# EMC Corporation
# EMC® VoyenceControl™ v4.1.0

# Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.6

Prepared for:

**EMC Corporation**
176 South Street
Hopkinton, MA 01748
Phone: (508) 435-1000

http://www.emc.com

Prepared by:

**Corsec Security, Inc.**
10340 Democracy Lane, Suite 201
Fairfax, VA  22030
Phone: (703) 267-6050

http://www.corsec.com

# Revision History

| Version | Modification Date | Modified By | Description of Changes |
|---|---|---|---|
| 0.1 | 2008-11-21 | Nathan Lee | Initial draft. |
| 0.2 | 2009-05-15 | Christopher Lockard | Addressed OR1-5 and CR1-5. |
| 0.3 | 2009-05-29 | Christopher Lockard | Further updates based on previous ORs. |
| 0.4 | 2009-06-23 | Christopher Lockard | Further updates based on EVC-ASE-INT-CR-5. |
| 0.5 | 2009-07-21 | Christopher Lockard | Further updates based on CB-OR-2 |
| 0.6 | 2009-08-06 | Christopher Lockard | Further updates based on evaluator ORs and CRs. Specification of Solaris 10 (Release 6/06) |

# Table of Contents

# Table of Figures

# Table of Tables

# 1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is EMC VoyenceControl v4.1.0, and will hereafter be referred to as the TOE throughout this document. The TOE is an automated compliance management, change management, and configuration management solution.

## 1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem Definition (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

## 1.2 Security Target and TOE References

**Table 1 - ST and TOE References**

| | |
|---|---|
| **ST Title** | EMC Corporation EMC® VoyenceControl™ v4.1.0 Security Target |
| **ST Version** | Version 0.6 |
| **ST Author** | Corsec Security, Inc.<br>Nathan Lee |
| **ST Publication Date** | 2009-08-06 |
| **TOE Reference** | EMC® VoyenceControl™ v4.1.0 build 863 |
| **Keywords** | automated compliance management, change management, configuration management |

## 1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

VoyenceControl is an automated compliance management, change management, and configuration management solution. It allows administrators to collaboratively design their network infrastructure while enforcing control over change processes. It also checks for and enforces compliance with corporate and regulatory requirements. End-users (both administrative and non-privileged) primarily use VoyenceControl as the central management "hub" for their IT[1] infrastructure – all changes to infrastructure devices are made via VoyenceControl, which performs full auditing and compliance checking of every change and pushes the changes out to the managed devices.

### 1.3.1 Brief Description of the Components of the TOE

VoyenceControl embodies a client-server architecture and consists of four (4) main components:

- Application and Database Server – The central management "hub" of the product. Also stores the data gathered and generated by the product, including device configuration data and audit data.
- Advisor Server – Hosts the report generators that analyze the device data stored by the product.
- Device Server(s) – Communicates with the managed devices on the network on behalf of the Application Server.
- Management Client ("Thick Client") – Provides the primary administrative user interface for the product.

Each of these components is modular, and can be installed on a server by itself or can be installed together with other components on the same server. The components are shown in Figure 1 below (in the figure, the Database Server and the Application Server are shown installed on the same physical server). VoyenceControl supports the following server operating system (OS) types:

- Windows Server 2003 Enterprise Edition Service Pack 1
- Red Hat Enterprise Linux 5 Server (update 3, x86_64)
- Red Hat Enterprise Linux 5 Advanced Platform (update 3, x86_64)
- Solaris 10 (Release 6/06)

The TOE requires Java version 1.6 update 12 or later be installed to function.

[1] IT – Information Technology

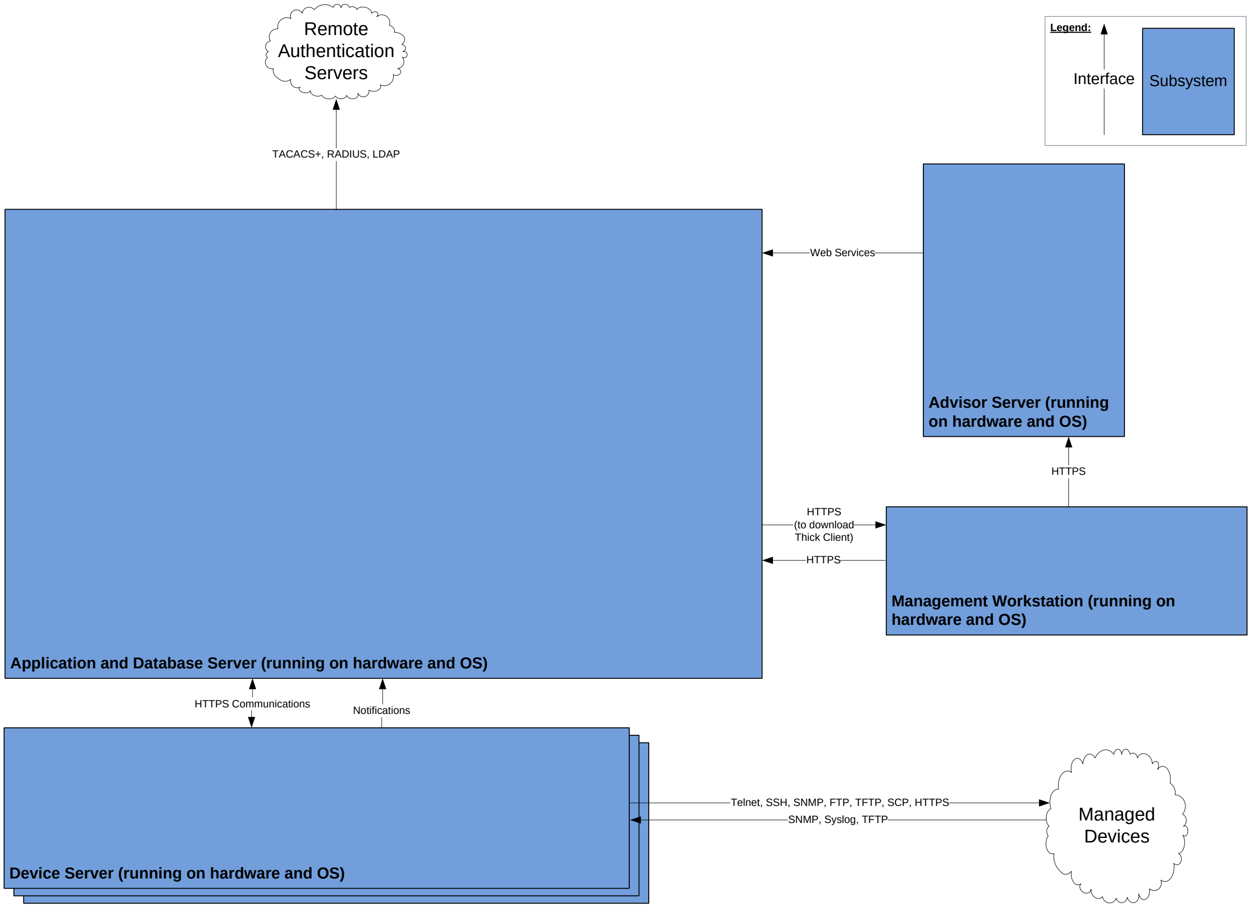
Remote Authentication Servers
TACACS+, RADIUS, LDAP
Legend:
Interface
Subsystem
Web Services
Advisor Server (running on hardware and OS)
HTTPS
HTTPS (to download Thick Client)
HTTPS
Management Workstation (running on hardware and OS)
Application and Database Server (running on hardware and OS)
HTTPS Communications
Notifications
Device Server (running on hardware and OS)
Telnet, SSH, SNMP, FTP, TFTP, SCP, HTTPS
SNMP, Syslog, TFTP
Managed Devices

**Figure 1 - VoyenceControl Architecture**[2]

### 1.3.2 TOE Environment

VoyenceControl is a software-only TOE that is installed and deployed on general-purpose server hardware running a general-purpose operating system.

