NetIQ Identity Manager 4.7

Security Target (ST)

Date:	June 1, 2020
Version:	2.6
Prepared By:	NetIQ Corporation
Prepared For:	NetIQ Corporation 515 Post Oak Blvd Suite 1200 Houston, Texas 77027

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Identity Manager 4.7. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1. Security Target Reference:

ST Title	NetIQ Identity Manager 4.7 Security Target:
ST Revision	2.6
ST Publication Date	June 1, 2020
ST Author	Michael F. Angelo

1.2. TOE Reference

TOE Reference	NetIQ Identity Manager 4.7
TOE Developer	NetIQ Corporation
Evaluation Assurance Level (EAL)	EAL3+

Note: The file download name is: Identity_Manager_4.7_Linux.iso .
Note: The official name of the product is NetIQ Identity Manager 4.7 Advanced Edition. The released product can be uniquely identified as: NetIQ Identity Manager 4.7.3. The product name may also be abbreviated as Identity Manager 4.7 AE, Identity Manager, IDM 4.7.3AE or IDM 4.7 or simply IDM . Finally the TOE, if examined for the build number will be identified as NetIQ Identity Manager 4.7.3.0.317. For the purpose of this document all of the above references are equivalent, and the document may refer to the product simply as IDM or the TOE.

1.3. Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE

SECTION	TITLE	DESCRIPTION
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4. Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation 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 *refinement, selection, assignment* and *iteration*.

- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- 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, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5. Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
IDM	Identity Manager
IDV	Identity Vault
IGA	Identity Governance and Administration
NMAS	NetIQ Modular Authentication Service
NTP	Network Time Protocol
ORSP	Organizational Security Policy
OSP	One SSO Provider
SSO	Single Sign On
SFP	Security Function Policy
SFR	Security Functional Requirement
SLM	Sentinel Log Manager

TERM	DEFINITION
SSPR	Self Service Password Reset
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 2 – Acronyms Used in Security Target

1.6. TOE Overview

The TOE is NetIQ Identity Manager 4.7. NetIQ Identity Manager provides data sharing and synchronization services which enable applications, directories, and databases to share information. It links scattered information and enables you to establish policies that govern automatic updates to designated systems when identity changes occur.

Identity Manager provides the foundation for account provisioning, security, single sign-on, user self-service, authentication, authorization, automated workflow, and Web services. It allows you to integrate, manage, and control your distributed identity information so you can securely deliver the right resources to the right people.

The following diagram shows a typical TOE deployment:

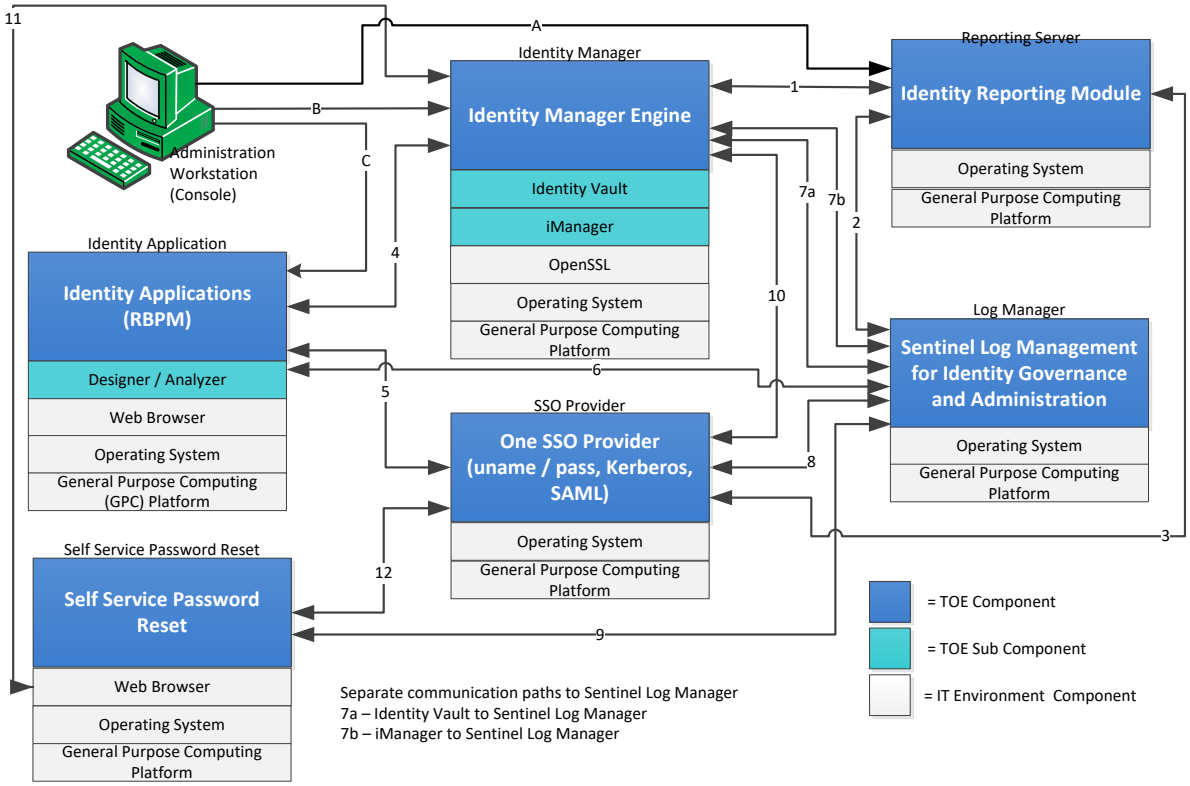


Figure 1 – TOE Deployment with Subsystems[1]

The TOE provides the following functions: data synchronization, role management, auditing/reporting, and management.

[11] Note the Administration Workstation Console is not included in the evaluation as there is no code that is added to it to make it explicitly a workstation console. It is included in the document as a component required for access.to the TOE.

- Data synchronization, including password synchronization, is provided by the base components of the Identity Manager solution: the Identity Vault, Identity Manager engine, drivers, Remote Loader, and connected applications
- Role management is provided by the User Application
- Auditing and reporting are provided by the Identity Reporting Module

1.7. TOE Description

NetIQ Identity Manager 4.7 is a comprehensive identity management suite. It provides an intelligent identity framework that leverages your existing IT assets and new computing models like Software as a Service (SaaS) by reducing cost and ensuring compliance across physical, virtual, and cloud environments. With the NetIQ Identity Manager solution, you can make sure that your business has the most current user identity information. You can retain control at the enterprise level by managing, provisioning, and de-provisioning identities within the firewall and extending to the cloud. Through streamlined user administration and processes, Identity Manager helps organizations reduce management costs, increase productivity and security, and comply with government regulations.
The TOE is a software TOE and includes the following functions.

Each function contains the components as follows:

1. Administration Workstation (Console)[2]
2. Identity Applications (RBPM) 4.7.3.0.1109
   - Designer aka Identity Manager Designer 4.7.3.0.20190614
   - Analyzer aka Identity Manager Analyzer
3. Identity Manager
   - Identity Manager Engine 4.7.3.0.AE
     - Identity Vault 9.1.4
     - iManager 3.1.4
4. Reporting Server
   - Identity Reporting Module 6.5.0. F14508F
5. Log Manager
   - Sentinel Log Management for Identity Governance and Administration 8.2.2.0_5415
6. SSO Provider
   - One SSO Provider (OSP) 6.3.3.0
7. Self Service Password Reset
   - Self Service Password Reset (SSPR) 4.4.0.2 B366 r39762

1.7.1. Administration Workstation (Console):

The Administration Workstation (Console) is used to access the Identity Applications (RBPM), Identity Manager, and the Reporting Server. Each of these functions is described below.

1.7.2. Identity Applications (RBPM)

The Identity Applications (RBPM) houses the Designer / Analyzer functions. The Identity Application is a Web application (browser-based) that gives users and business administrators the ability to perform a variety of identity self-service and roles provisioning tasks, including managing passwords and identity data, initiating and monitoring provisioning and role assignment requests, managing the approval process for provisioning requests, and verifying

[2] The Administration Workstation (Console) is not part of the TOE, in that there is no code added to it in order to function as the Console it is required to access features and function of the TOE and is included for completeness.

attestation reports. It includes the workflow engine that controls the routing of requests through the appropriate approval process. Designer aka Designer for Identity Manager helps you design, test, document, and deploy Identity Manager solutions in a network or test environment. Analyzer aka NetIQ Analyzer for Identity Manager is an identity management toolset that helps you ensure that internal data quality policies are adhered to by providing data analysis, data cleansing, data reconciliation, and data monitoring/reporting. Analyzer lets you analyze, enhance, and control all data stores throughout the enterprise.

1.7.3. Identity Manager:

The Identity Manager houses the Identity Manager Engine (and the Identity Vault which contains the Identity Applications data) and iManager. The Identity Manager Engine synchronizes identity data between applications. For example, data synchronized from a PeopleSoft system to Lotus Notes is first added to the Identity Vault and then sent to the Lotus Notes system. In addition, the Identity Vault stores information specific to Identity Manager, such as driver configurations, parameters, and policies.

The following packages are used to provide cryptographic functions, and are not included in the TOE boundary. NetIQ eDirectory is used for the Identity Vault. eDirectory provides access to the OpenSSL Cryptographic functionality.

