Hewlett Packard Enterprise Development LP
Network Automation Ultimate Edition v10.10

Security Target

Evaluation Assurance Level: EAL 2+
Document Version: 0.13

Prepared for:

Hewlett Packard Enterprise Development LP
3000 Hanover Street
Palo Alto, CA 94304
United States of America

Phone: +1 305 267 4220
Email: info@hpe.com
http://www.hpe.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Hewlett-Packard (HP) Network Automation Ultimate Edition v10.10, and will hereafter be referred to as the TOE throughout this document. The TOE is a software solution that tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers, and wireless access points. The TOE provides visibility into network changes, enabling an IT staff to identify and correct trends that could lead to problems, while mitigating compliance issues, security hazards, and disaster recovery risks.

1.1 Purpose

This ST is divided into nine sections, as follows:

- 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), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (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 (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 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Hewlett Packard Enterprise Development LP Network Automation Ultimate Edition v10.10 Security Target
ST Version	Version 0.13
ST Author	Corsec Security, Inc.
ST Publication Date	9/22/2015
TOE Reference	HP Network Automation Ultimate Edition 10.10 build #413-052115

ST Title	Hewlett Packard Enterprise Development LP Network Automation Ultimate Edition v10.10 Security Target
FIPS[1] 140-2 Status	Level 1, RSA[2] BSAFE Crypto-J JSAFE and JCE[3] Software Module, Software Version 6.1, Certificate No. 2057

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, 1.4 TOE Overview, will introduce the parts of the overall product offering that are specifically being evaluated.

HP's Network Automation Ultimate Edition (NA) Software v10.10 is a centralized infrastructure management and policy enforcement solution that tracks and regulates network device configuration changes across routers, switches, firewalls, load balancers, and wireless access points. When integrated with another HP product offering, HP Network Node Manager i (NNMi), these two products provide a comprehensive solution that unifies network fault, availability, and performance with change, configuration, compliance, and automated diagnostics.

NA discovers network devices and obtains and stores each device's current configuration. Device discovery is natively supported by NA for leading vendors such as HP, Cisco, Nortel, Extreme Networks, and F5 Networks, and it can also be extended through customization to support any network device. To access the devices, NA maintains a database containing all device credentials. NA encrypts all credentials using an AES[4]-256-bit encryption key prior to storage in the database to prevent these credentials from disclosure.

For each discovered device, NA will obtain the device's currently running configuration (also referred to as a 'configuration snapshot') and then store that information for historical and compliancy purposes. NA will then continue to monitor the discovered devices for any subsequent configuration changes. When a change is detected, NA automatically obtains the updated configuration snapshot and stores this (and all future changes) alongside the original configuration snapshot. NA also stores the following additional metrics with each configuration snapshot:

- Where the change occurred,
- What changed,
- Who committed the change, and
- Why the change was made.

In addition to the collection and storage of configuration snapshots, the NA solution continuously mitigates compliance issues, security hazards, and disaster recovery risks through the NA Policy Manager component. Policy Manager is capable of enforcing both best practices and regulatory compliance policies to ensure that the network meets security, reliability, and quality goals. If a device is found to be out of compliance with one or more policies, NA triggers a non-compliance event. NA provides administrators the ability to configure specific remediation actions that should occur if a non-compliance event occurs. NA automates the laborious task of validating that the devices and configurations are in compliance with the defined best practices or regulatory standards, as well as the remediation steps required to bring the device back into compliance.

NA supports multiple deployment scenarios:

- Standalone – single instance of NA with a single database (DB) Server (shown in Figure 1 below),
- Multimaster Distributed System – multiple instances of NA, each with a dedicated DB Server, and

[1] FIPS – Federal Information Processing Standard
[2] RSA – Ron Rivest, Adi Shamir, and Leonard Adleman
[3] JCE – Java Cryptography Extension
[4] AES – Advanced Encryption Standard

- Horizontal Scalability (HS) – multiple instances of NA sharing a common DB Server.

For the purposes of the CC Evaluation, only the 'Standalone' deployment scenario will be evaluated.

A standalone instance of NA can support approximately 25,000 devices and can scale in size for even the largest of organizations using a Horizontal Scalability or Multimaster Distributed System deployment. In the Multimaster Distributed System deployment scenario, the DB Servers are replicated between NA instances, providing some disaster recovery capabilities. In the Horizontal Scalability deployment, there is a single DB Server that multiple NA servers share, and also provides some failover and disaster recovery configuration options.

Figure 1 contains the following undefined acronyms:

- CLI – Command Line Interface
- HTTPS – Hypertext Transfer Protocol – Secure
- LDAP – Lightweight Directory Access Protocol
- JRE – Java Runtime Environment
- API – Application Programming Interface
- RHEL – Red Hat Enterprise Linux

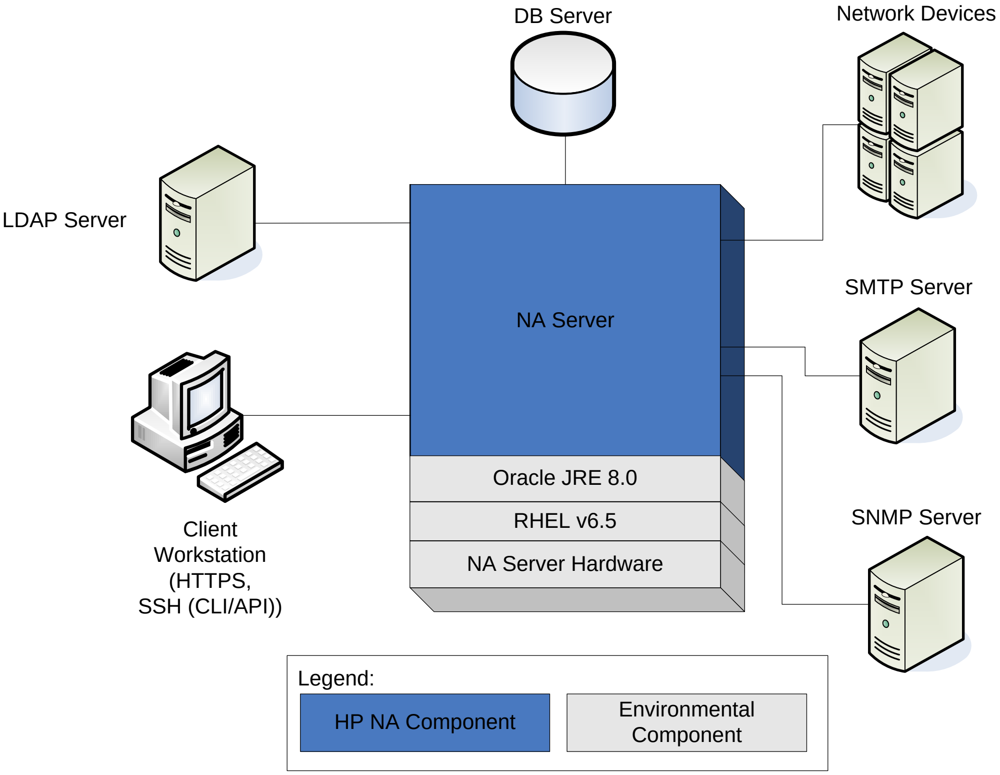

Figure 1 Stand Alone Deployment Configuration

1.4 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.

The TOE is a centralized infrastructure management and policy enforcement solution that tracks and regulates network device configuration changes across routers, switches, firewalls, load balancers, and wireless access points. The TOE discovers network devices and retrieves and stores each device's current configuration information. The TOE provides all of the management and policy compliance functionality in addition to locally discovering devices connected to the same network.

To discover network devices, the TOE uses internal components called 'drivers' (preinstalled or created) that are designed specifically for the network devices. Each driver contains the credentials required to access the network devices. The TOE encrypts the credentials for network devices using an AES-256-bit key prior to storage in the database. Once the drivers are in place, the TOE will discover all of the devices in the network for which a driver exists and store each device's configuration to the DB Server as a configuration snapshot. The TOE will then monitor each device closely through syslog messages sent from the device to an internal syslog server. When a change in the device configuration is detected, an updated configuration snapshot will be obtained from the device and stored with the existing configuration snapshots. The TOE queries configuration snapshots from the DB Server on behalf of a TOE administrator during manual device compliance checks or during automated policy enforcement tasks.

