SailPoint IdentityIQ v8.3p2
Common Criteria Security Target

ST Version: 1.2
March 31, 2023

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. This ST targets exact conformance with the following Protection Profile (PP):

- Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1

1.1.1 ST Identification

ST Title: SailPoint IdentityIQ v8.3p2 Common Criteria Security Target
ST Version: 1.2
ST Publication Date: March 31, 2023
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 terminology used throughout this ST is defined in Table 1-1 and 1-2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
Administrator	The subset of organizational users who have authorizations to manage the TSF.

Term	Definition
Entitlement	A privilege assigned to an account on a target system that is configured through provisioning.
Governance-based	A "top down" approach to provisioning with a focus on managing entitlements within a defined governance lifecycle.
Identity Store	The repository in the Operational Environment where organizational users are defined along with their credential data and identity attributes.
Organizational User	A user defined in the identity store that has the ability to interact with assets in the Operational Environment.
Provisioning	The process of configuring the settings and/or account information of environmental assets based on the privileges that different types of organizational users need on them to carry out their organizational responsibilities.
User	In an IdentityIQ context, is synonymous with organizational user.

Table 1-1: Customer Specific Terminology

Term	Definition
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the 'admin' role.
Security Administrator	Synonymous with Authorized Administrator.
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 Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
AD	Active Directory
ADSI	Active Directory Services Interface
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ICF	Identity Connector Framework
ICM	Identity and Credential Management
JDBC	Java Database Connectivity
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
MS	Microsoft

Acronym	Definition
OS	Operating System
PP	Protection Profile
SMTP	Simple Mail Transfer Protocol
SPML	Service Provisioning Markup Language
SysAdmin	System Admin
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 1-3: Acronym Definition

1.1.5 References

[1] Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 (ICM PP)

[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003

[5] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004

[6] NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009

[7] NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, December 2001

[8] NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012

[9] FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001

[10] FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

[11] Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008

[12] SailPoint IdentityIQ IdentityIQ System Configuration version 8.3

[13] SailPoint IdentityIQ Lifecycle Manager version 8.3

[14] SailPoint IdentityIQ Active Directory Connector version 8.3

[15] SailPoint IdentityIQ Installation Guide version 8.3

[16] SailPoint IdentityIQ IdentityIQ Tasks version 8.3

[17] SailPoint IdentityIQ Password Management version 8.3

[18] SailPoint_IdentityIQ_Capabilities.xls

1.2 TOE Reference

The TOE is SailPoint IdentityIQ v8.3p2.

1.3 TOE Overview

IdentityIQ is a governance-based Identity and Access Management (IAM) software solution for enterprise users. IdentityIQ provides a variety of IAM processes that include automated access certifications, policy management, access request and provisioning, password management and identity intelligence. The evaluated TOE functionality includes only the security functional behavior which is defined in the claimed Security Functional Requirements, including the identity and password management functionality described above.

The TOE communicates with authentication stores in the operational environment to provide password management as well as create, modify, and delete enterprise user data. Provisioning is done automatically using connectors provided by the operational environment to the authentication stores. In the evaluated configuration, the TOE uses two Microsoft Active Directory installed on Windows Server 2016 in separate domains. If a single user has different accounts across multiple domains, the administrator of the TOE can correlate all of the user's accounts into a single identity within IdentityIQ. This provides a centralized user interface to manage each of the user's accounts across the separate domains. The TOE does not store any enterprise passwords or user data locally. The TOE only acts as a centralized location to manage enterprise user data. When a user authenticates to an enterprise endpoint, the password is still being compared to the password that is stored in the enterprise's authentication store.

The following figure depicts the TOE boundary:

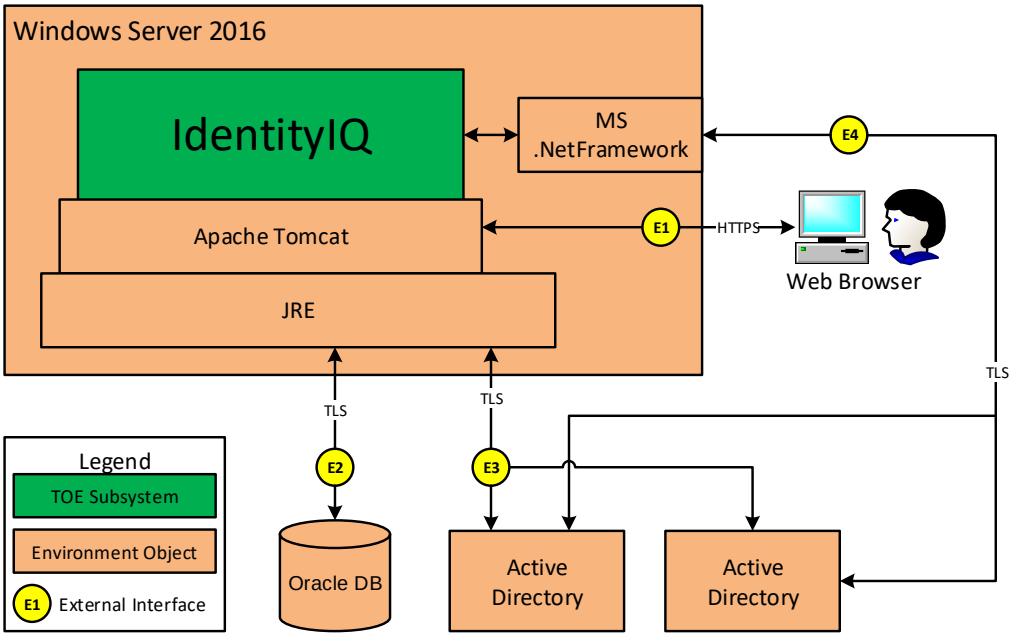

Figure 1-1: TOE Boundary

As illustrated in Figure 1-1, the IdentityIQ is the lone component of the evaluation. There are 4 secure interfaces that are external to the TOE. The data that traverses these interfaces is protected by TLS. This secure protocol is provided by the Operational Environment.

All management activities are completed through the web browser that connects to the Administrative GUI. All administrators attempting to access the TOE have to provide valid identification and authentication credentials. This channel is secured using HTTPS that is provided by the Apache Tomcat using its OpenSSL module.

Policy data, enterprise user data, and IdentityIQ user data that includes password data, attributes and entitlements and other user information is stored in an external database. In the evaluated configuration, the database used is Oracle 19c. This connection is secured using a TLS protected channel between the environmental JRE's JDBC and the Oracle database.

IdentityIQ connects to Active Directory to perform authentication of enterprise users and administrative users to IdentityIQ. This connection occurs over a TLS protected channel between the environmental JRE's JNDI and the environmental Active Directory server.

IdentityIQ connects to Active Directory to perform compliance checks (aka "certifications") by reading the enforced policies and enterprise user data that is stored within Active Directory. The compliance check is done to identify any conflicts between the Active Directory instances. The TOE performs provisioning by writing updates to this data on the Active Directory instances based upon configuration updates made in the TOE by administrators. This connection occurs over a TLS protected channel between the environmental MS .NET Framework's ADSI and the environmental Active Directory server.

The following figure, taken from the ICM PP, shows the reference architecture for an identity and credential management product:

