Infoblox Inc.
NetMRI® Version 4.2.2.45

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.2

Prepared for:

Infoblox Inc.
2431 Solomons Island Road, Suite 302
Annapolis, MD 21401
Phone: (410) 573-2271

http://www.Infoblox.com

Prepared by:

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

http://www.corsec.com

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 Infoblox NetMRI® v4.2.2.45, and will hereafter be referred to as the TOE throughout this document. The TOE is a Network Configuration and Change Management (NCCM) product.

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	Infoblox Inc. NetMRI® Version 4.2.2.45 Security Target
ST Version	Version 1.2
ST Author	Corsec Security, Inc. Nathan Lee
ST Publication Date	4/29/2010
TOE Reference	Infoblox® NetMRI® v4.2.2.45
Keywords	automated network compliance management, network change management, network configuration management

1.3 TOE Overview and Description

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.

NetMRI is a NCCM product. NetMRI enables organizations to manage network configurations and network configuration changes, making it easier to find configuration problems and assess compliance requirements. NetMRI collects configuration and performance data for critical nodes throughout the network and then analyzes that data to generate information that can be used by network managers.

NetMRI continuously collects data from network devices. The collected data is used to build a database consisting of the configuration parameters, current statistics, and topology of the network devices. NetMRI collects configuration data about a range of network devices, including servers, routers, switches, firewalls, and networked phone systems. The automated information-gathering process can include the following activities:

- Ping the network devices
- Perform port scans on each device
- Use SNMP[1] v2 or v3 to collect Standard and Enterprise MIBs[2]
- Logon to each device using administrator-provided credentials to access device configuration files
- Logon to each device by attempting to guess passwords to access device configuration files
- Use TFTP[3] to pull information from phone system components.
- Analyze *syslog* records sent to NetMRI by the network devices.

NetMRI performs basic data analysis functions in real-time as data is collected, and more in-depth analysis is performed on a scheduled basis. Analysis focuses on identifying network configuration problems related to network configuration correctness, stability, performance, and other network-wide factors. NetMRI analyzes the contents of various router and switch tables to detect system-level problems, such as router and VLAN[4] instability. NetMRI also performs "Configuration Management", which allows administrators to automatically verify the correctness of each infrastructure device's configuration file against one or more configuration policies. These policies include Infoblox-defined configuration policies that help ensure compliance with PCIDSS[5], SOX[6], DISA[7], STIG[8], IAVA[9], other NSA[10]-published best practices, or client-defined policies specific to their network. Additionally, NetMRI provides a tool to develop scripts to make changes to or pull specific information from devices. Pre-defined and custom-created scripts can be run to make configuration changes to devices across the network. The information

[1] Simple Network Management Protocol

[2] Management Information Bases

[3] Trivial FTP

[4] Virtual Local Area Network

[5] Payment Card Industry Data Security Standard

[6] Sarbanes-Oxley Act of 2002

[7] Defense Information Systems Agency

[8] Security Technical Implementation Guides

[9] Information Assurance Vulnerability Alert

[10] National Security Agency

provided by NetMRI is designed to provide a systems-level view of the network, including the configuration issues, communication issues, and topography view of the network. In addition to detecting and alerting the user to configuration or other device changes that violate corporate policies, NetMRI also has a corrective action (remediation) feature that can automatically repair, reconfigure or restore network settings.

NetMRI Distributed Configuration is a special product configuration that allows multiple deployed NetMRIs to work in tandem. In a Distributed Configuration deployment, one NetMRI acts as a "consolidator" for the other deployed NetMRIs across a large controlled network. In this mode, the other NetMRIs perform normal monitoring and analysis of their assigned network segments, and the NetMRI assigned the "consolidator" function provides a unified view of the overall configuration and health of the network. Data that is passed between instances of the TOE in this configuration are protected by the environment via SSL[11] VPN[12], and includes control information, remotely collected data, centrally defined configurations, policies and scripts, and software updates.