## 1.4 TOE Description

In order to communicate with and manage the devices on the network, VoyenceControl stores the administrative credentials (*i.e.*, username and password) for each device to be managed. Administrators authenticate to VoyenceControl, and then VoyenceControl performs operations on the devices on the administrator's behalf by accessing the devices on the network using their administrative credentials. Using VoyenceControl in this manner – as the central management "hub" for the devices – helps to ensure that all device configuration changes are audited, and that device configurations remain in compliance with corporate policies.

The Report Advisor Server allows administrators to generate highly configurable custom reports about their infrastructure. The TOE Evaluated version of the Report Advisor is 2.2.0 build 561.

[2] SQL: Structured Query Language

SMTP: Simple Mail Transport Protocol

The Application Server is responsible for collecting data about the devices from the Device Servers and storing this information in the Database. It is also responsible for handling all administrative requests by administrators, and for providing data to the Advisors on request.

The Device Servers communicate with numerous devices on the network in order to collect status information from them and to push configuration changes from the Application Server to them. The Device Servers do not make any administrative decisions – they simply act on behalf of the Application Server. Communications between the Application Server and the Device Servers are encrypted using Secure Sockets Layer (SSL). The Device Servers can communicate with and manage devices via the following protocols:

- Simple Network Management Protocol (SNMP) versions 1, 2, and 3
- Telnet
- Secure Shell (SSH)
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Secure Copy (SCP)
- Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
- Syslog (inbound from devices to the Device Server)

Management is performed through these interfaces. This evaluation does not consider the cryptography implemented by these interfaces. VoyenceControl supports both local and remote authentication for TOE operators. For local authentication, hashes of user passwords are stored in the Database for comparison to hashes of entered passwords at the time of login. For remote authentication, RADIUS[3], TACACS+[4] and LDAP[5] servers (including Active Directory servers) are supported. The RADIUS, TACACS+, and LDAP remote authentication servers are considered part of the operating environment of the TOE.

Very granular access control permissions are applied to authenticated users. By default, users have no privileges until privileges are assigned to them (or until they are assigned to a group which has permissions). VoyenceControl provides a rich set of permissions which can be granted to individual users or groups of users, allowing very fine-grained access control distinctions between users. VoyenceControl also generates robust audit logs of every successful event and every failed event in the product – an audit record is generated every time a permission check is performed and every time a login or logout occurs.

Although the intended use of VoyenceControl is for device configurations to be stored within VoyenceControl and then pushed out to devices on administrators' behalves, the product also offers a "cut-through" feature for administrators to use when they desire direct access to a device's administrative interface. To use the "cut-through" feature, an administrator first logs into VoyenceControl and then tells VoyenceControl to initiate a cut-through to a specific device; VoyenceControl then sets up the appropriate connection for the administrator – for example, by opening a telnet connection to the device and presenting the telnet interface to the administrator.

Administration of VoyenceControl is primarily performed through the Management Client, also called the "Thick Client." The Thick Client is a Java-based utility that is installed on an administrator's workstation and

[3] RADIUS: Remote Authentication Dial-In User Service

[4] TACACS: Terminal Access Controller Access-Control System Plus

[5] LDAP: Lightweight Directory Access Protocol

communicates with the Application Server on the administrator's behalf. All security-related decisions are made by the Application Server; the Thick Client simply provides the user interface used by the administrator. Administrators can view reports by logging into the Advisor Server using any web browser.

### 1.4.1 TOE Physical and Logical Scope

Figure 2 illustrates the physical and logical scope and boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

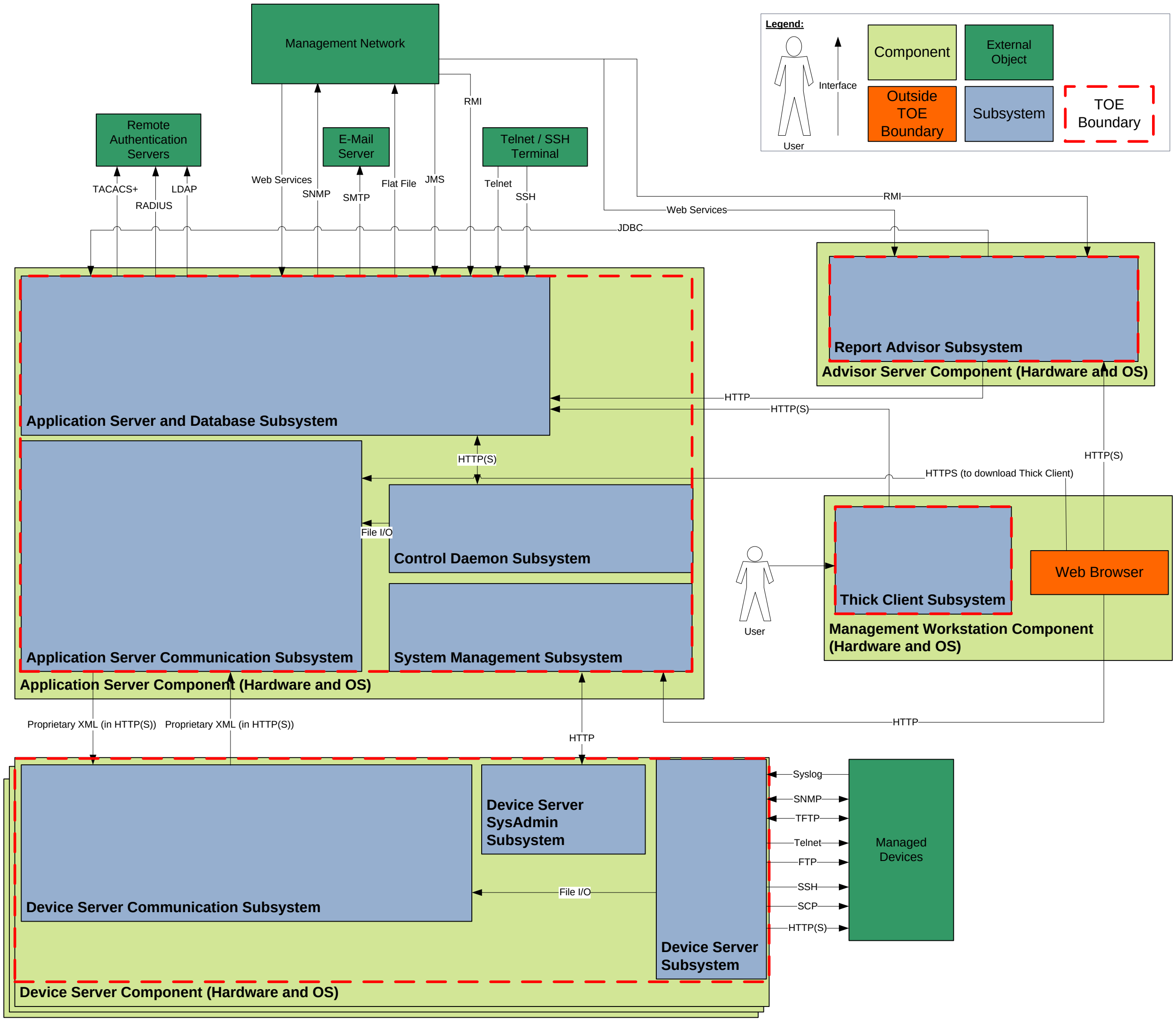
Management Network
Legend:
User
Interface
Component
External Object
Outside TOE Boundary
Subsystem
TOE Boundary
Remote Authentication Servers
E-Mail Server
Telnet / SSH Terminal
RMI
TACACS+
LDAP
RADIUS
Web Services
SNMP
SMTP
Flat File
JMS
Telnet
SSH
RMI
Web Services
JDBC
Report Advisor Subsystem
Advisor Server Component (Hardware and OS)
Application Server and Database Subsystem
HTTP
HTTP(S)
HTTP(S)
HTTPS (to download Thick Client)
HTTP(S)
File I/O
Control Daemon Subsystem
Application Server Communication Subsystem
System Management Subsystem
Application Server Component (Hardware and OS)
User
Thick Client Subsystem
Web Browser
Management Workstation Component (Hardware and OS)
Proprietary XML (in HTTP(S))
Proprietary XML (in HTTP(S))
HTTP
HTTP
Device Server SysAdmin Subsystem
Device Server Communication Subsystem
File I/O
Device Server Subsystem
Syslog
SNMP
TFTP
Telnet
FTP
SSH
SCP
HTTP(S)
Managed Devices
Device Server Component (Hardware and OS)

