Applied Identity ID-Enforce Security Target

Version 1.0
29 September 2008

Prepared for:
Applied Identity, Inc.
456 Montgomery, Suite 400
San Francisco, CA 94104

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. SECURITY TARGET INTRODUCTION 4
1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 4
1.2 CONFORMANCE CLAIMS 4
1.3 CONVENTIONS 5
1.3.1 Conventions 5
1.3.2 Terminology and Acronyms 5
2. TOE DESCRIPTION 6
2.1 TOE OVERVIEW 6
2.2 TOE ARCHITECTURE 7
2.2.1 Physical Boundaries 9
2.2.2 Logical Boundaries 10
2.3 TOE DOCUMENTATION 11
3. SECURITY ENVIRONMENT 12
3.1 THREATS 12
3.2 ASSUMPTIONS 12
4. SECURITY OBJECTIVES 13
4.1 SECURITY OBJECTIVES FOR THE TOE 13
4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 13
4.3 SECURITY OBJECTIVES FOR THE ENVIRONMENT 13
5. IT SECURITY REQUIREMENTS 14
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 14
5.1.1 Security audit (FAU) 14
5.1.2 User data protection (FDP) 15
5.1.3 Identification and authentication (FIA) 16
5.1.4 Security management (FMT) 16
5.1.5 Protection of the TSF (FPT) 17
5.2 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 17
5.2.1 Security audit (FAU) 17
5.2.2 Identification and authentication (FIA) 18
5.2.3 Security management (FMT) 18
5.2.4 Protection of the TSF (FPT) 18
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 19
5.3.1 Configuration management (ACM) 19
5.3.2 Delivery and operation (ADO) 19
5.3.3 Development (ADV) 20
5.3.4 Guidance documents (AGD) 21
5.3.5 Tests (ATE) 21
5.3.6 Vulnerability assessment (AVA) 22
6. TOE SUMMARY SPECIFICATION 23
6.1 TOE SECURITY FUNCTIONS 23
6.1.1 Security audit 23
6.1.2 User data protection 23
6.1.3 Identification and authentication 25
6.1.4 Security management 25
6.1.5 Protection of the TSF 26
6.2 TOE SECURITY ASSURANCE MEASURES 27
6.2.1 Configuration management 27
6.2.2 Delivery and operation 27
6.2.3 Development 28

6.2.4 Guidance documents 28
6.2.5 Tests 29
6.2.6 Vulnerability assessment 29

7. PROTECTION PROFILE CLAIMS 31

8. RATIONALE 32

8.1 SECURITY OBJECTIVES RATIONALE 32
8.1.1 Security Objectives Rationale for the TOE and Environment 32
8.2 SECURITY REQUIREMENTS RATIONALE 33
8.2.1 Security Functional Requirements Rationale 34
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 36
8.4 STRENGTH OF FUNCTIONS RATIONALE 36
8.5 REQUIREMENT DEPENDENCY RATIONALE 36
8.6 EXPLICITLY STATED REQUIREMENTS RATIONALE 37
8.7 TOE SUMMARY SPECIFICATION RATIONALE 38
8.8 PP CLAIMS RATIONALE 39

LIST OF TABLES

Table 1 - TOE Security Functional Components 14
Table 2 - IT Environment Security Functional Components 17
Table 3 - EAL 2 Assurance Components 19
Table 4 – Environment to Objective Correspondence 32
Table 5 - Objective to Requirement Correspondence 34
Table 6 - Requirement Dependencies 36
Table 7 - Security Functions vs. Requirements Mapping 38

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3 including the ID-Enforce Client ID-Mark v3.3 and the Identisphere Manager (ID-Policy v3.3) provided by Applied Identity, Inc. The TOE is designed to protect and conceal servers and data resources by creating a virtual User Local Area Network (ULAN) that allows authenticated users to access network resources based on their access rights.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
-

IT Security Requirements (Section 5)

- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Applied Identity ID-Enforce Security Target

ST Version – 1.0

ST Date – 29 September 2008

TOE Identification – Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3 including the ID-Enforce Client ID-Mark v3.3 and the Identisphere Manager (ID-Policy v3.3)

> *Note that the TOE can consist of either one product identified above or two products as identified above connected using a High Availability port to facilitate failover.*
>
> *Note also that the WebAuth client that ships with the product has been excluded from the evaluated configuration.*

TOE Developer – Applied Identity

Evaluation Sponsor – Applied Identity

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
  - Part 3 Conformant
  - Assurance Level: EAL 2
  - Strength of Function Claim: SOF-Basic

1.3 Conventions

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - o Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a

and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.

  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

- Explicitly stated SFRs – Explicitly stated requirements are those that are not already define in the CC and are created to address some specific security claim of the TOE. Explicitly stated requirements are identified with "_EXP" following the CC class and the uniquely named component/family descriptor and concluding with the _EXP and the component number. For example, Timing of authentication, FIA_UAU_EXP.1 reflects the CC class FIA and the family UAU; however, the requirement was changed to reflect some specific detail of the TOE that did not otherwise correspond with an exis5ting CC requirement.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

CAD	Computer-Aided Design
CLI	Command Line Interface
GUI	Graphical UI
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
UI	User Interface
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SYSLOG	System Log
TLS	Transport Layer Security
ULAN	User Local Area Network

2. TOE Description

The Target of Evaluation (TOE) is Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000; the primary differences being performance and physical network connections – e.g., copper vs. fiber) with ID-Enforce Gateway, Version 3.3 including the ID-Enforce Client ID-Mark and the Identisphere Manager (ID-Policy) application. The TOE is designed to protect and conceal servers and data resources by creating a virtual User Local Area Network (ULAN) that allows users to access network resources based on their access rights.

2.1 TOE Overview

The TOE is an appliance that serves as an inline gateway designed primarily to protect resources located on a protected network from users on an untrusted network. The TOE can be configured to run in bridged or routed mode where the security behavior remains the same with the exception that in bridged mode the TOE has some additional access control rules. The appliance implements a granular security access control model that serves to mediate user operations on that protected network as they pass through the TOE.

The TOE requires each user (on the untrusted network) to be successfully identified and authenticated (except as summarized below) at the network interface served by the gateway so that it can effectively apply user-specific access policies. Note that policies can be created that allow access to specific resources without requiring the user to be authenticated. The product includes a client application (i.e., ID-Mark) allowing network users to interact with the TOE in order to access the resources it protects. The client access in all these cases is for the purpose of identifying and authenticating the user to the TOE. Once the user establishes a session with the TOE, they can use other applications (FTP, e-mail, web browser, etc.) to access network resources in accordance with the TOE access policies. The TOE can be configured to allow access to network resources without requiring an authenticated user session and in those cases the client identified above is not necessary.

Note that while the TOE can be configured to restrict the access of users (e.g., servers) on the protected network to defined resources on the untrusted network, that is beyond the scope of the claims made in this Security Target. The primary function of the TOE is to control access to resources on a protected network. As such, communication originating from the protected network is not a subject of this evaluation.

While not subject to specific evaluation claims, the ID-Mark client offers some functional benefits such as tagging to provide some measure of non-repudiation and more flexible authentication choices (e.g., authentication via the domain of the user). These features are outside this evaluation, since the client resides in a presumably untrusted space which would otherwise extend the scope and complicate the Common Criteria evaluation with an unclear security boundary.

