OpenText Access Manager 5.1.2

Security Target

Last Updated:	December 12, 2025
Version:	0.18
Prepared By:	Dawn Adams
Prepared For:	OpenText 275 Frank Tompa Drive Waterloo ON N2L 0A1 Canada

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), OpenText Access Manager 5.1.2. 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: OpenText Access Manager 5.1.2
ST Revision	0.18
ST Publication Date	December 12, 2025
Author	Dawn Adams

1.2. Target of Evaluation Reference

TOE Reference	OpenText Access Manager 5.1.2.0-95. (build no.)

1.3. Document Organization

This Security Target follows the following format:

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

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

Table 1 – ST Organization and Section Descriptions

1.4. Document Conventions

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

- The 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

TERM	DEFINITION
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, OpenText Access Manager 5.1.2, provides Single Sign-on[1] 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 authentications including multi-factor authentication and one can configure a type authentication for a resource. OpenText Access Manager enables identity federation using protocols like SAML, OAuth/OIDC, Liberty, WS-Fed it simplifies access for partner and customer applications.

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.

[1] 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.

And for large implementations, the Management Console lets you group multiple Access Gateways and then deploy configuration changes to them simultaneously. OpenText 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

OpenText Access Manager integrates out-of-the-box with identity stores like eDirectory™, Active Directory and Sun One, and standard HTTP applications. One way OpenText 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.

Business-to-Business Federated Access

OpenText 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

OpenText 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.

You can use OpenText 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, OpenText Access Manager includes support for major federation standards, including SAML, OAuth/OIDC and WS-Federation.

Access Manager is a comprehensive access management solution that provides single sign-on and secure access to web-based applications, SaaS services, and federated business-to-business interactions. Access Manager uses industry standards, such as SAML, OAuth, OpenID Connect, and WS-Federation to deliver federated single sign-on and supports multi-factor authentication, role-based access control, and data encryption.

Types of authentications and authorization supported by Access Manager are:

Single Sign-On - Access Manager establishes authentication to applications and provides authorization for those applications.

Secure Identity Federation -. Access Manager provides federated identity management to enable users to authenticate seamlessly and securely across autonomous identity domains.

Multi-Factor Authentication – Access Manager supports multi-factor authentication to provide secure access from any device with minimal administration.

Context-aware Authentication and Access Control - Access Manager enables organizations to select the authentication methods that fit the context of access. It provides risk-based access control, authentication, and authorization of users based on the context, pattern, location, and various other attributes.

Passwordless Authentication - Kerberos Authentication, Certificate-based Authentication, or Integration with Advanced Authentication are supported.

OAuth and OpenID - Access Manager supports OAuth and OpenID Connect for secure token-based authorization.

In this evaluation identity and passwords are used.