They meet the cryptographic quality requirements as evidenced by the following certificates:

Component	CAVP Cert #
AES	Certs. #3090 and #3264
HMAC	Certs. #1937 and #2063
RSA	Certs. #1581 and #1664

Table 3 – CAVP Certificate Numbers

1.7.4. Reporting Server:

The reporting server houses the Identity Reporting Module. The Identity Reporting Module generates reports that show critical business information about various aspects of your Identity Manager configuration, including information collected from Identity Vaults and managed systems such as Active Directory or SAP. The reporting module provides a set of predefined report definitions you can use to generate reports. In addition, it gives you the option to import custom reports defined in a third-party tool. The user interface for the reporting module makes it easy to schedule reports to run at off-peak times to optimize performance.

The IDM Tools are used to manage the Identity Manager solution. This includes functions to:

- Analyze, enhance, and control all data stores throughout the enterprise
- Design, deploy, and document the TOE
- Manage Identity Manager and receive real-time health and status information about the Identity Manager system
- Define and maintain which authorizations are associated with which business roles

1.7.5. Log Manager:

The Log Manager, also known as Sentinel Log Manager for Identity Governance and Administration (SLM for IGA), collects and acknowledges receipt of auditing data from all aspects of the product.

1.7.6. OneSSO Provider:

The OneSSO Provider, also known as OSP) is a single interface for access authentication. This provider can handle user name / password, Kerberos, and SAML tokens.

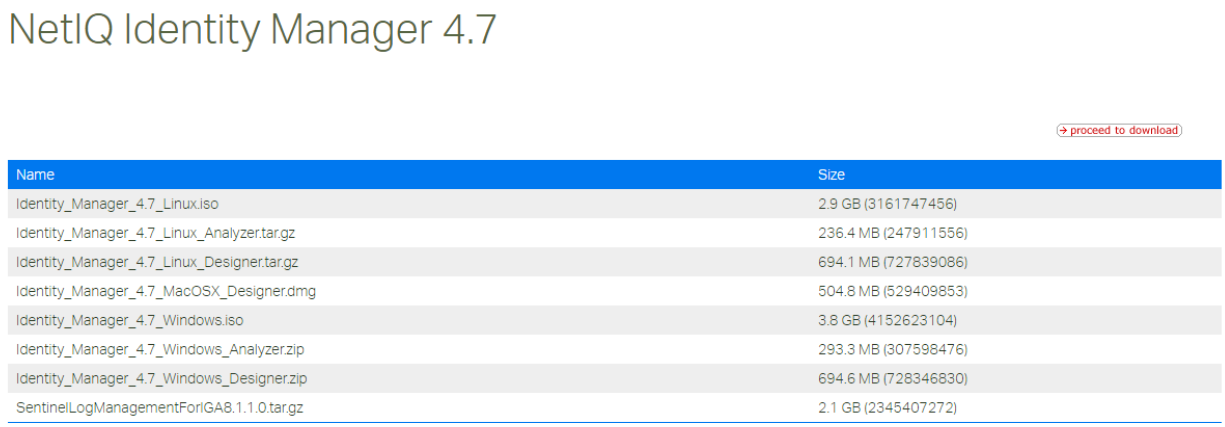
1.7.7. Self Service Password Reset:

Self Service Password Reset (SSPR) allows users to enroll, update, and reset their passwords without administrative intervention in the Identity Vault (IDV).

Note: that the components above can be installed on one or multiple distributed systems. Also, the hardware, operating systems and third-party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

1.7.8. TOE Delivery:

The TOE software is provided to customers via secure download from the download portal (https://dl.netiq.com/index.jsp). The software is available as either a gnu zip (.gz), iso formatted optical disk (.iso). zip (.zip) or dmg (if mac) depending on your destination platform. Once downloaded, and extracted, the setup files can be executed to perform the installation.


NetIQ Identity Manager 4.7

proceed to download

Name	Size
Identity_Manager_4.7_Linux.iso	2.9 GB (3161747456)
Identity_Manager_4.7_Linux_Analyzer.tar.gz	236.4 MB (247911556)
Identity_Manager_4.7_Linux_Designer.tar.gz	694.1 MB (727839086)
Identity_Manager_4.7_MacOSX_Designer.dmg	504.8 MB (529409853)
Identity_Manager_4.7_Windows.iso	3.8 GB (4152623104)
Identity_Manager_4.7_Windows_Analyzer.zip	293.3 MB (307598476)
Identity_Manager_4.7_Windows_Designer.zip	694.6 MB (728346830)
SentinelLogManagementForIGA8.1.1.0.tar.gz	2.1 GB (2345407272)

Figure 2 – Sample Download List

1.8. TOE Environment

1.8.1. Virtual Machines

The following TOE components can be installed in virtual machines (VM).

