CIS ExtremeNetworks SLX-OS-20.X.X Benchmark

v1.0.1 - 07-17-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)]()
- [CIS Benchmarks™ Certified 3rd Party Tooling]()

These tools make the hardening process much more scalable for large numbers of systems and applications.

> **NOTE**: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that *ALL* Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

> **When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.**

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completes successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

> **NOTE**: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite](#)® members.
>
> CIS-CAT® Pro is also available to CIS [SecureSuite](#)® members.

Target Technology Details

This document, Security Configuration Benchmark for Extreme Networks SLX OS, provides prescriptive guidance for establishing a secure configuration posture for Extreme Network switches running SLX OS version 20.6.3 or later. This guide was tested against SLX OS 20.6.3.

This is a development version and is meant to encourage the SLX-OS user community to test configurations and make recommendations.

To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at benchmarkinfo@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Extreme Networks SLX OS on an Extreme Networks routing and switching platforms.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as a defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

- **BGP Enabled**

  Use this profile when BGP is in use

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Recommendations

1 General Recommendations

1.1 Ensure the system is on a supported Network Operating System (Manual)

Profile Applicability:

- Level 1

Description:

Extreme Networks releases software releases periodically to close defects, upgrade security postures, and close security vulnerabilities. Customers are expected to be utilizing a supported software release.

Rationale:

Having up to date software is important for the security of your environment. Software defects, bugs, and vulnerabilities are patched in new software releases. Failing to update can result in a compromise to your network.

Audit:

Enter the following command

```
config#show version | in SLX-OS.*:
```

This command should display the following with the current version running on the device

```
device# show version | in SLX-OS.*:SLX-OS Operating System Version: 20.1.1
```

Remediation:

Update to the latest stable release

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.1 Ensure Network Infrastructure is Up-to-Date** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	🟢	🟠	🔵
v7	**11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices** Install the latest stable version of any security-related updates on all network devices.	🟢	🟠	🔵

1.2 Configure Host Name (Automated)

Profile Applicability:

- Level 1

Description:

Extreme Networks switches ship with a default host name. The host-name property should be set up to be unique name on the management network. This enables the switch to be resolved with a unique FQDN.

Rationale:

Assigning a unique hostname allows you to pinpoint what device you are looking for in logs and prevents confusion when a security incident happens.

Audit:

```
config#show system | in Unit.*:
```

Remediation:

```
SLX#config terminal
SLX(config)#switch-attributes host-name new_switch
SLX(config)#end
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.3 Ensure that the Default Chassis Name is changed (Manual)

Profile Applicability:

- Level 1

Description:

It is incredibly important to change default ID's to ensure that they are not easily compromised from an attacker.

Rationale:

The default name of the chassis is the product model. This should be changed

Audit:

```
SLX#show chassis | in Chassis.*Name:
```

Remediation:

```
SLX#config terminal
SLX(config)#switch-attributes chassis-name new_switch
SLX(config)#end
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2 System Configuration

The system configuration benchmark section applies to the Global Config of the switch.

2.1 Banner Configuration

2.1.1 Login Banner (Automated)

Profile Applicability:

- Level 1

Description:

An approved use notification, in the form of a Login Banner, should be displayed before granting access to the switch. Such a banner ensures that the privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Rationale:

Audit:

```
SLX# show running-config | in banner
```

Remediation:

```
SLX(config)# banner login "Please do not disturb the setup on this switch"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2 Password Configuration

2.2.1 Change default username and password (Manual)

Profile Applicability:

- Level 1

Description:

Extreme switches have a default username and password. These need to be changed from their default values.

Rationale:

Changing the default username and password is critical for maintaining the security of any system. Here's why it's important:

- Prevent Unauthorized Access: Default credentials are well-known to attackers, making it easy for them to gain access to systems that use default usernames and passwords. Changing these credentials significantly reduces this risk.
- Improve Security Posture: Customized usernames and strong, unique passwords add an additional layer of security, making it harder for attackers to guess or brute-force their way into your system.
- Compliance: Many security standards and regulations require changing default credentials as a basic security measure. Adhering to these requirements helps in achieving compliance and avoiding potential penalties.
- Reduce Attack Surface: Using default credentials increases the attack surface of your system. By changing them, you reduce the number of potential entry points for attackers.
- Protection of Sensitive Data: Default credentials can expose sensitive data to unauthorized users. Changing them ensures that only authorized personnel have access to important information.

By updating default usernames and passwords, you enhance your system's security, protect sensitive data, and comply with regulatory standards, ultimately maintaining a safer and more secure environment.

Audit:

```
SLX# show running-config | in username.*password
```
Sample output:

```
SLX# show running-config | in username.*password
username admin password
6$mAog0c./JxVGu1zy$6wFogQmek0KOEgTav.0DVKXz1vRodc1UCAbipYft/DWnT5R6/Y3qpq7V3J
HlhRNVtwguLgXnzdtBDKPKaXbBg/ encryption-level 10 role admin desc
Administrator
username user password
$6$mAog0c./JxVGu1zy$6wFogQmek0KOEgTav.0DVKXz1vRodc1UCAbipYft/DWnT5R6/Y3qpq7V3
JHlhRNVtwguLgXnzdtBDKPKaXbBg/ encryption-level 10 role user desc User
SLX#
```

Remediation:

```
password_digest = ^username.admin.(*).encryption-level
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.7 Manage Default Accounts on Enterprise Assets and Software** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.2 Change Default Passwords** Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

2.2.2 Ensure Password complexity is configured (Automated)

Profile Applicability:

- Level 1

Description:

It is prudent to use a minimum length to 14 characters. Maximum length should be as long as possible based on system constraints

Rationale:

Password composition or complexity requirements are often used to increase the strength of a user-created password of a given length. For example, a complex password would need some number of characters from all three of the following categories: • Uppercase characters • Lowercase characters • Non-alphabetic characters such as numbers or special characters like <*&(^%$>!: While there is no standard for password composition in use today, it is very common for these requirements to vary from system to system (e.g., system one allows special characters, but system two does not). Using a radius system to manage logins will decrease the need to have actual passwords and username on the device. Generally, it is recommended to have 1 emergency account on the device with the password stored in a secure location to use in case of loss of communication with the Radius servers.
This password should be changed after every use.

Audit:

```
SLX#show running-config | in password
```

Remediation:

```
SLX(config)# password-attributes min-length 8
SLX(config)# password-attributes max-retry 4
SLX(config)# password-attributes character-restriction upper 1
SLX(config)# password-attributes character-restriction lower 2
SLX(config)# password-attributes character-restriction numeric 1
SLX(config)# password-attributes character-restriction special-char 1
```

References:

1. https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2** <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4** <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.3 TLS Version

2.3.1 Ensure system is running TLS 1.2 or later (Manual)

Profile Applicability:

- Level 1

Description:

Ensuring secure data transmission is crucial in our digital age. TLS 1.2 stands out by offering advanced encryption algorithms, improved key exchange mechanisms, and enhanced protection against known vulnerabilities. This level of security ensures the privacy and integrity of sensitive information transmitted over the internet. As a result, most modern browsers and services now mandate the use of TLS 1.2 or higher for secure connections.

Rationale:

Using TLS 1.2 or higher is crucial for ensuring secure and reliable communication over the internet. Here's why it's so important:

- Enhanced Security: TLS 1.2 and higher versions incorporate stronger encryption algorithms and improved cryptographic techniques, making it much harder for attackers to intercept and decipher data.
- Protection Against Vulnerabilities: Older versions like TLS 1.0 and TLS 1.1 have known vulnerabilities that can be exploited by attackers. TLS 1.2 and higher provide better defenses against these threats, ensuring that data remains secure during transmission.
- Compliance with Standards: Many regulatory frameworks and security standards now require the use of TLS 1.2 or higher. Adopting these versions helps organizations stay compliant and avoid potential legal and financial penalties.
- Interoperability with Modern Systems: Most modern browsers, servers, and applications require TLS 1.2 or higher to establish secure connections. Using outdated protocols can lead to compatibility issues and interrupted service.
- Improved Performance: Newer versions of TLS offer optimizations that can enhance performance, providing faster and more efficient secure connections.

Overall, migrating to TLS 1.2 or higher is essential for maintaining robust security, ensuring regulatory compliance, and achieving seamless interoperability with contemporary technology.