**Figure 2 - TOE and TOE Environment**

VoyenceControl is a software-only TOE that is installed and deployed on general-purpose server hardware running a general-purpose operating system. The TOE boundary depicted above includes all of the Application Server subsystems, the Device Server subsystems, the Advisor Server subsystems, and the Thick Client. The server hardware, server operating systems, managed devices, remote authentication servers, and web browser are not included, since they are not provided as part of the product delivery.

The TOE requires at least the following specifications to function:

- a 2GHz[6] processor,
- 1 GB[7] of memory,
- 200 MB[8] of storage space,
- Firefox 1.5 and/or Internet Explorer 6.0 or later,
- SSH version 2 or later,
- and Java 1.6.0_12 or later.

The TOE runs on Microsoft Windows Server 2003, Red Hat Enterprise Linux 4 or 5, and Solaris 10 (Release 6/06). The specific hardware and software requirements for the TOE can be found in "Step 2: System Requirements" of the

- *EMC VoyenceControl 4.1.0 Installing VoyenceControl on Solaris 10 P/N*[9] *300-008-397 Rev A01*,
- *EMC VoyenceControl 4.1.0 Installing VoyenceControl on Red Hat Enterprise Linux 4 and 5 P/N 300-008-392 Rev A01*, and
- *EMC VoyenceControl 4.1.0 Installing VoyenceControl on Windows Server 2003 P/N 300-008-395 Rev A01* documents.

#### 1.4.1.1 Security Audit

The TOE performs auditing of all events (whether they succeed or fail), and can be configured to store these events. The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

#### 1.4.1.2 User Data Protection

The TOE enforces a Management Access Control Policy as well as a Device Information Flow Control Policy. The Management Access Control Policy dictates TOE permissions and their implementation. The Device Information Flow Control Policy describes the interactions TOE users can have with devices based on their roles and permissions.

#### 1.4.1.3 Identification and Authentication

The TOE requires that all TOE users are authenticated by the TOE or the TOE environment prior to being granted access to the TOE functionality.

#### 1.4.1.4 Security Management

The TOE offers robust and granular permissioning of users, groups, and devices. TOE users are divided into two types: "Admins" are users who administer the TOE; "Users" are users who administer devices, but not the TOE itself.

#### 1.4.1.5 Protection of the TSF

The TOE implements a "health checker" daemon that periodically checks the status of all TOE components. If a component is malfunctioning, alerts are sent by the health checker daemon and (if installed on a Linux or Solaris OS) a "watchdog" daemon restarts the malfunctioning process.

[6] GHz refers to gigahertz, or one billion cycles per second.

[7] GB refers to a gigabyte, or one billion bytes.

[8] MB refers to a megabyte, or one million bytes.

[9] P/N – Part Number

#### 1.4.1.6 TOE Access

The TOE will end the session of any idle user after a configurable period of inactivity.

### 1.4.2 Physical/Logical Features and Functionality Not Included in the TSF

- Cryptography used for SSL, SSH, HTTPS, SCP, and RMI over HTTPS

The Advisor Server provides two primary reporting "advisors" excluded from the Evaluated version of the TOE:

- PCI[10] Advisor – parses device data stored in the Database and generates a report indicating areas of non-compliance with the Payment Card Industry standard

- Network Advisor – parses device data stored in the Database and generates a report indicating potential applicable vulnerabilities

Java 1.6.0_12, Firefox 1.5, Internet Explorer 6.0, and server-side RADIUS, TACACS+, LDAP, and Active Directory implementation.

[10] PCI – Payment Card Industry

# 2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

**Table 2 – CC and PP Conformance**

| | |
|---|---|
| **Common Criteria (CC) Identification and Conformance** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 conformant; CC Part 3 conformant. |
| **PP Identification** | None |
| **Evaluation Assurance Level** | EAL2 augmented with Flaw Remediation (ALC_FLR.1) |

# 3 Security Problem Definition

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

## 3.1 Threats to Security

This section identifies the threats against which the TOE must protect itself. The threat agents are individuals who are not authorized to use the TOE. The threat agents are assumed to:

- have public knowledge of how the TOE operates
- possess a basic skill level
- have limited resources to alter TOE configuration settings
- have no physical access to the TOE
- possess a basic level of motivation
- have a basic attack potential

The IT assets requiring protection are the audit data, TOE configuration data, and the managed devices.