User access rights to the protected network are determined by access control policies controlled and defined in an associated LDAP server in the IT environment. The LDAP server also serves to implement authentication functions for the TOE. The Identisphere Manager (ID-Policy v3.3) application offers a Graphical User Interface (GUI) that may be used by the network administrator, in lieu of the native tools provided by the LDAP server itself, to define the user access policies stored in the LDAP server.

Given user authentication and access controls, the TOE is designed to carefully audit attempts to access resources in order to ensure user accountability. In order to help ensure integrity of an evidentiary chain, the TOE is designed to be configured and then left to operate with little or no on-going administration (or other direct user functions). Once configured, the TOE is designed to rely on an external, trusted LDAP server as a source of access policies and also a syslog server as a drop point for generated audit information.

2.2 TOE Architecture

The TOE is the gateway appliance comprised of hardware and software components.

- **ID-Enforce 5000, 7000, and 10000 Hardware Appliances** – The hardware appliance includes the external Ethernet ports used to communicate with the untrusted network, protected network, a dedicated management network[1] and console port for direct serial connection of a terminal computer for TOE management, and a high availability port used to connect a failover appliance for redundancy[2].
- **ID-Enforce Gateway v3.3**- The software component, executing within the hardware appliance, provides the functions to control user access to protected network resources and implement a Command-Line Interface (CLI), which provides the local authorized administrator the interfaces to configure the TOE.

[1] Note that the dedicated management network is distinct from the untrusted and protected networks and is assumed to be appropriately protected so that the security management functions cannot be somehow subverted.

[2] Note that the High Availability port can be configured for use within the TOE. The port is used primarily to allow two appliances to communicate so that when one stops responding the other could take over (i.e., failover). Since both appliances are essentially the same and would be configured to use the same security settings hosted on other servers within the environment, the only need for actual synchronization is to ensure that user sessions are shared between the appliances to ensure a smooth transition should that become necessary.

- **ID-Enforce Client (ID-Mark v3.3)** – Optional client component design specifically for use with the ID-Enforce Gateway (see below).
- **Identisphere Manager (ID-Policy v3.3)** – An optional application that can be used to define user access policies (see below).

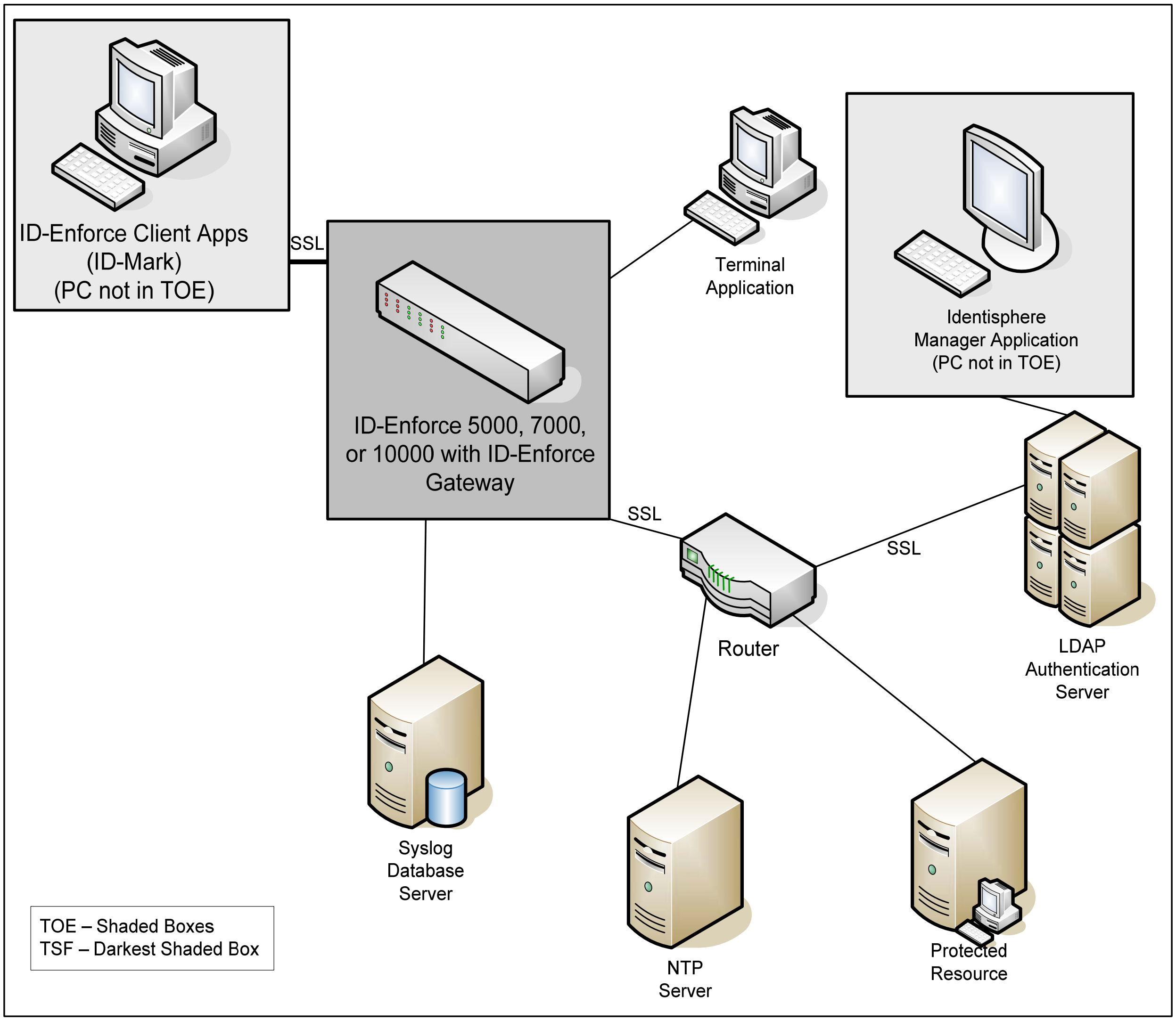

Figure 1: Basic ID-Enforce Gateway System Topology

The TOE supports two operational configurations determined by its location in a network:

- **Protecting critical application servers' configuration** – In this configuration, the TOE is deployed near application servers, so that all traffic destined to the protected servers will pass through the TOE.
- **Remote user restriction configuration** – In this configuration, the TOE is deployed near a group of users so that the TOE will control access to a protected network that is available to the group of users.

The TOE supports the use of a client/driver module utilizing the ID-Enforce Client that is deployed at user endpoints and is designed to support tagging packets generated by authenticated users and destined to the protected network resources. However, while the client provided with the product is part of the TOE no security claims are made about it (i.e., it is not security relevant), so it is outside the TSF (i.e., the security boundary of the TOE). Note that the tagging feature above is not claimed since the client, unlike the TOE appliance and Gateway software, executes in an environment that is entirely controlled by the IT environment. As such, many of the claims in this Security Target (e.g., regarding tampering and bypassability) simply cannot be made for the client.

To be more specific about the evaluated configuration, in the context of this ST, it is assumed that the client is outside the secure boundary of the TOE (i.e., on the untrusted network) and that the supporting IT environment components (in particular, the LDAP server and syslog server) are either within the protected network as defined by the TOE or are secured using SSL or TLS when configured on the untrusted network.

2.2.1 Physical Boundaries

The components that make up the TOE are:

- Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 10000) with ID-Enforce Gateway, Version 3.3.
- ID-Enforce Client (ID-Mark v3.3) –a software agent that associates the user's identity to network traffic and is used as an interface to access the protected network or resource.