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

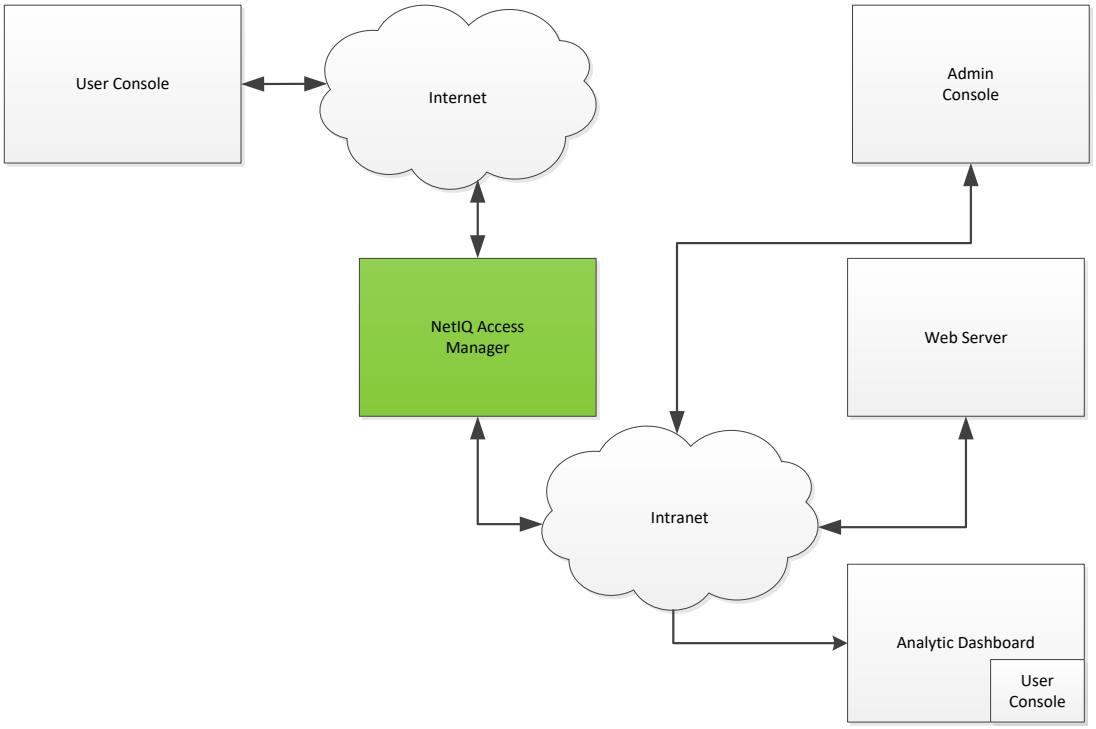

Figure 1 – Open Text Access Manager

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

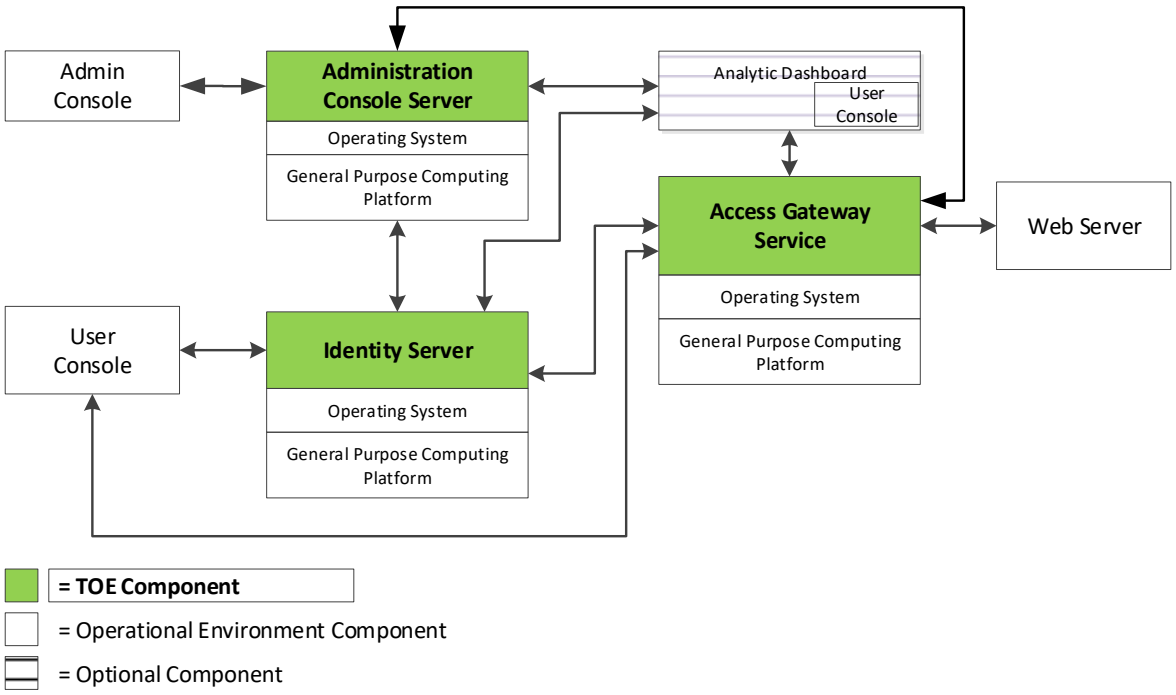

Figure 2 – TOE Evaluated Configuration

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

- Administration Console Server
- Identity Server
- Access Gateway Service

1.6.1.1. 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 OpenText Access Manager components. It contains a Dashboard option, which allows you to assess the health of all OpenText 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. Administration Console Server requirements are as follows:

COMPONENT	HARDWARE REQUIREMENTS	SOFTWARE REQUIREMENTS
Administration Console Server	• 100 GB of disk space • 4 GB RAM • X86-64-bit Dual CPU	SLES 12 SP5 64-bit OS Chrome
Admin Console	• 16 GB of disk space • 2 GB RAM • x86 CPU	Microsoft Windows 10 Chrome

Table 3 - Operational Environment Component Requirements[2]

