# SolarWinds Log and Event Manager Software

# Security Target

Version 1.5

August 25, 2014

SolarWinds Worldwide, LLC
3711 South MoPac Expressway
Building Two
Austin, Texas 78746

## DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

SolarWinds Worldwide, LLC
3711 South MoPac Expressway
Building Two
Austin, Texas 78746
http://www.solarwinds.com

## REVISION HISTORY

| Rev | Description |
|---|---|
| 1.0 | October 30, 2013, Initial release |
| 1.1 | December 16, 2013, Consistency with ADV documents |
| 1.2 | January 17, 2014, Addressed lab ORs/CRs |
| 1.3 | April 2, 2014, Addressed lab ADV ORs/CRs |
| 1.4 | April 16, 2014, Clarified audit records |
| 1.5 | August 25, 2014, Updated versions of TOE components |

## TABLE OF CONTENTS

## LIST OF TABLES

## ACRONYMS LIST

**CC** ..... **Common Criteria**
**CPU** ..... **Central Processing Unit**
**EAL** ..... **Evaluation Assurance Level**
**GB** ..... **GigaByte**
**GHz** ..... **GigaHertz**
**GUI** ..... **Graphical User Interface**
**IDS** ..... **Intrusion Detection System**
**IP** ..... **Internet Protocol**
**IT** ..... **Information Technology**
**I&A** ..... **Identification and Authentication**
**LEM** ..... **Log and Event Management**
**OS** ..... **Operating System**
**SFR** ..... **Security Functional Requirement**
**SIEM** ..... **Security Information and Event Management**
**ST** ..... **Security Target**
**TOE** ..... **Target of Evaluation**
**TSF** ..... **TOE Security Function**

# 1. Security Target Introduction

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

## 1.1 Security Target Reference

SolarWinds Log and Event Manager Software Security Target, version 1.5, August 25, 2014.

## 1.2 TOE Reference

SolarWinds Log and Event Manager (LEM) V5.7.0 and Log & Event Manager Reports V5.7.0 (Build 9)

## 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 4, and augmented by ALC_FLR.2.

## 1.4 Keywords

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

## 1.5 TOE Overview

### 1.5.1 Usage and Major Security Features

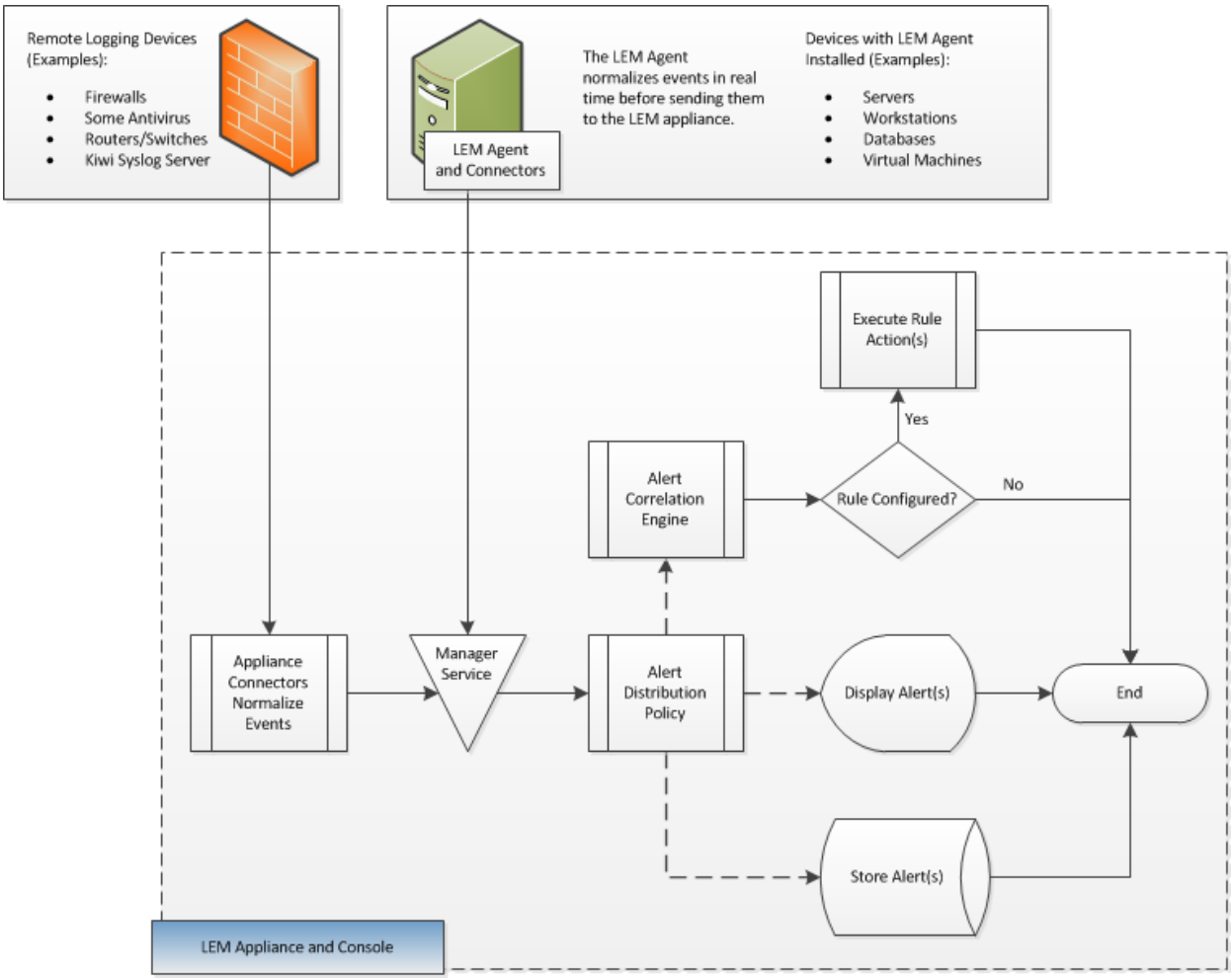
LEM collects, stores, and normalizes log and event data from a variety of sources, and displays that data in a web interface for monitoring, searching, and analysis. Data is also available for scheduled and ad hoc reporting.

