NATEK Network

And

System Manager

NSM GUI v2.4.1 with NSM SERVER v2.3.9

Security Target

Release Date: 18.06.2015

Version 1.13

AUTHOR:

NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK
YAZILIM TİCARET SANAYİ ANONİM ŞİRKETİ

Revision History

Version No	Reason for Change	Release Date	Prepared By	Approved By
1.0	First Draft	17.10.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.1	“Survey Report 1” Update (GR_1)	04.11.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.2	“Survey Report 2” Update (GR_2)	06.11.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.3	“Survey Report 3” Update (GR_3)	07.11.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.4	SFR Update	10.12.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.5	“Survey Report 8” Update (GR_8)	18.12.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.6	“Survey Report 9” Update (GR_9)	18.12.2014	Ertuğrul BALABAN	Necati ERTUĞRUL
1.7	Product Version Update	26.01.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.8	“Survey Report 11” Update (GR_11)	03.02.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.9	“Survey Report 12” Update (GR_12)	16.02.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.10	“Survey Report 13” Update (GR_13)	24.02.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.11	“Survey Report 13-14-15-16-17-18-19” Updates	01.04.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.12	Cookie Secure Parameter and Renew Session Id	15.05.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.13	Survey Report	18.06.2015	Ertuğrul BALABAN	Necati ERTUĞRUL

TABLE OF CONTENTS

1. Introduction

The need for monitoring the status of IT systems has become an important need for organizations. Increased dependency to the IT services and requirements for better service levels create challenges for IT experts. Due to the late detection of possible problems, critical failures can have a high impact in computer infrastructure. Difficulties in measuring system performance make capacity management a difficult task.

NATEK NSM monitors the status of servers and network devices and measures the performance of IT infrastructure. It offers an integrated platform for network configuration management and application management. NATEK NSM also satisfies capacity and service level management requirements.

Structural Features

NATEK NSM is agentless. So there is no need to install software on servers. Web based drill down network and server maps offers a single interface for monitoring the IT infrastructure. System and network infrastructure can be monitored with a single solution eliminating the need for dealing with different products for managing IT infrastructure. With central event management engine, event correlation rules can be configured centrally. Integrated incident management offers an integrated platform for tracking important events. Alarms can be suppressed based on root cause. Network configuration management offers network administrators a single tool for configuring network devices with different vendors. Service levels can be defined based on monitored instances, hosts and services. Advanced auto discovery mechanism offers a simple method to discover devices and starts monitoring of managed devices automatically.

This Security Target is for evaluation of Natek Network and System Manager (NSM) at Evaluation Assurance Level 3. This section presents Security Target Identification, TOE Overview and Description. It also includes Document Conventions and Document Terminology.

1.1. Security Target Reference

ST Title:	NATEK Network and System Manager (NSM) Security Target
Version:	1.13
Publication Date:	18.06.2015
ST Author:	Natek Bilişim Bilgisayar, Eğitim, Danışmanlık, Yazılım Ticaret Sanayi Anonim Şirketi.
Assurance Level:	The ST is EAL 3 conformant.

1.2. TOE Reference

TOE Identification:	NATEK Network and System Manager (NSM)
Version:	NSM GUI 2.4.1 with NSM Server 2.3.9
Publication Date:	18.06.2015
Vendor:	Natek Corporation
Assurance Level:	The TOE is EAL 3 conformant.

1.3. TOE Overview

The TOE Description summarizes the usage and major security features. It also provides a context for the TOE Evaluation by identifying the TOE type, describing the product and defining the specific evaluated configuration.

The Target of Evaluation (TOE) is the Natek Network and System Manager (NSM) NSM GUI Version 2.4.1 with NSM SERVER v2.3.9 and will hereafter be referred to as the TOE through this document. The TOE is a network and system manager that monitors the status of servers and network devices and measures the performance of IT infrastructure. It offers an integrated platform for network configuration management and application management.

Natek NSM is software-only product for the administration of enterprise IT Environments and consists of 2 main modules; NSM GUI and NSM Server (includes NSM Health Check, NSM Scanner, NSM Alert, NSM SNMP TRAP, NSM Network Engine and NSM Analysis Server). It also provides platform-independent control over the combined IT infrastructure and the applications they support. Its architecture and design provides users a single management

approach to monitor resources. For example; network resources on the each cities on Turkey Map, can be monitored and also network resources can be shown.

TOE of the Natek NSM System should contain 5 main Security Functions which are Security Audit, User Data Protection, Identification and Authentication, Security Management and Cryptographic Support. All of these security functions will be examined in a detailed on Chapter 6.

1.3.1. TOE Type

The TOE belongs to the "Network and Network-Related Devices and Systems" category. TOE Type is software based Network and Systems Manager (Monitoring).

1.3.2. Required non-TOE Hardware, Software or Firmware

The TOE is software product that runs on a host computer. The host computer must run the operating system platform on which the TOE can execute. Natek NSM has 2 main modules; NSM GUI and NSM Server (includes NSM Health Check, NSM Scanner, NSM Alert, NSM SNMP TRAP, NSM Network Engine and NSM Analysis Server).

The minimum operating system (O/S) and hardware requirements for the NSM GUI host computer are:

O/S:	Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU:	Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM:	At least 2GB, preferably 4GB
Connectivity:	TCP/IP network interfaces
Disk space for TOE:	At least 1 GB
Disk space for logs:	Subject to Log details

The minimum operating system (O/S) and hardware requirements for the NSM Server host computer are:

O/S:	Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU:	Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM:	At least 2GB, preferably 4GB
Connectivity:	TCP/IP network interfaces
Disk space for TOE and logs:	At least 1 GB / Subject to Log details

1.3.3. Operating Environment

This section describes the general environment in which the TOE is expected to perform. The environment of operation for the TOE is expected to be a facility that is physically secure from unauthorized intrusion. Personnel with explicit physical access to the hardware storing log data and application execution files must be authorized, trained and competent. In addition to this:

For NSM GUI;

• The operational environment must include a web browser (offered Internet Explorer 8.0 or higher, or Mozilla Firefox 30.0 or higher, Google Chrome 32.0 or higher) to be used by authorized administrators of the TOE as a medium of communication with the TOE's web GUI.

• The operational environment must include .NET Framework 4.0 and IIS 7.5 or higher

• The operational environment must include the database MSSQL 2008 or higher

• The operational environment must include either Windows 2008 or Windows 2012

At a minimum, a monitor, keyboard and mouse must be locally collected to the server machine in which the TOE is deployed or operated on.

For NSM Server;

• The operational environment must include. NET Framework 4.0

• The operational environment must include the database MSSQL 2008 or higher

• The operational environment must include either Windows 2008 or Windows 2012

At a minimum, a monitor, keyboard and mouse must be locally collected to the server machine in which the TOE is deployed or operated on.

