

# Sesa Goa Iron Ore Information Security Management System (ISMS)

## Procedure Documented information – Network Hardening Guidelines

**Documented information Name: Procedure Documented information – Network Hardening Guidelines**

**Version No: 3.0**

**Last Updated: 25th July,2023**

**Documented information Owner: Sesa Group**

**Approval Authority: Sesa Group**

**This Documented information is a confidential documented information of Sesa Group**

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the written permission of Sesa Group. This Documented information includes confidential information related to Sesa Group and shall not be distributed to any persons other than those mentioned in the distribution

## Documented information Management Information

**Documented information Title:** Procedure Documented information – Network Hardening Guidelines

**Abstract:** This Documented information is a guideline Documented information for Network hardening.

## Documented information Publication History

(All revisions made to this documented information must be listed in chronological order, with the most recent revision at the top)

Type of Information	Documented information Data
Documented information Title	Procedure Documented information – Network Hardening Guidelines
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_Network Device Hardening Guidelines
Date of Release	06 Dec 2011
Documented information Revision	25th July,2023
Documented information Owner	Sesa Group – IT Department
Documented information Author(s)	Sujay Maskara – Wipro Consultancy Services Arjun N Rao – Wipro Consultancy Services
Documented information Change Reviewer	Sandhya Khamesra, Pricoirs LLP
Checked By	Dileep Singh – CISO
Security Classification	Internal
Documented information Status	Final

## Documented information Approver List

S. No	Approver	Approver Contact	Signature
1	Shobha Raikar (CDIO - IOB)	Shobha.raikar@vedanta.co.in	Electronically Approved 10-Aug 2023

## Documented information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.1	28-03-2013	Sesa Goa Logo Change		28-03-2013
1.2	18-10-2013	Sesa Group Logo , file name change for Sesa Sterlite Ltd – IOB		18-10-2013

1.3	25-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT		27-01-2014
1.4	01 – 12 - 2014	Aligned to ISO 27001:2013	1.1,1.3,1.4,7	05-12-2014
1.5	10-Feb-2016	Company name logo update		15-Feb-2016
1.6	13-Feb-2017	Procedure review		18-Feb-2017
1.7	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.8	22-Aug-2018	Review		29-Aug-2018
1.9	23-Aug-2019	Review		30-Aug-2019
1.10	09-Sep-2020	Review		16-Sep-2020
1.11	28-Sep-2021	Review and Update	1.1	21-Oct-2021
2.0	18 Mar 2022	Review and Update		25-Aug-2022
3.0	25th July,2023	Review and Update		10-Aug 2023

### Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep K Singh	dileep.singh@vedanta.co.in

## Table of Contents

<b>1. Introduction .....</b>	<b>5</b>
<b>1.1 Scope of the Documented information .....</b>	<b>5</b>
<b>1.2 Introduction .....</b>	<b>6</b>
<b>1.3 Objective.....</b>	<b>6</b>
<b>1.4 Device Applicability .....</b>	<b>6</b>
<b>2. Operating System .....</b>	<b>6</b>
<b>2.1 OS Upgrade.....</b>	<b>6</b>
<b>2.2 Check for Vulnerabilities .....</b>	<b>6</b>
<b>2.3 Boot Loader / Boot Sequence Protection.....</b>	<b>6</b>
<b>2.4 Recovery Environment / Feature Protection .....</b>	<b>7</b>
<b>2.5 Disable USB and CD ROM write access .....</b>	<b>7</b>
<b>2.6 Disable auto-mounting / auto-run.....</b>	<b>7</b>
<b>3. Management Control .....</b>	<b>7</b>
<b>3.1 Console and Auxilliary Port .....</b>	<b>7</b>
<b>3.1.1 Secure Console Access .....</b>	<b>7</b>
<b>3.1.2 Reserve Memory for Console Access .....</b>	<b>7</b>
<b>3.1.3 Disable Aux Port.....</b>	<b>7</b>
<b>3.2 Administrative Access.....</b>	<b>7</b>
<b>3.2.1 Use SSH instead of Telnet .....</b>	<b>7</b>
<b>3.2.2 Use SSH instead of Telnet .....</b>	<b>8</b>
<b>3.2.3 Restrict Administrative Access to Specific IPs .....</b>	<b>8</b>
<b>3.3 User and Password Management.....</b>	<b>8</b>
<b>3.3.1 Disable default controls .....</b>	<b>8</b>
<b>3.3.2 Ensure account names do not reveal privileges .....</b>	<b>8</b>
<b>3.3.3 Ensure passwords comply to Sesa Group Password Policy .....</b>	<b>8</b>
<b>3.3.4 Enable Secret .....</b>	<b>8</b>
<b>3.3.5 Service Password Encryption .....</b>	<b>8</b>
<b>3.4 Session Timeout as per Sesa Group Security Regulations.....</b>	<b>8</b>
<b>3.5 Login Banner .....</b>	<b>9</b>
<b>3.6 AAA.....</b>	<b>9</b>
<b>3.6.1 Authentication and Authorization.....</b>	<b>9</b>
<b>3.6.2 Accounting.....</b>	<b>9</b>