Audit:

```
SLX# show running-config management-security
```

Sample Output

```
SLX# show running-config management-security
management-security
 ssl-profile server
  tls min-version 1.2
 !
 ssl-profile client
  tls min-version 1.2
 !
!
```

Remediation:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4 NTP

2.4.1 Ensure multiple NTP servers are configured (Automated)

Profile Applicability:

- Level 1

Description:

NTP servers ensure that the system maintains the correct time to prevent drift and delays. If an adversary gains access to an NTP server it is more difficult to cause issues if there are multiple servers configured on the device

Rationale:

Using multiple Network Time Protocol (NTP) servers is vital for maintaining accurate and reliable time synchronization across systems. Here's why having multiple NTP servers is important:

- Redundancy: If one NTP server fails or becomes unreachable, having additional servers ensures that time synchronization can continue without interruption.
- Accuracy: Multiple NTP servers provide a more accurate and reliable time by averaging the time received from various sources, reducing the impact of any single incorrect or misleading time source.
- Load Balancing: Distributing the time synchronization load across multiple servers prevents any single server from being overwhelmed, leading to more stable and reliable timekeeping.
- Fault Tolerance: In case of network issues or server maintenance, multiple NTP servers provide fault tolerance, ensuring that time synchronization remains consistent and accurate.
- Diverse Sources: Using NTP servers from different geographic locations or networks helps mitigate the risk of localized issues affecting the accuracy and reliability of time synchronization.

Overall, leveraging multiple NTP servers helps ensure accurate, reliable, and resilient time synchronization, which is essential for the smooth operation of many systems and applications.

Audit:

```
SLX# show running-config | in ntp.server
```

Sample output:

```
ntp server 192.168.0.10 source-interface-type management source-interface-
number 0
```

Remediation:

```
SLX(config)# ntp server 192.168.0.10 source-interface-type management source-
interface-number 0
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4 Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	**6.1 Utilize Three Synchronized Time Sources** Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.4.2 Enable NTP Server Authentication (Automated)

Profile Applicability:

- Level 1

Description:

The switch should be synchronized with NTP server with authentication turned on. Authenticating to the NTP servers prevent an adversary from spoofing the NTP address and establishing connection.

Rationale:

NTP server authentication is essential for ensuring the accuracy and security of time synchronization across networks. Here's why it should be done:

- Preventing Spoofing: Without authentication, malicious actors can send false time information to your systems, leading to incorrect time synchronization. Authentication ensures that the time data comes from a legitimate source.
- Ensuring Data Integrity: Authentication verifies that the time data has not been tampered with during transmission. This maintains the integrity of the time information being synchronized across your network.
- Maintaining Network Security: Accurate time synchronization is critical for many security protocols, such as Kerberos. Authentication helps maintain the accuracy of time, which in turn supports the overall security of your network.
- Compliance: Many regulatory frameworks require secure time synchronization. Using authenticated NTP servers helps meet these compliance requirements by ensuring that time data is accurate and trustworthy.
- Troubleshooting and Forensics: Accurate time stamps are essential for troubleshooting and forensic analysis in case of security incidents. Authentication ensures that these time stamps are reliable and precise.

By implementing NTP server authentication, you enhance the reliability, accuracy, and security of time synchronization in your network, supporting both operational efficiency and regulatory compliance.

Audit:

```
SLX# show running-config | in ntp.authenticate
```

Remediation:

Configure the NTP Server configuration and authentication

```
SLX(config)# ntp authenticate
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4 <u>Standardize Time Synchronization</u>** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		🟠	🔵
v7	**6.1 <u>Utilize Three Synchronized Time Sources</u>** Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		🟠	🔵

2.5 Syslog Configuration

Syslog server should be configured to capture and retain events, and logs generated with the system. There two categories of logs in SLXOS that can be configured to stream messages to syslog.

- RASlog – Reliability, Availability and Security log provided central logging of CRITICAL, ERROR, WARNING and INFO class events.
- Auditlog - To meet STIG/SRG requirements logs are directed to a syslog server. By default auditlog classes SECURITY, CONFIGURATION and FIRMWARE are logged.

2.5.1 Syslog Server Configuration (Automated)

Profile Applicability:

- Level 1

Description:

Switches should have a syslog server configuration to enable the syslog logging activity to function.

