NetIQ® Identity Manager™ 4.5

Security Target

Date: *February 25h, 2015*
Version: *2.2*
Prepared By: *NetIQ Corporation*
Prepared For: *NetIQ Corporation*
515 Post Oak Blvd
Suite 1200
Houston, Texas 77027

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 ST Reference

ST Title	Security Target: NetIQ® Identity Manager™ 4.5
ST Revision	*2.2*
ST Publication Date	February 25th, 2015
ST Author	Michael F. Angelo 713-418-5396 angelom@netiq.com

1.2 TOE Reference

TOE Reference	NetIQ® Identity Manager™ 4.5
TOE Developer:	NetIQ Corporation
Evaluation Assurance Level (EAL):	EAL 3+

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
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 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)].
- 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.
- 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
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

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™ 4.5. 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.

Note: The official name of the product is NetIQ® Identity Manager™ 4.5 Advanced Edition. The released product can be uniquely identified as: NetIQ® Identity Manager™4.5.0. The product name may also be abbreviated as *Identity Manager* 4.5 *AE, Identity Manager, IDM45# AE* or *IDM4.5* or simply *IDM*. Finally the TOE, if examined for the build number will be identified as NetIQ Identity Manager 4.5.0.42199. 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*.

The following diagram shows a typical TOE deployment:

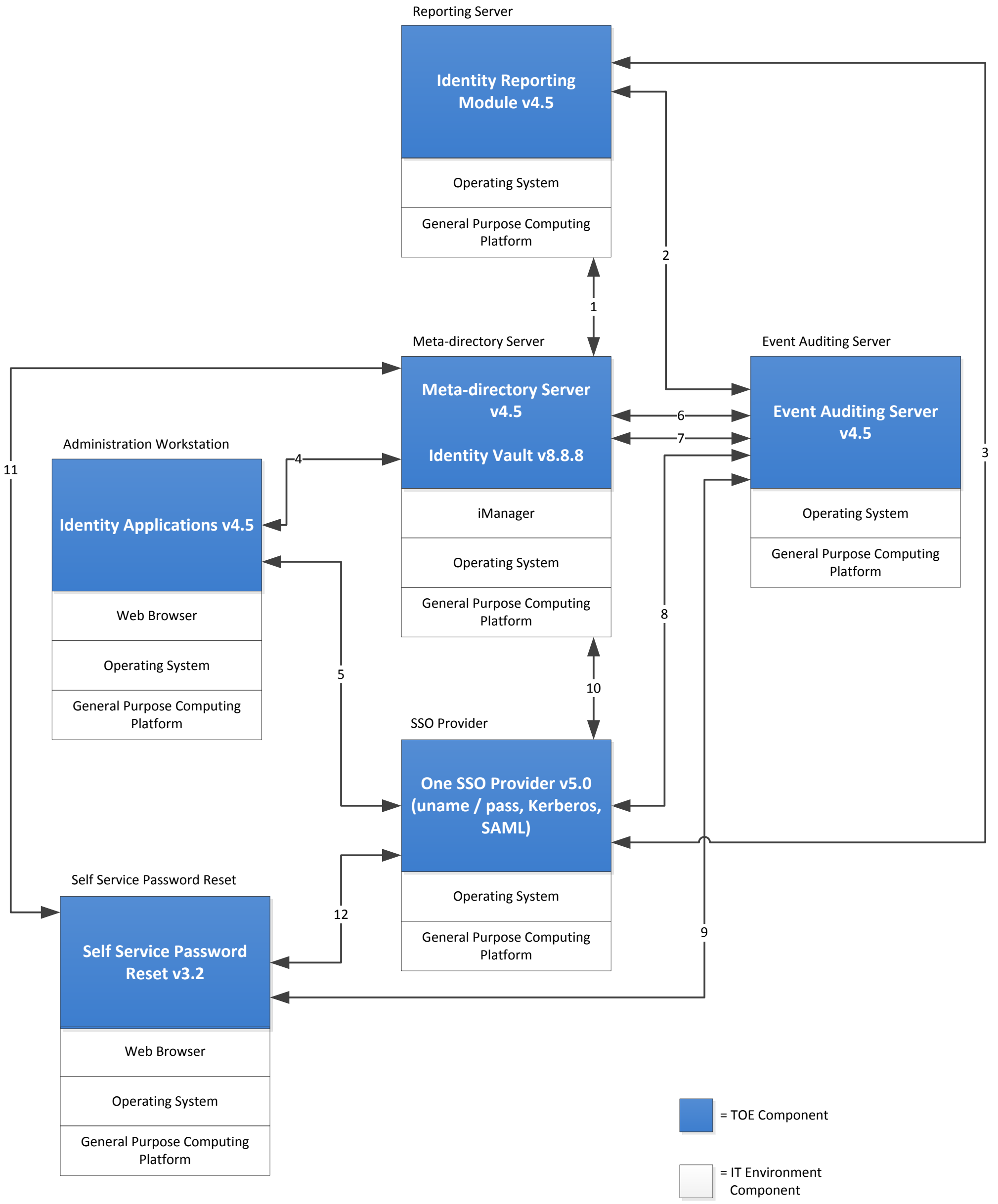
Reporting Server
Identity Reporting Module v4.5
Operating System
General Purpose Computing Platform
Meta-directory Server
Meta-directory Server v4.5
Identity Vault v8.8.8
iManager
Operating System
General Purpose Computing Platform
Event Auditing Server
Event Auditing Server v4.5
Operating System
General Purpose Computing Platform
Administration Workstation
Identity Applications v4.5
Web Browser
Operating System
General Purpose Computing Platform
SSO Provider
One SSO Provider v5.0 (uname / pass, Kerberos, SAML)
Operating System
General Purpose Computing Platform
Self Service Password Reset
Self Service Password Reset v3.2
Web Browser
Operating System
General Purpose Computing Platform
1
2
3
4
5
6
7
8
9
10
11
12
= TOE Component
= IT Environment Component

