SailPoint IdentityIQ File Access Manager 8.1

Security Target

ST Version: 1.1
November 30, 2020

SailPoint Technologies, Inc.
11120 Four Points Drive
Suite 100
Austin, TX 78726

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.1.1 ST Identification

ST Title: SailPoint IdentityIQ File Access Manager 8.1 Security Target
ST Version: 1.1
ST Publication Date: November 30, 2020
ST Author: Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The product-specific terminology used throughout this ST is defined in Table 1. Technology terms that are related to the security functionality claimed by the TOE are defined in the introductory materials of the claimed Protection Profile. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Table 1: Customer Specific Terminology

Term	Definition
Administrator	An administrator is an individual who has permissions to modify the behavior of the TOE. This includes the individual that installs it on the underlying platform but can also include other individuals if administrator access is granted to them on the TOE's GUI or fat client.
Fat Client	The portion of the TOE which allows local authentication to and administration of the TOE.
Governed Data	The data created by the IdentityIQ File Access Manager for its primary functionality that is an abstract of information gathered from a managed resource, for example, file names and data-type tags.
GUI	The GUI is a web-based interface of the TOE that can be used to manage the TOE remotely using HTTPS.
Managed Resource	Remote system which the IdentityIQ File Access Manager product monitors to create governed data for its primary functionality.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Administrator uses to manage it (web browser, terminal client, etc.).
User	An individual who has access to the TOE but is not able to manage its behavior.

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 2. This table is to be used by the reader as a quick reference guide for acronym definitions.

Table 2: Acronym Definition

Acronym	Definition
AA	Assurance Activity
API	Application Programing Interface
ASLR	Address Space Layout Randomization
CC	Common Criteria
CFG	Control Flow Guard
CVSS	Common Vulnerability Scoring System
DEP	Data Execution Prevention
DRBG	Deterministic Random Bit Generator
EAF	Export Address Filtering
FAM	File Access Manager
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAF	Import Address Filtering

IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OSP	Organizational Security Policy
PII	Personally Identifiable Information
PP	Protection Profile
NIAP	National Information Assurance Partnership
RBG	Random Bit Generator
SFR	Security Functional Requirement
SAR	Security Assurance Requirement
SQL	Structured Query Language
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
WCF	Windows Communication Foundation

1.1.5 References

[1] Protection Profile for Application Software, version 1.3 (App PP)
[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-001
[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-002
[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-003
[5] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-004
[6] SailPoint IdentityIQ v8.1 File Access Manager Administrator Guide
[7] SailPoint IdentityIQ v8.1 File Access Manager Installation Guide
[8] SailPoint IdentityIQ File Access Manager 8.1 Supplemental Administrative Guidance for Common Criteria, Version 1.0

1.2 TOE Reference

The TOE is SailPoint IdentityIQ File Access Manager (FAM) version 8.1, which is an application installed/operated on an operating system.

1.3 TOE Overview

The TOE is the SailPoint IdentityIQ File Access Manager (FAM) version 8.1 application, referred to as IdentityIQ FAM or TOE from this point forward. IdentityIQ FAM's primary functionality is to allow its users to review and manage the governed data created by IdentityIQ FAM for monitoring enterprise data stored on one or more managed resources. The governed data allows IdentityIQ FAM users to identify

and classify data, understand on which managed resources within the network the data is stored, and understand which enterprise users have access to the data. IdentityIQ FAM's primary functionality of monitoring enterprise data was not evaluated, except where the product's functionality relates to the Security Functional Requirements (SFRs) included within the scope of the evaluation.

The following figure depicts the TOE boundary in the evaluated configuration:

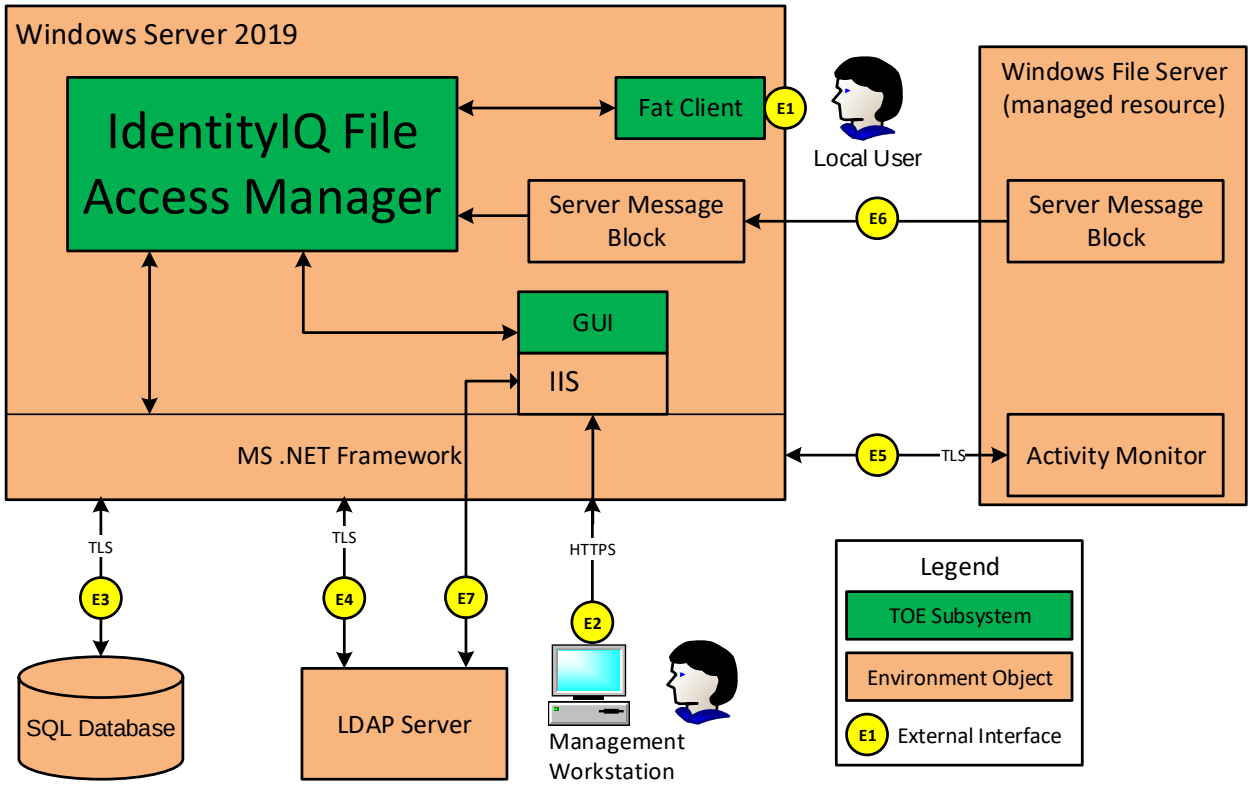

Figure 1: TOE Boundary

As illustrated in Figure 1, the TOE is comprised of the following components:

- **IdentityIQ File Access Manager** – The main portion of the TOE which performs all functionality of the application not related to direct interaction with administrators.
- **Fat Client –** The portion of the TOE which allows local authentication to and administration of the TOE.
- **GUI –** The portion of the TOE, which is comprised of only web pages, that allows remote administration of the TOE.
    - Window's Internet Information Services (IIS) is required to host the TOE's website content. IIS is a Windows service that is initiated during the platform's startup. The platform's IIS web server, via the .NET framework, enforces the establishment of the HTTPS trusted channel. IIS collects and authenticates the user provided credentials and then delivers the TOE's website content (remote management functionality) only to successfully authenticated users. The TOE (web pages) provides no functionality to control IIS nor does it collect, read, store, or authenticate the user provided credentials.

The TOE is installed on a Windows Server 2019 and through APIs the TOE utilizes several functions of the operating system to perform its operations. Specifically, the TOE relies on .NET Framework to function and IIS to host its GUI web pages. The diagram also depicts the use of the Windows operating

system's Server Message Block component to receive information about data on managed resources which IdentityIQ FAM turns into governed data.

The TOE has the following external interfaces:

- **E1: Local User to fat client** – Accessed through the Windows operating system, this is the local interface for authentication to and administration of the TOE.
- **E2: Remote Workstation to IIS (TOE GUI)** – Accessed through a web browser on a remote general-purpose management workstation, this is the remote administration interface of the TOE. This interface is over a secure HTTPS connection which is provided by .NET framework invoked by IIS. IIS and .NET framework are components of the Windows platform. This interface is being described for completeness of the required operational environment. To be clear, this operational environment interface is out-of-scope for testing but is required in order to test the GUI TOE component, which is in-scope of the evaluation.
- **E3: IdentityIQ FAM to SQL Database** – The TOE stores all of its configuration data, local user credentials, and governed data within a remote SQL Database. During operation, the TOE will read and write this data to the SQL Database over a secure TLS connection which is provided by .NET framework component of the Windows platform.
- **E4: IdentityIQ FAM to LDAP Server** – The TOE communicates with an LDAP Server that contains enterprise user data. The TOE verifies enterprise user credentials which are used for authenticating to the TOE's fat client as well as queries enterprise user account information for the IdentityIQ FAM product's primary functionality. This interface is over a secure TLS connection which is provided by .NET framework component of the Windows platform.
- **E5: IdentityIQ FAM to Activity Monitor** – If an Activity Monitor is installed on a managed resource, the TOE will communicate with the Activity Monitor to collect data on the managed resource for the IdentityIQ FAM product's primary purpose. This interface is over a secure TLS connection which is provided by .NET framework component of the Windows platform.
- **E6: Server Message Block to Server Message Block** – This is not a direct interface for the IdentityIQ FAM product as the connection is completely handled between the instance of Windows on each managed resource and the Windows platform IdentityIQ FAM is installed on. This interface is being described for completeness since the IdentityIQ FAM product creates governed data based upon the information provided over this interface which can result in the invocation of or display of data through the interfaces described above. This interface is not tested as part of the evaluated configuration.
- **E7: IIS to LDAP Server** – This is not a direct interface for the IdentityIQ FAM product as the connection is completely handled between the instance of Windows IIS and the LDAP server. This interface is being described for completeness of the required operational environment. This interface is not tested as part of the evaluated configuration.

1.4 TOE Type

The TOE type for SailPoint IdentityIQ FAM 8.1 is Application Software. The Protection Profile for Application Software specifies several use cases that conformant TOEs may implement. In particular, Use Case 2, Content Consumption, is defined as follows: "The application allows a user to consume content, retrieving it from either local or remote storage." SailPoint IdentityIQ FAM 8.1 meets the expectations of Use Case 2 because it implements content consumption by allowing its users to review and manage governed data created by IdentityIQ FAM for the monitoring of enterprise data stored on one or more managed resources.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

Table 3: Evaluated Components of the TOE

Component	Definition
IdentityIQ File Access Manager v8.1	The data monitoring software application. The TOE's software includes the main application, the fat client, and the web pages which comprise the GUI.