1.6.1.2. 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. Identity Server requirements are as follows:

COMPONENT	HARDWARE REQUIREMENTS	SOFTWARE REQUIREMENTS
Identity Server	• 100 GB of disk space • 4 GB RAM • x86-64-bit Dual CPU	SLES 12 SP5 64-bit operating system
User Console	• 16 GB of disk space • 2 GB RAM • x86 CPU	Microsoft Windows 10 Chrome

Table 4 - Operational Environment Component Requirements

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

In an OpenText 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

1.6.1.3. 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 OpenText 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

The Access Manager requirements are e as follows:

COMPONENT	HARDWARE REQUIREMENTS	SOFTWARE REQUIREMENTS
Access Gateway	• 100 GB of disk space • 4 GB RAM • x86-64-bit Dual CPU	SLES 12 SP5 64-bit operating system
Web Server	• 16 GB of disk space • 2 GB RAM • X86-64-bit Dual CPU	SLES 12 SP5 64-bit OS Apache web server v2.4.38

Table 5 - Operational Environment Component Requirements

1.6.2. Non - TOE Software Supplied by the Environment

The TOE uses JDK, Tomcat and Apache HTTPS Server to provide cryptography for TLS connections.

The TOE uses an LDAP Server for Identification and Authorization.

Environment non-TOE software used:

- Apache httpd 2.4.64
- JRE 11.80.21
- OpenSSL 3.0.12 (Access Gateway)
- Tomcat 9.0.107

See section 1.6.1.1, 1.6.1.2, and 1.6.1.3 for the non-TOE hardware requirements for each TOE component.

1.6.3. Security Functional Policies

The TOE supports the following Security Functional Policy:

- *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

1.7. TOE Description

1.7.1. Physical Boundary

1.7.1.1. TOE Delivery

The TOE consists of the following components:

- Administration Console Server:
- Identity server:
- Access Gateway Service:

The TOE software is provided to customers via secure download from the download portal (https://sld.microfocus.com/mysoftware/index). 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_51_AccessManagerService_Linux64.tar.gz and AM_51_AccessGatewayService_Linux64.tar.gz . Once downloaded, and extracted, the setup files can be executed to perform the installation.

