



Extreme SLX-OS Security Hardening Guide, 20.5.2a

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

9037850-01 Rev AA
September 2023



Copyright © 2023 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: www.extremenetworks.com/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/>

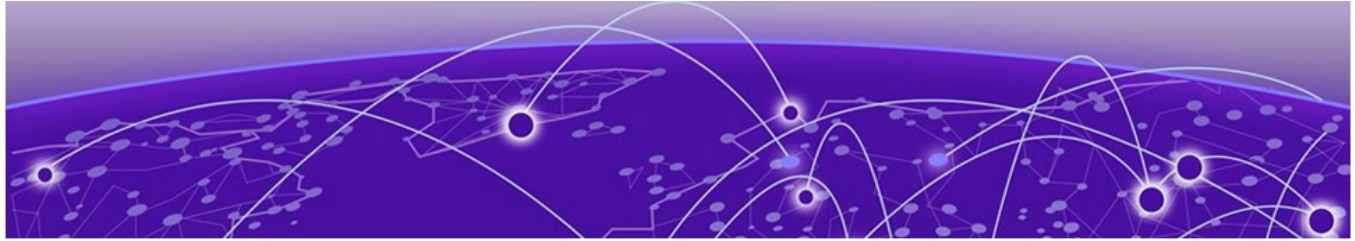


Table of Contents

Preface.....	4
Text Conventions.....	4
Documentation and Training.....	5
Open Source Declarations.....	6
Training.....	6
Help and Support.....	6
Subscribe to Product Announcements.....	7
Send Feedback.....	7
About this document.....	8
What's New in this Document	8
Supported Hardware.....	8
Security Hardening Guide.....	10
Security Hardening Guidance Overview.....	10
Configure password policies.....	10
Administrator logout.....	11
SSH Configuration.....	11
Disable TLS 1.1 and older.....	13
Enable authentication services	14
Disable unused remote authentication services.....	15
Configure IP ACLs to block services.....	15
Configure banners.....	15
Support for RSA 4096 bit SSH hostkey.....	15
Connlimit as an option for ip access-lists.....	16
Version control for TLS.....	16
Securing GNMI.....	16
Mutual authentication support for TLS.....	16
Certificate expiry alert levels and period configuration.....	16
User account expiry period configuration upon inactivity.....	16
Forcing default users password change.....	16
GRUB Bootloader Password Protection.....	16
Measured boot and Remote Attestation.....	16
Security Enhanced Linux (SE Linux).....	16



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 ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






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

Table 2: Text

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products
[Extreme Optics Compatibility](#)
[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

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

Training

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

Help and Support

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

[Extreme Portal](#)

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

[The Hub](#)

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

[Call GTAC](#)

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

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

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

Subscribe to Product Announcements

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

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

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

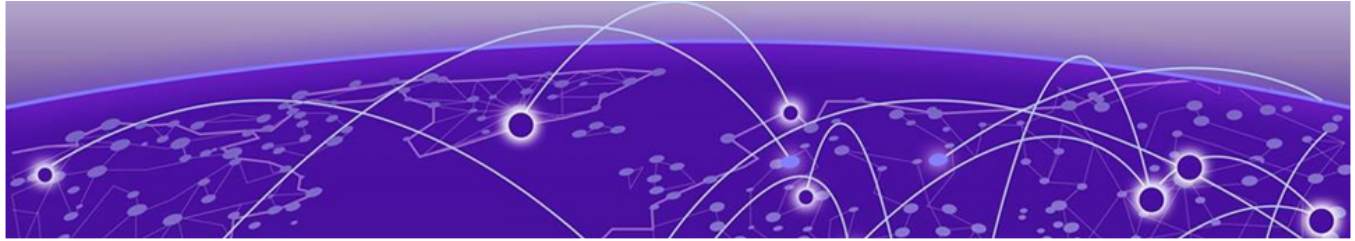
Send Feedback

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

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

To send feedback, email us at 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 8

[Supported Hardware](#) on page 8

What's New in this Document

This document is released with the SLX-OS 20.5.2a software release. No changes were made to this document for this version.

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

Supported Hardware

SLX-OS 20.5.2a 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.