The following threats are applicable:

**Table 3 – Threats**

| Name | Description |
|---|---|
| T.COMINT | An unauthorized individual may attempt to compromise the integrity of the audit data collected and produced by the TOE or TOE configuration data by bypassing a security mechanism. |
| T.FAILURE | A component of the TOE software might encounter an error which causes that component to malfunction, causing the TOE to operating in an incorrect or insecure manner. |
| T.PRIVILEGE | An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data or managed devices. |

## 3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

**Table 4 – Organizational Security Policies**

| Name | Description |
|---|---|
| P.PASSWORD | An authorized TOE user must use a sound password to access the TOE. A user password must have a minimum password length of eight characters and |

| Name | Description |
|---|---|
| | must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and two alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated). |

## 3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

**Table 5 – Assumptions**

| Name | Description |
|---|---|
| A.NOEVIL | Administrators are non-hostile, appropriately trained, and follow all administrator guidance. |
| A.PHYSICAL | Physical security will be provided for the TOE and its environment. |

# 4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

## 4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

**Table 6 – Security Objectives for the TOE**

| Name | Description |
|---|---|
| O.ACCESS | The TOE must allow authorized users to access only appropriate TOE management functions and data, and only appropriate managed devices with appropriate permissions. |
| O.ADMIN | The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can exercise such control. |
| O.AUDIT | The TOE must gather audit records of actions on the TOE which may be indicative of misuse. |
| O.IDAUTH | The TOE or must be able to identify and authenticate users. |
| O.INTEGR | The TOE must ensure the integrity of all audit data. |
| O.PROTECT | The TOE must protect itself and the managed devices from unauthorized modifications and access to management functions, audit data, and configuration data. |
| O.TESTS | The TOE must perform periodic self-tests to ensure that the TOE is operating properly. |

## 4.2 Security Objectives for the Operational Environment

### 4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

**Table 7 – IT Security Objectives**

| Name | Description |
|---|---|
| OE.IDAUTH | The TOE environment must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. |
| OE.SEP | The IT Environment will protect the TOE from external interference or tampering. |

| | |
|---|---|
| OE.TIME | The IT Environment will provide reliable timestamps for the TOE's use. |

### 4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

**Table 8 – Non-IT Security Objectives**

| Name | Description |
|---|---|
| NOE.NOEVIL | TOE users are non-hostile, appropriately trained, and follow all user guidance. |
| NOE.PHYSICAL | The TOE will be located within controlled access facilities, which will prevent unauthorized physical access. |
| NOE.PASSWORD | TOE users will only use strong passwords to access the TOE. A user password must have a minimum password length of eight characters and must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and two alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated). |

# 5 Extended Components Definition

There are no extended SFRs or extended SARs met by the TOE.

# 6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

### 6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

## 6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

**Table 9 – TOE Security Functional Requirements**

| Name | Description | S | A | R | I |
|---|---|---|---|---|---|
| FAU_GEN.1 | Audit data generation | ✓ | ✓ | | |
| FAU_SAR.1 | Audit review | | ✓ | | |
| FAU_SAR.3 | Selectable audit review | | ✓ | | |
| FAU_STG.1 | Protected audit trail storage | ✓ | | | |
| FDP_ACC.2(a) | Complete access control (audit and TOE configuration data) | | ✓ | | ✓ |
| FDP_ACF.1(a) | Security attribute based access control (audit and TOE configuration data) | | ✓ | | ✓ |
| FDP_ACC.2(b) | Complete access control (I&A data) | | ✓ | | ✓ |
| FDP_ACF.1(b) | Security attribute based access control (I&A data) | | ✓ | | ✓ |
| FDP_IFC.2 | Complete information flow control | | ✓ | | |
| FDP_IFF.2 | Hierarchical security attributes | | ✓ | | |

| Name | Description | S | A | R | I |
|---|---|---|---|---|---|
| FIA_ATD.1 | User attribute definition | | ✓ | | |
| FIA_UAU.2 | User authentication before any action | | | | |
| FIA_UID.2 | User identification before any action | | | | |
| FMT_MOF.1 | Management of security functions behaviour | ✓ | ✓ | | |
| FMT_MSA.1 | Management of security attributes | ✓ | ✓ | | |
| FMT_MSA.3 | Static attribute initialisation | ✓ | ✓ | | |
| FMT_MTD.1 | Management of TSF data | ✓ | ✓ | | |
| FMT_SMF.1 | Specification of management functions | | ✓ | | |
| FMT_SMR.1 | Security roles | | ✓ | | |
| FPT_TST.1 | TSF testing | ✓ | ✓ | | |
| FTA_SSL.3 | TSF-initiated termination | | ✓ | | |

*Note: S=Selection; A=Assignment; R=Refinement; I=Iteration*

### 6.2.1 Class FAU: Security Audit

## FAU_GEN.1 Audit data generation

**Hierarchical to: No other components.**

**FAU_GEN.1.1**

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

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [*all user actions*].

**FAU_GEN.1.2**

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

**Dependencies: FPT_STM.1 Reliable time stamps**

## FAU_SAR.1 Audit review

**Hierarchical to: No other components.**

**FAU_SAR.1.1**

The TSF shall provide [*System Admins and Network Admins*] with the capability to read [*audit information*] 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.

**Dependencies: FAU_GEN.1 Audit data generation**

## FAU_SAR.3 Selectable audit review

**Hierarchical to: No other components.**

**FAU_SAR.3.1**

The TSF shall provide the ability to apply [*searching, sorting, and ordering*] of audit data based on [*user-specified parameters*].

**Dependencies: FAU_SAR.1 Audit review**

## FAU_STG.1 Protected audit trail storage

**Hierarchical to: No other components.**

**FAU_STG.1.1**

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

**FAU_STG.1.2**

The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

**Dependencies: FAU_GEN.1 Audit data generation**

### 6.2.2 Class FDP: User Data Protection

#### FDP_ACC.2(a) Complete access control (audit and TOE configuration data)

**Hierarchical to: FDP_ACC.1 Subset access control**

**FDP_ACC.2.1(a)**

The TSF shall enforce the [*Management Access Control SFP*[11]] on [*subjects: TOE users and managed devices, and objects: audit data and TOE configuration data*] and all operations among subjects and objects covered by the SFP.

**FDP_ACC.2.2(a)**

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

**Dependencies: FDP_ACF.1 Security attribute based access control**

#### FDP_ACF.1(a) Security attribute based access control (audit and TOE configuration data)

**Hierarchical to: No other components.**

**FDP_ACF.1.1(a)**

The TSF shall enforce the [*Management Access Control SFP*] to objects based on the following: [

- *Subjects: TOE users, managed devices*
  - *Security Attributes:*
    - *Username*
    - *Group memberships*
    - *Individual user permissions*
    - *Inherited group permissions*
- *Objects: audit data and TOE configuration data*
  - *Security Attributes:*
    - *Permissions*

].

**FDP_ACF.1.2(a)**

[11] SFP: Security Function Policy

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an authorized user can manipulate audit data and/or the TOE configuration if the user has the appropriate permissions*].

**FDP_ACF.1.3(a)**

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

**FDP_ACF.1.4(a)**

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

**Dependencies: FDP_ACC.1 Subset access control**
**FMT_MSA.3 Static attribute initialization**

### FDP_ACC.2(b) Complete access control (I&A data)

**Hierarchical to: FDP_ACC.1 Subset access control**

**FDP_ACC.2.1(b)**

The TSF shall enforce the [*I&A Access Control SFP*[12]] on [*subjects: TOE users and groups, and objects: TOE user credentials and permissions*] and all operations among subjects and objects covered by the SFP.