In addition to collecting and storing configuration snapshots, the TOE mitigates compliance issues, security hazards, and disaster recovery risks through the TOE's Policy Manager component. Policy Manager is capable of enforcing compliance policies to ensure that the devices monitored by the TOE always remain in compliance. If a device is found to be out of compliance with one or more policies, an event is generated. TOE administrators can create tailored actions for the TOE to invoke, when specific non-compliance events occur.

The TOE performs compliance checks on the device's configuration snapshots using 'Policies.' Policies may be created or imported by a TOE administrator and are composed of one or more 'Rules.' Each Rule in the Policy is applied to a set of devices and their corresponding configuration snapshots. The set of devices can be manually chosen by a TOE administrator or based on a set of matching attributes. If any Rule is broken, the device will be flagged as out of compliance causing a non-compliance event to be generated. The TOE administrator can configure non-compliance events to trigger actions such as executing tasks (snapshot or diagnostic), sending email notifications, sending SNMP[5] traps, or sending syslog messages.

The TOE provides a web-based graphical user interface (GUI) and a CLI/API that can be used by TOE administrators to manage Policies and Rules, create and edit user accounts, review audit logs, and manage cryptographic functionality. The TOE functionality is available only to authenticated TOE operators and further restricted based upon the role permissions associated with their account (such as the ability to review audit logs or compliance violation data). Both the CLI/API and web GUI enforce identification and authentication of TOE operators before any TOE functionality may be invoked. The TOE audits administrative actions such as logins and logouts, TOE operator account management activities, policy creation and manipulation, and other configuration changes performed on the TOE.

The TOE uses a FIPS-validated cryptographic module to provide secure communication channels and paths. The TOE provides secure connection with the web GUI using HTTPS (via TLS) and with the CLI/API using SSH. For device discovery and configuration snapshots, the TOE can connect to remote devices in the TOE environment over a trusted channel using SSH.

Figure 2 below shows the details of the CC Evaluated configuration of the TOE.

[5] SNMP – Simple Network Management Protocol

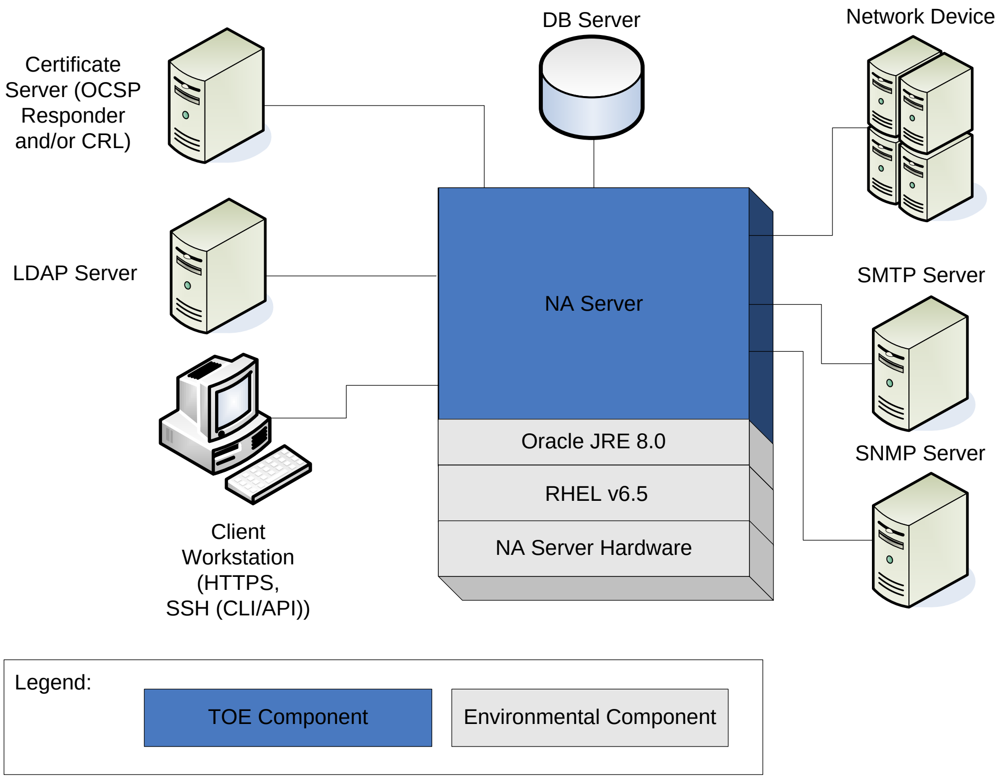

Figure 2 CC Evaluated Configuration of the TOE

1.4.1 TOE Environment

The TOE is intended to be deployed on TOE environmental hardware in a physically secure cabinet room or data center with appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

The RHEL v6.5 underlying operating system, Oracle JRE 8.0, and NA Server hardware are parts of the TOE environment. The entire management workstation, its browsers, SSH clients, and API tools are all considered part of the TOE environment as well. The TOE actively monitors network devices for compliance, and all the monitored network devices are components of the TOE environment. The TOE supports an external authentication server for LDAP, the authentication server is also a TOE environmental component.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE boundary consists of only the NA Server software, which comprises the HP NA v10.10 binary. The TOE is installed on the RHEL v6.5 OS running on hardware. The deployment configuration of the TOE is shown as depicted in Figure 3 below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Hardware running RHEL v6.5 for the TOE (NA Server)
- Client workstation used to connect to the TOE, installed with:
  - Mozilla Firefox 24 Extended Support Release (or newer) or Internet Explorer 11.0 or newer
  - SSH client such as PuTTy .61 or newer
- Authentication Server to support LDAP external authentication requests
- Certificate Server configured for X.509 certificates (CAC/PIV configuration requires access to at least one of the following: CRL distribution point or OCSP[6] responder)
- MySQL Database Server version 5 or newer
- Oracle JRE 8.0
- Actively monitored network devices
- SNMP Server
- SMTP Server