<b>3.7</b>	<b>Audit &amp; Logging</b>	<b>9</b>
3.7.1	Enable Auditing	9
3.7.2	Configure Logging	10
<b>4.</b>	<b>Protocols</b>	<b>10</b>
4.1	Secure Routing Protocol	10
4.2	NTP	10
4.3	SNMP	10
4.3.1	Version	10
4.3.2	Default Community Strings	10
4.3.3	Port Filtering	11
4.3.4	Access Control List	11
<b>5.</b>	<b>Services</b>	<b>11</b>
5.1	Disable Unneeded Services	11
5.2	Keepalives for TCP Sessions	12
<b>6.</b>	<b>Interface Hardening</b>	<b>12</b>
<b>7.</b>	<b>Annexure</b>	<b>13</b>
<b>8.</b>	<b>References and Related Policies</b>	<b>13</b>
<b>9.</b>	<b>Templates</b>	<b>14</b>
<b>10.</b>	<b>References and Related Policies</b>	<b>14</b>
<b>11.</b>	<b>Abbreviation</b>	<b>14</b>

## 1. Introduction

### 1.1 Scope of the Documented information

This procedure document is applicable for Vedanta Limited –Sesa Goa Iron Ore Division including SRL and SMCL in Goa, Karnataka, Odisha and Liberia, Pig Iron Division, Met Coke Division , Power Division in Goa Sesa Coke - Gujarat & Vazare , FACOR – Odisha , and VGCB , Visakhapatnam; referred as Sesa Group in this document.

The Network Hardening Guidelines is applicable to the Sesa Group IT Network devices such as routers, switches, firewalls and NIDS.

## 1.2 Introduction

This documented information defines secure configuration parameters to be used when deploying Network devices in the Sesa Group IT network. All Network devices in Sesa Group should at a minimum comply with the standard. Hardening should be carried out in accordance with the Sesa Group Device Hardening Procedure.

## 1.3 Objective

The objective of this documented information is to introduce Network Device Hardening Guidelines required for the preparation of Standard Operating Procedures (SOPs) by platform owners of FMS Team. Checklist has been attached with this documented information for tracking compliance. Filled checklists shall be retained as artifacts by FMS Team. Refer Network hardening Checklist – Annexure 1.

## 1.4 Device Applicability

The settings recommended in this documented information are primarily meant for Cisco devices. However, some of the settings may be applicable to non-cisco devices as well. The respective platform owners shall be responsible for:

- Creating security checklist and security settings for the respective device types (switches/routers/firewalls/IDS/Load balancer etc.) and platforms (Cisco, Fortigate, McAfee etc.) combinations. The template for the checklist is provided in 'Annexure A – Hardening Checklist'.
- Ensuring each new device is hardened as per the defined checklist before it is rolled out into the production environment.

# 2. Operating System

## 2.1 OS Upgrade

**Ensure current stable version of OS supported for the platform.**

- If an operating system is not kept current then the device may be susceptible to information gathering and network attacks. Attackers find weaknesses in versions of an operating system over time. New security features are added to each new version of an operating system.

## 2.2 Check for Vulnerabilities

Before deploying the device into production environment as well as on regular basis post deployment, the device must be scanned and cleaned of vulnerabilities.

- The device should be scanned with a vulnerability scanner. Most vendors have major known vulnerabilities detailed on their websites. Any vulnerability identified should be immediately closed by upgrades/patches or vendor detailed recommendations. Patches should be deployed in accordance with the Sesa Group Patch Management Procedure.

## 2.3 Boot Loader / Boot Sequence Protection

Boot loader / boot sequence should be protected against unauthorized modification.

## 2.4 Recovery Environment / Feature Protection

Access to any recovery environment / feature must be protected to ensure they do not provide unauthorized access to either the device configuration or the data held on it.