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the TOE's operational environment that must be present for the TOE to be operating in its evaluated configuration:

Table 4: Components of the Operational Environment

Component	Definition
Activity Monitor	A SailPoint software application which optionally can be installed on a Windows File Server (managed resource) to collect additional information to create governed data for the IdentityIQ FAM product's primary functionality. Although this software is produced by the same vendor as the TOE, the Activity Monitor is not part of the TOE and is not required for IdentityIQ FAM to perform its primary functionality.
Host Server	Physical system on which the IdentityIQ FAM software is installed.
Host Platform	The Microsoft Windows Server 2019 operating system on which the IdentityIQ FAM software is installed. This includes the required Windows Server components: Internet Information Services (IIS), .NET Framework (.NET), and Server Message Block (SMB).
LDAP Server	Stores enterprise user data which IdentityIQ FAM uses to authenticate users to its fat client and to query for the product's primary functionality. IIS uses the LDAP server to authenticate users for access to the TOE's GUI interface.
SQL Database	Stores a variety of configuration, operation, and governed data for the IdentityIQ FAM product. The connection to the SQL database is required in order for the TOE to function.
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE remotely via a web browser. Note that the fat client can also be used to administer the TOE locally.
Windows File Server(s)	One or more Windows Servers which the IdentityIQ FAM product monitors as a managed resource to create governed data for its primary functionality. Each Windows Server may optionally have an Activity Monitor installed on it to collect additional data for the IdentityIQ FAM product's primary functionality.

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate

license, and installed but not part of the TSF.

2.3.1 Not Installed

There are no optional components that are omitted from the installation process.

2.3.2 Installed but Requires a Separate License

There are no excluded components, applications, and or functionality that are installed and require a separate license for activation.

2.3.3 Installed But Not Part of the TSF

The TOE includes a number of functions that are outside the scope of the claimed Protection Profile. These functions are not part of the TSF because there are no SFRs that apply to them. This includes IdentityIQ FAM's primary functionality which allows its users to review and manage the governed data created by IdentityIQ FAM for the monitoring of enterprise data stored on one or more managed resources. The governed data allows IdentityIQ FAM users to identify and classify data, understand on which managed resources within the network the data is stored, and which enterprise users have access to the data.

2.4 Physical Boundary

SailPoint IdentityIQ FAM 8.1 is a software-only TOE and therefore its physical boundary is its software. The TOE does not include the hardware or operating system of the system on which it is installed. It also does not include the third party software which is required for the TOE to run. The following table lists the components that are required for the TOE's use in the evaluated configuration. These Operational Environment components are expected to be patched to include the latest security fixes for each component.

Table 5: Requirements for Operational Environment Components

OE Component	Requirement
Host Platform	Microsoft Windows Server 2019 Datacenter (1809) (includes: IIS, .NET, and SMB services)
Host Platform OS Type	64-bit
Host Server's Processor	Intel Xeon Gold 6230 (Cascade Lake)
SQL Database	SQL Server 2016
LDAP Server	Microsoft Windows Server 2019 Active Directory

2.5 Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Cryptographic Support
2. User Data Protection
3. Security Management
4. Privacy
5. Protection of the TSF
6. Trusted Path/Channel

2.5.1 Cryptographic Support

The TOE invokes the Windows platform's cryptographic services to secure data in transit communication. Due to this, the TOE does not directly invoke any DRBG functionality nor does the TOE perform generation of asymmetric cryptographic keys. The TOE also uses the Windows platform's Data Protection API to store the credentials for accessing the SQL database.

2.5.2 User Data Protection

The TOE relies on the Windows platform to handle the following network connections, to include all of their cryptographic operations:

- respond to TLS connection requests from an Activity Monitor to receive managed resource data,
- initiate a TLS connection to an LDAP server to perform authentication requests and query enterprise user account information, and
- initiate a TLS connection to read and write TOE configuration data and governed data to the SQL database.

2.5.3 Security Management

The administrator that installs the TOE will set the initial credentials for accessing the TOE and will also be assigned the owner permissions for the TOE's software by the Windows platform. Due to the Windows platform's access permissions and the TOE's install directory being C:\Program Files, the TOE's binaries and data files are protected from unprivileged modification. The TOE's administrators are able to configure the TOE and perform tasks via the TOE's GUI and fat client. All TOE configuration options are stored in the remote SQL database.

2.5.4 Privacy

The TOE ensures the privacy of its administrators and users by not providing any ability to collect or transmit personally identifiable information (PII) over the network.

2.5.5 Protection of the TSF

The TOE relies on the Windows platform to request memory and will not request an explicit memory address. The TOE does not allocate any memory region with both write and execute permissions. As a .NET framework application, the TOE has stack-based buffer overflow protections. The TOE uses a number of Windows platform APIs and third party libraries as part of its operation.

Administrators can verify the TOE's version by checking any of the TOE's binary files or by authenticating to the fat client. The TOE automatically checks its software version against the latest available software version provided by SailPoint. TOE software, including patch updates, is signed with a DigiCert certificate. Administrators can initiate the software update process through the fat client. The TOE's uninstallation process results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

2.5.6 Trusted Path/Channel

The TOE invokes the Windows platform to encrypt all data-in-transit communications between itself and another trusted IT product. The trusted IT products, encryption protocols used, and the purpose of the connection have been described under the “User Data Protection” section above.

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 April 2017.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through November 30, 2020.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 extended to include all applicable NIAP and International interpretations through November 30, 2020.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profile:

- Protection Profile for Application Software, version 1.3 [App PP]

3.5 Package Claims

The TOE claims exact conformance to the App PP, version 1.3, which is extended with CC Part 3.

The TOE claims following Selection-Based SFRs that are defined in the appendices of the claimed PP:

- FPT_TUD_EXT.2

This does not violate the notion of exact conformance because the PP specifically indicates these as allowable selections and options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are in exact conformance with the App PP.

3.7 Conformance Claim Rationale

The App PP states the following: “The requirements in this document apply to application software which runs on any type of platform. Some application types are covered by more specific PPs, which may be expressed as PP-Modules of this PP. Such applications are subject to the requirements of both this PP and the PP-Module that addresses their special functionality. PPs for some particularly specialized applications may not be expressed as PP-Modules at this time, though the requirements in this document should be seen as objectives for those highly specialized applications.