Security Hardening Guide

[Security Hardening Guidance Overview](#) on page 10
[Configure password policies](#) on page 10
[Administrator logout](#) on page 11
[SSH Configuration](#) on page 11
[Disable TLS 1.1 and older](#) on page 13
[Enable authentication services](#) on page 14
[Disable unused remote authentication services](#) on page 15
[Configure IP ACLs to block services](#) on page 15
[Configure banners](#) on page 15
[Support for RSA 4096 bit SSH hostkey](#) on page 15
[Connlimit as an option for ip access-lists](#) on page 16
[Version control for TLS](#) on page 16
[Securing GNMI](#) on page 16
[Mutual authentication support for TLS](#) on page 16
[Certificate expiry alert levels and period configuration](#) on page 16
[User account expiry period configuration upon inactivity](#) on page 16
[Forcing default users password change](#) on page 16
[GRUB Bootloader Password Protection](#) on page 16
[Measured boot and Remote Attestation](#) on page 16
[Security Enhanced Linux \(SE Linux\)](#) on page 16

Security Hardening Guidance Overview

Configure password policies

This section details on how to configure the password policies.

The minimum password strength and configurable attributes are recommended that includes minimum length, character sets, with the number of retries when logging in. This record details on how long an account can be locked out when the maximum number of login failures is observed.

An example password policy configuration:

```
device(config)# password-attributes min-length 8
device(config)# password-attributes max-retry 4
```

```
device(config)# password-attributes max-lockout-duration 5000
device(config)# password-attributes character-restriction upper 1
device(config)# password-attributes character-restriction lower 2
device(config)# password-attributes character-restriction numeric 1
device(config)# password-attributes character-restriction special-char 1
```

The default password encryption policy is Encryption Level 10, which utilizes salted SHA512 for password storage.

Refer to the [Extreme SLX-OS Security Configuration Guide, 20.3.3](#), topic *Password Policies* for further details.

Administrator logout

This topic provides information about the administrator locout details.

By default, the administrator is not locked out of the device even after `max-retry` failures. To lock the administrator out, execute the below command:

```
device(config)# password-attributes admin-lockout
```

When the administrator is locked-out, the device allows access for the administrator after the value set for `max-lockout-duration` has elapsed.



Note

The administrator logs in over the serial port/console, which is never locked out and can login over the network again only if the `admin-lockout` password attribute is disabled.

To allow the administrator to login over the network and disable administrator lockout execute the below commands:

```
device# configure terminal
```

```
device(config)# no password-attributes admin-lockout
```

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – Password Policies](#) for further details

SSH Configuration

SSH ciphers

The following ciphers are recommended for the SSH client and SSH server:

- aes256-ctr
- aes256-cbc

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – Configure SSH Ciphers](#) for specific guidance configuring SSH ciphers.

SSH MAC algorithms

The following MAC algorithms are recommended for the SSH client and SSH server:

- `hmac-sha2-256`
- `hmac-sha2-512`

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – Configure SSH MAC](#) for specific guidance configuring SSH MAC algorithms.

SSH Key-exchange

The following MAC algorithms are recommended for the SSH client and SSH server:

- `ecdh-sha2-nistp256`
- `diffie-hellman-group14-sha1`

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – Configure SSH Key-exchange](#) for specific guidance configuring SSH Key-exchange algorithms.

SSH server timeout and login policies

Enter the `ssh server max-idle-timeout` command to set the timeout value for SSH connections to the server. This setting affects `ssh` connections to the server including the `netconf` sessions.

```
device(config)# ssh server max-idle-timeout 20
```

Enter the **`sshserver max-auth-tries`** command to set the number of login attempts

```
device(config)# ssh server max-auth-tries 2
```

Enter the **`sshserver max-login-timeout`** command to set the login timeout. Set the value to an appropriate timeout period in the administrator's environment.

```
device(config)# ssh server max-login-timeout 30
```

Configuring SSH session re-key interval by volume and time

The SSH servers can trigger re-keying once a certain time interval is reached or data traffic reaches a specified volume. During re-keying, a set of key exchange messages are transferred between the SSH client and the server, changing the key used for the session security.

Re-keying by volume

The **`re-key-volume`** option cannot exceed a value equal to 1024 MB. The default value is 1024 MB. The range of the rekey volume configured using the **`ssh-server`** command is 512 to 1024 MB.

```
device(config)# ssh server rekey-volume ? Possible completions:
```

```
<DECIMAL> <512-4095> Megabytes"
```

Re-keying by time

The SSH rekey can also be configured based on time. The default value is 3600 seconds. The following command is used to specify the time.

```
device(config)# ssh server rekey-interval ?Possible completions:
```

```
<DECIMAL> <900-3600> Seconds
```

Configure SSH authentication method

The SSH provides public key and password authentication methods, including support for X.509 v3 certificates.