In addition to the functionality provided by the core NetMRI product, there are four option modules available which provide additional functionality:

- IPv6 Module: Provides compatibility with IPv6[13] networks to meet U.S. government requirements.
- IP Telephony Module: Provides analysis of call detail and performance on Cisco and Avaya Voice Over IP (VoIP) systems.
- API Module: Provides access to NetMRI's application programming interfaces (APIs) to allow development of custom solutions based on NetMRI's data, analysis, and automation capabilities.
- Event Analysis: Provides high-performance collection and analysis of *syslog* and SNMP trap events from network infrastructure devices.

NetMRI is sold in two types of configurations: as a Virtual Machine (VM) software image that can be installed on a host virtualization server, and as a range of physical appliances. Each appliance (virtual and physical) includes the underlying operating system (OS) (the "NetMRI OS") and provides several management interfaces, including a web-based GUI[14] and a CLI[15] protected by the environment via SSH[16].

The TOE can be configured to use a local user database, or to use remote authentication databases (such as RADIUS[17] or TACACS+[18]). The authentication database, if used, is not part of the TOE; but the TOE provides client-side support of these authentication methods.

1.3.1 TOE Environment

NetMRI is a software-only TOE that includes the underlying NetMRI OS and the NetMRI Application software. The Virtual Appliance version of the TOE is installed and deployed on general-purpose server hardware running a virtualization server, such as VMware ESX. The Physical Appliance version of the TOE is installed and deployed

[11] SSL – Secure Sockets Layer

[12] VPN – Virtual Private Network

[13] IP: Internet Protocol

[14] Graphical User Interface

[15] Command Line Interface

[16] Secure Shell

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

[18] TACACS+: Terminal Access Controller Access-Control System (plus)

on Infoblox-supplied appliance hardware. The management workstation provides access to the administrative management functions of the TOE.

The following NetMRI appliances can be used to run NetMRI:

- Model: Campus Rackmount 7200rpm
  - Processor: Intel E2160 Pentium Dual Core 1.8GHz, 800MHz FSB
  - RAM: 1GB DDR2 667MHz
  - Hard Drive: Seagate 250GB SATA , 7200rpm, 3GB/s, 16MB cache
- Model: Campus Rackmount 10k rpm
  - Processor: Intel E2160 Pentium Dual Core 1.8GHz, 800MHz FSB
  - RAM: 1GB DDR2 667MHz
  - Hard Drive: Seagate 250GB SATA , 10,000rpm, 3GB/s, 16MB cache
- Model: Small Enterprise Rackmount 7200rpm
  - Processor: Core 2 Duo E6700, 2.66GHz CPU, 4M 1066 MHz
  - RAM: 3GB DDR2 667MHz
  - Hard Drive: Seagate 250GB SATA , 7200rpm, 3GB/s, 16MB cache
- Model: Large Enterprise Rackmount with SAS drives
  - Processor: Intel Q6600 Quad Core Processor, 2.40GHz, 1066MHz FSB, 8MB L2 Cache
  - RAM: 4GB DDR2 667MHz
  - Hard Drive: Seagate 147GB SAS , 15,000rpm, 3GB/s, 16MB cache
- Model: NextGen Large Enterprise Rackmount
  - Processor: Intel X3220 Quad Core Processor, 2.40GHz, 1066MHz FSB, 8MB L2 Cache
  - RAM: 8GB DDR2 667MHz
  - Hard Drive: Western Digital 300GB VelociRaptor SATA , 10,000rpm, 300MB/s, 16MB cache

The following versions of VMWare can be used to run NetMRI:

- VMWare vSphere 4 (ESX/ESXi 3.5/4.0 managed hosts)
- VMWare ESX/ESXi 4.0 (standalone)
- Virtual Center 2.5 managed ESX/ESXi 3.5 hosts
- VMWare ESX/ESXi 3.5 (standalone)
- VMWare Workstation 6.51+
- VMWare Player 2.5.3+
- VMWare Server 2.0.1+
- VMWare ACE 2.5.3+
- VMWare Fusion

Management workstations can run any operating system that supports a supported web browser client or secure shell client. Infoblox supports the following web browsers to manage the NetMRI:

- Microsoft Internet Explorer version 7
- Microsoft Internet Explorer version 8
- Mozilla Firefox version 3.0+

Version 9 or later of Adobe Flash Player must be installed on the management workstations accessing the NetMRI.

