Security Target for
SolarWinds Security Event Manager 2024.2.1

Version 1.10

SolarWinds Worldwide, LLC
7171 Southwest Parkway
Building 400
Austin, Texas 78735

DOCUMENT INTRODUCTION

Prepared By:

SolarWinds Worldwide, LLC
7171 Southwest Parkway
Building 400
Austin, Texas 78735
http://www.solarwinds.com

REVISION HISTORY

Rev	Description
1.0	April 23, 2024 – Initial release.
1.1	June 19, 2024 – Updated the FIA_SOS.1(2) SFR.
1.2	June 24, 2024 – Adjusted the document based on the evaluator's comments.
1.3	June 27, 2024 – Updated OE.NETWORK description in section 4.2, updated FIA_USB components definitions in section 7.
1.4	July 16, 2024 – Updated the TOE version to 2024.2.1.
1.5	September 03, 2024 – Updated section 8.1.5 table.
1.6	September 04, 2024 – Added versions to guidance documents in section 1.6.1.
1.7	October 21, 2024 – Updated Table 13. Removed FCS and FTP SFRs, updated section 1.6, 3, 4, and 5.
1.8	November 4, 2024 – Addressed evaluator’s observations and comments.
1.9	November 29, 2024 – Updated Table 13.
1.10	December 23, 2024 – Add T.COMM, O.COMM and FTP_TRP.1 SFR, updated section 1.6, 3, 4, 5, 7, and 8.

TABLE OF CONTENTS

1. SECURITY TARGET INTRODUCTION 7
1.1 Security Target Reference 7
1.2 TOE Reference 7
1.3 Evaluation Assurance Level 7
1.4 Keywords 7
1.5 TOE Overview 7
1.5.1 Usage and Major Security Features 7
1.5.2 TOE Type 9
1.5.3 Required Non-TOE Hardware/Software/Firmware 9
1.6 TOE Description 9
1.6.1 Physical Boundary 10
1.6.2 Logical Boundary 10
1.7 TSF Data 11
1.8 Evaluated Configuration 12

2. CONFORMANCE CLAIMS 14
2.1 Common Criteria Conformance 14
2.2 Security Requirement Package Conformance 14
2.3 Protection Profile Conformance 14

3. SECURITY PROBLEM DEFINITION 15
3.1 Introduction 15
3.2 Assumptions 15
3.3 Threats 15
3.4 Organisational Security Policies 16

4. SECURITY OBJECTIVES 17
4.1 Security Objectives for the TOE 17
4.2 Security Objectives for the Operational Environment 17

5. RATIONALE 18
5.1 Rationale for IT Security Objectives 18
5.2 Security Requirements Rationale 20
5.2.1 Rationale for Security Functional Requirements of the TOE Objectives 20
5.2.2 Security Assurance Requirements Rationale 22

6. EXTENDED COMPONENTS DEFINITION 23
6.1 Extended Security Functional Components 23
6.1.1 Class FNM: Network Management 23
6.1.1.1 FNM_MDC Monitor Data Collection 23
6.1.1.2 FNM_ANL Monitor Analysis 24
6.1.1.3 FNM_RCT Management React 24
6.1.1.4 FNM_RDR Restricted Data Review 25
6.2 Extended Security Assurance Components 26

7. SECURITY REQUIREMENTS 27
7.1 TOE Security Functional Requirements 27
7.1.1 Security Audit (FAU) 27

7.1.1.1 FAU_GEN.1 Audit Data Generation 27
7.1.1.2 FAU_SAR.1 Audit Review 28
7.1.1.3 FAU_SAR.2 Restricted Audit Review 28
7.1.2 Identification and Authentication (FIA) 28
7.1.2.1 FIA_ATD.1(1) User Attribute Definition (Web Console) 28
7.1.2.2 FIA_ATD.1(2) User Attribute Definition (CMC Console) 28
7.1.2.3 FIA_SOS.1(1) Verification of Secrets (Web Console) 29
7.1.2.4 FIA_SOS.1(2) Verification of Secrets (CMC Console) 29
7.1.2.5 FIA_UAU.2 User Authentication Before any Action 29
7.1.2.6 FIA_UAU.7 Protected Authentication Feedback 29
7.1.2.7 FIA_UID.2 User Identification Before any Action 30
7.1.2.8 FIA_USB.1(1) User-Subject Binding (Web Console) 30
7.1.2.9 FIA_USB.1(2) User-Subject Binding (CMC Console) 30
7.1.3 Security Management (FMT) 30
7.1.3.1 FMT_MTD.1 Management of TSF Data 30
7.1.3.2 FMT_SMF.1 Specification of Management Functions 31
7.1.3.3 FMT_SMR.1 Security Roles 32
7.1.3.4 FMT_MOF.1 Management of security functions behaviour 32
7.1.4 Network Management (FNM) 32
7.1.4.1 FNM_MDC.1 Monitor Data Collection 32
7.1.4.2 FNM_ANL.1 Monitor Analysis 32
7.1.4.3 FNM_RCT.1 Management React 32
7.1.4.4 FNM_RDR.1 Restricted Data Review 32
7.1.5 Protection of the TSF (FPT) 33
7.1.5.1 FPT_STM.1 Reliable Time Stamps 33
7.1.6 Trusted Path (FTP) 33
7.1.6.1 FTP_TRP.1 Trusted Path 33
7.2 TOE Security Assurance Requirements 34
7.3 CC Component Hierarchies and Dependencies 34

8. TOE SUMMARY SPECIFICATION 36
8.1 Security Functions 36
8.1.1 Audit 36
8.1.2 Identification and Authentication 36
8.1.3 Management 36
8.1.4 Log and Event Management 36
8.1.5 Secure Communication 37

