Hewlett Packard Enterprise Development LP

HPE Network Node Manager i Premium Edition 10.21.402

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.3

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

Email: info@hpe.com
www.hpe.com

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Email: info@corsec.com
www.corsec.com

Table of Contents

List 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 HPE Network Node Manager i Premium Edition 10.21.402 and will hereafter be referred to as the TOE throughout this document. The TOE is a highly-scalable, customizable network management solution that provides unified fault, availability, and performance monitoring for physical, virtual, hybrid, and cloud network environments.

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 functionality 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 (PP), 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 including both 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 Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs 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 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 HPE Network Node Manager i Premium Edition 10.21.402 Security Target
ST Version	Version 1.3
ST Author	Corsec Security, Inc.
ST Publication Date	03-28-2017
TOE Reference	HPE Network Node Manager i Premium Edition 10.21.402

FIPS[1] 140-2 Status	Level 1 Validated Cryptographic Modules: RSA[2] BSAFE Crypto-J JSAFE and JCE[3] Software Module Software Version 6.2 Cert. # 2468

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, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

1.3.1 HPE Network Node Manager i Premium Edition Overview

HPE Network Node Manager i (NNMi) Premium Edition software is a highly-scalable, customizable network management solution that provides unified fault, availability, and performance monitoring for physical, virtual, hybrid, and cloud network environments. HPE NNMi Premium Edition consists of HPE NNMi and several HPE NNMi Smart Plug-in (SPI) add-on modules (also referred to as NNM[4] iSPIs).

HPE NNMi is the core component of the network management solution. Its continuous spiral discovery[5] automatically keeps network topology data accurate and up-to-date. Network events are automatically correlated and analyzed for root cause to aid in identifying service-impacting events. These features help to reduce downtime and increase network service levels for a managed network. A single HPE NNMi server scales up to 30,000 network devices (nodes). Network and device load are minimized with unified polling of fault, availability, and performance data using SNMP[6], ICMP[7], HTTPS[8], and Network Configuration Protocol (NETCONF)/SSH[9] communication protocols.

HPE NNMi's web-based graphical user interface (GUI), called the NNMi Console, provides a centralized operations and management console with workflow-based navigation and filtering (e.g., by incidents, nodes, paths, and metrics) for fast access to information. User roles and administrator-configured user and security groups control access to node data and logically partition the network for security and multi-tenancy capability. There is also an SOA[10]-based web services API (referred to hereafter as the NNMi API) that allows for integrations with third-party software products as well as other HPE software products, like HPE Network Automation Software and HPE Operations Orchestration. An NNMi command-line interface (CLI) allows for automating administration activities.

NNM iSPIs extend HPE NNMi's capabilities to enable unified fault, availability, and performance management. They also add reports, including graphs and charts, to improve the efficiency and productivity of network operations teams. Two NNM iSPIs are included with HPE NNMi Premium Edition: HPE NNM iSPI Performance for

[1] FIPS – Federal Information Processing Standard
[2] RSA – Rivest, Shamir, Adelman
[3] JCE - Java Cryptography Extension
[4] NNM – Network Node Manager
[5] Spiral discovery is a Layer 2 and Layer 3 network discovery process that allows HPE NNMi to track dynamic changes in the network topology in near real time.
[6] SNMP – Simple Network Management Protocol
[7] ICMP – Internet Control Message Protocol
[8] HTTPS – Hypertext Transfer Protocol Secure. HTTPS is used for web services management of devices.
[9] SSH – Secure Shell
[10] SOA – Service Oriented Architecture

Metrics and HPE NNM iSPI Performance for Quality Assurance. The capabilities of these NNM iSPIs are described below:

- **HPE NNM iSPI Performance for Metrics –** This NNM iSPI gathers, processes, and aggregates performance related metrics and topology files from HPE NNMi to produce a variety of customizable performance reports. It installs a Network Performance Server (NPS) platform that includes an embedded Sybase IQ[11] database system and configurable reporting interface. It also provides seamless access to the reporting interface from the NNMi Console and allows operators to schedule reports for automatic generation and delivery. A web-based GUI called the NPS Console allows for direct access to reports from a Web browser. HPE NNM iSPI Performance for Metrics upholds the security configured through HPE NNMi to control access to the NPS Console and the information available through reports. It may be installed on the same or separate physical or virtual system as HPE NNMi.
- **HPE NNM iSPI Performance for Quality Assurance** – This NNM iSPI monitors quality of service levels across a managed network by automatically discovering pre-configured IP[12] SLA[13] probes (or tests) running on network devices (also referred to as QA[14] probes) and class-based quality of service (CBQoS) interfaces. It gathers performance metrics (e.g., round-trip delay, node reachability), determines performance inconsistencies, and generates incidents for violations of configured thresholds. It also displays the QA probe results and incidents seamlessly on the NNMi Console and provides a separate CLI (referred to hereafter as the QA SPI CLI) and web-based GUI called the QA SPI Configuration Console for administrators to configure HPE NNM iSPI Performance for Quality Assurance. HPE NNM iSPI Performance for Quality Assurance is installed on the same physical or virtual system as HPE NNMi.

HPE NNMi Premium Edition may be configured to run in a high availability (HA) cluster[15] to provide for uninterrupted service if a failure occurs. In this configuration, HPE NNMi, and optionally the NNM iSPIs, are installed on two physical or virtual systems: one is the primary, or Active server that is running the HPE NNMi Premium Edition processes, and the other is the secondary, or Standby server that is waiting for a failover event. HPE NNMi's embedded Postgres database, which stores configuration files and topology information, is maintained on a separate shared disk accessed only by the Active server. The Active and Standby servers continuously exchange "heartbeat" signals and initiate failover if there is loss of signal from the Active server, in which case the Standby system automatically becomes the new Active server. If the NNM iSPIs are configured for HA, HPE NNM iSPI Performance for Quality Assurance is installed on the same systems as HPE NNMi, whereas HPE NNM iSPI Performance for Metrics may be installed either with HPE NNMi or on standalone systems.

For highly distributed networking environments, HPE NNMi Premium Edition may be configured for Global Network Management (GNM). This deployment allows specified NNMi Management Servers[16] to act as "Global Managers", displaying consolidated data (e.g., topology and incidents) from multiple NNMi Management Servers acting as "Regional Managers". This provides a centralized view of a corporate-wide network. Both Global and Regional Managers can also be configured in an HA cluster. Upon a failover in any HA cluster, HPE NNMi will reestablish the connection between a Global and Regional Manager. Figure 1 shows an example of a GNM deployment where the Global and Regional Managers are configured in an HA cluster. An encrypted message bridge protects data transmitted between the Global and Regional Managers.

[11] IQ – Intelligent Query
[12] IP – Internet Protocol
[13] SLA – Service Level Agreement
[14] QA – Quality Assurance
[15] Separately purchased HA products support the HA cluster configuration, including Microsoft Failover Clustering for Windows Server and Veritas Cluster Server.
[16] NNMi Management Server – HPE NNMi and any NNM iSPIs on the same system

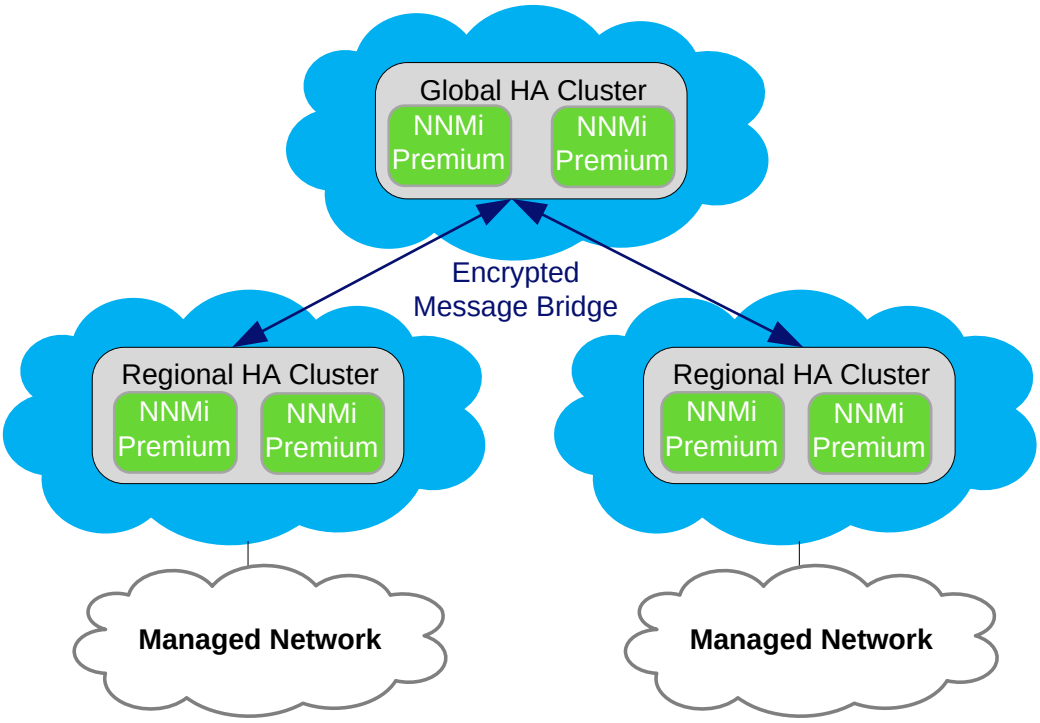

Figure 1 – High Availability Global Network Management Deployment

1.3.2 HPE NNMi Premium Edition System Architecture

HPE NNMi Premium Edition is built on an n-tier architecture with separate presentation, application, and data layers allowing for easier upgrades. The presentation layer consists of the NNMi Console, NNMi API, and NNMi CLI. The application layer is provided by an application server running several processes, including a causal engine[17], state polling[18], and continuous spiral discovery. Finally, the data layer is an embedded Postgres database for storing configuration files and network topology information. The NNM iSPIs are extensions, or add-on modules, to the core n-tier architecture.