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

Alerts are created from normalized data. Alerts are containers LEM uses to display events/messages from LEM monitored devices. Log data is processed by LEM'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 LEM database for future analysis and reporting within the Reports application. 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 LEM.

**Figure 1 - Basic Data Flow**




Within LEM, 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 nDepth or Reports.

Users primarily interact with LEM with the Console, which is a GUI interface accessed via web browsers from remote workstations. Both real-time viewing and historical viewing (via nDepth) may be performed. The Console supports multiple roles. Roles are assigned to sessions when users successfully complete Identification and Authentication with LEM. Credentials are collected via the GUI and validated by LEM. LEM also supports credential validation by a third-party authentication server, but this functionality is not included in the evaluation.

A Console application may be installed on Windows workstations, and provides comparable functionality to the Console access via browsers. The Console application is not included in the evaluation.

Users may also interact with LEM via a Reports application running on Windows workstations. The application may be used to run, schedule, and view Reports that present information from LEM. All users of the Reports application have full access to all data that the Reports are designed to access. Access to LEM via the Reports application is restricted by authorizing access for specific IP addresses (of Windows workstations that are authorized to use the Reports application).

### 1.5.2 TOE type

Network Management

### 1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of two components: a virtual appliance providing the collection and processing of log and event information, and a desktop component supporting user access to the collected information via a Windows application (Reports).

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

**Table 1 - Virtual Platform Minimum Requirements**

| Item | Requirements |
|---|---|
| Virtualization Software | VMware vSphere 4 or later<br>Microsoft Hyper-V 2008 R2<br>Microsoft Hyper-V 2012 |
| CPU Speed | 2 GHz |
| Memory | 8 GB |
| Hard Drive Space | 250 GB |

The desktop component software is installed on each system authorized to access the LEM data and satisfies the following minimum requirements.