LIST OF TABLES

Table 1 - SEM Software/Hardware Minimum Requirements 9
Table 2 - TSF Data Descriptions 11
Table 3 - Assumptions 15
Table 4 - Threats 15
Table 5 - Organisational Security Policies (OSPs) 16
Table 6 - Security Objectives for the TOE 17
Table 7 - Security Objectives of the Operational Environment 17
Table 8 - Threats, Assumptions, and OSPs to Security Objectives Mapping 18
Table 9 - Threats, Assumptions and OSPs to Security Objectives Rationale 19
Table 10 - SFRs to Security Objectives Mapping 20
Table 11 - Security Objectives to SFR Rationale 20
Table 12 - Auditable Events 27
Table 13 - TSF Data Detail 31
Table 14 - EAL2+ Assurance Requirements 34
Table 15 - TOE SFR Dependency Rationale 34

ACRONYMS LIST

CC.....**Common Criteria**
CPU ..... **Central Processing Unit**
EAL ..... **Evaluation Assurance Level**
GB..... **GigaByte**
GHz..... **GigaHertZ**
GUI..... **Graphical User Interface**
HTTPS .....**HTTP Secure**
IDS……..**Intrusion Detection System**
IP.....**Internet Protocol**
IT .....**Information Technology**
I&A .....**Identification and Authentication**
NTP.....**Network Time Protocol**
OS ..... **Operating System**
OSP.....**Organisational Security Policy**
SFR ..... **Security Functional Requirement**
SIEM ..... **Security Information and Event Management**
SSH .....**Secure Shell**
ST .....**Security Target**
SEM……..**Security Event Manager**
TLS……**Transport Layer Security**
TOE……**Target of Evaluation**
TSF ..... **TOE Security Function**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements, and rationale for the TOE. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Security Target for SolarWinds Security Event Manager 2024.2.1, version 1.10, December 23, 2024.

1.2 TOE Reference

TOE Name	SolarWinds Security Event Manager
TOE Version	2024.2.1

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5, and augmented by ALC_FLR.2.

1.4 Keywords

SIEM, Log Manager, Event Manager, Security Information and Event Manager

1.5 TOE Overview

1.5.1 Usage and Major Security Features

The Target of Evaluation is SolarWinds Security Event Manager 2024.2.1. SolarWinds Security Event Manager will also be referred to as SEM throughout this document. SEM is a security information and event management (SIEM) virtual appliance that adds value to existing security products and increases efficiencies in administering, managing, and monitoring security policies and safeguards on the network. SEM provides access to log data for forensic and troubleshooting purposes, and tools to help manage log data.

SEM collects, stores, and normalizes log and event data from a variety of sources, and displays that data in a web interface for monitoring, searching, and analysis. Data is also available for scheduled and ad hoc reporting. SEM leverages collected logs, analyzes them in real time, and notifies problem before it causes further damage.

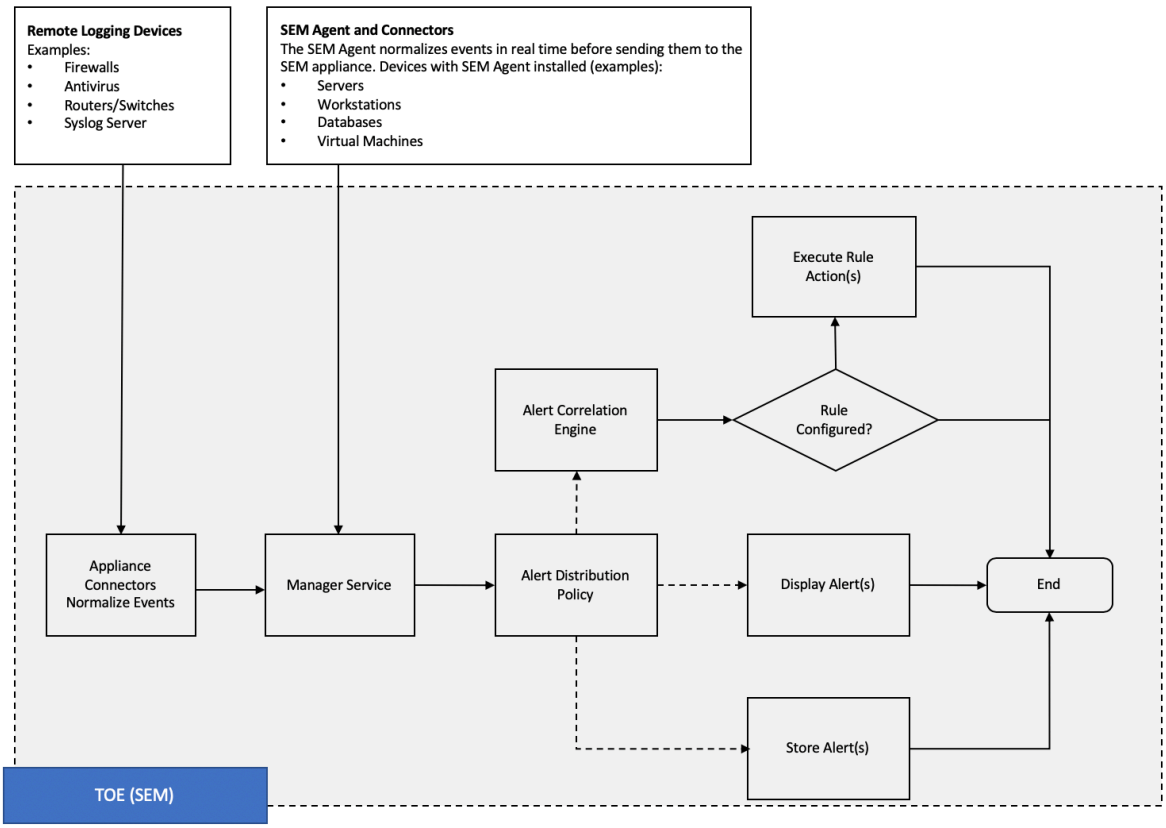
SEM accepts normalized data and raw data from a wide variety of devices. SEM Agents (running on remote systems) normalize the data before sending the data to the SEM. Non-Agent remote devices send their log data in raw form to SEM where it is normalized by device-specific Connectors. SEM Agents are not included in the evaluation.

