NetIQ Access Manager 4.5

Security Target

Initial Draft Date:	January 10, 2018
Last Updated:	October 11, 2019
Version:	2.0
Prepared By:	Michael F. Angelo
Prepared For:	NetIQ / Micro Focus Corporation Suite 1200 515 South Post Oak Blvd Houston, Texas 77027

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), NetIQ Access Manager 4.5. 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	Security Target: NetIQ Access Manager 4.5
ST Revision	2.0
ST Publication Date	October 11, 2019
Author	Michael F. Angelo

1.2. Target of Evaluation Reference:

TOE Reference	NetIQ Access Manager 4.5.0.0_191[1]

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*.

[1] NetIQ Access Manager 4.5.0.0_191 is also referred to as NAM 4.5. 0, or as NAM 4.5, or Access Manager, simply NAM. The first 0 refers to the service pack, the second 0 refers to the hot fix, and the 191 refers to the build number.

- 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
HMAC	Keyed Hash Message Authentication Code
HTTPS	Hyper Text Transport Protocol Secure
OAuth	Open Authorization
OIDC	Open ID Connect
OSP	Organizational Security Policy
SAML	Secure Assertion Markup Language
SFP	Security Function Policy
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality

Table 2 – Acronyms Used in Security Target

1.6. Target of Evaluation (TOE) Overview:

The TOE, NetIQ Access Manager 4.5 provides Single Sign-on[2] to the enterprise web application. It provides authorized users with intelligent access to secured applications and information based on who they are, what devices they are using and where they are located. It supported various types of authentication including multi-factor authentication and one can configure a type authentication for a resource. NetIQ Access Manager enables identity federation using protocols like SAML, OAuth/OIDC, Liberty, WS-Fed it simplifies access for partner and customer applications.

[2] Single Sign-on is accomplished via SAML, OAuth/OIDC, Liberty, WS-Fed. When referencing Single Sign-On in sections below we are referring to these standards.

The TOE is a software TOE and its components execute on general purpose computing hardware and software that are provided by the Operational Environment.

Centralized Administration

The browser-based Management Console provides a central place where your administrators can view, configure and manage all installed components and policies. It's also where your IT manager can monitor the health of the network in real time and automate certificate distribution.

And for large implementations, the Management Console lets you group multiple Access Gateways and then deploy configuration changes to them simultaneously. Access Manager replicates all component and policy configurations in a secure, fault-tolerant store.

To meet your administration needs, Management Console allows you to delegate administration for:

- Identity servers
- Access gateways
- Devices
- Policies

Ease of Integration

NetIQ Access Manager integrates out-of-the-box with identity stores like eDirectory™, Active Directory and Sun One, and standard HTTP applications. One way Access Manager achieves this integration is through the Access Gateway component—an HTTP proxy. As the access point for Web applications, it provides security via:

- authentication
- authorization
- Web single sign-on
- identity injection

And it is all done without requiring modification to Web applications.

s.

Business-to-Business Federated Access

NetIQ Access Manager gives businesses and organizations a simple and secure way to provide controlled access to information when they need it, from wherever they are. Now you can deliver simple access to employees, customers, and partners using standards-based access management technologies that make it easy to securely share information across business and infrastructure boundaries.

Single Sign-on Web Access

NetIQ Access Manager can deploy standards-based Web single sign-on, which means your employees, partners and customers only have to remember one password or login routine to access all the Web-based applications they are authorized to use.

Secure Communications

NetIQ Access Manager uses HTTPS/TLS[3] to communicate with external web browsers. NAM also uses HTTPS/TLS to communicate with backend web servers that are part of the operational environment. The TOE supports TLS v1.1 and 1.2 which is configurable by the administrator. The operational environment must also support TLS v1.1 or 1.2 in order to interoperate with the TOE.

[3] The TOE user guides make reference to SSL. For the purposes of this evaluation, those references apply to TLS.

The TOE implements a cryptographic module that provides the underlying cryptographic functions needed to support the HTTPS/TLS protocol.