Rationale:

The syslog logging function plays a crucial role in maintaining the security and efficiency of a system by centralizing log data from various sources. Here's why it's important:

- Security Monitoring: Syslog helps detect security breaches and suspicious activities by providing real-time alerts and historical data for analysis.
- Troubleshooting: It aids in diagnosing issues by logging errors and unusual system behavior, allowing for quick identification and resolution of problems.
- Compliance: Many industries require strict adherence to regulations that mandate the logging of specific events. Syslog ensures that these requirements are met.
- Centralized Management: It consolidates logs from multiple devices into a single location, simplifying the monitoring and management of a network.
- Audit Trails: Syslog maintains detailed records of system and user activities, which are essential for audits and forensic investigations.

Overall, syslog is a foundational tool for maintaining system integrity, ensuring security, and complying with regulatory requirements.

Audit:

```
SLX# show running-config | in logging.*syslog-facility
```

Sample Output:

```
logging syslog-server 192.168.0.10 use-vrf mgmt-vrf source-interface
management 0
```

Remediation:

```
SLX(config)# logging syslog-server 192.168.0.10 use-vrf mgmt-vrf source-
interface management 0
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 <u>Collect Detailed Audit Logs</u>** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 <u>Enable Detailed Logging</u>** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

2.5.2 Syslog Facility Configuration (Automated)

Profile Applicability:

- Level 1

Description:

Switches should have a syslog server configuration to enable the syslog logging activity to function.

Rationale:

Configuring the syslog facility correctly is vital for effective log management and system security. Here are some reasons why it's important:

- Efficient Log Categorization: By properly configuring syslog facilities, logs from different sources (e.g., applications, system processes, security events) can be categorized and stored separately. This makes it easier to locate and analyze specific logs.
- Enhanced Security Monitoring: Proper facility configuration ensures that security-related events are logged to the appropriate facility, making it simpler to monitor and respond to potential threats.
- Simplified Troubleshooting: When logs are organized by facility, troubleshooting becomes more efficient. You can quickly identify and address issues by focusing on the relevant log entries.
- Compliance and Audit Readiness: Accurate facility configuration helps meet regulatory and compliance requirements by ensuring that critical events are logged correctly and are easily accessible for audits.
- Resource Management: Configuring facilities helps manage storage and processing resources efficiently by preventing unnecessary or redundant logging, ensuring that only important data is captured.

By configuring syslog facilities properly, you can improve log management, security, and system performance, ultimately leading to a more robust and secure IT environment.

Audit:

```
SLX# show running-config | in logging.*syslog-server
```

Sample Output:

```
logging syslog-facility local LOG_LOCAL7
```

Remediation:

```
SLX(config)# logging syslog-facility local LOG_LOCAL7
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

2.5.3 Syslog Audit Class Configuration (Automated)

Profile Applicability:

- Level 1

Description:

A syslog audit class is a categorization mechanism used in logging systems to classify and group different types of audit events. This allows administrators to define what specific events or activities should be logged.

Rationale:

Syslog audit classes are essential for maintaining a comprehensive and organized logging system. Here's why they're important:

- Targeted Logging: Audit classes allow you to specify which types of events to log. This ensures that only relevant information is captured, reducing unnecessary clutter and making the logs more manageable.
- Improved Security: By configuring audit classes, you can focus on logging security-related events such as login attempts, permission changes, and access to sensitive data. This makes it easier to detect and respond to potential security threats.
- Compliance: Many regulations require detailed logs of specific activities. Configuring audit classes helps ensure that all necessary events are recorded, making it easier to meet compliance requirements.
- Efficient Troubleshooting: When audit classes are properly configured, it becomes easier to pinpoint issues by analyzing logs related to specific system components or activities. This speeds up the troubleshooting process.
- Resource Optimization: Audit classes help manage logging resources by ensuring that only pertinent events are logged. This prevents excessive use of storage and processing power, maintaining system performance.

By effectively utilizing syslog audit classes, you can enhance security monitoring, simplify compliance, and optimize system resources.

Audit:

```
SLX# show running-config | in logging.*auditlog.[SECURITY|CONFIG|FIRMWARE]
```