**Table 2 - Desktop Minimum Requirements**

| Item | Requirements |
|---|---|
| Operating System | Windows XP<br>Windows Vista<br>Windows 7<br>Windows Server 2003<br>Windows Server 2008<br>Windows Server 2008 R2 |
| CPU | 1 GHz Pentium III or equivalent |
| Memory | 1 GB |
| Hard Drive Space | 5 GB |
| Adobe Flash | Flash Player 11 |
| Browser | Microsoft Internet Explorer 8 and later<br>Mozilla Firefox 10 and later<br>Google Chrome 17 and later |

Console users and Reports applications communicate with LEM virtual appliances 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

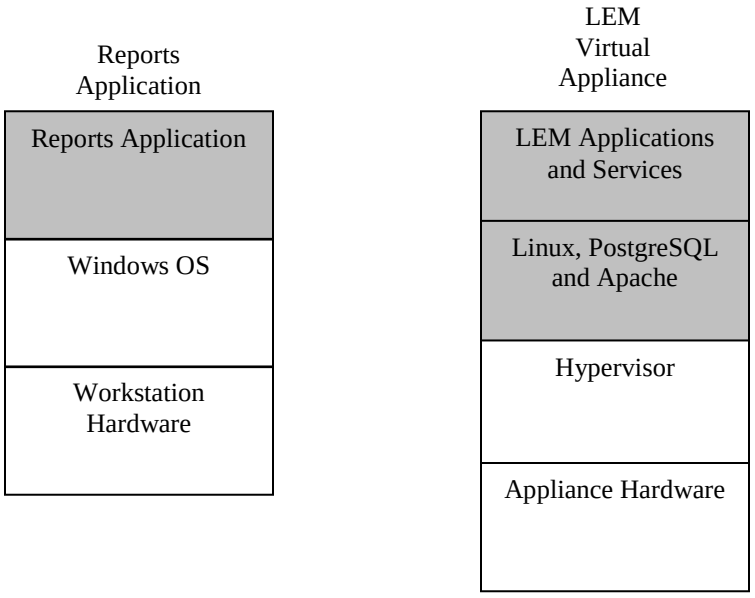
LEM acts as a monitoring and management tool for use by network managers. It collects logs and events from multiple remote third-party systems, and alerts the network managers to specified conditions.

Users interact with the TOE via multiple mechanisms. Consoles are provided for remote interaction with users and administrators for configuration and data access. The Reports application may be used to review data collected by the TOE.

#### 1.6.1 Physical Boundary

The TOE consists of the LEM virtual appliance and the Reports application. The physical boundary of the TOE is depicted in the following diagram (shaded items are within the TOE boundary).

**Figure 2 - Physical Boundary**




The physical boundary includes the following guidance documentation:

1. *SolarWinds Log & Event Manager Quick Start Guide*
2. *SolarWinds Log & Event Manager User Guide*
3. *SolarWinds Log & Event Manager Common Criteria Supplement*

### 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 and/or Reports 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 – Management functionality is provided to authorized users. The functionality provided to individual users is determined by the user's role, which is one of the security attributes for users.
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.

The following functionality included in the LEM product suite is not evaluated:

- LEM Desktop Console application.
- Agents executing on remote systems.
- Receipt and processing of NetFlow information.
- Directory Service query tool.
- Actions dependent upon agents installed on remote systems.

### 1.6.3 TSF Data

The following table describes the TSF data.

**Table 3 - 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:<br>• Alias (user friendly name)<br>• Log file used to hold messages<br>• 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:<br>• Event Name<br>• Event Information<br>• Insertion IP (name/address of the Appliance that inserted the Event into the database)<br>• Manager (name/address of the controlling Appliance)<br>• DetectionIP (name/address of the system on which the Event occurred)<br>• InsertionTime (time the Event was inserted into the database)<br>• DetectionTime (time the Event was detected on the remote system or Appliance)<br>• Severity<br>• 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 LEM. Attributes include:<br>• IP Address<br>• Name<br>• 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:<br>• Name<br>• Description<br>• Conditions<br>• Correlation Time<br>• Actions<br>• Status (e.g. Enabled)<br>• User subscriptions |
| User Accounts | Defines the authorized users of an Appliance. Attributes include:<br>• User Name<br>• Password<br>• Role |

## 1.7 Evaluated Configuration

The evaluated configuration consists of the following:

1. One instance of the LEM, installed and executing on a supported virtualization server.
2. One or more instances of the Reports application, executing on a supported Windows workstation.

The following installation and configuration options must be used:

1. Access from Reports applications to LEM Appliances is restricted by the IP address of the system on which the Reports application is executing.
2. Access to the Reports application on workstations is restricted to workstation users authorized to access the TOE.
3. All User Accounts are defined as LEM Users.
4. Custom Widgets are not configured.
5. The Password Policy must be configured to require all passwords to meet complexity requirements.
6. Administrators configure passwords in accordance with the password policies for their organization.
7. Administrators do not assign the Guest role for user accounts. This role currently has the same access privileges as the Auditor role, but SolarWinds may change the privileges for this role in future releases.
8. The LEM appliance is configured for log message storage and nDepth search.
9. 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

Common Criteria version: Version 3.1 Revision 4, dated September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

## 2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2.

The TOE does not claim conformance to any security functional requirement packages.