**FDP_ACC.2.2(b)**

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

**Dependencies: FDP_ACF.1 Security attribute based access control**

### FDP_ACF.1(b) Security attribute based access control (I&A data)

**Hierarchical to: No other components.**

**FDP_ACF.1.1(b)**

The TSF shall enforce the [*I&A Access Control SFP*] to objects based on the following: [

- *Subjects: TOE users and groups*
    - *Security Attributes:*
        - *Username*
        - *Group memberships*
        - *Individual user permissions*

[12] SFP: Security Function Policy

        - *Inherited group permissions*

- *Objects: TOE user credentials and permissions*
    - *Security Attributes:*
        - *Usernames*
        - *Passwords (if the users are local users)*
        - *Group names*
        - *Group memberships*
        - *Individual user permissions*
        - *Group permissions*

].

**FDP_ACF.1.2(b)**

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an authorized user can manipulate user credentials and permissions if the user has the appropriate permissions*].

**FDP_ACF.1.3(b)**

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

**FDP_ACF.1.4(b)**

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

**Dependencies: FDP_ACC.1 Subset access control**
**FMT_MSA.3 Static attribute initialization**

### FDP_IFC.2 Complete information flow control

**Hierarchical to: FDP_IFC.1 Subset information flow control**

**FDP_IFC.2.1**

The TSF shall enforce the [*Device Information Flow Control SFP*] on [*subjects: TOE users, and objects: managed devices*] and all operations that cause that information to flow to and from subjects covered by the SFP.

**FDP_IFC.2.2**

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

**Dependencies: FDP_IFF.1 Simple security attributes**

## FDP_IFF.2 Hierarchical security attributes

**Hierarchical to: FDP_IFF.1 Simple security attributes**

**FDP_IFF.2.1**

The TSF shall enforce the [*Device Information Flow Control SFP*] based on the following types of subject and information security attributes: [assignment: *l*

- *Subjects:*
  - *TOE users and managed devices*
    - *Security Attributes:*
      - *Username*
      - *Group memberships*
      - *Individual user permissions*
      - *Inherited group permissions*
  - *Managed devices*
    - *Security Attributes:*
      - *Identity*
- *Information: management traffic data*
  - *Security Attributes:*
    - *Destination device*

].

**FDP_IFF.2.2**

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [*an authorized user can send management traffic to a managed device if the user has the appropriate permissions*].

**FDP_IFF.2.3**

The TSF shall enforce the [*none*].

**FDP_IFF.2.4**

The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

**FDP_IFF.2.5**

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

**FDP_IFF.2.6**

The TSF shall enforce the following relationships for any two valid information flow control security attributes:

- There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and
- There exists a “least upper bound” in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
- There exists a “greatest lower bound” in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

**Dependencies:** **FDP_IFC.1 Subset information flow control**
**FMT_MSA.3 Static attribute initialisation**

### 6.2.3 Class FIA: Identification and Authentication

#### FIA_ATD.1 User attribute definition

**Hierarchical to: No other components.**

**FIA_ATD.1.1**

The TSF shall maintain the following list of security attributes belonging to individual users: [*username, group memberships, individual user permissions, inherited group permissions, password (if the user is a local user)*].

**Dependencies: No dependencies**

#### FIA_UAU.2 User authentication before any action

**Hierarchical to: FIA_UAU.1 Timing of authentication**

**FIA_UAU.2.1**

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

**Dependencies: FIA_UID.1 Timing of identification**

#### FIA_UID.2 User identification before any action

**Hierarchical to: FIA_UID.1 Timing of identification**

**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.

**Dependencies: No dependencies**

### 6.2.4 Class FMT: Security Management

#### FMT_MOF.1 Management of security functions behaviour

**Hierarchical to: No other components.**

**FMT_MOF.1.1**

The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [*all functions*] to [*the users and groups with appropriate permissions*].

**Dependencies: FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

#### FMT_MSA.1 Management of security attributes

**Hierarchical to: No other components.**

**FMT_MSA.1.1**

The TSF shall enforce the [*Management Access Control SFP and Device Information Flow Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*relevant to those SFPs*] to [*the users and groups with appropriate permissions*].

**Dependencies: [FDP_ACC.1 Subset access control or**
**FDP_IFC.1 Subset information flow control]**
**FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

#### FMT_MSA.3 Static attribute initialisation

**Hierarchical to: No other components.**

**FMT_MSA.3.1**

The TSF shall enforce the [*Management Access Control SFP and Device Information Flow Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2**

The TSF shall allow the [*users and groups with appropriate permissions*] to specify alternative initial values to override the default values when an object or information is created.

**Dependencies: FMT_MSA.1 Management of security attributes**
**FMT_SMR.1 Security roles**

#### FMT_MTD.1 Management of TSF data

**Hierarchical to: No other components.**

**FMT_MTD.1.1**

The TSF shall restrict the ability to [*change_default, query, modify, delete*] the [*audit data and TOE configuration data*] to [*the users and groups with appropriate permissions*].

**Dependencies: FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

### FMT_SMF.1 Specification of management functions

**Hierarchical to: No other components.**

**FMT_SMF.1.1**

The TSF shall be capable of performing the following management functions: [*security attribute management, TSF data management, and security function management*].

**Dependencies: No Dependencies**

### FMT_SMR.1 Security roles

**Hierarchical to: No other components.**

**FMT_SMR.1.1**

The TSF shall maintain the roles [*System Admin; Network Admin; User Admin; and User*].

**FMT_SMR.1.2**

The TSF shall be able to associate users with roles.

**Dependencies: FIA_UID.1 Timing of identification**

### 6.2.5 Class FPT: Protection of the TSF

#### FPT_TST.1 TSF testing

**Hierarchical to: No other components.**

**FPT_TST.1.1**

The TSF shall run a suite of self tests [*periodically during normal operation*] to demonstrate the correct operation of [*the TSF*].

**FPT_TST.1.2**

The TSF shall provide authorised users with the capability to verify the integrity of [*[running TSF executable code]*].

**FPT_TST.1.3**

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

**Dependencies: No dependencies**

### 6.2.6 Class FTA: TOE Access

#### FTA_SSL.3 TSF-initiated termination

**Hierarchical to: No other components.**

**FTA_SSL.3.1**

The TSF shall terminate an interactive session after a [*configurable time interval of user inactivity*].