  Note that the product also ships with a WebAuth client facilitating the use of a browser to authenticate a client, but this client is excluded from the evaluated configuration.
- Identisphere Manager (ID-Policy v3.3) – an optional component that provides a Graphical User Interface (GUI) that may be used by the network administrator to define user access policies in the authentication server in lieu of the tools provided by the authentication server.[3] Note that given that the Identisphere Manager resides on a computer outside the TOE and the Authentication Server (below) with which it communicates is also outside the TOE, the network administrator needs to ensure appropriate protection of the communication channel to protect the TOE user access policies. The Identisphere Manager could be hosted on the same computer, for example, or alternately the Authentication Server could be configured to offer SSL/TLS connectivity.

The TOE's intended environment can be described in terms of the following components

- Simple Network Management Protocol (SNMP) server – an optional component to receive alerts generated by the ID-Enforce Gateway v3.3 server. Note that the specific capability to generate alerts is not claimed in this Security Target and hence is not a subject of the evaluation.
- System Log (SYSLOG) server – required to store the audit records generated by the TOE before the (local) records are overwritten.
- Authentication Server (i.e., Lightweight Directory Access Protocol (LDAP)) – required to provide/store the user credentials (for both authentication and access) used by the TOE in making network access control decisions and by the authentication server in order to authenticate users.
- Network Time Protocol (NTP) or Time Server – required to provide the reliable timestamp used by the TOE.
- Terminal application - a local system connected directly to the TOE for local administration. Access to the CLI can be accomplished by one of the following ways:
  - A direct connection to the ID-Enforce serial console port.
  - A network connection to the High Availability port using SSH. This connection should only be used during configuration and should subsequently be disconnected or used to facilitate the High Availability feature.
  - A network connection to protected, untrusted, or managed ports using SSH. This requires explicit policy configuration to allow such access.

[3] Note that the ID-Policy Identisphere Manager application is delivered with the product and operates outside the security domain implemented by the TOE (i.e., in the appliance). As such, definitive security claims cannot be applied to this component. Note, however, that the component is expected to work properly in terms of translating GUI policies to LDAP rules enforced by the TOE.

Note that accessing the CLI via one of the network connection is recommended only if the connected network is dedicated and isolated for that purpose. Reliance on SSH is not recommended, since the SSH implementation is not FIPS certified, and is not subject to security claims in this Security Target. ***As such, the evaluated configuration includes only the use of direct serial connections and/or dedicated isolated networks for the purpose of accessing the CLI.***

- Operating system (Windows ME, Windows 2000 Server or Professional, Windows XP, or Windows Server 2003) – required to host any ID-Mark client applications.

2.2.2 Logical Boundaries

This section identifies the security functions that ID-Enforce product provides.

2.2.2.1 Security audit

The TOE generates audit records that trace the actions of the administrator and user attempts to access protected resources. At a minimum, the log records includes the date time the event occurred, the user identification, the event type and the outcome of the event. The CLI provides commands the administrator can use to review the internal audit record buffer. The TOE allows an administrator to define limits for the maximum number of audit log files and the maximum size of each log file. When a log file reaches the maximum size, a new log file is created. When the maximum number of log file is exceeded, the oldest log file is deleted. In this manner, the administrator can defined the volume of audit data to retain with the oldest audit records being the first to be deleted should the available space become exhausted.

The TOE provides the ability for the log records to be exported to a SYSLOG server in the IT environment in order to retain a more comprehensive audit record history. Note also that the TOE uses a NTP server to obtain reliable time information.

2.2.2.2 User data protection

The TOE enforces network identity-based access control policies. The TOE acquires identity-based access policy that controls how an authenticated user, on an untrusted network, is allowed to access resources, on a protected network, based on several attributes including resource identification (i.e., address), service, port, and user privileges derived from their identity and groups. By default, the TOE will not allow access to the protected resources until access control policies are defined specifically allowing access. Note that while the TOE enforces the access policies, those policies are defined and stored in an associated LDAP server in the IT environment. Note also that the TOE can be configured to allow access to specific resources without requiring users to be authenticated.

Furthermore, while operating in bridged mode the TOE can be configured to restrict access attempts based on source and destination Media Access Control (MAC) addresses. Any requests matching a filtered MAC address are discarded so that access is denied.

2.2.2.3 Identification and authentication

The TOE requires both administrators and network users (attempting to access protected resources requiring authentication) to be identified and authenticated prior to obtaining services. Administrators are able to access the TOE via a direct serial connection to the TOE or thru the (dedicated) management network if enabled. The administrator is required to login with a user id and password in order to access the CLI where administrative functions are available. The TOE stores the administrator's logon credentials internally and verifies the user's credentials and allows or disallows access to the TOE.

To access the protected network or resource (where the policies are configured to require user authentication), the TOE requires network users enter their credentials via the available client or the TOE's web interface and the TOE utilizes the services of the IT environment to authenticate the user's identity. The TOE is dependent upon the environment to validate the user credentials and return a result to be enforced by the TOE. Network users use a client provided with the TOE (i.e., ID-Mark) in order to identify and authenticate themselves to the rest of the TOE (i.e., ID-Enforce).

2.2.2.4 Security management

The TOE includes interfaces used to manage the TOE accessible via a direct serial connection or via a dedicated management network that is distinct and separate from the networks controlled by the TOE. In addition to, in effect, being directly connected to the TOE, the administrator is only able to access the TOE after having successfully logged into the TOE. The interfaces allow the administrator the ability to configure, manage, and troubleshoot the TOE. The management functions include the ability to establish the gateway within the network, review the local log records, and create and manage other administrator accounts.

Note that the TOE depends on the IT environment to facilitate and control the management of the access control policies (i.e., when using Identisphere Manager) enforced by the TOE, network users that can be authenticated in the IT environment, and the syslogs that can be used to stored audit records generated by the TOE.

Note also that in the IT environment the administrator is refereed to as the 'network administrator' to distinguish that role from the 'administrator' known to the TOE. Note also that while the TOE technically includes three distinct administrator roles – unprivileged, monitor, and administrator – this Security Target does not distinguish them in the context of the security claims being made since they are all trusted to have physical access to the TOE and are generally trusted not to attempt to exceed their defined authorities.

2.2.2.5 Protection of the TSF

The TOE hardware appliance ensures separation of internal and external networks and ensures that its interfaces cannot be bypassed. Furthermore, the appliance is designed to protect itself from tampering by being a physically separate device with carefully designed services available only at well defined interfaces. Transmission of data between the trusted LDAP server and the TOE is secured using Secure Sockets Layer (SSLv3.0) or Transport Layer Security (TLSv1.0). Similarly, communication between the ID-Mark clients and the ID-Enforce gateway is secured using SSL to ensure that authentication data is not subject to disclosure.

When the TOE is configured such that two products are connected via their High Availability ports, the TOE has the ability to continue to enforce its security policies when one of the products fails and the other takes over.

2.3 TOE Documentation

Applied Identity offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of system security features. Refer to Section 6.2 for information about these and other evidence assurance documents.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the TOE and the environment of the TOE counters
- Assumptions made about the operational environment and the intended method of use for the TOE

Furthermore, the TOE is intended to be used in environments where the relative assurance that its security functions are enforced is commensurate with EAL 2 as defined in the CC.

3.1 Threats

T.ACCESS Users may be able to access network resources for which they are not authorized.

T.ACCOUNT Users might not be accountable for management of the TOE and access to controlled network resources.