## 2.3 Protection Profile Conformance

The TOE does 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 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 4 - Assumptions**

| A.Type | Description |
|---|---|
| A.ACCESS | The TOE has access to all the IT System data it needs to perform its functions. |
| A.ASCOPE | The TOE is appropriately scalable to the IT Systems the TOE monitors. |
| 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 distributed components of the TOE. This network functions properly. |
| A.NOEVILADMIN | Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going. |

## 3.3 Threats

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

**Table 5 - Threats**

| T.Type | Description |
|---|---|
| T.MASQUERADE | A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources. |
| 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. |

## 3.4 Organisational Security Policies

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

**Table 6 - Organizational Security Policies**

| P.Type | Organizational 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.DISCLOSURE | Credentials passed between the TOE and remote users will be protected from disclosure. |
| P.MANAGE | The TOE shall only be managed by authorized users. |
| P.PASSWORDS | Passwords for User Accounts defined in the TOE are only 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 7 - 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 data received from remote systems and generate Incidents and take specified actions when configured conditions are detected. |
| O.PASSWORDS | The TOE will permit Administrators to configure passwords for User Accounts defined in the TOE. Users may not configure passwords, even for their own account. |
| 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. |

## 4.2 Security Objectives for the Operational Environment

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

**Table 8 - Security Objectives of the Operational Environment**

| OE.Type | Description |
|---|---|
| OE.COMM | The Operational Environment will protect communication between the TOE 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 TOE is interoperable with the IT Systems it monitors. |
| OE.NETWORK | The Administrator will install and configure a network that supports communication between the distributed TOE components. The administrator will ensure that this network functions properly. |
| OE.NOEVILADMIN | Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going. |

| OE.Type | Description |
|---|---|
| OE.REPORTS | Administrators on Windows systems that are authorized to access the Reports functionality on the LEM appliance shall restrict access to the Reports Application to authorized users of the Reports functionality. |

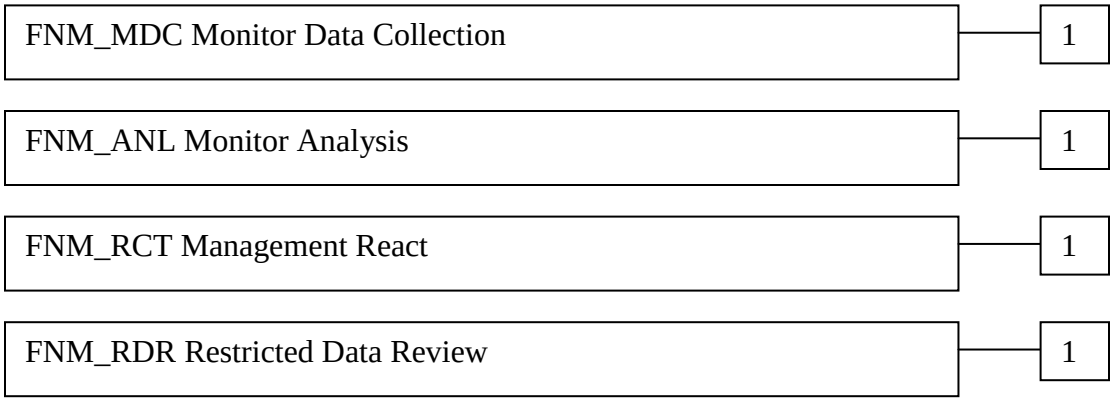
# 5. Extended Components Definition

## 5.1 Extended Security Functional Components

### 5.1.1 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 analyzed 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 analyzing, reviewing and managing the data.

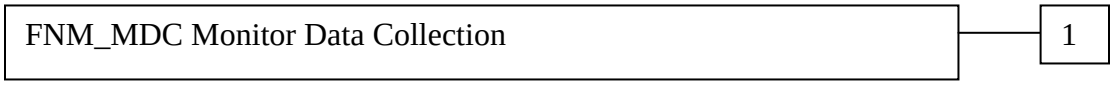



#### 5.1.1.1 FNM_MDC Monitor Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding receipt of information from monitored devices.