Figure 1 - TOE Deployment

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

- Data synchronization, including password synchronization, is provided by the five 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 is provided by the Identity Reporting Module
- TOE management is provided by IDM Tools.

1.7 TOE Description

NetIQ® Identity Manager™ 4.5 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 components:

- Meta-directory Server which includes the Identity Vault and Meta-Directory functionality
  - Meta-directory Server (v4.5)
  - Identity Vault (v8.8.8) (inc Catalog Administrator data)
- Identity Application (v4.5.0) (in Administration Workstation)
  - User Application
  - Home and Provisioning Dashboard
  - Catalog Administrator
- Identity Reporting Module (v4.5.0) (in Reporting Server)
- Event Auditing Server (v4.5.0)
- One SSO Provider (v5.0.0)
- Self Service Password Reset (v3.2 b61 r38380)

1.7.1 Meta-directory Server:

The Meta-directory Server[1] (including the Identity Vault which contains the Catalog Administrator data) 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. NetIQ® eDirectory is used for the Identity Vault.

1.7.2 Identity Application:

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 attestation reports. It includes the workflow engine that controls the routing of requests through the appropriate approval process.

1.7.3 Identity Reporting Module (in Reporting Server):

The Identity Reporting Module generates reports that show critical business information about various aspects of your Identity Manager configuration, including information collected from

[1] The combined Meta-Directory Server and Identity Vault are also referred to as the Identity Engine

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. Incudes 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

1.7.4 Event Auditing Server:

The Event Auditing Server collects and acknowledges receipt of auditing data from all aspects of the product.

1.7.5 SSO Provider:

The SSO Provider (also referred to as One SSO Provider) is a single interface for access authentication. This provider can handle user name / password, Kerberos, and SAML tokens.

1.7.6 Self Service Password Reset (SSPR):

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.

1.8 TOE Environment

1.8.1 Virtual Machines

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

- NetIQ® Identity Applications
- NetIQ® Reporting Server
- NetIQ® Meta-directory Server which includes the Identity Vault(which contains the Catalog Administrator data), and Meta-Directory functionality
- NetIQ® Event Auditing Server
- NetIQ® One SSO Provider
- NetIQ® Self Service Password Reset

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

Component	Minimum Requirement
Processor	4 cores 64-bit - Dual Core2/Nehalem or higher or AMD Dual Athlon 64/Dual Opteron 64 or higher
RAM	4 GB
Disk	500 GB
VM Software	VMware ESXi 5.5 (64-bit)

Table 3 - 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:

Component	Requirements
Administration Workstation	Web Browsers • Mozilla Firefox 32 Designer & Analyzer - One of the following operating systems, at a minimum: • Windows 7 SP1 (32-bit or 64-bit)
Reporting Server 4.5	SUSE Linux Enterprise Server 11 SP3
Meta-directory 4.5 Server (Includes Identity Vault, Catalog Administrator, Meta-directory Engine, and Remote Loader Including security patch for POODLE vulnerability.	SUSE Linux Enterprise Server 11 SP3 (64-bit)
One SSO Provider	SUSE Linux Enterprise Server 11 SP3
Event Auditing Service 6.1	SUSE Linux Enterprise Server 11 SP3
Self Service Password Reset	SUSE Linux Enterprise Server 11 SP3

Table 4 - 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 4GB 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 be a multi-CPU server with a 2 GHz processor.