HPE NNMi Premium Edition is installed on 64-bit hardware on either Microsoft Windows or Linux operating systems (OSs). It is also supported in virtualized environments, such as those provided by VMware ESXi or Microsoft Hyper-V. HPE NNMi Premium Edition is a distributed system. The HPE NNMi and HPE NNM iSPI Performance for Quality Assurance components are installed together on an NNMi Management Server. HPE NNM iSPI Performance for Metrics may be installed either with HPE NNMi or on a standalone system.

HPE NNMi Premium Edition includes a FIPS-validated cryptographic module to provide cryptographic functionality This includes protecting communications between Global and Regional Managers, to external LDAP[19]/AD[20] servers

[17] The causal engine performs deterministic root cause analysis on events.
[18] State polling occurs over the network management protocols to collect data from the network devices.
[19] LDAP – Lightweight Directory Access Protocol
[20] AD – Active Directory

and SNMP version 3 (SNMPv3) and web-services[21] managed network devices, and from remote users. The RSA BSAFE Crypto-J library provides a Special Publication (SP) SP 800-90A compliant HMAC[22] DRBG[23] for key generation.

1.4 TOE Overview

The TOE Overview identifies the TOE type and describes the TOE. It summarizes the usage and major security features of the TOE and defines the evaluated configuration and the TOE environment.

The TOE is a software only TOE. The TOE is HPE Network Node Manager i Premium Edition 10.21.402 consisting of three components:

- HPE NNMi 10.21.402
- HPE NNM iSPI Performance for Quality Assurance 10.21.402
- HPE NNM iSPI Performance for Metrics 10.21.402

The TOE is a network management solution that provides unified fault, availability, and performance monitoring for physical, virtual, hybrid, and cloud network environments. It implements several key security features:

- Auditing – event records are created for actions that result in changes to the NNMi database; for example, changes to user accounts or NNMi topology objects will generate an event record. Event records are also generated for actions at the NNM iSPIs. Every event record identifies the user that made the change. Only TOE administrator users can view the audit logs, which are protected from deletion.
- Predefined User Groups (roles) – the TOE maintains roles that are assigned by user account mappings to one or more of the following predefined user groups:
    - NNMi Administrator – this is a TOE administrator who manages and configures the TOE.
    - NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest – these are TOE users: network operators and guest users who use the TOE to monitor and maintain a managed network. A secondary role called NNMi Global Operator can be applied to TOE users. This provides access to all topology objects (i.e., nodes and related objects), but it does not change any other aspects of the TOE user's role.
    - Web Services Client – this is a role used exclusively by Web Services Clients or software that is integrated with the TOE through the NNMi API.
- Access controls – the TOE protects its user interfaces and managed network data (NNMi and NPS database objects such as nodes, interfaces, QA probes, incidents, and reports) by implementing multiple layers of security. The first layer protects the TOE's user interfaces using role-based access control (RBAC); the second layer restricts views of and actions taken on managed network data using custom user groups, security groups, and security group mappings (with associated object access privileges). NNMi Administrators configure these groups and mappings using the NNMi Console or NNMi CLI. Any user account that is not mapped to a role is denied access to the TOE. NNMi Administrators have full access rights to all of the TOE's user interfaces and managed network data.
- Multiple authentication mechanisms – either LDAP or X.509/PKI[24] certificate authentication can be configured to identify and authenticate users. However, X.509/PKI certificate authentication is not supported on the TOE's CLIs and NPS Console (when started directly from the NNMi Management Server).

[21] HTTPS is used to provide for web-services based management of virtual infrastructure devices (e.g., hypervisors).
[22] HMAC – Hash Message Authentication Code
[23] DRBG – Deterministic Random Bit Generator
[24] PKI – Public Key Infrastructure

if PKI is configured the TOE uses System account authentication at the CLIs. The NPS Console does support X.509/PKI certificate authentication when SSO[25] from the NNMi Console is used.

- FIPS-validated cryptographic module – the TOE uses the RSA BSAFE Crypto-J JSAFE and JCE Software cryptographic module to provide all cryptographic functionality. This includes securing its own internal communications between distributed components as well as communications from TOE users, NNMi Administrators, and Web Services Clients, and communications to LDAP/AD servers and SNMPv3 and web services managed devices in the TOE environment.
- Security attribute and user and TSF data management – security attributes and TOE configuration files are stored in the NNMi database. The TOE also makes use of an LDAP/AD server in the TOE environment to store user security attributes, such as passwords and user groups. User data including topology and other network information for both HPE NNMi and HPE NNM iSPI Performance for Quality Assurance is stored in the NNMi database. User data for HPE NNM iSPI Performance for Metrics is stored in the NPS database.

1.4.1 Evaluated Configuration

Figure 2 shows the details of the evaluated configuration of the TOE that consists of a GNM deployment. The following previously undefined acronyms appear in Figure 2:

- RHEL – Red Hat Enterprise Linux
- R2 – Release 2
- TLS – Transport Layer Security

[25] SSO – Single Sign-On

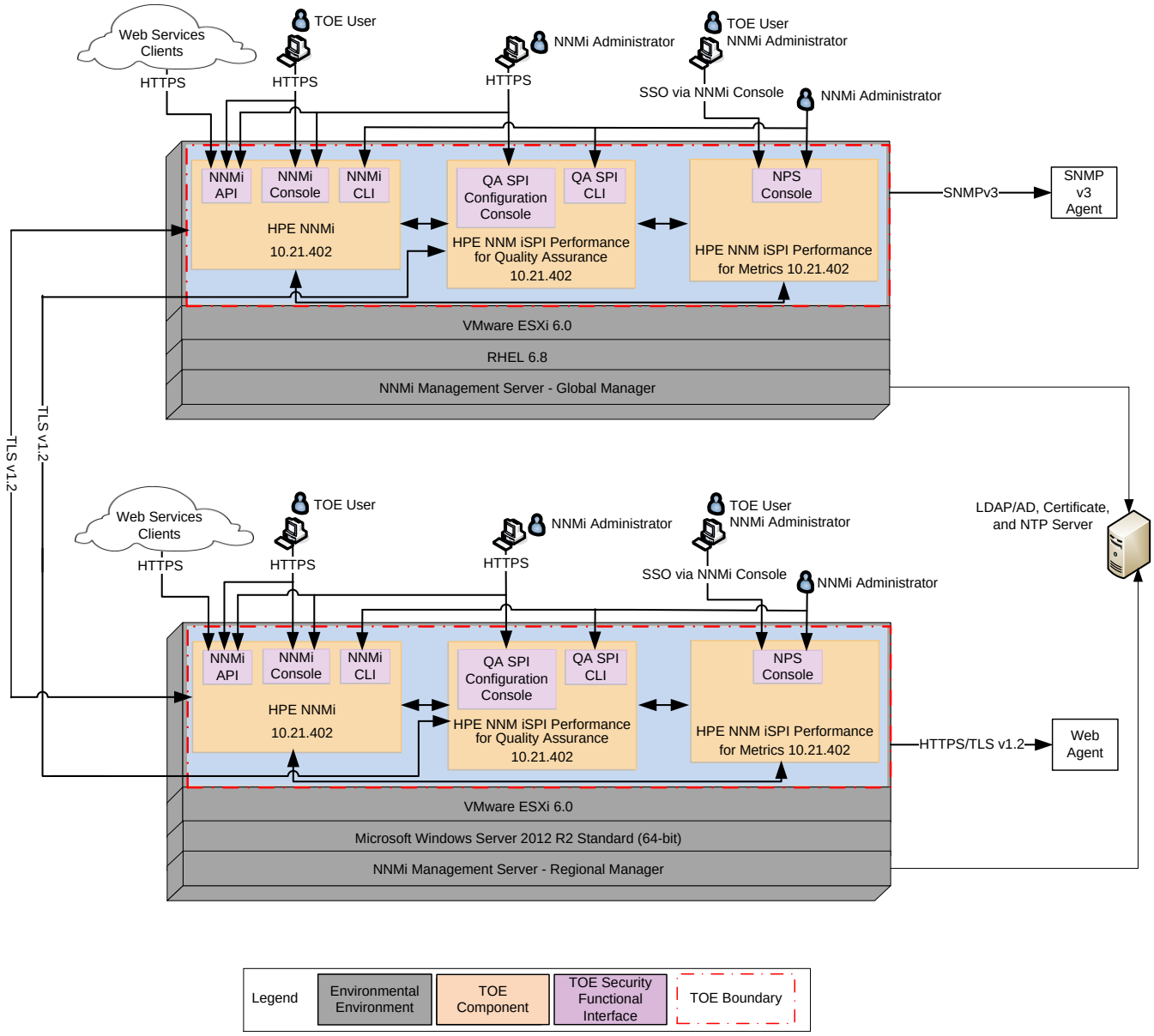

Figure 2 – Evaluated Configuration of the TOE

In the evaluated configuration shown in Figure 2, the TOE is configured as both a Global and Regional Manager. Both the Global and Regional Manager are running all of the TOE components on a single virtual machine (VM) provided by VMware ESXi 6.0 with the minimum hardware requirements listed in Table 2; however they are configured for Linux and Windows, respectively. More specifically, the Global Manager OS is RHEL 6.8 whereas the Regional Manager OS is Microsoft Windows Server 2012 R2 Standard (64-bit). The TOE binaries, which are specific to each OS, are downloaded from HP's support website at https://softwaresupport.hp.com/ as both zip and tar files.