The TOE is intended to be used in cases where there is a low level of risk. The TOE is intended to protect itself against attackers assumed to be unsophisticated with access to only standard equipment and public information about the product. The EAL 3 Assurance Requirements are consistent with such an environment. There should also physical protection of TOE component host platforms that are critical to the security policy enforcement. No untrusted users or software are allowed on the host platforms of the Natek NSM components.

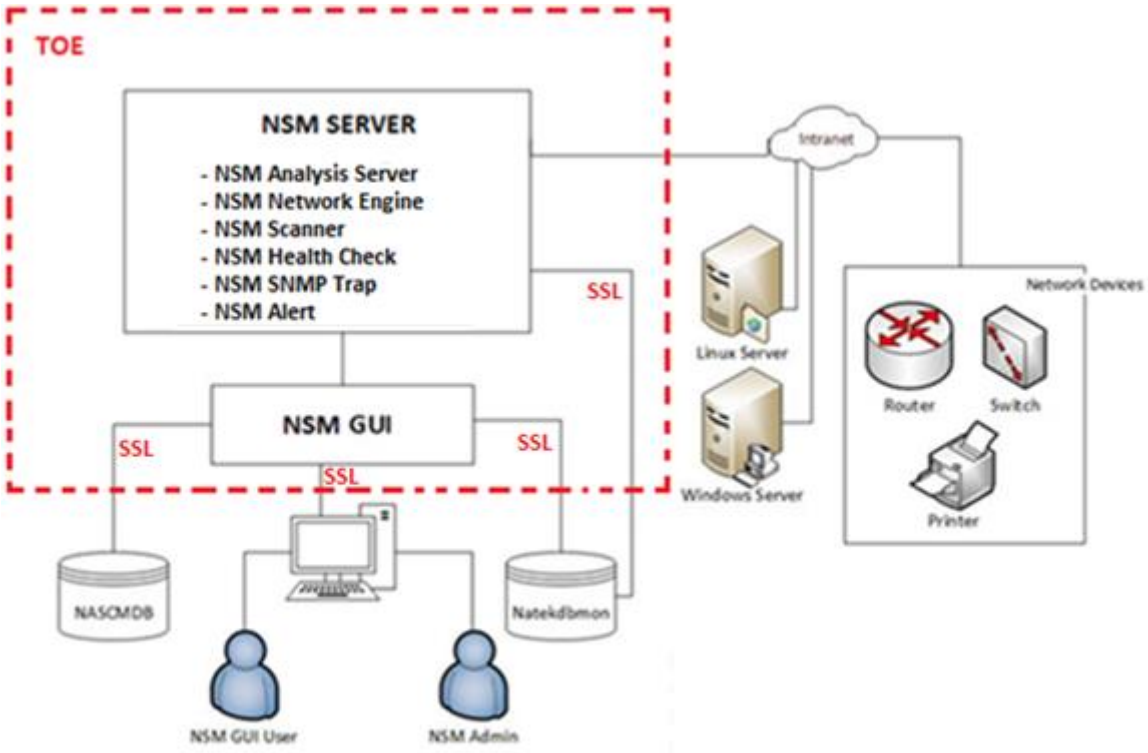
1.4. TOE Description

This section provides the detailed information and description of TOE included physical and Logical boundaries of the system.

NATEK NSM is a solution, which centrally monitors and manages the network and system infrastructure. It operates based on below scenario. There are two main components which are NSM GUI and NSM Server. NSM Server has more responsibilities and services like Analysis Server, Network Engine, Scanner, Health Check, SNMP Trap and Alert. Besides, there are also two roles for NSM GUI that NSM GUI User and NSM Base User. Each role has specified and defined authorization according to needs. Moreover, there two database to store informations which are NASCMDB and Natekdbmon. They provide to store user and network device informations and configurations. NASCMDB stores user and user related informations like username, password, roles, tickets, etc... Natekdbmon stores all NSM system operation informations like devices data, maps, alerts, etc… All these items included in the physical boundary of the system.

The TOE of Natek NSM System also provides logical boundary of the system. It depends on security audits, security functions (included cryptographic security functions), identification and authentication informations, and management functions, system and user secure interactions.

Example scenario for the system operation figured below;



Note: Two components (NSM GUI and NSM Server) of Natek NSM System should be installed same machine or server.

Natek NSM components (NSM GUI and NSM Server) connect with each other using with Natekdbmon Database. The steps of operation are as follows:

1) Admin logged in from GUI.

2) Enter the informations about network (IP Range 10.0.0.0 – 10.0.0.100) and/or host (IP Address) which will be monitored by GUI

3) Credential Informations are defined and stored for discovering of the network

4) According to the defined credential's informations, connections and classifications will be done.

5) The NSM Server identifies and classifies the device with the following methods:

- **a.** WMI; Inventory information is collected. Any WMI data can be collected, get hard disk space, username informations.
- **b.** Remote Registry; Inventory information is collected. Any key value can be enumerated.
- **c.** RPC; Calling the Procedure on Target Device, computer name is collected for classification.
- **d.** SNMP; Get inventory information from Device, MIB-2 Inventory Information is collected.
- **e.** Active Directory; Computer name is collected for classification.
- **f.** In case of company request (company decide whether to install Agent or not), Natek Agent Component installs to the target devices. Inventory information is collected. Any WMI data and registry key data can also be collected.

6) NSM Server Engine connects to the corporate network using Telnet, SSH or SNMP.

7) If classification is successful i.e., NSM Server gets information from hosts and/or networks using above methods, inventory is collected for the device.

8) According to informations taken from hosts and/or networks, monitoring will be done.

9) NSM GUI show reports the collected informations from devices like map.

10) Alarm mechanism will be available according to monitoring operations.

According to scenarios above, as a summary with the concept of the TOE, NSM GUI and NSM Server' s components have the following functions;

- NSM NetFlow Engine; collects NetFlow informations data from Cisco Devices and stored in database. It helps to report from GUI.
- NSM Analysis Server; System Decision Operations will be done.
    - SLA Management
    - Network Device Discovery
    - Network Device Interface and MIB/OID Relations
    - Switch Maps
    - Configuration Backups for monitored network devices
    - Event Manager
    - Cluster Management
    - Delete old logs from Log Folder
- NSM Health Check; checks and controls the NSM Component's status (NSM Server Engine), if one of them down, it is restarted.
- NSM SNMP Trap; listens SNMP Traps and stores. Besides, it decides to create alarms for which tarp.
- NSM Scanner Engine; scans the devices and create scanner sets.
- NSM Network Engine; collects network device discovery, topology and inventory informations.
- NSM GUI Component; provides Management, Visualization and Configuration functions of the all NSM System. (Turkey Network Map, Reports and Status of the Devices)
- NSM Alert provides to collect alarm data from related database Alarm table and send alerts.
- NASCMDB and Natekdbmon Databases;
    - NASCMDB stores user's information for controlling access to GUI.
    - Natekdbmon stores discovered device information, logs, reports and configuration information about NSM System. Other NSM Components also use Natekdbmon and all add, delete and update operations are stored in it.