**Dependencies: No dependencies**

## 6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 10 – Assurance Requirements summarizes the requirements.

**Table 10 – Assurance Requirements**

| Assurance Requirements | |
|---|---|
| Class ADV: Development | ADV_ARC.1 Security Architecture Description |
| | ADV_FSP.2 Security-enforcing functional specification |
| | ADV_TDS.1 Basic design |
| Class AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| Class 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.1 Basic Flaw Remediation |
| Class ATE: Tests | ATE_COV.1 Evidence of coverage |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing – sample |
| Class AVA: Vulnerability assessment | AVA_VAN.2 Vulnerability analysis |

# 7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

## 7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

**Table 11 – Mapping of TOE Security Functions to Security Functional Requirements**

| TOE Security Function | SFR ID | Description |
|---|---|---|
| Security Audit | FAU_GEN.1 | Audit data generation |
| | FAU_SAR.1 | Audit review |
| | FAU_SAR.3 | Selectable audit review |
| | FAU_STG.1 | Protected audit trail storage |
| User Data Protection | FDP_ACC.2(a) | Complete access control (audit and TOE configuration data) |
| | FDP_ACF.1(a) | Security attribute based access control (audit and TOE configuration data) |
| | FDP_ACC.2(b) | Complete access control (I&A data) |
| | FDP_ACF.1(b) | Security attribute based access control (I&A data) |
| | FDP_IFC.2 | Complete information flow control |
| | FDP_IFF.2 | Hierarchical security attributes |
| Identification and Authentication | FIA_ATD.1 | User attribute definition |
| | FIA_UAU.2 | User authentication before any action |
| | FIA_UID.2 | User identification before any action |
| Security Management | FMT_MOF.1 | Management of security functions behaviour |
| | FMT_MSA.1 | Management of security attributes |
| | FMT_MSA.3 | Static attribute initialisation |
| | FMT_MTD.1 | Management of TSF data |
| | FMT_SMF.1 | Specification of management functions |
| | FMT_SMR.1 | Security roles |

| TOE Security Function | SFR ID | Description |
|---|---|---|
| Protection of the TSF | FPT_TST.1 | TSF testing |
| TOE Access | FTA_SSL.3 | TSF-initiated termination |

### 7.1.1 Security Audit

The TOE performs auditing of all events (whether they succeed or fail), and can be configured to store all of these events in the Central Event Log (CEL). The CEL is stored in a database and records all device events, application events, security events, configuration events, logins/logouts, job approvals, and credential changes. The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Audit review is performed through the "Event Manager" UI (User Interface). Event Manager provides robust searching and sorting of the audit records to users with the appropriate individual or inherited group permissions. There is no mechanism in the UI for deleting arbitrary audited records.

**TOE Security Functional Requirements Satisfied:** FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1.

### 7.1.2 User Data Protection

#### 7.1.2.1 Management Access Control Policy

Management Access Control permissions are implemented in a very granular and hierarchical way. The "subjects" of the Policy are the users and managed devices. Each user has a username, group membership, inherited group permissions, and individual permissions; each managed device has an identity. The "objects" of the Management Access Control Policy are the audit data and TOE configuration data to be managed. Access Control decisions are made based on the "most specific" permission information available for a given subject and a given object – for example, if a user has "allow" permission on a specific device but "deny" permission on the network to which that device belongs, the user will be allowed to perform actions on that particular device but not on other devices in that network (unless he also has device-specific permissions on another device in that network).

#### 7.1.2.2 I&A Access Control Policy

I&A Access Control permissions are implemented in a very granular and hierarchical way. The "subjects" of the Policy are the users and user groups. Each user has a username, password (if the user is a local user), group membership, and individual permissions. Each user group has a group name and group permissions. The "objects" of the I&A Access Control Policy are the user and group credentials and permissions to be managed. As with the Management Access Control Policy, Access Control decisions are made based on the "most specific" permission information available for a given subject and a given object.

#### 7.1.2.3 Device Information Flow Control Policy

Information Flow Control permissions are also implemented in a very granular and hierarchical way. The "subjects" of the Device Information Flow Control Policy are the users and the managed devices. Each user has a username, group membership, inherited group permissions, and individual permissions; each managed device has an identity. The "information" controlled by the Policy is the management traffic to be sent to the managed devices. Information Flow Control decisions are made based on the "most specific" permission information available for a given potential information flow – for example, if a user has "allow" permission on a specific device but "deny" permission on the other devices on the network to which that device belongs, the user will be allowed to perform actions only on that particular device, unless he also has device-specific permissions on another device in that network.

**TOE Security Functional Requirements Satisfied:** FDP_ACC.2(a), FDP_ACF.1(a), FDP_ACC.2(b), FDP_ACF.1(b), FDP_IFC.2, FDP_IFF.2.

### 7.1.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting a service has provided a valid username and password and is authorized to access that service. For each user, the TOE stores the following security attributes in the database: username, group memberships, individual user permissions, inherited group permissions, and password (if the user is a local user). The TOE can be configured to use a local user database, or to use remote authentication databases (RADIUS, TACACS, TACACS+, or LDAP). This security functionality is the responsibility of the Operational Environment. When a TOE user enters his username and password at a management interface, the information is checked against the local database or sent to the configured remote authentication server. If the provided username and password are valid then the TOE allows the user to access the TOE with the permissions associated with that username. Before identification and authentication, the TOE user is only able to identify and authenticate himself.

**TOE Security Functional Requirements Satisfied:** FIA_ATD.1, FIA_UAU.2, FIA_UID.2.

### 7.1.4 Security Management

The TOE offers very robust and granular permissioning of users, groups, and devices. This allows the TOE to maintain an unbounded number of differently permissioned users and groups. There are two main types of TOE users: “Admins” are users who administer the TOE; “Users” are users who administer devices, but not the TOE itself. The “Admins” user type is further broken down into three general types of Admin:

1. System Admin – has full privileges over all of the TOE
2. Network Admin – has full privileges, but only for the network(s) he is assigned to.
3. User Admin – can create users and groups and assign permissions and roles, but cannot assign anything more privileged than his own privileges.

The TOE does not allow users to have null passwords and does not provide anonymous access. Admins can lock any user account at any time.

**TOE Security Functional Requirements Satisfied:** FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

### 7.1.5 Protection of the TSF

The TOE implements a “health checker” daemon that periodically checks the status of all product components. If a component is malfunctioning, configurable alerts are sent. In addition, if the product is installed on a Linux or Solaris operating system, a “watchdog” daemon periodically checks important TOE processes and restarts them if malfunctions are encountered.

**TOE Security Functional Requirements Satisfied:** FPT_TST.1.

### 7.1.6 TOE Access

The TOE will end the session of any idle user after a configurable period of inactivity.

**TOE Security Functional Requirements Satisfied:** FTA_SSL.3.

# 8 Rationale

## 8.1 Conformance Claims Rationale

There are no Protection Profile conformance claims associated with this Security Target.