Although the requirements in this document apply to a wide range of application software, consult guidance from the relevant national schemes to determine when formal Common Criteria evaluation is expected for a particular type of application. This may vary depending upon the nature of the security

functionality of the application."

The TOE is a standalone application which runs on a desktop/server Windows platform and is therefore considered to be relevant to the App PP. There are no PP-Modules to the App PP that are applicable to SailPoint, so the TOE is characterized only as a software application.

3.8 Technical Decisions

Technical Decisions that effected the SFR wording have been annotated with a Footnote. The following is a complete list of Technical Decisions that apply to the App PP evaluation activities that must be performed during the evaluation of this TOE:

Table 6: Technical Decisions

TD #	Title	References	Changes			Analysis to this evaluation	
			SFR	AA	Notes	NA	Reason
TD0554	iOS/iPadOS/Android AppSW Virus Scan	AVA_VAN.1		X			AA: Test modified for iOS/Android platforms and update for AVA_VAN search and analysis applicable for all.
TD0548	Integrity for installation tests in AppSW PP 1.3	FPT_TUD_EXT.1.3		X			AA: Test wording
TD0544	Alternative testing methods for FPT_AEX_EXT.1.1	FPT_AEX_EXT.1		X			AA: Test wording
TD0543	FMT_MEC_EXT.1 evaluation activity update	FMT_MEC_EXT.1		X			AA: Test wording
TD0540	Expanded AES Modes in FCS_COP	FCS_COP.1(1)	X	X		X	Not claiming SFR. AA Test.
TD0521	Updates to Certificate Revocation (FIA_X509_EXT.1)	FIA_X509_EXT.1	X	X	X	X	Not claiming X509.
TD0519	Linux symbolic links and FMT_CFG_EXT.1	FMT_CFG_EXT.1.2		X		X	Not claiming Linux OS.
TD0515	Use Android APK manifest in test	FDP_DEC_EXT.1		X		X	Not claiming Android OS.
TD0510	Obtaining random bytes for iOS/macOS	FCS_RBG_EXT.1		X		X	Not claiming iOS or macOS.
TD0498	Application Software PP Security Objectives and Requirements Rationale	Section 4.3 and Section 5.2 in PP			X		Updates PP rationale.
TD0495	FIA_X509_EXT.1.2 Test Clarification	FIA_X509_EXT.1.2		X		X	Not claiming X509.
TD0486	Changes to App PP v1.3 related to PP-Modules	Section 2, FDP_DAR_EXT.1	X			X	Change to selection in FDP_DAR_EXT.1 which is not being claimed
TD0473	Support for Client or Server TOEs in FCS_HTTPS_EXT	FCS_HTTPS_EXT.1, FCS_HTTPS_EXT.2	X	X	X	X	Not claiming HTTPS.
TD0465	Configuration Storage for .NET Apps	FMT_MEC_EXT.1		X			AA: Test TOE is a .NET App.
TD0445	User Modifiable File Definition	FPT_AEX_EXT.1.4		X	X		AA: Test User modifiable file definition clarity.

TD0444	IPsec selections	FTP_DIT_EXT.1.1, FIA_X509_EXT.2.1	X	X	X		AA:TSS, Test Change to wording of FTP_DIT_EXT.1.1 included. Not claiming IPSEC or X509.
TD0437	Supported Configuration Mechanism	FMT_MEC_EXT.1.1	X	X	X		AA: TSS, Tests Support of file encryption.
TD0435	Alternative to SELinux for FPT_AEX_EXT.1.3	FPT_AEX_EXT.1.3		X		X	Not claiming Linux.
TD0434	Windows Desktop Applications Test	FDP_DEC_EXT.1.1		X			AA Test.
TD0427	Reliable Time Source	A.Platform	X				Changes to wording in ST: Updated wording to Assumption.
TD0416	Correction to FCS_RBG_EXT.1 Test Activity	FCS_RBG_EXT.1.1		X			Test AA modified for invoking the platform.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the App PP.

Table 7: TOE Threats

Threat	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

4.2 Organizational Security Policies

There are no Organizational Security Policies in the App PP.

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the App PP.

Table 8: TOE Assumptions

Assumption	Assumption Definition
A.PLATFORM[1]	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE..
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

[1] TD0427

4.4.1 TOE Security Objectives

This section identifies the security objectives of the TOE as defined by the App PP.

Table 9: TOE Security Objectives

Objective	Objective Definition
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.4.2 Security Objectives for the Operational Environment

The TOE's operating environment must satisfy the following objectives:

Table 10: Operational Environment Objectives

Objective	Objective Definition
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required.

5.2 Extended Security Assurance Requirements

The extended Security Assurance Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with *italicized* text.
- **Refinement:** allows the addition of details. Indicated with **bold** text and italicized text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

If SFR text is reproduced verbatim from text that was formatted in a claimed PP (such as if the PP's instantiation of the SFR has a refinement or a completed assignment), the formatting is not preserved. This is so that the reader can identify the operations that are performed by the ST author as opposed to the PP author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Table 11: Security Functional Requirements for the TOE

Class Name	Component Identification	Component Name
Cryptographic Support	FCS_CKM_EXT.1	Cryptographic Key Generation Services
	FCS_RBG_EXT.1	Random Bit Generation Services
	FCS_STO_EXT.1	Storage of Credentials
User Data Protection	FDP_DAR_EXT.1	Encryption of Sensitive Application Data
	FDP_DEC_EXT.1	Access to Platform Resources
	FDP_NET_EXT.1	Network Communications
Security Management	FMT_CFG_EXT.1	Secure by Default Configuration
	FMT_MEC_EXT.1	Supported Configuration Mechanism
	FMT_SMF.1	Specification of Management Functions
Privacy	FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
Protection of the TSF	FPT_AEX_EXT.1	Anti-Exploitation Capabilities
	FPT_API_EXT.1	Use of Supported Services and APIs
	FPT_IDV_EXT.1	Software Identification and Versions
	FPT_LIB_EXT.1	Use of Third Party Libraries
	FPT_TUD_EXT.1	Integrity for Installation and Update
	FPT_TUD_EXT.2	Integrity for Installation and Update
Trusted Path/Channel	FTP_DIT_EXT.1	Protection of Data in Transit

6.3 Security Functional Requirements

6.3.1 Class FCS: Cryptographic Support

6.3.1.1 *FCS_CKM_EXT.1 Cryptographic Key Generation Services*

FCS_CKM_EXT.1.1

The application shall [

- generate no asymmetric cryptographic keys].