1.4.1. Physical Boundary

The TOE composed of multiple software modules that run as complete IT products on required host computers. The host computers must run with an operating system platform on which the TOE executes (Please refer to the "Operating Environment). For a graphical representation of the scope and the points of interaction between the various components of the TOE also refer to the Figure above.

1.4.2. Logical Boundary

This section outlines the boundaries of the security functions of the TOE. The Logical Boundary of the TOE includes the security functionality described here.

Security Functions	DESCRIPTION
Security Audit	The TOE generates audit records for security events. Only the admin role is allowed to view the audit trail.
User Data Protection	The TOE provides specifying requirements for TOE security functions and TOE security function policies related to protecting user data.
Identification and Authentication	All users are required to perform identification and authentication before any information flows are permitted.
Security Management	The TOE provides a wide range of security management functions. Administrator can configure the TOE, manage users and audit among other routine maintenance activities.
Cryptographic Support	The TOE support cryptographic security functions for storing crucial informations for user like User Password.

1.4.2.1. Security Audit

The TOE provides for a comprehensive auditing layer, which will monitor activities and executions occurring with the system. Activities in this context are defined as operations

occurring within the system that might or might not be initiated by a user. Each auditable event marks the exact time the event occurs, the account associated with that action as well as parametric details that are specific to that activity. The data can be viewed only by administrators.

1.4.2.2. User Data Protection

The information below which are identified in TOE scope, is protected against access by unauthorized users. This information is used by Natek NSM components.

- User Information (Super Admin or other user)
- Authorization and Authentication Information (Roles, Menu, Ticket etc...)
- Configuration and Configuration Items Information (Network and Credentials etc…)
- System Logs (GUI, functions and database etc…)
- Device and Inventory Information (Scanned Device, OS, Installed Applications etc…)
- Network resources

1.4.2.3. Identification and Authentication

The TOE provides an identification and authentication layer independent from that of the Operating System it executes on. This security feature acts to protect and prevent access by unauthorized users to the system. In addition, it will also require each user to be identified and authorized before any access to security functions and data is granted. In the case of an authentication or identification failure, the TOE will disregard any request made an issue a forward redirection to the login page.

1.4.2.4. Security Management

TOE provides Security Management functions like configuration of TOE; manage the users, audit, maintenance activities etc… In the Security Management activities of the TOE uses the list below;

- Users and passwords
- Roles, Tickets, Menus
- Authentication and Authorization Mechanism
- Audit Logs

The TOE allows for the management of sessions (NSM GUI) connection. Authorized administrators are granted the ability to define user role, ticket and their relations.

1.4.2.5. Cryptographic Support

In Natek NSM System, authentication and identification is performed via a username password combination that will not only identify a specific user to the system but also define the level of access permitted to that particular user account. On top of it, the password will be encapsulated by system automatically using AES Algorithm when saved into the database (NASCMDB). Besides, discovery operations on NSM, related user data are stored by the System Administrator and these informations will also be encapsulated by system automatically using AES Algorithm.

1.5. Document Conventions

The notation formatting and conventions used in this Security Target are consistent with those used in Version 3.1 Revision 4 of the Common Criteria. Selected section choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in part 2 of the Common Criteria are selection and assignment.

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *[italicized text]*.
- The assignment operation is used to assign a specific value to an unspecified parameter to a component element. Assignments are denoted by [Blue-Colored Text]
- The iteration operation is used to denote using SFR's more than one. Iteration is denoted by SFR component title (letter). For example, FCS_COP.1(A), FCS_COP.1(B)

1.6. Document Terminology

The table below defines the acronyms used in this Security Target document of Natek NSM.

ABBREVIATION	MEANING
ACL	Access Control List
CC	Common Criteria
DAU	Data Authentication
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IT	Information Technology
MAC	Media Access Control
MIB	Management Information Base
MSA	Management of Security Attribute
NSM	Network and System Manager
OS	Operating System
OSP	Organization Security Policy
PP	Protection Profile
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMF	Specification of Management Functions
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WMI	Windows Management Instrumentation

2. Conformance Claims

This section provides the identification for any CC, Protection Profile (PP) and EAL Package Conformance Claims.

2.1. CC Conformance Claim

The ST is Common Criteria Version 3.1 (September 2012) Part 2 conformant and Part 3 conformant.

2.2. PP Claim

The ST does not claim Conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL 3 assurance Package defined in Part 3 of the Common Criteria Version 3.1 Revision 4 (September 2012). The TOE does not claim conformance to any Functional Package.

2.4. Conformance Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology

Security Evaluations, Version 3.1, Revision 4, September 2012.

There are no extended SFRs or SARs contained within this ST.

There are no Protection Profile claims for this Security Target.

3. Security Problem Definition

Roles:

NSM GUI Roles

- NSM GUI User: Uses NSM GUI Module, defines new user, makes the configurations. It has administrative authority.
- NSM Base User: Monitors the system in limited screens.

Assets:

- Configuration and device data store in the Natekdbmon. These data are directly stored to the database.
- Audit data
- User information data such as role, ticket data related to GUI. This data is stored in the NASCMDB.
- Resources on the network

Threat Agents:

- Due to the lack of system resource and cannot be monitored, provided service will be stopped.
- Because of the density in the system network resources cannot be monitored, accessibility will be lost.

3.1. Threats

- ✓ **T.ACCOUNT AUDIT-T.ACC_AUD:** An attacker from the internal network could try to modify audit data. If the audits are not controlled regularly or the audit control could be bypassed, this action may not be noticed. Thus, the attacker succeeds without being detected.

- ✓ **T.FULL AUDIT-T.FUL_AUD:** An attacker from the internal network could take actions resulting in low importance audits so as to exhaust audit storage capacity. If the audit storage capacity is exhausted, future audits are lost since no further audit could be recorded.

- ✓ **T.LOSS AND MODIFY OF DATA-T.DATALOSS/MODIFY:** An attacker from the outside or internal network may attempt to remove, destroy or modify configuration, device and user information data store in the Natekdbmon and NASCMDB.

- ✓ **T.NO AUTHORIZATION-T.NOAUTH:** An attacker from internal network may attempt to bypass the security services of the TOE so as to access and use resources on the internal network.

3.2. Organizational Security Policy

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 two main OSPs defined for this Security Target. First policy is about operational environment will provide a secure channel so that credentials are protected between the NSM users (NSM GUI User and NSM Base User) and NSM GUI application server. SSL (Secure Socket Layer) which are cryptographic protocols designed to provide communications security over a computer network, is used for communication between NSM GUI Users and NSM GUI. It provides "HTTPS" connection. Second policy is same as first policy, SSL communication is used for communication between two databases (NASCMDB and Natekdbmon) and NSM GUI. Natekdbmon database also has connection with NSM Server. That's why SSL secure connnection is also applied for communication between NSM Server and Natekdbmon database.

