
| [FWDL_ERROR]:Connection timed out.<br>Hint: Verify if host exists and is reachable. | • TFTP | Cannot connect to the TFTP server. Connection timed out. | Verify if the TFTP server host-name/IP is correct and is reachable over the network. |
| | • USB | None | Not Applicable |

*Invalid Directory Errors*

The following table lists the various source/destination directory and file errors and their possible mitigations:

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:scp: {directory-or-file-with-path}: No such file or directory<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • SCP | The directory or file specified in {directory-or-file-with-path} is not valid or is not found. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location. Also ensure that the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:File {directory-or-file-with-path} not found.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • SFTP | The directory or file specified in {directory-or-file-with-path} is not valid or is not found. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location. Also ensure that the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:No such file {directory-or-file-with-path}<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • FTP | The directory or file specified in {directory-or-file-with-path} is not valid or is not found. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location. Also ensure that the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:Transfer timed out.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • TFTP | The transfer has timed out. This could be due to the file being not valid or is not found. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location. Also ensure that the directory or file has adequate permissions for the action being performed on it. |

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:No such file {directory-or-file-with-path}.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • USB | The file/directory is not found on the USB. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location on the USB. Also ensure that the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:{time-stamp} ERROR 404: Not Found.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • HTTP | The file/directory is not found on the HTTP server. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location on the HTTP server. Also ensure that the directory or file has adequate permissions for the action being performed on it. |

*Installing Same Build Errors*

The following table lists the error that is encountered when you try to install the same version of SLX-OS over an existing installation.

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:Upgrade to the same firmware version is not permitted.<br>Hint: Use another firmware version. | • SCP<br>• SFTP<br>• FTP<br>• TFTP<br>• HTTP<br>• USB | This error is displayed when you try to install the same version of the build that is currently installed on the device. | Ensure that you install a build that is not the same build that is currently installed on the device. |

*Invalid Firmware Filename Error*

The following table lists the errors that are generated when the firmware filename or source directory is incorrect.

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:Cannot find firmware. Firmware path is invalid.<br>Hint: Ensure that the Firmware image {image-file-name} is available in directory | • SCP<br>• SFTP<br>• FTP<br>• TFTP<br>• HTTP<br>• USB | This error is displayed when the firmware file that is to be installed cannot be found at the specified location. | Ensure that the firmware image file is correct and is available in the appropriate directory for installation. |

*Invalid File Permission Errors*

The following table lists the various source/destination directory and file permission errors and their possible mitigations:

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:scp: {directory-or-file-with-path} Permission denied<br>Hint: Directory/File path is not valid or has insufficient access permissions. | • SCP | The directory or file specified in {directory-or-file-with-path} does not have the required access permissions. | Verify if the directory or file is valid and ensure that the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:File {directory-or-file-with-path} not found.<br>Hint: Directory/File path is not valid or has insufficient access permissions. | • SFTP | The directory or file specified in {directory-or-file-with-path} is not valid or file has insufficient permissions to perform this action. | Verify if the directory or file is valid and the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:No such directory {directory-or-file-with-path}<br>Hint: Directory/File path is not valid or has insufficient access permissions. | • FTP | The directory or file specified in {directory-or-file-with-path} is not valid the file has insufficient permissions to perform this action. | Verify if the directory or file is valid and has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:Transfer timed out.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • TFTP | The transfer has timed out. This could be due to the file being not valid or is not found. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location. Also ensure that the directory or file has adequate permissions for the action being performed on it. |

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]:No such file {directory-or-file-with-path}.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • USB | The file/directory is not found on the USB. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location on the USB. Also ensure that the directory or file has adequate permissions for the action being performed on it. |
| [FWDL_ERROR]:{time-stamp} ERROR 404: Not Found.<br>Hint: Directory/file path is not valid or has insufficient access permissions. | • HTTP | The file/directory is not found on the HTTP server. This message is also generated if the specified file has insufficient permissions to perform this action. | Verify if the directory or file is valid and can be found at the specified location on the HTTP server. Also ensure that the directory or file has adequate permissions for the action being performed on it. |

*Protocol Errors*

The following table lists the error generated when there is an issue from the specific protocol used for file transfer.

| Error | Protocol | Description | Mitigation |
|---|---|---|---|
| [FWDL_ERROR]: <Respective error message from protocol><br>Hint: Protocol Error. Refer <protocol> man page or contact help. | • SCP<br>• SFTP<br>• FTP<br>• TFTP<br>• HTTP<br>• USB | This message is generated from the protocol used to transfer the firmware file to the device. | Use mitigations specified for that particular error for the particular protocol. |

## Download Software for a Standard Upgrade

Ensure that the server from which you download the software is reachable from the SLX device that you are upgrading.

1. Download the software from the hosting server.

```
device# firmware download ftp user user pass extreme host
10.x.x.x dir builds/slxos20.x.x

Performing system sanity check...
This command will cause a cold/disruptive reboot and will require that existing
telnet, secure telnet or SSH sessions be restarted.
Do you want to continue? [y/n]:y
```

   If you enter **y** after the prompt, the device commits the software automatically upon booting up.

2. Log back into the device.

3. Verify the new software version.

   Both partitions on the device or on the modules should contain the new software after the firmware commit is complete.

```
device# show version

SLX-OS Operating System Version: 20.x.x
Copyright (c) 1995-2019 Extreme Networks, Inc.
Firmware name: 20.x.x
Build Time: 21:34:29 Nov 2, 2019
Install Time: 20:29:12 Nov 8, 2019
Kernel: 4.14.67
Control Processor: Intel(R) Atom(TM) CPU C3758 @ 2.20GHz, 8 cores
Microcode Version: 0x24
Memory Size: System Total: 15632 MB
System Uptime: 1days 1hrs 29mins 27secs
Name Primary/Secondary Versions
----------------------------------------
SLX-OS 20.x.x
20.x.x
device#
```

## Download Software for a Delayed Upgrade

Ensure that the server from which you download the software is reachable from the SLX device that you are upgrading.
Do not perform a standard delayed upgrade with the **`default-config`** option or the **`fullinstall`** option.

1. Download the software from the hosting server.

```
device# firmware download ftp noactivate user user pass extreme host
10.x.x.x dir builds/slxos20.1.1a

Performing system sanity check...
You are running firmware download without Activating the downloaded firmware.
  Please use firmware activate to activate the firmware.
Do you want to continue? [y/n]:y
If you enter y after the prompt, the device will download and install the firmware
  to the secondary image location. This can be verified using the 'show version'
  command. In the output below, note that firmware 20.x.x is active, but 20.x.x
  has been loaded to the secondary, for future activation.
device# show ver

SLX-OS Operating System Version: 20.x.x
Copyright (c) 1995-2020 Extreme Networks, Inc.
Firmware name:      20.x.x
Build Time:         09:27:29 Dec 19, 2019
Install Time:       17:44:23 Dec 20, 2019
Kernel:             4.14.67
Control Processor:  Intel(R) Atom(TM) CPU C3758 @ 2.20GHz,  8 cores
Microcode Version:  0x2e
Memory Size:        System Total: 15632 MB
System Uptime:      19days 4hrs 8mins 8secs

Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   20.x.x
         20.x.x
```

   The device loads the software (firmware) image to the secondary image location. At this point, you can activate the image during a maintenance window.

2. During a maintenance window, active the image.

```
device# firmware activate

This command will activate the firmware. It will cause a cold reboot and will
require that existing telnet, secure telnet or SSH sessions be restarted.

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

The device reboots and the new software is committed.

## Download Software with the default-config Option

Use the **firmware download** command with the **default-config** option to download new software, and, after a forced cold reboot, clean up all in-band configuration. In other words, all configuration (except for the mgmt-VRF and the management interface) is removed, including TACACS, RADIUS, AAA, SNMP, syslog, DNS, and telemetry data streaming.

The default-config option is useful when the SLX device is repurposed for a different position in the network.



**Caution**

- When you use the **default-config** option, traffic is disrupted and the configuration is lost. Save the configuration information before you run the command. You can restore the configuration after upgrade, if needed.
- To use the **default-config** option over an in-band connection, you need a serial port connection to recover or remotely access the device, because all in-band configuration will be removed.

1. Download the software from the hosting server.