Sample Output:

```
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
```

Remediation:

```
SLX(config)# logging auditlog class SECURITY
SLX(config)# logging auditlog class CONFIGURATION
SLX(config)# logging auditlog class FIRMWARE
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

2.6 AAA Configuration

2.6.1 Enable Local Login Authentication (Automated)

Profile Applicability:

- Level 1

Description:

Enabling local login authentication in AAA (Authentication, Authorization, and Accounting) allows a system to authenticate users using a local database instead of relying on an external server like RADIUS or TACACS+. Here's how it works:

- Local User Database: The system uses its own local database to store usernames and passwords.
- Authentication Process: When a user attempts to log in, the system checks the local database for the credentials.
- Fallback Option: It can be used as a fallback method if the external authentication server is unavailable.

This setup is useful as a backup method to ensure users can still authenticate even if the external server is down.

Rationale:

Enabling local login with AAA (Authentication, Authorization, and Accounting) provides several key benefits:

- Redundancy and Reliability: In scenarios where the external authentication servers (like RADIUS or TACACS+) are unavailable due to network issues or maintenance, local login serves as a reliable fallback method. This ensures continuous access for users.
- Simplified Configuration: For smaller networks or environments with a limited number of users, using a local database can simplify the configuration and management of authentication processes.
- Immediate Access Control: Local login allows for immediate adjustments to user access, such as quickly adding or removing users, without needing to interact with external authentication servers.
- Testing and Troubleshooting: Local login is useful for testing and troubleshooting the AAA configuration. It allows administrators to verify that the system's authentication mechanisms are working properly without relying on external factors.
- Enhanced Security: By keeping a local user database, you can secure critical accounts that must always have access, even if external systems are compromised or offline. This is particularly important for emergency situations or maintenance activities.

Using local login with AAA ensures that you have a robust, flexible, and reliable authentication mechanism that enhances overall system security and availability.

Audit:

```
SLX# show running-config | in aaa.authentication.*login.local
```

Sample Output:

```
aaa authentication login local
```

Remediation:

```
SLX(config)# aaa authentication login local
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.2 Enable Accounting (Automated)

Profile Applicability:

- Level 1

Description:

AAA accounting, a crucial component of the AAA framework, stands for Authentication, Authorization, and Accounting. Here's a breakdown of what AAA accounting entails:

- Tracking User Activities: AAA accounting monitors and records user activities on a network, such as login attempts, resource access, and changes to system configurations.
- Usage Auditing: It helps in auditing the usage of network resources by keeping detailed logs of user interactions with the system, which can be vital for both security and performance analysis.
- Resource Management: By tracking resource utilization, AAA accounting aids in managing network resources efficiently, ensuring that users are billed or charged accurately for the resources they consume.
- Compliance and Reporting: It supports compliance with regulatory requirements by maintaining detailed records of user actions, which can be used for reporting and auditing purposes.
- Troubleshooting and Diagnostics: Detailed logs generated by AAA accounting assist in troubleshooting network issues and diagnosing problems by providing a historical record of user activities and system events.

In essence, AAA accounting ensures that all user actions are tracked and recorded, which is essential for maintaining security, compliance, and efficient resource management in a network environment.

Rationale:

Using accounting in AAA (Authentication, Authorization, and Accounting) is essential for several reasons:

- Security and Monitoring: Accounting provides detailed logs of user activities, which are crucial for monitoring and detecting unauthorized access or unusual behavior. This enhances overall network security.
- Compliance: Many regulatory frameworks require organizations to maintain detailed records of user activities. Accounting helps meet these compliance requirements by providing a comprehensive log of interactions and transactions.
- Troubleshooting and Auditing: Detailed accounting logs are invaluable for troubleshooting network issues and performing audits. They provide a historical record of user activities and system events, making it easier to diagnose problems and ensure accountability.

- Performance Analysis: Accounting data can be used to analyze the performance of the network and identify areas for improvement. It helps in understanding how resources are being used and where potential bottlenecks might occur.

By implementing accounting within the AAA framework, organizations can enhance security, comply with regulations, manage resources more effectively, and ensure accurate billing and performance analysis.

Audit:

```
SLX# show running-config | in aaa.accounting
```

Sample Output:

```
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none
aaa authorization command none
```