The TLS protocol implementation is supported by:

CRYPTOGRAPHIC FUNCTION	ALGORITHM	KEY SIZE	STANDARD
Encryption and Decryption	AES	128 bits	FIPS PUB 197
Cryptographic Signature	RSA	2048 bits	FIPS PUB 186-4
Message Authentication	HMAC SHA-2	256 bits	FIPS PUB 198-1

1.7. TOE Description:

1.7.1. Overview:

You can use NetIQ Access Manager to centralize access control for all web sites, eliminating your need for multiple software tools at various locations. One access solution fits all applications and information assets. In addition, Access Manager includes support for major federation standards, including SAML, OAuth/OIDC and WS-Federation.

The following diagram illustrates the NetIQ Access Manager connections to the Internet, Intranet, User Console browsers, and corporate internal web servers.

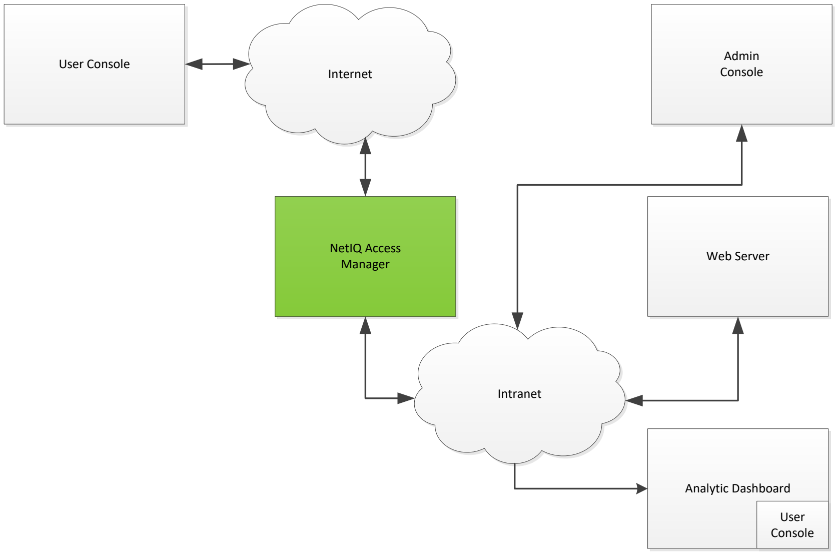


Figure 1 – NetIQ Access Manager

The following diagram shows the TOE deployed with the Access Gateway Service component.