```
device# firmware download default-config ftp user user pass extreme host
                    10.x.x.x dir builds/slxos20.x.x
                    Performing system sanity check...
                    This command will set the configuration to default.
                    This command will cause a cold/disruptive reboot and will require
that existing telnet,
                    secure telnet or SSH sessions be restarted.
                    Do you want to continue? [y/n]:y
```

If you enter **y** after the prompt, the device commits the software automatically upon booting up.

2. Log back into the device.

   If your remote connection to the SLX device was over in-band interfaces, log back in to the device from the management serial connection.

3. Verify the new software version.

   Both partitions on the device or on the modules should contain the new software.

```
device# show version

            SLX-OS Operating System Version: 20.x.x
            Copyright (c) 1995-2019 Extreme Networks, Inc.
            Firmware name:      20.x.x
            Build Time:         21:34:29 Nov  2, 2019
            Install Time:       20:29:12 Nov  8, 2019
```

```
Kernel:              4.14.67
Control Processor:   Intel(R) Atom(TM) CPU C3758 @ 2.20GHz,  8 cores
Microcode Version:   0x24
Memory Size:         System Total: 15632 MB
System Uptime:       1days 1hrs 29mins 27secs

Name      Primary/Secondary Versions
----------------------------------------
SLX-OS    20.x.x
20.x.x

device#
```

## Download Software with the fullinstall Option

Before downloading the software with the *fullinstall* option, do the following:

1. Take a backup of the existing running config and move it out of the device.
2. Copy the running config to the startup config.
3. Auto persistence configuration - take a backup of the configuration and move it out of the device.



**Note**

Note that the configurations done using the Privilege Execution Mode are not saved in the *running-config* and these configurations are also not backed up automatically. Extreme recommends that you take a manual (physical) note of these configurations before downloading the software.

Use the **`firmware download`** command with the fullinstall option to download a larger file selection to cover the differences between 32-bit and 64-bit software (firmware) or between 2.6 and 4.14 kernel software when upgrading or downgrading the device.

1. Download the software from the hosting server.

```
device# firmware download fullinstall ftp ftpuser user pass password host 10.xx.xx.61
dir builds/slxos20.1.1
Performing system sanity check...

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware
download and auto-replay configs
This command will cause a cold/disruptive reboot and will require that existing
telnet,
secure telnet or SSH sessions be restarted.

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

2. Log back into the device.

   The **`fullinstall`** option retains the startup configuration file. Upon the automatic reboot of the device, the startup configuration file is reloaded automatically.

3. Verify the new software version.

   Both partitions on the device or on the modules should contain the new software.

```
device# show version

SLX-OS Operating System Version: 20.x.x
Copyright (c) 1995-2019 Extreme Networks, Inc.
```

```
Firmware name:      20.x.x
Build Time:         21:34:29 Nov  2, 2019
Install Time:       20:29:12 Nov  8, 2019
Kernel:             4.14.67
Control Processor:  Intel(R) Atom(TM) CPU C3758 @ 2.20GHz,  8 cores
Microcode Version:  0x24
Memory Size:        System Total: 15632 MB
System Uptime:      1days 1hrs 29mins 27secs

Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   20.x.x
         20.x.x

device#
```

Once the software is installed successfully, the device boots with the *default configuration*. The device then restores the configuration using the saved *startup configuration*. Once the configuration is applied, the *startup configuration* becomes *running-config*.

Then do the following:

1. Compare the backup of the *running-config* with the current *running-config* on device. If different, manually apply the missing configurations.
2. Manually apply all the configuration there were done using the Privilege Execution Mode.

## Download Software from a USB 3.0 Device

Extreme Networks devices support software (firmware) download from a USB 3.0 device. Before you can access the USB device, you must enable the device and mount it as a file system. The software images to be downloaded must be stored in the `/brocade/firmware` directory. Multiple images can be stored under this directory.



**Note**

The USB 3.0 device used for firmware download must be formatted either as FAT32 (Windows) or as EXT4 (Linux) format. As a best practice, use an USB device that is, at the least, 16GB in size.

1. Ensure that the USB device is connected to the device.
2. Enable the USB device from Privileged EXEC mode.

```
device# usb on
Trying to enable USB device. Please wait...
USB storage enabled
```

3. (Optional) Review the USB directory.

```
device# usb dir
config\                 24kB     2019 Oct 30 15:49
  slx1-1.cfg            7kB      2019 Oct 30 15:49
  slx8-1.cfg            16kB     2018 Sep 04 18:34
support\                0B       2018 Aug 20 12:36
firmwarekey\            0B       2018 Aug 20 12:36
firmware\               12374MB  2019 Oct 30 17:59
  slxos20.1.1\          8222MB   2019 Oct 30 18:04
  slxos18s.1.03\        4151MB   2019 Oct 28 17:48
scripts\                0B       2018 Aug 20 12:36
```

```
Available space on usbstorage 84%(101730496512 Bytes)

device#
```

4. Download the software.

   The command includes the relative path to the software directory, which you can see in the output of the **usb dir** command.

```
device# firmware download usb directory slxos20.1.1
```

## Intel Microcode Update

Intel provides updates to its processor code through microcodes. These microcodes contain mitigations to critical CVEs and processor vulnerabilities for these processors.

Each family of Intel processor has its own microcode.

Extreme bundles the latest Intel microcode for the different processors used within its devices along with the SLX-OS software bundle.

This microcode is installed whenever SLX-OS is installed on the device. The following table describes the scenarios when the Intel Microcode is updated along with the SLX-OS firmware.

**Table 6: Intel microcode upgrade matrix**

| Process | Current Microcode Version | Action |
|---|---|---|
| Upgrade / Downgrade | On the device: Lower version<br>Within SLX-OS firmware: Higher version | The higher microcode version from SLX-OS will be loaded. |
| Upgrade / Downgrade | On the device: Higher version<br>Within SLX-OS firmware: Lower version | No action is taken. |
| Upgrade / Downgrade | Same microcode version on both the device and within SLX-OS firmware. | No action is taken. |

## Upgrade the SLX 9540 FPGA Image

1. Confirm that the peripheral software (firmware) requires an upgrade.

   If the dates are not identical, the software must be upgraded.

```
device# show firmware peripheral fpga

        +---------------+----------------------+-------------------------------
+
        |     Type      |   Current Version    |   Latest Version Available   |
        +---------------+----------------------+-------------------------------
+
        |    sysfpga    |    02/09/2017(92)    |        02/09/2017(92)         |
        +---------------+----------------------+-------------------------------+
```

2. Update the software.

```
device# firmware peripheral-update fpga
erasing .. ... done
programming ........................... 25% ........................
50% ........................... 75% ........................ 100
sysfpga image is upgraded successfully.
```

3. Reboot the device.

```
device# reload system
```

## Upgrade the SLX 9540 CPLD Image

1. Confirm that the peripheral software (firmware) requires an upgrade.

   If the dates are not identical, the software must be upgraded.

```
device# show firmware peripheral cpldSLX# show firmware peripheral cpld

+---------------+----------------------+-------------------------------+
|     Type      |   Current Version    |   Latest Version Availalble   |
+---------------+----------------------+-------------------------------+
|    CPLD0      |    02/09/2017(93)    |        02/09/2017(93)         |
+---------------+----------------------+-------------------------------+
|    CPLD1      |    02/09/2017(93)    |        02/09/2017(93)         |
+---------------+----------------------+-------------------------------+
```