Any secure shell client can be used to access the NetMRI CLI as long as the secure shell client provides support for SSH, such as Putty, CopSSH, and eSSH.

NetMRI does not place restrictions on the OS of the Authentication Server used for remote authentication, as RADIUS and TACACS+ are installed and configured separately from the NetMRI.

1.3.2 TOE Physical and Logical Scope

Figure 1 and Figure 2 illustrate the physical and logical scope and boundary of the two deployment scenarios and tie together all of the components of the TOE and the constituents of the TOE Environment.

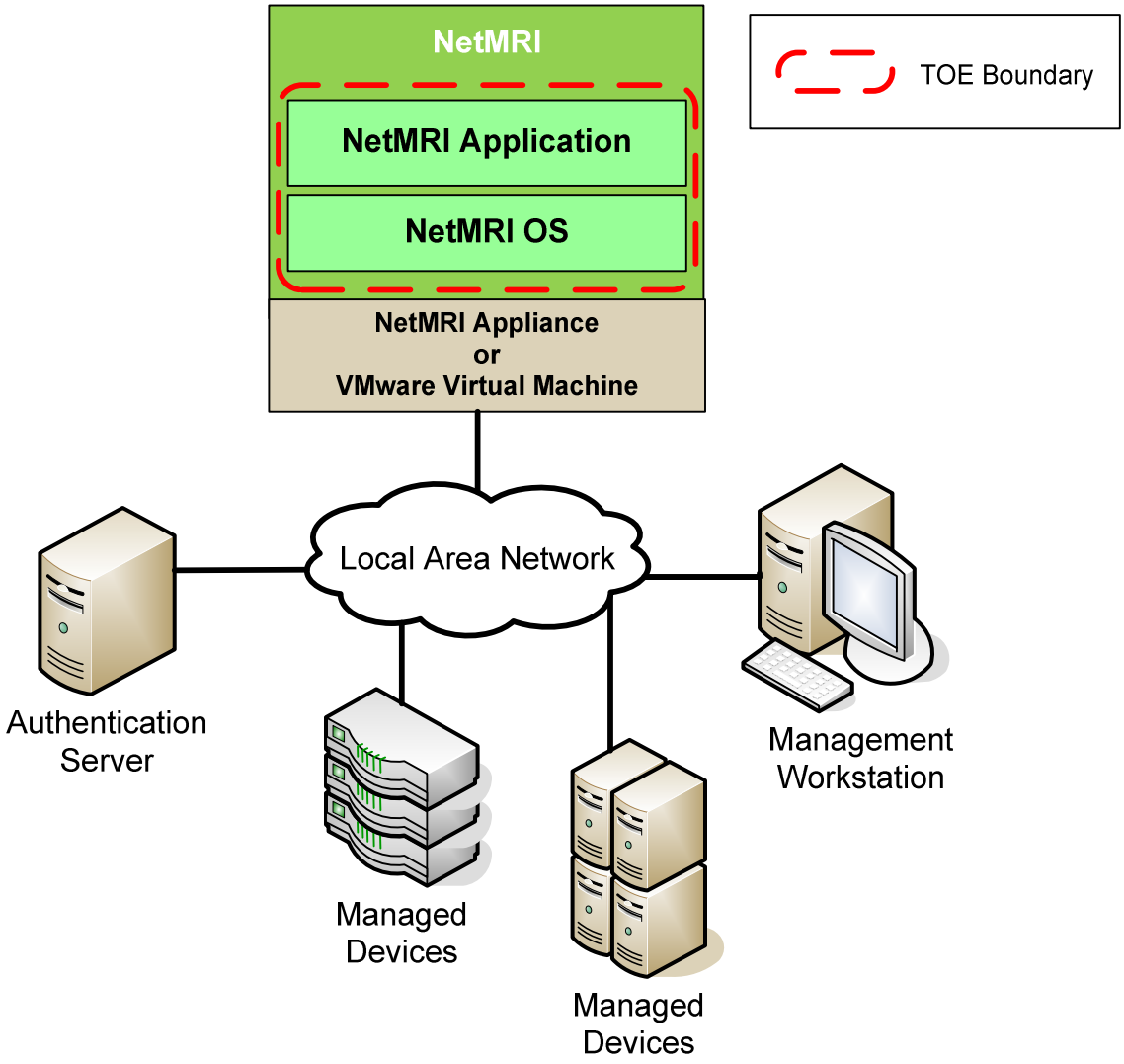