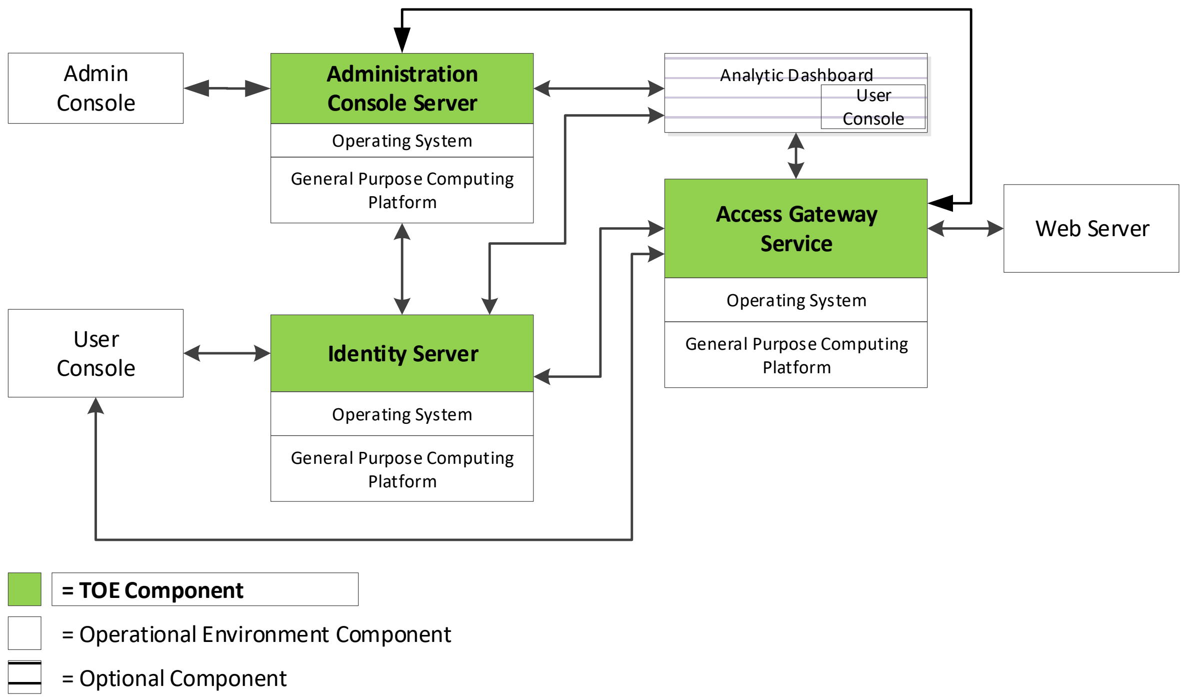


Figure 2 – TOE Deployment

The TOE includes of the following components:

- Administration Console Server
- Identity Server
- Access Gateway Service

1.7.2. Administration Console Server:

The Administration Console Server is the central configuration and management tool for the product. It can be used only to manage the Access Manager components. It contains a Dashboard option, which allows you to assess the health of all Access Manager components.
The Administration Console also allows you to configure and manage each component, and allows you to centrally manage resources, such as policies, hardware, and certificates, which are used by multiple components.

1.7.3. Identity Server:

The Identity Server is the central authentication and identity access point for all other services. It is responsible for authenticating users and distributing role information to facilitate authorization decisions. It also provides the Liberty Alliance Web Service Framework to distribute identity information.

An Identity Server always operates as an identity provider and can optionally be configured to run as an identity consumer (also known as a service provider), using Liberty, SAML 1.1, or SAML 2.0, OAuth/OIDC 2.0 protocols. As an identity provider, the Identity Server validates authentications against the supported identity user store, and is the heart of the user's identity federations or account linkage information.

In an Access Manager configuration, the Identity Server is responsible for managing:

- Account Provisioning
- Authentication

- Clustering
- Custom Attribute Mapping
- Identity Integration
- Identity Federation
- Identity Stores
- OAuth/OIDC
- Risk Based Authentication
- SAML Assertions
- Single Sign-on and Logout

1.7.4. Access Gateway Service:

An Access Gateway Service provides secure access to existing HTTP-based Web servers. It provides the typical security services (authorization, single sign-on, and data encryption), and is integrated with the identity and policy services of Access Manager.

The Access Gateway Service is designed to work with the Identity Server to enable single sign-on to protected Web services. The following features facilitate single sign-on to Web servers that are configured to enforce authentication or authorization policies:

- Access Gateway
- Identity Injection
- Form Fill[4]

1.7.5. 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:

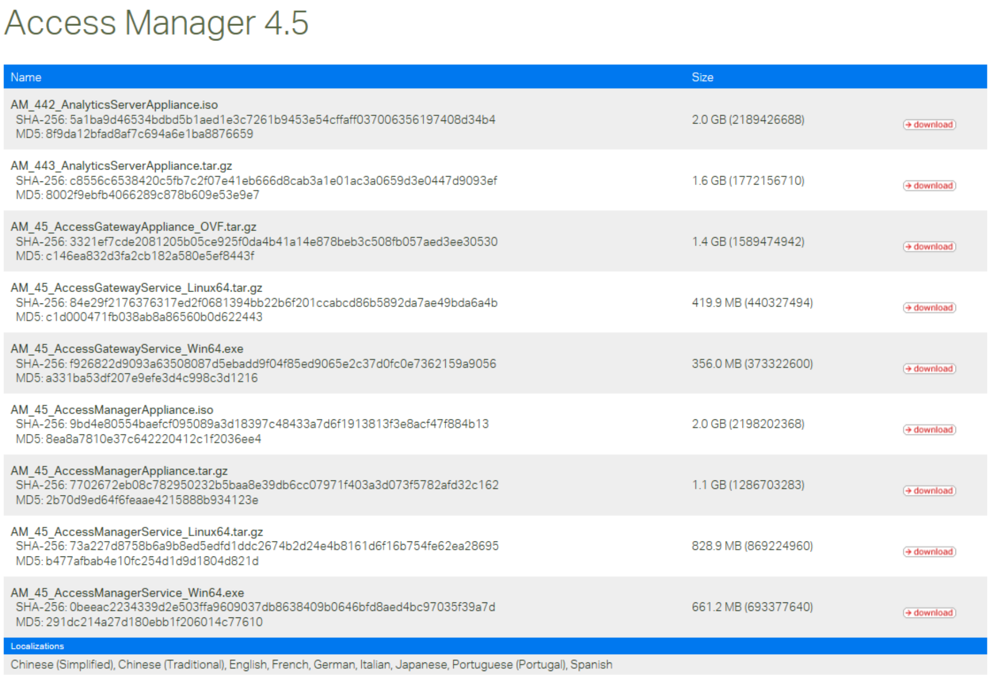
TSF	DESCRIPTION
Security Audit	The TOE supports the provision of log data from each system component, such as user login/logout and user HTTP transactions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis.
Cryptographic Support	The TOE includes a cryptographic module that provides the primitive cryptographic functions used to support the secure communications features of the TOE.
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.
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.
Trusted Path/Channels	The TOE provides HTTPS/TLS capabilities to authorized users. The TOE supports TLS v1.1 and 1.2 as configured by the Administrator.