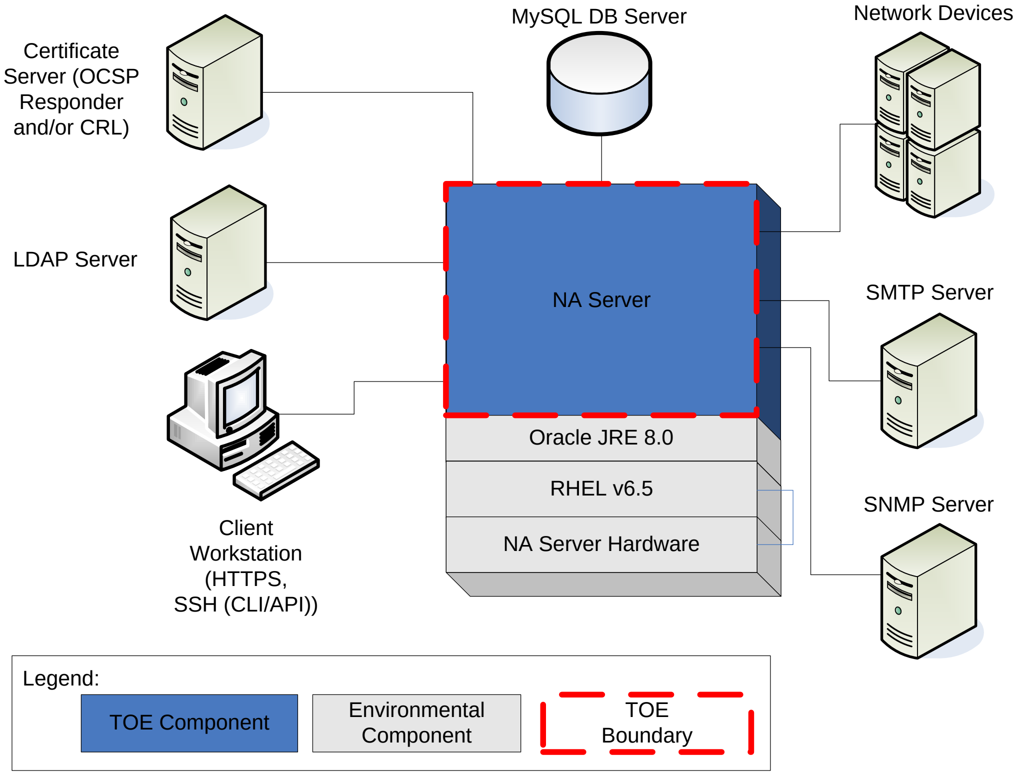

Figure 3 Physical TOE Boundary

1.5.1.1 Guidance Documentation

Table 2 lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

[6] OCSP – Online Certificate Status Protocol

Table 2 Guidance Documentation

Document Name	Description
HP Network Automation Software For the Windows ®, Linux, and Solaris operating systems, Software Version 10.10, Installation and Upgrade Guide, June 2015	Includes steps for the installation and upgrade of the TOE.
HP Network Automation Software For the Windows ®, Linux, and Solaris operating systems, Software Version 10.10, Administrator Guide, June 2015	Contains detailed steps for how to properly configure and maintain the TOE.
HP Network Automation Software For the Windows ®, Linux, and Solaris operating systems, Software Version 10.10, User Guide, June 2015	
HP Network Automation Software (NA) CLI/API Command Reference, Software Version 10.10, June 2015	Contains a list of commands and their descriptions that can be entered in over the CLI.
HP Network Automation Software For the Windows ®, Linux, and Solaris operating systems, Software Version 10.10, Support Matrix, June 2015	Provides an overview of the system requirements and supported platforms for HP Network Automation Software version 10.10.
HP Network Automation Software For the Windows ®, Linux operating systems, Software Version 10.10, Release Notes, June 2015	Provides an overview of the changes made to HP NA software.
HP Network Automation Software For the Windows ®, Linux operating systems, Software Version 10.10, Hardening Guide, June 2015	Provides guidance on putting HP NA into secure mode for CC compliance.
HP Network Automation Open Source and Third Party Software License Agreements, June 2015	Provides verification of all open source and thirdy party licenese included in HP NA.
HP Inc. Network Automation Ultimate Edition v10.10 Guidance Supplement v0.4	Contains information regarding specific configuration for the TOE evaluated configuration.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- TOE Access
- Trusted path/channels
- Network Automation Support

1.5.2.1 Security Audit

The TOE generates log files to record auditable events. The TOE audits login and logout events, user account administration, and policy creation, import, modification, and deployment actions. The audit logs contain the identity of the user (if applicable) that caused event to occur. The TOE provides TOE operators with the ability to review the audit logs via the web GUI.

1.5.2.2 Cryptographic Support

The TOE utilizes the FIPS 140-2 validated RSA BSAFE Crypto-J JSAFE and JCE Software Module, Software Version 6.1 library for performing all cryptographic operations. The TOE provides cryptographic functions to secure sessions between:

- The client workstation and the TOE using HTTPS/TLS (for web GUI sessions) and SSH (for CLI/API sessions).
- The TOE and an LDAP authentication server using TLS.
- The TOE to network devices during discovering and monitoring using SSH.

Cryptographic keys are generated using a NIST[7] Special Publication (SP) 800-90A deterministic random bit generator (DRBG). Keys are securely erased when no longer needed by the application.

1.5.2.3 Identification and Authentication

The TOE enforces identification and authentication on users attempting to access the TOE prior to allowing any TOE functionality being invoked. The TOE maintains the following list of attributes for each user: a username, a secret (password or X.509 certificate depending on the authentication method specified), emaswil address and a role. Upon successful identification and authentication, the user is permanently associated with these attributes during the active session. The TOE also provides obscured authentication feedback during login over the web GUI and provides no feedback during login via the CLI/API.

1.5.2.4 Security Management

The TOE supports the default roles of: Limited Access User, Full Access User, Power User, and Administrator. Only the Power User and Administrator roles may manage the TOE’s configuration. The remaining two roles provide access to the monitored network device compliance information but do not provide any access to configure the TOE Security Functions (TSF). The management of TSF data is categorized by role and operations that can be performed for a given role. The TOE offers user management via the ‘Users’ option under the ‘Admin’ menu option. Only the Administrator role can manage TOE user accounts.

1.5.2.5 TOE Access

Operators accessing the TOE via the web GUI are presented by a TOE access banner prior to identification and authentication. All operators must acknowledge and accept the contents of the access banner before they can proceed with the login process.

1.5.2.6 Trusted Paths/Channels

The cryptographic functionality of the TOE provides the TOE with the ability to create trusted paths and trusted channels. The TOE implements trusted channels using HTTPS/TLS between itself and a remote LDAP authentication server during remote authentication attempts to provide protection of the credentials during transmission. The TOE also implements a trusted channel via SSH during network device discovery and monitoring activities. Additionally, the TOE provides trusted paths between TOE operators and the CLI/API via SSH, and between TOE operators and the web GUI via HTTPS.

The management communication path and trusted channels are distinct from other communication paths and channels and provide mutual identification and authentication. In addition, the communications are protected from modification and disclosure.

[7] NIST – National Institute of Standards and Technology

1.5.2.7 Network Automation Support

The TOE provides the ability to automatically discover and monitor devices within a local or remote network for compliance against Policies, made up of a collection of Rules. The TOE obtains configuration snapshots and compares the snapshots against all applicable Policies. The TOE applies its configured policies against the collected device configuration snapshots. If a Rule is not matched, and therefore a device is found to be out of compliance, the TOE will generate a non-compliance event. TOE administrators can define automatic actions for the TOE to invoke for non-compliance events. Additionally, the TOE restricts access to data regarding the compliance violations to all roles within the TOE except the Limited Access User role.

1.5.3 Product Physical and Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Plaintext device discovery over all protocols except SSH

2 Conformance Claims

This section and Table 3 provide 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 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2014/06/20 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 2+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

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 to the IT[8] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 Threats

Name	Description
T.NOAUDIT	Threat agents may perform security-relevant operations on the TOE without being held accountable for it.
T.TRANSMIT	A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit.
T.UNAUTH	An unauthorized user may bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize gain access to the TOE's management functions, TSF Data, or IT network device data.
T.UNDETECT	An actively monitored device may transition from a known good state into a compromised/non compliant state. An authorized TOE administrator may not be aware that the device has now become non compliant, and therefore their ability is limited to identify and take action against a possible security problem in the TOE environment.

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. Table 5 below lists the OSPs that are presumed to

[8] IT – Information Technology

be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 5 Organizational Security Policies

Name	Description
P.BANNER	The TOE server shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

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. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.LOCATE	The TOE and the connections between the TOE and TOE environmental components, including the MySQL DB Server, SMTP Server, SNMP Server and all ports over the network, are located within a controlled access facility on a secured network.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMPS	The TOE environment will provide the TOE with the necessary reliable timestamps.

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 listed in Table 7 below.