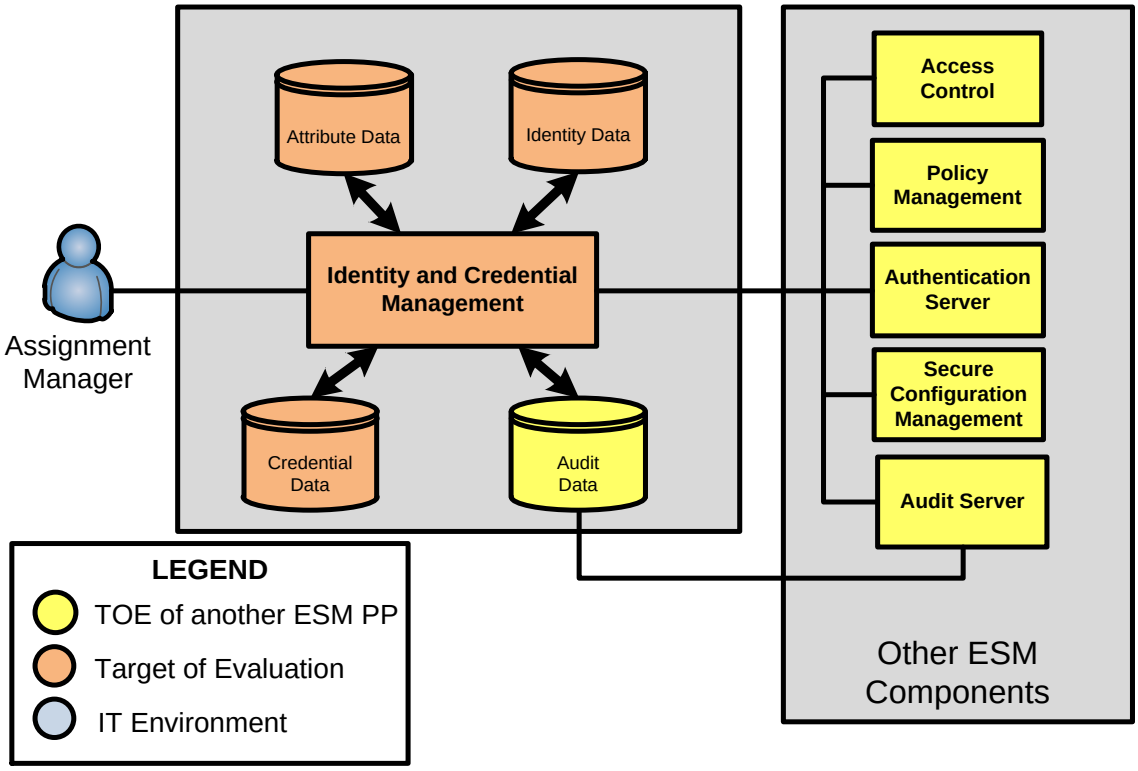

Figure 1-2: ESM PP context for the TOE

In general, the following correspondence can be seen between Figure 1-2 above and the TOE diagram shown in Figure 1-1

- Identity and Credential Management – the TOE
- Attribute Data, Credential Data, Identity Data – Active Directory store
- Audit Data – Oracle Database
- Other ESM Components – endpoint systems

Figure 1-2 was derived from the conceptual diagram presented in the ICM PP with some minor differences. These differences do not impact the ability of the TOE to claim exact conformance with the ICM PP. They are as follows:

- The TOE does not interface with an ESM Audit Server, ESM Authentication Server, or ESM Secure Configuration Management product since these Protection Profiles have not been published as of the publication of this ST.
- In the evaluated configuration, the TOE is expected to interface with existing organizational data stores rather than introducing its own, so these are part of the Operational Environment and not the TSF.
- The environmental components that the TSF is expected to provision are general organizational assets and not explicitly ESM products. For example, the TSF can assign an individual a certain set of privileges on an operating system or manage some attributes of the individual that are defined in an organizational data store. However, if another ESM product uses data from this organizational data store to enforce its own TSF (e.g. another product derives its administrator login and privileges from Active Directory attributes), the TSF may implicitly manage the behavior of this product by managing the organizational user attributes that govern its behavior.

1.4 TOE Type

The TOE type for IdentityIQ is Enterprise Security Management, and more specifically identity and credential management. The TOE is a software application that is used to associate an organization's computer system users with role and privilege information based on their position within the organization. This concept of correlating the attributes of an individual with permissions assigned to their account(s) on IT resources can be understood as identity management. Additionally, the TSF provides measures to govern a user's authentication credential (password), including the ability to change this credential and the ability to effectively revoke it by changing the status of the associated account. These capabilities can collectively be understood as identity and credential management. This facilitates Enterprise Security Management by providing more effective and centralized control over what kinds of users have what access to what kinds of resources within the organization.

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:

Component	Definition
IdentityIQ v8.3p2	The identity and credential management software application. The evaluated configuration of IdentityIQ includes the license for Lifecycle Manager portion of IdentityIQ. **Lifecycle Manager** — IdentityIQ Lifecycle Manager manages changes to access through password management interfaces and automated lifecycle events.

Table 2-1: Evaluated Components of the TOE

2.2 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.

2.2.1 Not Installed

Privileged Account Management Module — IdentityIQ Privileged Account Management module provides a standardized approach for extending critical identity governance processes and controls to highly privileged accounts, enabling IdentityIQ to be used as a central platform to govern standard and privileged accounts.