Table 3 – Logical Boundary Descriptions

[4] Form Fill Options are found in the product documentation located: https://www.netiq.com/documentation/access-manager-45/admin/data/b5548mg.html

1.7.6. 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 tar'ed gnu zip (.tar.gz), iso formatted optical disk (.iso). or windows executable (.exe) depending on your destination platform. To install the TOE you will need to download and expand AM_45_AccessManagerService_Linux64.tar.gz and AM_45_AccessGatewayService_Linux64.tar.gz . Once downloaded, and extracted, the setup files can be executed to perform the installation.



Access Manager 4.5

Name	Size	
AM_442_AnalyticsServerAppliance.iso SHA-256: 5a1ba9d46534bdbd5b1aed1e3c7261b9453e54cffaff037006356197408d34b4 MD5: 8f9da12bfad8af7c694a6e1ba8876659	2.0 GB (2189426688)	→ download
AM_443_AnalyticsServerAppliance.tar.gz SHA-256: c8556c6538420c5fb7c2f07e41eb666d8cab3a1e01ac3a0659d3e0447d9093ef MD5: 8002f9ebfb4066289c878b609e53e9e7	1.6 GB (1772156710)	→ download
AM_45_AccessGatewayAppliance_OVF.tar.gz SHA-256: 3321ef7cde2081205b05ce925f0da4b41a14e878beb3c508fb057aed3ee30530 MD5: c146ea832d3fa2cb182a580e5ef8443f	1.4 GB (1589474942)	→ download
AM_45_AccessGatewayService_Linux64.tar.gz SHA-256: 84e29f2176376317ed2f0681394bb22b6f201ccabcd86b5892da7ae49bda6a4b MD5: c1d000471fb038ab8a86560b0d622443	419.9 MB (440327494)	→ download
AM_45_AccessGatewayService_Win64.exe SHA-256: f926822d9093a63508087d5ebadd9f04f85ed9065e2c37d0fc0e7362159a9056 MD5: a331ba53df207e9efe3d4c998c3d1216	356.0 MB (373322600)	→ download
AM_45_AccessManagerAppliance.iso SHA-256: 9bd4e80554baefcf095089a3d18397c48433a7d6f1913813f3e8acf47f884b13 MD5: 8ea8a7810e37c642220412c1f2036ee4	2.0 GB (2198202368)	→ download
AM_45_AccessManagerAppliance.tar.gz SHA-256: 7702672eb08c782950232b5baa8e39db6cc07971f403a3d073f5782afd32c162 MD5: 2b70d9ed64f6feaae4215888b934123e	1.1 GB (1286703283)	→ download
AM_45_AccessManagerService_Linux64.tar.gz SHA-256: 73a227d8758b6a9b8ed5edfd1ddc2674b2d24e4b8161d6f16b754fe62ea28695 MD5: b477afbab4e10fc254d1d9d1804d821d	828.9 MB (869224960)	→ download
AM_45_AccessManagerService_Win64.exe SHA-256: 0beeac2234339d2e503ffa9609037db8638409b0646bfd8aed4bc97035f39a7d MD5: 291dc214a27d180ebb1f206014c77610	661.2 MB (693377640)	→ download

Localizations

Chinese (Simplified), Chinese (Traditional), English, French, German, Italian, Japanese, Portuguese (Portugal), Spanish

Figure 3 – Sample Download List

The TOE is delivered via the web as a zipped tar file, or as an iso. If the zipped tar file is used it must be expanded and the various elements installed. If the iso file is used, it must be imaged to an appropriate material, and then executed. The documentation is available on the web in either html or pdf formats. For addition information please see the product guidance documents.