The TOE includes patches that update the version 10.20 of each component to 10.21.402. The TOE binaries for RHEL 6.8 are listed below:

- HPE NNMi 10.20 – TB768-15009.tar.gz

- HPE NNM iSPI Performance for Quality Assurance 10.20 – TB759-15035.tar.gz
- HPE NNM iSPI Performance for Metrics 10.20 – TB771-15021.tar.gz
- V10.21.402 software patches for each component:
  - HPE NNMi 10.21.402 – NNM1020L_00001.rpm
  - HPE NNM iSPI Performance for Quality Assurance 10.21.402 – QA1020L_00001.rpm
  - HPE NNM iSPI Performance for Metrics 10.21.402 – NPS1020L_00001.rpm

The TOE binaries for Microsoft Windows Server 2012 R2 Standard (64-bit) are listed below:

- HPE NNMi 10.20 – TB765-15017.zip
- HPE NNM iSPI Performance for Quality Assurance 10.20 – TB759-15034.zip
- HPE NNM iSPI Performance for Metrics 10.20 – TB771-15020.zip
- V10.21.402 software patches for each component
  - HPE NNMi 10.21.402 – NNM1020W_00001.msi
  - HPE NNM iSPI Performance for Quality Assurance 10.21.402 – QA1020W_00001.msi
  - HPE NNM iSPI Performance for Metrics 10.21.402 – NPS1020W_00001.msi

The Global Manager receives and displays node data from the Regional Manager. The Regional Manager collects data from managed network devices (i.e., devices with agents[26] on them) and forwards it to the Global Manager based on administrator-configured forwarding filters. The Global Manager also independently collects data from managed network devices. All communication to the managed network devices is secured using SNMPv3 and TLS sockets. The following managed network devices are included in the TOE environment of the evaluated configuration:

- Net-SNMP for Linux, which provides an SNMPv3 agent that responds to SNMPv3 protocol requests from the TOE. The Global Manager is connected to one of these SNMPv3 agents as shown in Figure 2.
- ESXi hypervisor, which includes a web agent that responds to HTTPS protocol requests from the TOE. The Regional Manager is connected to one of these web agents as shown in Figure 2.

Access to the TOE's NNMi and QA SPI Configuration consoles and NNMi API is provided through encrypted HTTPS connections. The NNMi and QA SPI CLIs and the NPS Console may be accessed locally by NNMi Administrators. In the evaluated configuration, TOE users have no access to the CLIs and only access the NPS Console via SSO from the NNMi Console.

Both Global and Regional Managers are on the same domain and share an LDAP/AD server in the TOE environment to provide LDAP authentication and store user security attributes. Communication to the LDAP/AD server is secured through TLS v1.2. The LDAP/AD server is configured to provide NTP for reliable system time for the TOE.

1.4.2 TOE Environment

The TOE is installed on hardware or virtual platforms and is deployed in a secure data center that protects physical access to the TOE.

The TOE is installed on a network and can have numerous deployment scenarios since it presents a distributed architecture. It is designed to run on one or more hardware or virtual platforms depending on the requirements

[26] The agent stores information about the network device.

of the operational environment (e.g., number of managed network devices and QA probes in the managed networks).

1.4.2.1 Non-TOE Hardware/Software

The TOE relies on non-TOE hardware/software for its essential operation. Though this hardware/software is necessary for the TOE's operation, it is not part of the TOE. The non-TOE hardware/software listed in Table 2 below is required for essential operation of the TOE.

Table 2 – TOE Environment Hardware/Software Requirements

Category	Requirement
OS	Windows (64-bit only): • Microsoft Windows Server 2012 R2 Standard (used in evaluated configuration) or Datacenter Edition (or later SP[27]) • Windows Server 2008 R2 x64 Datacenter, Enterprise or Standard Edition with SP1 (or later SP) Linux: • RHEL 6.x, starting with 6.4 (6.8 used in the evaluated configuration) SUSE Linux Enterprise Server 11 SP3 (or later SP)
Hardware/Hypervisor	Hypervisor: • VMware ESXi 5.x • VMware ESXi 6.x (6.0 used in evaluated configuration) • Microsoft Hyper-V 2008 R2 with SP1 (or later SP) • Microsoft Hyper-V 2012 or 2012 R2 (or later SP) • Red Hat Enterprise Virtualization 3.5 (or later minor versions) • Oracle VM 3.x (starting with 3.2) Hardware (based on tiers of managed network environments): HPE NNMi, HPE NNM iSPI Performance for Quality Assurance, and HPE NNM iSPI Performance for Metrics installed on a single physical or virtual system (as per the evaluated configuration) Global Manager - • Medium (25K[28] to 40K regionally managed nodes/120K probes) - 24 CPU[29] cores, 96 GB[30] RAM[31], 12 GB NNMi Java Heap Size, 12 GB QA Java Heap Size, 15 GB installation disk space, 2 TB data disk space Regional Manager - • Entry (up to 250 nodes/5K probes) - 8 CPU cores, 16 GB RAM, 2 GB NNMi Java Heap Size, 2 GB QA Java Heap Size, 15 GB installation disk space, 45 GB data disk space • Small (250 to 3K nodes/30K probes) - 12 CPU cores, 32 GB RAM, 4 GB NNMi Java Heap Size, 6 GB QA Java Heap Size, 10 GB installation disk space, 300 GB data disk space • Medium (3K to 8K nodes/30K probes) - 16 CPU cores, 48 GB RAM, 8 GB NNMi Java Heap Size, 6 GB QA Java Heap Size, 10 GB installation disk space, 1 TB data disk space HPE NNMi and HPE NNM iSPI Performance for Quality Assurance installed on a single physical or virtual system Global Manager - • Medium (25K to 40K regionally managed nodes/120K probes) - 12 CPU cores, 40 GB RAM, 12 GB NNMi Java Heap Size, 12 GB QA Java Heap Size, 5 GB installation disk space, 140 GB data disk space • Large (40K to 80K regionally managed nodes/250K probes) - 20 CPU cores, 72 GB RAM, 16 GB NNMi Java Heap Size, 20 GB QA Java Heap Size, 5 GB installation disk space, 180 GB data disk space Regional Manager - • Entry (up to 250 nodes/5K probes) - 4 CPU cores, 8 GB RAM, 2 GB NNMi Java Heap Size, 2 GB QA Java Heap Size, 5 GB installation disk space, 30 GB data disk space • Small (250 to 3K nodes/30K probes) - 8 CPU cores, 16 GB RAM, 4 GB NNMi Java Heap Size, 6 GB QA Java Heap Size, 5 GB installation disk space, 90 GB data disk space • Medium (3K to 8K nodes/30K probes) - 12 CPU cores, 24 GB RAM, 8 GB NNMi Java Heap Size, 6 GB QA Java Heap Size, 5 GB installation disk space, 100 GB data disk space • Large (8K to 18K nodes/50K probes) - 12 CPU cores, 36 GB RAM, 12 GB NNMi Java Heap Size, 8 GB QA Java Heap Size, 5 GB installation disk space, 140 GB data disk space • Very Large (18K to 30K nodes/50K probes) - 16 CPU cores, 60 GB RAM, 16 GB NNMi Java Heap Size, 8 GB QA Java Heap Size, 5 GB installation disk space, 160 GB data disk space
NNM iSPI Performance for Metrics Server (when HPE NNM iSPI Performance for Metrics is installed on a dedicated physical or virtual system). Note that this is not the evaluated configuration.	

Category	Requirement
Software	Same as NNMi Management Server
OS	Same as NNMi Management Server
Hardware/Hypervisor	Hypervisor: VMware ESXi 5.5, VMware ESXi 6.x, or Microsoft Hyper-V 2012 R2 Hardware (based on tiers of managed network environments – dedicated server install): Global and Regional NNMi iSPI Performance for Metrics Servers – • Entry - 10 CPU cores, 28 GB RAM, 10 GB installation disk space, 800 GB database disk space • Medium - 12 CPU cores, 48 GB RAM, 10 GB installation disk space, 1500 GB database disk space • Large - 24 CPU cores, 96 GB RAM, 10 GB installation disk space, 3 TB[32] database disk space • Medium- 16 CPU cores, 64 GB RAM, 10 GB installation disk space, 2.5 TB data disk space • Large- 32 CPU cores, 96 GB RAM, 10 GB installation disk space, 4 TB database disk space
Client/Administrator Workstations	
Web Browser/Adobe Flash Player	Microsoft Internet Explorer (32-bit and 64-bit) version 11 or higher (not running in Compatibility View mode) Install Adobe Flash for proper display of real-time line graphs: Adobe Flash Player Plug-in version 11.2.202.285 or later on Linux or version 11.7.700.202 or later on Windows
Hardware	Standard desktop or laptop used in a corporate environment
Network	
LDAP Server	LDAP server capable of supporting TLS v1.2 connections
Certificate Server	A certificate server for CA[33] certificates used for secure communications with the TOE. May also use AD authentication server.
Network	High-speed connection to all components and systems in the configuration with sufficient bandwidth to process the expected workload
Other Environmental Components	
Managed Network Devices	A managed network consisting of SNMPv3, web services, and other managed network devices supported for management by HPE Network Node Manager i Premium Edition 10.21.402

Linux RPM[34] Requirements	Linux installations require the following RPM package libraries on the NNMi Management Server:
	• RPM: glibc
	  ○ /lib64/libc-2.12.so
	• RPM: libaio
	  ○ /lib64/libaio.so.1
	• RPM: libXtst
	  ○ /usr/lib64/libXtst.so.6
	• RPM: libXi
	  ○ /usr/lib64/libXi.so.6

File Sharing	All servers must have CIFS installed.

[27] SP – Service Pack
[28] K – Thousand
[29] CPU – Central Processing Unit
[30] GB – Gigabyte
[31] RAM – Random-Access Memory
[32] TB – TeraByte
[33] CA – Certificate Authority
[34] RPM – RedHat Package Manager

1.4.3 Product Physical/Logical Features and Functionality not included in the TOE

HPE Network Node Manager i Premium Edition 10.21.402 provides other security features that are out of the scope of the TOE. These features are not included in the TOE and will not be evaluated, and therefore there is no assurance level associated with them. The features not included in the TOE are the following:

- Oracle database configuration
- HA cluster configuration and Application Failover
- LW-SSO[35] to the TOE
- Local password based authentication
- Common Access Card (CAC)
- NNM iSPI Performance for Metrics BI Server Portal – this is the NPS Console BI Server tab and includes the BI Portal page, BI Server Administration page, and Query Studio
- URL Cross Actions – "URL launch" or "Integrate with NNMi from Elsewhere using URL" functionality
- System Account access on TSFIs except as required for NNMi CLI
- SNMP v1 and v2 management of network devices (except as needed for QA probe communications)
- Remote access to the NPS Console (except as provided through the **Actions** menu of the NNMi Console)
- Samba for file sharing between HPE NNMi and HPE NNM iSPI Performance for Metrics
- HPE NNM iSPI Performance for Metrics command line tools, including the Configuration Utility, Diagnostics Collector, and other tools that are run from the Windows Start menu
- HPE NNM iSPI Performance for Quality Assurance API
- HPE NNM iSPI Performance for Quality Assurance IRA[36]
- Backup and restore NNMi CLI functions - `nnmbackup.ovpl`, `nnmbackupembdb.ovpl`, and `nnmrestoreembdb.ovpl`
- NNMi API methods used to push data out to third party clients (WE-E methods)
- HPE NNM iSPI Performance for Metrics NPS Console Log File Monitor

1.5 TOE Description

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

1.5.1 Physical Scope

The TOE is HPE Network Node Manager i Premium Edition 10.21.402 that consists of three software components:

- HPE NNMi 10.21.402
- HPE NNM iSPI Performance for Quality Assurance 10.21.402
- HPE NNM iSPI Performance for Metrics 10.21.402

The TOE software runs on Windows or Linux physical or virtual platforms compliant with the minimum software and hardware requirements listed in Section 1.4.2.