2. Update the software.

   Both units are upgraded automatically.

```
device# firmware peripheral-update cpld
erasing ….. done
programing …….…….…….……. 25% ……….…….……. 50% .......…….…….…… 75% ……………………. 100%
cpld0 image is upgraded successfully.

erasing ….. done
programming …….…….…….……. 25% ……….…….……. 50% .......…….…….…… 75% ……………………. 100%
cpld1 image is upgraded successfully.
```

3. Reboot the device.

```
device# reload system
```

4. Verify that the units were upgraded.

   The dates should be identical.

```
device# show firmware peripheral cpld
+----------+----------------+----------------+
|  Type    | Current Version| Latest Version |
+----------+----------------+----------------+
|  CPLD0   | 02/09/2017(93) | 02/09/2017(93) |
+--------- +----------------+----------------+
|  CPLD1   | 02/09/2017(93) | 02/09/2017(93) |
+--------- +----------------+----------------+
```

## Upgrading MCT Clusters to SLX-OS 20.1.1 and Later

The format of the SLX-OS 20.1.1 and later startup-config has changed from the earlier releases. You can upgrade MCT clusters and preserve your MCT configuration in one of the following scenarios:

- Upgrade MCT Clusters from SLX-OS 18r.2.00b on page 28: For this release, you can download a script that preserves your MCT configuration during upgrade.

- Upgrade MCT Clusters from the SLX-OS 20.1.1 Controlled Release on page 30: The controlled release uses the new format for `startup-config`, so upgrading poses no risk to your MCT configuration.

**Important**

MCT configuration is not preserved if you upgrade clusters from any release other than 18r.2.00b or the 20.1.1 controlled release. For such upgrades, you have the following options:

- Upgrade your clusters to 18r.2.00b, and then upgrade to 20.1.1 or later using the script that preserves your MCT configuration.
- Upgrade to 20.1.1 or later and manually create the MCT `startup-config` after upgrade.

## Upgrade MCT Clusters from SLX-OS 18r.2.00b

Perform the following steps to upgrade your MCT clusters while preserving your startup configuration after upgrade.

**Important**

Do not change `startup-config` after you run the `mct_config_convert.py` tool. Changes made after the tool runs are not reflected after the upgrade to SLX-OS 20.1.1 or later.

1. On Node A and Node B, download the `mct_config_convert.py` tool from github.extremenetworks.com.
2. On Node A and Node B, copy the tool to the `flash://` path.

```
device# copy scp://<username>:<password>@<hostname>//<path to file>/
mct_config_convert.py  flash://mct_config_convert.py
```

3. On Node A and Node B, configure client isolation mode to be loose.

```
device(config)# cluster <cluster-name> <cluster-id>
device(config-cluster-1)# client-isolation loose
```

4. Isolate Node A from the network.
   a. On Node A, disable the MCT client interfaces.

```
device(config-cluster-1)# client-interfaces-shutdown
```

   b. Disable the uplink to the core network.
   c. Shut the link connected to the MCT peer node (ICL interface).

   At this point, all CCEP traffic is switched to Node B within 30 seconds, depending on the scale and other parameters.
5. On Node A, copy the running configuration to the startup configuration.

```
device# copy running-config startup-config
```

6. On Node A, run the tool from privileged EXEC mode using the following syntax: `python mct_config_convert.py --peer_ip <MCT peer-ip-address> --peer_int <MCT peer interface>`.

   For example:

   ```
   device# python mct_config_convert.py --peer_ip "10.x.x.x" --peer_int "Port-Channel 64"
   ```

   This step converts your existing MCT configuration to the format required for SLX-OS 20.1.1 and later.
7. Upgrade Node A to the 20.1.1 or later image using the **`firmware download`** command with the **`fullinstall`** option.

   During the upgrade on Node A, traffic passes through Node B.
8. Verify that Node A is back online after the upgrade and initialization is complete.
9. Isolate Node B from the network.

   **Important**
   There is complete traffic loss at this step.

   a. On Node B, disable the MCT client interfaces.

      ```
      device(config-cluster-1)# client-interfaces-shutdown
      ```

   b. Disable the uplink to the core network.
   c. Shut the link connected to the MCT peer node (ICL interface).
10. On Node B, copy the running configuration to the startup configuration.

    ```
    device# copy running-config startup-config
    ```
11. On Node A, enable the uplink to the core network and the link connected to the MCT peer node (ICL interface).
12. Restore Node A to the network.

    ```
    device(config-cluster-1)# no shutdown clients
    ```

    All CCEP traffic switches to Node A within 30 seconds, depending on the scale and other parameters.
13. On Node B, run the tool from privileged EXEC mode using the following syntax: `python mct_config_convert.py --peer_ip <MCT peer-ip-address> --peer_int <MCT peer interface>`. For example:

    ```
    device# python mct_config_convert.py --peer_ip "10.x.x.x" --peer_int "Port-Channel 63"
    ```
14. Upgrade Node B to the 20.1.1 or later image using the **`firmware download`** command with the **`fullinstall`** option.

    During the upgrade on Node B, traffic passes through Node A.
15. On Node B, enable the uplink to the core network and the link connected to the MCT peer node (ICL interface).
16. When the cluster peer is up, restore Node B to the network.

    ```
    device(config-cluster-1)# no shutdown clients
    ```
17. Save the configuration changes to the respective nodes.

## Upgrade MCT Clusters from the SLX-OS 20.1.1 Controlled Release

This procedure is based on the presence of Layer 2 VPN configuration. If Layer 2 VPN configuration is not present, swap steps 5 and 6 with steps 7 and 8 to minimize traffic loss.

1. Isolate Node A from the network.
   a. On Node A, disable the MCT client interfaces and ICL interface.

      ```
      device(config-cluster-1)# shutdown all
      ```

   b. Disable the uplink to the core network.

      This command causes all CCEP traffic to switch to Node B within 10 seconds, depending on the scale and other parameters.
2. On Node A, copy the running configuration to the startup configuration.

   ```
   device# copy running-config startup-config
   ```

3. Upgrade Node A to the 20.1.1 or later image using the **`firmware download`** command with the **`fullinstall`** option.

   During the upgrade on Node A, traffic passes through Node B.
4. Verify that Node A is back online after the upgrade and initialization is complete.
5. Isolate Node B from the network.

   **Important**
   There is complete traffic loss at this step.

   a. On Node B, disable the MCT client interfaces and ICL interface.

      ```
      device(config-cluster-1)# shutdown all
      ```

   b. Disable the uplink to the core network.
6. On Node B, copy the running configuration to the startup configuration.

   ```
   device# copy running-config startup-config
   ```

7. On Node A, enable the uplink to the core network.
8. Restore Node A to the network.

   ```
   device(config-cluster-1)# no shutdown all
   ```

   This command causes all CCEP traffic to switch to Node A within 10 seconds, depending on the scale and other parameters.
9. Upgrade Node B to the 20.1.1 or later image using the **`firmware download`** command with the **`fullinstall`** option.

   During the upgrade on Node B, traffic passes through Node A.
10. Verify that Node B is back online after the upgrade and initialization is complete.
11. On Node B, enable the uplink to the core network.
12. Restore Node B to the network.