- Console / Administration Workstation (Identity Applications)
- Identity Manager
- Reporting Server
- Sentinel Log Manager
- One SSO Provider
- Self Service Password Reset (SSPR)

The hardware and software requirements for the operational environment to support the VM are listed in the table below:

Category	Console / Administration Workstation (Identity Applications[3])	Identity Manager (Identity Manager Engine)	Reporting Server (Identity Reporting Module)	Log Manager (SLM for Identity Gov & Adm)	SSO Provider (OneSSO Provider)	Self Service Password Reset (SSPR)
Processor	**2 CPU cores**	**2 CPU cores**	**2 CPU cores**	**4 to 8 CPU cores**	**2 CPU cores**	**2 CPU cores**
Memory	**8 GB**	**8 GB**	**8 GB**	**8 to 16 GB**	**8 GB**	**8 GB**

Table 4 – Virtual Machine Environment Requirements

1.8.2. Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications run on one or multiple distributed systems. The TOE requires the following software components as part of the evaluated configuration:

Component	Requirements
Administration Workstation	Mozilla Firefox 65
Identity Applications (RBPM) Designer / Analyzer)	SUSE Linux Enterprise Server 12 SP4
Identity Manager (Identity Manager Engine)	SUSE Linux Enterprise Server 12 SP4
Reporting Server (Identity Reporting Module)	SUSE Linux Enterprise Server 12 SP4
Log Manager (Sentinel Log Management for Identity Governance and Administration)	SUSE Linux Enterprise Server 12 SP4
SSO Provider (OneSSO Provider)	SUSE Linux Enterprise Server 12 SP4
Self Service Password Reset	SUSE Linux Enterprise Server 12 SP4

Table 5 – IT Environment Component Requirements

In addition to the platform requirements mentioned above, the following hardware resources are needed in order to install and configure Identity Manager on each platform:

- A minimum of 8 GB RAM
- 15 GB available disk space to install all the components.
- Additional disk space to configure and populate data. This might vary depending on your connected systems and number of objects in the Identity Vault.

For server-based components, it is recommended that the platform have a minimum of 2 CPUs or cores

1.8.3. Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

[3] The system requirements also apply to the following components that you use with the identity applications: PostgreSQL, Tomcat, NetIQ One SSO Provider (OSP), and NetIQ Self Service Password Reset.

TSF	DESCRIPTION
Security Management	The TOE restricts the ability to enable, modify and disable security policy rules and user roles to an authorized Administrator. The TOE also provides the functions necessary for effective management of the TOE security functions. Administrators configure the TOE with the Management Console via Web-based connection.
Security Audit	The TOE supports the provision of log data from each system component, such as user login/logout and incident/ticket management actions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis.
Cryptographic Support	The TOE utilizes the OpenSSL cryptographic module to provide support for HTTPS / TLS communications with administrators and TOE components.
Identification and Authentication	The TOE enforces individual I&A. Operators must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.
User Data Protection	The TOE enforces discretionary access rules using an access control list with user attributes.
Trusted Path / Channels	The TOE utilizes HTTPS/TLS to provide trusted paths and inter-TSF trusted channels.

Table 6 – Logical Boundary Descriptions

1.8.4. TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

1.8.4.1. Discretionary Access Control SFP

The TOE implements an access control SFP named *Discretionary Access Control SFP*. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the Management Console.

1.8.5. TOE Vendor Documentation / Guidance

In addition to the documentation generated for the certification, the TOE includes the following product and guidance documentation generated by NetIQ:

- Quick Start Guide for Installing NetIQ Identity Manager 4.7 February 2018
- NetIQ Identity Manager Setup Guide for Linux February 2018
- NetIQ Identity Manager 4.7, Operational User Guidance and Preparative Procedures Supplement (AGD-IGS), version 0.6, is supplied for those customers that need guidance on how to set the TOE in the evaluated configuration.

1.8.6. Features / Functionality NOT Included in the TOE

The following supported operating systems and software were not included in the evaluated configuration:

Functions	Requirements
Administration Workstation (Console)	Web Browsers

Functions	Requirements
	• Internet Explorer 11 • Google Chrome
Identity Applications (Includes Designer / Analyzer)	RHEL 7.5 Windows Server 2016
Identity Manager (Includes Identity Vault and, iManager)	RHEL 7.5 Windows Server 2016
Reporting Server (includes Identity Reporting Module)	RHEL 7.5 Windows Server 2016
Log Manager (includes Sentinel Log Management for Identity Governance and Administration)	RHEL 7.5
One SSO Provider (uname / pass, Kerberos, SAML)	RHEL 7.5 Windows Server 2016
Self Service Password Reset (SSPR)	RHEL 7.5 Windows Server 2016

Table 7 – IT Environment Components - Not In TOE

2. Conformance Claims

2.1. CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 conformant and Part 3 conformant.

2.2. PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 5 (April 2017). The TOE does not claim conformance to any functional package. The TOE EAL3 assurance package is augmented with ALC_FLR.2

2.4. Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1. Threats

The following are threats identified for the TOE and the IT System (or operating environment) the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.
T.USER_ACCESS_DENY	An authorized user may be able to change user authentication data and or user access policies and deny their access to it later.
T.PASSWD_COMPROMISE	An unauthorized user may be able to obtain and use user passwords.
T.PROT_TRANS	An unauthorized user may be able to gather information from communications between components.