## 2.5 Disable USB and CD ROM write access

If available, write access to USB and CD-ROM should be disabled.

## 2.6 Disable auto-mounting / auto-run

If applicable, auto-mounting / auto-run should be disabled.

# 3. Management Control

## 3.1 Console and Auxiliary Port

### 2.1.1 Secure Console Access

**Console Access must be protected by using adequate controls like strong passwords.**

- Any method used in order to access the console port of a device must be secured in a manner that is equal to the security that is enforced for privileged access to a device. A Cisco device's console port is the most important port on the device. Password recovery on the device can only be done using the console port.
- Cisco devices are vulnerable if there is physical access to the devices. However, if someone is trying to access the console port of the router remotely, an additional layer of security should be applied by prompting the user for a password.

### 2.1.2 Reserve Memory for Console Access

**If applicable, reserve memory for console access to ensure access for administrative and troubleshooting purposes.**

- The Reserve Memory for Console Access feature can be used in order to reserve enough memory to ensure console access to a Cisco IOS device for administrative and troubleshooting purposes. This feature is especially beneficial when the device runs low on memory. The memory reserve console global configuration command can be used in order to enable this feature.

### 2.1.3 Disable Aux Port

**The AUX port of a device must be disabled to prevent unauthorized access**

- The auxiliary port's primary purpose is to provide remote administration capability. It can allow a remote administrator to use a modem to dial into the Cisco device. The aux port should be disabled if there is no business need for the same. Any specific business requirement for enabling it should be properly documented. Additionally, if the auxiliary port is required for remote administration, the callback feature should be configured to dial a specific preconfigured telephone number for additional security

## 3.2 Administrative Access

### 2.2.1 Use SSH instead of Telnet

**SSH to be used instead of clear-text protocols, such as Telnet and rlogin.**

- SSH is a preferred protocol over Telnet for vty access since it encrypts the data while in transit on the network. It is recommended that SSH v2 be used, where possible.

- The Telnet protocol transfers data in clear text thereby allowing an intruder to sniff valuable data such as passwords.

### 2.2.2 Use SSH instead of Telnet

**Disable HTTP service and use HTTPS where OS version supports the same.**

- HTTP is a clear-text protocol and is vulnerable to various packet-capture methods. A hacker could monitor network traffic and capture authentication usernames and passwords. This issue is made more serious when the enable password is used for authentication because this knowledge would give the attacker full administrative access to the device. Once usernames and passwords have been captured, it is simply a matter of using the credentials to log into the router.

### 2.2.3 Restrict Administrative Access to Specific IPs

**Restrict management interface access to specific workstations.**

- If not restricted, an unauthorized person can try to connect and possibly launch a brute force attack to gain access.

## 3.3 User and Password Management

### 2.3.1 Disable default controls

**Default accounts must be disabled. If required, the account should be renamed.**

- Successful exploitation may allow an unauthorized user to modify the configuration and the operating system settings or gain complete administrative control of the device.

### 2.3.2 Ensure account names do not reveal privileges

**The names of the user / service accounts / privilege accounts should not reveal privileges associated with the account.**

### 2.3.3 Ensure passwords comply to Sesa Group Password Policy

**All passwords should comply with the Sesa Group Password policy (refer to “Sesa Group\_Policy\_Identity and Access Management\_v 1.2”)**

- Non-compliance can result in password compromise leading to unauthorized access to network devices.

### 2.3.4 Enable Secret

**The enable secret command should be enabled to implement MD5 hashed password on enable mode.**

- The ‘enable secret’ is more secure than the ‘enable password’ because of the stronger encryption used. In case of ‘enable password’, anyone who gets a copy of the configuration file can easily crack this type of password.

### 2.3.5 Service Password Encryption

**Password encryption should be enabled.**

- This ensures all passwords, including console and VTY line passwords, are encrypted when stored in NVRAM, and are not visible in clear text within the configuration file or when the configuration is viewed using “show” commands.

## 3.4 Session Timeout as per Sesa Group Security Regulations

**Management sessions to the infrastructure elements should have a time out of no more than 15 minutes.**



Session timeout should be configured on the network devices to limit any unauthorized access.

### 3.5 Login Banner

**All infrastructure elements must be configured with a login banner below to comply with Sesa Group's Security Regulations:**

*"This system is for use of authorized users only. Unauthorized access to this system is prohibited and may lead to legal or disciplinary action. All authorized and unauthorized activity on this system can be monitored and recorded for analysis and monitoring purpose. Evidences of such monitoring can be provided to law enforcement or other officials."*

Banners helps in notifying the users that system is to be logged in or used by authorized personnel only. Warning banner serves a notice that any unauthorized use of the system is unlawful and might be subject to civil and criminal penalties. Banners help in assigning legal liability, and assigning due care in line with state and federal law considerations.