1.7.7. TOE Guidance:

The TOE includes the following guidance documentation[5]:

- Access Manager 4.5, Administration Guide
- Access Manager 4.5, Best Practices Guide
- Access Manager 4.5, Security Guide

For additional generic TOE Documentation, refer to NetIQ Access Manager 4.5 (found at https://www.netiq.com/documentation/access-manager-45/) . Additional TOE operational

[5] Note the guidance says you will use an NTP server. This may be either an internal or internet hosted NTP service.

guidance and installation procedures will be provided in the NetIQ Access Manager 4.5 Operational Guidance and Installation Procedures (AGD-IGS.1) document.

1.8. Excluded TOE Items:

The following product features have been excluded from the evaluation:

- Access Gateway Appliance
- Analytic Dashboard
- Secure API Manager
- SAS Account Manager
-

1.8.1. Non-TOE Hardware and Software:

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

COMPONENT	HARDWARE REQUIREMENTS	SOFTWARE REQUIREMENTS
Administration Console Server	• 100 GB of disk space • 4 GB RAM. • Dual CPU or Core (3.0 GHz or comparable chip)	• SLES 11 SP4 64-bit operating system • SLES 12 SP3 64-bit operating system • Chrome version > 70.0
Identity Server	• 100 GB of disk space • 4 GB RAM. • Dual CPU or Core (3.0 GHz or comparable chip)	• SLES 11 SP4 64-bit operating system • SLES 12 SP3 64-bit operating system
Access Gateway Service	• 100 GB of disk space • 4 GB RAM. • Dual CPU or Core (3.0 GHz or comparable chip)	• SLES 11 SP4 64-bit operating system • SLES 12 SP3 64-bit operating system

Table 4 - Operational Environment Component Requirements[6]

1.8.2. Security Functional Policies:

The TOE supports the following Security Functional Policy:

1.8.2.1. Discretionary Access Control SFP:

The TOE implements an access control SFP named *Discretionary Access Control SFP*. This SFP determines and enforces the access allowed to users. An authorized administrator can define access policies for external users to access internal corporate web servers.

[6] Note: For each of the hardware components VMWare ESXi can also be used for testing.

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 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 5 (April 2017). The TOE does not claim conformance to any functional package. The TOE EAL3 assurance package is augmented with ALC_FLR.1.

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

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL3+) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1. Introduction:

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*.

3.2. 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 user access policies and gain unauthorized access to corporate web servers.
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 including user access policies.
T.USER_ACTION_DENY	An authorized user may be able to access user authentication data and user access policies and deny their access to it later.

Table 5 – Threats Addressed by the TOE

The Operational Environment does not explicitly address any threats.

3.3. Organizational Security Policies

The TOE defines no organizational security policies:

3.4. Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. 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

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.PROT_ENV	The Operational Environment is configured to protect against unauthorized modification and access,
A.CONFIG	The Operational Environment shall allow the TOE to receive all passwords and associated data from network-attached systems.
A.TIMESOURCE	The TOE has access to a trusted source for system time.
A.WEB_PROTECT	The Operational Environment will not allow access to corporate web servers from external access. All Access is directed to web servers through the TOE.
A.HTTPS	Web browsers used to access the TOE shall support HTTPS using TLS. Web servers in the intranet shall support HTTPS using TLS.

Table 6 – 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_POLICY	The TOE shall enforce authentication and access control policies to allow or deny user access to corporate web servers.
O.SEC_ACCESS	The TOE shall ensure that only authorized users and applications are granted access to security functions and associated data.

Table 7 – 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 Operational Environment shall provide an accurate timestamp to the TOE.
OE.ENV_PROTECT	The Operational 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.
OE.WEB_PROTECT	The Operational Environment will not allow access to corporate web servers except through the TOE.
OE.HTTPS	Web browsers and web servers used to access the TOE shall support HTTPS using TLS.