Component Levelling:




FNM_MDC.1 Monitor Data Collection provides for the functionality to require TSF controlled processing of data received from monitored devices.

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.

#### 5.1.1.2 FNM_ANL Monitor Analysis

Family Behaviour:

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

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.

#### 5.1.1.3 FNM_RCT.1 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.

#### 5.1.1.4 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 Restricted Data Review | 1 |

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.

## 5.2 Extended Security Assurance Components

None

# 6. 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**

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)).

## 6.1 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.

### 6.1.1 Security Audit (FAU)

#### 6.1.1.1 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 9 - Auditable Events**

| SFR | Event | Details |
|---|---|---|
| FIA_ATD.1 | User account changes | Type of change, user account |
| FIA_UAU.2 | Successful Console login<br>Failed Console login | User identity, IP address of the remote system |
| FIA_UID.2 | Successful Console login<br>Failed Console login | User identity, IP address of the remote system |
| FMT_MTD.1 | Modifications to the values of TSF data | Entity changed |
| | Scheduled Report started | IP address Reports application is executing on, Report name |
| | Scheduled Report completed | IP address Reports application is executing on, Report name |
| | Scheduled Report failed | IP address Reports application is executing on, Report name |

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, *no additional information*.

#### 6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *all 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.

#### 6.1.1.3 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.

### 6.1.2 Identification and Authentication (FIA)

#### 6.1.2.1 FIA_ATD.1 User Attribute Definition

*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 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 Console.*

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

1. *Role*

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

*Application Note: The Reports role is explicitly assigned to each user that accesses the LEM appliance using the Reports application.*

#### 6.1.2.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.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 (!, $, #, %, ^, etc.).*

#### 6.1.2.3 FIA_UAU.2 User Authentication Before any Action

*Refinement Rationale: Authentication is required for Console users Access to the Reports application on authorized systems is restricted via Windows permissions (OE.REPORTS).*

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.

#### 6.1.2.4 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.

#### 6.1.2.5 FIA_UID.2 User Identification Before any Action

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

#### 6.1.2.6 FIA_USB.1 User-Subject Binding

*Refinement Rationale: The TOE provides multiple access mechanisms for users. The security attributes bound to a session for the users vary based upon the mechanism. Therefore, iterations for this SFR are specified for each access mechanism. The collection of iterations addresses the user attribute definition for all TOE access mechanisms.*

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

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

1. *Role*

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 **Reports application** users: *attributes are implicitly bound based on the access mechanism.*

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 **Reports application** 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 Reports applications.*

### 6.1.3 Security Management (FMT)

#### 6.1.3.1 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 the following table* to *users with the roles specified in the following table*.

**Table 10 - TSF Data Detail**

| TSF Data | Administrator | Auditor | Monitor | Contact | Report |
|---|---|---|---|---|---|
| Connectors | Query, Create, Modify, Delete | Query | None | None | None |
| Dashboard Widgets | Query, Create, Delete, Execute | Query, Create, Delete, Execute | Query, Execute | None | None |
| Events | Query | Query | Query | None | Query |

| TSF Data | Administrator | Auditor | Monitor | Contact | Report |
|---|---|---|---|---|---|
| Filters | Query, Create, Modify, Delete, Execute | Query, Create, Modify, Delete, Execute | Query (Names only), Execute | None | None |
| Groups | Query, Create, Modify, Delete | Query (Names only) | Query (Names only) | None | Query |
| Nodes | Query, Create, Modify, Delete | Query | Query | None | Query |
| Password Policy | Query, Modify | Query | Query | None | None |
| Rules | Query, Create, Modify, Delete | Query | Query (Names only) | None | Query (Names only) |
| User Accounts | Query, Create, Modify, Delete | Query | Query (User Names only) | None | Query (User Names only) |

*Application Note: Access permissions for Alerts, Incidents and Internal Events are addressed by the Events row.*

#### 6.1.3.2 FMT_SMF.1 Specification of Management Functions

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

1. *User Account management*
2. *Rules management*
3. *Node management*
4. *Connector management.*

#### 6.1.3.3 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*

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

*Application Note: The Report role is automatically assumed for all users of the Reports application; it is never configured by an Administrator.*

### 6.1.4 Network Management (FNM)

#### 6.1.4.1 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.

#### 6.1.4.2 FNM_ANL.1 Monitor Analysis

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

#### 6.1.4.3 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.

#### 6.1.4.4 FNM_RDR.1 Restricted Data Review

FNM_RDR.1.1 The TSF shall provide *authorized users except Contacts* with the capability to read *all 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.