[35] LW-SSO – Lightweight Single Sign-On

[36] IRA – Intelligence Response Agent

1.5.1.1 TOE Software

The TOE is delivered as software binaries that are downloaded from HP's support website at https://softwaresupport.hp.com/. As described in Section 1.4.1, the binaries are different depending on whether they are to be installed on Windows or Linux OSs.

1.5.1.2 Guidance Documentation

The following guides are provided in PDF [37] format, are downloaded from HP's support website at https://softwaresupport.hp.com/, and are required reading and part of the TOE. Although the titles of the guidance documentation make reference to 10.20, they are also applicable to the TOE version 10.21.402.

- *HPE Network Node Manager i Software, Software Version: 10.20, for the Windows and Linux operating systems, Deployment Reference, June 2016*
- *HPE Network Node Manager i Software, Software Version: 10.20, Windows and Linux operating systems, Online Help: Help for Administrators, June 2016*
- *HPE Network Node Manager i Software, Software Version: 10.20, Windows and Linux operating systems, Online Help: Help for Operators, June 2016*
- *HPE Network Node Manager i Software, Software Version: 10.20, Windows and Linux operating systems, Online Help: Using the Console, June 2016*
- *HPE Network Node Manager i Software, For the Windows and Linux operating systems, Software Version: 10.20, Reference Pages, July 2016*
- *HPE Network Node Manager i Software Premium Edition, Software Version: 10.20 , for the Windows and Linux operating systems, Release Notes, July 2016*
- *HPE Network Node Manager i Software Premium Edition, Software Version: 10.20, for the Windows and Linux operating systems, Support Matrix, July 2016*
- *HPE Network Node Manager i Software Read me first, July 2016*
- *HPE Network Node Manager iSPI Performance for Quality Assurance Software For the Windows and Linux operating systems, Software Version: 10.20, Online Help, June 2016*
- *HPE Network Node Manager iSPI Performance for Quality Assurance For the Windows and Linux operating systems, Software Version: 10.20, Deployment Reference, June 2016*
- *HP Network Node Manager iSPI Performance for Quality Assurance Software Version: 10.20, for the Windows and Linux operating systems, Reference Pages, November 2015*
- *HPE Network Node Manager iSPI Performance for Metrics Software For the Windows and Linux operating systems, Software Version: 10.20, Online Help, July 2016*
- *HPE Network Node Manager iSPI Performance for Metrics For the Windows and Linux operating systems, Software Version: 10.20, Deployment Reference, July 2016*
- *HPE Network Node Manager iSPI Performance for Metrics Read me first, July 2016*
- *HPE Network Node Manager I Software, Software Version: 10.20 for the Windows and Linux operating systems, Hardening Guide, August 2016*

The following guides are provided in HTML[38] format and are required reading and part of the TOE:

- *HPE Network Node Manager i Software (NNMi) Device Support Matrix, Software Version: 10.20, Last Updated: 07/26/2016*
- *HPE Network Node Manager i Software Interactive Installation and Upgrade Guide, July 2016*

[37] PDF – Portable Document Format

[38] HTML – Hyper Text Markup Language

- *HPE Network Node Manager iSPI Performance for Quality Assurance Interactive Installation and Upgrade Guide, July 2016*
- *HPE Network Node Manager iSPI Performance for Metrics Interactive Installation and Upgrade Guide, July 2016*

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
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- Trusted Path/Channels

1.5.2.1 Security Audit

The TOE generates audit records for actions at the NNMi Console, NNMi API, and NNMi CLI that result in changes to the NNMi database. The TOE also generates audit records for actions at the QA SPI Configuration Console and QA SPI CLI. Lastly the TOE generates audit records for login and logout activities at its user interfaces. Every event record identifies the user that made the change.

NNMi Administrators can view the HPE NNMi, HPE NNM iSPI Performance for Quality Assurance, and HPE NNM iSPI Performance for Metrics audit records through the NNMi Console **Tools → NNMi Audit Log, Tools → QA Audit Log, and Tools → NPS Audit Log** menu options, respectively. Only the most recent log files (for the current day) may be viewed. NNMi Administrators are prevented from modifying or deleting audit records.

Audit information is written to three different log files per day, one each for HPE NNMi, HPE NNM iSPI Performance for Quality Assurance, and HPE NNM iSPI Performance for Metrics. The log files are retained for 14 days by default.

1.5.2.2 Cryptographic Support

The TOE uses the FIPS 140-2 validated RSA BSAFE Crypto-J JSAFE and JCE Software Module to support all cryptographic functionality such as encryption, decryption, and hashing. Cryptographic operations are provided to secure communications among various physically-separated TOE components, to LDAP/AD servers and SNMPv3 and web services managed devices in the TOE environment, and from remote users.

The TOE generates cryptographic keys to be used with encryption, decryption, keyed hash, and signature operations. Each of the cryptographic algorithms supported by the TOE have been tested and validated by the CAVP[39]. The TOE uses the Java Garbage Collection mechanism to destroy keys.

[39] CAVP – Cryptographic Algorithm Validation Program

1.5.2.3 User Data Protection

The TOE enforces the Resource Access Control SFP[40] to control user access to the following TOE resources: the NNMi Console, QA SPI Configuration Console, NPS Console, NNMi API and CLI, QA SPI CLI, HPE NNM iSPI Performance for Metrics reports, NNMi SNMP-managed and NPS database objects. An NNMi Administrator configures user access by setting security attributes (i.e., NNMi roles, custom User Groups, Security Groups, and Security Group Mappings) via the NNMi Console or NNMi CLI. If these security attributes are not configured, users have no access to any of the TOE's user interfaces, NNMi SNMP-managed database objects, HPE NNM iSPI Performance for Metrics reports, or NPS database. The TOE gives NNMi Administrators full access rights to all resources.

Web Services Clients have access only to the NNMi API, not the TOE's consoles or CLIs. Web Services Clients do not have access to the CLIs in the evaluated configuration. TOE users (NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest) are only permitted to use the NNMi Console and the NPS Console and are restricted based on their NNMi role, custom User Groups, and Security Group Mappings. They do not have access to the CLIs in the evaluated configuration.

The TOE also maintains a "System" user account for authorized TOE administrators to access the NNMi and QA SPI CLI when the TOE is in PKI/X.509 authentication mode. Though this account may also be used to access the NNMi Console and NNMi API, this is excluded in the evaluated configuration.

1.5.2.4 Identification and Authentication

User authentication can be performed in multiple ways on the TOE. System account, LDAP, and X.509/PKI certificate (including smart card) authentication is supported. The following commands can be executed prior to identification and authentication:

- `nmsqaauthconfigreload.ovpl` – QA SPI CLI command used to apply/reload the changes made to the authentication mechanism used by the HPE NNM iSPI Performance for Quality Assurance software
- `nnmenableperfspi.ovpl` – NNMi CLI command that configures NNMi to operate with NPS

All users must be successfully identified and authenticated prior to performing any other TSF-mediated actions.

For X.509/PKI certificate authentication, the TOE stores usernames and user account mappings (for role and custom User Group membership) in the NNMi database. Alternatively, for LDAP authentication, the TOE relies on the LDAP/AD server to store usernames, passwords, and user account mappings. Security Group Mappings are stored solely in the NNMi database. The TOE obscures passwords entered at its consoles using bullets.

1.5.2.5 Security Management

The TOE is managed primarily by NNMi Administrators. Web Services Clients have limited (query only) management abilities over the NNMi API as explained below.

The TOE provides NNMi Administrators with the ability to perform specific management functions, including configuring X.509/PKI authentication, viewing the audit logs, managing the Resource Access Control SFP security attributes, configuring QA probes, and configuring communications between Global and Regional Managers. Only NNMi Administrators can configure the security attributes used to control access to the TOE resources. These

[40] SFP – Security Function Policy

attributes must be configured for TOE users or Web Services Clients to have access to the TOE's resources. NNMi Administrators are also able to configure TOE user accounts.

Using the Web API, Web Services Clients have the ability to query the Resource Access Control SFP security attributes.

1.5.2.6 Protection of the TOE Security Functionality (TSF)

Using its cryptographic module, the TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. The TOE uses TLS sockets to secure communication between a Global and Regional NNMi Management Server.

1.5.2.7 Trusted Path/Channels

The TOE provides a trusted channel between HPE NNMi and LDAP/AD servers in the TOE environment using an LDAPS[41] connection over TLS v1.2. The TOE also provides a trusted channel between HPE NNMi and SNMPv3 and web services managed devices in the TOE environment using the RSA BSAFE Crypto-J JSAFE and JCE Software modules to provide SNMPv3 and HTTPS network packet encryption. Only the TOE is allowed to initiate these secure channel communications.

A TOE user, NNMi Administrator, or Web Services Client can initiate a secure remote connection to the TOE over HTTPS. The HTTPS connection uses TLS v1.2 to protect data communications from modification or disclosure and ensures end point identification. The TOE uses FIPS-validated cryptographic algorithms to implement the above cryptographic functions.