Connectors and Integration Modules — IdentityIQ offers Integration Modules that support the extended enterprise IT infrastructure. Third party provisioning and service desk integration enable multiple sources of fulfillment to access change. Service catalog integration supports a unified service request experience with integrated governance and fulfillment. Mobile device management integration mitigates risk posed by mobile devices through centralized visibility, control and automation.

Open Identity Platform — SailPoint's Open Identity Platform lays the foundation for effective and scalable IAM within the enterprise. It establishes a common framework that centralizes identity data, captures business policy, models roles, and takes a risk-based, proactive approach to managing users and resources.

Password Manager — IdentityIQ Password Manager delivers a simple-to-use solution for managing user passwords across cloud and on-premises applications policies from any desktop browser or mobile device.

Amazon Web Services (AWS) Governance Module — Enables organizations to extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments to provide a central point of visibility, administration, and governance across the entire

enterprise. This includes policy discovery and access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and federated access support.

SAP Governance Module — Improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures.

AI Services — AI Services is a SaaS-delivered data analysis product designed to work with IdentityIQ. The goal of AI Services is to improve the identity governance process provided by IdentityIQ through data analysis and machine learning. The features provided when IdentityIQ and AI Services operate together are called IdentityAI.

IdentityIQ File Access Manager (FAM) — IdentityIQ FAM allows 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 (i.e. classifications), understand on which managed resources within the network the data is stored, and understand which enterprise users have access to the data.

Cloud Access Management Module — Cloud Access Management module provides the ability to discover who has access to what, how that access is being granted, and implement pre-configured policies that automate detection of compliance violations in multi-cloud environments.

2.2.2 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.

2.2.3 Installed but Not Part of the TSF

Compliance Manager — IdentityIQ Compliance Manager automates access certifications, policy management, and audit reporting through a unified governance framework.

Unevaluated out-of-the-box Capabilities — IdentityIQ includes the following out-of-the-box capabilities that are not evaluated: Alert Admin, Plugin Admin, SCIM Executor, Form Admin, Full Access Admin Console, PAM Admin, View Admin Console, FAM Admin, AIServices Admin, Rapid Setup Admin, Rapid Setup Viewer, Rapid Setup Configuration Admin, Rapid Setup Configuration Viewer, Rapid Setup Birthright Role Admin, Rapid Setup Identity Operations Admin, PAM Viewer, and CAM Admin. These out-of-the-box capabilities are unevaluated because they are unrelated to the functionality covered by the SFRs and most of which require components which have been excluded from the TOE.

Rapid Setup — Rapid Setup provides pre-configured, best practice use cases to onboard applications, and reduce deployment time.

2.3 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
Active Directory	Stores enterprise user data and policies for the operational environment. Also serves as an authentication store for the TOE.
Application Server	Apache Tomcat application server that is used to host the IdentityIQ software as well as the GUI.
Database	Stores a variety of configuration, operation, and audit data for the TOE. In the evaluated configuration, the TOE will use Oracle 19c for its database. The connection to the database is required in order for the TOE to function.
Server	Physical system on which the IdentityIQ software is installed. The physical system is comprised of a Microsoft Windows Server 2016 OS, Microsoft .NET Framework, Apache Tomcat Application Server and JRE.
Web Browser	The interface that is used to access the IdentityIQ Web GUI. In the evaluated configuration the GUI will be managed via Chrome, version 110 (or later).

Table 2-2: Components of the Operational Environment

2.4 Physical Boundary

The physical boundary of the TOE includes the IdentityIQ software that is installed on top of the Apache Tomcat application server. The TOE does not include the hardware or operating systems of the systems 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 software 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.

Component	Requirement
Server OS	Microsoft Windows Server 2016
OS Type	64-bit
Application Server	Apache Tomcat 9.0
Database	Oracle 19c
Authentication Store	Windows Server 2016 Active Directory
Java Platform	Oracle JDK 11

Table 2-3: Operational Environment Software Requirements

In addition to the server requirements, a web browser is required for any system used to administer the TOE. In the evaluated configuration, the TOE was tested using Chrome version 110 (or later) and the compatibility of other browsers was not assessed.