Table 8 – 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_POLICY	O.SEC_ACCESS	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC	OE.WEB_PROTECT	OE.HTTPS
A.CONFIG					✓			
A.MANAGE					✓			
A.NOEVIL					✓			

OBJECTIVES THREATS/ ASSUMPTIONS/ POLICIES	O.MANAGE_POLICY	O.SEC_ACCESS	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC	OE.WEB_PROTECT	OE.HTTPS
A.PROT_ENV				✓		✓		
A.LOCATE						✓		
A.TIMESOURCE			✓					
A.WEB_PROTECT							✓	
A.HTTPS								✓
T.NO_AUTH		✓		✓	✓	✓		
T.NO_PRIV		✓						
T.USER_ACCESS_DENY	✓							

Table 9 – Mapping of Assumptions, Threats, Policies and OSPs to Security Objectives

4.3.1. Rationale for Security Threats, Policies and Assumptions to Objectives

ASSUMPTION/THREAT/POLICY	RATIONALE
A.CONFIG	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.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 non-hostile 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.PROT_ENV	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 • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed

ASSUMPTION/THREAT/POLICY	RATIONALE
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.
A.WEB_PROTECT	This assumption is addressed by • OE.WEB_PROTECT which ensures that web servers cannot be accessed except through the TOE.
A.HTTPS	This assumption is addressed by • OE.HTTPS which ensures that web browsers and web servers use HTTPS with TLS to communicate with the TOE.
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.
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 10 – Mapping of Threats, Policies, and Assumptions to Objectives

5. Extended Components Definition

There are no extended components used in this ST.

6. Security Requirements

The security requirements that are levied on the TOE 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
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1), (2), (3)	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Trusted Path/Channels	FTP_ITC.1	Trusted channel

Table 11 – 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) [HTTP transactions between the user web browser and the Access Gateway;

d) HTTP transactions between the Access Gateway and the Web servers in the corporate intranet protected by the TOE;
e) HTTP transactions between the Admin Console and the Administration Console Server[7];
f) HTTP transactions between the Admin Console and the Access Gateway Service].

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

[7] All communications to / from the Admin Console are considered administrative access.

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].

6.1.2. 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 [AES, RSA, HMAC] and specified cryptographic key sizes [128 bits for AES, 2048 bits for RSA, 160 bits for HMAC] that meet the following: [FIPS PUB 197 for AES, FIPS PUB 186-4 for RSA, FIPS 198-1 for HMAC].

Application Note: Symmetric AES keys are used for encryption and decryption for HTTPS sessions. Private RSA keys are generated for cryptographic signatures and HMAC for message authentication.

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].

Application Note: Symmetric AES keys used for encryption and decryption are destroyed from memory when TLS sessions are closed. Private RSA keys and HMAC keys are destroyed from memory when TLS sessions are closed.

6.1.2.3. FCS_COP.1 (1) Cryptographic operation (encryption /decryption)

FCS_COP.1.1 (1) The TSF shall perform [encryption, decryption] in accordance with a specified cryptographic algorithm [AES (in CBC Mode)] and cryptographic key sizes [128 bits] that meet the following: [FIPS 197].

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

6.1.2.4. FCS_COP.1 (2) Cryptographic operation (cryptographic signatures)

FCS_COP.1.1 (2) The TSF shall perform [cryptographic signature] in accordance with a specified cryptographic algorithm [RSA (RSA SSA-PKCS1-v1_5)] and cryptographic key sizes [2048 bits] that meet the following: [PKCS#1 v2.2 (RSA PKCS#1 v2.2 SHA-2)].

Application Note: RSA SSA-PKCS1-v1_5 is the signature scheme used by the TOE. RSA PKCS#1 v2.2 SHA-2 is used for cryptographic signatures used in support of TLS.

Application Note: RSA cryptographic signature and verification is used in support of TLS communications.

6.1.2.5. FCS_COP.1 (3) Cryptographic operation (HMAC)

FCS_COP.1.1 (3) The TSF shall perform [message authentication] in accordance with a specified cryptographic algorithm [HMAC SHA-2] and cryptographic key sizes [256 bits] that meet the following: [FIPS PUB 198-1 for HMAC, FIPS PUB 180-4 for SHA-2].