[41] LDAPS – Lightweight Directory Access Protocol Secure

2. Conformance Claims

This section and Table 3 provide the identification for any CC, 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, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2015/12/16 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 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 users of the TOE: 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. An attacker may initiate a process within the TOE to act on its behalf. This process is assumed to have all attributes of the attacker.
- TOE users and Web Services Clients: 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.

All users 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. Both the confidentiality and integrity of the data must be protected. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4. Table 4 below lists the applicable threats.

Table 4 – Threats

Name	Description
T.DATA_COMPROMISE	An attacker may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.INTERCEPT	The TOE may communicate with remote IT entities and TOE user, TOE administrator, and Web Services Client workstations that lie outside of the organization's trusted network. An attacker may attempt to intercept these communications in order to read or modify critical TSF data.
T.MASQUERADE	An attacker or process may masquerade as another entity to gain unauthorized access to data or TOE resources.
T.TAMPERING	An attacker or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	Attackers, TOE users, or Web Services Clients may gain access to user or TSF data on the TOE, even though they are not authorized in accordance with the TOE security policy.

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. There are no OSPs imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

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 5 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 5 – Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate dedicated hardware and operating system.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its functions.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	TOE and OS administrators are non-hostile, appropriately trained, and follow all guidance.
A.NPS_CONSOLE_PROTECT	TOE users and administrators will only access the NPS Console by starting it at the NNMi Management Server (TOE administrators only) or through SSO access to it via the NNMi Console.
A.AGENT_PROTECT	Machines with SNMPv3/hypervisor agents located outside the controlled access facility are protected and no malicious software is running on them.
A.USER_PROTECT	No malicious software is installed or running on the Administrator and TOE user workstations.

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 6 below.

Table 6 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to user data stored on the TOE.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its security attributes and TSF data, ensuring that only authorized TOE administrators may exercise such control.
O.AUDIT	The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users through multiple authentication mechanisms prior to allowing any access to its security functionality and data.
O.PROTECT	The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 – IT Security Objectives

Name	Description
OE.NETWORK	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.AGENT_PROTECT	Sites deploying the machines running the SNMPv3 and hypervisor agents will protect them from external interference or tampering. Administrators will ensure there is no malicious software running on them.
OE.USER_PROTECT	The Administrator and TOE user workstations must be protected from any external interference or tampering.

4.2.2 Non-IT Security Objectives

Table 8 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 8 – Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE and OS administrators who are appropriately trained and follow all administrator guidance. TOE and OS administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.AUTHORIZED_ACCESS	Only TOE and OS administrators are granted access to the controlled access facility in which the TOE is located

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

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

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 [*italicized and 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.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration, and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

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

Table 9 – TOE Security Functional Requirements

Name	*Description*	*S*	*A*	*R*	*I*
FAU_GEN.1	*Audit Data Generation*	✓	✓		
FAU_GEN.2	*User Identity Association*				
FAU_SAR.1	*Audit review*		✓		
FAU_STG.1	*Protected audit trail storage*	✓			
FAU_STG.4	*Prevention of audit data loss*	✓	✓		
FCS_CKM.1	*Cryptographic key generation*		✓		
FCS_CKM.4	*Cryptographic key destruction*		✓		
FCS_COP.1	*Cryptographic operation*		✓		
FDP_ACC.1	*Subset access control*		✓		
FDP_ACF.1	*Security attribute based access control*		✓		

Name	Description	S	A	R	I
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF Data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		

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. [

For NNMi:

- *Login and logout at the NNMi Console*
- *The following TOE user, TOE administrator, or Web Services Clients actions at any of the HPE NNMi user interfaces that result in changes to the NNMi database -*
  - *changes to user and authentication information*
  - *changes to NNMi topology objects*
  - *changes to incident lifecycle information*
  - *configuration changes made using the NNMi Console Configuration workspace*
  - *actions taken from the NNMi Console Actions menu*

For HPE NNM iSPI Performance for Metrics:

- *TOE User and NNMi Administrator login at the NPS Console*

For HPE NNM iSPI Performance for Quality Assurance:

- *Login at the QA SPI Configuration Console*
- *Configuration changes made using the QA SPI Configuration Console and QA SPI CLI*
- *Changes made to the configuration of managed QA probes*].

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, [*hostname of the user's workstation (if available), type of change, action performed, information about the object that was changed, additional metadata available for the object or action*].

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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 [*NNMi Administrator*] with the capability to read [*all audit information for the current day*] 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.

FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.1

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

FAU_STG.1.2

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

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1

The TSF shall [*overwrite the oldest stored audit records*] and [*no other actions*] if the audit trail is full.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
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 [*key generation using a deterministic random bit generator*] and specified cryptographic key sizes [*listed in* Table 10] that meet the following: [*none*].

Table 10 List of Key Sizes that the TOE can Generate

Key Type	Key Sizes
AES[42] Key	128, 192, 256
Triple-DES[43] 3-Key	192

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
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 [*Java Garbage Collection mechanism*] that meets the following: [*none*].

Application Note: The Java Garbage Collector reclaims the memory occupied by keys that are no longer in use by the TOE. Once the TOE releases all references to a key, the Java Garbage Collector clears the memory occupied by the key and then releases this memory back to the TOE for reuse. The time it takes for the Java Garbage Collector to destroy keys is dependent on the TOE configuration (system sizing and load). For the evaluated configuration, the keys were shown to be destroyed within two hours.

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations Table 11 "Cryptographic Operations" column*] in accordance with a specified cryptographic algorithm [*listed in Table 11 "Cryptographic Algorithm" column*]

[42] AES – Advanced Encryption Standard
[43] DES – Digital Encryption Standard

and cryptographic key sizes [*listed in Table 11 "Key/Digest Size (bits)" column*] that meet the following: [*list of standards in Table 11 "Certificate # column"*].

Table 11 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key/Digest Size (bits)	Certificate #
Symmetric Encryption and Decryption	AES CBC[44] Triple-DES[45] CBC	128, 256 192	3263 1852
Message Digest	SHA-1 SHA-256 MD5 (for use in TLS only)	SHA-1 (160) SHA-2 (256)	2701
Message Authentication Code	HMAC with SHA-1, SHA-256	SHA-1 (160) SHA-2 (256)	2062
Signature Generation	RSA X9.31, PKCS[46] #1 V.1.5, RSASSA-PSS[47]	2048	1663
	DSA	2048 and 3072	932
Signature Verification	RSA X9.31, PKCS #1 V.1.5, RSASSA-PSS	1024, 2048	1663
	DSA	2048 and 3072	932

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*Resource Access Control SFP*] on [

Subjects:

- *TOE users (NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest)*
- *TOE administrators (NNMi Administrator)*
- *Web Services Clients (user account mapped to Web Services Client role – for software integration via NNMi API only)*

Objects:

- *NNMi Console*

[44] CBC – Cipher Block Chaining
[45] DES – Data Encryption Standard
[46] PKCS – Public-Key Cryptography Standards
[47] PSS – Probabilistic Signature Scheme

- *SNMP-managed NNMi database objects – topology inventory objects (nodes, sub-node objects such as interfaces, inter-node objects such as connections), resolved incidents, QA probes and QoS[48] elements hosted on a node, sites*
- *NPS Console*
- *NPS database objects*
- *HPE NNM iSPI Performance for Metrics Reports*
- *QA SPI Configuration Console*
- *NNMi CLI*
- *NNMi API*
- *QA SPI CLI*

Operations:

- *View and execute in NNMi Console (no SNMP-managed NNMi database objects preselected)*
- *View SNMP-managed NNMi database objects*
- *Execute NNMi Console menu items against one or more visible SNMP-managed NNMi database objects*
- *View and execute in NPS Console*
- *View NPS database objects*
- *View HPE NNM iSPI Performance for Metrics Reports*
- *View and execute in QA SPI Configuration Console*
- *Execute NNMi CLI*
- *Execute NNMi API*
- *Execute QA SPI CLI*

].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1

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

- *Subject SFP-relevant security attributes:*
  - *TOE administrators (NNMi Administrator) – NNMi Role and System account authorization*
  - *TOE users (NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest) SFP-relevant security attributes – NNMi Role, Custom User Groups, and Security Group Mappings[49]*
  - *Web Services Clients SFP-relevant security attributes – NNMi role*
- *Object SFP-relevant security attributes:*
  - *NNMi Console – default NNMi Role[50] and Object Access Privilege[51]*
  - *SNMP-managed NNMi database object (nodes only) – Security Group and Security Group Mappings*
  - *SNMP-managed NNMi database objects other than nodes – Security Group Mappings for related nodes*

[48] QoS – Quality of Service

[49] Security Group mappings form an association between a custom User Group, Security Group, and Object Access Privilege.

[50] NNMi Administrators may change the default NNMi role required for execution of NNMi Console Actions and Tools menu items as long as it does not go below a minimum required NNMi role.

[51] Object Access Privilege – a permission required to execute NNMi Console menu items against nodes in a Security Group.

- *NPS Console – NNMi role*
- *NPS database objects – Security Group Mappings for related nodes*
- *HPE NNM iSPI Performance for Metrics Reports – Security Group Mappings for related nodes*
- *QA SPI Configuration Console – NNMi role*
- *NNMi and QA SPI CLI – NNMi role*
- *NNMi API – NNMi Role and Security Group Mappings*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *NNMi Console Visibility and Execution: If a TOE user's NNMi role meets or exceeds[52] the default NNMi role for a part of the NNMi Console, the TOE user can see those parts of the NNMi Console. Parts of the NNMi Console that are visible and do not require a user to pre-select a node or other SNMP-managed NNMi database object to perform an operation can also be executed.*
- *NNMi Console Database Object Visibility: If a TOE user is a member of a custom User Group that is mapped (via a Security Group Mapping) to a Security Group, then that TOE user can see (via NNMi Console Workspace views and forms) all nodes that are part of the Security Group as well as other SNMP=managed NNMi database objects related to the nodes (i.e., interfaces[53], connections[54], resolved incidents[55], QA probes[56], and sites[57]). TOE users can also see HPE NNM iSPI Performance for Metrics reports and performance views (launched via the NNMi Console Actions menu) for visible nodes. TOE users that have the NNMi Global Operator role assigned can see all SNMP-managed NNMi database objects.*
- *NNMi Console Execution Against Visible SNMP-managed NNMi Database Objects: A TOE user in a custom User Group can execute visible NNMi Console menu items against the nodes contained in a mapped Security Group and the node's related SNMP-managed NNMi database objects if the Object Access Privilege configured in the Security Group Mapping meets or exceeds[58] the default Object Access Privilege for the NNMi Console menu item.*
- *NPS Console access: All TOE users have visibility to and can execute the NPS Console Report menu (with the exception of the Self Monitoring report option) launched via the NNMi Console Actions menu.*
- *NPS Console database object visibility: Content in the HPE NNM iSPI Performance for Metrics reports is restricted to the nodes for which a user has NNMi Console database object visibility.*
- *QA SPI Configuration Console: TOE administrators (i.e., subjects with the NNMi Administrator role assigned) are granted full access to the QA SPI Configuration Console; otherwise, access is denied.*

[52] The NNMi roles are hierarchical, with NNMi Administrator the highest, followed by NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest.