To use SSH public-key authentication, enter the **certutil import sshkey directory pubkey-directory filename protocol SCP host remote-ip user user-account password password** command to import the public key.

```
device# certutil import sshkey user admin host 10.70.4.106 directory /  
users/home40/bmeenaks/.ssh file id_rsa.pub login fvt
```

```
Password: *****
```

```
2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX, Event: sshutil, Status:  
success, Info: Imported SSH public key from 10.70.4.106 for user  
'admin'.
```

To support password less SSH authentication, externally generated key pairs using RSA-2048.

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – Secure Shell](#) for further guidance configuring SSH authentication method.

Disable telnet server

Enter the **telnet server shutdown** command in global configuration mode to disable the Telnet server.

```
device(config)# telnet server shutdown
```

Disable TLS 1.1 and older

This topic details the procedure to disable TLS 1.1 and older versions.

1. SSH to the system and acquire a root shell:

```
SLX# start shell  
Entering Linux shell for the user: admin  
[admin@SLX]# su -  
Password:  
[root@SLX]#
```

2. Edit the Apache webserver config located at '/fabos/webtools/bin/web.conf.0' and replace the line that contains the 'SSLProtocol' variable with the following:

```
SSLProtocol -all +TLSv1.2
```

3. Grep the process table to look for `httpd` processes and kill the lowest numbered one (first in the list). For example:

```
# ps auxww |grep httpd
nobody    5046  0.0  0.0  88956  4220 ?        S    20:32   0:00
           /usr/sbin/httpd.0 -DSSL -f /fabos/webtools/bin/httpd.conf.0
root      24164 0.0  0.0  88688  6360 ?        Ss   01:59   0:14
           /usr/sbin/httpd.0 -DSSL -f /fabos/webtools/bin/httpd.conf.0
nobody    29385 0.0  0.0  88956  4220 ?        S    19:22   0:00
           /usr/sbin/httpd.0 -DSSL -f /fabos/webtools/bin/httpd.conf.0
# kill 5046
```

4. Restart Apache by manually executing the following command:

```
# /usr/sbin/httpd.0 -DSSL -f /fabos/webtools/bin/httpd.conf.0
```

5. At this point, SLX-OS will be running Apache with TLS < 1.2 disabled.



Note

The `httpd.conf.0` file includes the `web.conf.0` file automatically and there is no persistent change across reboots. However, this will be fixed in future SLX-OS release.

Enable authentication services

Enable HTTPS

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – HTTPS Certificates](#) for specific guidance on installing certificates and enabling HTTPS.

Enable TLS for remote authentication services

RADIUS over TLS and LDAP over TLS are supported.

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – RADIUS Server Authentication](#) for specific guidance on configuring RADIUS over TLS.

Reference the Extreme [SLX-OS Security Configuration Guide, 20.2.1 – Lightweight Directory Access Protocol](#) for specific guidance on configuring LDAP over TLS.

Enable TLS for SYSLOG

To enable secure logging using the `syslog` server, complete the following steps.

1. Enter the `crypto import syslogca` command in privileged EXEC mode to import the syslog CA certificate.

```
device# crypto import syslogca rbridge-id 1 protocol SCP host 10.2.2.101 directory
           /home/certs/ file chainCA02.cert.pem user admin password <password>
```

The CA certificate imported must be generated using RSA-2048 with SHA-256.

- Enter the `logging syslog-server ip-address` command in global configuration mode to configure the syslog server.

```
device(config)# logging syslog-server 10.20.238.120
                secure port 1999
```

The device enforces certificate validation during import and TLS server certificate validation occurs during the TLS handshake according to the following rules:

- Certificate validation and the certificate path validation support a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The certificate path should be validated by verifying the presence of the `basic Constraints` extension and that the CA flag is set to TRUE for all CA certificates.
- The revocation status of the certificate should be validated.
- For `SYSLOG`, the device currently requires that an IP address must be used for Common Name (CN) and Subject Alternative Name (SAN).