6.3.1.2 *FCS_RBG_EXT.1 Random Bit Generation Services*

FCS_RBG_EXT.1.1

The application shall [

- use no DRBG functionality

] for its cryptographic operations.

6.3.1.3 *FCS_STO_EXT.1 Storage of Credentials*

FCS_STO_EXT.1.1

The application shall [

- invoke the functionality provided by the platform to securely store [*SQL database credentials*]

] to nonvolatile memory.

6.3.2 Class FDP: User Data Protection

6.3.2.1 *FDP_DAR_EXT.1 Encryption of Sensitive Application Data*

FDP_DAR_EXT.1.1

The application shall [

- protect sensitive data in accordance with FCS_STO_EXT.1

] in non-volatile memory.

6.3.2.2 *FDP_DEC_EXT.1 Access to Platform Resources*

FDP_DEC_EXT.1.1

The application shall restrict its access to [

- network connectivity].

FDP_DEC_EXT.1.2

The application shall restrict its access to [

- no sensitive information repositories].

6.3.2.3 *FDP_NET_EXT.1 Network Communications*

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- respond to [*connection requests from an Activity Monitor*],
- [*query an LDAP server, reading and writing to the SQL database*]].

6.3.3 Class FMT: Security Management

6.3.3.1 *FMT_CFG_EXT.1 Secure by Default Configuration*

FMT_CFG_EXT.1.1

The application shall only provide enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

6.3.3.2 *FMT_MEC_EXT.1 Supported Configuration Mechanism*

FMT_MEC_EXT.1.1[2]

The application shall [

- invoke the mechanisms recommended by the platform vendor for storing and setting configuration options].

6.3.3.3 *FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1

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

- [*configuration of the LDAP server(s) to which the TOE will communicate*,
  perform tasks that read data from LDAP server(s),
  perform tasks that read or write data to the SQL database,
  query the current version of the TOE,
  perform the software update process]].

6.3.4 Class FPR: Privacy

6.3.4.1 *FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information*

FPR_ANO_EXT.1.1

The application shall [

[2] TD0437

- not transmit PII over a network].

6.3.5 Class FPT: Protection of the TSF

6.3.5.1 *FPT_AEX_EXT.1 Anti-Exploitation Capabilities*

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [*none*].

FPT_AEX_EXT.1.2

The application shall [

- not allocate any memory region with both write and execute permissions].

FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4

The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5

The application shall be built with stack-based buffer overflow protection enabled.

6.3.5.2 *FPT_API_EXT.1 Use of Supported Services and APIs*

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

6.3.5.3 *FPT_IDV_EXT.1 Software Identification and Versions*

FPT_IDV_EXT.1.1

The application shall be versioned with [[*major release number, minor release number, patch number, service pack number*]].

6.3.5.4 *FPT_LIB_EXT.1 Use of Third Party Libraries*

FPT_LIB_EXT.1.1

The application shall be packaged with only [*third party libraries listed in Table 13*].

6.3.5.5 *FPT_TUD_EXT.1 Integrity for Installation and Update*

FPT_TUD_EXT.1.1

The application shall [provide the ability] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2

The application shall [provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3

The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4

The application installation package and its updates shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5

The application is distributed [as an additional software package to the platform OS].

6.3.5.6 *FPT_TUD_EXT.2 Integrity for Installation and Update*

FPT_TUD_EXT.2.1

The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2

The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

6.3.6 Class FTP: Trusted Path/Channel

6.3.6.1 *FTP_DIT_EXT.1 Protection of Data in Transit*

FTP_DIT_EXT.1.1[3]

The application shall [

- invoke platform-provided functionality to encrypt all transmitted data with [TLS]

] between itself and another trusted IT product.

6.4 Statement of Security Functional Requirements Consistency

The SFRs included in the ST represent all required SFRs specified in the claimed PP as well as a subset of the optional SFRs. All hierarchical relationships, dependencies, and unfulfilled dependency rationales in the ST are considered to be identical to those that are defined in the claimed PP.

[3] TD0444

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are in exact conformance with the App PP.

7.1 Class ASE: Security Target evaluation

7.1.1 ST introduction (ASE_INT.1)

7.1.1.1 *Developer action elements:*

ASE_INT.1.1D

The developer shall provide an ST introduction.

7.1.1.2 *Content and presentation elements:*

ASE_INT.1.1C

The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C

The ST reference shall uniquely identify the ST.

ASE_INT.1.3C

The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C

The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C

The TOE overview shall identify the TOE type.

ASE_INT.1.6C

The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C

The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C

The TOE description shall describe the logical scope of the TOE.

7.1.1.3 *Evaluator action elements:*

ASE_INT.1.1E

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

ASE_INT.1.2E

The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

7.1.2 Conformance claims (ASE_CCL.1)

7.1.2.1 *Developer action elements:*

ASE_CCL.1.1D

The developer shall provide a conformance claim.

ASE_CCL.1.2D

The developer shall provide a conformance claim rationale.