Figure 1 - TOE and TOE Environment: Standalone Deployment

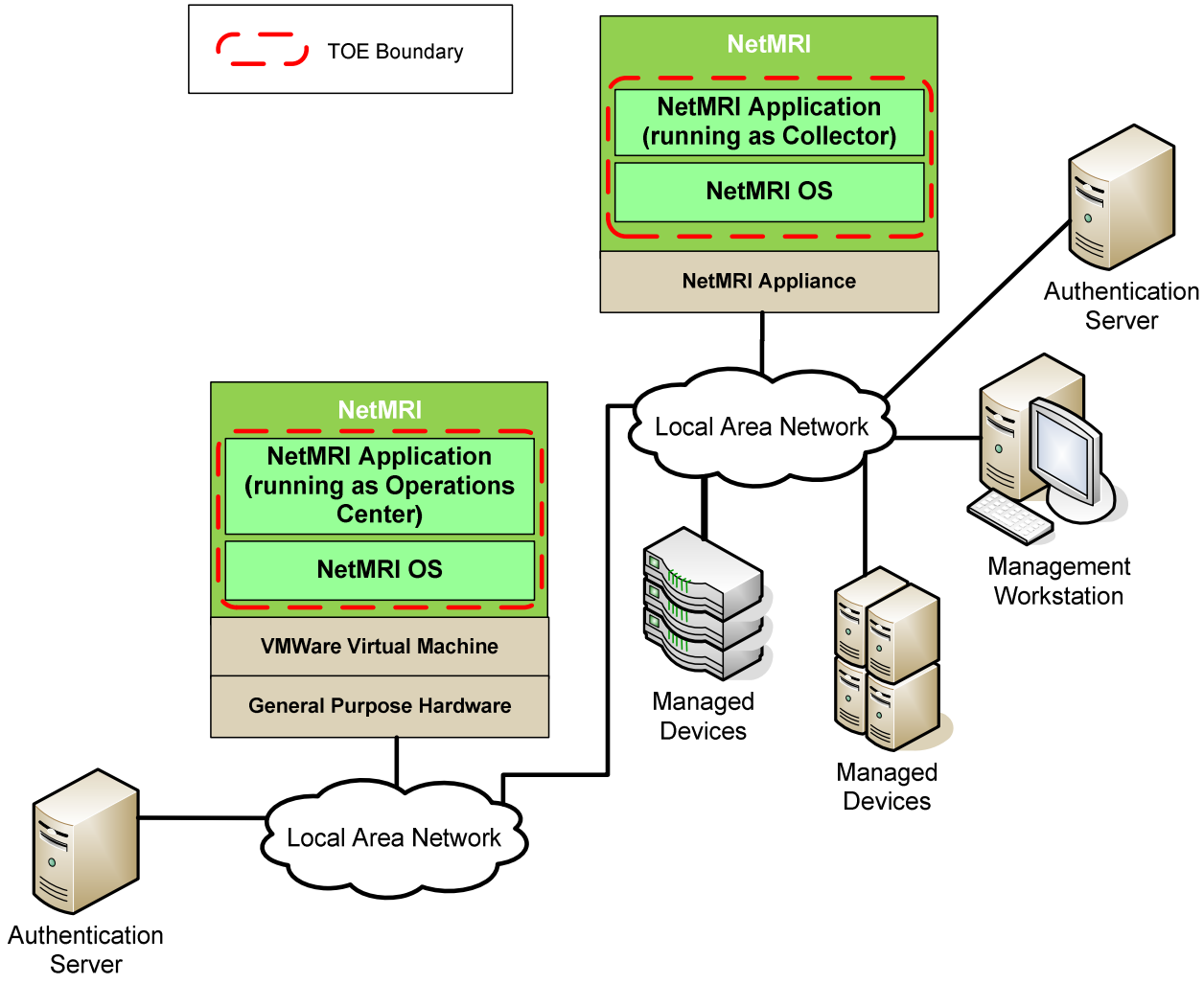

Figure 2 - TOE and TOE Environment: Distributed Configuration Deployment

The TOE boundary depicted above includes the NetMRI Application software and the NetMRI operating system, whether installed on a VM or a physical appliance. The underlying hardware, managed devices, and other connected systems are not included in the TOE boundary, but are required or optional components of the TOE environment. The NetMRI can be deployed in either standalone or Distributed Configuration modes.