3.2 Assumptions

A.LOCATE It is assumed that the TOE and its IT environment will be located such that the IT environment can deliver security policies to the TOE and such that the TOE can effectively control the resources it is intended to protect without the risk of bypassing the TOE altogether in order to access the resources to be protected.

A.MANAGE It is assumed that the TOE and its IT environment will be installed, configured, and managed in accordance with applicable security management guidance.

A.NOEVIL It is assumed that all administrators regardless of individual authority will be appropriately trusted not to intentionally attempt to exceed their authority using either physical or logical means.

A.PHYSICAL It is assumed that the TOE and its IT environment will be physically protected from tampering.

4. Security Objectives

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats, comply with defined organizational security policies, and address applicable assumptions.

4.1 Security Objectives for the TOE

O.ACCESS The TOE must enforce an access control policy defined by its environment to limit access to controlled network resources by network users.

O.AUDIT The TOE must be able to record security relevant events and in order to identify potential security violations and make that information readily available to authorized administrators.

O.AUTH The TOE must ensure that users are appropriately identified and have been authenticated prior to offering access to its own security management functions.

O.PROTECT The TOE must protect itself from potential tampering and bypass attempts.

4.2 Security Objectives for the IT Environment

OE.AUDIT The IT Environment must protect audit records generated by the TOE and provide reliable time information to include in the audit records.

OE.AUTH The IT environment must identify and authenticate users on behalf of itself and the TOE.

OE.POLICY The IT environment must ensure that access control policies to be enforced by the TOE have appropriate defaults and can be managed only by authorized users.

4.3 Security Objectives for the Environment

OE.LOCATE The TOE and its IT environment must be located such that the IT environment can deliver security policies to the TOE and so that the TOE can effectively control the resources it is intended to protect without the risk of bypassing the TOE altogether in order to access the resources to be protected.

OE.MANAGE The TOE and its IT environment must be installed, configured, and managed in accordance with applicable security management guidance.

OE.NOEVIL All administrators regardless of individual authority will be appropriately trusted not to intentionally attempt to exceed their authority using either physical or logical means.

OE.PHYSICAL The TOE and its IT environment must be physically protected from tampering.

5. IT Security Requirements

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

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are being satisfied by the TOE.

Table 1 - TOE Security Functional Components

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_STG.1a: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU_EXP.1: Timing of Authentication
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MTD.1a: Management of TSF data
	FMT_SMF.1a: Specification of Management Functions
	FMT_SMR.1a: Security roles
FPT: Protection of the TSF	FPT_FLS.1: Failure with preservation of secure state
	FPT_ITC.1: Inter-TSF confidentiality during transmission
	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

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) [**security management functions performed on the ID-Enforce appliance by authorized administrators, attempts of users to access protected network resources, attempts to log into the ID-Enforce appliance**].

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, 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, [**network resource (when applicable)**].

5.1.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**the administrator**] with the capability to read [**all audit data**] from the audit records.

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

5.1.1.4 Protected audit trail storage (FAU_STG.1a)

FAU_STG.1a.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1a.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

5.1.1.5 Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [**allow an administrator to export a copy of the audit record to external SYSLOG**] if the audit trail is full.

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**Network-based Access Control SFP**] on [**subjects – authenticated user sessions and unauthenticated user sessions; objects – network resources; and, operations – access**].

5.1.2.2 Security attribute based access control (FDP_ACF.1)

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

subjects

– authenticated user sessions (user ID, group, access privileges, IP address, and source MAC address) and

– unauthenticated user sessions (IP address and source MAC address);

objects

– network resources (IP address, port, service, and destination MAC address)].

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

1) if the TOE is in bridged mode and the source MAC address is configured to be denied in the TOE, access is denied and no further checking is performed;

2) if the TOE is in bridged mode and the destination MAC address is configured to be denied in the TOE, access is denied and no further checking is performed;

3) each of the following policies (Global, User, or Exception) is applied only if the current date is within the commencement and expiration date range defined for the policy;

4) for each of the following policies (Global, User, and Exception) if an optional schedule is configured, the policy is applied only if the current time is within the schedule defined for that policy;

5) if a 'Global Policy' as defined in the LDAP server associated with the TOE specifically allows or denies access to the requested IP address, port, and service for the user's IP address, the unauthenticated user session is granted or denied access to the resource (in accordance with the Global Policy) and no further checking is performed;

6) if the user's access privileges (based on user ID and group and optionally based on source IP address) are defined in a 'User Policy' in the LDAP server associated with the TOE in relation to the requested IP address, port, and service, the

authenticated user session is granted or denied access to the resource in accordance with the defined access privileges and no further checking is performed;
7) if the previous rules do not apply to the requested IP address, port, and service and if an 'Exception Policy' as defined in the LDAP server associated with the TOE specifically allows or denies access to the requested IP address, port, and service for the user's IP address, the unauthenticated user session is granted or denied access to the resource (in accordance with the Exception Policy);
8) if no previous rule applies access is denied].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**if the specific object being accessed is configured such that user authentication is not required, the user session is granted access to the resource**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**if the specific object being accessed is configured such that no access is allowed, the user session is refused access to the resource**].

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**administrator identities, administrator passwords**].

5.1.3.2 Timing of Authentication (FIA_UAU_EXP.1)

FIA_UAU_EXP.1.1 The TSF shall require each administrator user to be successfully authenticated before allowing any security management functions on behalf of that user.

FIA_UAU_EXP.1.2 The TSF shall require each network user to be successfully authenticated by the IT environment before allowing any TSF-mediated action on behalf of that user, except for accesses specifically configured to be allowed without authentication.

5.1.3.3 User identification before any action (FIA_UID.2)

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

5.1.4 Security management (FMT)

5.1.4.1 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [***delete*, [create]]** the [**administrator accounts**] to [**the administrator**].

5.1.4.2 Specification of Management Functions (FMT_SMF.1a)

FMT_SMF.1a.1 The TSF shall be capable of performing the following security management functions: [**review and archival of the audit logs, management of the local administrator identification and authentication security attributes**].

5.1.4.3 Security roles (FMT_SMR.1a)

FMT_SMR.1a.1 The TSF shall maintain the roles [**administrator**].
FMT_SMR.1a.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**the primary TOE component configured using the High Availability port ceases to respond to the secondary TOE component resulting in the secondary TOE component to take over**].

5.1.5.2 Inter-TSF confidentiality during transmission (FPT_ITC.1)

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted ~~IT product~~ **LDAP server** from unauthorised disclosure during transmission.

5.1.5.3 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure***] when it is transmitted between separate parts of the TOE.

5.1.5.4 Non-bypassabilitybypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.5 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are being satisfied by the IT environment of the TOE.

Table 2 - IT Environment Security Functional Components

Requirement Class	Requirement Component
FAU: Security audit	FAU_STG.1b: Protected audit trail storage
FIA: Identification and authentication	FIA_UAU_EXP.2: Authentication service
	FIA_UID.1: Timing of identification
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1b: Specification of Management Functions
	FMT_SMR.1b: Security roles
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps

5.2.1 Security audit (FAU)

5.2.1.1 Protected audit trail storage (FAU_STG.1b)

FAU_STG.1b.1 The ~~TSF~~ **IT environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1b.2 The ~~TSF~~ **IT environment** shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

5.2.2 Identification and authentication (FIA)

5.2.2.1 Authentication service (FIA_UAU_EXP.2)

FIA_UAU_EXP.2.1 The IT environment shall require each user to be successfully authenticated before allowing any security management functions to be performed by that user.