Table 8 – Threats Addressed by the TOE

3.2. Organizational Security Policies

The TOE meets the following organizational security policies:

ASSUMPTION	DESCRIPTION
P.REMOTE_DATA	Passwords and account information from network-attached systems shall be monitored and managed.

Table 9 – Organizational Security Policies

3.3. Assumptions

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access
A.CONFIG	The TOE is configured to receive all passwords and associated data from network-attached systems.
A.TIMESOURCE	The TOE has a trusted source for system time via NTP server

Table 10 – Assumptions

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.MANAGE_DATA	The TOE shall provide a means to manage secrets and data associated with remote IT systems.
O.MANAGE_POLICY	The TOE shall provide a workflow to manage authentication and access control policies.
O.SEC_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data.
O.PASSWD_PROT	The TOE shall provide cryptographic mechanisms to protect passwords via cryptographic processes including the ability to generate and destroy keys.
O.TRANS_PROT	The TOE shall provide mechanisms to protect data that is in transit between elements within the TOE.

Table 11 – TOE Security Objectives

4.2. Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed
OE.PERSONNEL	Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility

Table 12 – Operational Environment Security Objectives

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.

OBJECTIVES THREATS/ ASSUMPTIONS/ POLICIES	O.MANAGE_DATA	O.MANAGE_POLICY	O.SEC_ACCESS	O.PASSWD_PROT	O.TRANS_PROT	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC
A.CONFIG							✓	✓	✓
A.MANAGE								✓	
A.NOEVIL								✓	
A.LOCATE									✓
A.TIMESOURCE						✓			
T.NO_AUTH			✓						
T.NO_PRIV			✓						
T.USER_ACCESS_DENY		✓							
T.PASSWD_COMPROMISE				✓					
T.PROT_TRANS					✓				
P. REMOTE_DATA	✓								

Table 13 – Mapping of Assumptions, Threats, Policies and ORSP s to Security Objectives

4.3.1. Mapping of Objectives

ASSUMPTION /THREAT/ POLICY	RATIONALE
A.CONFIG	This assumption is addressed by • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed • OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility

ASSUMPTION /THREAT/ POLICY	RATIONALE
A.MANAGE	This assumption is addressed by • OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.LOCATE	This assumption is addressed by OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.
T.NO_AUTH	This threat is countered by the following: • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications
T.NO_PRIV	This threat is countered by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
T.PASSWD_COMPROMISE	This threat is countered by O.PASSWD_PROT, which ensures the passwords are not in the clear and cannot be exposed to un authorized users for use.
T.PROT_TRANS	This threat is countered by O.TRANS_PROT, which protects data that is in transit between elements within the TOE.
P.REMOTE_DATA	This organizational security policy is enforced by • O.MANAGE_DATA, which ensures that the TOE provide a means to manage secrets and data associated with remote IT systems.
T.USER_ACCESS_DENY	This threat is countered by O.MANAGE_POLICY which ensures that the TOE provides a workflow to manage authentication and access control policies.

Table 14 – Mapping of Threats, Policies, and Assumptions to Objectives

5. Extended Components Definition

This Security Target does include any extended components.

6. Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1. Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
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_UID.2	User Identification before Any Action
	FIA_UAU.2	User Authentication before Any Action
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_TDC.1	Inter-TSF basic TSF data consistency
Trusted Path / Channels	FTP_ITC.1	Trusted Channel
	FTP_TRP.1	Trusted Path

Table 15 – TOE Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. FAU_GEN.1 Audit Data Generation

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 login/logout and;

d) Login failures;]

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

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

6.1.1.2. FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator] with the capability to read [all audit data generated within the TOE] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.2. Cryptographic Support

6.1.2.1. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [cryptographic key generation algorithm in Table 16] and specified cryptographic key sizes [cryptographic key sizes in Table 16] that meet the following: [list of standards in Table 16].

Usage	Key Generation Algorithm	Key Size (bits), Elliptical Curves	Standard
RSA	RSA Key Generation	2048	FIPS 186-4
AES	Deterministic Random Bit Generator (DRBG)	128, 256	SP 800-90A
Diffie-Hellman	Diffie-Hellman Key Generation	1024, 2048	FIPS 186-4

Table 16 – Cryptographic Standards

6.1.2.2. FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroize] that meets the following: [FIPS 140-2].

6.1.2.3. FCS_COP.1 Cryptographic operation (Encryption / Decryption)

FCS_COP.1.1 The TSF shall perform [cryptographic operations in Table 17] in accordance with a specified cryptographic algorithm [cryptographic algorithm in Table 17] and cryptographic key sizes [cryptographic key sizes in Table 17] that meet the following: [list of standards in Table 17].