Remediation:

```
SLX(config)# aaa authentication login local
SLX(config)# aaa accounting exec default start-stop none
SLX(config)# aaa accounting commands default start-stop none
SLX(config)# aaa authorization command none
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

3 Interface Configuration

3.1 Handle Unused Interfaces

3.1.1 Disable Unused Interfaces (Manual)

Profile Applicability:

- Level 1

Description:

Any unused interface should be disabled. The SLX-OS switches enable all ports by default. However, unused ports should be disabled and only used ports should be enabled.

Rationale:

Disabling unused network interfaces is a crucial best practice for maintaining security and optimizing network performance. Here's why:

- Enhanced Security: Unused network interfaces can be exploited by attackers to gain unauthorized access to a network. Disabling these interfaces reduces the attack surface, making it harder for malicious actors to find entry points.
- Preventing Misconfigurations: Active but unused interfaces might inadvertently be configured incorrectly or left with default settings, which can pose security risks. Disabling them ensures they don't become unintentional vulnerabilities.
- Network Performance: Active interfaces consume system resources, even if they're not in use. Disabling them can free up resources, leading to improved network performance and efficiency.
- Simplified Network Management: Managing a network with fewer active interfaces simplifies monitoring and maintenance tasks. It's easier to keep track of active devices and their configurations.
- Compliance: Some security standards and policies require minimizing the number of active network interfaces to reduce risks. Disabling unused interfaces helps meet these compliance requirements.
- Fault Isolation: During troubleshooting, having unused interfaces disabled makes it easier to isolate and identify issues, as there are fewer potential sources of problems.

By disabling unused network interfaces, you enhance the security, performance, and manageability of your network, ultimately creating a more robust and resilient IT environment.

Audit:

```
SLX# show interface status | in Eth.*Down | count
```

Sample Output:

```
SLX# show interface status | in Eth.*Down | count
Count: 32 lines
```

Remediation:

```
SLX(config)# interface ethernet 1-32
SLX(config)# shutdown
```

Default Value:

Enabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

3.1.2 Disable Proxy Arp (Manual)

Profile Applicability:

- Level 1

Description:

Proxy ARP (Proxy Address Resolution Protocol) is a network technique that allows one device on a local network to respond to ARP (Address Resolution Protocol) requests on behalf of another device

While Proxy ARP can be useful, it also has some drawbacks:

- Security Risks: It can potentially expose the network to security risks, such as ARP spoofing and man-in-the-middle attacks.
- Network Performance: It can introduce additional traffic on the network, which may impact performance.

Rationale:

Disabling Proxy ARP is often recommended for several important reasons:

- Security Enhancement: Proxy ARP can expose your network to various security risks, including ARP spoofing and man-in-the-middle attacks. Disabling Proxy ARP helps mitigate these vulnerabilities, thereby enhancing overall network security.
- Preventing Network Loops: Proxy ARP can create complex and hard-to-troubleshoot network loops, leading to potential broadcast storms and other network issues. Disabling it simplifies network topology and reduces the risk of such problems.
- Improved Performance: Proxy ARP can generate unnecessary ARP traffic, which can degrade network performance. Disabling it helps reduce this overhead, ensuring more efficient use of network resources.
- Better Network Control: When Proxy ARP is disabled, network administrators have better control over routing and traffic management, leading to more predictable and manageable network behavior.
- Simplified Troubleshooting: Without Proxy ARP, troubleshooting network issues becomes simpler and more straightforward, as the network's behavior is easier to understand and diagnose.

By disabling Proxy ARP, you can enhance the security, performance, and manageability of your network, leading to a more stable and reliable IT environment.

Audit:

```
SLX# show running config | in Eth.*Down | count
```

Sample Output:

```
SLX# show interface status | in Eth.*Down | count
Count: 32 lines
```

Remediation:

```
SLX(config)# interface ethernet 1-32
SLX(config)# shutdown
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

4 Protocol Configuration

4.1 BGP

4.1.1 Ensure BGP Configuration (Automated)

Profile Applicability:

- BGP Enabled

Description:

BGP, or Border Gateway Protocol, is a standardized exterior gateway protocol used to exchange routing information between different autonomous systems (AS) on the internet.

Rationale:

Ensuring proper BGP (Border Gateway Protocol) configuration is essential for maintaining the stability, performance, and security of a network. Here's why it's crucial:

- Network Stability: Proper BGP configuration ensures that routing information is accurate and up-to-date, preventing routing loops and black holes that can disrupt network stability.
- Optimal Path Selection: BGP configurations influence how data is routed through the network. Correctly setting policies and attributes ensures that traffic takes the most efficient path, improving performance and reducing latency.
- Redundancy and Failover: BGP can provide multiple paths for data to travel. Proper configuration ensures seamless failover in case one path becomes unavailable, maintaining continuous connectivity.
- Security: Incorrect BGP configurations can expose networks to route hijacking and other security threats. Proper configuration includes implementing route filtering, prefix lists, and other security measures to protect against these risks.
- Scalability: BGP is designed to handle large numbers of routes. Proper configuration ensures that the network can scale efficiently as it grows, avoiding performance issues and routing table overloads.
- Compliance and Best Practices: Following industry standards and best practices in BGP configuration helps ensure compliance with regulatory requirements and reduces the risk of network misconfigurations.