The `extendedKeyUsage` field should be validated according to the following rules:

- Certificates used for trusted updates and executable code integrity verification should have the Code Signing purpose (`id-kp 3` with OID `1.3.6.1.5.5.7.3.3`) in the `extended Key Usage` field.
- Server certificates presented for TLS should have the Server Authentication purpose (`id-kp 1` with OID `1.3.6.1.5.5.7.3.1`) in the `extended Key Usage` field.
- Client certificates presented for TLS should have the Client Authentication purpose (`id-kp 2` with OID `1.3.6.1.5.5.7.3.2`) in the `extended Key Usage` field.
- OCSP certificates presented for OCSP responses should have the OCSP Signing purpose (`id-kp 9` with OID `1.3.6.1.5.5.7.3.9`) in the `extended Key Usage` field.
- A certificate should only be treated as a CA certificate if the `basic Constraints` extension is present and the CA flag is set to TRUE.

Disable unused remote authentication services

Configure IP ACLs to block services

Configure banners

Support for RSA 4096 bit SSH hostkey

```
SLX(config)# ssh server key rsa ?
Possible completions:
[2048]
1024 1024 bits RSA key
2048 2048 bits RSA key [default]
4096 4096 bits RSA key
SLX(config)# ssh server key rsa 4096
```

The default **RSA** hostkey for **SSH** when the above hostkey is not configured, is **2048** bits.

The SLX provides the **SSH** server hostkey algorithms **RSA**, **ECDSA P256** and **DSA** to be configured. It's recommended to use only **ECDSA** or **RSA**(minimum **2048** bits) as the hostkeys **DSA** and **RSA 1024** are both insecure with **1024** bit length.

The **ECDSA** being the strongest algorithm, the OpenSSH server in SLX sends this as the hostkey if it is present. On a linux, the SSH client receives the following message to accept the hostkey sent by the SLX.

```
The authenticity of host 10.24.12.129 (10.24.12.129) can't be established.  
ECDSA key fingerprint is SHA256:LlgBLdBedpJ1AU6Gwa40Yjtye6JM4CfR8i8k2SwGOfw.  
Are you sure you want to continue connecting yes/no ?
```

If you remove ECDSA hostkey configured from SSH server key CLI , then the OpenSSH server in SLX negotiates **RSA** hostkey based on the bit length, which you configured using **ssh** server key **RSA** CLI.

The default being 2048 bits. Hence, you need to explicitly configure **ssh** server key **RSA 4096** to use the **RSA 4096** bit hostkey and remove **ECDSA** if it does not consider, so that the server sends **RSA 4096** as the hostkey.

Connlimit as an option for ip access-lists

Version control for TLS

Securing GNMI

Mutual authentication support for TLS

Certificate expiry alert levels and period configuration

User account expiry period configuration upon inactivity

Forcing default users password change

GRUB Bootloader Password Protection

Measured boot and Remote Attestation

Security Enhanced Linux (SE Linux)

Security-Enhanced Linux (SE Linux) is a Linux Kernel Module that enhances the security of SLXOS's underlying Linux OS. SE Linux works by providing security policies for access control at the operating system level. Support for Mandatory Access Control (MAC) is also available for use.

Security policies are a set of rules that implement access control restrictions for applications, processes, and files on the SLXOS's operating system. These rules are used by SE Linux to enhance security by preventing bypass of application security mechanism and enable containing the potential damages due to malicious or misbehaving applications.

Support for SE Linux is introduced in SLXOS version 20.4.1. As a part of this, MAC policy support for *SSHD* and *HTTPD* modules and their dependencies are added.

SE Linux has three modes of operation:

- In the *Disabled* mode, the operating system does not implement SE Linux policy and also does not label any persistent objects such as files. Not marking these persistent objects makes it harder to implement SE Linux in the future.
- In the *Permissive* mode, the operating system implements the SE Linux policy fully. All policy enforcement activities are logged. However, the policy is not enforced.
- In the *Enforcing* mode, the operating system implements the SE Linux policy completely including denying access, and activity logging.

SE Linux *Permissive* mode is enabled by default and cannot be changed.

**Note**

The last 1000 error log entries will be saved in the `INFRA.txt` file within the support save logs.

**Note**

This feature is enabled on all platforms of SLXOS.

Use the **show selinux status** command to verify the current SE Linux status.

```
SLX # show selinux status
SE Linux status:           enabled
SE Linuxfs mount:         /sys/fs/selinux
SE Linux root directory:  /etc/selinux
Loaded policy name:       mls
Current mode:             permissive
Mode from config file:    enforcing
Policy MLS status:        enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 31
```