### 6.1.5 Protection of the TSF (FPT)

#### 6.1.5.1 FPT_STM.1 Reliable Time Stamps

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

## 6.2 TOE Security Assurance Requirements

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

**Table 11 - EAL2 Assurance Requirements**

| Assurance Class | Component ID | Component Title |
|---|---|---|
| Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.2 | Security-enforcing functional specification |
| | ADV_TDS.1 | Basic design |
| Guidance Documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| 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 |
| Tests | ATE_COV.1 | Evidence of coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing - sample |
| Vulnerability Assessment | AVA_VAN.2 | Vulnerability analysis |

## 6.3 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 12 - 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 | No other components. | None | n/a |
| FIA_SOS.1 | No other components. | None | n/a |
| FIA_UAU.2 | FIA_UAU.1 | FIA_UID.1 | Satisfied by FIA_UID.2 |
| FIA_UAU.7 | No other components. | FIA_UAU.1 | Satisfied by FIA_UAU.2 |
| FIA_UID.2 | FIA_UID.1 | None | n/a |
| FIA_USB.1 | No other components. | FIA_ATD.1 | Satisfied |
| FMT_MTD.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 |
| 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 |

# 7. TOE Summary Specification

## 7.1 Security Functions

## 7.2 Audit

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

The TOE generates audits for the events specified in the table included with FAU_GEN.1(1). Startup and shutdown of the audit function is equivalent to starting and stopping the LEM appliance. 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 stored in plaintext in the LEM database. Audit records may be viewed via the Console by viewing Events, or via the Reports application. All authorized users except Contacts have access to all audit records, subject to the configured Dashboard Widgets and Filters.

### 7.2.1 Identification and Authentication

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

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) are bound to the session (FIA_USB.1) and the user is given access to the management functions.

When the Reports application interacts with the TOE, the source IP address is checked against the authorized addresses. If it is in the list, the interaction is allowed; otherwise the request is dropped (FIA_UID.2). For authorized interactions, the Role is automatically set to Reports (FIA_USB.1).

### 7.2.2 Management

Relevant SFRs: FIA_SOS.1, FMT_MTD.1(*), FMT_SMF.1, FMT_SMR.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).

Limited management functionality is available through the Reports application. Users may query information from the TOE using the preconfigured reports available with the application (FMT_MTD.1).

### 7.2.3 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 LEM. The data received by LEM 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 available to users of the TOE via the Console and Reports (FNM_RDR.1). Real-time views are available in the Console via Dashboard Widgets and Filters. Queries against saved data can be performed via the Console (nDepth) or Reports.

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. 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.

## 8.1 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 and assumption is addressed by a security objective.

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

**Table 13 - Threats and Assumptions to Security Objectives Mapping**

| | O.AUDITS | O.AUDIT_REVIEW | O.MANAGE | O.MONITOR | O.PASSWORDS | O.TIME | O.TOE_ACCESS | OE.COMM | OE.ENVIRON | OE.INSTALL | OE.INTROP | OE.NETWORK | OE.NOEVILADMIN | OE.REPORTS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.ACCESS | | | | | | | | | | | X | | | |
| A.ASCOPE | | | | | | | | | | X | | | | |
| A.ENVIRON | | | | | | | | | X | | | | | |
| A.INSTALL | | | | | | | | | | X | | | | |
| A.NETWORK | | | | | | | | | | | | X | | |
| A.NOEVILADMIN | | | | | | | | | | | | | X | |
| P.ACCACT | X | | | | | X | X | | | | | | | |
| P.ACCESS | | | X | | | | X | | | | | | | X |
| P.ANALYZ | | | | X | | | | | | | | | | |
| P.DISCLOSURE | | | | | | | | X | | | | | | |
| P.MANAGE | | | | | | | X | | | | | | | X |
| P.PASSWORDS | | | | | X | | | | | | | | | |
| T.MASQUERADE | | | | | | | X | X | | | | | | |
| T.TSF_COMPROMISE | | | X | | | | | | | | | | | |
| T.UNIDENT_ACTIONS | X | X | | | | X | | | | | | | | |