6.1.3. User Data Protection (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: Management functions for: Access Gateway Conditions, Identity Injection Actions, Form Fill Options
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: Management functions for: Access Gateway Conditions, Identity Injection Actions, Form Fill Options
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: [users are granted or denied access based on User Role].

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].

6.1.4. 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: [Role].

6.1.4.2. FIA_UAU.1 Timing of User Authentication before Any Action

FIA_UAU.1.1 The TSF shall allow [none] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3. FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [none] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5. Security Management

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* [*create*], the security attributes [

- Access Gateway Conditions,
- Identity Injection Actions,
- Form Fill Options]

to [Administrator].

6.1.5.2. 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 **Refinement:** The TSF shall **not** allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

Application Note: Restrictive default values are enforced by the TOE by requiring the Administrator to explicitly grant users access to the functionality.

6.1.5.3. FMT_SMF.1 Specification of Management Functions

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

a) Query Access Gateway Authorization policies, Identity Injection policies, Form Fill policies,
b) Create Access Gateway Authorization policies, Identity Injection policies, Form Fill policies,
c) Modify Access Gateway Authorization policies, Identity Injection policies, Form Fill policies,
d) Delete Access Gateway Authorization policies, Identity Injection policies, Form Fill policies].

6.1.5.4. 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. Trusted Path/Channel

6.1.6.1. 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 *another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [HTTPS/TLS connections

- between the User Console and the TOE components and
- between the TOE and the web servers].

Application Note: The TOE supports TLS v1.1 and 1.2 as configured by the Administrator.

Application Note: AES, RSA and HMAC as claimed in FCS_COP_1(1), (2), and (3) are used to support TLS.

Application Node: As defined in TLS 1.1 and 1.2, Diffie-Hellman is used to exchange keys for TLS.

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_POLICY	O.SEC_ACCESS
FAU_GEN.1	✓	
FCS_CKM.1		✓
FCS_CKM.4		✓
FCS_COP.1(1)		✓
FCS_COP.1(2)		✓
FCS_COP.1(3)		✓
FDP_ACC.1		✓
FDP_ACF.1		✓
FIA_ATD.1		✓
FIA_UID.1		✓
FIA_UAU.1		✓
FMT_MSA.1		✓
FMT_MSA.3		✓
FMT_SMF.1	✓	
FMT_SMR.1	✓	
FTP_ITC.1		✓

Table 12 – 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
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 and FCS_CKM.4	YES	Satisfied by FCS_COP.1(1), (2), (3) and FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	YES	Satisfied by FCS_CKM.1 for AES and RSA private keys.
FCS_COP.1(1), (2), (3)	FDP_ITC.1 or FDP_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_UAU.1	FIA_UID.1	YES	
FIA_UID.1	N/A	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 and FMT_SMF.1 and FMT_SMR.1	YES	Satisfied by FDP_ACC.1, FMT_SMF.1, and FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1	FIA_UID.1	YES	
FTP_ITC.1	N/A	N/A	

Table 13 – 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_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 define the auditing capability for incidents and administrative access control which are stored in the system. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role

OBJECTIVE	RATIONALE
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. • FCS_CKM.1, FCS_CKM.4, and FCS_COP.1(1), (2), (3) provides the cryptographic support functions for secure communications within the TOE and with external IT entities. • FDP_ACC.1 requires that all management functions for Access Gateway Conditions, Identity Injection Actions, and Form Fill Options are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to management functions for Access Gateway Conditions, Identity Injection Actions, and Form Fill Options is based on the user privilege level and their allowable actions • FIA_UID.1 requires the TOE to enforce identification of all users prior to performing TSF-initiated actions on behalf of the user. • FIA_UAU.1 requires the TOE to enforce authentication of all users prior to performing TSF-initiated actions on behalf of the user. • FIA_ATD.1 specifies security attributes for users of the TOE • FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data. • 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 HTTPS/TLS functionality is available to authorized users.