Alerts are created from normalized data. Alerts are containers SEM uses to display events/messages from SEM monitored devices. Log data is processed by SEM's policy engine to correlate data based on user defined Rules; when a user defined condition is detected, an Incident is created and the configured actions are initiated (when applicable). These actions can include notifying users (both locally in the Console and by email), blocking an IP address, shutting down

or rebooting a workstation, and passing the alerts on to the SEM database for future analysis and reporting. Actions that are dependent upon processing by remote
systems that are outside the scope of the TOE are not included in the evaluation

The following diagram illustrates the basic data flow through SEM.

Figure 1 – Basic Data Flow



Within SEM, Filters organize Alerts into user-defined real-time views. Filters are always related to the user who is using them and can be shared between users. Only real-time data is displayed in Filters.

Rules configured by users are applied against the Alerts to determine if additional actions should be taken. Rules can be used to detect multiple instances of specific events (within a designated time period) as well as correlate multiple types of Alerts. Triggered Rules create an Incident; Incidents may be viewed in real-time or via Historical Events search.

Users primarily interact with SEM with the Console, which is a GUI interface accessed via web browsers from remote workstations. Both real-time viewing and historical viewing (via Historical Events search) may be performed. The Console supports multiple roles. Roles are assigned to sessions when users successfully complete Identification and Authentication with SEM. From the Console, the Administrator is able to access the management functions as specified in Section 7.1.3.2 of this document. Credentials are collected via the GUI and validated by SEM. SEM also supports credential validation by a third-party authentication server, but this functionality is not included in the evaluation.

1.5.2 TOE Type

Network Management

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of a virtual appliance providing the collection and processing of log and event information. The virtual appliance includes essential components required for the proper functioning of the TOE, such as the Linux operating system, SSH server, Syslog server, Web server, and Database, which are outside of the scope of the TOE.

The virtual appliance is installed on a hypervisor that satisfies the following minimum requirements.

Table 1 - SEM Software/Hardware Minimum Requirements

Item	Requirements
Hypervisor (required on the VM host)	One of the following: • VMware vSphere ESXi 6.0 or ESXi 6.0 and later • Microsoft Hyper-V Server 2012 R2, 2016, and 2019
CPU	2 - 4 core processors at 2.0 GHz
Memory	8 GB
Hard Drive storage	250 GB, 15k hard drives (RAID1/mirrored settings)
Input/output operations per second (IOPS)	40 – 200 IOPS
NIC	1 GBE NIC
Web Browser (required on a remote computer to run the web console)	• Google Chrome 120 or newer • Mozilla Firefox 120 or newer • Microsoft Edge v120 or newer
Time synchronization	NTP Server

Console users communicate with SEM virtual appliance via a segregated management network to prevent disclosure or modification of the data exchanged between TOE components. It is the responsibility of the operational environment to protect the traffic on the management network.

If the log and event data collected from remote systems must be protected from disclosure or modification while in transit to the TOE, this protection must be provided by the operational environment.

1.6 TOE Description

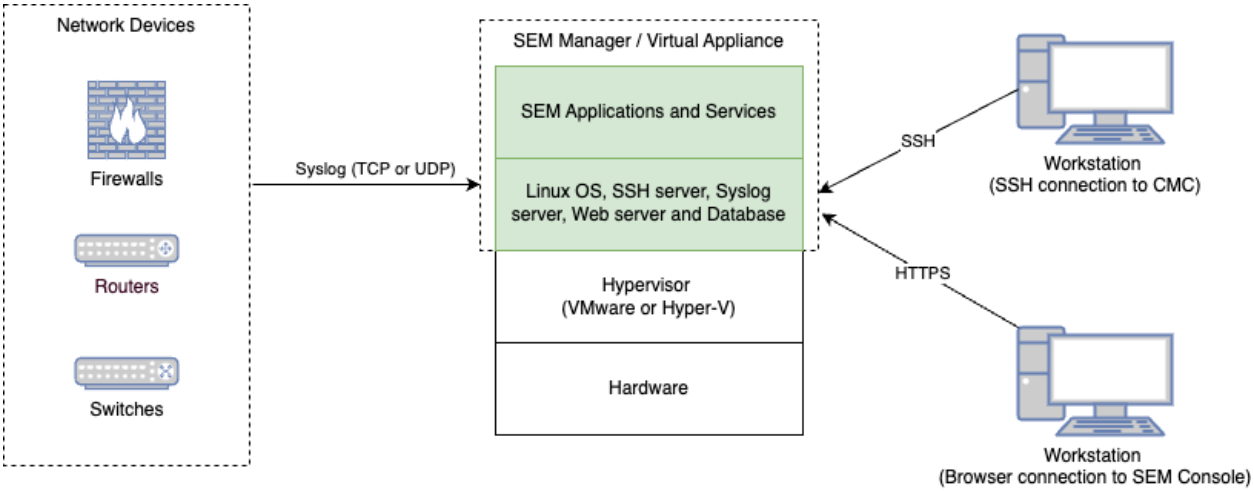
SEM acts as a monitoring and management tool for use by network managers. It collects logs and events from multiple remote third-party systems and alerts the network managers to specified conditions.

Users interact with the TOE via multiple mechanisms. Consoles (including SEM console and SEM CMC console) are provided for remote interaction with users and administrators for configuration and data access.

1.6.1 Physical Boundary

The TOE consists of SEM Manager (SEM Virtual Appliance). Network devices use TCP or UDP to send Syslog data to the SEM Manager. The TOE can protect the communication between itself and user's web browser or SSH client. The operational environment will protect communication between the TOE and systems outside the TOE. The physical boundary of the TOE is depicted in Figure 2 (light green items are within the TOE boundary).

Figure 2 - Physical Boundary



The physical boundary includes the following guidance documentation:

1. SolarWinds Security Event Manager Getting Started Guide V2024.2.1
2. SolarWinds Security Event Manager Installation Guide V2024.2.1
3. SolarWinds Security Event Manager Administrator Guide V2024.2.1
4. SolarWinds Security Event Manager V2024.2.1 Common Criteria Supplement V1.4

1.6.2 Logical Boundary

The TOE provides the following security functionality:

1. Audit - Audit records are generated for specific actions performed by users. The audit records are stored in the database and may be viewed via the Console by authorized users.