### 3.6 AAA

The Authentication, Authorization, and Accounting (AAA) framework is critical to securing interactive access to network devices.

#### 2.6.1 Authentication and Authorization

**Enable AAA authentication with TACACS+/RADIUS. Authentication keys used must be configured in line with Sesa Group Password Policy. Additionally, authentication fallback through secondary authentication mechanisms (e.g. local authentication) should be considered in case the AAA infrastructure becomes unavailable.**

- TACACS+ (Terminal Access Controller Access Control System Plus) is an authentication protocol that Cisco IOS devices can use for authentication of management users against a remote AAA server (ACS). TACACS+ authentication, or more generally AAA authentication, provides the ability to use individual user accounts for each network administrator. In removing the dependence on a single shared password, the security of the network is improved and accountability is strengthened. Command authorization should also be setup with TACACS+ to provide a mechanism that permits or denies each command that is entered by an administrative user.
- RADIUS (Remote Authentication Dial In User Service) is an industry standard networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Authentication and Authorization for non-Cisco devices should be setup with RADIUS.

#### 2.6.2 Accounting

**Enable accounting to send information about each command that is entered to the configured TACACS+/RADIUS server.**

- The information sent to the TACACS+/RADIUS server includes the command executed, the date it was executed, and the username of the user entering the command.

### 3.7 Audit & Logging

#### 2.7.1 Enable Auditing

**Logging should be enabled for the device and syslogs sent to SIEM (Local/Remote Collectors) where applicable.**

- By sending logging information to a remote syslog server (SIEM), it becomes possible to correlate and audit network and security events across network devices more effectively. Concurrence/approval is to be sought by device owner from Sesa Group IT security on which device is to be integrated to SIEM before deploying the device in the environment.

## 2.7.2 Configure Logging

### **Configure Logging source interface to the Loopback interface. Configure Logging Timestamps**

- In order to provide an increased level of consistency when collecting and reviewing log messages, it is advised to statically configure a logging source interface which ensures that the same IP address appears in all logging messages that are sent from an individual Cisco IOS device. For added stability, it is advised to use a loopback interface as the logging source.
- The configuration of logging timestamps helps to correlate events across network devices. It is important to implement a correct and consistent logging timestamp configuration to ensure that logging data can be correlated. Logging timestamps should be configured to include the date and time with millisecond precision and to include the time zone in use on the device.

## 4. Protocols

### 4.1 Secure Routing Protocol

Security settings associated with the routing protocols being used should be evaluated and implemented to prevent attacks against them.

### 4.2 NTP

**Enable Network Time Protocol (NTP) which provides a universal time base for routers, switches, and other networked devices. All devices must point to the same NTP source and the same time zone being used within Sesa Group.**

- A synchronized time enables to associate syslog and Cisco IOS debug output to specific events across multiple devices. Configure NTP only on required interfaces, and configure NTP to listen only to certain specified peers.
- If the NTP service is not enabled, there may not be clock synchronization between networking devices and a consistent time would not be maintained, which is essential for diagnostic and security alerts and log data. Also, if configured insecurely, it could be used to corrupt the time clock of the network devices. To prevent this, restrict which devices have access to NTP.

### 4.3 SNMP

#### 3.3.1 Version

**SNMPv3 shall be used for remote management. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c.**

- If this is not possible due to technical or operational constraints the requirement shall be handled through exception management process.

#### 3.3.2 Default Community Strings

**Default community strings “public” for read-only access and “private” for read-write access shall be changed to comply with Sesa Group’s password policy.**

- Community strings are passwords that are applied to a device to restrict access, both read-only and read-write access, to the SNMP data on the device. These community strings, as with all passwords, should be carefully chosen to ensure they are not trivial.

### 3.3.3 Port Filtering

**Port Filtering at infrastructure layer should be setup for SNMP**

- Filter SNMP (port 161 TCP/UDP and 162 TCP/UDP) at the ingress points to the networks.
- Other ports that handle SNMP-related services—including TCP and UDP ports 161, 162, 199, 391, 750, and 1993—shall require ingress filtering as well
- Devices that provide public services do not normally initiate outbound traffic to the Internet. To control traffic leaving the network, implement egress filtering. Filtering outgoing traffic from UDP ports 161 and 162 at the network border can prevent the system from being used as a launching pad for attack.