## 8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

### 8.2.1 Security Objectives Rationale Relating to Threats

**Table 12 – Threats:Objectives Mapping**

| Threats | Objectives | Rationale |
|---|---|---|
| T.COMINT<br>An unauthorized individual may attempt to compromise the integrity of the audit data collected and produced by the TOE or TOE configuration data by bypassing a security mechanism. | O.ACCESS<br>The TOE must allow authorized users to access only appropriate TOE management functions and data, and only appropriate managed devices with appropriate permissions. | The O.ACCESS objectives ensure that unauthorized modifications and access to functions and data is prevented. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data. |
| | O.AUDIT<br>The TOE must gather audit records of actions on the TOE which may be indicative of misuse. | The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. |
| | O.IDAUTH<br>The TOE or the TOE environment must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | The O.IDAUTH objective requires that the TOE must be able to identify and authenticate operators. |
| | O.INTEGR<br>The TOE must ensure the integrity of all audit data. | This threat is primarily diminished by the O.INTEGR objective, which requires that the TOE ensure the integrity of all audit data. |
| | O.PROTECT<br>The TOE must protect itself and the managed devices from unauthorized modifications and access to management functions, audit data, and configuration data. | The O.PROTECT objective requires that the TOE protect itself from unauthorized modifications and access to its functions and data. |

| Threats | Objectives | Rationale |
|---|---|---|
| | OE.IDAUTH | The OE.IDAUTH objective requires that the TOE environment must be able to identify and authenticate operators prior to allowing access to TOE functions and data. |
| | OE.SEP<br>The IT Environment will protect the TOE from external interference or tampering. | The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions. |
| | OE.TIME<br>The IT Environment will provide reliable timestamps for the TOE's use. | The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. |
| T.FAILURE<br>A component of the TOE software might encounter an error which causes that component to malfunction, causing the TOE to operating in an incorrect or insecure manner. | O.TESTS<br>The TOE must perform periodic self-tests to ensure that the TOE is operating properly. | The O.TESTS objective requires that the TOE run a series of tests on its software components to ensure that they are operating correctly. |
| T.PRIVILEGE<br>An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data or managed devices. | O.ACCESS<br>The TOE must allow authorized users to access only appropriate TOE management functions and data, and only appropriate managed devices with appropriate permissions. | The O.ADMIN and O.ACCESS objectives together ensure that policies won't be subverted or changed by unauthorized users. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data. |
| | O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can exercise such control. | The O.ADMIN and O.ACCESS objectives together ensure that policies won't be subverted or changed by unauthorized users. The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the functions and data of the TOE. |
| | O.AUDIT<br>The TOE must gather audit records of actions on the TOE which may be indicative of misuse. | The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. |
| | O.IDAUTH<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | This threat is primarily diminished by the O.IDAUTH objective, which requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data. |
| | O.PROTECT<br>The TOE must protect itself and the | The O.PROTECT objective requires that the TOE protect itself from |

| Threats | Objectives | Rationale |
|---|---|---|
| | managed devices from unauthorized modifications and access to management functions, audit data, and configuration data. | unauthorized modifications and access to its functions and data. |
| | OE.SEP<br>The IT Environment will protect the TOE from external interference or tampering. | The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions. |
| | OE.TIME<br>The IT Environment will provide reliable timestamps for the TOE's use. | The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. |

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

### 8.2.2 Security Objectives Rationale Relating to Policies

**Table 13 – Policies:Objectives Mapping**

| Policies | Objectives | Rationale |
|---|---|---|
| P.PASSWORD<br>An authorized TOE user must use a sound password to access the TOE. A user password must have a minimum password length of eight characters and must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and two alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated). | NOE.PASSWORD<br>TOE users must use strong passwords that are not susceptible to brute force attacks or dictionary attacks by ensuring the characters that make up their passwords contain many different numeric and alphanumeric characters. | NOE.PASSWORD ensures that TOE users use strong passwords to gain access to the TOE. |
| | O.IDAUTH<br>The TOE must be able to identify and authenticate users. | O.IDAUTH ensures that a user must identify and authenticate before access to the TOE and its managed devices is granted. |
| | OE.IDAUTH<br>The OE.IDAUTH objective requires that the TOE environment must be able to identify and authenticate operators prior to allowing access to TOE functions and data. | OE.IDAUTH ensures that the TOE environment is able to identify and authenticate operators prior to access to TOE functions and data. |

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

### 8.2.3 Security Objectives Rationale Relating to Assumptions

**Table 14 – Assumptions:Objectives Mapping**

| Assumptions | Objectives | Rationale |
|---|---|---|
| A.NOEVIL<br>Administrators are non-hostile, appropriately trained, and follow all administrator guidance. | NOE.NOEVIL<br>TOE users are non-hostile, appropriately trained, and follow all user guidance. | The NOE.NOEVIL objective ensures that TOE users are non-hostile, appropriately trained, and follow all operator guidance. |
| A.PHYSICAL<br>Physical security will be provided for the TOE and its environment. | NOE.PHYSICAL<br>The TOE will be located within controlled access facilities, which will prevent unauthorized physical access. | The NOE.PHYSCL objective requires that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. |

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

## 8.3 Rationale for Extended Security Functional Requirements

There are no extended security functional requirements associated with this Security Target.

## 8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements associated with this Security Target.

## 8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

### 8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

**Table 15 – Objectives:SFRs Mapping**

| Objective | SFR | Rationale |
|---|---|---|
| O.ACCESS<br>The TOE must allow authorized users to access only appropriate TOE management functions and data, and only appropriate managed devices with appropriate permissions. | FDP_ACC.2(a)<br>Complete access control (audit and TOE configuration data) | The TOE has an access control policy that ensures that only authorized users gain access to TOE functions and data. |
| | FDP_ACF.1 (a)<br>Security attribute based access control (audit and | The TOE is required to provide authorized users access to TOE functions and data. |

| Objective | SFR | Rationale |
|---|---|---|
| | TOE configuration data) | |
| | FDP_ACC.2(b)<br>Complete access control (I&A data) | The TOE has an access control policy that ensures that only authorized users can modify user credentials and permissions. |
| | FDP_ACF.1 (b)<br>Security attribute based access control (I&A data) | The TOE is required to provide authorized users the ability to modify user credentials and permissions. |
| | FDP_IFC.2<br>Complete information flow control | The TOE has an information flow control policy that ensures that only authorized users gain access to managed devices. |
| | FDP_IFF.2<br>Hierarchical security attributes | The TOE is required to provide authorized users access to managed devices. |
| | FIA_UAU.2<br>User authentication before any action | The TOE will not give any security sensitive access to a user until the TOE has authenticated the user. |
| | FIA_UID.2<br>User identification before any action | The TOE will not give any security sensitive access to a user until the TOE has identified the user. |
| | FMT_MOF.1<br>Management of security functions behaviour | The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE. |
| | FMT_MSA.3<br>Static attribute initialisation | Restrictive values for TOE functions and data are provided, and the authorized administrator can change them when an object is created. |
| | FMT_MTD.1<br>Management of TSF data | Only authorized users of the System may query and modify TOE data. |
| O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can exercise such control. | FMT_MOF.1<br>Management of security functions behaviour | Only those roles defined in FMT_SMR.1 are given the right to control the behavior of the TSF. |
| | FMT_MSA.3<br>Static attribute initialisation | Restrictive values for TOE functions and data are provided, and the authorized administrator can change them when a data object is created. |
| | FMT_MTD.1<br>Management of TSF data | Only those roles defined in FMT_SMR.1 are given the right to access TSF data. |
| | FMT_SMF.1<br>Specification of management functions | Mechanisms exist to enforce the rules defined in FMT_MOF.1, FMT_MTD.1(a), and FMT_MTD.1(b). |