    ```
    device(config-cluster-1)# no shutdown all
    ```

13. Save the configuration changes to the respective nodes.

# Guidelines for Upgrading TCAM Profiles

## TCAM Profile Changes

| Previous TCAM Profiles | SLX 20.1.1 and Later Profiles | Difference |
|---|---|---|
| DefaultLayer2-optimized | Default | The Layer2-optimized profile is merged into the new Default profile. |
| BGP-Flowspec | Border-routing | The BGP-Flowspec profile is renamed as the Border-routing profile. |
| VXLAN-extended | VXLAN-visibility | The VXLAN-extended profile is renamed as the VXLAN-visibility profile. |
| Layer2-Ratelimit | Layer2-Ratelimit | No change in the profile name. |
| Multicast | Multicast | No change in the profile name. |
| App-telemetry | | App Telemetry is deprecated from SLX-OS 20.7.3 |
| NPB-optimized-1 | | Deprecated |
| Openflow-optimized-1 | | Deprecated |
| Openflow-optimized-2 | | Deprecated |
| Openflow-optimized-3 | | Deprecated |

## Upgrade Considerations

- When you upgrade to SLX-OS 20.1.1 and later, warning messages capture the difference between the new TCAM profiles and the TCAM profiles in the version from which you are upgrading.
- The deprecated profiles and the Layer2-optimized profile are not supported in SLX-OS 20.1.1 and later. When the warning messages appear, press `n` to cancel the upgrade and choose a supported TCAM profile.
- For the supported TCAM profiles, you can remain in your current profile (press `y` in the warning message) or choose a different profile (press `n`) based on the recommendation in the warning message.
- If you change a TCAM profile based on the recommendation, then the warning message for the new TCAM profile will not be displayed during the upgrade restart.
- If you press `n` to cancel the upgrade and choose a supported profile, you need to save the TCAM configuration before restarting the upgrade.
- Renamed TCAM profiles are automatically converted to the new profile after the upgrade.
- The warning messages describe the feature parity between the new and old profiles.

- You cannot change a TCAM profile after running the MCT script. You have to wait to change the TCAM profile after the upgrade is complete.
- If you change a profile before starting the upgrade (by means of the **`firmware download`** command) and the upgrade then fails, you must manually change the profile back to the previous configuration.
- For renamed, merged, and deprecated profiles, you need to save the `running-config` to the `startup-config` after the upgrade is complete.

## Sample Warning Message to Remain in the Current Profile

```
Performing system sanity check ...
Warning: The current TCAM profile is 'default'. This profile does not support VNI Match
for IPv4 ACL, VRF Match for IPv4 BGP-Flowspec rules, SA port authentication, VM Tracking,
LOAM Loopback, and DSCP remarking in SLXOS version 20.x.x. The scale limits for ACL will
be
reduced to 4K (MAC + IPv4) and for MPLS-XC-Stats will be reduced to 256. Rules above new
scale limit will not be effective after upgrade to SLX version 20.x.x.

You are running firmware download with 'fullinstall' option.
This command will preserve startu-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure
telnet or SSH sessions be restarted.

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

## Sample Warning Message with a Recommended Profile

This example includes the selection of a new profile and the restart of the software download process.

```
Performing system sanity check ...
Warning: The current TCAM profile is 'vxlan-ext'. This profile does not support MCT in
SLXOS
version 20.1.1. The recommended TCAM profile is 'default'. Please run the 'profile tcam'
command to change the profile to 'default' to retain the MCT support else proceed
normally.
Note that if 'default' profile is chosen, VXLAN visibility ACL is not supported, ACL
scale limit
will be reduced to 4K (MAC + IPv4). The ACL rules above 4K will not be effective after
upgrade to
SLX version 20.1.1.

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure
telnet or SSH sessions be restarted.

Do you want to continue? [y/n]: n
device# configure terminal
Entering configuration mode terminal
device(config)# hardware
device(config-hardware)# profile tcam default
```

```
Warning: To activate the new profile config, please run 'copy running-config startup-
config'
followed by 'reload system.'

device(config-hardware)# end
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [y/n]: y

device#
device# firmware download fullinstall

Performing system sanity check ...

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure
telnet or SSH sessions be restarted.

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

Checking conditions for downloading to 20.x.x
System settings check passed (0).

You are running firmwaredownload with auto-reboot and auto-commit enabled. After the
firmware is
downloaded the system will reboot and commit firmware automatically.

Preparing for firmware download ...
```

## Sample Warning Message for a Deprecated Profile

This example includes the selection of a new profile and the restart of the software download process.

```
Performing system sanity check ...
Warning: The current TCAM profile is 'npb-optimized-1'. This profile is not supported in
SLXOS
version 20.x.x. Please run the 'profile tcam' command to change to 'default'. Note that
in 20.1.1,
if 'default' profile is chosen, the scale limit for PORT RL, BD/VLAN RL, UNK Unicast RL
(collectively)
scale limit will be reduced to 1.5K and scale for ACL will be reduced to 4K (MAC + IPv4).
Rules above
new scale limit will not be effective after upgrade to SLX version 20.x.x.

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure telnet
or SSH sessions be restarted.

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

device# configure terminal
Entering configuration mode terminal
device(config)# hardware
device(config-hardware)# profile tcam default
Warning: To activate the new profile config, please run 'copy running-config startup-
```

```
config'
followed by 'reload system.'

device(config-hardware)# end
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [y/n]: y

device#
device# firmware download fullinstall

Performing system sanity check ...

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure
telnet or SSH sessions be restarted.

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

Checking conditions for downloading to 20.x.x
System settings check passed (0).

You are running firmwaredownload with auto-reboot and auto-commit enabled. After the
firmware is
downloaded the system will reboot and commit firmware automatically.

Preparing for firmware download ...
```

## Sample Warning Message for a Merged Profile

This example includes the selection of a new profile and the restart of the software download process.

```
Performing system sanity check ...
Warning: The current TCAM profile is 'layer2-optimized-1'. This profile is merged to the
Default
TCAM profile in SLXOS version 20.1.1.
Please run the 'profile tcam' command to change to a suitable TCAM profile.

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure
telnet or SSH sessions be restarted.

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

device# configure terminal
Entering configuration mode terminal
device(config)# hardware
device(config-hardware)# profile tcam default
Warning: To activate the new profile config, please run 'copy running-config startup-
config'
followed by 'reload system.'

device(config-hardware)# end
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [y/n]: y
```

```
device#
device# firmware download fullinstall

Performing system sanity check ...

You are running firmware download with 'fullinstall' option.
This command will preserve startup-config file and license file across firmware download
and
auto-replay configs.
This command will cause a cold/disruptive reboot and will require that existing telnet,
secure
telnet or SSH sessions be restarted.

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

Checking conditions for downloading to 20.x.x
System settings check passed (0).

You are running firmwaredownload with auto-reboot and auto-commit enabled. After the
firmware is
downloaded the system will reboot and commit firmware automatically.

Preparing for firmware download ...
```

## SLX-OS Software Downgrade Considerations

- If a feature is new for the current version of your software, the feature will not function if you downgrade your version.
- Software downgrades to previous versions are prohibited when security parameters are configured for HTTPS support.
- CFM configurations are not compatible with versions earlier than SLX-OS 17r.2.01.
- To downgrade from a 64-bit to a 32-bit system or from 4.14x to 2.6x kernel versions, use the **`firmware download`** command with the **`fullinstall`** option.
- Before downgrading to a version that does not support RADIUS accounting, disable both login and command accounting.
- Before downgrading to a version that does not support RADIUS accounting, remove the source interface for the RADIUS configuration.
- After downgrading from an enhanced routing profile, perform an additional reload to ensure that the hardware profile is enabled.

Always refer to the release notes for compatibility information and for any restrictions about upgrades and downgrades under particular circumstances.

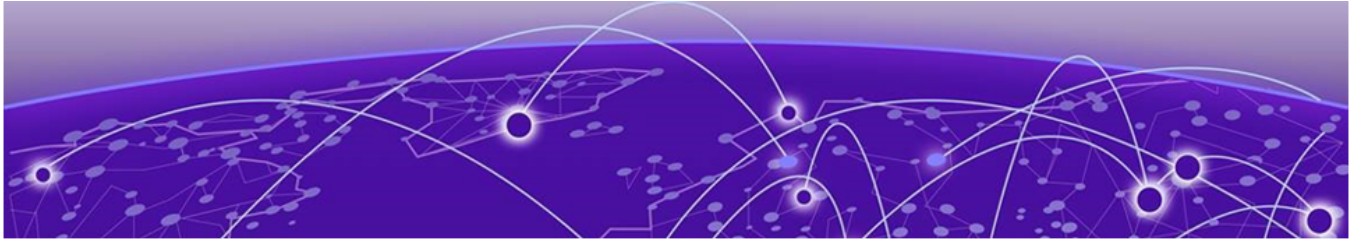
## SLX-OS Software Licenses

You can use the **`show license`** command to display the installed SLX-OS licenses.

This examples shows the licenses on an SLX 9640.