FIA_UAU_EXP.2.1 The IT environment shall provide user authentication decisions when requested by the TOE.

5.2.2.2 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The ~~TSF~~ **IT environment** shall allow [**functions unrelated to the management of the TOE by network administrators**] on behalf of the user to be performed before the user is identified.

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

5.2.3 Security management (FMT)

5.2.3.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The ~~TSF~~ **IT environment** shall enforce the [**Network-based Access Control SFP**] to restrict the ability to [***change_default, query, modify, delete***] the security attributes [**user access privileges**] to [**the Network administrator**].

5.2.3.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The ~~TSF~~ **IT environment** shall enforce the [**Network-based Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.1 The ~~TSF~~ **IT environment** shall allow the [**Network administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.2.3.3 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The ~~TSF~~ **IT environment** shall restrict the ability to [***query, modify, delete, [create]***] the [**network users**] to [**the Network Administrator**].

5.2.3.4 Specification of Management Functions (FMT_SMF.1b)

FMT_SMF.1b.1 The ~~TSF~~ **IT environment** shall be capable of performing the following security management functions: [**management of output syslog files for audit storage; management of network user authorization and identification; management of the Network-based Access Control SFP**].

5.2.3.5 Security roles (FMT_SMR.1b)

FMT_SMR.1b.1 The ~~TSF~~ **IT environment** shall maintain the roles [**Network administrator**].

FMT_SMR.1b.2 The ~~TSF~~ **IT environment** shall be able to associate users with roles.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT environment** shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 3 - EAL 2 Assurance Components

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

Each ID-Enforce appliance provides its own audit mechanism that will generate audit records for the security events that happen relative to the appliance. Auditable events include each security management function (see FMT_SMF.1a) performed by the administrator on the ID-Enforce appliance, attempts of users to access protected (including anonymous access attempts) network resources and attempts of users (presumably authorized administrators) to log into the ID-Enforce Command Line Interface (CLI) or for network resource access. Each audit record includes an explicit date and time stamp, explicit identification of the source (e.g., Policy or ID-Enforce modules) of the event, and other information depending on the type and source of the event. The type of event is apparent in its contents as is the outcome (e.g., success or failure) of the event. For most events the responsible user (either by username and/or IP address) is explicitly identified, but in the case of CLI functions, the events must be traced to CLI login events where the responsible user is identified. Additionally, each record includes any network resource applicable to the recorded event – note that some auditable events are not related to a given network resource.

An administrator is able to read all audit data stored within the TOE audit buffer via CLI functions.

The TOE protects audit records stored internally in the ID-Enforce appliance from unauthorized deletion and prevents unauthorized modifications to the audit records by restricting access to the associated functions. Using CLI commands, an administrator can define the maximum number of audit log files and also the maximum size for each log file in MBs. Once the maximum size is reached, the current log file is archived and a new log file is created. As the maximum number of log files is exceeded, the oldest log file is deleted. However, a copy of the audit records can also (if required) be exported to an external SYSLOG by an administrator for retention.

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

- FAU_GEN.1: The TOE generates audit events as indicated above.
- FAU_GEN.2: The TOE associated each auditable event with the identity of the user that caused the event.
- FAU_SAR.1: The TOE provides an interface that can be used by authorized administrators to read the audit trail.
- FAU_STG.1a: The TOE protects stored audit records from deletion and prevents unauthorized modification.
- FAU_STG.4: The TOE overwrites the oldest stored audit records and an authorized administrator is able to export a copy of the audit record to an external SYSLOG.

6.1.2 User data protection

The TOE enforces access control policies to determine what network resources a user will be able to access. This applies to users on an untrusted network that are identified and authenticated, and to a lesser extent to unauthenticated users, attempting to access defined resources on the protected network. Note that while the enforcement of the rules is a function of the TOE, the specific rules and applicable users are defined in the IT environment by the IT environment administrator (i.e., Network Administrator).

When a user (on the untrusted network) establishes a network session (recognized by IP address and user tags associated with each specific client when using ID-Mark[4]) the TOE retrieves the policies (i.e., User Policies) associated with that user, and the user's assigned groups, from its associated LDAP server to use when making subsequent network resource access decisions.

Those policies identify specifically which combinations of IP address, port, and network service the user is allowed to access, which IP addresses the user can access them from, and specifically how the user can access the resources (i.e., access privileges allowing or denying access). The TOE will either allow or deny the access attempt based on those policies in comparison with the specific resource access attempt. More specifically the TOE policies can specify one of four action types for each specified combination of user attributes:

- Accept – allow access without requiring the user to be authenticated (used in Global and Exception policies – see below);
- Auth – allow access to an authenticated user (used in User policies – see below);
- Deny – deny the requested access; or
- Reject – deny the requested access and also send a TCP reset to attempt to interrupt the connection request.

In this way, the TOE enforces a Network-based access control policy on user ID and group which resolve to a set of privileges that in turn specify allowable combinations of resource IP addresses, ports and services.

However, if a user (on the untrusted network) doesn't establish an authenticated session, the TOE will retrieve the policies associated with the requested resource (on the other network) in order to determine whether anonymous access is allowed. If anonymous access is allowed from the source IP address of the requester, the TOE will establish a session with the unauthenticated client to facilitate the anonymous access.

The above is accomplished by the definition of Global and Exception access policies. Global policies are always applied first and serve to identify resources (on the protected network) that are either always accessible or not accessible to unauthenticated users. Exception policies are used only when no other policy applies. When that happens, the Exception policies serve to define whether users (e.g., servers) with specific IP addresses should be able to access or not access specified resources. If the Exception policies also do not apply, then access is denied.

Each policy – Global, User, or Exception – has a commencement and expiration date and can optionally be configured with a schedule. Policies are only applied when the current date is within the defined commencement/expiration range. If there is a configured schedule, the policy is applied only when the current time is within the defined schedule. The commencement and expiration dates and the schedule can be defined in terms of combinations of specific day and time ranges (e.g., Monday through Friday from 8 am to 5 pm).

In addition, when the TOE is operating in bridged mode, before any policies are retrieved and applied, the TOE enforces MAC filtering rules. The MAC filtering rules are stored as tables within the TOE (i.e., the ID-Enforce appliance). When attempts are made to access resources protected by the TOE, the MAC address of the requesting traffic is compared against the source MAC address filter table and if a match is found the traffic is discarded and the attempt is denied. Similarly, the MAC address of the target resources is compared against the target MAC address filter table and if a match is found the traffic is discarded and the attempt is denied.

The access control policy as defined in this Security Target addresses the rules for authenticated and unauthenticated users on an untrusted network attempting to access resources on a protected network. While the TOE can impose restrictions on users on the protected network attempting to access resources on the untrusted network, that feature has not been subject to this evaluation and no relevant claims are presented for that feature. The product is primarily intended to control access to resources on a protected resource and in practice cannot reliably control access to resources on an untrusted network regardless of any features currently designed for that purpose.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1: The TOE enforces a Network-based access control policy.

[4] Note that the policies can be configured so that users can have access to network resources only when coming from predetermined IP addresses.

- FDP_ACF.1: The TOE enforces the access control policy based on authorized administrator configured rules to determine if access by subjects to objects is allowed.

6.1.3 Identification and authentication

The TOE implements a username/password authentication mechanism where each administrator is required to be identified and successfully authenticated (with matching user identifier and password stored by the TOE) prior to accessing any TOE security management functions available via the ID-Enforce CLI. Note that multiple administrators can be defined, each with their own unique identity and corresponding password.