Table 7 Security Objectives for the TOE

Name	Description
O.ATTRIB	The TOE will be capable of maintaining user security attributes.
O.AUDIT	The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review the audit trail.
O.AUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.AUTO	The TOE must provide the ability to automatically discover devices in the network, download a configuration snapshot, check the devices for non-compliance, automatically invoke actions if a device is found to be out of compliance, and restrict the viewing of non compliant devices to only explicitly authorized users.
O.BANNER	The TOE client will display an advisory warning regarding use of the TOE.
O.CRYPTO	The TOE must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.
O.MANAGE	The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the TOE as discussed in FMT_SMF.1, and restrict these functions and facilities from unauthorized use.
O.SECURE	The TOE shall securely transfer data with remote authentication servers, remote users and administrators, and monitored devices when sent using SSH and TLS.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 IT Security Objectives

Name	Description
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.
OE.TIMESTAMPS	The operational environment will provide reliable time stamps.
OE.SECURE_NETWORK	The Local Area Network that the TOE and TOE environmental components are connected to is a secure network that provides protection against outside attacks.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that 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 9 Non-IT Security Objectives

Name	Description
NOE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
NOE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE

Table 10 Extended TOE Security Functional Requirements

Name	Description
EXT_NAS_DCD.1	Device and Configuration Discovery
EXT_NAS_PCM.1	Policy Compliance
EXT_NAS_NCE.1	Non-Compliance Events
EXT_NAS_RDR.1	Restricted Data Review

5.1.1 Class NAS: Network Automation Support

The Network Automation Support functions involve discovering network devices and obtaining a ‘configuration snapshot’ of the device’s current configuration. The configuration snapshot is then evaluated against existing Policies and Rules for compliance. Any devices found to be out of compliance will trigger non-compliance events, which in turn will trigger administrator defined actions such as running a task (snapshot or diagnostic), sending an email notification, sending an SNMP trap, or sending a syslog message. Additionally, the ability to review discovered devices and their corresponding configuration snapshots is restricted to only operators with the appropriate permissions. The EXT_NAS: Network Automation Support functionality class was modeled after the CC FAU: Security audit class. The extended family EXT_NAS_DCD: Device and Configuration Discovery and related components were modeled after the family FAU_GEN: Audit Data Generation. The extended family and related components for EXT_NAS_PCM: Policy Compliance were modeled after the family FAU_SAA: Security Audit Analysis. The extended family EXT_NAS_NCE: Non-Compliance Events and related components were modeled after the CC family FAU_ARP: Security Alarms. The extended family EXT_NAS_RDR: Restricted Data Review and related components were modeled after the CC family FAU_SAR: Security Audit Review.

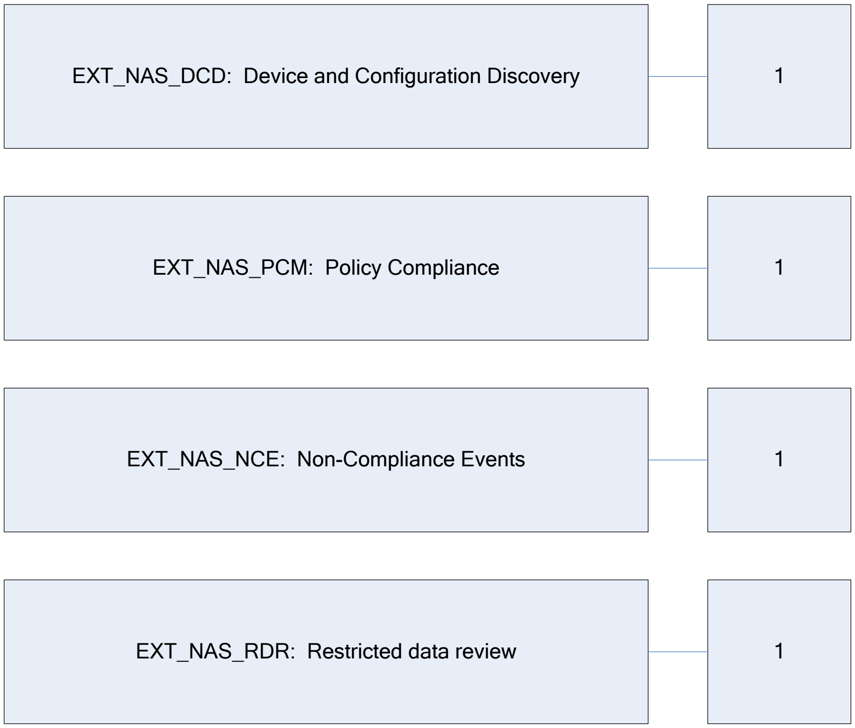
EXT_NAS_DCD: Device and Configuration Discovery
1
EXT_NAS_PCM: Policy Compliance
1
EXT_NAS_NCE: Non-Compliance Events
1
EXT_NAS_RDR: Restricted data review
1

Figure 4 EXT_NAS: Network Automation Support Class Decomposition

5.1.1.1 Device and Configuration Discovery (EXT_NAS_DCD)

Family Behaviour

This family defines the requirements for recording the occurrence of events that take place under TSF control. This family identifies the level of monitored resource data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of event-related information that should be provided within various record types.

Component Leveling

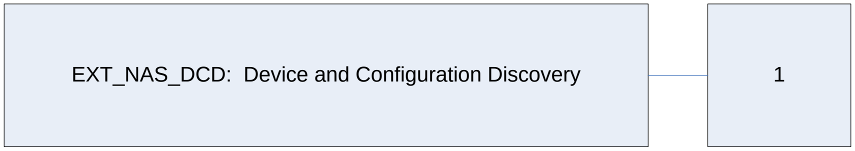

Figure 5 EXT_NAS_DSD Device and Configuration Discovery Family Decomposition

EXT_NAS_DCD.1: Monitored resource data collection, defines the level of events and specifies the list of data that shall be captured in each event recorded.

Management: EXT_NAS_DCD.1

- There are no auditable events foreseen.

Audit: EXT_NAS_DCD.1

- There are no auditable events foreseen.

EXT_NAS_DCD.1	**Device and Configuration Discovery**
Hierarchical to:	**No other components**
Dependencies:	**FPT_STM.1 Reliable time stamps**

EXT_NAS_DCD.1.1

The TSF shall be able to perform discovery of and obtain configuration snapshots of network devices at [assignment: *specifically defined events*.]

EXT_NAS_DCD.1.2

At a minimum, the TSF shall collect and record the following information:

a) Current device configuration, date and time of snapshot, device model, type of device, OS version, and the IP address of the device.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other configuration snapshot relevant information*]

5.1.1.2 Non-Compliance Events (EXT_NAS_NCE)

Family Behaviour

This family defines the requirements for the response to be taken in case of a detected policy compliance violation of a monitored resource.

Component Leveling

Figure 6 EXT_NAS_NCE Non-Compliance Events Family Decomposition

EXT_NAS_NCE.1 Non-compliance events, the TSF shall take actions when a device is found to be out of compliance with one or more Policies.

Management: EXT_NAS_NCE.1

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

- Management (addition, removal, or modification) of the task to be invoked upon a non-compliance event.

Audit: EXT_NAS_NCE.1

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

- Minimal: The non-compliance event.

EXT_NAS_NCE.1	**Non-compliance events**
Hierarchical to:	**No other components**
Dependencies:	**EXT_NAS_DCD.1**

EXT_NAS_NCE.1.1

The TSF shall take [*assignment: list of actions*] upon the trigger of a non-compliance event.

5.1.1.3 Policy Compliance (EXT_NAS_PCM)

Family Behaviour

This family defines requirements for automated means that check the discovered devices and configuration snapshots against the administrator defined Policies. The actions to be taken based on the detection can be specified using the EXT_NAS_NCE: Non-Compliance Event family.

Component Leveling

Figure 7 EXT_NAS_PCM Policy Compliance Family Decomposition

EXT_NAS_PCM.1 Policy Compliance, specifies that the TOE will perform compliance checks on the collected configuration snapshot data. The TSF shall be able to detect the occurrence of non-compliance in a device and generate an event that represents a potential threat in the TOE environment.

Management: EXT_NAS_PCM.1

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

- Management of Policies and Rules (addition, modification, removal, deletion).

Audit: EXT_NAS_PCM.1

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

- Minimal: maintenance (addition, modification, deletion, removal) of Policies.

EXT_NAS_PCM.1 Policy Compliance

Hierarchical to: No other components

Dependencies: EXT_NAS_DCD.1

EXT_NAS_PCM.1.1

The TSF shall be able to apply a set of Policies on the configuration snapshots of the devices. If the Policies are violated, the TSF shall generate a non-compliance event that represents potential problem scenarios in the TOE environment.

EXT_NAS_PCM.1.2

The TSF shall be able to enforce the Rules specified in each Policy against the configuration snapshot for each device.

5.1.1.4 Restricted Data Review (EXT_NAS_RDR)

Family Behaviour

This family defines the requirements for the monitoring tools that should be available to authorized users to assist in the review of compliance violation data.