The following documents provide end-user guidance:

- NetMRI User's Guide v4
- NetMRI Installation Guide v4

1.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

The following features or functionality are excluded from the evaluated configuration of the TOE:

- Encryption
- Server-side RADIUS and TACACS+ functionality.

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 3, July 2009; CC Part 2 conformant; CC Part 3 conformant.
PP Identification	None
Evaluation Assurance Level	EAL2 augmented with Flaw Remediation (ALC_FLR.2)

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 low skill level
- have limited resources to alter TOE configuration settings
- have no physical access to the TOE
- possess a low level of motivation
- have a low attack potential

The Information Technology (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.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 must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and one alphabetical character (from a set of 52, including upper-case and lower-case letters).

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 must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.INTEGRITY	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.TIME	The TOE will provide reliable timestamps for its own use.

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.PROTECT	The IT Environment will protect data from unauthorized modification and disclosure when it is transmitted between physically-separated parts of the TOE.
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.

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_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FDP_ACC.2	Complete access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_ETC.1	Export of user data without security attributes		✓		
FDP_ITC.1	Import of user data without security attributes		✓		

Name	Description	S	A	R	I
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
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_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable time stamps				
FTA_SSL.3	TSF-initiated termination		✓		
FTA_TAB.1	Default TOE access banners				

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[19] 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_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

[19] TOE Security Functionality

The TSF shall provide [*administrators*] 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.2 Restricted audit review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

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 [*event type*].

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

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

FAU_STG.4.1

The TSF shall [*ignore audited events*] and [*cease operating*] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

6.2.2 Class FDP: User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

FDP_ACC.2.1

The TSF shall enforce the [*Management Access Control SFP*[20]] on [*subjects: TOE users, and objects: network device configuration data, network device authentication data, audit data and TOE configuration data*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2

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 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

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

- *Subjects: TOE users*
  - *Security Attributes:*
    - *Username*
    - *User permissions*
- *Objects: network device configuration data, network device authentication data, audit data and TOE configuration data*
  - *Security Attributes:*
    - *Permissions*

].

FDP_ACF.1.2

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 network device configuration data, network device authentication data, audit data, and/or the TOE configuration if the user has the appropriate permissions*].

[20] SFP: Security Function Policy

FDP_ACF.1.3

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

FDP_ACF.1.4

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_ETC.1 Export of user data without security attributes

Hierarchical to: **No other components.**

FDP_ETC.1.1

The TSF shall enforce the [*Management Access Control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]

Application Note: There is one exception to this requirement: The username of the user performing the action will be exported with the audit logs.

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: **No other components.**

FDP_ITC.1.1

The TSF shall enforce the [*Management Access Control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*imported user data will be placed under the control of the Management Access Control SFP while stored within the TOE*].

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [*an administrator configurable positive integer within [zero to ten]*] unsuccessful authentication attempts occur related to [*failed login attempts*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [*surpassed*], the TSF shall [*lock out the affected account for an administrator configurable period within five minutes to twenty four hours, and send an email to an administrator if so configured*].

Dependencies: FIA_UAU.1 Timing of 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, user permissions, role, role permissions, password (if the user is a local user)*].

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [*the following requirements: have a minimum password length of eight characters, must contain at least one numeric character (from a set of 10) and one alphabetical character (from a set of 52, including upper-case and lower-case letters), and must not contain any of the following special characters: ; , | = “ ‘)*].

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*] to restrict the ability to [*query, modify, delete*] the security attributes [*relevant to that SFP*] 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*] 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_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 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 [*Default: View; SysAdmin; UserAdmin; ConfigAdmin; PolicyManager; ChangeEngineerHigh; ChangeEngineerMedium; ChangeEngineerLow; AnalysisAdmin; EventAdmin; FindIT; GroupManager*].