In the evaluated configuration, administrator passwords will be at least eight (8) characters from the printable character set. Passwords must also include at least one uppercase letter and one punctuation mark. Note that initially the TOE has a single administrator account with a pre-configured default password - the administrator will be prompted to change the password with a warning during installation.

The TOE uses services of its IT environment in order to authenticate network users requesting access to protected network resources that require users to be identified. The TOE client, ID-Mark, can be integrated with the Windows graphical identification and authentication (GINA) library so that the authentication mechanism of the client host is used and the resulting credentials are forwarded to the TOE server, ID-Enforce, using the Windows mechanisms to do so. Alternately, the TOE client collects user credentials (e.g., username and password) and forwards those credentials to the TOE server for identification and authentication purposes. The TOE server supports two means of authentication in this manner. The first is via LDAP – the TOE can be configured to use a LDAP server in the IT environment where usernames and passwords provided by TOE users are forwarded to the LDAP server in order to authenticate the claimed identity. Alternately, the ID-Enforce Gateway software is linked with an RSA library that makes it compatible with RSA SecurID two-factor authentication. However, a user configured to use RSA SecurID two-factor authentication can cancel out of the SecurID login and establish an ID-Enforce session based only on his LDAP server user identity. The policies applied to him would then be based on the single-factor authentication and could be defined to be more restrictive than if he has been authenticated by SecurID. Note that both of these authentication solutions are considered to be outside the scope of this evaluation, except to the extent that they can be configured and invoked properly by the TOE.

Note that network users are defined in the IT environment, but the TOE requires users to provide identification and authentication information that is passed to the IT environment for authentication. The TOE then enforces the authentication decision it receives from the IT environment in order to decide whether to establish a user session that would facilitate interaction between the user and protected resources.

However, the TOE can be configured to allow access to specific resources without requiring user authentication, though the user would still be identified by the TOE. When anonymous access is allowed, the TOE still identifies users based on their IP addresses, though this information is not provided to the IT environment since no authentication is possible.

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

- FIA_ATD.1: The TOE maintains user identity and password for each administrator defined in the TOE.
- FIA_UAU_EXP.1: The TOE directly authenticates its own administrators and relies on an associated LDAP server in the IT environment for authentication of network users except where the access policy does not require users to be authenticated.
- FIA_UID.2: The TOE requires all users to be identified prior to offering any services.

6.1.4 Security management

The TOE provides an interface to administer the TOE and restricts access to its interfaces by requiring administrators to successfully logon with a valid user identity and password combination in order to access security management functionality. The TOE relies on the IT environment to facilitate and control access to security management functions associated with the TOE (e.g., management of the access control policies, network users, and syslog files). However, the TOE does include the Identisphere Manager (ID-Policy) application that can be run within a workstation in the environment to help facilitate management of access control policies.

The TOE restricts the ability to create or delete administrator accounts (including all applicable attributes) to the authorized administrator. Note that the only users defined explicitly within the TOE are administrators. Administrators, and only administrators, can access (i.e., for review or archival) the audit buffer and manage identification and authentication security attributes (including setting or changing passwords).

While the TOE technically supports a hierarchy of administrator roles with different authorities – *unprivileged*, *monitor*, and *administrator* – there is no claimed security distinct in this Security Target. This is because they all must directly connect to the TOE using a serial port or dedicated network connection and as such have physical access to the TOE and must all be relatively trusted to not attempt to exceed their authorities, physically or logically.

Network administrators (in the IT environment) manage the specific Network-based access control policies to query, modify, delete or change the default of user resource policies where restrictive default values are provided to the TOE that can only be altered by an authorized network administrator. Network administrators further manage the output of SYSLOG files for audit storage (as copied from the TOE); manage client authorization and identification and the Network-based SFP.

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

- FMT_MTD.1a: The TOE restricts administrator account creation and deletion to an authorized local administrator for the TOE.
- FMT_SMF.1a: The TOE provides an authorized administrator functions to review or archive audit logs and manage administrator identification and authentication attributes.
- FMT_SMR.1a: While the TOE technically supports multiple administrator roles, they are all considered to be an ‘administrator’ relative to this requirement.

6.1.5 Protection of the TSF

The TOE protects all TSF data transmitted between the TOE to a remote trusted IT product (i.e., LDAP server) from unauthorized disclosure by requiring the use of SSLv3.0 or TLSv1.0.[5] The same SSL implementation is included in the ID-Mark client and the ID-Enforce gateway to protect the communication between client and server to ensure that user authentication data is not disclosed on the network.

Within the networked architecture, the TOE sits between users and network resources to provide protection mechanisms for accessing the network resources on the trusted network, and as such ensures that all network resource access attempts are subject to the TOE access policies. Also, the TOE maintains a security domain for its own use that is protected from interference and tampering by virtue of the fact that it is a stand alone appliance carefully designed to limit access to its own configuration and functions. Further, the network appliance distinguishes network user sessions by virtue of their network connections which are managed as distinct entities within the TOE.

The TOE can be configured as a single product or as a pair of products connected via their High Availability ports. When configured for High Availability, one product (or TOE component) is configured as the primary and the other as the secondary and both are configured so that they are in the path between users and resources subject to the access control policy. Both components are also configured to use the same external LDAP server and the same security policies therein. During normal operation, the primary will enforce the policies and the secondary will monitor the primary via the High Availability port connection. Should the primary fail to respond, the secondary will immediately take over the enforcement of the access control policy. Since both component implement the same

[5] Note that the TOE uses OpenSSL FIPS version 1.1.2 for its server applications and forces the use of OpenSSL in FIPS mode. The TOE accommodates the following configurations: 3DES-CBC-SHA, AES128-SHA, and AES256-SHA. While the invocation of the OpenSSL library in order to establish an SSL or TLS connection with the LDAP server in the IT environment has been subject to this evaluation, this evaluation does not address evaluation of the OpenSSL implementation itself.

rules and share the same configuration (in the external LDAP server) the policy enforcement will continue, effectively unchanged and secure.

Once the ID-Enforce hardware appliance is installed and configured with the Network-based policy set, minimal access is required to interface directly with the unit. Only administrators are able to logon in order to access the CLI of the TOE.

The TOE provides authentication of administrator identities and passwords prior to allowing any access to security management functions and can be configured to enforce access decisions from an LDAP server in the IT environment where network users are also defined and authenticated (except when anonymous access is allowed) for the TOE.

Note that during the initial configuration of the ID-Enforce hardware appliance, the TOE is configured to connect to an NTP service in IT environment and uses the resulting information to provide reliable time stamps for TOE audit records.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_FLS.1: The TOE, when configured with two products connected via their High Availability ports, will switch from the primary to the secondary TOE component when the primary fails so that the secondary can continue to securely enforce the defined security policies.
- FPT_ITC.1: The TSF protects data transmitted from the TSF to a remote trusted IT product via use of SSL.
- FPT_ITT.1: The TSF protects TSF data sent between the TOE clients and server from disclosure via use of SSL.
- FPT_RVM.1: The TSF authenticates and validates the identity of authorized administrators to access protected objects.
- FPT_SEP.1: The TOE provides a security domain for its own use as it is a hardware appliance that sits on the network.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The Configuration Management (CM) measures applied by Applied Identity ensure that Configuration Items (CIs) are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Applied Identity performs CM on the TOE implementation representation, development, tests, user and administrator guidance, delivery and operation, vulnerability analysis and the CM Plan (CMP) where all is reflected in the configuration list as CIs. The CM documentation describes the procedures to uniquely identify CIs; the unique version of the TOE; labeling the TOE and all associated assurance evidence documentation; and describes the methods used to uniquely identify CIs.