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:

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.
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.

Table 5 – 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

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

- NetIQ® Identity Manager User Application: Administration Guide (dated December 2014)
- NetIQ® Identity Manager Driver Administration Guide (dated December 2014)
- NetIQ® Designer for Identity Manager 4.5 Understanding Designer (dated December 2014)
- NetIQ® Identity Manager Analyzer Administration Guide (dated December 2014)
- NetIQ® Identity Manager Designer Administration Guide (dated December 2014)
- NetIQ® iManager 2.7.7 Administration Guide (dated September 2013)
- NetIQ Identity Manager NetIQ Identity Manager Catalog Administrator (dated December 2014)
- NetIQ® Identity Manager Understanding Policies (dated December 2014)
- NetIQ® Identity Manager Policies in Designer (dated December 2014)
- NetIQ® Identity Manager Policies in iManager (dated December 2014)
- NetIQ® Identity Manager Credential Provisioning (dated December 2014)
- NetIQ® Identity Manager Password Management Guide (dated October 2014)
- NetIQ Client Login Extension Administration Guide (dated September 2014)

- NetIQ® Identity Manager Identity Reporting Module Guide (dated December 2014)
- NetIQ Identity Manager Setup Guide (dated February 2015)
- NetIQ Identity Manager 4.5 Release Notes (dated December 2014)
- NetIQ Identity Manager 4.5 Standard Edition Release Notes (dated February 2015
- NetIQ Identity Manager Home and Provisioning Dashboard (dated December 2014)
- NetIQ® Identity Manager Identity Reporting Module Guide (dated December 2014)
- NetIQ® Identity Manager™ 4.5 Operational User Guidance and Preparative Procedures Supplement
- Version 1.2 (dated February 12, 2015)

1.8.6 Features / Functionality NOT Included in the TOE

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

Component	Requirements
Administration Workstation	Web Browsers • Internet Explorer 11 Designer & Analyzer - One of the following operating systems, at a minimum: • openSUSE 13.1 (32-bit or 64-bit) • Windows Server 2012 R2 (64-bit) • Windows 8.1 (32-bit or 64-bit) • Windows 7 SP1 (32-bit or 64-bit)
Identity Applications Server 4.5	Open Enterprise Server 11 SP2 Red Hat Enterprise 6.5 Windows Server 2012 R2
Reporting Server 4.5	Open Enterprise Server 11 SP2 Red Hat Enterprise 6.5 Windows Server 2012 R2
Meta-directory 4.5 Server (Includes Identity Vault, Catalog Administrator, Meta-directory Engine, and Remote Loader	Open Enterprise Server 11 SP2 (64-bit) Red Hat 6.5 (64-bit) Windows Server 2012 R2 (64-bit)
One SSO Provider	Open Enterprise Server 11 SP2 Red Hat Enterprise 6.5 Windows Server 2012 R2
Event Auditing Service 6.1	Open Enterprise Server 11 SP2 Red Hat Enterprise 6.5
Self Service Password Reset	Open Enterprise Server 11 SP2 Red Hat Enterprise 6.5 Windows Server 2012 R2

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant and augmented with ALC_FLR.1.

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 3 (July 2009). The TOE does not claim conformance to any functional package.

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 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.

THREAT	DESCRIPTION
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.

Table 6 – Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

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 7 – 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 8 – 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.

Table 9 – 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 10 – 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	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			✓				
P. REMOTE_DATA	✓			✓			

Table 11 – Mapping of Assumptions, Threats, Policies and ORSP s to Security Objectives

4.3.1.1 Rationale for Security Threats to the TOE

ASSUMPTION/THREAT/POLICY	RATIONALE
A.CONFIG	This assumption is addressed by • O.MANAGE_DATA, which ensures that the TOE provide a means to manage secrets and data associated with remote IT systems. • 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

ASSUMPTION/THREAT/POLICY	RATIONALE
A.MANAGE	This assumption is addressed 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. - 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.