Application Note: AES in CBC mode is used for encrypting/decrypting data in support of TLS.

Operation	Algorithm	Key Size, Curve or Digest	Standard
Encryption and Decryption in support of TLS	AES (Advanced Encryption Standard)	128, 256	FIPS PUB 197
Key agreement in support TLS	Key Agreement Schemes (KAS) and Key Confirmation	P-256, P384, P521	SP800-56A
Authentication algorithm in support of TLS	ECDSA (Elliptic Curve Digital Signature Algorithm)	P-256, P384, P521	FIPS 186-4
Secure Hashing in support of TLS	Secure Hash Algorithm (SHA)	160 (SHA-1) 256 (SHA-256) 384 (SHA-384)	FIPS PUB 180-4
Message Authentication in support of TLS	Keyed-Hash Message Authentication Code (HMAC)	160 (HMAC-SHA1) 256 (HMAC-SHA2-256) 384 (HMAC-SHA2-384)	FIPS 198-1
Asymmetric cryptography in support of TLS	Rivest, Shamir, Adleman (RSA)	2048	FIPS 186-4

Table 17 – Cryptographic Operations

6.1.3. Information Flow Control (FDP)

6.1.3.1. FDP_ACC.1 Subset Access Control

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

Subjects: All users

Objects: System reports, component audit logs, TOE configuration, operator account attributes
Operations: all user actions]

6.1.3.2. FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Discretionary Access Control SFP]to objects based on the following: [

Subjects: All users

Objects: System reports, component audit logs, TOE configuration, operator account attributes

Operations: all user actions]

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

ACL identifies the user or a group of users that contains the user requesting access for the type of resource that the user is requesting, and the user (or group of users) has the specific rights required for the type of operation requested on the object then the user is granted access].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [password restrictions, login restrictions, time based access controls, ip access controls, intruder lockout].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules [password restrictions, login restrictions, time based access controls, ip access controls, intruder lockout]

6.1.4. Identification and Authentication (FIA)

6.1.4.1. FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Status, and Privilege Level].

6.1.4.2. FIA_UAU.2 User Authentication before Any Action

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.

6.1.4.3. FIA_UID.2 User Identification before Any Action

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.

6.1.5. Security Management (FMT)

6.1.5.1. FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Discretionary Access Control SFP] to restrict the ability to [*query, modify, delete*] the security attributes [Accounts, privileges, ACLs] to [Administrator].

6.1.5.2. FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [security attributes listed with Discretionary Access Control SFP].

6.1.5.3. FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Discretionary 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 [Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*control*] the [data described in the table below] to [Administrator]:

DATA	CHANGE	QUERY	MODIFY	DELETE	CLEAR
Discretionary Access Control SFP	✓	✓	✓	✓	✓
User Account Attributes		✓	✓		
Audit Logs		✓			
Date/Time			✓		

Table 18 – Management of TSF data

6.1.5.5. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) Create accounts

b) Modify accounts

c) Define privilege levels Change Default, Query, Modify, Delete, Clear the attributes associated with the Discretionary Access Control SFP

d) Modify the behavior of the Discretionary Access Control SFP

e) Manage ACLs].

6.1.5.6. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, User].

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

6.1.6. Protection of the TSF (FPT)

6.1.6.1. FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [secrets (passwords)] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [the secret with the newest associated timestamp] when interpreting the TSF data from another trusted IT product.

6.1.7. Trusted Path / Channel (FTP)

6.1.7.1. FTP_ITC.1 Inter-TSF trusted channel

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 [HTTPS/TLS connections • for communications labeled 1 – 12 in Figure 1] Application Note: The TOE supports TLS v1.1 and 1.2 as configured by the Administrator. Application Note: Crypto as claimed in FCS_COP_1 is used to support TLS.

6.1.7.2. FTP_TRP.1 Trusted Path

FTP_TRP.1.1	The TSF shall provide a communication path between itself and [local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure].
FTP_TRP.1.2	The TSF shall permit [the TSF] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [key requests, and encryption operations • for communications labeled A, B, and C in Figure 1]

6.2. Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.3.4 – Security Assurance Requirements.

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements

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

SFR \ OBJECTIVE	O.MANAGE_DATA	O.MANAGE_POLICY	O.SEC_ACCESS	O.PASSWD_PROT	O.TRANS_PROT
FAU_GEN.1		✓			
FAU_SAR.1		✓			
FCS_CKM.1				✓	
FCS_CKM.4				✓	
FCS_COP.1				✓	
FDP_ACC.1			✓		
FDP_ACF.1			✓		
FIA_ATD.1			✓		
FIA_UID.2			✓		
FIA_UAU.2			✓		
FMT_MSA.1			✓		
FMT_MSA.2			✓		
FMT_MSA.3			✓		
FMT_MTD.1			✓		
FMT_SMF.1		✓			
FMT_SMR.1		✓			
FPT_TDC.1	✓				
FTP_ITC.1					✓
FTP_TRP.1					✓