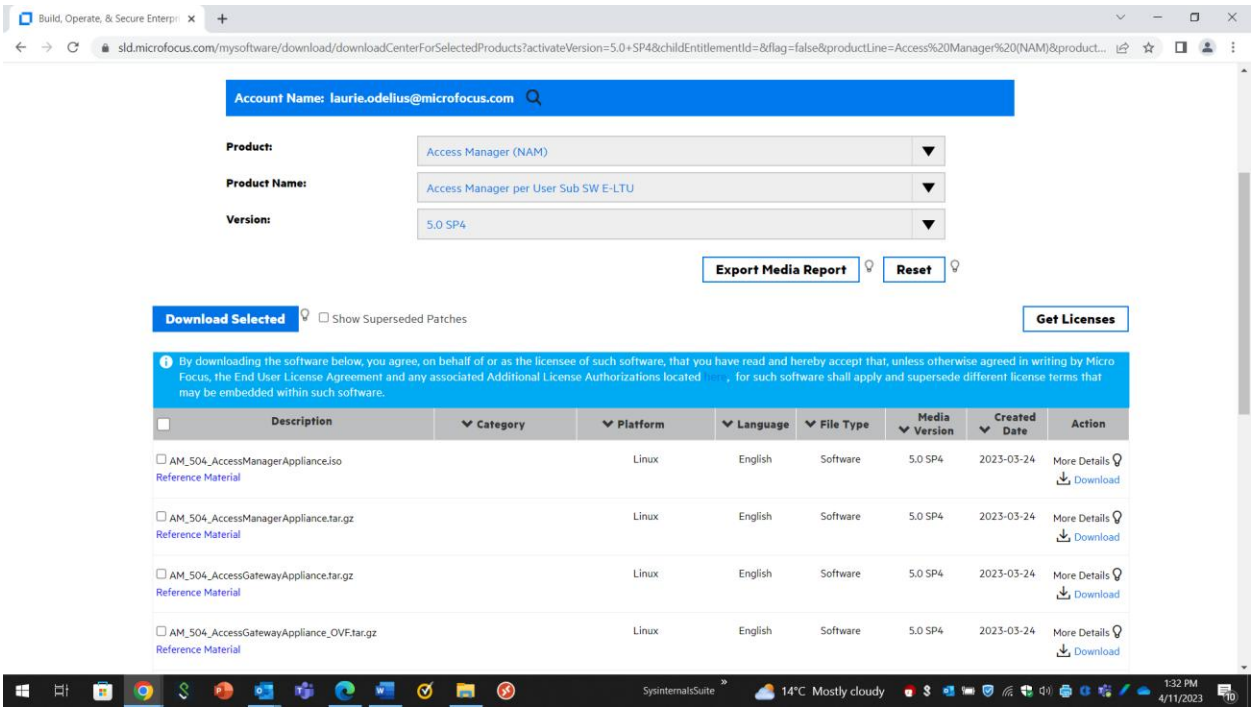

Figure 3 – Example Download List

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.

1.7.1.2. TOE Guidance

The TOE includes the following guidance documentation in pdf format[3]:

- OpenText Access Manager CE 24.2(v5.1), Administration Guide, May 2024
- OpenText Access Manager CE 24.2 (v5.1), Installation and Upgrade Guide, May 2024
- OpenText Access Manager System Requirements, May 2024

For additional generic TOE Documentation, refer to OpenText Access Manager 5.1 found at Access Manager CE 24.2 (v5.1) - Documentation | Mico Focus

Additional TOE operational guidance and installation procedures will be provided in the OpenText Access Manager 5.1 Operational Guidance and Installation Procedures (AGD-IGS.1) v0.11, 12 December 2025 (Word document).

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

Excluded TOE Items:

The following product features have been excluded from the evaluation:

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

1.7.2. 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.
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.

Table 6 – Logical Boundary Descriptions

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.3.

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.3.

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 assets are:

- Configuration files -files only accessible by the administrator used to configure the TOE.
- User authentication information – User credentials that grant authorization to access the TOE.
- Audit data – audit logs
- User access policies – policies that determine access to TOE functionality.

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.

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 including user access policies.
T.AUDIT	An unauthorized user may access the audit files and modify or delete the data.

Table 7 – 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
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.

ASSUMPTION	DESCRIPTION
A.COMMS	Communications are protected by TLS v1.2.
A.LDAP	A LDAP Server is provided by the environment.

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_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.
O.AUDIT	The TOE shall generate audit logs and ensure that all audit records are accessible only by an authorized user.

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 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 (including underlying OS administrators / users) 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 (including the underlying OS administrators and users) 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.

OBJECTIVE	DESCRIPTION
OE.SEC_COMMS	Communications links are protected by TLS supplied by the environment.
OE.LDAP	The environment supplies a method for authentication and identification of users of the TOE.

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_POLICY	O.SEC_ACCESS	O.AUDIT	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC	OE.WEB_PROTECT	OE.SEC_COMMS	OE.LDAP
A.CONFIG						✓				
A.MANAGE						✓				
A.NOEVIL						✓				
A.PROT_ENV					✓		✓			
A.LOCATE							✓			
A.TIMESOURCE				✓						
A.WEB_PROTECT								✓		
A.COMMS									✓	
A.LDAP										✓
T.NO_AUTH	✓	✓			✓	✓	✓			
T.NO_PRIV		✓								
T.AUDIT			✓		✓	✓				

Table 11 – 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

ASSUMPTION/THREAT/POLICY	RATIONALE
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
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.COMMS	This assumption is addressed by • OE.SEC_COMMS which ensures that the environment protects TOE communications using TLS v1.2.
A.LDAP	This assumption is addressed by • OE.LDAP which ensures a mechanism for identification and authorization for TOE users.

ASSUMPTION/THREAT/POLICY	RATIONALE
T.NO_AUTH	This threat is countered by the following: • O.MANAGE_POLICY, which ensures the TOE manages access control to the corporate web servers. • 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.

ASSUMPTION/THREAT/POLICY	RATIONALE
T.AUDIT	This threat is countered by • O.AUDIT, which ensures TOE generate of logs, and only an authorized user is able to have access to audit records. • OE.ENV_PROTECT and OE.PERSONNEL ensures the log files are protected and can only be accessed by trusted OS administrators / users

Table 12 – 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
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.2	User authentication before any action
	FIA_UID.2	User identification before any action
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

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) [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[4];

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

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. User Data Protection (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 [Table:

Subjects	Objects	Operations
Administrator This is the "super user" that can perform all functions.	Administration Server, Identity Server, Access Gateway	Install configure and maintain NAM; Assign delegated users; create, query, modify, delete user authorizations, design policies used in Identity Server and Access Gateway, access audit data
Delegated Administrator Created by administrator but needs to be	**Access Gateway: Authorization policies -** Authorization policies are used to protect a resource based on criteria other than authentication and Access Manager enforces	View/Modify