Component Leveling

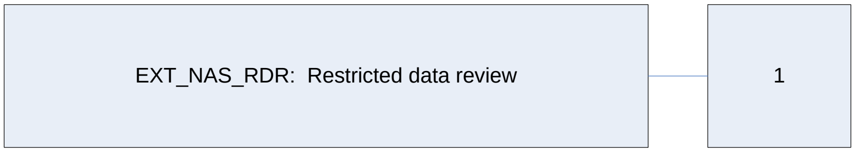

Figure 8 EXT_NAS_RDR Restricted Data Review family decomposition

EXT_NAS_RDR.1 Restricted data review, the TSF shall ensure that no other users other than those identified can read the compliance violation data.

Management: EXT_NAS_RDR.1
The following actions could be considered for the management functions in FMT:

- Maintenance (deletion, modification, addition) of the group of users with read access right to the compliance violation data.

Audit: EXT_NAS_RDR.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: all attempts to view compliance data.

EXT_NAS_RDR.1 Restricted data review
Hierarchical to: No other components
Dependencies: No dependencies

EXT_NAS_RDR.1.1

The TSF shall provide [assignment: *authorized users*] with the capability to read compliance violation data for the devices.

EXT_NAS_RDR.1.2

The TSF shall provide the compliance violation data in a manner suitable for the user to interpret the information.

EXT_NAS_RDR.1.3

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

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.

6.1 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 Part 2 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 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 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 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		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	Timing of authentication				
FIA_UAU.5	Multiple authentication mechanism		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	Timing of Identification		✓		
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		

Name	Description	S	A	R	I
FMT_SMR.1	Security roles		✓		
FTA_TAB.1	Default TOE access banners				
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted Path	✓	✓		
EXT_NAS_DCD.1	Device and configuration discovery		✓		
EXT_NAS_PCM.1	Policy compliance				
EXT_NAS_NCE.1	Non-compliance events		✓		
EXT_NAS_RDR.1	Restricted data review		✓		

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.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*login and logout events, Policy maintenance (creation, modification, and activation actions), and user account management*].

FAU_GEN.1.2

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

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

Application Note: While the TOE does not explicitly generate an event for the start-up and shutdown of the audit function, the TOE does generate an audit event for startup and shutdown of the system. Because the start-up and shutdown events of the system are tied to the startup and shutdown events of the audit functionality, these records can be considered to provide equivalent notice.

FAU_GEN.2 User Identity Association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FPT_STM.1 Reliable time stamps

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.

FAU_SAR.1 Audit Review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*Administrators, Power Users, Full Access Users, and Limited Access Users*] with the capability to read [*all 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.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm – see* Table 12 *below*] and specified cryptographic key sizes [*cryptographic key sizes – see* Table 12 *below*] that meet the following: [*list of standards* – see *Table 12* below].

Table 12 Cryptographic Key Generation Standards

Key Generation Algorithm	Key Sizes Tested	Standards (Certificate #)
HMAC[9] DRBG	HMAC-SHA[10]-1, 224, 256, 384, 512	NIST SP[11] 800-90A (CAVP cert #273)
RSA	2048	ANSI[12] X9.31 PKCS[13] #1 V1.5, RSASSA-PSS[14] (CAVP cert #1154)
DSA[15]	2048	FIPS 186-4, CAVP cert #701
DH[16]	DH & MQV[17] with public keys ≥ 2048 bits and private keys ≥ 224 bits	SP 800-56A, Allowed
ECC[18] (for use in ECDH[19] and ECDSA[20])	Curves: P-224 P-256 P-384 P-521 K-224 K-256 K-384 K-521 B-224 B-256 B-384 B-521	SP 800-56A, ECDH – Allowed FIPS 186-3, ECDSA – CAVP cert #357

[9] HMAC – Hash-Based Message Authentication Code
[10] SHA – Secure Hash Algorithm
[11] SP – Special Publication
[12] ANSI – American National Standards Institute
[13] PKCS – Public Key Cryptography Standard
[14] RSASSA-PSS – RSA Signature Scheme with Appendix – Probabilistic Signature Scheme
[15] DSA – Digital Signature Algorithm
[16] DH – Diffie Hellman
[17] MQV – Menezes-Qu-Vanstone
[18] ECC – Elliptic Curve Cryptography
[19] ECDH – Elliptical Curve Diffie-Hellman
[20] ECDSA - Elliptical Curve Digital Signature Algorithm

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations – see Table 13 below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm* – see *Table 13* below] and cryptographic key sizes [*cryptographic key sizes* – see *Table 13* below] that meet the following: [*list of standards* – see *Table 13* below].

Table 13 Cryptographic Operation

Algorithm	Standard and Cert #
Symmetric Key Algorithms	
AES: ECB[21], CBC[22], OFB[23], CFB[24] CTR[25], CCM[26], GCM[27], XTS[28,29,30]-128 bit mode for 128-, 192-, and 256-bit key sizes	FIPS 197, CAVP cert #2249
Triple-DES[31]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	FIPS 46-3, CAVP cert #1408
Digital Signature Algorithms	
RSA X9.31, PKCS#1 V.1.5, RSASSA-PSS Signature generation; Signature verification – 1024- (signature verification only), 2048-, 3072-bit	ANSI X9.31 (FIPS 186-4), CAVP cert #1154
DSA Signature generation; Signature verification – 1024- (Signature verification only), 2048-, 3072-bit	FIPS 186-4, CAVP cert #701
ECDSA Signature generation for all NSA[32] Suite B P, K, and B Curves, Signature Verification for all P, K, and B curves.	FIPS 186-4, CAVP cert #357
Key Derivation	
KDFTLS10, KDFTLS12 with SHA-256, SHA-384, SHA-512	SP 800-135, CAVP cert #39

[21] ECB – Electronic Codebook
[22] CBC – Cipher Block Chaining
[23] OFB – Output Feedback
[24] CFB – Cipher Feedback
[25] CTR – Counter Mode
[26] CCM – Counter with CBC-MAC
[27] GCM – Galois Counter Mode
[28] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[29] XEX – XOR-Encrypt-XOR
[30] XOR – Exclusive Or
[31] DES – Data Encryption Standard
[32] NSA – National Security Agency

Algorithm	Standard and Cert #
Hashing Functions Asymmetric Key Algorithms	
SHA-1, 224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256	FIPS 180-2, CAVP cert #1938
Message Authentication Code (MAC) Functions	
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 198, CAVP cert #1378

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password or X.509 certificate, email address, account status, and role*].

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of identification
Dependencies: FIA_UID.1 Timing of identification
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.

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_UAU.5.1

The TSF shall provide [*the following authentication mechanisms:*

- *password-based*
- *CAC/PIV certificate-based*

] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*internally stored identity and credential information*].

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1

The TSF shall provide only [*obscured feedback in the form of bullets for the web GUI and no feedback for the CLI/API*] to the user while authentication is in progress.

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

FIA_UID.2.1

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

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1

The TSF shall restrict the ability to [modify the behaviour of] the functions [*identification and authentication method, TOE access banner content, TOE operator session timeouts*] to [*Administrators and Power Users*].

FMT_MTD.1 Management of TSF Data
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [modify] the [*the TSF data in the 'TSF Data' column of Table 14*] to [*the roles listed in the 'Role' column of Table 14*].

Table 14 TSF Data Access by Role

Role	TSF Data Access
Administrator	• Session timeouts • Authentication method used • Configure LDAP settings • Device creation, modification, import • View devices • Policy/Rule creation/modification/deletion • View and run policy compliance. • Event notification and response rules (Policy non compliance events) • Task creation/modification/execution • Create/modify/delete Users • View logged on users • View drivers • General configuration data (IP Address, port configuration, database configuration) • View audit log • Enable/disable the audit feature

Role	TSF Data Access
Power User	• Session timeouts • Authentication method used • Device creation, modification, import • View devices • Policy/Rule creation/modification • View and run policy compliance. • Task creation/modification/execution • View Users, • View logged on users • Create and view devices and device templates. • Edit self • View drivers • General configuration data (IP Address, port configuration, database configuration) • View audit log • Enable/disable the audit feature
Full Access User	• View logged on users • View users • Create and view devices and device templates. • Change own password. • View and Run policy compliance. • Execute tasks • View audit log
Limited Access User	• View logged on users • view users • View devices and device templates • Change own password • Run policy compliance • Execute tasks • View audit log

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of user accounts, view the audit log, session timeout configuration, Policies and Rules, TOE access banner, FIPS mode]*.