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_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

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 [*a configurable interval of user inactivity up to twenty-fours, unless the autoupdate command has been issued*].

Dependencies: No dependencies

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

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.2. 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.2 Flaw reporting procedures
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_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_ITC.1	Import of user data without security attributes
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	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_SMF.1	Specification of management functions

	FMT_SMR.1	Security roles
Protection of the TSF	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners

7.1.1 Security Audit

The TOE audits administrative actions (whether they succeed or fail) and stores the audit trail in a central database. The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity, user identity, and a message indicating the outcome (success or failure) of the event. The TOE also audits the startup and shutdown of the audit function.

The TOE provides robust audit review functions, including searching, sorting, and ordering of the audit records. It restricts audit review to users with the appropriate permissions. The TOE does not allow the unauthorized deletion or modification of audit records. If the audit trail is filled to capacity, the TOE will ignore further audit events and cease operation.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4.

7.1.2 User Data Protection

User data for the TOE comprises the configuration data gathered from the network devices and the authentication data used to access those devices. User data can be imported to and exported from the TOE. Any external security attributes are ignored when user data is imported, and the data's associated TOE security attributes are stripped from the data before it is exported.

Management Access Control permissions are implemented in a granular and hierarchical way. The "subjects" of the Policy are the users. Each user has a username and permissions. The "objects" of the Management Access Control Policy are the system data and devices to be managed. System data for the TOE comprises TOE audit data and configuration data.

7.1.2.1 Management Access Control SFP

The Management Access Control SFP defines the access restrictions on the system data, that is TOE configuration and audit data, and user data, which is network device configuration and authentication data. These restrictions state that only users with sufficient privilege to access this data may access it.

TOE Security Functional Requirements Satisfied: FDP_ACC.2, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1.

7.1.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting an authenticated service has provided a valid username and password and is authorized to access that service (users may access licensing functions without authentication). For each user, the TOE stores the following security attributes in the database: username, user permissions, role, role permissions, and password (if the user is a local user). Passwords 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 one alphabetical character (from a set of 52, including upper-case and lower-case letters.

The TOE can be configured to use a local user database, or to use remote authentication databases (such as RADIUS or TACACS+). 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; if not, then the user is allowed to re-authenticate until an administrator-configurable number of successive unsuccessful authentication attempts have been made, at which point the TOE will lock the account for a configurable amount of time and optionally inform an administrator via email. TOE users must identify and authenticate themselves to the TOE before they can perform any action.

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

7.1.4 Security Management

The TOE offers robust and granular permissioning of users, groups, and devices. This allows the TOE to maintain an unbounded number of differently permissioned users and groups. Table 12 below provides a list of the default roles provided with the TOE; other roles can be created and defined by authorized administrators. The TOE does not allow users to have null passwords and does not provide anonymous access. Accounts can be locked after a configurable number of failed access attempts, and administrators can also effectively disable any user account at any time by administratively changing that account's password.

Table 12 - Pre-defined Roles

Name	Description
Default: View	Gives general access to NetMRI with view of non-sensitive data only.
SysAdmin	NetMRI System Administration Role. Allows access to all sections of NetMRI.
UserAdmin	Provides privileges that allow a user to create and modify NetMRI Users.
ConfigAdmin	Allows users to view sensitive device information including configuration information and passwords.
PolicyManager	Define and deploy policies for one or more groups within NetMRI.
ChangeEngineerLow	Execute and schedule scripts designated Level 1 (Low Risk).
ChangeEngineerMedium	Execute and schedule scripts designated Level 2 (Medium Risk).
ChangeEngineerHigh	Author, execute and schedule scripts designated Level 3 (High or Unknown Risk).
AnalysisAdmin	Create and manage NetMRI Issues.
EventAdmin	Create event symptoms.

Name	Description
FindIT	User will only have access to the FindIT NetMRI interface.
GroupManager	Create and manage device groups, interface groups and result sets in NetMRI.