By ensuring BGP is correctly configured, organizations can maintain a robust, secure, and efficient network, capable of handling the demands of modern internet traffic.

Audit:

```
SLX# show running config | in router.bgp
```

Sample Output:

```
router bgp
```

Remediation:

```
SLX(config)# router bgp
SLX(config)# write
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.1.2 Ensure AS number configuration (Automated)

Profile Applicability:

- BGP Enabled

Description:

A BGP AS number (ASN), or Autonomous System Number, is a unique identifier assigned to each autonomous system (AS) on the internet.

Rationale:

BGP AS are important because:

- Global Internet Routing: ASNs enable the global routing of IP traffic by ensuring that routing policies are maintained and followed. This is critical for the stability and efficiency of the internet.
- Network Identity: An ASN provides a unique identity to an autonomous system, distinguishing it from others on the internet.
- Policy Implementation: ASNs are used to implement and manage routing policies, allowing organizations to control how traffic enters and exits their networks.

In summary, ASNs are a fundamental component of BGP, enabling the internet to function as a cohesive and interconnected network of networks.

Audit:

```
SLX# show running config | in local-as
```

Sample Output:

```
local-as 64512
```

Remediation:

```
SLX(config)# router bgp
SLX(bgp)# local-as 65512
SLX(bgp)# capability as4-enable
SLX(bgp)# fast-external-fallover
SLX(bgp)# end
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

Controls Version	Control	IG 1	IG 2	IG 3
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

5 SNMP Configuration

5.1 Ensure V3 host is enabled

5.1.1 Check V3 host configuration (Automated)

Profile Applicability:

- Level 1

Description:

SNMPv3 (Simple Network Management Protocol version 3) is the latest version of SNMP, designed to provide secure access to devices by incorporating robust security features

Rationale:

Using SNMPv3 (Simple Network Management Protocol version 3) offers significant advantages for network management, mainly due to its enhanced security features. Here are the key reasons to use SNMPv3:

- Improved Security: SNMPv3 incorporates strong security mechanisms, including message integrity, authentication, and encryption. This ensures that the data being transmitted is protected from tampering and unauthorized access.
- Confidentiality: With encryption, SNMPv3 keeps sensitive information, such as network configuration and management data, confidential. This is particularly important in preventing data breaches and ensuring that only authorized users can view the information.
- Authentication: SNMPv3 verifies the identity of users and devices, preventing unauthorized entities from accessing or altering network management data. This helps maintain the integrity and trustworthiness of the network.
- Compliance: Many organizations and regulatory bodies require secure network management protocols. SNMPv3 meets these requirements, helping organizations comply with industry standards and regulations.
- Compatibility and Interoperability: SNMPv3 is a standardized protocol, ensuring compatibility and interoperability with a wide range of network devices and management systems. This makes it easier to integrate SNMPv3 into existing network environments.
- Reliability: By providing mechanisms to ensure data integrity and confidentiality, SNMPv3 enhances the reliability of network management. This means administrators can trust the data they receive and make informed decisions based on accurate information.

Overall, SNMPv3 is a robust and secure protocol that enhances the safety and efficiency of network management, making it a vital tool for modern network environments.