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

trusted individual	access restrictions. Authorization policies are enforced when a user requests data from a resource. **Identity Injection policies -** Identity injection allows adding information to the URL or HTML page before it is posted to a web server. Access to the resource is enforced by NAM. **Form Fill -** A Form Fill policy pre-populates fields in a form on first login and then saves the information in the completed form to a secret store for subsequent logins. Form Fill enables single sign-on.	
Delegated Administrator Created by administrator but needs to be trusted individual	**Identity Server:** **Roles policies** - Role-based access control (RBAC) assigns a user to a particular job function or set of permissions within an enterprise, to control access. **External Attributes –** Some of service providers require attributes that are not part of the user store where the user is authenticated and can accept those from external sources.	View/Modify

Policy View Administrator	Administrators on the Console can only view and not modify or create accounts, permissions or policies.	View
User These are end users of NAM	Only access resources (web pages)	View

]

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: [

According to the table:

Subjects	Objects	Operations
Administrator This is the "super user" that can perform all functions.	Administration Server, Identity Server, Access Gateway	Install configure and maintain NAM; Assign delegated users; create, query, modify, delete user authorizations, design policies used in Identity Server and Access Gateway, access audit data
Delegated Administrator Created by administrator but needs to be trusted individual	**Access Gateway: Authorization policies -** Authorization policies are used to protect a resource based on criteria other than authentication and Access Manager enforces access restrictions. Authorization policies are enforced when a user requests data from a resource.	View/Modify

	Identity Injection policies - Identity injection allows adding information to the URL or HTML page before it is posted to a web server. Access to the resource is enforced by NAM. **Form Fill -** A Form Fill policy pre-populates fields in a form on first login and then saves the information in the completed form to a secret store for subsequent logins. Form Fill enables single sign-on.	
Delegated Administrator Created by administrator but needs to be trusted individual	**Identity Server:** **Roles policies** - Role-based access control (RBAC) assigns a user to a particular job function or set of permissions within an enterprise, to control access. **External Attributes -** Some of service providers require attributes that are not part of the user store where the user is authenticated and can accept those from external sources.	View/Modify
Policy View Administrator	Administrators on the Console can only view and not modify or create accounts, permissions or policies.	View
User These are end users of NAM	Only access resources (web pages)	View

]

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].

6.1.3. 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: [Role].

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.

6.1.4. Security Management

6.1.4.1. 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 Configuration,
- Audit data
- Identity Injection Actions,

- Form Fill Options
- Assign user roles to users

]

to [Administrator].

6.1.4.2. 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.

6.1.4.3. 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].

6.1.4.4. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, Delegated Administrator for Access Gateway, Delegated Administrator for Identity Server, Policy View Administrator, User].

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

6.2. 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.3	Systematic Flaw Remediation
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 14 – Security Assurance Requirements at EAL3

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

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

OBJECTIVE / SFR	O.MANAGE_POLICY	O.SEC_ACCESS	O.AUDIT
FAU_GEN.1		✓	✓
FDP_ACC.1	✓	✓	
FDP_ACF.1	✓	✓	
FIA_ATD.1		✓	
FIA_UID.2	✓	✓	
FIA_UAU.2	✓	✓	
FMT_MSA.1		✓	
FMT_MSA.3		✓	
FMT_SMF.1		✓	
FMT_SMR.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
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.2	FIA_UID.1	YES	Satisfied by FIA_UID.2 because FIA_UID.2 is hierarchical to FIA.UID.1
FIA_UID.2	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	Satisfied by FIA_UID.2 because FIA_UID.2 is hierarchical to FIA.UID.1

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_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: • FDP_ACC.1 and FDP_ACF.1 ensure that the access control policy is applied when allowing or denying access to the corporate web servers • FIA_UID.2 requires the TOE to enforce identification of all users prior to performing TSF-initiated actions on behalf of the user. • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to performing TSF-initiated actions on behalf of the user.