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

7.1.5 Protection of the TSF

The TOE's operating system communicates with the underlying hardware's real-time clock in order to generate reliable time stamps.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.6 TOE Access

The TOE will end the session of any idle user after twenty-four hours of inactivity. It also displays a configurable advisory warning message to the user during login. The only exception to this is when the administrator executes the autoupdate command in the admin shell. While the autoupdate is executing, autologout will be disabled.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_TAB.1.

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

The following table maps threats to objectives.

Table 13 - Threats:Objectives Mapping

Threats	Objectives	Rationale
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.	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.	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 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 The TOE 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 prior to allowing access to TOE functions and data.
	O.INTEGRITY The TOE must ensure the integrity of all audit data.	This threat is primarily diminished by the O.INTEGRITY objective, which requires that the TOE 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.	The O.PROTECT objective requires that the TOE protect itself from unauthorized modifications and access to its functions and data.
	O.TIME The TOE will provide reliable timestamps for its own use.	The O.TIME objective requires the TOE to provide reliable timestamps for its own use. The OE.TIME environmental objective supports this

Threats	Objectives	Rationale
		objective.
	OE.PROTECT The IT Environment will protect data from unauthorized modification and disclosure when it is transmitted between physically-separated parts of the TOE.	The OE.PROTECT objective supports these objectives by requiring that the IT environment provide mechanisms, such as an SSL[21] or TLS[22] tunnel, that protect data from unauthorized modification and disclosure during transmission between physically separate TOE components.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.TIME 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.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.	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.	The O.ADMIN and O.ACCESS objectives together ensure that policies will not 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 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 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 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.

[21] Secure Sockets Layer

[22] Transport Layer Security

Threats	Objectives	Rationale
	O.PROTECT 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.
	O.TIME The TOE will provide reliable timestamps for its own use.	The O.TIME objective requires the TOE to provide reliable timestamps for its own use. The OE.TIME environmental objective supports this objective.
	OE.PROTECT The IT Environment will protect data from unauthorized modification and disclosure when it is transmitted between physically-separated parts of the TOE.	The OE.PROTECT objective supports these objectives by requiring that the IT environment provide mechanisms, such as an SSL or TLS tunnel, that protect data from unauthorized modification and disclosure during transmission between physically separate TOE components.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.TIME 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

The following table maps policies to objectives.

Table 14 - Policies:Objectives Mapping

Policies	Objectives	Rationale
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 must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of	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.ACCESS ensures that only authorized users are allowed access to the TOE and its managed devices.
	O.IDAUTH	O.IDAUTH ensures that a user must identify and authenticate before

10), and one alphabetical character (from a set of 52, including upper-case and lower-case letters).	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	access to the TOE and its managed devices is granted.

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

The following table maps assumptions to objectives.

Table 15 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL 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 Physical security will be provided for the TOE and its environment.	NOE.PHYSICAL 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

The following table maps objectives to SFRs.