7.1.2.2 *Content and presentation elements:*

ASE_CCL.1.1C

The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C

The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C

The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C

The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C

The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C

The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C

The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C

The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C

The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

7.1.2.3 *Evaluator action elements:*

ASE_CCL.1.1E

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

7.1.3 Security objectives for the operational environment (ASE_OBJ.1)

7.1.3.1 *Developer action elements:*

ASE_OBJ.1.1D

The developer shall provide a statement of security objectives.

7.1.3.2 *Content and presentation elements:*

ASE_OBJ.1.1C

The statement of security objectives shall describe the security objectives for the operational environment.

7.1.3.3 *Evaluator action elements:*

ASE_OBJ.1.1E

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

7.1.4 Extended components definition (ASE_ECD.1)

7.1.4.1 *Developer action elements:*

ASE_ECD.1.1D

The developer shall provide a statement of security requirements.

ASE_ECD.1.2D

The developer shall provide an extended components definition.

7.1.4.2 *Content and presentation elements:*

ASE_ECD.1.1C

The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C

The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C

The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C

The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C

The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

7.1.4.3 *Evaluator action elements:*

ASE_ECD.1.1E

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

ASE_ECD.1.2E

The evaluator shall confirm that no extended component can be clearly expressed using existing components.

7.1.5 Stated security requirements (ASE_REQ.1)

7.1.5.1 *Developer action elements:*

ASE_REQ.1.1D

The developer shall provide a statement of security requirements.

ASE_REQ.1.2D

The developer shall provide a security requirements rationale.

7.1.5.2 *Content and presentation elements:*

ASE_REQ.1.1C

The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C

The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C

All operations shall be performed correctly.

ASE_REQ.1.5C

Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C

The statement of security requirements shall be internally consistent.

7.1.5.3 *Evaluator action elements:*

ASE_REQ.1.1E

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

7.1.6 TOE summary specification (ASE_TSS.1)

7.1.6.1 *Developer action elements:*

ASE_TSS.1.1D

The developer shall provide a TOE summary specification.

7.1.6.2 *Content and presentation elements:*

ASE_TSS.1.1C

The TOE summary specification shall describe how the TOE meets each SFR.

7.1.6.3 *Evaluator action elements:*

ASE_TSS.1.1E

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

ASE_TSS.1.2E

The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

7.2 Class ADV: Development

7.2.1 Basic Functional Specification (ADV_FSP.1)

7.2.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.2.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.2.1.3 *Evaluator action elements:*

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 SFRs.

7.3 Class AGD: Guidance Documentation

7.3.1 Operational User Guidance (AGD_OPE.1)

7.3.1.1 *Developer action elements:*

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.3.1.2 *Content and presentation elements:*

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.3.1.3 *Evaluator action elements:*

AGD_OPE.1.1E

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

7.3.2 Preparative Procedures (AGD_PRE.1)

7.3.2.1 *Developer action elements:*

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.3.2.2 *Content and presentation elements:*

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.3.2.3 *Evaluator action elements:*

AGD_ PRE.1.1E

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

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.4 Class ALC: Life Cycle Support

7.4.1 Labeling of the TOE (ALC_CMC.1)

7.4.1.1 *Developer action elements:*

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.4.1.2 *Content and presentation elements:*

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.4.1.3 *Evaluator action elements:*

ALC_CMC.1.1E

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

7.4.2 TOE CM Coverage (ALC_CMS.1)

7.4.2.1 *Developer action elements:*

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.4.2.2 *Content and presentation elements:*

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.4.2.3 *Evaluator action elements:*

ALC_CMS.1.1E

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

7.4.3 Timely Security Updates (ALC_TSU_EXT.1)

7.4.3.1 *Developer Actions Element:*

ALC_TSU_EXT.1.1D

The developer shall provide a description in the TSS of how timely security updates are made to the TOE.

ALC_TSU_EXT.1.2D

The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

7.4.3.2 *Content and presentation elements:*

ALC_TSU_EXT.1.1C

The description shall include the process for creating and deploying security updates for the TOE software.

ALC_TSU_EXT.1.1C

The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

ALC_TSU_EXT.1.1C

The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

7.4.3.3 *Evaluator action elements:*

ALC_TSU_EXT.1.1E

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

7.5 Class ATE: Tests

7.5.1 Independent Testing - Conformance (ATE_IND.1)

7.5.1.1 *Developer action elements:*

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

ATE_IND.1.1E

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

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.6 Class AVA: Vulnerability Assessment

7.6.1 Vulnerability Survey (AVA_VAN.1)

7.6.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.6.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.6.1.3 *Evaluator action elements:*

AVA_VAN.1.1E

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

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

8.1 Cryptographic Support

8.1.1 FCS_CKM_EXT.1:

The TOE does not perform generation of asymmetric cryptographic keys.

8.1.2 FCS_RBG_EXT.1:

The TOE does not directly invoke any DRBG functionality for any SFR related functionality.

8.1.3 FCS_STO_EXT.1:

The credentials for accessing the SQL database are stored using the Data Protection API. The TOE will invoke the Windows platform to encrypt these credentials using a certificate located in the Windows Certificate Store and will then invoke the Windows platform to store the encrypted credentials.

Note that the following credentials are not applicable to this SFR because they are not stored by the TOE. The user credentials used for authentication to the TOE are stored on one or more LDAP servers or in the SQL database (both external to the TOE). The LDAP server(s) contains the enterprise user credentials for authenticating the fat client and for authenticating to IIS for access to the GUI. The SQL database contains the local user credentials for authenticating to the TOE's fat client. The SQL database also contains the credentials for accessing the LDAP server(s). The TOE relies on the Windows platform to establish a secure TLS connection with the LDAP server(s) and SQL database before sending these credentials to ensure they are transmitted over an encrypted channel. These credentials include the usernames and their associated hashed passwords as well as the credentials for access to the applicable LDAP server(s).