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*Administrator, Power User, Full Access User, and Limited Access User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5 Class FTA: TOE Access

FTA_TAB.1 TOE access banners
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_TAB.1.1

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

6.2.6 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*device monitoring and discovery, remote authentication requests*].

FTP_TRP.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies

FTP_TRP.1.1

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

FTP_TRP.1.2

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

*The TSF shall require the use of the trusted path for [*initial user authentication [*no other services*].

6.2.7 Class NAS: Network Automation Support

EXT_NAS_DCD.1 Device and Configuration Discovery
Hierarchical to: No other components
EXT_NAS_DCD.1.1

The TSF shall be able to perform discovery of and obtain configuration snapshots of network devices at [
Discovery:

- *import,*
- *scheduled task,*
- *manual addition*

Obtain configuration snapshots:

- *at device discovery,*
- *scheduled task,*
- *ad-hoc task invocation,*
- *automated based on the occurrence of a non-compliance event,*
- *change detection via syslog,*
- *after a device is accessed by the TOE]*

EXT_NAS_DCD.1.2

At a minimum, the TSF shall collect and record the following information:

a) Current device configuration, date and time of snapshot, device model, type of device, OS version, and the IP address of the device.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no *other information*]

EXT_NAS_NCE.1 Non-compliance events
Hierarchical to: No other components
Dependencies: EXT_NAS_DCD.1
EXT_NAS_NCE.1.1

The TSF shall take [*one of the following actions:*

- *Running tasks, such as snapshots or diagnostics*
- *Sending Email notification*
- *Sending Email digests*
- *Sending SNMPv1/v2 traps*
- *Sending Syslog messages*

] upon the trigger of a non-compliance event.

EXT_NAS_PCM.1 Policy Compliance
Hierarchical to: No other components
Dependencies: EXT_NAS_DCD.1
EXT_NAS_PCM.1.1

The TSF shall be able to apply a set of Policies on the configuration snapshots of the devices. If the Policies are violated, the TSF shall generate a non-compliance event that represents potential problem scenarios in the TOE environment.

EXT_NAS_PCM.1.2

The TSF shall be able to enforce the Rules specified in each Policy against the configuration snapshot for each device.

EXT_NAS_RDR.1 Restricted data review
Hierarchical to: No other components
Dependencies: No dependencies
EXT_NAS_RDR.1.1

The TSF shall provide [*Administrators, Power Users, and Full Access Users*] with the capability to read compliance violation data for the devices.

EXT_NAS_RDR.1.2

The TSF shall provide the compliance violation data in a manner suitable for the user to interpret the information.

EXT_NAS_RDR.1.3

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

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 EAL 2 augmented with ALC_FLR.2. Table 15 Assurance Requirements summarizes the requirements.

Table 15 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
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 ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Complete functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Focused 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 16 lists the security functions and their associated SFRs.

Table 16 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
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	Timing of Identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_TAB.1	Default TOE access banners
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path
Network Automation Support	EXT_NAS_DCD.1	Device and configuration discovery
	EXT_NAS_NCE.1	Non-compliance events
	EXT_NAS_PCM.1	Policy compliance
	EXT_NAS_RDR.1	Restricted data review

7.1.1 Security Audit

The TOE is capable of auditing a variety of events, including startup and shutdown of the system, login and logout events, Policy creation, management, and activation actions, and user account management. For each action that is invoked by a user, the TOE will associate his or her username with the generated audit log. The TOE generates an audit event for startup and shutdown of the system, which is tied to the startup and shutdown of the audit functionality. Since the system starts up and shuts down at the same time as the audit function, these records can be considered to provide equivalent notice.

The Audit Log entries contain at a minimum the following fields:

- Date and time of the event
- Type of event
- Identity of the subject
- Outcome of the event

The TOE does not audit any additional fields in addition to these fields. Administrators, Power Users, Full Access Users, and Limited Access Users accessing the TOE's web GUI have the ability to review the audit logs by navigating to the 'Server Page' and clicking the 'View Audit Logs' button or by clicking the 'NA Events' button.

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

7.1.2 Cryptographic Support

Cryptographic operations necessary to support SSH, TLS, HTTPS, encryption, decryption, and key generation are provided by the RSA B-SAFE Crypto-J JSAFE and JCE Cryptographic Library v6.1 (CMVP[33] validated cryptographic module (Certificate #2057). For a complete list of the cryptographic algorithms, modes, and key sizes, please see Table 13 above. The TOE uses SSH and HTTPS to protect administrative communications. SSH provides a trusted path for remote TOE administrators accessing the TOE's CLI/API. HTTPS (via TLS) provides a trusted path for remote TOE administrators accessing the web GUI. Additionally, TLS is also used to protect communications with a remote authentication server. For both TLS and SSH session keys, the TOE uses symmetric AES and Triple-DES keys to encrypt and decrypt data.

Keys are generated via the use of the HMAC_DRBG to provide random keying material. The TOE implements DH, DSA, RSA, and ECC (ECDSA and ECDH) key-pair establishment methods.

The TOE's cryptographic module is also used when the TOE has been configured to support CAC/PIV authentication. Under these circumstances, the TOE will validate a TOE operator's certificate against a chosen certificate authority (CA) list. CAC authentication will take place against a Certificate realm, and TOE administrator authorization takes place against a local or configured LDAP realm. The authentication procedure leverages 3rd party middleware in order to facilitate two factor authentication of the operator to their CAC using a Personal Identification Number (PIN). This process enables the TOE to retrieve the X.509 certificate from the microprocessor smart card and authenticate the certificate against the CA list using CRLs followed by online certificate status protocol (OCSP) to check for certificate revocation. The operator is granted access to the TOE if the user principal name (UPN) or common name (CN) is found in the LDAP directory.

The TOE provides zeroization techniques that meets the FIPS 140-2 zeroization requirement for all plaintext secret and private keys. TLS and SSH session keys reside in volatile memory only and are never stored persistently. To zeroize the ephemeral TLS and SSH session keys, the TOE must be restarted by a TOE administrator. Persistent keys are zeroized when the FIPS Approved mode is disabled.

[33] CMVP – Cryptographic Module Validation Program

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.3 Identification and Authentication

The TOE does not allow any unauthorized access to its internal functionality and enforces identification and authentication for all management requests received on the CLI/API and web GUI. For all TOE operators, the TOE maintains username, password, email address, account status, and role attributes. All attributes can be modified by the Administrator over the CLI/API and web GUI. The account status attribute can be configured to be 'Enabled' (the default) or 'Disabled,' allowing the account to remain within the TOE but disallowing its use.

Operators can authenticate to the TOE using a password-based authentication mechanism. During password entry, the TOE obscures feedback in the form of bullets ('•') over the web GUI and provides no feedback over the CLI/API.

Operators can also authenticate to the TOE using a certificate-based authentication mechanism. For certificate based authentication, the TOE is configured to support PKI[34] user authentication and accepts X.509 formatted certificates. Certificates may be installed in the browser or installed on a separate external device, such as a Common Access Card (CAC). In order for an operator to be granted access to the TOE, the X.509 certificate's 'Common name' must match the username of an existing TOE account. If the TOE cannot reach the external authentication server, the TOE supports local authentication failover, allowing TOE operators to access the TOE even if there is a problem with the external authentication server.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2.

7.1.4 Security Management

The TOE provides management facilities to TOE operators for TSF data and security functions. TSF data includes general TOE configuration data, database settings, operator accounts and authentication, the TOE access banner, Policy and Rule creation, and auditing. The TOE maintains roles that provide varying levels of privileges that determine what TSF data an authenticated operator can access. Table 14 above lists the roles and TSF data access supported by the TOE.