[53] Sub-node objects like interfaces are visible only if the hosting node is visible.

[54] Inter-node objects like connections are visible only if one of the participating nodes is visible; however, connections will only be shown in a Map view if both nodes are visible.

[55] Resolved incidents are visible only if the source node on which the associated QA probe is configured is visible.

[56] QA probes and QoS elements are visible only if the nodes they are configured on are visible.

[57] Source and destination sites are visible only if at least one of the QA probes or QoS elements associated with the source site are visible.

[58] The Object Access Privileges are hierarchical, meaning the higher level Object Access Privilege includes all privileges of the lower level Object Access Privileges. (Object Administrator is highest, followed by Object Operator Level 2, Object Operator Level 1, and Object Guest.)

- *NNMi and QA SPI CLI access: TOE administrators are granted access to the NNMi and QA SPI CLI based on their NNMi role and System account authorization.*
- *NNMi API access: Web Services Clients (i.e., subjects with the Web Services Client role assigned), and TOE administrators are granted full access to the NNMi API; otherwise access is granted to TOE users based on their NNMi role, Custom User Groups, and Security Group Mappings. Guest role does not have access to the NNMi API.*
- *TOE Users that have multiple NNMi roles obtain the superset of the role privileges.*
- *TOE users that are part of multiple custom User Groups that are mapped to the same Security Group receive the highest Object Access Privilege defined by the Security Group Mappings.*

].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*TOE administrators are granted full access rights to the NNMi Console, the QA SPI Configuration Console, the NPS Console, the NNMi API, the NNMi and QA SPI CLIs, all NNMi and NPS database objects, and HPE NNM iSPI Performance for Metrics Reports.].*

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.4 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 and password (for LDAP authentication only), User Account Mapping (NNMi role and Custom User Group membership), Security Group Mapping*].

Application Note: When the TOE is configured for LDAP authentication, "LDAP Mixed Mode" is used. In this configuration, the TOE relies on the AD server to store usernames and passwords. User account mappings are stored in the NNMi database. When the TOE is configured for PKI authentication, "PKI Mixed Mode" is used. In this configuration, usernames and User Account Mappings are stored in the NNMi database.

FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1

The TSF shall allow [*the NNMi CLI command nnmenableperfspi.ovpl and the QA SPI CLI command nmsqaauthconfigreload.ovpl] on behalf of the user to be performed before the user is authenticated.*

FIA_UAU.1.2

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 [*System account, LDAP, and X.509/PKI certificates (including smart cards)*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*username and password provided by user matches that in LDAP server (for LDAP authentication); PKI certificate username matches an NNMi user account name*].

Application Note: PKI certificates is not supported for login to the TOE's CLIs. LDAP is not supported for some specific NNMi and QA SPI CLI tools that only execute using the System account.

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 when accessing the NNMi Console, QA SPI Configuration Console, and NPS Console; no feedback at the NNMi API*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.1.1

The TSF shall allow [*the NNMi CLI command nnmenableperfspi.ovpl and the QA SPI CLI command nmsqaauthconfigreload.ovpl*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

6.2.5 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1

The TSF shall enforce the [*Resource Access Control SFP*] to restrict the ability to [*change_default, query, modify, delete, [add]*] the security attributes [*NNMi roles, custom User Groups, Security Groups, and Security Group Mappings*] to [*NNMi Administrator, Web Services Client (query only)*].

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

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

FMT_MSA.3.1

The TSF shall enforce the [*Resource Access Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*NNMi Administrator*] to specify alternative initial values to override the default values when an object or information is created.

Application Note: FMT_MSA.3.2 does not apply to the NNMi Console.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, [add]*] the [*user accounts*] to [*NNMi Administrator, Web Services Client (query only)*].

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: [

- *configure PKI/X.509 authentication,*
- *view the audit logs,*
- *manage Resource Access Control SFP security attributes,*
- *configure QA probes, and*
- *configure communications between global and regional managers*].

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 [

- *NNMi Administrator,*
- *TOE users*
  - *NNMi Level 2 Operator,*
  - *NNMi Level 1 Operator,*
  - *NNMi Guest,*
  - *NNMi Global Operator, and*
- *Web Services Client*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_ITT.1.1

The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

6.2.7 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 [*connections to an external LDAP server for authentication and connections to SNMP v3 and web services managed devices for network packet encryption*].

FTP_TRP.1 Trusted path

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, *[HTTPS connections to the NNMi API, NNMi Console, and QA SPI Configuration Console]*].

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 Flaw Remediation (ALC_FLR.2)
Table 12 summarizes these requirements.

Table 12 – 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 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class 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 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 Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 13 lists the security functionality and their associated SFRs.

Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functionality	FPT_ITT.1	Basic internal TSF data transfer protection
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE generates audit records for actions initiated at the HPE NNMi and NNM iSPI user interfaces.

For HPE NNMi, the TOE generates audit records for login and logout at the NNMi Console and the following TOE user, TOE administrator, or Web Services Client actions at any of its user interfaces that result in changes to the NNMi database:

- Changes to user and authentication information
- Changes to NNMi topology objects
- Changes to incident lifecycle information
- Configuration changes made using the NNMi Console **Configuration** workspace
- Actions taken from the NNMi Console **Actions** menu

For HPE NNM iSPI Performance for Metrics, the TOE generates audit records for TOE user and TOE administrator login at the NPS Console.

For HPE NNM iSPI Performance for Quality Assurance, the TOE generates audit records for the following events:

- Login at the QA SPI Configuration Console
- Configuration changes made using the QA SPI Configuration Console and QA SPI CLI
- Changes made to the configuration of managed QA probes

The TOE audit records contain the following information:

Table 14 – Audit Record Contents

Field	Content
Timestamp	Date and time of the event
Username	Subject Identify
After	Outcome of the event (new value of a database field); this field is optional as every change record many not reflect the After
Remote Hostname	The remote user's workstation (if available)
Category	Type of change
RecordType	Action performed (outcome of the event)
TargetType	Type of object that was changed
TargetId	Target object identifier
Field	Changed field
Before	Previous value of a database field

NNMi Administrators can view the HPE NNMi, HPE NNM iSPI Performance for Quality Assurance, and HPE NNM iSPI Performance for Metrics audit records through the NNMi Console **Tools → NNMi Audit Log, Tools → QA Audit Log, and Tools → NPS Audit Log** menu options, respectively. Only the most recent log files (for the current day) may be viewed. NNMi Administrators are prevented from modifying or deleting audit records. The audit records show the identity of the user that caused the event.

Audit information is written to three different log files per day, one each for HPE NNMi, HPE NNM iSPI Performance for Quality Assurance, and HPE NNM iSPI Performance for Metrics. The log files are retained for 14 days by default. The TOE overwrites the oldest audit records when the retention period is met to prevent audit data loss.

Although the TOE does not audit the startup and shutdown of the audit function, it does audit the startup and shutdown of the TOE, thereby indicating when the audit function is started and stopped as well.

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

7.1.2 Cryptographic Support

The TOE uses the RSA BSAFE Crypto-J JSAFE and JCE Software Module Software Version 6.2 cryptographic module for performing all cryptographic operations.

The RSA BSAFE Crypto-J JSAFE and JCE Software module resides in all three TOE components and provides HTTPS for secure communications from remote users accessing the NNMi Console, NNMi API, and QA SPI Configuration Console. It also provides TLS sockets for secure communications between Global and Regional Managers. Lastly, it is used to encrypt data in the Postgres and Sybase IQ databases and to secure communications to LDAP/AD servers and SNMPv3 and web services managed devices in the TOE environment.

The TOE uses the RSA BSAFE Crypto-J JSAFE and JCE Software module to generate the asymmetric and symmetric keys with key sizes as listed in Table 10. The cryptographic module is completely contained within the TOE boundary and contains all instructions to generate cryptographic keys. All cryptographic keys are generated by a deterministic random bit generator. The TOE destroys all keys using the Java Garbage Collection mechanism. The Java Garbage Collector reclaims the memory occupied by keys that are no longer in use by the TOE. Once the TOE releases all references to a key, the Java Garbage Collector clears the memory occupied by the key and then releases this memory back to the TOE for reuse. The time it takes for the Java Garbage Collector to destroy keys is dependent on the TOE configuration (system sizing and load). For the evaluated configuration, the keys were shown to be destroyed within two hours. All cryptographic operations performed by the module use FIPS-validated algorithms. All algorithms and certificate numbers are listed above in Table 11.