8.2 User Data Protection

8.2.1 FDP_DAR_EXT.1:

The credentials for accessing the SQL database are stored using the Data Protection API, in accordance with FCS_STO_EXT.1. The TOE will invoke the Windows platform to encrypt these credentials using a certificate located in the Windows Certificate Store and then invoke the Windows platform to store the encrypted credentials.

8.2.2 FDP_DEC_EXT.1:

During operation of the TOE, access to the underlying Windows platform is limited to use of network connectivity hardware for communication with web browsers for GUI access, the SQL database, the LDAP server(s), and Activity Monitor application(s). The TOE does not access any sensitive data repository provided by the underlying Windows platform.

8.2.3 FDP_NET_EXT.1:

During TOE operation, the TOE will rely on the Windows platform to handle the following network connections, to include all of their cryptographic operations:

- respond to TLS connection (TCP port 8000) requests from an Activity Monitor to receive managed resource data,
- initiate a TLS connection to an LDAP server to perform authentication requests and query enterprise user account information, and
- initiate a TLS connection to read and write TOE configuration data and governed data to the SQL database.

Note the TOE opens default TCP ports 8001, 8005, 8006, 8008, 8010, and 9200 for local communication between components on the machine where the TOE is installed.

The following description is for completeness in understanding the operational environment network requirements of the TOE. The host platform's IIS web server (part of the OE) is required to handle user-initiated HTTPS requests from a web browser for remote access to the administrative GUI TOE component (TCP port 443). IIS is a Windows service, of which the TOE has no control over, and is initiated during the platform's startup. IIS performs the credential collection and authentication prior to allowing access to the TOE's website content (remote management functionality).

8.3 Security Management

8.3.1 FMT_CFG_EXT.1:

The TOE's installation directory is C:\Program Files. The administrator that performs the installation will receive the owner permissions for the TOE's binaries and data files. Due to C:\Program Files being the installation directory, the Windows platform will protect the TOE's binaries and data files from modification by unprivileged users. There are no default credentials for the TOE. During the installation process, the administrator that performs the installation will define their own password for the TOE's main administrative account.

8.3.2 FMT_MEC_EXT.1:

The TOE maintains a set of configuration options to run in the evaluated configuration. These configuration options are stored in the remote SQL database and are accessed by the TOE invoking a Windows platform-provided TLS connection.

8.3.3 FMT_SMF.1:

The TOE provides the following management functions to its users:

- configuration of the LDAP server(s) to which the TOE will communicate via the fat client
- perform tasks that read data from LDAP server(s) via the GUI and the fat client
- perform tasks that read or write data (i.e., local user credentials, configuration data, governed data) to the SQL database via the GUI and the fat client
- query the current version of the TOE via the fat client
- perform the software update process via the fat client

8.4 Privacy

8.4.1 FPR_ANO_EXT.1:

The TOE application does not collect personally identifiable information (PII) for administrators or users. Therefore, the TOE application does not transmit PII data over the network.

8.5 Protection of the TSF

8.5.1 FPT_AEX_EXT.1:

The TOE relies on the Windows platform to request memory and will not request an explicit memory address. During the compilation of the TOE's software, the /NXCOMPAT flag is set to ensure that Data Execution Prevention (DEP) protections are enabled. The TOE does not allocate any memory region with both write and execute permissions. The TOE's software runs as Managed Code in the .NET framework, and therefore no additional stack-based buffer overflow protection needs to be enabled. The TOE will operate on Windows Server 2019 with the security features of Windows Defender Exploit Guard Exploit Protection configured on, with the following enabled: Control Flow Guard (CFG), randomize memory allocations (Bottom-Up ASLR), Export Address Filtering (EAF), Import Address Filtering (IAF), and DEP. The TOE does not write user-modifiable files to directories that contain executable files.

8.5.2 FPT_API_EXT.1:

The TOE is installed on the Windows platform and uses only the following supported Windows platform APIs in order to function.

Table 12: .Net Framework APIs

Microsoft.AspNet	Microsoft.Deployment	Microsoft.Fsharp	Microsoft.Online
Microsoft.Owin	Microsoft.Practices	Microsoft.SharePoint	Microsoft.SqlServer
Microsoft.VisualBasic	Microsoft.Web	Microsoft.Win32	Microsoft.Windows
System.Collections	System.ComponentModel	System.Configuration	System.Data
System.Deployment	System.Diagnostics	System.DirectoryServices	System.Drawing
System.Dynamic	System.Globalization	System.IO	System.IdentityModel
System.Linq	System.Management	System.Media	System.Net
System.Reactive	System.Reflection	System.Resources	System.Runtime
System.Security	System.ServiceModel	System.ServiceProcess	System.Text
System.Threading	System.Timers	System.Transactions	System.Web
System.Windows	System.Xml		

8.5.3 FPT_IDV_EXT.1:

Every binary file of the TOE is marked with the TOE's version. An administrator can right click the binary file, click properties, and view the TOE's version under the details tab. The versioning nomenclature used by the TOE is #.#.#.#. The first number indicates the major release number and is incremented by the value of 1. The second number is the minor release number and is incremented by the value of 1. The third number represents the patch number and is incremented by the value of 1000. The fourth number represents the service pack number and is incremented by the value of 1000.