```
device# show license
Chassis:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       100G Port Upgrade license
       Feature name:PORT_100G_UPGRADE
       Capacity: 8
```

```
       License is Node-Lock and valid
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       Advanced Features license
       Feature name:ADVANCED_FEATURES
       License is Trust Based
       EULA acceptance date: Thu Aug 23 02:13:08 2018
```



# Upgrading SLX-OS Software with ONIE

ONIE Overview on page 37
Upgrade the SLX-OS Software with ONIE on page 37
Update ONIE on page 43

## ONIE Overview

Open Network Install Environment (ONIE) is the 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 SLX device boots SLX-OS from the images stored on the hard disk of the device. Extreme Networks installs these images before shipping the SLX devices. ONIE also provides mechanisms to re-install or update SLX-OS if the normal software download process fails.

The **`firmware download`** command updates the ONIE image and diag OS images automatically as part of the process. You do not need to run the **`onie install`** and **`diag install`** commands to install the ONIE image and diag OS image.

The process supported by the **`firmware download`** command is not affected by this feature. The SLX-OS software is not updated to the snapshot partition during the normal upgrade process.

For more information about ONIE, see the Open Compute Project website.

## Upgrade the SLX-OS Software with ONIE

- Decide on a supported method of transferring the SLX-OS software (firmware).
  - Local or remote mounted file system, such as:
    - Prepared USB 3.0 disk inserted into the device
    - Remote NFS share mounted inside the ONIE shell
  - HTTP
  - FTP (anonymous server access only)
  - TFTP
- 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 may allow 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.
- For step 6, have a method of storing the recovered startup-config to an external server using SCP or a mounted USB device.

Perform the following steps from the serial console.

1. Access the ONIE Recovery Shell.
   a. Reboot the SLX device using the CLI or power-cycle.
   b. When the BIOS splash screen is displayed, repeatedly press the down arrow key to access the GRUB boot menu and stop the boot timer.
   c. Select **ONIE** from the first menu, and immediately press the down arrow to stop the boot timer.
   d. Select **ONIE: Rescue**, and press `Enter` when prompted.

      The ONIE shell opens. At this point, you can use ONIE for recovering or upgrading the SLX device.
2. If you have a DHCP server running on the network, skip to step 5.
3. If you are using a USB 3.0 device to recover the SLX, skip to step 7.
4. Configure static networking on eth0 for ONIE.
   a. Add the IP address to the eth0 interface using the **ip addr add / dev eth0** command.

      ```
      ONIE:/ # ip addr add 10.25.101.199/22 dev eth0
      ```

   b. Configure the default gateway using the **ip route add default via <GATEWAY>_IP dev eth0** command.

      ```
      ONIE:/ # ip route add default via 10.25.100.1 dev eth0
      ```

5. Check network connectivity to the server hosting the software.
   a. Ping the remote server that will be used to transfer the software.

      ```
      PING 10.25.101.61 (10.25.101.61): 56 data bytes
      64 bytes from 10.25.101.61: seq=0 ttl=64 time=0.259 ms
      64 bytes from 10.25.101.61: seq=1 ttl=64 time=0.252 ms
      64 bytes from 10.25.101.61: seq=2 ttl=64 time=0.300 ms
      64 bytes from 10.25.101.61: seq=3 ttl=64 time=0.291 ms
      64 bytes from 10.25.101.61: seq=4 ttl=64 time=0.247 ms

      --- 10.25.101.61 ping statistics ---
      5 packets transmitted, 5 packets received, 0% packet loss
      round-trip min/avg/max = 0.247/0.269/0.300 ms
      ```

b. If the ping fails, use the **ip addr**, **ip route show**, and **ifconfig** commands to gather information on the connection state, and then resolve the issue using the commands in step 4.



**Note**
If you plan to use a network-based recovery (such as NFS, FTP, HTTP, or TFTP), ensure that the network is operational and that the host with the software is reachable before proceeding with the rest of this procedure.

6. (Optional for SLX 9250, SLX 9150, Extreme 8720, and Extreme 8520 only) Recover the startup-config file if you have no backups.

   You cannot perform this step if you have started the **onie-nos-install** command.

   a. Run the **mkdir /slxfs** and **mount /dev/sda6 /slxfs** commands.

      You may see a warning, but the file system should mount.

```
ONIE:/ # mkdir /slxfs
ONIE:/ # mount /dev/sda6 /slxfs
EXT4-fs (sda6): couldn't mount as ext3 due to feature incompatibilities
ONIE:/ #
```

   b. Copy the startup-config to the USB 3.0 device or remote server using the appropriate command and information.

```
ONIE:/ # scp /slxfs/var/config/vcs/scripts/startup-config
user@10.25.101.61:~/device.cfg
Host 10.25.101.61 is not in the trusted hosts file.
Do you want to continue connecting? (y/n) y
user@10.25.101.61's password:
startup-config                                        100% 8451     8.3KB/s
00:00
ONIE:/ # cp /slxfs/var/config/vcs/scripts/startup-config
/media/brocade/config/device.cfg
ONIE:/ #
```

   c. Unmount the SLX OS partition using the **umount /slxfs** command.

      Ensure that the console session is at the root of the file system before running the **umount** command.



**Note**
Steps 7-11 describe the options for recovery. Choose one, depending on whether you configured networking or are using the USB 3.0 device. For SLX 9540 devices, use only the NFS or USB-based recovery. These devices do not support the **onie-nos-install** command.

7. Perform a USB disk-based recovery.
   a. On a computer, download and decompress the software tarball using the recommended tools.
   b. Transfer the resulting directory to an inserted USB 3.0 device.
   c. Eject or unmount the USB device and insert it into the correct port of the SLX device.

d. Run the **fdisk -l** command, and locate the device identifier of the inserted USB device.

The USB device is generally the last device listed. In the following example, `/dev/sdb` is the USB device, and `/dev/sdb1` is the main partition you are working with.

```
ONIE:/ # fdisk -l
Disk /dev/sda: 128.0 GB, 128035676160 bytes
256 heads, 63 sectors/track, 15505 cylinders
Units = cylinders of 16128 * 512 = 8257536 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/sda1               1       15506   125034839+ ee EFI GPT
Disk /dev/sdb: 123.0 GB, 123010547712 bytes
47 heads, 3 sectors/track, 1703936 cylinders
Units = cylinders of 141 * 512 = 72192 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/sdb1                  15     1703936   120126464  83 Linux
ONIE:/ #
```

e. Run the **mkdir /media** and **mount /dev/ /media** commands.

You may see a warning, but the disk should mount.

```
ONIE:/ # mkdir /media
ONIE:/ # mount /dev/sdb1 /media
EXT4-fs (sdb1): couldn't mount as ext3 due to feature incompatibilities
ONIE:/ #
```

f. Change directory into the SLX-OS software that you want to install and start the installation using the `onie-nos-installer file://` or the **./install_pbr/onie-installer-avalanche** command.

g. Select the binary file for the SLX device you are working on.



**Note**

For SLX 9640 devices, you must select the `SLXOS_SWBD4001-20.1.1-ONIE.bin` file.