2. Identification and Authentication – When a connection is established to the Console, the TOE prompts the user for login credentials. The credentials are validated by the TOE. If the credentials are valid, the username is used to retrieve the user's security attributes inside the TOE from the TOE database.

3. Management – The management functionality provides multiple management access mechanisms for users. For each specific TOE security function data, dedicate access table will be established, the security function data privileges for the users vary based upon the

definition. Individual user's access right for each TOE component security function data is determined by the user's role of each TOE component.

4. Log and Event Management – Log and Event information is collected from remote systems. The results are saved and may be viewed by authorized users. Incidents may be generated in response to configured conditions detected about the collected information.

5. Secure Communication – The TOE can protect the user data from disclosure and modification by using Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) protocols to provide communication security over a computer network. It protects data transmitted between SEM Manager and user's web browser or SSH client.

The following functionality included in the SolarWinds Security Event Manager is not evaluated:

- SEM Agents executing on remote systems.
- Receipt and processing of NetFlow and SNMP information.
- Integration with a third-party Directory Services for authentication and authorization (e.g. Active Directory).
- Actions dependent upon agents installed on remote systems.

1.7 TSF Data

The following table describes the TSF data.

Table 2 - TSF Data Descriptions

TSF Data	Description
Alerts	Events created from information received from remote systems.
Connectors	Defines the handling of information received from remote devices. Attributes include: • Alias (user friendly name) • Log file used to hold messages • Status (e.g. Started)
Dashboard Widgets	Determine the information displayed to Console users on the Dashboard screen

TSF Data	Description
Events	The collection of Alerts, Internal Events, and Incidents. Attributes include: • Event Name • Event Information • Insertion IP (name/address of the Appliance that inserted the Event into the database) • Manager (name/address of the controlling Appliance) • Detection IP (name/address of the system on which the Event occurred) • Insertion Time (time the Event was inserted into the database) • Detection Time (time the Event was detected on the remote system or Appliance) • Severity • Inference Rule (associated Rule if applicable)
Filters	Define the Events to be displayed in a real-time view.
Groups	Define groupings that can be referenced in Filters and Rules
Incidents	Events resulting from Events correlation performed by the Correlation Engine on an Appliance
Internal Events	Events for activities within an appliance, such as a Rule firing or modifying a User Account
Nodes	Defines the remote systems that are sending information to SEM. Attributes include: • IP Address • Name • Associated Connector
Password Policy	Defines the minimum allowed password length and whether composition complexity is enforced
Rules	Defines conditions to be detected in the Events. Attributes include: • Name • Description • Conditions • Correlation Time • Actions • Status (e.g. Enabled) • User subscription
User Accounts	Defines the authorized users of an Appliance. Attributes include: • Username • Password • Role

1.8 Evaluated Configuration

The evaluated configuration consists of the following:

1. One instance of the SEM installed and executing on a supported hypervisor.

The following installation and configuration options must be used:

1. All User Accounts are defined as SEM Users.
2. Custom Widgets are not configured.
3. The Password Policy must be configured to require all passwords to meet complexity

requirements.

4. Administrators configure passwords in accordance with the password policies for their organization.
5. The SEM is configured for log message storage and Historical Events search.
6. The Enable Global Automatic Updates parameter is not set, since this could cause the TOE to be changed from the evaluated version.

2. Conformance Claims

2.1 Common Criteria Conformance

This ST and the TOE are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
  - Part 2 Extended

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
  - Part 3 Conformant

2.2 Security Requirement Package Conformance

This ST is conformant to the following assurance package:

- EAL2 Augmented (ALC_FLR.2).

2.3 Protection Profile Conformance

The ST do not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically, this chapter identifies:

a) assumptions about the environment,

b) threats to the assets, and

c) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and organisational security policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
A.NETWORK	There will be a network that supports communication between the TOE and the monitored network devices. This network functions properly.
A.NODISCLOSURE	Credentials passed between the TOE and remote users will be protected from disclosure.
A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the Operational Environment.

Table 4 - Threats

T.Type	Description
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to TSF data or User Data.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data to be modified.
T.UNIDENT_ACTIONS	The administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

T.Type	Description
T.COMM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between the TOE and user's web browser or SSH client.

3.4 Organisational Security Policies

An organisational security policy is a set of rules, practices, and procedures imposed by an organisation to address its security needs.

Table 5 - Organisational Security Policies (OSPs)

P.Type	Organisational Security Policy
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about element or network problems must be applied to data received from managed elements and appropriate notification to users generated.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PASSWORDS	Passwords for User Accounts defined in the TOE shall initially configured by Administrators.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 6 - Security Objectives for the TOE

O.Type	Description
O.AUDITS	The TOE must record audit records for data accesses and use of the system functions.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit and system data information in a human readable form.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.
O.MONITOR	The TOE will monitor the performance and status of the configured Managed Elements and generate alerts when configured conditions are detected.
O.PASSWORDS	The TOE will permit Administrators to configure passwords for User Accounts defined in the TOE.
O.TIME	The TOE will provide reliable timestamps.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.COMM	The TOE must protect confidentiality of its dialogue between itself and user's web browser or SSH client.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 7 - Security Objectives of the Operational Environment

OE.Type	Description
OE.COMM	The Operational Environment will protect communication between the TOE, SEM Agent and systems outside the TOE boundary from disclosure.
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
OE.INTROP	The IT Systems which the TOE monitors is interoperable with the TOE
OE.NETWORK	The Administrator will install and configure a network that supports communication between the TOE and the monitored network devices. The administrator will ensure that this network functions properly.

OE.Type	Description
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE.

5. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

5.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat, assumption, and organisational security policy is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 8 - Threats, Assumptions, and OSPs to Security Objectives Mapping

Security Objectives / Threats, OSPs & Assumptions	O.AUDITS	O.AUDIT_REVIEW	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TIME	O.TOE_ACCESS	O.COMM	OE.COMM	OE.ENVIRON	OE.INSTALL	OE.INTROP	OE.NETWORK	OE.NOEVILADMIN
A.ACCESS												X		
A.ENVIRON										X				
A.INSTALL											X			
A.NETWORK													X	
A.NODISCLOSURE									X					
A.NOEVILADMIN														X
P.ACCACT	X	X				X	X							
P.ACCESS			X				X							
P.ANALYZ				X										
P.MANAGE							X							
P.PASSWORDS					X									
T.MASQUERADE							X		X					
T.TSF_COMPROMISE			X											
T.UNIDENT_ACTIONS	X	X				X								
T.COMM								X						

The following table describes the rationale for the threats, assumptions, and organisational security policies to security objectives mapping.

Table 9 - Threats, Assumptions and OSPs to Security Objectives Rationale

TYPE	Security Objectives Rationale
A.ACCESS	The **OE.INTROP** objective ensures the TOE has the needed access.
A.ENVIRON	**OE.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.INSTALL	**OE.INSTALL** objective ensures the TOE is installed per the vendor guidance, which addresses scalability.
A.NETWORK	**OE.NETWORK** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NODISCLOSURE	**OE.COMM** addresses the policy by requiring the environment to supply functionality to protect the communication between remote systems and TOE components.
A.NOEVILADMIN	**OE.NOEVILADMIN** addresses this assumption by restating it as an objective for the Administrator to satisfy.
P.ACCACT	The **O.AUDITS** objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The **O.TIME** objective supports this policy by providing a time stamp for insertion into the audit records. The **O.TOE_ACCESS** objective supports this policy by ensuring each user is identified and authenticated. The **O.AUDIT_REVIEW** objective helps to mitigate this threat by providing the Administrator with the ability to review the actions taken by users.
P.ACCESS	**O.MANAGE** defines the access privileges to the data for the supported roles. **O.TOE_ACCESS** requires the TOE to control access based upon the user's role.
P.ANALYZ	**O.MONITOR** requires the TOE to analyze information collected from the managed elements to detect conditions specified by administrators.
P.MANAGE	**O.TOE_ACCESS** requires the TOE to control access based upon the user's role, which requires the TOE to bind a role to each user's session.
P.PASSWORDS	**O.PASSWORDS** addresses this policy by requiring the TOE to provide functionality for Administrators, but not non-Administrators, to configure passwords.
T.MASQUERADE	**O.TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. **OE.COMM** mitigates this threat by protecting data when it is transferred between remote systems and the TOE.
T.TSF_COMPROMISE	**O.MANAGE** is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data.
T.UNIDENT_ACTIONS	The **O.AUDITS** objective helps to mitigate this threat by recording actions for later review. The **O.AUDIT_REVIEW** objective helps to mitigate this threat by providing the Administrator with the ability to review the actions taken by administrators. The **O.TIME** helps to mitigate this threat by ensuring that correct timestamps are available for audit records.
T.COMM	The **O.COMM** objective helps to protect the confidentiality of its dialogue between SEM Manager and user's web browser or SSH client.

5.2 Security Requirements Rationale

5.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 10 - SFRs to Security Objectives Mapping

Security Objectives / SFRs	O.AUDITS	O.AUDIT_REVIEW	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TIME	O.TOE_ACCESS	O.COMM
FAU_GEN.1	X							
FAU_SAR.1		X						
FAU_SAR.2		X						
FIA_ATD.1			X				X	
FIA_SOS.1							X	
FIA_UAU.2							X	
FIA_UAU.7							X	
FIA_UID.2							X	
FIA_USB.1							X	
FMT_MTD.1			X		X			
FMT_SMF.1			X					
FMT_SMR.1			X		X			
FMT_MOF.1			X					
FNM_MDC.1				X				
FNM_ANL.1				X				
FNM_RCT.1				X				
FNM_RDR.1			X	X				
FPT_STM.1						X		
FTP_TRP.1								X

The following table provides the detail of TOE security objective(s).

Table 11 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDITS	**FAU_GEN.1** requires the TOE to generate audit log records for a specified set of security-relevant events.

Security Objective	SFR and Rationale
O.AUDIT_REVIEW	**FAU_SAR.1** requires the TOE to provide authorized users with a mechanism to review audit logs. **FAU_SAR.2** requires the TOE to prevent unauthorized users from reading the audit logs.
O.MANAGE	**FIA_ATD.1 (all iterations)** define the security attributes that must be able to be managed for users of the TOE. **FMT_MTD.1** defines the data access privileges associated with each role. **FMT_MOF.1** requires the TOE to specify the restrictions on which role is able to manage the TOE's user accounts **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported. **FNM_RDR.1** requires the TOE to provide information collected from managed elements to be displayed in human readable form.
O.MONITOR	**FNM_MDC.1** requires the TOE be able to collect and save information about the managed elements **FNM_ANL.1** requires the TOE to be able to analyze the information collected about the managed elements. **FNM_RCT.1** requires the TOE be able to generate alerts upon detection of configured conditions concerning the managed elements. **FNM_RDR.1** requires that data collected about the managed elements and analysis results be able to be viewed in human readable form.
O.PASSWORDS	**FMT_MTD.1** defines the access privileges for Administrators and non-Administrators, stating that only Administrators may configure passwords. **FMT_SMR.1** defines the specific security roles to be supported.
O.TIME	**FPT_STM.1** ensures that an accurate timestamp will be available for audit records
O.TOE_ACCESS	**FIA_ATD.1** defines the attributes of users, including a userid that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE (e.g., the TOE associates a userid with a role). **FIA_UID.2** requires that a user be identified to the TOE in order to access TOE functionality or data. **FIA_UAU.2** requires that a Console user be authenticated by the TOE before accessing TOE functionality or data. **FIA_UAU.7** provides that the authentication data provided by the user is not echoed back in plaintext, thus serving to protect that data. **FIA_USB.1 (all iterations)** defines the attributes that are bound to user sessions for the access mechanisms provided by the TOE. **FIA_SOS.1** supports the objective by ensuring that all passwords satisfy a minimum complexity policy

Security Objective	SFR and Rationale
O.COMM	**FTP_TRP.1** ensures that data sent between SEM Manager and user's web browser or SSH client is protected from modification or disclosure.