| Objective | SFR | Rationale |
|---|---|---|
| | FMT_SMR.1<br>Security roles | The TOE defines a set of roles. |
| | FTA_SSL.3<br>TSF-initiated termination | The TOE automatically terminates administrative sessions after a configurable period of inactivity. |
| O.AUDIT<br>The TOE must gather audit records of actions on the TOE which may be indicative of misuse. | FAU_GEN.1<br>Audit data generation | The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event. |
| | FAU_SAR.1<br>Audit review | The TOE must provide the ability to review the audit trail of the system. |
| | FAU_SAR.3<br>Selectable audit review | The TOE must provide the ability to search, sort, and order the audit trail of the system. |
| O.IDAUTH<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | FIA_ATD.1<br>User attribute definition | Security attributes of subjects used to enforce the authentication policy of the TOE must be defined. |
| | FIA_UAU.2<br>User authentication before any action | The TOE will not give any security sensitive access to a user until the TOE has authenticated the user. |
| | FIA_UID.2<br>User identification before any action | The TOE will not give any security sensitive access to a user until the TOE has identified the user. |
| | FMT_SMR.1<br>Security roles | The TOE must be able to recognize the different user roles that exist for the TOE. |
| O.INTEGR<br>The TOE must ensure the integrity of all audit data. | FAU_STG.1<br>Protected audit trail storage | The TOE is required to protect the audit data from unauthorized deletion. |
| | FDP_ACF.1 (a)<br>Security attribute based access control (audit and TOE configuration data) | Only authorized TOE users with the appropriate permissions may access audit data. |
| | FMT_MSA.1<br>Management of security attributes | Only authorized users of the System may query and modify TOE data. |
| | FMT_MTD.1<br>Management of TSF data | Only authorized users of the System may query and modify TOE data. |
| O.PROTECT<br>The TOE must protect itself and the managed devices from | FDP_ACC.2(a)<br>Complete access control(audit and TOE | The TOE has an access control policy that ensures that only authorized users can modify and access TOE functions and data. |

| Objective | SFR | Rationale |
|---|---|---|
| unauthorized modifications and access to management functions, audit data, and configuration data. | configuration data) | |
| | FDP_ACF.1(a)<br>Security attribute based access control (audit and TOE configuration data) | The TOE provides access control functionality to manage access to TOE functions and data. |
| | FDP_ACC.2(b)<br>Complete access control (I&A data) | The TOE has an access control policy that ensures that only authorized users can modify user credentials and permissions. |
| | FDP_ACF.1 (b)<br>Security attribute based access control (I&A data) | The TOE is required to provide authorized users the ability to modify user credentials and permissions. |
| | FDP_IFC.2<br>Complete information flow control | The TOE has an information flow control policy that ensures that only authorized users gain access to managed devices. |
| | FDP_IFF.2<br>Hierarchical security attributes | The TOE provides information flow control functionality to manage access to managed devices. |
| | FMT_MOF.1<br>Management of security functions behaviour | The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE. |
| | FMT_MTD.1<br>Management of TSF data | Only authorized users of the System may query and modify TOE data. |
| O.TESTS<br>The TOE must perform periodic self-tests to ensure that the TOE is operating properly. | FPT_TST.1<br>TSF testing | The TOE runs a “health checker” daemon which periodically checks all components of the TOE for correct operation. |

### 8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE controls access to devices which might be deployed in a hostile environment, the TOE itself is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the system will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer’s on-going flaw remediation processes.

### 8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

**Table 16 – Functional Requirements Dependencies**

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | ✓ | This dependency is met by the TOE environment. |
| FAU_SAR.1 | FAU_GEN.1 | ✓ | |
| FAU_SAR.3 | FAU_SAR.1 | ✓ | |
| FAU_STG.1 | FAU_GEN.1 | ✓ | |
| FDP_ACC.2(a) | FDP_ACF.1 | ✓ | Met by FDP_ACF.1(a). |
| FDP_ACF.1(a) | FDP_ACC.1 | ✓ | Although FDP_ACC.1 is not included, the hierarchical SFR FDP_ACC.2(a) is included. This satisfies this dependency. |
| | FMT_MSA.3 | ✓ | |
| FDP_ACC.2(b) | FDP_ACF.1 | ✓ | Met by FDP_ACF.1(b). |
| FDP_ACF.1(b) | FDP_ACC.1 | ✓ | Although FDP_ACC.1 is not included, the hierarchical SFR FDP_ACC.2(b) is included. This satisfies this dependency. |
| | FMT_MSA.3 | ✓ | |
| FDP_IFC.2 | FDP_IFF.1 | ✓ | Although FDP_IFF.1 is not included, the hierarchical SFR FDP_IFF.2 is included. This satisfies this dependency. |
| FDP_IFF.2 | FDP_IFC.1 | ✓ | Although FDP_IFC.1 is not included, the hierarchical SFR FDP_IFC.2 is included. This satisfies this dependency. |
| | FMT_MSA.3 | ✓ | |
| FIA_ATD.1 | None | ✓ | |
| FIA_UAU.2 | FIA_UID.1 | ✓ | Although FIA_UID.1 is not included, the hierarchical SFR FIA_UID.2 is included. This satisfies this dependency. |
| FIA_UID.2 | None | ✓ | |
| FMT_MOF.1 | FMT_SMR.1 | ✓ | |
| | FMT_SMF.1 | ✓ | |
| FMT_MSA.1 | FDP_ACC.1 | ✓ | Although FDP_ACC.1 is not included, the hierarchical SFRs FDP_ACC.2(a) and FDP_ACC.2(b) are included. This satisfies this dependency. |

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| | FMT_SMF.1 | ✓ | |
| | FMT_SMR.1 | ✓ | |
| FMT_MSA.3 | FMT_MSA.1 | ✓ | |
| | FMT_SMR.1 | ✓ | |
| FMT_MTD.1 | FMT_SMF.1 | ✓ | |
| | FMT_SMR.1 | ✓ | |
| FMT_SMF.1 | None | ✓ | |
| FMT_SMR.1 | FIA_UID.1 | ✓ | Although FIA_UID.1 is not included, the hierarchical SFR FIA_UID.2 is included. This satisfies this dependency. |
| FPT_TST.1 | None | ✓ | |
| FTA_SSL.3 | None | ✓ | |

# 9 Acronyms

**Table 17 – Acronyms**

| Acronym | Definition |
|---|---|
| CC | The Common Criteria for Information Technology Security Evaluation |
| CEL | Central Event Log |
| EAL | Evaluation Assurance Level |
| FTP | File Transfer Protocol |
| GB | Gigabyte (one billion bytes) |
| GHz | Gigahertz (one billion cycles per second) |
| HTTPS | Hypertext Transfer Protocol over SSL |
| IT | Information Technology |
| LDAP | Lightweight Directory Access Protocol |
| MB | Megabyte (one billion bytes) |
| PCI | Payment Card Industry |
| P/N | Part Number |
| PP | Protection Profile |
| OS | Operating System |
| OSP | Organizational Security Policy |
| RADIUS | Remote Authentication Dial-In User Service |
| SAR | Security Assurance Requirement |
| SCP | Secure Copy |
| SFR | Security Functional Requirement |
| SFP | Security Function Policy |
| SMTP | Simple Mail Transport Protocol |
| SNMP | Simple Network Management Protocol |
| SQL | Structured Query Language |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| TACACS+ | Terminal Access Controller Access-Control System Plus |
| TFTP | Trivial FTP |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| UI | User Interface |