TOE operator accounts can be managed via the web GUI under the **Admin -> Users** ('All Users' page) menu option and via the CLI/API using the '`mod user`' command. Only the Administrator role can use either of these facilities to modify operator attributes, (username, password, email address, role), enable or disable an operator's account, and create and delete operators. Each TOE operator has the ability to change their own password via the web GUI under the **MySettings -> Change Password** menu option**.**

The TOE provides the Administrator role the capability to manage the authentication mechanisms used by the TOE. The Administrator may configure the TOE to use PKI and support certificate based authentication under the **Admin -> Administrative Settings -> User Authentication** menu option. The Administrator has the ability to configure the specific field within the certificate that should match the username stored within the TOE. The Administrator can also configure the CRL and OSCP parameters to ensure that invalid or revoked certificates are not accepted.

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

[34] PKI – Public Key Infrastructure

7.1.5 TOE Access

At the login screen, operators are shown a TOE access banner warning against unauthorized use of the TOE. The message is shown to users of both the web GUI and the CLI.

TOE Security Functional Requirements Satisfied: FTA_TAB.1.

7.1.6 Trusted Path/Channels

The TOE provides a trusted path between the TOE management interfaces and remote TOE operators. These interfaces are the CLI/API over SSH and the web GUI over HTTPS (via TLS). The protocols and the cryptography implemented by the TOE provide adequate defense against unauthorized disclosure and provide for the detection of modification of TSF data while it is in transit.

Additionally, the TOE provides a trusted channel between the TOE and trusted IT entities. Trusted IT entities consist of the authentication server and the remotely monitored network devices. The trusted channel to secure the communication between the TOE and the authentication server is established using TLS to prevent unauthorized disclosure and detect modification of authentication data. A trusted channel is initiated by the TOE to the managed devices using SSH to secure the communications between the monitored network devices and the TOE. This channel is used to prevent unauthorized disclosure during device monitoring and retrieval of configuration data.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1.

7.1.7 Network Automation Support

The TOE provides the ability to automatically discover and monitor devices within a local or remote network for compliance against Policies. Device discovery can occur through Administrator import, according to a scheduled task, or through manual addition of the device to the TOE. Device import can be accomplished the Administrator using the **Admin -> Administrative Settings -> Server Page -> New Task/Template – Import Devices'** page**.** The TOE will accept a comma separated value file containing the device data to import and add to the database. By scheduling a task, the Administrator can configure the TOE to detect network devices to be imported into the TOE. To create a discovery task, the Administrator navigates to the **Taskas -> Detect Network Devices.'** The discovery task will require the range of IP addresses to include in device discovery, an optional range for IP address exclusion, the maximum number of devices to discover, and a schedule of when to run, the number of times to run, the interval between each run, how many times to retry if there is a failure, and how long to wait between failure retries. Administrators may manually add new devices to be monitored by NA navigating to the **Devices -> New Device** page. To manually add devices, the Administrator will require the IP address, appropriate driver, the authentication information required to access the device, and the communication protocol.

Configuration snapshots are obtained when the following events occur: discovery of a device, scheduled or manually invoked task, detection of a Policy violation,detection of a configuration change, or accessing the device from the TOE. The TOE will then store the snapshot and then compare it against all applicable Policies. For device discovery, part of the discovery operation includes obtaining the configuration snapshot for the device and storing that in the database. The Administrator can create a 'Take Snapshot' task that will take a snapshot for the specified device. Once the 'Take Snapshot' task has been scheduled, the Administrator has the option to view all tasks and invoke the 'Run Now' action rather than waiting for the original task schedule. When a Policy is violated and a non-compliance event is generated, the TOE can be configured to run a 'Take Snapshot' task.

The TOE can obtain configuration snapshots using change detection via Syslog messages. To utilize the Syslog messages as a configuration change source, the TOE configures itself as one of the monitored device's Syslog destinations during the device discovery event, allowing it to receive all subsequent Syslog messages.

The TOE is able to then detect patterns in the Syslog messages that are used to identify potential configuration changes. Once the TOE verifies that a change occurred, it will obtain a new configuration snapshot.

Using ‘Post Task Snapshots,’ the TOE can also be configured to obtain snapshots after the TOE has accessed a device to perform any of the following actions: a configuration deployment action, run a command script on the device, after a diagnostic run, or after device access control list modification.

The stored snapshots are used to maintain a historical record of all configuration changes specific to that device that allow for review, corporate policy compliance, and future trouble shooting by TOE administrators.

During Policy application, each Rule in the Policy is enforced against a device’s configuration snapshot. If a Rule is not matched, and therefore a device is found to be out of compliance, the TOE will generate a non-compliance event. Based on the preconfigured behavior for the non-compliance event, the TOE will automatically perform one of several actions to notify the administrator that there is a potential threat in the TOE environment. The TOE is capable of running additional tasks (snapshots, diagnostics), sending Email notifications, sending Email digests, sending SNMPv1 or SNMPv2 traps, and sending Syslog messages. With this functionality, the TOE can provide a high level of assurance that if a potential threat is detected, it will not go unnoticed by the administrator. The Policy and Rule broken that triggered the compliance violation are available to all roles within the TOE except the Limited Access User role. The Administrator role do have the ability to explicitly manage the Limited Access User role and therefore give permission for this role to view the compliance violation data.

Application Note: All syslog messages are sent from the managed devices to the TOE over ports 514 and 9901. Configuration snapshots can be sent from the managed devices to the TOE over FTP (port 21) or TFTP (port 69). All ports are open upon installation of the TOE. The ports are only accessible over the interal secure network and are located on the NA server, which is maintained in a secure access facility.

TOE Security Functional Requirements Satisfied: EXT_NAS_DCD.1, EXT_NAS_NCE.1, EXT_NAS_PCM.1, EXT_NAS_RDR.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

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, policies, and assumptions to the security objectives are 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 17 below provides a mapping of the objects to the threats they counter.

Table 17 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.NOAUDIT Threat agents may perform security-relevant operations on the TOE without being held accountable for it.	O.AUDIT The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review the audit trail.	O.AUDIT mitigates this threat by ensuring that security relevant events of the TOE are preserved through an audit trail.
T.TRANSMIT A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit.	O.CRYPTO The TOE must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.	O.CRYPTO mitigates this threat by ensuring that the cryptographic keys are managed securely conformant to the FIPS 140-2 standards.
	O.SECURE The TOE shall securely transfer data with remote authentication servers, remote users and administrators, and monitored devices when sent using SSH and TLS.	O.SECURE mitigates this threat by providing trusted mechanisms to protect the TOE data that is transferred between the specified trusted IT entities and remote users and administrators.
T.UNAUTH An unauthorized user may bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly gain access to the TOE's management functions, TSF Data, or IT network device data.	O.ATTRIB The TOE will be capable of maintaining user security attributes.	O.ATTRIBUTES mitigates this threat by allowing only users with valid credentials to access the TOE.
	O.AUDIT The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide	O.AUDIT mitigates this threat by ensuring that unauthorized attempts to access the TOE or TSF-mediated resources are recorded.

Threats	Objectives	Rationale
	authorized administrators with the ability to review the audit trail.	
	O.AUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	O.AUTH mitigates this threat by ensuring that users are identified and authenticated prior to gaining access to TOE functions.
	O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the TOE as discussed in FMT_SMF.1, and restrict these functions and facilities from unauthorized use.	O.MANAGE mitigates this threat by ensuring that access to TOE security functions is limited to only authorized users.
T.UNDETECT An actively monitored device may transition from a known good state into a compromised/non compliant state. An authorized TOE administrator may not be aware that the device has now become non compliant, and therefore their ability is limited to identify and take action against a possible security problem in the TOE environment..	O.AUTO The TOE must provide the ability to automatically discover devices in the network, download a configuration snapshot, check the devices for non-compliance, automatically invoke actions if a device is found to be out of compliance, and restrict the viewing of non compliance event details to only explicitly authorized users.	O.AUTO mitigates this threat by ensuring that the TOE will discover and monitor devices in the network for compliance through Policy checks. If a Policy check fails, the TOE will automatically generate an event and invoke a TOE administrator defined action to ensure that no potential security violations go undetected.

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 18 below gives a mapping of policies and the objectives that support them.