Table 19 – Mapping of TOE Security Functional Requirements and Objectives

6.3.2. Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Satisfied by the Operational Environment (OE.TIME)
FAU_SAR.1	FAU_GEN.1 FPT_STM.1	YES	FPT_STM.1 satisfied by the Operational Environment (OE.TIME)

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FCS_CKM.1	FCS_CKM.1 or FCS_COP.1 and FCS_CKM.4	YES	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1	YES	Satisfied by FCS_CKM.1 for AES
FCS_COP.1	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1 and FCS_CKM.4	YES	Satisfied by FCS_CKM.1 and FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	YES	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	YES	
FIA_ATD.1	N/A	N/A	
FIA_UID.2	N/A	N/A	
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	YES	
FMT_MSA.2	FDP_ACC.1 FMT_MSA.1 FMT_SMR.1	YES	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_TDC.1	N/A	N/A	
FTP_ITC.1	N/A	N/A	
FTP_TRP.1	N/A	N/A	

Table 20 – Mapping of SFR to Dependencies and Rationales

6.3.3. Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

OBJECTIVE	RATIONALE
O.MANAGE_DATA	The objective to ensure that the TOE will collect events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events is met by the following security requirements: • FPT_TDC.1 ensures that the TOE provides consistency between passwords used on remote IT systems and those stored/managed within the TOE.
O.MANAGE_POLICY	The objective to ensure that the TOE provides a workflow to manage authentication and access control policies is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for incidents and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role
O.SEC_ACCESS	This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privilege level and their allowable actions • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to configuration of the TOE • FIA_ATD.1 specifies security attributes for users of the TOE • FMT_MTD.1 restricts the ability to query, add or modify TSF data to authorized users. • FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data. • FMT_MSA.2 specifies that only secure values are accepted for security attributes listed with access control policies. • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE • FTP_ITC.1 specifies that the trusted channel exists for components HTTPS/TLS. • FTP_TRP.1 specifies that the trusted path exists for components HTTPS/TLS.

OBJECTIVE	RATIONALE
O.PASSWD_PROT	This objective ensures that the TOE provides cryptographic mechanisms to generate and destroy keys. This objective is met by: FCS_CKM.1, FCS_CKM. 4, and FCS_COP.1 which provide the cryptographic support functions for secure communications within the TOE and with external IT entities.
O.TRANS_PROT	This objective ensures that the TOE protects data in transit between elements within the TOE. This objective is met by FTP_ITC (which specifies that the trusted channel exists for components) and FTP_TRP (which ensures that the trusted path exists for components).

Table 21 – Rationale for TOE SFRs to Objectives

6.3.4. Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	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: Lifecycle Support	ALC_CMC.3	Authorization Controls
	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
	ALC_FLR.2	Flaw Reporting Procedures
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

Table 22 – Security Assurance Requirements at EAL3

6.3.5. Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface,

offering essentially no opportunity for an attacker to subvert the security policies without physical access. The product was augmented to comply with ALC_FLR.2 in order to document and address requirements for remediation and reporting of faults that may be discovered in the product after release.

6.3.6. Security Assurance Requirements Evidence

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

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	NetIQ Identity Manager 4.7 Security Architecture (ADV_ARC)
ADV_FSP.3 Functional Specification with Complete Summary	NetIQ Identity Manager 4.7 Functional Specification (ADV_FSP)
ADV_TDS.2 Architectural Design	NetIQ Identity Manager 4.7 Architectural Design (IDM TDS)
AGD_OPE.1 Operational User Guidance[4]	NetIQ Identity Manager 4.7 Operational User Guidance and Preparative Procedures Supplement (AGD-IGS)
AGD_PRE.1Preparative Procedures	NetIQ Identity Manager 4.7 Operational User Guidance and Preparative Procedures Supplement (AGD-IGS)
ALC_CMC.3 Authorization Controls	NetIQ Identity Manager 4.7 Configuration Management Processes and Procedures (ALC_CM)
ALC_CMS.3 Implementation representation CM coverage	NetIQ Identity Manager 4.7 Configuration Management Processes and Procedures (ALC_CM)
ALC_DEL.1 Delivery Procedures	NetIQ Identity Manager 4.7 Secure Delivery Processes and Procedures (ALC_DEL)
ALC_DVS.1 Identification of Security Measures	NetIQ Identity Manager 4.7 Development Security Measures (ALC_DVS)
ALC_LCD.1 Developer defined life-cycle model	NetIQ Identity Manager 4.7 Life Cycle Development Process (ALC_LCD)
ALC_FLR.2: Flaw Remediation Procedures	NetIQ Identity Manager 4.7 Flaw reporting Procedures (ALC_FLR)
ATE_COV.2 Analysis of Coverage	NetIQ Identity Manager 4.7 Test Plan and Coverage Analysis (ATE)
ATE_DPT.1 Testing: Basic Design	NetIQ Identity Manager 4.7 Test Plan and Coverage Analysis (ATE)

[4] Additional documents can be found in Appendix A

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ATE_FUN.1Functional Testing	NetIQ Identity Manager 4.7 Test Plan and Coverage Analysis (ATE)

Table 23 – Security Assurance Rationale and Measures

7. TOE Summary Specification

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 Management
- Security Audit
- Identification and Authentication
- User Data Protection
- Trusted Path / Channels
- Cryptographic Support

7.2. Security Audit

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions (instantiated by startup of the TOE)
- User login/logout
- Login failures

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the console. The GUI provides a suitable means for an Administrator to interpret the information from the audit log.