3.3. Assumptions

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

- ✓ **A.NO EVIL USER-A.NOEVIL:** Authorized administrator, who manage the TOE are non-hostile use, configure and maintain the TOE and follow all guidance.

- ✓ **A.EDUCATED USER-A.EDUCUSER:** Authorized administrator and end users are educated so as to use the Natek NSM system suitably and correctly.

- ✓ **A.PHYSICAL ACCESS AND PROTECTION-A.PYHPROT:** The TOE resides in a physically controlled access facility that prevents unauthorized physical Access. Therefore, the physical hardware and software in which the TOE is deployed will be protected from unauthorized physical modification.

- ✓ **A.SECURE ENVIRONMENT-A.SECENV:** The Operating Systems, Database, Application and Web Server, on which the TOE is running are, fixed against all security bugs and protected against all threats. Secure environment should include server data collection is only related with the intranet, there is no internet connection.

- ✓ **A.TRUSTED PERSON-A.TRUST:** The designer, programmer (coder) and administrator who are responsible for creation of architecture, coding and administrative functions done by trusted persons.

- ✓ **A.SCANNED DATA ACCURACY - A.DATACCUR:** Inventory information obtained after the scan operations is done for network devices and device status is assumed to be correct data and correct informations.

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

- ✓ **O.ACCOUNTABILITY-O.ACCOUN:** The TOE will provide user accountability for information flows through the TSF.

- ✓ **O.ADMINISTRATION-O.ADMIN:** The TOE will include a set of functions that allow efficient management of TSF and TSF data, ensuring that TOE users with appropriate privileges exist.

- ✓ **O.AUDIT RECORD-O.AUDREC:** The TOE will provide a means to record a readable audit trail of security related events, with accurate dates and times and means to the search the audit trail based on relevant attributes.

- ✓ **O.IDENTIFY AND AUTHENTICATE-O.IDAUTH:** The TOE will uniquely identify and authenticate the claimed identity of all users before granting a user access to TOE functions. Besides, the TOE shall define the rules for user authentication that forces users to have strong password policy.

- ✓ **O.RESOURCE ACCESS-O.RESACC:** The TOE will control access to resources based on the identity of users. The TSF must allow authorized administrators (Super Admin) to specify which resources may be accessed by which users.

- ✓ **O.CORRECT DATA - O.CORRDATA:** The TOE will provide data security and accuracy to check if data is correct or not.

- ✓ **O.SECURITY FUNCTIONS-O.SECFUN:** The TOE will provide functionality that enables an authorized administrator to use the TOE security functions and will ensure that only authorized administrator are able to access such functionality.

- ✓ **O.DATA STORAGE-O.DATASTOR:** The TOE will provide audit data storage in a secure manner. When it will be out of memory, the audit data will be deleted according to Administrator decision or stored or transferred suitable data storage.

4.2. Security Objectives for the Operational Environment

The security objectives for the Operational Environment are addressed below:

- ✓ **OE.ADMINISTRATOR AUTHENTICATION-OE.ADMAUT:** The TOE environment will be able to have administrative privilege access permission and nobody access without defined user.

- ✓ **OE.ADMINISTRATOR TRAINING-OE.ADMTRA:** Authorized administrators will be trained to appropriately install, configure and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.

- ✓ **OE.ENVIRONMENT SECURITY-OE.ENVSEC:** The Company has responsibility for the TOE will ensure that those parts of TOE should be running in a secure and protected environment.

- ✓ **OE.GUIDAN-OE.GUIDAN:** The TOE will be delivered, installed, administrated and operated in a manner that maintains security and correctly.

- ✓ **OE.TRUSTED PERSON-OE.PERTRST:** Authorized administrators, coder, designer and also service personnel will be trusted person and they will not generate any threat for the TOE.

4.3. Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats and Organizational Security Policies.

Assumption & Threats / Objectives	T.ACC_AUD	T.FUL_AUD	T.DATALOSS/ MODIFY	T.NOAUTH	A.NOEVIL	A.DATACCUR	A.EDUCUSER	A.PYHPROT	A.SECENV	A.TRUST
O.ACCOUN	✓									
O.ADMIN			✓							
O.AUDREC		✓								
O.CORRDATA	✓	✓								
O.DATASTOR		✓								
O.IDAUTH				✓						
O.RESACC		✓	✓	✓						
O.SECFUN	✓			✓						
OE.ADMTRA					✓	✓				
OE.ADMAUT			✓				✓			
OE.GUIDAN						✓	✓			
OE.ENVSEC								✓	✓	
OE.PERTRST							✓			✓

4.3.1. Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.ACC_AUD	This threat is completely countered by • O.ACCOUN which ensures user accountability for information flows through the TOE and for administrator use of security functions related to audit. • O.SECFUN which ensures the TOE provides functionality that enables an administrator to use the TOE Security Functions and also ensures that only administrator are able to access such functionality. Admin also examines the log and takes the necessary actions. • O.CORRDATA which ensures user access corrects device data informations.
T.FUL_AUD	This threat is completely countered by • O.AUDREC which ensures the TOE provide a means to record a readable audit trail of security related events, with accurate dates and times and means to the search the audit trail based on relevant attributes. • O.CORRDATA which ensures user access corrects device data informations. • O.DATASTOR which provides audit data storage in a secure manner. When it will be out of memory, the audit data will be deleted according to Administrator decision or stored or transferred suitable data storage • O.RESACC which must control access to resources based on the identity of users. The TSF must allow authorized administrators to specify which resources may be accessed by which users.
T.DATALOSS /MODIFY	This threat is completely countered by • O.ADMIN requires that only users with appropriate privileges be allowed to exercise control over the TOE's functions and data. This prevents unauthorized users from removing or destroying data collected and produced by the TOE. • O.RESACC which must control access to resources based on the identity of users. The TSF must allow authorized administrators to specify which resources may be accessed by which users. • OE.ADMAUTH which ensures the identification and authentication for administrators prior to allowing access to TOE administrative functions and data

T.NOAUTH	This threat is completely countered by • O.IDAUTH which ensures the unique identification and authenticates the claimed identity of all users before granting a user access to TOE functions. • O.RESACC which must control access to resources based on the identity of users. The TSF must allow authorized administrators to specify which resources may be accessed by which users. • O.SECFUN which ensures the TOE provides functionality that enables an administrator to use the TOE Security Functions and also ensures that only administrator are able to access such functionality. Admin also examines the log and takes the necessary actions.