8.5.4 FPT_LIB_EXT.1:

The following is a list of the third party libraries used by the TOE:

Table 13: TOE Libraries

AlphaFS	am-js-tree	angular	Aspose.Cells
AutoMapper	bootstrap-daterangepicker	bootstrap-rtl	bootstrap-sass-official
Bouncy Castle	C1 Control	Caliburn Micro	Chart.js
CommandLineParser	Common.Logging	CommonServiceLocator	d3
Elasticsearch	Elasticsearch.Net and Nest	Ensure.That	es5-shim
font-awesome	Google API Client	Hyland Document Filters	jQuery-contextMenu
jquery-contextMenuRtl	jquery.easy-pie-chart	json3	Json.NET
jstree-bootstrap-theme	libphonenumber-csharp	LinqKit	LiteDB
lodash	log4net	Lucene.Net	Microsoft.ApplicationInsights
Microsoft.Asp.Net	Microsoft.Owin	Microsoft.Web	Microsoft Sharepoint Server & Client API
modernizr	moment	.NET Framework	NContext
Ncontext.Common	Netapp ManageOntap API	Nhibernate	Novel Directory LDAP
nvd3	offline	Oracle Data Provider for .Net	Owin
Owin.Scim	protobuf-net	Quartz.Net	RabbitMQ
ReadonlyREST	Remotion.Linq	restangular	RestSharp
spin.js	SSH.Net	Telerik Controls	ua-parser-js
Unity	Unity.Abstractions	Unity.log4net	Unity.WebAPI
Visifire for WPF	WebActivatorEx	WPFToolKit	WPFToolKit Extended
WPF Solution Drag and Drop			

8.5.5 FPT_TUD_EXT.1 and FPT_TUD_EXT.2:

Each customer that is entitled to the TOE software has a username and password for accessing SailPoint's customer portal. Connections to the SailPoint customer portal are protected using HTTPS. SailPoint's customer portal contains a full list of all versions of the product that are currently still supported. The TOE administrator downloads the software installation package or software update package from SailPoint's customer portal. This is the only method for distributing TOE software. Therefore, the TOE does not have the capability to download, modify, replace or update its own binary code.

The software installation package is in either the standard Windows Installer (.MSI) format or .EXE format. During the build process, SailPoint digitally signs the .MSI or .EXE file using their private key and their certificate signed by DigiCert. During the installation process, the platform will validate the certificate using the public key from DigiCert that is already loaded on the platform and verifies the digital signature on the .MSI or .EXE file using the public key in the certificate. The installation process will only occur if the signature validation is successful.

The software version of the TOE is always displayed after the administrator authenticates to the TOE via the fat client. The TOE automatically checks its software version against the latest available software version provided by SailPoint. If a newer software version is available, the TOE will send an email to the configured email address of an administrator.

Software update packages are in the Windows Universal Application package (.APPX) format. During the build process, SailPoint digitally signs a software update package using their private key and their certificate signed by DigiCert. Once a software update package is on the system where the TOE is installed, any administrator account with permission to the 'Start Installation' button via the fat client can initiate the update process. The administrator would identify the location of the software update package and select it for import through the fat client. The fat client will request the platform to validate the certificate using the public key from DigiCert that is already loaded on the platform and verifies the digital signature on the software update package using the public key in the certificate. If signature validation is successful, the administrator can click the 'Start Installation' button to initiate the update. If the validation of the digital signature fails, an error will be generated and the 'Start Installation' button will not be displayed.

The TOE's uninstallation process results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events. The administrator will execute the uninstall through the TOE's installers which will stop and remove all services and will then begin removing files related to the application. The administrator will then use the platform's uninstall application program to complete the TOE's uninstall.

8.5.5.1 *Timely Security Updates:*

SailPoint has defined a Product Vulnerability Management Policy for their operations which applies to all of their product lines, including the entire IdentityIQ FAM product. The contents of this section are the publicly releasable description of SailPoint's Product Vulnerability Management Policy.

SailPoint continuously performs security assessments of IdentityIQ FAM for vulnerabilities by performing internal testing as well as contracting third party security verification organizations. Customers can report security issues by opening a support case through SailPoint's support website: https://support.sailpoint.com/. The support website is protected with HTTPS and requires customers to enter their email address and password associated with their SailPoint customer account.

When a potential vulnerability is discovered or reported, SailPoint will confirm internally that a vulnerability is present in IdentityIQ FAM. SailPoint will then develop a mitigation to address the vulnerability which can either be a configuration change to IdentityIQ FAM or the development of a software update package. The mitigation will be relayed to customers by providing a security notification on the SailPoint support site along with information regarding the mitigation. SailPoint's support team also provide their customers a public key for support team emails which can contain updates regarding security notifications. This allows SailPoint to send signed and encrypted emails to customers which have signed up for email updates. Mitigations which require configuration changes to IdentityIQ FAM will have the steps defined within the security notification. Mitigations which require software updates will result in a software update package being created and released per the process described in Section 8.5.5.

SailPoint utilizes the Common Vulnerability Scoring System (CVSS) v3 scoring system to weight the severity of confirmed vulnerabilities. SailPoint is committed to having mitigations available for Critical and High vulnerabilities within 30 days. Medium vulnerabilities will have mitigations available within 90 days. Items that score as Low and Informational have no set commitment period but are often placed into consideration by SailPoint's Product Management team for prioritization in a future release.

8.6 Trusted Path/Channel

8.6.1 FTP_DIT_EXT.1:

The TOE invokes the platform's .NET framework to encrypt the communications between the TOE and the remote SQL database. The TOE calls the .NET System.Data API for this interface. All communication over this interface is protected by TLS.

The TOE invokes the platform to communicate with a remote LDAP server for two functions: authenticating TOE users via the fat client and performing queries of enterprise user account information for the product's primary functionality. For fat client authentication, the TOE invokes the platform's Windows Communication Foundation (WCF) to encrypt the communications between the TOE and the remote LDAP server. The TOE calls the System.ServiceModel API to perform this function. For querying enterprise user data, the TOE invokes the platform's .NET framework to encrypt the communications between the TOE and the remote LDAP server. The TOE calls the .NET System.DirectoryServices API for this function. All communication to the remote LDAP server is protected by TLS.

The TOE invokes the platform's .NET framework to encrypt the communications between the TOE and one or more remote Activity Monitors. The TOE calls the .NET System.ServiceModel API for this interface. All communication over this interface is protected by TLS.