5.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

a) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

b) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from Part 3 of the Common Criteria.

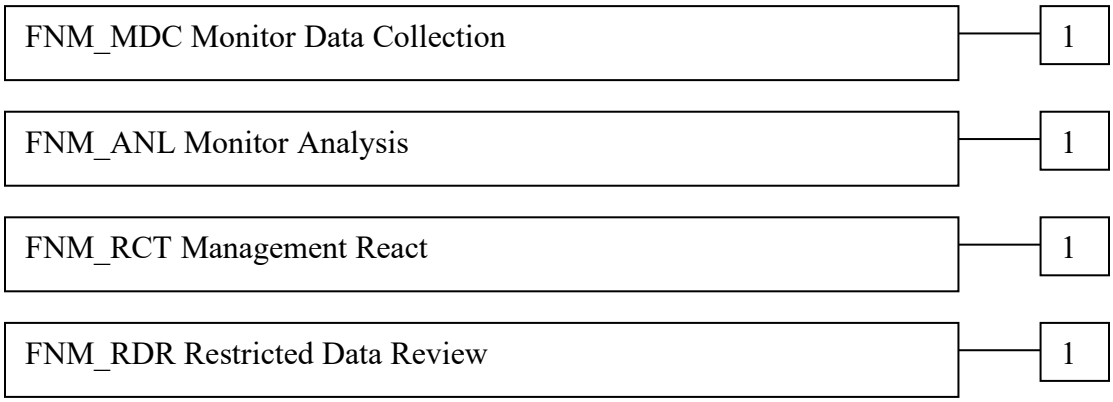
6. Extended Components Definition

6.1 Extended Security Functional Components

6.1.1 Class FNM: Network Management

All of the components in this section are derived from the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments

This class of requirements addresses the data collected and analysed by network management systems. The audit class of the CC (FAU) was used as a model for creating the IDS class in the Protection Profile, and the IDS class was used as a model for these requirements. The purpose of this class of requirements is to address the unique nature of network management data and provide for requirements about analysing, reviewing and managing the data. This document uses the term “Monitor data” to refer to the information collected and saved by the collection and analysis functions specified herein.

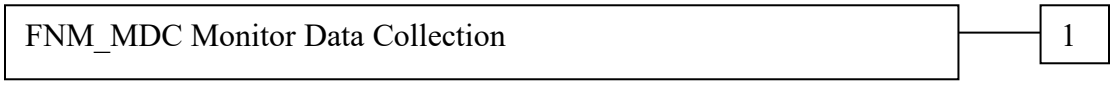


6.1.1.1 FNM_MDC Monitor Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding receipt of information related to the status and performance of managed elements.

Component Levelling:



FNM_MDC.1 Monitor Data Collection provides for the functionality to require TSF controlled processing of data received from managed elements regarding their status or performance.

Management:

The following actions could be considered for the management functions in FMT:

a) Management of the configuration information for real-time feeds.

Audit:

There are no auditable events foreseen.

FNM_MDC.1 Monitor Data Collection

Hierarchical to: No other components.

Dependencies: None

FNM_MDC.1.1 The TSF shall be able to normalize and store information received from remote systems via real-time feeds.

6.1.1.2 FNM_ANL Monitor Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of information related to status and performance received from managed elements.

Component Levelling:

FNM_ANL Monitor Analysis	1

FNM_ANL.1 Monitor Analysis provides for the functionality to require TSF controlled analysis of data received from monitored devices.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

FNM_ANL.1 Monitor Analysis

Hierarchical to: No other components.

Dependencies: FNM_MDC.1 Monitor Data Collection

FNM_ANL.1.1 The TSF shall perform the analysis function(s) configured for information received from monitored devices.

6.1.1.3 FNM_RCT Management React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information received from monitored devices.

Component Levelling:

FNM_RCT Management React	1

FNM_RCT.1 Management React provides for the functionality to require TSF controlled reaction to the analysis of data received from monitored devices

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

FNM_RCT.1 Management React

Hierarchical to: No other components.

Dependencies: FNM_ANL.1 Monitor Analysis

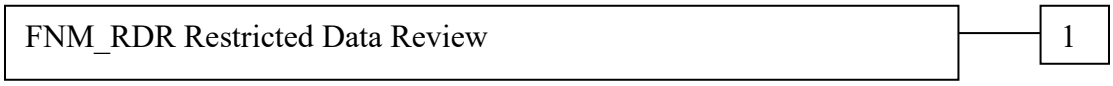
FNM_RCT.1.1 The TSF shall perform the specified action(s) when conditions specified by an authorized user are detected.

6.1.1.4 FNM_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the monitor data collected by the TOE.

Component Levelling:



FNM_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the monitor data collected by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the monitor data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read monitor data that are denied.

b) Detailed: Reading of information from the monitor data records.

FNM_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: FNM_MDC.1 Monitor Data Collection

FNM_ANL.1 Monitor Analysis

FNM_RDR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of Monitor data*] from the Monitor data.

FNM_RDR.1.2 The TSF shall provide the Monitor data in a manner suitable for the user to interpret the information.

FNM_RDR.1.3 The TSF shall prohibit all users read access to the Monitor data, except those users that have been granted explicit read-access.

6.2 Extended Security Assurance Components

None

7. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment*:* indicated in *italics*

Selection: indicated in underlined text

Assignments within selections: indicated in *italics and underlined text*

Refinement**:** indicated with **bold text** for additions**,** and ~~strike-through~~**,** for deletions.

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1) or FIA_USB.1.1(1)).

7.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

7.1.1 Security Audit (FAU)

7.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events in the following table*.

Table 12 - Auditable Events

SFR	Event	Details
FIA_ATD.1, FMT_MOF.1	User account changes	Type of change, user account
FIA_UAU.2, FIA_SOS.1	Successful Web Console login Failed Web Console login	User identity, IP address of the remote system
FIA_UID.2, FIA_SOS.1	Successful Web Console login Failed Web Console login	User identity, IP address of the remote system
FMT_MTD.1	Modifications to the values of TSF data	Entity changed
FIA_USB.1	User account creation	Username or role assignment
FPT_STM.1	Time management	Change of time or NTP server

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, *the information specified in the Details column of the Table 12 above*.