These activities are documented in:

- Applied Identity Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Applied Identity provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Applied Identity's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Applied Identity also provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration.

Delivery and Operation (ADO) documentation describes the procedures for delivery of the TOE and its associated CIs to the user; and describes the delivery process/procedures to include how a user maintains security when distributed versions of the TOE are delivered to the user's site.

Installation, Generation and Start-up (IGS) procedures describe the secure installation, generation and start-up of the TOE that describes all the steps necessary.

These activities are documented in:

- Applied Identity Delivery and Operation
- Applied Identity User's Guide
- Applied Identity Quick Start Guide and Applied Identity Identisphere Manager Guide

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Applied Identity has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

The Functional Specification (FSP) describes the TOE Security Functions (TSF) and its external internal interfaces; describes the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages that complete represents the TSF and is internally consistent with all other TOE documentation.

The High-level Design (HLD) describes the TSF in terms of sub-systems and the security functionality provided by each subsystem; identifies all interfaces to the sub-systems and which of these are externally visible; and identifies all underlying hardware, firmware and software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware or software.

The Correspondence Representation (RCR) describes an analysis of all correspondence between all adjacent pairs of TSF representation provided (e.g., evaluation assurance documentation); and for each adjacent pair of provided TSF representations, the analysis demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completed refined in the less abstract TSF representation.

These activities are documented in:

- Applied Identity Functional Specification
- Applied Identity High-level Design Document
- Applied Identity Correspondence Representation

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Applied Identity provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

The Administrator Guide (ADM) provides administrator guidance addressed to system administrative personnel that describes the administrative functions and interfaces available to administer the TOE; describes how to administer the TOE in a secure manner; contains warnings about functions and privileges that should be controlled in a secure processing environment; describes all assumptions regarding user behavior relevant to the secure operation; describes all security parameters under the control of the administrator, indicating secure values, as appropriate; describes each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF; describes all security requirements for the IT environment relevant to administration; and is consistent with all other evaluation evidence assurance documentation.

The User (USR) guide provides user guidance that describes the functions and interfaces available to non-administrative users; describes the use of user-accessible security functions; contains warnings about user-accessible functions and privileges that should be controlled in a secure processing environment; clearly presents all user responsibilities necessary for security operation, include those related to assumptions regarding user behavior found in the statement of TOE security environment (i.e., Section 3 of the ST); and is consistent with all other evaluation evidence assurance documentation.

These activities are documented in:

- Applied Identity Administrator Guide
- Applied Identity User Guide
- Applied Identity Quick Start Guide

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- Applied Identity Test Plan
- Applied Identity Test Procedures
- Applied Identity Test Results

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

Applied Identity has conducted a Strength of Function (SOF) analysis (SOF) wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum SOF claim, SOF-Basic. Note that FIA_UAU_EXP.1 is the only applicable mechanism identified in this Security Target.

Applied Identity performs regular vulnerability analyses (ADV) of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Applied Identity SOF Analysis
- Applied Identity Vulnerability Assessment

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

This ST does not claim conformance to a Protection Profile (PP).

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats and usage assumptions by the security objectives. The following table pertains:

Table 4 – Environment to Objective Correspondence

Threats & Assumptions **Objectives**	**T.ACCESS**	**T.ACCOUNT**	**A.LOCATE**	**A.MANAGE**	**A.NOEVIL**	**A.PHYSICAL**
O.ACCESS	X					
O.AUDIT		X				
O.AUTH	X					
O.PROTECT	X					
OE.AUDIT		X				
OE.AUTH	X					
OE.POLICY	X					
OE.LOCATE			X			
OE.MANAGE				X		
OE.NOEVIL					X	
OE.PHYSICAL						X

8.1.1.1 T.ACCESS

Users may be able to access network resources for which they are not authorized.

This Threat is satisfied by ensuring that:

- O.ACCESS: The TOE must enforce the network access security policy defined by its environment in order to ensure that network resources are appropriately controlled.

- O.AUTH: The TOE must ensure that only authenticated, authorized users are able to manage the security functions it implements.
- O.PROTECT: The TOE must protect itself and its communications in order to protect the security functions it implements.
- OE.AUTH: The IT environment ensures that only authenticated, authorized users are able to manage the security functions it implements.
- OE.POLICY: The IT environment must allow the management of the network access security policy that it provides to the TOE for enforcement.

8.1.1.2 T.ACCOUNT

Users might not be accountable for management of the TOE and access to controlled network resources.

This Threat is satisfied by ensuring that:

- O.AUDIT: The TOE must generate records of security relevant events that ensure proper identification of responsible users and must also provide authorized administrators with the means to effectively review the records.
- OE.AUDIT: The IT environment must provide reliable time information for audit records and ensure their protection when stored in the environment.

8.1.1.3 A.LOCATE

It is assumed that the TOE and its IT environment will be located such that the IT environment can deliver security policies to the TOE and such that the TOE can effectively control the resources it is intended to protect without the risk of bypassing the TOE altogether in order to access the resources to be protected.

This Assumption is satisfied by ensuring that:

- OE.LOCATE: This objective for the environment directly corresponds with the identified assumption.

8.1.1.4 A.MANAGE

It is assumed that the TOE and its IT environment will be installed, configured, and managed in accordance with applicable security management guidance.

This Assumption is satisfied by ensuring that:

- OE.MANAGE: This objective for the environment directly corresponds with the identified assumption.

8.1.1.5 A.NOEVIL

It is assumed that all administrators regardless of individual authority will be appropriately trusted not to intentionally attempt to exceed their authority using either physical or logical means.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: This objective for the environment directly corresponds with the identified assumption.

8.1.1.6 A.PHYSICAL

It is assumed that the TOE and its IT environment will be physically protected from tampering.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: This objective for the environment directly corresponds with the identified assumption.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the ST. Note that the following table indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this ST are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy. The following table pertains:

Table 5 - Objective to Requirement Correspondence

Objectives Requirements	O.ACCESS	O.AUDIT	O.AUTH	O.PROTECT	OE.AUDIT	OE.AUTH	OE.POLICY
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SAR.1		X					
FAU_STG.1a		X					
FAU_STG.4		X					
FDP_ACC.1	X						
FDP_ACF.1	X						
FIA_ATD.1			X				
FIA_UAU_EXP.1			X				
FIA_UID.2			X				
FMT_MTD.1a			X				
FMT_SMF.1a		X	X				
FMT_SMR.1a			X				
FPT_FLS.1	X						
FPT_ITC.1				X			
FPT_ITT.1				X			
FPT_RVM.1				X			
FPT_SEP.1				X			
FAU_STG.1b					X		
FIA_UAU_EXP.2						X	
FIA_UID.1						X	
FMT_MSA.1							X
FMT_MSA.3							X
FMT_MTD.1b							X
FMT_SMF.1b					X	X	X
FMT_SMR.1b						X	
FPT_STM.1					X		

8.2.1.1 O.ACCESS

> *The TOE must enforce an access control policy defined by its environment to limit access to controlled network resources by network users.*

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: The TOE must implement an access control policy between known subjects and controlled network resources.
- FDP_ACF.1: The TOE must enforce the access control policy as defined by the IT environment of the TOE.
- FPT_FLS.1: When configured for High Availability, the TOE must continue to securely enforce its access control policy even should one of the two TOE components fail to operate.