4.3.2. Rationale for Security Objectives of the TOE

OBJECTIVES	RATIONALE
O.ACCOUN	This security objective is necessary to counter the threat: T.ACC_AUD because it requires that users are accountable for information flows as well as management function.
O.ADMIN	This security objective is necessary to counter the threat: T.DATALOSS which contains an unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
O.AUDREC	This security objective is necessary to counter the threat: T.FUL_AUD by requiring that the TOE provides functionality that ensures that only authorized users have access to the TOE security functions.
O.CORRDATA	This security objective is necessary to counter the threat: T.ACC_AUD and T.FUL_AUD by requiring a readable audit trail and ensures that only authorized users have access to the TOE security functions.
O.DATASTOR	This security objective is necessary to counter the threat: T.FUL_AUD by requiring that the TOE provides functionality that ensures that only authorized users have access to the TOE security functions.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that user be uniquely identified before accessing the TOE and strong password policy for user authentication.
O.RESACC	This security objective is necessary to counter the threats: T.FUL_AUD, T.DATALOSS and T.NOAUTH which consists of unauthorized access to data and resources.
O.SECFUN	This security objective is necessary to counter the threat: T.ACC_AUD by requiring a readable audit trail and T.NOAUTH because it requires that user be uniquely identified before accessing the TOE and strong password policy for user authentication.
OE.ADMAUT	This security objective is necessary to counter the threat: T.DATALOSS requires that all administrators be identified and authenticated prior to being given access to TOE administrative functions and data. This prevents unauthorized users from removing or destroying data collected and produced by the TOE. A.EDUCUSER which ensures the authorized administrator and end users are educated so as to use the Natek NSM system suitably and correctly.

OE.ADMTRA	This non-IT security objective is necessary to counter the assumption: support the assumption A.NEOVIL because it ensures that authorized administrators, receives the proper training in the correct configuration, installation and usage of the TOE.
OE.ENVSEC	This non-IT security objective is necessary for the providing environment security of the product that the TOE ensure that it is protected and it has secure environment which also provides secure channel for administrator authentication procedure. (A.SECENV and A.PYHPROT)
OE.GUIDAN	This non-IT security objective is necessary to counter the assumption: A.EDUCUSER which ensures that it is delivered, installed, administrated and operated in a secure manner and usage.
OE.PERTRST	This non-IT security objective provides reliability about personality related with the TOE security. All personnel are faithful, trained and not permit offensive attack about product. (A.TRUST and A.EDUCUSER)

5. Extended Components Definition

This section defines the extended Security Functional Requirements (SFRs) and Extended Security Assurance Requirements (SARs) met by TOE.

5.1. Extended TOE Security Functional Components

There is no Extended TOE Security Functional Components Definition in the Security Target.

5.2. Extended TOE Security Assurance Components

There is no Extended TOE Security Assurance Components Definition in the Security Target.

5.3. Rationale for Extended Security Functional Components

There is no extended Security Functional Components and Security Assurance Components that have been defined for this Security Target.

6. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE.

6.1. Security Functional Requirements

This section specifies the list of included Security Functional Requirements Components.

CLASS	CLASS FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
	FAU_ARP	Security Alarms
	FAU_SAA	Potential Violation Analysis
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Simple Security Attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ITC.2	Import of user data with security attributes
	FDP_ETC.1	Export of user data without security attributes
	FDP_ETC.2	Export of user data with security attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before any action
	FIA_UID.2	User Identification before any action
	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of Secrets
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specifications of Management Functions
	FMT_MOF.1	Management of Security Functions
	FMT_SMR.1	Security Roles
TOE Access	FTA_SSL.3	TSF Initiated termination
Cryptographic Support	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1 (A)	Cryptographic operation
	FCS_COP.1 (B)	Hash operation

SFR	Dependency	Applied
FAU_GEN.1	FPT_STM.1 Reliable Time Stamp	*FAU_GEN.1 requires that FPT_STM.1 is included as a component. However, the TOE is not capable of providing this Functionality. This functionality will be provided by a TOE Environment. Hence, FPT_STM.1 is not included.*
FAU_SAR.1	FAU_GEN.1 Audit data generation	YES
FAU_STG.1	FAU_GEN.1 Audit Data Generation	YES
FAU_STG.4	FAU_STG.1 Protected audit trail storage	YES
FAU_ARP	FAU_SAA.1 Potential Violation Analysis	YES
FAU_SAA	FAU_GEN.1 Audit Data Generation	YES
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	YES
FDP_ACF.1	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization	YES
FDP_IFC.1	FDP_IFF.1 Simple Security Attributes	YES
FDP_IFF.1	FDP_IFC.1 Subset Information Flow Control FMT_MSA.3 Static Attribute Initialisation	YES
FDP_ITC.1	[FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control] FMT_MSA.3 Static Attribute Initialisation	YES (FDP_IFC.1)
FDP_ITC.2	[FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	YES (FDP_ACC.1) *FPT_ITC.1 or FTP_TRP.1 is not included, since the data transfer is encrypted (SSL support) between NSM GUI and client* *FPT_TDC.1 is not included because the information is not included TSF data on the NSM server*

FDP_ETC.1	[FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]	YES (FDP_ACC.1)
FDP_ETC.2	[FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]	YES (FDP_ACC.1)
FIA_ATD.1	No dependencies	-
FIA_UAU.2	FIA_UID.1 Timing of identification.	YES
FIA_UID.2	No dependencies	-
FIA_AFL.1	FIA_UAU.1 Timing of Authentication dependencies.	YES FIA_UAU.2 hierarchical to FIA_UAU.1 included
FIA_SOS.1	No dependencies	-
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.	YES (FDP_ACC.1)
FMT_MSA.3	FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles	YES
FMT_MOF.1	FMT_SMR.1 Security Roles and FMT_SMF.1 Specification of Management Functions	YES
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	YES FIA_UID.2 hierarchical to FIA_UID.1 is included
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specifications of Management Functions	YES
FTA_SSL.3	No dependencies	-

FCS_COP.1 (A)-Enc/Dec Operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	YES (FDP_ITC.1 andFDP_ITC.2) *The dependcy for FCS_CKM.4 is not met for component since TOE does not destruct the keys. AES keys stored on the TOE are protected by A.PYHPROT, A.NOEVIL and A.TRUST assumptions which specify that the TOE is deployed in a physically secure Location and TOE is implemented by trusted person and managed by trusted admin.*
FCS_COP.1 (B)-Hash Operation	[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	YES (FDP_ITC.1 and FDP_ITC.2) *Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys.*

6.1.1. Class Security Audit (FAU)

6.1.1.1. FAU_GEN.1 – Audit Data Generation

Description: Audit Data Generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamp

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)** [User access, database events and Exceptions]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- **a)** Date and time of 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, [event message according to event type].

6.1.1.2. FAU_SAR.1 – Audit Review

Description: Audit review, provides the capability to read information from the audit records.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1 The TSF shall provide [NSM Admin] with the capability to read [all recorded audit information] from the audit records.

6.1.1.3. FAU_STG.1 – Protected Audit Trail Storage

Description: Prevention of audit data loss, specifies actions in case the audit trail is full.

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 unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *[prevent]* unauthorised modifications to the stored audit records in the audit trail.

6.1.1.4. FAU_STG.4 – Prevention of Audit Data Loss

Description: Prevention of audit data loss, specifies actions in case the audit trail is full.