7.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized users except Contacts* with the capability to read *all data* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.1.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

7.1.2 Identification and Authentication (FIA)

7.1.2.1 FIA_ATD.1(1) User Attribute Definition (Web Console)

Refinement Rationale: The TOE provides multiple access mechanisms for users. The security attributes defined for the users vary based upon the mechanism. The collection of iterations addresses the user attribute definitions for the TOE access mechanisms.

FIA_ATD.1.1(1) The TSF shall maintain the following list of security attributes belonging to individual users **of the Web Console**:

1. *Username*
2. *Password*
3. *Role*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the Web Console.

7.1.2.2 FIA_ATD.1(2) User Attribute Definition (CMC Console)

FIA_ATD.1.1(2) The TSF shall maintain the following list of security attributes belonging to individual users **of the CMC Console**:

1. *Username*
2. *Password*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the CMC Console.

Application Note: CMC is a bash script that restricts access to the OS, cmc user is actually an OS user.

7.1.2.3 FIA_SOS.1(1) Verification of Secrets (Web Console)

FIA_SOS.1.1(1) The TSF shall provide a mechanism to verify that secrets meet *the following requirements:*

1. *The password length must be equal to or greater than the configured minimum length.*
2. *Passwords must not match or contain part of the user's user name.*
3. *Passwords must contain characters from three of the following four categories:*
    a. *English uppercase characters (A through Z).*
    b. *English lowercase characters (a through z).*
    c. *Base 10 digits (0 through 9).*
    d. *Non-alphanumeric characters (it's possible to use any Unicode character except control characters (0x00-0x1f; 0x7f-0x9f)).*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the Web Console

7.1.2.4 FIA_SOS.1(2) Verification of Secrets (CMC Console)

FIA_SOS.1.1(2) The TSF shall provide a mechanism to verify that secrets meet *the following requirements:*

1. *The password length must be between 12 and 255 characters.*
2. *Passwords must fulfil below requirements:*
    a. *Contains both upper- and lower-case characters.*
    b. *Contains at least one digit.*
    c. *Contains at least one special character.*
    d. *Does not contain following special characters:*
        i. *{}*
        ii. *[]*
        iii. *()*
        iv. *' or " or `*
        v. *~*
        vi. *;:.*
        vii. *<>*
        viii. *\/|*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the CMC Console. CMC account is a Debian OS account, so that the default password rules of Debian OS applied with additional password checking mentioned above.

7.1.2.5 FIA_UAU.2 User Authentication Before any Action

Refinement Rationale: Authentication is required for Console users.
FIA_UAU.2.1 The TSF shall require each **Console** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.2.6 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *dots* to the user while the authentication is in progress.

7.1.2.7 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The TSF shall require each **Console** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.1.2.8 FIA_USB.1(1) User-Subject Binding (Web Console)

FIA_USB.1.1(1) The TSF shall associate the following user security attributes with subjects acting on the behalf of that **Web Console** user:

1. *Username*
2. *Role*

FIA_USB.1.2(1) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **Web Console** users: *attributes are bound from*
the configured parameters for the identified user account.

FIA_USB.1.3(1) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **Web Console** users: *subject attributes do not change during a session.*

Application Note: Different security attributes are bound for different TOE access mechanisms. This iteration applies to security attributes for users of the Web Console.

7.1.2.9 FIA_USB.1(2) User-Subject Binding (CMC Console)

FIA_USB.1.1(2) The TSF shall associate the following user security attributes with subjects acting on the behalf of that **CMC Console** user:

1. *Username*

FIA_USB.1.2(2) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **CMC Console** users: *attributes are bound from the configured parameters for the identified user account.*
FIA_USB.1.3(2) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **CMC Console** users: *subject attributes do not change during a session.*

Application Note: Different security attributes are bound for different TOE access mechanisms. This iteration applies to security attributes for users of the CMC Console.

7.1.3 Security Management (FMT)

7.1.3.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create and execute* the *TSF data specified in Table 13* to *users with the roles and permissions specified in Table 13*.

Table 13 - TSF Data Detail

TSF Data	Administrator	Auditor	Monitor	Contact	Report	Guest
Connectors	Query, Create, Modify, Delete	Query (Names Only)	Query (Names Only)	None	None	Query (Names Only)
Dashboard Widgets	Query, Create, Delete, Execute	Query, Create, Delete, Execute	Query, Create, Delete, Execute	None	None	Query, Create, Delete, Execute
Events	Query	Query	Query	None	None	Query
Filters	Query, Create, Modify, Delete, Execute	Query, Create, Modify, Delete, Execute	Query (Names Only), Execute	None	None	Query, Create, Modify, Delete, Execute
Groups	Query, Create, Modify, Delete	Query (Names Only)	Query (Names Only)	None	None	Query (Names Only)
Nodes	Query, Create, Modify, Delete	Query (Names Only)	Query (Names Only)	None	None	Query (Names Only)
Password Policy	Query, Modify	Query	Query	None	None	Query
Rules	Query, Create, Modify, Delete	Query (Names only)	Query (Names Only)	None	None	Query (Names only)
User Accounts	Query, Create, Modify, Delete	Query (Name Only)	Query (Name Only)	None	None	Query (Name Only)

7.1.3.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. *Connectors Management (Query, Create, Modify, Delete)*
2. *Dashboard Widgets Management (Query, Create, Modify, Delete)*
3. *Filters Management (Query, Create, Modify, Delete)*
4. *Group Management (Query, Create, Modify, Delete)*
5. *Nodes Management (Query, Create, Modify, Delete)*
6. *Password Policy (Query, Modify)*
7. *Rules Management (Query, Create, Modify, Delete)*
8. *User Account Management (Query, Create, Modify, Delete)*

7.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. *Administrator*
2. *Auditor*
3. *Monitor*
4. *Contact*
5. *Report*
6. *Guest*

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

7.1.3.4 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions *User Accounts* to *Administrator*

7.1.4 Network Management (FNM)

7.1.4.1 FNM_MDC.1 Monitor Data Collection

FNM_MDC.1.1 The TSF shall be able to normalize and store information received from remote systems via real-time feeds.