```
ONIE:/ # cd /media/brocade/firmware/slxos20.1.1
ONIE:/media/brocade/firmware/slxos20.1.1 # ls
SLXOS_SWBD3006-20.1.1-ONIE.bin
SLXOS_SWBD4001-20.1.1-ONIE.bin
SWBD2500
SWBD2900
SWBD4000
breeze_tools
breeze_tools.tgz
common
install_cr
install_pbr
libbrcmsdk.a.SWBD3006.tgz
libbrcmsdk.a.SWBD4000.tgz
libbrcmsdk.a.SWBD4001.tgz
oss-binaries-x86_64-ubuntu-14.04-rootfs.tar.gz
preinst
pubkey.pem
release.xlist
signature2.tar
signature2.tar.sig
slx20.1.1_mib.tar.gz
slx20.1.1_proto_models.tar.gz
```

```
slx20.1.1_yang.tar.gz
ONIE:/media/brocade/firmware/slxos20.1.1 # onie-nos-install
file://SLXOS_SWBD3006-20.1.1-ONIE.bin
discover: Rescue mode detected. No discover stopped.
<further output omitted>
```

The SLX device reboots and loads into SLX-OS with no further user input.

8. Perform an NFS-based recovery.
   a. On a Linux device, configure a NFS share, download and decompress the software tarball using the recommended tools, and move the resulting directory to the root of the NFS share.
   b. On the SLX device, configure and verify network connectivity to the server.
   c. Run the **`mkdir /media`** and **`mount :/path/to/nfs/share/ /media`** commands.

      If you get an error, troubleshoot the mount command. You may need more parameters or a more explicit path.

      ```
      ONIE:/ # mkdir /media
      ONIE:/ # mount -o tcp,nolock,rsize=32768,wsize=32768 10.31.2.100:/builds/
      /media
      ONIE:/ #
      ```

   d. Change directory into the software you want to install, and start the installation using the `onie-nos-installer file://` or the **`./install_pbr/onie-installer-avalanche`** command.
   e. Select the binary file for the SLX device you are working on.

      **Note**
      For SLX 9640 devices, you must select the `SLXOS_SWBD4001-20.1.1-ONIE.bin` file.

      ```
      ONIE:/ # cd /media/slxos/slxos20.1.1/slxos20.1.1/
      ONIE:/media/slxos/slxos20.1.1/slxos20.1.1 # ls
      SLXOS_SWBD3006-20.1.1-ONIE.bin
      SLXOS_SWBD4001-20.1.1-ONIE.bin
      SWBD2500
      SWBD2900
      SWBD4000
      breeze_tools
      breeze_tools.tgz
      common
      install_cr
      install_pbr
      libbrcmsdk.a.SWBD3006.tgz
      libbrcmsdk.a.SWBD4000.tgz
      libbrcmsdk.a.SWBD4001.tgz
      oss-binaries-x86_64-ubuntu-14.04-rootfs.tar.gz
      preinst
      pubkey.pem
      release.xlist
      signature2.tar
      signature2.tar.sig
      slx20.1.1_mib.tar.gz
      slx20.1.1_proto_models.tar.gz
      slx20.1.1_yang.tar.gz
      ONIE:/media/slxos/slxos20.1.1/slxos20.1.1 # onie-nos-install
      file://SLXOS_SWBD3006-20.1.1-ONIE.bin
      discover: Rescue mode detected. No discover stopped.
      <further output omitted>
      ```

This process takes approximately 15 to 20 minutes to complete. When the process is complete, the SLX reboots and loads into SLX-OS with no further user input.

9. (Not supported for SLX 9540) Perform an HTTP-based recovery.
   a. On a web server, download and decompress the software tarball using the recommended tools and move the resulting directory to the root of the web server.
   b. Modify the permissions of the directory to allow access for the web server daemon.
   c. Verify that the software directory is accessible by using a web browser to access the directory.
   d. On the SLX device, configure and verify network connectivity to the server.
   e. Run the **onie-nos-install http://<URL_TO_BIN>** command with the URL to the applicable binary for the SLX device.

```
ONIE:/ # onie-nos-install
http://10.25.101.70/slxos20.1.1/SLXOS_SWBD3006-20.1.1-ONIE.bin
discover: Rescue mode detected. No discover stopped.
Info: Attempting http://10.25.101.70/slxos20.1.1/SLXOS_SWBD3006-20.1.1
-ONIE.bin...
Connecting to 10.25.101.70 (10.25.101.70:21)
installer            100% ******************************|  1848M  0:00:00
ETA
ONIE: Executing installer: http://10.25.101.70/slxos20.1.1/SLXOS_SWBD3006-
20.1.1-ONIE.bin
<further output omitted>
```

10. (Not supported for SLX 9540) Perform an FTP-based recovery.
    a. On an FTP server, download and decompress the software tarball using the recommended tools and move the resulting directory to the root of the web server.

       Modify the permissions of the directory to allow access for the FTP server daemon. The FTP server must allow anonymous access.
    b. Verify that the software directory is accessible by using an FTP client to access the directory.
    c. On the SLX device, configure and verify network connectivity to the server.
    d. Run the **onie-nos-install ftp://<path/to/bin>** command with the URL to the applicable binary for the SLX device.

```
ONIE:/ # onie-nos-install
ftp://10.25.101.70/pub/slxos20.1.1/SLXOS_SWBD3006-20.1.1-ONIE.bin
discover: Rescue mode detected. No discover stopped.
Info: Attempting ftp://10.25.101.70/pub/slxos20.1.1/SLXOS_SWBD3006-20.1.1
-ONIE.bin...
Connecting to 10.25.101.70 (10.25.101.70:21)
installer            100%|******************************|  1848M  0:00:00
ETA
ONIE: Executing installer: ftp://10.25.101.70/pub/slxos20.1.1/SLXOS_SWBD3006-
20.1.1-ONIE.bin
<further output omitted>
```

11. (Not supported for SLX 9540) Perform a TFTP-based recovery.
    a. On a TFTP server, download and decompress the software tarball using the recommended tools and move the resulting directory to the root of the TFTP server.
    b. Modify the permissions of the directory to allow access for the TFTP server daemon.
    c. On the SLX device, configure and verify network connectivity to the server.

       TFTP may appear to be non-operational while it transfers the file.
    d. Run the **onie-nos-install tftp://<path/to/bin>** command with the URL to the applicable binary for the SLX device.

```
ONIE:/ # onie-nos-install tftp://10.25.101.60/slxos20.1.1/SLXOS_SWBD3006-
20.1.1-ONIE.bin
discover: Rescue mode detected. No discover stopped.
Info: Attempting tftp://10.25.101.60/slxos20.1.1/SLXOS_SWBD3006-20.1.1
-ONIE.bin ...
slxos20.1.1/SL   0% |                    |   873k            0:36:07 ETA
<output omitted>
ONIE: Executing installer: tftp://10.25.101.60/slxos20.1.1/SLXOS_SWBD3006-
20.1.1-ONIE.bin
<further output omitted>
```

## Update ONIE

Sometimes it is required that the ONIE, ONIE-GRUB, and DIAG be updated to the latest available versions. Use the **update onie** command from the SLXOS CLI to update the above. The SLXOS device will reboot thrice during this upgrade process.



**Note**
This action is only available for SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720 devices.

From the *Privileged EXEC Mode* prompt execute the **update onie** command and provide the appropriate parameters.