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 [system auto detect for system storage capacity and delete old logs automatically] if the audit trail is full.

6.1.1.5. FAU_ARP.1 – Security Alarms

Description: Security alarms, the TSF shall take actions in case a potential security violation is detected.

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential Violation Analysis

FAU_ARP.1.1 The TSF shall take [sending alarms] upon detection of a potential security violation.

6.1.1.6. FAU_SAA.1 – Potential Violation Analysis

Description: Potential violation analysis, basic threshold detection on the basis of a fixed rule set is required.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [auditable events] known to indicate a potential security violation;

6.1.2. Class User Data Protection (FDP)

6.1.2.1. FDP_ACC.1 Subset Access Control

Description: Subset access control, requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on

[Subjects: users attempting to establish and interactive session with the TOE,

Objects: user interface items, NSM authentication and authorization configurations,

Operations: all interactions between the subjects and objects identified above].

6.1.2.2. FDP_ACF.1 Security Attribute Based Access Control

Description: Security attribute based access control Security attribute based access control allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes

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 [Administrative access control SFP] to objects based on the following:

[Subject attribute:

1. User Role,
2. User ID,
3. User's Tickets.

Object attributes:

1. Permissions assigned objects,

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[If the subject is the TOE Administrator, then access is granted,

1. If the subject request access to an object and subject has permission the object, then access is granted,
2. If none of the above rules apply, access is denied].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [no additional rules].

6.1.2.3. FDP_IFC.1 Subset Information Flow Control

Description: Subset information flow control, requires that each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE.

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple Security Attributes

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [

a) SUBJECTS: Network Devices that receive information through the TOE,

b) INFORMATION: receive information and send query

c) OPERATIONS: allow or deny].

RPC, WMI, SNMP, SSH and Telnet Protocols

6.1.2.4. FDP_IFF.1 Simple Security Attribute

Description: Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function, and describes how security attributes are derived by the function.

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset Information Flow Control

FMT_MSA.3 Static Attribute Initialisation

FDP_IFF.1.1 The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes:

[SUBJECT attributes:

1) IP Address

INFORMATION (traffic) attributes:

1) Source IP address,

2) Destination IP address,

3) Protocol type,

4) Port number, and

5) Port types or subtypes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

NSM Server connection establishment is allowed, if

- IP address = acceptable
- Protocol type = RPC, WMI, SNMP, SSH and Telnet Protocols].

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.2.5. FDP_ITC.1 Import of User Data without Security Attributes

Description: Import of user data without security attributes, requires that the security attributes correctly represent the user data and are supplied separately from the object.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]

FMT_MSA.3 Static Attribute Initialisation

FDP_ITC.1.1 The TSF shall enforce the [information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from.

6.1.2.6. FDP_ITC.2 Import of User Data with Security Attributes

Description: Import of user data with security attributes, requires that security attributes correctly represent the user data and are accurately and unambiguously associated with the user data imported from outside the TOE. Besides, credential informations should contains FDP_IFF to import user data with security attribute.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce [Administrative Access Control SFP] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

6.1.2.7. FDP_ETC.1 Export of User Data without Security Attributes

Description: Export of user data without security attributes, requires that the TSF enforce the appropriate SFPs when exporting user data outside the TSF. User data that is exported by this function is exported without its associated security attributes.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]

FDP_ETC.1.1 The TSF shall enforce the [information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.1.2.8. FDP_ETC.2 Export of User Data with Security Attributes

Description: Export of user data with security attributes, requires that the TSF enforce the appropriate SFPs using a function that accurately and unambiguously associates security attributes with the user data that is exported. Besides, credential informations should contains FDP_IFF to export user data with security attribute

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]

FDP_ETC.2.1 The TSF shall enforce the [Administrative Access Control SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

6.1.3. Class Identification and Authentication (FIA)

6.1.3.1. FIA_ATD.1 – User Attribute Definition

Description: User attribute definition, allows user security attributes for each user to be maintained individually.

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: [Authorization status as determined by the TOE, User role, User ID].

6.1.3.2. FIA_UAU.2 – User Authentication before any Action

Description: User authentication before any action, requires that users are authenticated before any other action will be allowed by the TSF.

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.1 Timing of identification.

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

6.1.3.3. FIA_UID.2 – User Identification before any Action

Description: User identification before any action, requires that users identify themselves before any other action will be allowed by the TSF.

Hierarchical to: FIA_UID.1 Timing of authentication.

Dependencies: No dependencies.

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

6.1.3.4. FIA_AFL.1 – Authentication Failure Handling

Description: Authentication failure handling requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs.

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication dependencies.

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within* [3] unsuccessful authentication attempts occur related to [user logon].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [Captcha Validation].

6.1.3.5 FIA_SOS.1 – Verification of Secrets

Description: Secrets can be generated by the user. This component ensures that those user generated secrets can be verified to meet a certain quality metric. This component allows the TSF to generate secrets for specific functions such as authentication by means of user authentication passwords.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

a) Should be at least 8 characters long,

b) Should contain at least three of following:

- uppercase letter,
- lowercase letter,
- number,
- symbol].

6.1.3. Class Security Management (FMT)

6.1.3.1. FMT_MSA.1 – Management of Security Attribute

Description: Management of security attributes allows authorized users (roles) to manage the specified security attributes.

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to *[query, modify, delete]* the security attributes [user role, user ID, user tickets, and permissions assigned objects] to [NSM admin].

6.1.3.2. FMT_MSA.3 – Static Attribute Initialization

Description: Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

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 [Administrative 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 [NSM admin] to specify alternative initial values to override the default values when an object or information is created.

6.1.3.3. FMT_MOF.1 – Management of Security Functions Behaviour

Description: Management of security functions behaviour allows the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable and enable*] the functions [password policy flag] to [admin and authorized by admin].

Application Note: The password policy is defined under the FIA_SOS.1 SFR.

6.1.3.4. FMT_SMF.1 – Specification of Management Functions

Description: Specification of Management Functions requires that the TSF provide specific 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: [Create, Delete, Modify and View security attribute values, enable and disable External IT entities from communicating to the TOE, review of audit trail].

6.1.3.5. FMT_SMR.1 – Security Roles

Description: Security roles specify the roles with respect to security that the TSF recognizes.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [NSM GUI User and NSM Base User].

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

6.1.3.6. FMT_MTD.1 – Management of TSF data

Description: Management of TSF data allows authorised users to manage TSF data.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [luser information] to [NSM Admin].

6.1.4. Class TOE Access (FTA)

6.1.4.1. FTA_SSL.3 TSF Initiated Termination

Description: TSF-initiated termination provides requirements for the TSF to terminate the session after a specified period of user inactivity.

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after [a logout or a specified time interval of user inactivity set by an authorized administrator. The default cookie session timeout value is 1 hour and it can be updated by user but, default session timeout value which is 20 minute can not updated.].