7.1.4.2 FNM_ANL.1 Monitor Analysis

FNM_ANL.1.1 The TSF shall perform the analysis function(s) configured for information received from monitored devices.

7.1.4.3 FNM_RCT.1 Management React

FNM_RCT.1.1 The TSF shall perform the specified action(s) when conditions specified by an authorized user are detected.

Application Note: For details of actions can take to respond to events, please refer SEM Administrators guide. Section "Actions SEM can take to respond to events".

7.1.4.4 FNM_RDR.1 Restricted Data Review

Refinement Rationale: Events are visible under the "Events" tab real time for monitoring purpose. Authorized user is able to query/read events data.

FNM_RDR.1.1 The TSF shall provide *authorized users except Contacts users* with the capability to read *all data* from the ~~Monitor data~~**Events**.

FNM_RDR.1.2 The TSF shall provide the ~~Monitor data~~**Events** in a manner suitable for the user to interpret the information.

FNM_RDR.1.3 The TSF shall prohibit all users read access to the ~~Monitor data~~**Events**, except those users that have been granted explicit read-access.

7.1.5 Protection of the TSF (FPT)

7.1.5.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps.

7.1.6 Trusted Path (FTP)

7.1.6.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, *and all further communication after authentication*.

7.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 and is augmented by ALC_FLR.2. These requirements are summarized in the following table.

Table 14 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

7.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 15 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FIA_ATD.1(1)	No other components.	None	N/A
FIA_ATD.1(2)	No other components.	None	N/A
FIA_SOS.1(1)	No other components.	None	N/A

SFR	Hierarchical To	Dependency	Rationale
FIA_SOS.1(2)	No other components.	None	N/A
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_UID.2	FIA_UID.1	None	N/A
FIA_USB.1(1)	No other components.	FIA_ATD.1	Satisfied by FIA_ATD.1(1)
FIA_USB.1(2)	No other components.	FIA_ATD.1	Satisfied by FIA_ATD.1(2)
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied, Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied, Satisfied
FMT_SMF.1	No other components.	None	N/A
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FNM_MDC.1	No other components.	None	N/A
FNM_ANL.1	No other components.	FNM_MDC.1	Satisfied
FNM_RCT.1	No other components.	FNM_ANL.1	Satisfied
FNM_RDR.1	No other components.	FNM_MDC.1, FNM_ANL.1	Satisfied, Satisfied
FPT_STM.1	No other components.	None	N/A
FTP_TRP.1	No other components.	None	N/A

8. TOE Summary Specification

8.1 Security Functions

8.1.1 Audit

Relevant SFRs: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FPT_STM.1

The TOE generates audits for the events specified in the table included with FAU_GEN.1. Startup and shutdown of the audit function is equivalent to starting and stopping the SEM. The following fields are included in all audit log records, although not all fields are populated in all records:

- Date/time
- Event Type
- Event information (details of the event)
- User performing the action (if applicable)

Audit records are encrypted and stored in the SEM database. Audit records may be viewed via the Console by viewing Events. All authorized users except Contacts have access to all audit records, subject to the configured Dashboard Widgets and Filters (FAU_SAR.1, FAU_SAR.2). The TOE by default will synchronize date and time with Hypervisor and provide a reliable time stamps to ensures that an accurate timestamp will be available for audit records (FPT_STM.1)

8.1.2 Identification and Authentication

Relevant SFRs: FIA_ATD.1(1), FIA_ATD.1(2)FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1(1), FIA_USB.1(2)

When a Console session is initiated, the TOE collects a username and password from the user. Dots are echoed for each character supplied for the password (FIA_UAU.7). Once the credentials are supplied, they are validated by the TOE (FIA_UID.2, FIA_UAU.2). If the credentials are not valid, an error message is displayed, and the user may try again. If the credentials are valid, the security attributes configured for the supplied username (FIA_ATD.1(1), FIA_ATD.1(2)) are bound to the session (FIA_USB.1(1), FIA_USB.1(2)) and the user is given access to the management functions.

8.1.3 Management

Relevant SFRs: FMT_MTD.1, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FIA_SOS.1

Management functionality is available to authorized users through the Console. The management functionality available to users is specified in FMT_SMF.1. The functionality made available to individual users is dependent on their security attributes (role). The roles are specified in FMT_SMR.1, and the access privileges available and associated security attributes are specified in FMT_MTD.1. When administrators configure passwords, the TOE enforces minimum complexity rules (FIA_SOS.1). Only the Administrator has the ability to modify the user accounts of the TOE (FMT_MOF.1)

8.1.4 Log and Event Management

Relevant SFRs: FNM_ANL.1, FNM_MDC.1, FNM_RCT.1, FNM_RDR.1

Log and event management is performed against monitored devices that provide information to SEM. The data received by SEM is normalized and saved (FNM_MDC.1). Information collected is analyzed according to the configured Rules (FNM_ANL.1). Incidents may be generated based upon conditions detected from the monitored devices and the actions configured in triggered Rules are taken (FNM_ANL.1, FNM_RCT.1).

Events (Alerts, Incidents, and Internal Events) are only available to authorized users of the TOE except Contacts via the Console (FNM_RDR.1). The TOE provides the capability to read these data from the Monitor data. Real-time views are available in the Console via Dashboard Widgets and Filters. Queries against saved data can be performed via the Console (Historical Events).

The information collected from the monitored devices, as well as the analysis results, is saved in the TOE database and may be reviewed by authorized users only.

8.1.5 Secure Communication

Relevant SFR: FTP_TRP.1

The TOE can protect the user data from disclosure and modification by using Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) protocols to provide communication security over a computer network (FTP_TRP.1). It protects data transmitted between SEM Manager and user's web browser or SSH client.