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

7.1.3 User Data Protection

The TOE enforces the Resource Access Control SFP to control user access to the NNMi Console, QA SPI Configuration Console, NPS Console, NNMi API and CLI, QA SPI CLI, HPE NNM iSPI Performance for Metrics reports, and NNMi SNMP-managed and NPS database objects. NNMi SNMP-managed objects are those that include an SNMPv3 agent, including objects with web agents - as these incorporate an underlying SNMPv3 agent for management. An NNMi Administrator configures user access by setting security attributes (i.e., NNMi roles, custom User Groups, Security Groups, and Security Group Mappings) via the NNMi Console or NNMi CLI. If these security attributes are not configured, users have no access to any of the TOE user interfaces, HPE NNM iSPI Performance for Metrics reports, or NNMi and NPS database objects. The TOE gives full access to all resources to a user with the NNMi Administrator role. Web Services Clients have access only to the NNMi API, not the TOE's

consoles or CLIs. TOE users (NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest) are only permitted to use the NNMi and NPS consoles and NNMi API. They are denied access to the QA SPI Configuration Console and have no physical access to the CLIs. TOE users are restricted access to the TSFIs based on their NNMi role, custom User Groups, and Security Group Mappings and enforced rules as explained below.

View and execute in NNMi Console (no SNMP-managed NNMi database objects preselected)

A TOE user's NNMi role is configured by an NNMi Administrator via a mapping to one of three predefined user groups: NNMi Level 2 Operator, NNMi Level 1 Operator, and NNMi Guest. The TOE matches this NNMi role to the default NNMi roles for the parts of the NNMi and NPS consoles (e.g., workspaces and menu items) to determine what parts of these consoles are displayed. The TOE user's NNMi role must meet or exceed the default NNMi role for the part of a console for it to be displayed. Parts of the NNMi and NPS consoles that are visible and do not require preselection of a node or other SNMP-managed NNMi database object can also be executed. TOE users that have not been assigned a role by an NNMi Administrator are unable to log in to the NNMi or NPS consoles. TOE users that have multiple NNMi roles obtain the superset of the role privileges or permitted actions.

View SNMP-managed NNMi database objects

A TOE user must be a member of a custom User Group[59] that is mapped to a Security Group for any access to NNMi SNMP-managed and NPS database objects via the NNMi or NPS consoles. NNMi Administrators assign users and nodes to custom User Groups and Security Groups, respectively. Then they map each custom User Group to one or more Security Groups using Security Group Mappings. Each member of the custom User Group in a Security Group Mapping has visibility to all nodes that are part of the Security Group as well as other NNMi SNMP-managed and NPS database objects related to the hosted nodes (i.e., interfaces, connections, resolved incidents, QA probes, sites, and HPE NNM iSPI Performance for Metrics reports). TOE users that have the NNMi Global Operator role assigned can see all SNMP-managed NNMi database objects.

Execute NNMi Console menu items against one or more visible SNMP-managed NNMi database objects

In configuring each Security Group Mapping, an NNMi Administrator assigns an object access privilege that applies to all users in the custom User Group. This object access privilege must meet or exceed the default object access privilege for a menu item within the NNMi or NPS console for a user to be able to execute the associated action against a node in the Security Group or one the node's related SNMP-managed NNMi database objects. TOE users can be members of multiple custom User Groups that are mapped to the same Security Group. In that case, they receive the highest object access privilege defined by the Security Group Mappings.

View NPS database objects and HPE NNM iSPI Performance for Metrics Reports

For each TOE user, HPE NNM iSPI Performance for Metrics filters the data queries for all reports so that the TOE user can only view data for nodes that are visible in the NNMi Console.

View and execute in NPS Console

All TOE users have visibility to and can execute the NPS Console Report menu (with the exception of the Self Monitoring report option) launched via the NNMi Console Actions menu.

View and execute in QA SPI Configuration Console

TOE administrators (i.e., subjects with the NNMi Administrator role assigned) are granted full access to the QA SPI Configuration Console; otherwise, access is denied.

[59] An NNMi Administrator is granted full access to all NNMi database objects and therefore does not need to be a member of any custom User Groups.

Execute NNMi CLI
TOE administrators are granted access to the NNMi CLI based on their NNMi role and System account authorization.

Execute NNMi API
Web Services Clients (i.e., subjects with the Web Services Client role assigned) and TOE administrators are granted full access to the NNMi API; otherwise access is granted to TOE users based on their NNMi role, Custom User Groups, and Security Group Mappings. Guest role does not have access to the NNMi API.

Execute QA SPI CLI
TOE administrators are granted access to the QA SPI CLI based on their NNMi role and System account authorization.

The out-of-the-box default configuration allows all TOE users to see all nodes via a default Security Group Mapping. For the evaluated configuration, this default Security Group Mapping will be replaced with explicit access configured by an NNMi Administrator.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1

7.1.4 Identification and Authentication

User authentication can be performed in multiple ways on the TOE. System account, LDAP, and X.509/PKI certificate (including smart card) authentication is supported.

The following commands can be executed prior to identification and authentication:

- `nmsqaauthconfigreload.ovpl` – QA SPI CLI command used to apply/reload the changes made to the authentication mechanism used by the HPE NNM iSPI Performance for Quality Assurance software
- `nnmenableperfspi.ovpl` – NNMi CLI command that configures NNMi to operate with NPS

All users must be successfully identified and authenticated prior to performing any other TSF-mediated actions.

As passwords are being entered by a user at the NNMi Console, NPS Console, and QA SPI Configuration Console, the characters are masked with bullets. No feedback is provided at the NNMi API.

Security Group Mappings are stored in the NNMi database, but other attributes may be stored in either the NNMi database or LDAP/AD server depending on the mode of authentication, as explained below.

With LDAP authentication, the TOE uses an LDAP/AD server in the TOE environment to authenticate users. The distinguished name and password entered by a user in any of the TOE console's Login pages, through the NNMi API, or at the CLIs must match those in the LDAP/AD server for LDAP authentication to be successful. When the TOE is configured for LDAP authentication, "LDAP Mixed Mode" is used. In this configuration, the TOE relies on the LDAP/AD server to store usernames and passwords. User account mappings (NNMi role and custom User Group membership) are stored in the NNMi database. HPE NNMi communicates with LDAP/AD servers using LDAPS. All NPS Console, QA SPI Configuration Console, and QA SPI CLI logins are redirected to HPE NNMi for LDAP authentication.

For X.509/PKI certificate authentication, an NNMi Administrator maps a PKI (X.509 client) certificate to an NNMi user account. When the TOE is configured for X.509/PKI certificate authentication, "PKI Mixed Mode" is used. In this configuration, usernames and user account mappings are stored in the NNMi database. HPE NNMi reads the PKI certificate to obtain a user's username, which must match an NNMi user account name for successful identification and authentication at the NNMi Console, QA SPI Configuration Console, and NNMi API. X.509/PKI certificate authentication is not supported for login to the TOE's CLIs, which are only accessed locally. It is also not supported for direct login to the NPS Console from the local NNMi Management Server. However, X.509/PKI certificate authentication is supported for SSO login to the NPS Console from the NNMi Console. LDAP is not supported for some specific NNMi CLI and QA SPI CLI tools that only execute using the System account.

Users sign in to the NNMi Console by pointing their browser https://<serverName><:portNumber>/nnm/, where "serverName" is the fully-qualified domain name (FQDN) of the NNMi Management Server and "portNumber" is the NNMi HTTPS port number.

Users at the NNMi Console may access the NPS Console Report Menu (with the exception of the Self Monitoring report option) via SSO. SSO allows the NPS Console to recognize the same user names and passwords the NNMi Console recognizes. A user who is already logged on to the NNMi Console can move from it to a NPS report via the Actions menu without having to log on to the NPS Console. Alternatively, an Administrator or root user can access the NPS Console directly, without going through HPE NNMi, by starting the NPS Console at the NNM iSPI Performance for Metrics Server. As noted above, however, this method is not supported for X.509/PKI certificate authentication.

Users at the NNMi Console of a Global Manager can directly log on to the NNMi Console of a Regional Manager by selecting any node being managed by the Regional Manager and clicking **Actions → Regional Manager Console**. Since LW-SSO to the TOE is excluded in the evaluated configuration, separate authentication is required. For LDAP authentication, a username and password must be provided. For X.509/PKI authentication, the user certificate is used.

NNMi Administrators can launch the QA SPI Configuration Console from the Configuration workspace in the NNMi Console (separate login required) or directly by pointing a Web browser to the URL for the QA SPI Configuration Console, which is https://<server>:<port>/qa/Main/AdminConsole.jsp, where <server> is the FQDN of the NNMi Management Server. The HTTPS port is 54043. Since LW-SSO to the TOE is excluded in the evaluated configuration, separate authentication is required. For LDAP authentication, a username and password must be provided. For PKI authentication, the user certificate is used.

A System account is used at installation for the first access to the NNMi Console; afterwards, an NNMi Administrator account is created for management of the TOE. In the evaluated configuration, the System account is only used by authorized TOE Administrators as needed for access to the NNMi and QA SPI CLI when X.509/PKI certificate authentication is configured.

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

7.1.5 Security Management

The TOE is managed primarily by users with the NNMi Administrator role. Web Services Clients have limited (query only) management abilities as explained below.

The TOE restricts the ability to manage the following security attributes:

- NNMi roles
- Custom User Groups
- Security Groups
- Security Group Mappings

For example, an NNMi Administrator can query, add, modify, change the default of, or delete these security attributes through the use of the NNMi Console **Configuration** workspace or the `nnmsecurity.ovpl` command line tool. In addition, NNMi Administrators and Web Services Clients have query only privileges on these security attributes using the NNMi API.

In the evaluated configuration, TOE users are not provided access to user data until an NNMi Administrator has assigned them to specific custom User Groups, Security Groups, and Security Groups mappings that determine how the Resource Access Control SFP is enforced.

The TOE restricts the ability to manage TSF data to NNMi Administrators and Web Services Clients. NNMi Administrators have access to the NNMi Console **Configuration** workspace or the `nnmsecurity.ovpl` command line tool used to query, modify, or add user accounts. NNMi Administrators and Web Services Clients can get user group membership of user accounts using the NNMi API.

The default NNMi role needed for TOE user access to parts of the NNMi Console Actions and Tools menu may be modified by NNMi Administrators.

The TSF is capable of performing specific management functions, including configuring X.509/PKI certificate authentication, viewing the audit logs, managing the Resource Access Control SFP security attributes, configuring QA probes, and configuring communications between Global and Regional Managers.

NNMi Administrators configure X.509/PKI certificates using the NNMi CLI `nnmsecurity.ovpl` command.