### 3.3.4 Access Control List

**In addition to the community string, an ACL should be applied that further restricts SNMP access to a select group of source IP addresses.**

- Employ host-based access control on SNMP agent systems. While this capability may be limited by SNMP agent operating system capabilities, control of what systems the agents will accept requests from, may be possible.

## 5. Services

### 5.1 Disable Unneeded Services

The following services should be disabled from security perspective:

Services	Details
<b>Disable BOOTP</b>	When the BOOTP server is disabled, access to the BOOTP ports cause the Cisco IOS software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.
<b>Disable udp-small-servers</b>	When you disable the servers, access to Echo, Discard, and Chargen ports causes the Cisco IOS® software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.
<b>Disable tcp-small-servers</b>	When you disable the minor TCP/IP servers, access to the Echo, Discard, Chargen, and Daytime ports cause the Cisco IOS® software to send a TCP RESET packet to the sender and discard the original incoming packet.
<b>Disable Finger Service</b>	Finger service allows a hacker to find out who is logged into the router and allows them to find out valid login names. The information they could access includes the processes running on the system, the line number, connection name, idle time, and terminal location. This information is provided through the Cisco IOS software show users EXEC command. Unauthorized persons can use this information for reconnaissance attacks.
<b>Disable Domain Lookup</b>	The Domain Name System (DNS) lookup client service is enabled by default and is not required.
<b>Disable IP Source Route</b>	To discard any IP datagram containing a source-route option use this command. It is not good practice to allow IP source-routing due to implicit tunnelling attacks.

## 5.2 Keepalives for TCP Sessions

Use service TCP-Keepalives to avoid hung sessions.

- The service TCP-Keepalive-in and service TCP-Keepalive-out global configuration commands enable a device to send TCP Keepalives for TCP sessions. This configuration must be used in order to enable TCP Keepalives on inbound connections to the device and outbound connections from the device. This ensures that the device on the remote end of the connection is still accessible and that half-open or orphaned connections are removed from the device.

## 6. Interface Hardening


The following should be ensured for the device interfaces:

Parameter	Applicable to	Details
<b>Shutdown</b>	All unused interfaces	All unused interfaces should be disabled
<b>Disable CDP</b>	All interfaces connected to untrusted / uncontrolled networks	Cisco Discovery Protocol (CDP) is a network protocol that is used in order to discover other CDP enabled devices for neighbour adjacency and network topology.  CDP must be disabled on all interfaces that are connected to untrusted/uncontrolled networks.
<b>Disable Directed Broadcast</b>	All interfaces	Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This feature should be disabled on all interfaces as it could be used in denial-of-service attacks.
<b>Disable IP Redirects</b>	All interfaces	ICMP redirects cause the router to send ICMP redirect messages whenever the router is forced to resend a packet through the same interface on which it was received. By sending ICMP redirects, a hacker can redirect packets to an un-trusted device.
<b>Disable IP Unreachable</b>	All interfaces	IP unreachable messages can be used to map out the network topology, and they should be disabled on all interfaces.
<b>Disable IP Mask Reply</b>	All interfaces	When enabled, this service tells the router to respond to ICMP mask requests by sending ICMP mask reply messages containing the interface IP address mask. This information can be used to map the network.
<b>Disable Proxy ARP</b>	All interfaces	This feature configures the router to act as a proxy for Layer 2 address resolution when hosts have no default gateway configured. When a host sends an ARP, the router responds to it with its own mac address as the one to use for the remote system. When DHCP is being

		used, there is no need to have Proxy ARP enabled. Attackers may be able to spoof packets and gather information about the router and network.
--	--	---

## 7. Annexure

- Network Device Hardening Standard Documented information


Sr. No.	Documented information Name	Documented information Version	Documented information Attachment
1	Network Device Hardening Documented information	V 1.1	 Sesa Group_Network Devices Hardening Gl

## 8. References and Related Policies

- Sesa Group\_Policy\_Identity and Access Management

## 9. Templates

- System Acceptance Form

Sr. No.	Documented information Name	Documented information Version	Documented information Attachment
1	System Acceptance Form	V 1.4	 Sesa Group_Form_System

## 10. References and Related Policies

- Computing Environment Policy

## 11. Abbreviation

**SPoC** – Single Point of Contact

**SOP** – Standard Operating Procedure

**FMS** – Facility Management System