```
SLX# update onie sftp host 10.10.10.23 user ftpuser password password directory /home/
ftpuser/binaries/ filename onie-updater-x86_64-quanta_dnv-r0-14-ix8t_3abca
```

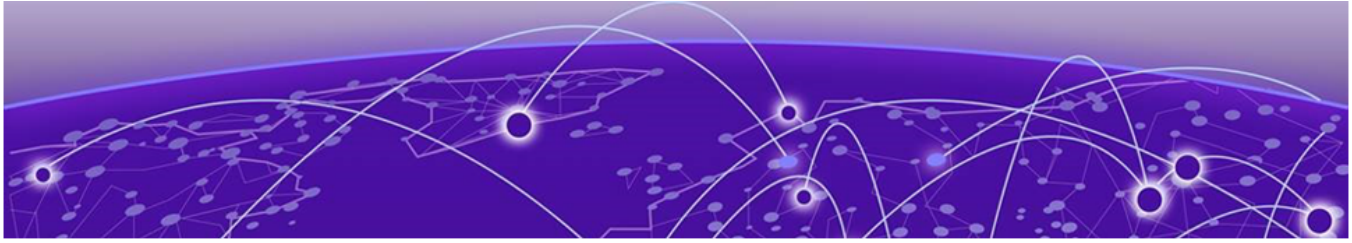


**Warning**
The ONIE upgrade will be aborted if the ONIE file download fails.

The upgrade process will download the file and then reboot the device for its first of three reboots.

After booting into to the *ONIE: Rescue* mode, the ONIE update process will automatically install ONIE and DIAG. On successful completion of this step, the upgrade process reboots the device for its second of three reboots.

Post the second reboot, ONIE-GRUB is installed and the SLXOS device is rebooted a final time.



# Installing the SLX-OS TPVM Package


TPVM Installation Overview on page 44
Prepare to Upgrade the SLX-OS TPVM Package on page 47
Install the SLX-OS TPVM Package on page 48
Installing TPVM Using tpvm deploy on page 49
Upgrading TPVM on page 50


## TPVM Installation Overview

The TPVM package is available separately from the SLX-OS software, and may be downloaded from the SLX-OS Release Server. This decoupling enables faster turnaround on enhancements and bug fixes, while reducing the file size of the SLX-OS distribution.

The TPVM firmware package is not updated as a part of a subsequent SLX-OS release firmware download. The TPVM firmware package installation procedure is independent of the SLX-OS release upgrade procedure. Manually copy the TPVM firmware package compatible with the SLX-OS release, uninstall the existing TPVM firmware, and install the new TPVM firmware package.

When you perform a fresh install of TPVM on a device, the installation creates a disk and partition separate from the TPVM root disk. The disk is visible as **vdb**, and the partition is **vdb1**. This configuration remains after the uninstallation of TPVM, and is used for subsequent TPVM installations. If the disk is deleted using **tpvm uninstall force** or **tpvm remove vdb**, then the next installation will create a new disk and partition.

If you have already installed a TPVM version and plan to upgrade to the next SLX-OS release version, it is recommended that you first uninstall the current TPVM firmware. Once a subsequent SLX-OS release firmware download is completed, install the TPVM firmware package that is compatible with that SLX-OS release. This option avoids TPVM firmware incompatibility with subsequent SLX-OS release firmware. In case of an upgrade to the next SLX-OS release, the current TPVM firmware remains installed and functioning.

Execute the **tpvm install** command to install the package.

**Important**
The installation is disruptive, and any data saved on the TPVM partition is erased. You must save any data manually before executing the **tpvm install** command.

You may also use the **tpvm-deploy** command to install and configure TPVM and the Insight Interface.

**Important**
From SLX-OS version 20.4.1 onwards, incremental upgrade of TPVM can be performed using the special TPVM Debian image. This file's name starts with *tpvm_inc_upg* followed immediately by the TPVM version number. This image cannot be used to perform a fresh install of TPVM. For more information on incremental upgrade, see Upgrading TPVM on page 50.
This is the TPVM incremental upgrade file name for version 4.7.1.

```
tpvm_inc_upg-4.7.1-1.amd64.deb
```

To perform a fresh TPVM install, download and use the full TPVM Debian image. This file name starts with *tpvm* followed immediately with the TPVM version number.
This is the full TPVM installation file name for version 4.7.1.

```
tpvm-4.7.1-0.amd64.deb
```

## Using tpvm deploy

*Command Overview*

The `tpvm deploy` command performs the following installation and configuration operations:

- Installation of TPVM
- TPVM Networking set up
- Enable Passwordless ssh to TPVM from `root@slx`
- Enable passwordless **sudo** inside TPVM
- Set the TPVM password for the default administrator-level account
- Set TPVM autoboot
- Start or boot the TPVM

**Note**
SLX 20.1.2 and later releases have the flexibility to run either `tpvm-3.0.0` or `tpvm-4.0.0`. The default administrator passwords are different for each version. `tpvm-3.0.0` uses `admin/password`, and `tpvm-4.0.0` uses `extreme/password`.
SLX 9540 is upgraded from hypervisor mode to bare metal mode in 20.2.x.

Prerequisites and considerations when using the `tpvm deploy` command:

- Extracted TPVM Debian package image – available in the `/tftpboot/SWBD2900` folder. If TPVM is already installed, skip this step.
- An Advanced Features License. Use the following command to activate the license: `license eula accept ADVANCED_FEATURES`.
- SLX 20.1.2 and later releases have the flexibility to run either `tpvm-3.0.0` or `tpvm-4.0.0`. Either one of the TPVM Debian package images can be copied to `/tftpboot/SWBD2900` and installed using `tpvm install` or `tpvm deploy`. However, it is recommended that only one TPVM Debian package image (the desired version tpvm) exists under `/tftpboot/SWBD2900` before executing `tpvm install` or `tpvm deploy`.

*TPVM Installation*

Verify the presence of the TPVM firmware package in the SLXVM `/tftpboot/SWBD2900` directory. If the latest version is not there, download before running the `TPVM deploy` command.

The `tpvm deploy` command begins with the standard TPVM installation.

*TPVM Networking Setup*

TPVM has two ethernet interfaces `eth0` and `eth1`. When using **`tpvm install`** the default setting is eth0 and DHCP. When using the **`tpvm deploy`**, the user can specify the interface to use `eth0` or `eth1` and set it to use either DHCP or specify an IP/netmask and gateway. In either case, the unused interface it set to manual mode without any IP configuration.



**Note**
The user can manually configure or override these settings by logging into the TPVM via **`ssh`** or **`tpvm console`** and manually modifying the linux network configuration.

*Passwordless SSH*

The passwordless parameter within `tpvm deploy` allows you to configure ssh access from the root user account on the SLX-OS to TPVM without a password. For example:

```
root@SLX# ssh -o "StrictHostKeyChecking no" extreme@10.23.30.153
```

When using the passwordless parameter, note the following:

- Passwordless ssh capability will be retained across firmware downgrade and upgrade.
- Passwordless ssh capability is lost in the case of a netinstall where `tpvm deploy` is used, regardless of whether TPVM is reinstalled or retained from previous install.
- The SLX-OS must be running and a compatible version of TPVM currently installed.

*Passwordless SUDO*

The TPVM default user is admin with `sudo` privileges. The `tpvm deploy` command configures TPVM so that `sudo` for this user does not ask for a password. Once set, this parameter persists for the lifetime of the TPVM.

If not set, the default behavior requires a password for `sudo` activities, as dictated by the Ubuntu 18.04 LTS Server Operating System.

*TPVM Password*

The `tpvm-4.0.0` package ships with SLX-OS 20.1.2 and uses `extreme/password` as the default login credential. To automate the TPVM setup and achieve one touch provisioning of TPVM, this optional parameter sets the password for the TPVM admin user account. Once set, this parameter persists for the lifetime of the TPVM.

**Note**
The `tpvm-3.0.0` package can be used/installed with SLX-OS 20.1.2. If you are using this TPVM package, note that the default login credentials are `admin/password`.

*TPVM Auto-boot*

This option restarts the TPVM image automatically in subsequent reboots, such as an SLX-OS start on a Baremetal platform.

*TPVM Start*

After configuring the TPVM, `tpvm deploy` starts TPVM. A reboot of the SLX-OS also reboots the TPVM.

## Prepare to Upgrade the SLX-OS TPVM Package

Perform the following tasks so that in the unlikely event of a failure or timeout, you can provide your router support provider the information needed to troubleshoot the problem.

1. Ensure that all production traffic is detoured from the device that is undergoing the upgrade.
2. Verify network connectivity, which will allow the **`scp`** or **`ftp`** command to complete the firmware download of the software image to the device.