The A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date provided by the operational environment are used to form the timestamps. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

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

- FAU_GEN.1
- FAU_SAR.1

7.3. Identification and Authentication

The IDM console application provides user interfaces that administrators may use to manage TOE functions. The operating system and the database in the TOE Environment are queried to individually authenticate administrators or users. The TOE maintains authorization information that determines which TOE functions an authenticated administrators or users (of a given role) may perform.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Authentication Status (whether the IT Environment validated the username/password)
- Privilege Level (Administrator or User)

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

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

7.4. User Data Protection

The TOE implements a discretionary access control policy to define what roles can access particular functions of the TOE. All access and actions for system reports, component audit logs, TOE configuration, operator account attributes (defined in FIA_ATD.1) are protected via access control list. When a user requests to perform an action on an object, the TOE verifies the role associated with the user name. Access is granted if the user (or group of users) has the specific rights required for the type of operation requested on the object.

Identity Manager can enforce password policies on incoming passwords from connected systems and on passwords set or changed through the User Application password self-service. If the new password does not comply, you can specify that Identity Manager not accept the password. This also means that passwords that don't comply with your policies are not distributed to other connected systems.

In addition, can enforce password policies on connected systems. If the password being published to the Identity Vault does not comply with rules in a policy, you can specify that Identity Manager not only does not accept the password for distribution, but actually resets the noncompliant password on the connected system by using the current Distribution password in the Identity Vault.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1
- FPT_TDC.1

7.5. Security Management

The TOE maintains the operator roles described in the following table. The individual roles are categorized into two main roles: the Administrator and the User.

ROLE	MANAGEMENT FUNCTIONS
Administrator	A user who has rights to configure and manage all aspects of the TOE
User	The user's capabilities can be configured to: View hierarchical relationships between User objects View and edit user information (with appropriate rights). Search for users or resources using advanced search criteria (which can be saved for later reuse). Recover forgotten passwords.

Table 24 – Roles and Functions

Only an Administrator can determine the behavior of, disable, enable, and modify the behavior of the functions that implement the Discretionary Access Control SFP. The TPE ensures only secure values are accepted for the security attributes listed with Discretionary Access Control SFP.

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

- FMT_MTD.1
- FMT_MSA.1
- FMT_MSA.2
- FMT_MSA.3
- FMT_SMF.1
- FMT_SMR.1

7.6. Trusted Path / Channels

The Trusted Path/Channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1 – the TOE supports establishment of trusted channels for communicating TOE entities using HTTPS.
- FTP_TRP.1 – the TOE provides a trusted path for TOE Users, using HTTPS

7.6.1. Trusted Channel

The TOE provides a trusted channel between the TOE and external web servers.

Trusted channels are implemented using HTTPS. The TOE supports TLS v1.1 and TLS v1.2. The TOE supports the following TLS cipher suites, as defined in RFC 2246, RFC 4346 and RFC 5246:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_ CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

7.6.2. Trusted Path:

The TOE provides a trusted path for TOE administrators and TOE users to communicate with the TOE. The trusted path is implemented using HTTPS. The TOE's implementation of TLS is described in the previous section (Trusted Channel).

7.7. Cryptographic Support

Cryptographic protection of data in transit between the TOE and remote users, and between the TOE and external web servers is provided by the OpenSSL FIPS Object Module software version 2.0.10 (Cryptographic Module Validation Program (CMVP) certificate number 1747) libraries.

The following table identifies the CAVP algorithm certificates.

Operation	Algorithm	CAVP Certificate
Encryption and Decryption in support of TLS	AES (Advanced Encryption Standard)	AES 3264
Key Generation in support of TLS	DRBG (Deterministic Random Bit Generation)	DRBG 723
Key agreement in support of TLS	Key Agreement Schemes (KAS) and Key Confirmation	CVL 472
Keyed-Hash Message Authentication in support of TLS	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384	HMAC 2063
Secure Hash in support of TLS	SHA-1, SHA-256, SHA-384	SHS 2702

Asymmetric cryptography in support of TLS	RSA	RSA 1664
Authentication algorithm in support of TLS	ECDSA	ECDSA 620

Table 25 – CAVP

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1