Table 14 – 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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	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 15 – 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	NetIQ Access Manager 4.5 Security Architecture (ADV_ARC.1)
ADV_FSP.3 Functional Specification with Complete Summary	NetIQ Access Manager 4.5 Functional Specification (ADV_FSP.3)
ADV_TDS.2 Architectural Design	NetIQ Access Manager 4.5 Architectural Design (ADV_TDS.2)
AGD_OPE.1 Operational User Guidance	NetIQ Access Manager 4.5 Operational Guidance and Installation Procedures (AGD-IGS.1)
AGD_PRE.1 Preparative Procedures	NetIQ Access Manager 4.5 Operational Guidance and Installation Procedures (AGD-IGS.1)
ALC_CMC.3 Authorization Controls	NetIQ Access Manager 4.5 Configuration Mgmt Processes & Procedures (ALC_CMS.3 / ALC_CMC.3)
ALC_CMS.3 Implementation representation CM coverage	NetIQ Access Manager 4.5 Configuration Mgmt Processes & Procedures (ALC_CMS.3 / ALC_CMC.3)
ALC_DEL.1 Delivery Procedures	NetIQ Access Manager 4.5 Secure Delivery Processes and Procedures (ALC_DEL.1)
ALC_DVS.1 Identification of Security Measures	NetIQ Access Manager 4.5 Development Security Measures (ALC_DVS.1)
ALC_LCD.1 Developer defined life-cycle model	NetIQ Access Manager 4.5 Life-Cycle Development Process (ALC_LCD.1)

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ALC_FLR.1: Flaw Remediation Procedures	NetIQ Access Manager 4.5 Basic Flaw Remediation Procedures (ALC_FLR.1)
ATE_COV.2 Analysis of Coverage	NetIQ Access Manager 4.5 Test Plan and Coverage Analysis (ATE.1)
ATE_DPT.1 Testing: Basic Design	NetIQ Access Manager 4.5 Test Plan and Coverage Analysis (ATE.1)
ATE_FUN.1Functional Testing	NetIQ Access Manager 4.5 Test Plan and Coverage Analysis (ATE.1)

Table 16 – 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 Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Trusted Path/Channels

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)
- HTTPS transactions between the User web browser and the Access Gateway
- HTTPS transactions between the Access Gateway and the back-end Web server protected by the TOE.

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

7.3. Cryptographic Support

The TOE implements a cryptographic module that provides support for the HTTPS/TLS communications used between TOE components and between the TOE and external web servers. The cryptographic module implements the following functions in support of TLS 1.1 and 1.2 communications:

- AES for encryption and decryption
- RSA for cryptographic signature and verification
- HMAC SHA-2 for message authentication.

These algorithms adhere to the following standards:

- AES follows FIPS PUB 197 with key generation follows FIPS PUB 197
- RSA follows PKCS#1 v2.2 with key generation follows FIPS PUB 186-4
- HMAC follows FIPS PUB 198-1 and SHA-2 follows FIPS PUB 180-4

Cryptographic session key exchange is performed in accordance with the TLS 1.1 and 1.2 standards as negotiated with the remote web browser.

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

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1(1), (2), (3)

7.4. User Data Protection

The TOE implements a Discretionary Access Control policy to define what roles can access particular functions of the TOE. Access to web sites is controlled by policies containing the following:

- Access Gateway Conditions
- Identity Injection Actions
- Form Fill Options

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

- FDP_ACC.1
- FDP_ACF.1

7.5. Identification and Authentication

The TOE maintains a role for each individual user to determine access privileges. Role-based access control is used to provide a convenient way to assign a user to a particular job function or set of permissions within an enterprise, in order to control access. The TOE can assign users to roles, based on attributes of their identity, and then associate authorization policies to the role.

Users and administrators are required to login to the TOE using a valid user name and password in order to gain access to the data and functions allowed by their assigned roles.

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

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

7.6. Security Management

The TOE maintains two user roles: the Administrator and the User.

Only an Administrator can query, create, modify or delete the Access Gateway Conditions, Identity Injection Actions, and Form Fill Options in user access policies. The TOE ensures only secure values are accepted for the security attributes listed with Discretionary Access Control SFP.

Users can gain access to web servers based on the Discretionary Access Control SFP defined by the Administrator.

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

- FMT_MSA.1
- FMT_MSA.3
- FMT_SMF.1
- FMT_SMR.1

7.7. Trusted Path/Channels

The TOE provides HTTPS/TLS capabilities to authorized users to gain access to web servers protected by the TOE. The TOE supports TLS v1.1 and 1.2 as configured by the Administrator.

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

- FTP_ITC.1