Audit:

```
SLX# show running-config | in snmp-server
```

Sample Output:

```
snmp-server v3host 10.18.120.110 efav3User
```

Remediation:

```
SLX(config)# snmp-server v3host 10.18.120.110 efav3User
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.8 Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	**0.0 Explicitly Not Mapped** Explicitly Not Mapped			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**General Recommendations**		
1.1	Ensure the system is on a supported Network Operating System (Manual)	☐	☐
1.2	Configure Host Name (Automated)	☐	☐
1.3	Ensure that the Default Chassis Name is changed (Manual)	☐	☐
2	**System Configuration**		
2.1	**Banner Configuration**		
2.1.1	Login Banner (Automated)	☐	☐
2.2	**Password Configuration**		
2.2.1	Change default username and password (Manual)	☐	☐
2.2.2	Ensure Password complexity is configured (Automated)	☐	☐
2.3	**TLS Version**		
2.3.1	Ensure system is running TLS 1.2 or later (Manual)	☐	☐
2.4	**NTP**		
2.4.1	Ensure multiple NTP servers are configured (Automated)	☐	☐
2.4.2	Enable NTP Server Authentication (Automated)	☐	☐
2.5	**Syslog Configuration**		
2.5.1	Syslog Server Configuration (Automated)	☐	☐
2.5.2	Syslog Facility Configuration (Automated)	☐	☐
2.5.3	Syslog Audit Class Configuration (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.6	**AAA Configuration**		
2.6.1	Enable Local Login Authentication (Automated)	☐	☐
2.6.2	Enable Accounting (Automated)	☐	☐
3	**Interface Configuration**		
3.1	**Handle Unused Interfaces**		
3.1.1	Disable Unused Interfaces (Manual)	☐	☐
3.1.2	Disable Proxy Arp (Manual)	☐	☐
4	**Protocol Configuration**		
4.1	**BGP**		
4.1.1	Ensure BGP Configuration (Automated)	☐	☐
4.1.2	Ensure AS number configuration (Automated)	☐	☐
5	**SNMP Configuration**		
5.1	**Ensure V3 host is enabled**		
5.1.1	Check V3 host configuration (Automated)	☐	☐

Appendix: CIS Controls *v7* IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure the system is on a supported Network Operating System	☐	☐
2.2.1	Change default username and password	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure the system is on a supported Network Operating System	☐	☐
2.2.1	Change default username and password	☐	☐
2.2.2	Ensure Password complexity is configured	☐	☐
2.4.1	Ensure multiple NTP servers are configured	☐	☐
2.4.2	Enable NTP Server Authentication	☐	☐
2.5.1	Syslog Server Configuration	☐	☐
2.5.2	Syslog Facility Configuration	☐	☐
2.5.3	Syslog Audit Class Configuration	☐	☐
2.6.2	Enable Accounting	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure the system is on a supported Network Operating System	☐	☐
2.2.1	Change default username and password	☐	☐
2.2.2	Ensure Password complexity is configured	☐	☐
2.4.1	Ensure multiple NTP servers are configured	☐	☐
2.4.2	Enable NTP Server Authentication	☐	☐
2.5.1	Syslog Server Configuration	☐	☐
2.5.2	Syslog Facility Configuration	☐	☐
2.5.3	Syslog Audit Class Configuration	☐	☐
2.6.2	Enable Accounting	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation	Set Correctly	
	Yes	No
No unmapped recommendations to CIS Controls v7	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure the system is on a supported Network Operating System	☐	☐
2.2.1	Change default username and password	☐	☐
2.2.2	Ensure Password complexity is configured	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure the system is on a supported Network Operating System	☐	☐
2.2.1	Change default username and password	☐	☐
2.2.2	Ensure Password complexity is configured	☐	☐
2.3.1	Ensure system is running TLS 1.2 or later	☐	☐
2.4.1	Ensure multiple NTP servers are configured	☐	☐
2.4.2	Enable NTP Server Authentication	☐	☐
2.5.1	Syslog Server Configuration	☐	☐
2.5.2	Syslog Facility Configuration	☐	☐
2.5.3	Syslog Audit Class Configuration	☐	☐
2.6.2	Enable Accounting	☐	☐
3.1.1	Disable Unused Interfaces	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	**No**
1.1	Ensure the system is on a supported Network Operating System	☐	☐
2.2.1	Change default username and password	☐	☐
2.2.2	Ensure Password complexity is configured	☐	☐
2.3.1	Ensure system is running TLS 1.2 or later	☐	☐
2.4.1	Ensure multiple NTP servers are configured	☐	☐
2.4.2	Enable NTP Server Authentication	☐	☐
2.5.1	Syslog Server Configuration	☐	☐
2.5.2	Syslog Facility Configuration	☐	☐
2.5.3	Syslog Audit Class Configuration	☐	☐
2.6.2	Enable Accounting	☐	☐
3.1.1	Disable Unused Interfaces	☐	☐
5.1.1	Check V3 host configuration	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation	Set Correctly	
	Yes	No
No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Jul 17, 2025	1.0.1	AAC artifact incorrect (Ticket 25324)
Jul 17, 2025	1.0.1	Artifact incorrect for this recommendation (Ticket 25325)