Table 18 Policies: Objectives Mapping

Policies	Objectives	Rationale
P.BANNER The TOE server shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.BANNER The TOE server will display an advisory warning regarding use of the TOE.	O.BANNER ensures that an advisory warning is displayed regarding the use of the TOE.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 19 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 19 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM satisfies this assumption by ensuring that the TOE hardware meets minimum requirements and the OS supports all the TOE functions.
A.LOCATE The TOE and the connections between the TOE and TOE environmental components, including the MySQL DB Server, SMTP Server, SNMP Server and all ports over the network, are located within a controlled access facility on a secured network.	OE.SECURE_NETWORK The Local Area Network that the TOE and TOE environmental components are connected to is a secure network that provides protection against outside attacks.	OE.SECURE_NETWORK Upholds this assumption by ensuring that the TOE and TOE environmental components connected to the Local Area Network are protected from outside attacks.
	NOE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.	NOE.PHYSICAL satisfies the assumption by ensuring that the TOE environment provides protection from unauthorized modification.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.	OE.NETWORK The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETWORK upholds this assumption by ensuring that the environment provides the TOE with the appropriate network configuration.
A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NO_EVIL Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	NOE.NO_EVIL satisfies this assumption by ensuring that administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	OE.PROTECT satisfies the assumption by ensuring that the TOE environment provides protection from unauthorized modification.
A.TIMESTAMPS The TOE environment will provide the TOE with the necessary reliable timestamps.	OE.TIMESTAMPS The operational environment will provide reliable time stamps.	OE.TIME_STAMPS satisfies this assumption by stating that the environment will maintain reliable timestamps and those will be used by the TOE to stamp each audit record with a date and time.

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

A class of EXT_NAS requirements was created to specifically address the discovery of network devices, collection of configuration snapshots, and the policy compliance capabilities of the TOE. The CC FAU: Security Audit class was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature device discovery and monitoring and provide for requirements for alerting when violations are detected. These requirement's dependencies have been noted in 5.1.1. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended Security Assurance Requirements have been defined for this ST.

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 20 below shows a mapping of the objectives and the SFRs that support them.

Table 20 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ATTRIB The TOE will be capable of maintaining user security attributes.	FIA_ATD.1 User attribute definition	The TOE is required to maintain a defined list of security attributes belonging to individual users.
O.AUDIT The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit data generation	The TOE is required to record audit events as defined in this SFR. This requirement ensures that the administrator has the ability to audit security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event.

Objective	Requirements Addressing the Objective	Rationale
	FAU_GEN.2 User identity association	The TOE is required to associate auditable events with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The TOE is required to present the audit logs to the authorized administrator in a suitable manner for interpretation.
O.AUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	FIA_UAU.2 Timing of authentication	The TOE is required to authenticate users requesting access to TSF data before any actions may be taken on the behalf of that user.
	FIA_UAU.5 Multiple authentication mechanism	The TOE is required to authenticate users requesting access to the TSF before any actions may be taken on the behalf of that user. There are multiple authentication mechanisms supported as specified in this SFR.
	FIA_UAU.7 Protected authentication feedback	The TOE is required to obscure the feedback of passwords entered by users of the TOE during authentication.
	FIA_UID.2 Timing of Identification	The TOE is required to identify all users requesting access to the TSF before any actions may be taken on the behalf of that user.
O.AUTO The TOE must provide the ability to automatically discover devices in the network, download a configuration snapshot, check the devices for non-compliance, automatically invoke actions if a device is found to be out of compliance, and restrict the viewing of non compliant devices to only explicitly authorized users.	EXT_NAS_DCD.1 Device and configuration discovery	The TOE is required to provide the ability to automatically discover devices in the network and download a configuration snapshot.
	EXT_NAS_NCE.1 Non-compliance events	Upon the generation of a non-compliance event the TOE is required to automatically invoke a TOE operator defined action to raise awareness of the non-compliance event.
	EXT_NAS_PCM.1 Policy compliance	The TOE is required to check the devices for non-compliance based on one or more TOE operator defined compliance Policies. If a device is found to be out of compliance, the TOE will generate a non-compliance event.

Objective	Requirements Addressing the Objective	Rationale
	EXT_NAS_RDR.1 Restricted data review	The TOE is required to restrict the viewing of device non-compliance data to only explicitly authorized users.
O.BANNER The TOE client will display an advisory warning regarding use of the TOE.	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that a banner is displayed to users prior to identification and authentication.
O.CRYPTO The TOE must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.	FCS_CKM.1 Cryptographic key generation	The TOE is required to generate cryptographic keys in accordance with FIPS 140-2 approved techniques.
	FCS_CKM.4 Cryptographic key destruction	The TOE is required to destroy cryptographic keys according to FIPS 140-2 zeroization requirements.
	FCS_COP.1 Cryptographic operation	The TOE is required to perform cryptographic operations according to the FIPS 140-2 approved algorithms and key sizes.
O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the TOE as discussed in FMT_SMF.1, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1 Management of security functions behavior	The TOE is required to restrict administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The TOE is required to restrict access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The TOE is required to include administrative functions to facilitate the management of security attributes.
	FMT_SMR.1 Security roles	The TOE is required to associate users with roles to provide access to TSF management functions and data.
O.SECURE The TOE shall securely transfer data with remote authentication servers, remote users and administrators, and monitored devices when sent using SSH and TLS.	FTP_ITC.1 Inter-TSF trusted channel	The TOE is required to provide a trusted communication path between itself and an external trusted IT entity which provides for the protection of the data from disclosure and modification when in transit.
	FTP_TRP.1 Trusted Path	The TOE is required to provide a trusted communication path

Objective	Requirements Addressing the Objective	Rationale
		between itself and remote users which provides for the protection of the data from disclosure and modification when in transit.

8.5.2 Security Assurance Requirements Rationale

EAL 2 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 System may monitor a hostile environment, it 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 EAL 2, 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 flaw reporting procedures.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 21 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 21 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1		FPT_STM.1 is not included because time stamps are provided by the TOE environment. An environmental objective states that the TOE will receive reliable time stamps.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UAU.5	None	N/A	
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency.
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FTA_TAB.1	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	
EXT_NAS_DCD.1	FPT_STM.1		FPT_STM.1 is not included because time stamps are provided by the TOE environment. An environmental objective states that the TOE will receive reliable time stamps.
EXT_NAS_PCM.1	EXT_NAS_DCD.1	✓	
EXT_NAS_NCE.1	EXT_NAS_DCD.1	✓	
EXT_NAS_RDR.1	None	N/A	

9 Acronyms and Terms

Table 22 and Table 23 below define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 22 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certificate Authority
CAC	Common Access Card
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter Mode with CBC-MAC
CFB	Cipher Feedback
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CN	Common Name
CTR	Counter Mode
DB	Database
DES	Data Encryption Standard
DH	Diffie Hellman
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EJB3	Enterprise JavaBeans 3.0
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash-Based Message Authentication Code

Acronym	Definition
HP	Hewlett-Packard
HS	Horizontal Scalability
HTTPS	Hypertext Transfer Protocol – Secure
IP	Internet Protocol
IT	Information Technology
JCE	Java Cryptography Extension
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NA	Network Automation
NIST	National Institute of Standards and Technology
NNMi	Network Node Manager i
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
OFB	Output Feedback
OS	Operating System
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RHEL	RedHat Enterprise Linux
RSA	Rivest, Shamir, and Adelman
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SHA	Secure Hash Algorithm
SFR	Security Functional Requirement
SP	Special Publication
ST	Security Target
SWIM	Software Image
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy

Acronym	Definition
UPN	User Principal Name
XEX	XOR-Encrypt-XOR
XOR	Exclusive Or
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Table 23 defines the terms used in this document.

Table 23 Terms

Term	Definition
Policy	A Policy is the parent element that is used to check the discovered devices for compliance. A Policy contains one or more Rules that are checked by the TOE. If any of the Rules in the Policy are broken, a non-compliance event is generated for the Policy.
Rule	Rules are the sub elements that comprise Policies. If any Rule is broken, the Policy will be flagged as a violation.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com