```
# ping <server_address>  vrf [mgmt-vrf|default-vrf|<vrf_name>]
```

3. Ensure that the console you use to perform the upgrade has access to the device.
4. Save the `startup-config` file to a remote server.

```
# copy running-config tftp://@<server_address>/<filename> use-vrf [mgmt-vrf|default-vrf|<vrf_name>]
```

5. Run the following commands to collect the system context.

```
show version
show chassis
show environment fan
show environment power
show environment history
```

```
show environment sensor
show environment temp
show interface status
show license
show firmwaredownloadhistory
show firmwaredownloadstatus
show media
show run
```

## Install the SLX-OS TPVM Package

In the unlikely event that installation fails or times out, provide your router support provider the information you prepared in Prepare to Upgrade the SLX-OS TPVM Package on page 47.

**Important**

Use the `CTRL+\` key combination to return to the SLX-OS CLI from the LINUX shell.

1. Log in to the SLX device as a user with an administrative role.
2. Verify that the ADVANCED_FEATURES license exists.

```
device# show license
```

3. Copy the TPVM package to the flash drive of the SLX device using any applicable method. Use the below SLX command to download the TPVM package to the switch's flash drive.

```
SLX# tpvm download sanity yes host 10.6.46.51 directory /buildsjc/
sre_fusion/Nightly/raphael/slxos20.4.1/slxos20.4.1_220325_1800/dist/SWBD2900 filename
tpvm-4.5.0-1.amd64.deb user fvt password pray4green protocol scp
2022/04/18-12:49:04, [DCM-1454], 2310,, INFO, SLX, Operation:download mode:sync
started.
Starting TPVM download, please DO NOT press CTRL+C
```

4. Install the TPVM package.

```
device# tpvm install
Installation starts. To check the status use 'show tpvm status' command
device# show tpvm status
SSH and Sudo passwordless :Disabled
AutoStart :Disabled
Tpvm status :Installed
device#
```

After you run the **`tpvm install`** command, it can take a few minutes for TPVM to be provisioned and show as installed in the **`show tpvm status`** output.

5. Start TPVM.

```
device# tpvm start
start succeeds
device# show tpvm status
SSH and Sudo passwordless :Disabled
AutoStart :Disabled
Tpvm status :Running
device#
```

If the networking setup is DHCP (default or explicitly specified) and if the DHCP server doesn't assign a IP (or is not reachable) to the TPVM interface, the bootup may take several minutes

6. Access the TPVM console.

```
device# tpvm console
...
device#
```

7. Use the CTRL+\ key combination to return to the SLX-OS CLI.
8. (Optional) Configure TPVM to boot automatically when the SLX device is operational.

```
device# tpvm auto-boot enable
```

By default, TPVM is not automatically booted when the SLX device is operational.

## Installing TPVM Using tpvm deploy

1. Switch to the Linux shell from the SLX-OS CLI.

```
SLX# start-shell
```

2. Enter the Linux admin user shell.

```
[admUser@SLX]# su
             password: <password>
```

The default password is "extreme".

3. Remove the existing TPVM package at the following path in the device's SLX-OS VM, at the Linux shell login prompt.

```
[admUser@SLX]# rm -rf /tftpboot/SWBD2900/tpvm-3.0.0.amd64.deb
```

4. Using SCP or FTP, copy the new TPVM package that is compatible with the SLX-OS release from the release server, and copy it to the SLX-OS VM /tftpboot/SWBD2900/ folder.
5. Return to the SLX-OS CLI shell.

```
[root@SLX]# exit
[admUser@SLX]# exit
```

6. Stop TPVM if it is running.

```
SLX# tpvm stop
```

7. Uninstall existing TPVM firmware.

```
SLX# tpvm uninstall
```

8. Use tpvm deploy to configure the network and management settings, and install TPVM.

```
SLX# tpvm deploy mgmt ipaddr 10.25.101.121/22 gw 10.25.100.1 admin-pwd mypassword
confirm mypassword
Starting TPVM deploy CLI, please DO NOT hit CTRL+C
Tpvm install started
..Tpvm is installed
Tpvm set_ip succeeds
Tpvm password succeeds
auto-boot enable succeeds
Tpvm is started
```

Above is one example of using TPVM deploy. The following are additional examples.

- Eth0 with DHCP and passwordless login

```
SLX# tpvm deploy mgmt dhcp allow-pwless
```

- Eth1 with static IP, default gateway and passwordless login

```
SLX# tpvm deploy insight ipaddr 10.10.10.1/24 gw 10.10.10.100 allow-pwless
```

- Eth1 with static IP, default gatway, passwordless login and new TPVM password setup

```
SLX# tpvm deploy insight ipaddr 10.10.10.1/24 gw 10.10.10.100 allow-pwless admin-
pwd admin123 confirm-pwd admin123
```

- Eth0 with static IP, default gateway, passwordless login and new TPVM password setup

```
SLX# tpvm deploy mgmt ipaddr 10.10.10.1/24 gw 10.10.10.100 allow-pwless admin-pwd
admin123 confirm-pwd admin123
```

- Eth1 with Static IP, default gateway

```
SLX# tpvm deploy insight ipaddr 10.10.10.1/24 gw 10.10.10.100
```

## Upgrading TPVM

The installed instance of TPVM can be upgraded fully or incrementally when upgrading/downgrading TPVM. When upgrading/downgrading TPVM, it was required that TPVM be re-installed completely and its configuration was later restored from configuration persisted during the upgrade process. The general full upgrade process was to download the TPVM file to the SLX device. Once the download is successful, the existing TPVM instance was stopped and a snapshot taken. Post this, the TPVM was uninstalled. The new version of TPVM was then installed and its configuration restored from stored configuration.

From SLXOS version 20.4.1 onwards, support for incremental upgrade is available. When incrementally upgrading TPVM, the TPVM image is downloaded, along with the OS packages, updated scripts, and XML files. The existing TPVM installation is stopped, and the OS packages are updated first, followed by replacement of existing scripts and XML files. The last upgrade step is to upgrade the TPVM itself.



**Note**

The default installation mode for SLXOS version 20.4.1 is full upgrade. You must explicitly use the *incremental* keyword with the **tpvm upgrade** command to perform incremental upgrade. All SLXOS versions before 20.4.1 supported full install only.

Snapshot of the TPVM instance is not taken when performing incremental update.

When incrementally upgrading TPVM, the following requirements must be met:

- A minimum of 1Gb space must be available for TPVM upgrade.
- The existing installation of TPVM must be running for incremental upgrade to work.
- The minimum required TPVM version is 4.5.0 and the minimum SLXOS version is 20.4.1. If these constraints are not met, you must perform full installation of TPVM.

When TPVM upgrade fails, the following actions are performed to restore the previous installation:

- The old Scripts and XML files are restored from backup.
- The TPVM instance is restored from the snapshot (if available and only for full installations). For incremental upgrade, the updated OS files are replaced with the older copies.
- Log entries are created with the failure reasons.

This example shows the command to perform an incremental upgrade of TPVM.

```
SLX# tpvm upgrade incremental directory /proj/tpvm_upgrade/ filename
tpvm_inc_upg-4.5.0-0.amd64.deb host 10.10.10.1 user fav password testpassword protocol
scp use-vrf mgmt-vrf
```

This example shows the command to perform a full installation of TPVM.

```
SLX# tpvm upgrade directory /proj/tpvm_upgrade/ filename tpvm-4.5.0-0.amd64.deb host
10.10.10.1 user fav password testpassword protocol scp use-vrf mgmt-vrf
```