Table 16 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
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.	FDP_ACC.2 Complete access control	The TOE has an access control policy that ensures that only authorized users gain access to TOE functions and data.
	FDP_ACF.1 Security attribute based access control	The TOE is required to provide authorized users access to TOE functions and data.
	FDP_ETC.1 Export of user data without security attributes	The TOE will export user data stripped of its TOE security attributes.
	FDP_ITC.1 Import of user data without security attributes	The TOE will ignore external security attributes when importing user data.
	FIA_AFL.1 Authentication failure handling	The TOE will lock out user accounts that have experienced too many successive unsuccessful authentication attempts.
	FIA_SOS.1 Verification of secrets	The TOE will verify that user passwords meet administrator-specified complexity requirements.
	FIA_UAU.2 User authentication before any action	The TOE will not give any access to a user until the TOE has authenticated the user.
	FIA_UID.2 User identification before any action	The TOE will not give any access to a user until the TOE has identified the user.
	FMT_MOF.1 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 Static attribute initialisation	Restrictive values for TOE functions and data are provided, and the authorized administrator can change them when an object is created.
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.	FMT_MOF.1 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 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.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMF.1 Specification of management functions	Mechanisms exist to enforce the rules defined in FMT_MOF.1.
	FMT_SMR.1 Security roles	The TOE defines a set of roles.
	FTA_SSL.3 TSF-initiated termination	The TOE automatically terminates administrative sessions after twenty-four hours of inactivity, unless the autoupdate command is executing.
	FTA_TAB.1 Default TOE access banners	The TOE must display a warning banner during user login.
O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	FAU_GEN.1 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_GEN.2 User identity association	The TOE must associate auditable events with the user that caused them to occur.
	FAU_SAR.1 Audit review	The TOE must provide the ability to review the audit trail of the system.
	FAU_SAR.2 Restricted audit review	The TOE must restrict read access to the audit records to only those users that have been granted read-access.
	FAU_SAR.3 Selectable audit review	The TOE must provide the ability to search, sort, and order the audit trail of the system.
	FPT_STM.1 Reliable time stamps	The TOE must provide reliable time stamps for use in the audit trail.
O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_ATD.1 User attribute definition	Security attributes of subjects used to enforce the authentication policy of the TOE must be defined.
	FIA_UAU.2 User authentication before any action	The TOE will not give any access to a user until the TOE has authenticated the user.
	FIA_UID.2 User identification before any action	The TOE will not give any access to a user until the TOE has identified the user.
	FMT_SMR.1 Security roles	The TOE must be able to recognize the different user roles that exist for

Objective	Requirements Addressing the Objective	Rationale
		the TOE.
O.INTEGRITY The TOE must ensure the integrity of all audit data.	FAU_STG.1 Protected audit trail storage	The TOE is required to protect the audit data from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	If the audit trail is filled to capacity, the TOE is required to ignore auditing events and cease operation.
	FDP_ACF.1 Security attribute based access control	Only authorized TOE users with the appropriate permissions may access audit data.
	FMT_MSA.1 Management of security attributes	Only authorized users of the System may query and modify TOE 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.	FDP_ACC.2 Complete access control	The TOE has an access control policy that ensures that only authorized users can modify and access TOE functions and data.
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to TOE functions and data.
	FMT_MOF.1 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.
O.TIME The TOE will provide reliable timestamps for its own use.	FPT_STM.1 Reliable time stamps	The TOE must provide reliable time stamps for use in the audit trail.

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 connected to 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.2 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 17 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 17 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Although FIA_UID.1 is not included, the hierarchical SFR FIA_UID.2 is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.2	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	Although FDP_ACC.1 is not included, the hierarchical SFR FDP_ACC.2 is included. This satisfies this dependency.
	FMT_MSA.3	✓	
FDP_ETC.1	FDP_ACC.1	✓	Although FDP_ACC.1 is not included, the hierarchical SFR FDP_ACC.2 is included. This satisfies this dependency.
FDP_ITC.1	FDP_ACC.1	✓	Although FDP_ACC.1 is not included, the hierarchical SFR FDP_ACC.2 is included. This satisfies this dependency.
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, the hierarchical SFR FIA_UAU.2 is included. This satisfies this dependency
FIA_ATD.1	None	✓	
FIA_SOS.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.

SFR ID	Dependencies	Dependency Met	Rationale
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 SFR FDP_ACC.2 is included. This satisfies this dependency.
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.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_STM.1	None	✓	
FTA_SSL.3	None	✓	
FTA_TAB.1	None	✓	

9 Acronyms

Table 18 - Acronyms

Acronym	Definition
API	Application Programming Interface
CC	The Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
DISA	Defense Information Systems Agency
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IAVA	Information Assurance Vulnerability Alert
IP	Internet Protocol
IT	Information Technology
MIB	Management Information Base
NCCM	Network Configuration and Change Management
NSA	National Security Agency
OS	Operating System
OSP	Organizational Security Policy
PCIDSS	Payment Card Industry Data Security Standard
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy

Acronym	Definition
SNMP	Simple Network Management Protocol
SOX	Sarbanes-Oxley Act of 2002
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
STIG	Security Technical Implementation Guides
TACACS+	Terminal Access Controller Access-Control System (plus)
TFTP	Trivial FTP
TOE	Target of Evaluation
TSF	TOE Security Functionality
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VM	Virtual Machine
VPN	Virtual Private Network