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

**Table 14 - Threats, Assumptions and Policies to Security Objectives Rationale**

| x.TYPE | Security Objectives Rationale |
|---|---|
| A.ACCESS | The **OE.INTROP** objective ensures the TOE has the needed access. |
| A.ASCOPE | The **OE.INSTALL** objective ensures the TOE is installed per the vendor guidance, which addresses scalability. |
| A.ENVIRON | **OE.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy. |
| A.INSTALL | **OE.INSTALL** addresses this assumption by restating it as an objective for the Administrator to satisfy. |
| A.NETWORK | **OE.NETWORK** addresses this assumption by restating it as an objective for the Administrator to satisfy. |
| 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 OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.TOE_ACCESS objective supports this objective by ensuring each user is identified and authenticated. |
| P.ACCESS | **O.MANAGE** defines the access privileges to the data for the supported roles.<br>**O.TOE_ACCESS** requires the TOE to control access based upon the user's role.<br>**OE.REPORTS** requires Windows administrators to control access to the Reports Application to users authorized for access to TOE data. |
| P.ANALYZ | **O.MONITOR** requires the TOE to analyze information collected from the managed elements to detect conditions specified by administrators. |
| P.DISCLOSURE | **OE.COMM** addresses the policy by requiring the environment to supply functionality to protect the communication between remote systems and TOE components. |
| 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.<br>**OE.REPORTS** requires Windows administrators to control access to the Reports Application to users authorized for access to TOE data. |
| 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.<br>**OE.COMM** mitigates this threat by protecting sesnitive data from disclosure 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.<br>The **O.AUDIT_REVIEW** objective helps to mitigate this threat by providing the Administrator with the ability to review the actions taken by administrators.<br>The **O.TIME** helps to mitigate this threat by ensuring that correct timestamps are available for audit records. |

## 8.2 Security Requirements Rationale

### 8.2.1 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 15 - SFRs to Security Objectives Mapping**

| | O.AUDITS | O.AUDIT_REVIEW | O.MANAGE | O.MONITOR | O.PASSWORDS | O.TIME | O.TOE_ACCESS |
|---|---|---|---|---|---|---|---|
| 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 | | |
| FNM_MDC.1 | | | | X | | | |
| FNM_ANL.1 | | | | X | | | |
| FNM_RCT.1 | | | | X | | | |
| FNM_RDR.1 | | | X | X | | | |
| FPT_STM.1 | | | | | | X | |

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

**Table 16 - Security Objectives to SFR Rationale**

| Security Objective | SFR and Rationale |
|---|---|
| O.AUDIT | **FAU_GEN.1** requires the TOE to generate audit log records for a specified set of security-relevant events. |
| O.AUDIT_REVIEW | **FAU_SAR.1** requires the TOE to provide authorized users with a mechanism to review audit logs.<br>**FAU_SAR.2** requires the TOE to prevent unauthorized users from reading the audit logs. |

| Security Objective | SFR and Rationale |
|---|---|
| O.MANAGE | **FIA_ATD.1(*)** define the security attributes that must be able to be managed for users of the TOE.<br>**FMT_MTD.1(*)** define the data access privileges associated with each role.<br>**FMT_SMF.1** defines the specific security management functions to be supported.<br>**FMT_SMR.1** defines the specific security roles to be supported.<br>**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<br>**FNM_ANL.1** requires the TOE to be able to analyze the information collected about the managed elements.<br>**FNM_RCT.1** requires the TOE be able to generate alerts upon detection of configured conditions concerning the managed elements.<br>**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(*)** define the access privileges for Administrators and non-Administrators, explicitly stating that only Administrators may configure passwords for User Accounts defined in the TOE.<br>**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.<br>**FIA_SOS.1** supports the objective by ensuring that all passwords satisfy a minimum complexity policy.<br>**FIA_UID.2** requires that a user be identified to the TOE in order to access TOE functionality or data.<br>**FIA_UAU.2** requires that a Console user be authenticated by the TOE before accessing TOE functionality or data.<br>**FIA_UAU.7** provides that the authentication data provided by the user is not echoed back in plaintext, thus serving to protect that data.<br>**FIA_USB.1(*)** defines the attributes that are bound to user sessions for the access mechanisms provided by the TOE. |

### 8.2.2 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 from part 3 of the Common Criteria.