8.2.1.2 O.AUDIT

The TOE must be able to record security relevant events and in order to identify potential security violations and make that information readily available to authorized administrators.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE must generate records of security relevant events.
- FAU_GEN.2: The TOE must ensure that applicable users are associated with audit records for accountability.
- FAU_SAR.1: The TOE must ensure that authorized users can access the audit trail.
- FAU_STG.1a: The TOE must protect the audit trail to the extent it is within its control to ensure the integrity of the recorded events.
- FAU_STG.4: The TOE will overwrite the oldest audit records to ensure that the most current events are available for review, but will also be capable of sending the audit records to an external server if so configured to help mitigate potential loss of audit records.
- FMT_SMF.1a: The TOE must provide functions necessary to manage the audit function of the TOE.

8.2.1.3 O.AUTH

The TOE must ensure that users are appropriately identified and have been authenticated prior to offering access to its own security management functions.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE must allow users to be defined so that authorized users can be recognized and offered appropriate security functions.
- FIA_UAU_EXP.1: The TOE must ensure that administrators are authenticated (directly) and other users are authenticated (by the IT environment) prior to offering access to security functions.
- FIA_UID.2: The TOE must ensure that all users are identified prior to offering access to security functions.
- FMT_MTD.1a: The TOE must limit the ability to manage user accounts to authorized administrators.
- FMT_SMF.1a: The TOE must provide any functions necessary for the management of user accounts.
- FMT_SMR.1a: The TOE must distinguish administrators from other users in order to appropriately limit access to security functions.

8.2.1.4 O.PROTECT

The TOE must protect itself from potential tampering and bypass attempts.

This TOE Security Objective is satisfied by ensuring that:

- FPT_ITC.1: The TOE must appropriately protect any communication of TSF data between the TOE and its associated LDAP server.
- FPT_ITT.1: The TOE must appropriately protect any communication of TSF data between the distributed TOE components.
- FPT_RVM.1: The TOE must protect itself from any bypass attempts.
- FPT_SEP.1: The TOE must protect itself from any tampering attempts and also must be able to distinguish users from itself and one another.

8.2.1.5 OE.AUDIT

The IT Environment must protect audit records generated by the TOE and provide reliable time information to include in the audit records.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_STG.1b: The IT environment must ensure that the audit trail is appropriately protected.
- FMT_SMF.1b: The IT environment must provide any necessary audit management functions.
- FPT_STM.1: The IT environment must provide reliable time information for use in audit records.

8.2.1.6 OE.AUTH

The IT environment must identify and authenticate users on behalf of itself and the TOE.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_UAU_EXP.2.1: The IT environment must provide authentication services to itself as well as the TOE to authenticate network users.
- FIA_UID.1: The IT environment must ensure that the identity of any users per forming functions related to the operation of the TOE must be identified prior to accessing any security related functions.
- FMT_SMF.1b: The IT environment must provide security management functions for the management of users that can be identified and authenticated by the IT environment.
- FMT_SMR.1b: The IT environment must distinguish administrators from other users in order to appropriately limit access to security functions.

8.2.1.7 OE.POLICY

The IT environment must ensure that access control policies to be enforced by the TOE have appropriate defaults and can be managed only by authorized users.

This IT Environment Security Objective is satisfied by ensuring that:

- FMT_MSA.1: The IT environment must restrict access to create or modify user access privileges.
- FMT_MSA.3: The IT environment must ensure that the security policy, to be enforced by the TOE, is restrictive by default and this default can be changed only by authorized users.
- FMT_MTD.1b: The IT environment must restrict access to create or modify network users.
- FMT_SMF.1b: The IT environment must provide security management functions for the security policy to be enforced by the TOE.

8.3 Security Assurance Requirements Rationale

The TOE is intended for an environment requiring a low to moderate level of assurance in the security functionality of conventional commodity TOEs, as presented in the statement of security environment (Section 3). The target assurance level of EAL 2 is appropriate for such an environment.

8.4 Strength of Functions Rationale

In accordance with EAL 2, a Strength of Functions claim of SOF-Basic has been made. EAL 2 represents a low to moderate level of security assurance and hence SOF-Basic should represent an appropriate strength of function. Note that both SOF-basic and EAL2 are intended to address only attackers with low attack potentials.

FIA_UAU_EXP.1 is the only SFR addressed by the TOE using a probabilistic or permutational mechanism and as such will be subject to a strength of functions analysis in order to ensure that mechanism is adequate.

8.5 Requirement Dependency Rationale

The following table identifies the dependencies of the requirements in this ST, including the requirements explicitly defined in the ST. As indicated in the table, all of the dependencies are satisfied or a rationale provides as to why a dependency is not being satisfied.

Table 6 - Requirement Dependencies

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	*FPT_STM.1*
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1a	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1a

ST Requirement	CC Dependencies	ST Dependencies
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and *FMT_MSA.3*
FIA_ATD.1	none	none
FIA_UAU_EXP.1	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1a and FMT_SMF.1a
FMT_SMF.1a	none	none
FMT_SMR.1a	FIA_UID.1	FIA_UID.2
FPT_FLS.1	ADV_SPM.1	This dependency is not applicable since the TOE consists of redundant components sharing the same configuration data. As such, there is no need to define the secure state since the resulting state is identical to the state prior to the failure.
FPT_ITC.1	none	none
FPT_ITT.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FAU_STG.1b	FAU_GEN.1	FAU_GEN.1
FIA_UAU_EXP.2	FIA_UID.1	*FIA_UID.1*
FIA_UID.1	none	none
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	*FMT_SMR.1b* and *FMT_SMF.1b* and FDP_ACC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	*FMT_MSA.1* and *FMT_SMR.1b*
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	*FMT_SMR.1b* and *FMT_SMF.1b*
FMT_SMF.1b	none	none
FMT_SMR.1b	FIA_UID.1	*FIA_UID.1*
FPT_STM.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

8.6 Explicitly Stated Requirements Rationale

This security target includes two explicitly stated requirements (i.e., requirements not defined in the Common Criteria (CC)). Each of these requirements, FIA_UAU_EXP.1 and FIA_UAU_EXP.2, have been designed to be very similar to FIA_UAU.1 as defined in the CC. Each is dependent that the user to be authenticated has already been identified and is placed within an existing security functional requirement class (FIA) and family (FIA_UAU).

FIA_UAU_EXP.1 is necessary since the CC only supports the case where the TOE does its own authentication. However, in this case the TOE authenticates administrators but relies on the environment to authenticate other (i.e., network) users.

FIA_UAU_EXP.2 is necessary since the CC does not support the case where authentication is performed on behalf of another component. In this case, the IT environment not only performs authentication for itself, but also when requested by the TOE.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The following table demonstrates the relationship between security requirements and security functions.

Table 7 - Security Functions vs. Requirements Mapping

Security Functions Requirements	Security audit	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAR.1	X					
FAU_STG.1a	X					
FAU_STG.4	X					
FDP_ACC.1		X				
FDP_ACF.1		X				
FIA_ATD.1			X			
FIA_UAU_EXP.1			X			
FIA_UID.2			X			
FMT_MTD.1a				X		
FMT_SMF.1a				X		
FMT_SMR.1a				X		
FPT_FLS.1					X	
FPT_ITC.1					X	
FPT_ITT.1					X	
FPT_RVM.1					X	
FPT_SEP.1					X	

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.