6.1.5. Class Cryptographic support (FCS)

6.1.5.1. FCS_COP.1 (A) Cryptographic Operation – Enc/Dec Operation

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

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 [Encryption and Decryption Operation] in accordance with a specified cryptographic algorithm [AES operating in CBC mode] and cryptographic key sizes [256 bit] that meet the following: [FIPS 140-2 and Annex A, NIST FIBS 197].

6.1.5.2. FCS_COP.1 (B) Cryptographic Operation – Hash Operation

Description: Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys.

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 [Hash Operations] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [none] that meet the following: [FIPS 180-2].

6.2. Security Assurance Requirements

EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behavior.

The assurance security Requirements for the Security Target are taken from Part 3 of the CC v.3.1 Revision 4 September 2012. These assurance requirements compose an Evaluation Assurance Level 3 (EAL 3). The assurance components are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural Design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorization Control
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component 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 specifications
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.3. Security Functional Requirements Rationale

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

Objective / SFR	O.ACCOUN	O.ADMIN	O.AUDREC	O.CORRDATA	O.DATASTOR	O.IDAUTH	O.RESACC	O.SECFUN
FAU_GEN.1	✓		✓		✓			
FAU_SAR.1	✓		✓		✓			
FAU_STG.1	✓		✓		✓		✓	
FAU_STG.4			✓		✓		✓	
FAU_ARP.1	✓		✓					
FAU_SAA.1	✓		✓					
FDP_ACC.1		✓					✓	
FDP_ACF.1		✓					✓	
FDP_IFC.1	✓			✓	✓			
FDP_IFF.1	✓			✓	✓			
FDP_ITC.1		✓		✓			✓	
FDP_ITC.2		✓		✓			✓	
FDP_ETC.1		✓		✓			✓	
FDP_ETC.2		✓		✓			✓	
FIA_ATD.1						✓	✓	
FIA_UAU.2						✓	✓	
FIA_UID.2	✓					✓	✓	
FIA_AFL.1						✓		
FIA_SOS.1						✓		
FMT_MSA.1					✓		✓	✓
FMT_MSA.3					✓		✓	✓
FMT_MOF.1								✓
FMT_SMF.1								✓
FMT_SMR.1							✓	✓
FMT_MTD.1	✓						✓	
FTA_SSL.3								✓
FCS_COP.1 (A)					✓	✓	✓	
FCS_COP.1 (B)				✓	✓			

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC, O.ACCOUN and O.DATASTOR.
FAU_SAR.1	This requirement provides the ability to review logs. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN and O.DATASTOR.
FAU_STG.1	This requirement is placed on the audit trail. It will be protected from unauthorised deletion and/or modification. This component traces back to and aids in meeting the following objectives: O.AUDREC, O.ACCOUN, O.DATASTOR and O.RESACC.
FAU_STG.4	This requirement specifies actions in case the audit trail is full and prevents the audit data loss. This component traces back to and aids in meeting the following objectives: O.RESACC, O.AUDREC and O.DATASTOR.
FAU_ARP.1	This requirement defines the response to be taken in case of detected events indicative of a potential security violation. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
FAU_SAA.1	This requirement defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to a potential security violation. It meets the following objectives: O.AUDREC and O.ACCOUN.
FDP_ACC.1	This requirement defines subjects, objects and operations controlled by the Natek Access Control Policy. This component traces back to and aids in meeting the following objectives: O.ADMIN and O.RESACC.
FDP_ACF.1	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the Administrative Access Control SFP. This component traces back to and aids in meeting the following objectives: O.RESACC. This component also identifies control access to resources based on the subject attributes of users. The TSF must allow authorized administrators (Super Admin) to specify which resources may be accessed by which users. This component traces back to and aids in meeting the following objectives: O.ADMIN

FDP_IFC.1	This component identifies the information flow control SFPs and defines the scope of control for each named information flow control SFP. Each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE. This component traces back to and aids in meeting the following objectives: O.ACCOUN, O.CORRDATA and O.DATASTOR.
FDP_IFF.1	This component describes the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy. This component traces back to and aids in meeting the following objectives: O.ACCOUN, O.CORRDATA and O.DATASTOR.
FDP_ITC.1	This requirement defines the mechanisms for TSF-mediated importing of user data (without security attribute) into the TOE such that it has appropriate security attributes and is appropriately protected. This component traces back to and aids in meeting the following objectives: O.ADMIN, O.CORRDATA and O.RESACC.
FDP_ITC.2	This requirement defines the mechanisms for TSF-mediated importing of user data (with security attribute) into the TOE such that it has appropriate security attributes and is appropriately protected. This component traces back to and aids in meeting the following objectives: O.ADMIN, O.CORRDATA and O.RESACC.
FDP_ETC.1	This requirement defines functions for TSF-mediated exporting of user data (without security attribute) from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. This component traces back to and aids in meeting the following objectives: O.ADMIN, O.CORRDATA and O.RESACC.
FDP_ETC.2	This requirement defines functions for TSF-mediated exporting of user data (with security attribute) from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. This component traces back to and aids in meeting the following objectives: O.ADMIN, O.CORRDATA and O.RESACC.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH This component also identifies control access to resources based on the subject attribute of users. This component traces back to and aids in meeting the following objectives: O.RESACC

FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and such aids in meeting O.IDAUTH. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and such aids in meeting O.IDAUTH and O.ACCOUN This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
FIA_AFL.1	This component contains requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. This component traces back to and aids in meeting the following objectives: O.IDAUTH
FIA_SOS.1	This component can be used to ensure that the external generated secret adheres to certain standards, for example user authentication strong password policy. This component traces back to and aids in meeting the following objectives: O.IDAUTH
FMT_MSA.1	This component restricts the ability to modify, delete, or query object and subject security attributes for the Administrative Access Control SFP to super admin. It also assists in effective management and such as aids in meeting O.SECFUN and O.DATASTOR. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
FMT_MSA.3	This component ensures that the TOE provides a default restrictive value for security attributes, yet allows a super admin to override the default values. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.DATASTOR. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
FMT_MOF.1	This component ensures that the TOE provides a default restrictive value for security attributes, yet allows a super admin to override the default values. This component traces back to and aids in meeting the following objectives: O.SECFUN.

FMT_SMF.1	This component was chosen to consolidate all TOE management, administration and security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
FMT_MTD.1	This component allows authorised users (roles) control over the management of TSF data, for example change password operation. This component traces back to and aids in meeting the following objectives: O.ACCOUN and O.RESACC.
FTA_SSL.3	This component ensures that TOE terminates interactive session after specified time interval of user inactivity set by an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN
FCS_COP.1 (A)	This requirement includes data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.RESACC and O.DATASTOR.
FCS_COP.1 (B)	This requirement includes data encryption and/or decryption, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement. This component traces back to and aids in meeting the following objectives: O.DATASTOR and O.CORRDATA.