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. • FAU_GEN.1 defines the auditing capability for administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • FAU_SAR.1 Specifies which role has the ability to review audit events • FDP_ACC.1 requires that all management functions for Access Gateway, 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, Identity Injection Actions, and Form Fill Options 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 performing TSF-initiated actions on behalf of the user. • FIA_UAU.2 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' • FMT_SMF.1 ensures the TOE manages the following functions: Query Access Gateway Authorization policies Identity Injection policies, Form Fill policies, Create Access Gateway Authorization policies, Identity Injection policies, Form Fill policies, Modify Access Gateway Authorization policies, Identity Injection policies, Form Fill policies,

OBJECTIVE	RATIONALE
	Delete Access Gateway Authorization policies, Identity Injection policies, Form Fill policies • FMT_SMR.1 ensures that the TOE maintains the roles Administrator, Delegated Administrator for Access Gateway, Delegated Administrator for Identity Server, Policy View Administrator, User.
O.AUDIT	• FAU_GEN.1 ensures that the TOE audits events. • FDP_ACC.1 and FDP_ACF.1 ensures only administrator can access audit data

Table 17 – Rationale for TOE SFRs to Objectives

6.3.4. 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.

6.3.5. 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	OpenText Access Manager Security Architecture (ADV_ARC.1)
ADV_FSP.3 Functional Specification with Complete Summary	OpenText Access Manager Functional Specification (ADV_FSP.3)
ADV_TDS.2 Architectural Design	OpenText Access Manager Architectural Design (ADV_TDS.2)

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
AGD_OPE.1 Operational User Guidance	OpenText Access Manager Operational Guidance and Installation Procedures (AGD-IGS.1)
AGD_PRE.1 Preparative Procedures	OpenText Access Manager Operational Guidance and Installation Procedures (AGD-IGS.1)
ALC_CMC.3 Authorization Controls	OpenText Access Manager Configuration Mgmt Processes & Procedures (ALC_CMS.3 / ALC_CMC.3)
ALC_CMS.3 Implementation representation CM coverage	OpenText Access Manager Configuration Mgmt Processes & Procedures (ALC_CMS.3 / ALC_CMC.3)
ALC_DEL.1 Delivery Procedures	OpenText Access Manager Secure Delivery Processes and Procedures (ALC_DEL.1)
ALC_DVS.1 Identification of Security Measures	OpenText Access Manager Development Security Measures (ALC_DVS.1)
ALC_LCD.1 Developer defined life-cycle model	OpenText Access Manager Life-Cycle Development Process (ALC_LCD.1)
ALC_FLR.3: Flaw Remediation Procedures	OpenText Access Manager Systematic Flaw Remediation (ALC_FLR.3)
ATE_COV.2 Analysis of Coverage	OpenText Access Manager Test Plan and Coverage Analysis (ATE.1)
ATE_DPT.1 Testing: Basic Design	OpenText Access Manager Test Plan and Coverage Analysis (ATE.1)
ATE_FUN.1Functional Testing	OpenText Access Manager Test Plan and Coverage Analysis (ATE.1)

Table 18 – 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
- User Data Protection
- Identification and Authentication
- Security Management

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.

Authorized administrators can access the audit logs by exporting the audit log to the underlying OS, and review the logs at underlying OS. The audit logs are in a presented in a searchable structured language that can be readily interpreted by the administrator.

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

- FAU_GEN.1

7.3. User Data Protection

NAM has a super user administrator that is able to perform all functionality provided by NAM. This administrator installs, configures and maintains NAM. This administrator also can assign users as

delegate administrators that have reduced administrative access, but the Access Gateway and the Identity Server each have a delegate Administrator to provide administrative duties.

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 Configuration
- Identity Injection Actions
- Form Fill Options

- **Access Gateway:**
  - **Authorization** policies are used to protect a resource based on criteria other than authentication, and Access Manager enforces access restrictions. Authorization policies are enforced when a user requests data from a resource.
  - **Identity injection** policies allow the addition of information to a URL or HTML page before it is posted to a web server. The web server uses this information to determine whether a user can access the resource. This enables NAM to provide single sign-on for users.
  - A **Form Fill** policy pre-populates fields in a form on first login and then saves the information in the completed form to a secret store for subsequent logins. The user is prompted to reenter the information only when something changes such as when a password expires. Form Fill also enables the provision of single sign-on.
- **Identity Server:**
  - **Role-based access control** (RBAC) allows an administrator to assign a user to a particular job function or set of permissions within an enterprise, to control access.
  - The **External Attribute Source** enables you to retrieve attributes from external sources. Some of these service providers require attributes that are not part of the user store where the user is authenticated.

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

  - FDP_ACC.1
  - FDP_ACF.1

7.4. 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.2
- FIA_UID.2

7.5. 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 Configuration, 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