ASSUMPTION/THREAT/POLICY	RATIONALE
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 and • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • 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 and • 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
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.
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. • OE.TIME, which provides support for enforcement of this policy by ensuring the provision of an accurate time source

Table 12 – 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
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

Table 13 – 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 Information Flow Control (FDP)

6.1.2.1 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]

6.1.2.2 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: [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].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 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, Privilege Level].

6.1.3.2 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.

6.1.3.3 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.

6.1.3.4 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].

6.1.3.5 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].

6.1.3.6 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.

6.1.3.7 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 14 – Management of TSF data

6.1.3.8 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].

6.1.3.9 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.

6.1.4 Protection of the TSF (FPT)

6.1.4.1 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.

6.2 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 for the TOE and the requirements that satisfy them.

OBJECTIVE SFR	O.MANAGE_DATA	O.MANAGE_POLICY	O.SEC_ACCESS
FAU_GEN.1		✓	
FAU_SAR.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	✓		

Table 15 – 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)

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

Table 16 – 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

OBJECTIVE	RATIONALE
	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

Table 17 – 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.1	Flaw Remediation 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 18 – 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.

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	Security Architecture: NetIQ Identity Manager 4.5 (IDM ARC)
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: NetIQ Identity Manager 4.5. (IDM FSP)
ADV_TDS.2 Architectural Design	Architectural Design: NetIQ Identity Manager 4.5. (IDM TDS)
AGD_OPE.1 Operational User Guidance[2]	• Operational User Guidance and Preparative Procedures Supplement: NetIQ Identity Manager 4.5 • NetIQ Identity Manager, User Application: Administration Guide • NetIQ Identity Manager Driver Administration Guide • NetIQ Designer for Identity Manager 4.5 Understanding Designer • NetIQ Identity Manager Analyzer Administration Guide • NetIQ Identity Manager Designer Administration Guide • NetIQ iManager 2.7.7 Administration Guide • NetIQ Identity Manager Catalog Administrator User Guide • NetIQ Identity Manager Understanding Policies • NetIQ Identity Manager 4.5 Policies in Designer • NetIQ Identity Manager Policies in iManager • NetIQ Identity Manager Credential Provisioning • NetIQ Identity Manager Password Management Guide • NetIQ Client Login Extension Administration Guide • NetIQ Identity Manager Identity Reporting Module Guide

[2] Additional documents can be found in Appendix A

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
AGD_PRE.1Preparative Procedures	• Operational User Guidance and Preparative Procedures Supplement: NetIQ Identity Manager 4.5 • NetIQ Identity Manager, Setup Guide • NetIQ Identity Manager 4.5 Release Notes • NetIQ Identity Manager User Application: Administration Guide • User Guide NetIQ Identity Manager Home and Provisioning Dashboard • NetIQ® Identity Manager Identity Reporting Module • NetIQ® Identity Manager Understanding Policies • NetIQ® Identity Manager Analyzer Administration Guide • NetIQ® Designer for Identity Manager 4.5 Understanding Designer • NetIQ® iManager 2.7.7 Administration Guide • NetIQ Identity Manager Catalog Administrator User Guide
ALC_CMC.3 Authorization Controls	Configuration Management Processes and Procedures: NetIQ Identity Manager 4.5
ALC_CMS.3 Implementation representation CM coverage	Configuration Management Processes and Procedures: NetIQ Identity Manager 4.5
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: NetIQ Identity Manager 4.5
ALC_DVS.1 Identification of Security Measures	Development Security Measures: NetIQ Identity Manager 4.5
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Development Process: NetIQ Identity Manager 4.5
ALC_FLR.1: Flaw Remediation Procedures	Basic Flaw Remediation Procedures: NetIQ Identity Manager 4.5
ATE_COV.2 Analysis of Coverage	Testing Evidence: NetIQ Identity Manager 4.5
ATE_DPT.1 Testing: Basic Design	Testing Evidence: NetIQ Identity Manager 4.5
ATE_FUN.1Functional Testing	Testing Evidence: NetIQ Identity Manager 4.5

Table 19 – 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

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, Identity Manager 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

ROLE	MANAGEMENT FUNCTIONS
	• 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 20 – 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