6.4. Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

ASSURANCE REQUIREMENTS	EVIDENCE
ASE_INT.1 Security Target Introduction	Security Target: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ASE_CCL.1 Conformance Claim	Security Target: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ASE_SPD.1 Security Problem Definition	Security Target: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ASE_OBJ.1 Security Objectives	Security Target: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ASE_REQ.2 Security Requirements	Security Target: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ADV_ARC.1 Security architecture description	Security and Design Architecture: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ADV_FSP.3 Functional specification with complete summary	Functional Specification: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ADV_TDS.2 Architectural Design	Security and Design Architecture: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
AGD_OPE.1 Operational user guidance	Operational User Guide: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
AGD_PRE.1 Preparative procedures	Installation and Delivery: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ALC_CMC.3 Authorization Control	Configuration Management: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ALC_CMS.3 Implementation Representation CM coverage	Configuration Management: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ALC_DEL.1 Delivery procedures	Installation and Delivery: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ALC_DVS.1Identification of Security Measures	Development Environment Security: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ALC_LCD.1 Developer defined life-Cycle model	Software Life-Cycle: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ATE_COV.2 Analysis of Coverage	Testing Plan and Analysis: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9

ATE_DPT.1 Testing: Basic Design	Testing Plan and Analysis: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
ATE_FUN.1 Functional Testing	Testing Plan and Analysis: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9
AVA_VAN.1 Vulnerability Analysis	Vulnerability Tests: Natek Network and System Manager NSM GUI v2.4.1 with NSM Server v2.3.9

6.5. Security Assurance Requirements Rationale

The general level of assurance for the TOE consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market. Besides, TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria. Therefore EAL 3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices.

7. TOE Summary Specifications

This section presents the Security Functions implemented by the TOE.

7.1. TOE Security Functions

The Security functions performed by the TOE are as follows:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Cryptographic support

7.1.1. Security Audit

The TOE generates a set of audit logs. These logs are stored on the database and administrator can also view them to a local machine.

The TOE generates Local Logs for the following list of events:

- All user of user identification and authentication mechanism, which includes the user identities provided to the TOE in each related log;
- All user database interactions logs like Create, Update, Delete Operations;
- All system Exception logs within any failure

The logs are only accessible through the Web-Based Administrative interface, which only authorized operators can access. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based Administrative interface.

The Security Audit functions are designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details. The log which is generated by this security function also includes Time Stamp value.
- FAU_ARP.1: TOE provides ability to generate security alarms for the configured alerts on monitored devices.
- FAU_SAR.1: TOE provides ability to review logs.
- FAU_STG.4: TOE provides logs storage management capability.

- FAU_SAA.1: TOE provides to specify the set of auditable events whose occurrence or accumulated occurrence held to indicate a potential violation of the enforcement of the SFRs, and any rules to be used to perform the violation analysis.

7.1.2. User Data Protection

Natek NSM determines access to the management functions for users identifying and authenticating to the TOE through the Natek NSM GUI. Administrators are given access to functions based on their User ID, User Role, Group ID, Ticket ID, User's configured permissions, and Group's configured permissions. If the administrator's permissions match the permissions assigned to the object to which the administrator is attempting access, then that access is granted. Otherwise, it is denied. (Administrative Control SFP)

The User Data Protection functions are designed to satisfy the following security functional requirements:

- FDP_ACC.1: This component ensures that the access control policies are enforced on all operations among subjects and objects in the Administrative Access Control SFP.
- FDP_ACF.1: This component ensures that permissions and privileges can be granted to specific subjects and objects for different accesses according to Administrative Access Control SFP.
- FDP_IFC.1: This component requires that an information flow control policy apply to a subset of the possible operations in the TOE.
- FDP_IFF.1: This component requires security attributes on information, and on subjects that cause that information to flow and subjects that act as recipients of that information.
- FDP_ITC.1: This component is used to specify the import of user data that does not have reliable security attributes associated with it. This function requires that the security attributes for the imported user data be initialised within the TSF.
- FDP_ITC.2: This component is used to specify the import of user data that has reliable security attributes associated with it. This function relies upon the security attributes that are accurately associated with the objects on the import medium.
- FDP_ETC.1: This component is used to specify the TSF-mediated exporting of user data without the export of its security attributes.

- FDP_ETC.2: The user data is exported together with its security attributes. The security attributes are unambiguously associated with the user data. There are several ways of achieving this association.

7.1.3. Identification and Authentication

The TOE performs identification and authentication of all users and administrators accessing the TOE. The TOE has the ability to authenticated users locally using a password or can integrate with a remote authentication server. Users enter a username and password, which is validated by the TOE against the user information stored by the database. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: For each registered user, the TOE stores the following information:
  - User Identity
  - User Name
  - User Roles
  - Password
- FIA_UAU.2: The TOE requires a valid password associated with a username before providing access to the TOE.
- FIA_UID.2: The TOE requires a username during the identification and authentication Process. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username.
- FIA_AFL.1: The session establishment process is the interaction with the user to perform the session establishment independent of the actual implementation. If the number of unsuccessful authentication attempts exceeds the indicated threshold (3 times), either the captcha will be shown.
- FIA_SOS.1 The TOE requires a strong password policy for user authentication and it should contain at least 8 characters long and include at least three of uppercase, lowercase, number and symbol.

7.1.4. Security Management

The TOE provides security management functions via browser interface. The Administrator logs on to the TOE perform all management functions through the browser interface. The administrator has the ability to control all aspects of the TOE configuration including:

- User Management
- Audit Management

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: This component restricts the ability to modify, delete or query the subject and object security attributes for the Administrative Access Control SFP to the super admin role
- FMT_MSA.3: TOE provides restrictive default values for security attributes specified in FDP_ACF.1
- FMT_SMF.1: The TOE supports the following security management functions:
    - System and Service Start-up and Shutdown
    - Create, Delete, Modify and View user attribute values, which include a user's identity, association and authentication credentials.
    - Enable and Disable External IT entities from communicating to the TOE.
    - Review the Audit Records
    - Configure authorization rules
- FMT_SMR.1: The TOE supports the roles NSM GUI User and NSM Base User for limited administrator role user.
    - The NSM GUI User role can perform all management functionalities. The administrator dynamically sets up user roles and access rules associated with the roles.
    - The NSM Base User role can perform limited functionalities according to permitted authorization.
- FMT_MTD.1: This component allows users with a certain role to manage values of TSF data. The users are assigned to a role within the component FMT_SMR.1 Security roles.

- FMT_MOF.1: This component allows identified roles to manage the security functions of the TSF. This might entail obtaining the current status of a security function, disabling or enabling the security function, or modifying the behaviour of the security function.

- FTA_SSL.3: TOE terminates interactive session after specified time interval of user inactivity set by an authorized administrator. Default value is 1 hour.

7.1.5. Cryptographic Support

- FCS_COP.1 (A): This component requires the cryptographic algorithm and key size used to perform specified cryptographic operation which can be based on an assigned standard.

- FCS_COP.1 (B): This component requires the hash operation which can be based on an assigned standard.