NNMi Administrators can view the HPE NNMi, NNM iSPI Performance for Quality Assurance, and HPE NNM iSPI Performance for Metrics audit logs with the NNMi Console **Tools → NNMi Audit Log**, **Tools → QA Audit Log**, and **Tools → NPS Audit Log** menu options, respectively.

NNMi Administrators configure QA probes using either the NNMi Console **Probe Configuration** form or the QA SPI CLI `nmsqaprobeconfig.ovpl` command.

NNMi Administrators use the NNMi Console **Configuration → Global Management** view and the QA SPI Configuration Console **Global Network Management** menu item to configure communications between Global and Regional Managers.

The TSF maintains the following roles: NNMi Administrator, NNMi Level 2 Operator, NNMi Level 1 Operator, NNMi Guest, NNMi Global Operator, and Web Services Client. Users are restricted access to the TSFIs and NNMi and NPS database objects according to the Resource Access Control SFP (refer to Section 7.1.3).

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

7.1.6 Protection of the TSF

The TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. The TOE uses TLS sockets to secure communication between a Global Manager and a Regional Manager.

TOE Security Functional Requirements Satisfied: FPT_ITT.1

7.1.7 Trusted Path/Channels

The TOE provides a trusted channel between HPE NNMi and LDAP/AD servers in the TOE environment by making secure connections over TLS v1.2 using the RSA BSAFE Crypto-J JSAFE and JCE libraries. The TOE uses an LDAPS connection over TLS v1.2 for communications with the LDAP server during user authentication. The TOE also provides a trusted channel between HPE NNMi and SNMPv3 and web services managed devices in the TOE environment using the RSA BSAFE Crypto-J JSAFE and JCE libraries to provide SNMPv3 and HTTPS network packet encryption. Only the TOE is allowed to initiate these secure channel communications.

A TOE user, NNMi Administrator, or Web Services Client can initiate a secure remote connection to the TOE over an HTTPS connection. The HTTPS connection uses TLS v1.2 to protect data communications from modification or disclosure and ensures end point identification. The TOE uses FIPS-validated cryptographic algorithms to implement the above cryptographic functions.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.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 Release 4.

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 15 below provides a mapping of the objectives to the threats they counter.

Table 15 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_COMPROMISE An attacker may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	The objective O.PROTECT ensures that the TOE ensures the integrity of TSF data by protecting itself from unauthorized modifications and access.
T.INTERCEPT The TOE may communicate with remote IT entities and TOE user, TOE administrator, and Web Services Client workstations that lie outside of the organization's trusted network. An attacker may attempt to intercept these communications in order to read or modify critical TSF data.	O.AUTHENTICATE The TOE must be able to identify and authenticate users through multiple authentication mechanisms prior to allowing any access to its security functionality and data.	The objective O.AUTHENTICATE ensures that the users of the TOE must be authenticated before they are granted access to any data stored on the TOE.
	O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	The objective O.PROTECT ensures that the TOE ensures the integrity of TSF data by protecting itself from unauthorized modifications and access.
T.MASQUERADE An attacker or process may masquerade as another entity to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate users through multiple authentication mechanisms prior to allowing any access to its security functionality and data.	By ensuring that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE satisfies this threat.
T.TAMPERING An attacker or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.ADMIN The TOE must include a set of functions that allow efficient management of its security attributes and TSF data, ensuring that only authorized TOE administrators may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.

Threats	Objectives	Rationale
	O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.	O.AUDIT satisfies the threat by ensuring that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
T.UNAUTH Attackers, TOE users, or Web Services Clients may gain access to user or TSF data on the TOE, even though they are not authorized in accordance with the TOE security policy.	O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to user data stored on the TOE.	The objective O.ACCESS ensures that access control policies prevent unauthorized users from gaining access to user data stored on the TOE.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its security attributes and TSF data, ensuring that only authorized TOE administrators may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users through multiple authentication mechanisms prior to allowing any access to its security functionality and data.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining any access to TOE security data.

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

There are no Organizational Security Policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL	OE.PLATFORM	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.

Assumptions	Objectives	Rationale
The TOE is installed on the appropriate dedicated hardware and operating system.	The TOE hardware and OS must support all required TOE functions.	
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE and OS administrators who are appropriately trained and follow all administrator guidance. TOE and OS administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its 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 satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.LOCATE The TOE is located within a controlled access facility.	OE.AUTHORIZED_ACCESS Only TOE and OS administrators are granted access to the controlled access facility in which the TOE is located.	OE.AUTHORIZED_ACCESS satisfies the assumption by ensuring only authorized users have access to the controlled access facility in which the TOE is located.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE and OS administrators who are appropriately trained and follow all administrator guidance. TOE and OS administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL TOE and OS administrators are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE and OS administrators who are appropriately trained and follow all administrator guidance. TOE and OS administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.NPS_CONSOLE_PROTECT TOE users and administrators will only access the NPS Console by starting it at the NNMi Management Server (TOE administrator only)_ or through SSO access to it via the NNMi Console.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.

Assumptions	Objectives	Rationale
A.NPS_CONSOLE_PROTECT TOE users and administrators will only access the NPS Console by starting it at the NNMi Management Server (TOE administrator only) or through SSO access to it via the NNMi Console.	OE.AUTHORIZED_ACCESS Only TOE and OS administrators are granted access to the controlled access facility in which the TOE is located.	OE.AUTHORIZED_ACCESS ensures only authorized users have access to the controlled access facility and dedicated NNMi Management Server for access to the NPS Console.
A.AGENT_PROTECT Machines with SNMPv3/hypervisor agents located outside the controlled access facility are protected and no malicious software is running on them.	OE.AGENT_PROTECT Sites deploying the machines running the SNMPv3 and hypervisor agents will protect them from external interference or tampering. Administrators will ensure there is no malicious software running on them.	OE.AGENT_PROTECT ensures the sites deploying the machines running the SNMPv3 and hypervisor agents are protected from external interference or tampering and there is no malicious software running on them.
A.USER_PROTECT No malicious software is installed or running on the Administrator and TOE user workstations.	OE.USER_PROTECT The Administrator and TOE user workstations must be protected from any external interference or tampering.	OE.USER_PROTECT satisfies the assumption by ensuring that the Administrator and TOE user workstations are protected from external interference or tampering.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended Security Functional Requirements in this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended Security Functional Requirements in 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 17 below shows a mapping of the objectives and the SFRs that support them.

Table 17 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that access control is applied to all users before granting access to data stored on the TOE.

Objective	Requirements Addressing the Objective	Rationale
users from gaining access to user data stored on the TOE.	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces access control based on the implemented policy.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that only authorized administrators have the capability to modify the permissions for the access control policy.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that appropriate default values are granted for new user accounts and that only authorized administrators can modify the initial default permissions.
O.ADMIN The TOE must include a set of functions that allow efficient management of its security attributes and TSF data, ensuring that only authorized TOE administrators may exercise such control.	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts management of security attributes to only those users with the appropriate privileges.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF Data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets the objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	This requirement meets the objective by ensuring all events are associated with the TOE user or administrator that invoked the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides authorized administrators the ability to review logs.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must be able to identify and authenticate users through multiple authentication mechanisms prior to allowing any access to its security functionality and data.	FIA_ATD.1 User attribute definition	The requirement meets the objective by storing administrators' security attributes that are used for identification and authentication.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring each user is successfully authenticated before being allowed access to any TSF functionality other than the allowed CLI commands
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing both LDAP and X.509 certificate authentication mechanisms.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by obscuring feedback through the TOE's consoles during authentication.
	FIA_UID.1 Timing of identification	The requirement meets the objective by ensuring that each user is identified before being allowed access to any TSF functionality other than the allowed CLI commands.
	FMT_MTD.1 Management of TSF Data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	FCS_CKM.1 Cryptographic key generation	The requirement meets this objective by ensuring that cryptographic keys created for use by the TOE meet recommended standards for secure generation.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that cryptographic keys no longer in use by the TOE are destroyed via recommended standard key destruction methods.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE uses recommended standards for all cryptographic functionality implemented to secure communications with trusted remote IT systems, remote users, and physically separated parts of the TOE.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to all TOE functions.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by preventing password material from being obtained from an unauthorized person, thus protecting from unauthorized access.
	FIA_UID.1 Timing of identification	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this

Objective	Requirements Addressing the Objective	Rationale
		by ensuring that only identified users are allowed access to all TOE functions.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by protecting data being transferred between TOE components from disclosure and modification.
O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by providing a secure and trusted communications channel between all trusted IT products and the TOE.
	FTP_TRP.1 Trusted path	The requirement meets the objective by providing a secure communications path to all users accessing the TOE remotely.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

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 18 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 18 – 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 environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.1	No dependencies	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	No dependencies	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_ITT.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	

9. Acronyms

Table 19 defines the acronyms used throughout this document.

Table 19 – Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
CAC	Common Access Card
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DES	Data Encryption Standard
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ESR	Extended Support Release
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GB	Gigabyte
GNM	Global Network Management
GUI	Graphical User Interface
HA	High Availability
HMAC	Hash-based Messaged Authentication Code
HP	Hewlett Packard
HTML	Hyper Text Markup Language
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol

Acronym	Definition
IRA	Intelligence Response Agent
IQ	Intelligent Query
iSPI	I Smart Plug-In
IT	Information Technology
JCE	Java Cryptography Extension
JVM	Java Virtual Machine
K	Thousand
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
N/A	Not Applicable
NETCONF	Network Configuration Protocol
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NNM	Network Node Manager
NNMi	Network Node Manager i
NPS	Network Performance Server
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PP	Protection Profile
PSS	Probabilistic Signature Scheme
QA	Quality Assurance
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RAM	Random-Access Memory
RBAC	Role Based Access Control
RHEL	Red Hat Enterprise Linux
RPM	Red Hat Package Manager
RSA	Rivest, Shamir, Adelman
R2	Release 2
SAR	Security Assurance Requirement
SFP	Security Function Policy

Acronym	Definition
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SP	Security Policy
SPI	Smart Plug-in
SSO	Single Sign-On
ST	Security Target
TB	Terabyte
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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