2.4.1 Excluded from the Evaluated Configuration

The following list contains Operational Environment software that is supported by the TOE but is not included, installed, or tested in the evaluated configuration:

Operating Systems

- IBM AIX 7.2 and 7.3
- Red Hat Linux 8.5
- SuSE Linux 15
- Solaris 10 and 11

• Windows Server 2019 and 2022

Databases

• IBM DB2 11.5

• MySQL 5.7 and 8.0

• Microsoft SQL Server 2019 and 2017

Cloud Platforms

• AWS EC2

• AWS Aurora

• AWS RDS (MySQL, MS SQL, Oracle)

• Azure (VM, Azure SQL)

• Google Cloud Platform - Google Compute Engine

Application Servers

• IBM WebSphere 9.0

• IBM WebSphere Liberty 20.0 and 21.0

• JBoss Enterprise 7.3 and 7.4

• Oracle WebLogic 14c and 12cR2

Java Platform

• Oracle JDK 8 and 17

• Sun JDK 8, 11, and 17

• IBM JDK 8, 11, and 17

• AdoptOpenJDK 11 and 17 for Windows

• Red Hat OpenJDK 11 and 17 for Linux

Enterprise User Stores

All other enterprise user stores and their associated connectors are excluded from the evaluation. (In the evaluated configuration, Active Directory will be the only enterprise user store.)

2.5 Logical Boundary

The TSF is comprised of several security features. Each of the security features identified belongs to one of several general categories, as identified below.

1. Enterprise Security Management
2. Security Audit
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access

7. Trusted Path/Channels

2.5.1 Enterprise Security Management

The TOE performs enterprise user authentication using Active Directory as well as its own authentication mechanisms within the Operational Environment. IdentityIQ requires each user to enter valid identification in the form of a username and authentication in the form of a password to gain access to the TOE.

IdentityIQ uses connectors that are provided by the Operational Environment to communicate with third-party ESM products. In the evaluated configuration, IdentityIQ connects to Active Directory using the ADSI connector. The TOE will read and directly manage user data as well as configuration information, such as policy data, from any connected Active Directory. The TOE will also push user data to any instance of Active Directory to allow enterprise users to be centrally managed and address any conflicts of user data throughout the enterprise.

2.5.2 Security Audit

The TOE generates audit records of its behavior and administrator activities. Audit data includes date, time, event type, subject identity, and other data as required. Audit data is written to a remote Oracle 19c database. The communication between the TOE and the remote database is secured using TLS that is provided by the JRE's JDBC that resides in the Operational Environment.

2.5.3 Identification and Authentication

When an administrator authenticates to the TOE, the TOE will associate the username with a principal. The principal, along with the capabilities, rights, and dynamic scopes determine the access that the administrator will have while logged into the TOE.

The TOE provides mechanisms to reduce the likelihood of unauthorized access. The TOE is able to lock out an administrative account after a specific number of unsuccessful authentication attempts. This setting is defaulted to lockout users after five failed authentication attempts but is configurable by an administrator. Password complexity, history, length, and lifetime can be configured by administrators. These security parameters are used to reduce the likelihood of a successful brute force attack to gain unauthorized access to the system.

2.5.4 Security Management

The TOE is managed by authorized administrators using a web GUI. All administrative actions are performed via the web GUI. The TOE uses capabilities to control user access to functionality within the product. Users or a group of users can be assigned to one or more of the 27 evaluated out-of-the-box capabilities. The TOE also allows administrators to create or modify capabilities and assign them to users or groups of users.

2.5.5 Protection of the TSF

In the evaluated configuration, the TOE requests the JRE to encrypt administrator credentials before being sent to the Operational Environment's Oracle database. The TOE does not store any cleartext password data in memory and there are no credentials stored locally on the TOE. Similarly, the answers

to user security questions (used if the user has forgotten their password) are stored in an encrypted format in the Oracle database. In the evaluated configuration, the TOE does not store any secret or private keys and thus, there is no mechanism to disclose this information.

2.5.6 TOE Access

The TOE can display a warning banner prior to allowing any administrative actions to be performed. In the event that the maximum timeout value for inactivity has been reached, the TOE will terminate the remote session. A user can also terminate their own session by selecting the logout button.

2.5.7 Trusted Path/Channels

The TOE's evaluated configuration enforces secure communication between the TOE and IT entities in the operational environment by using the Operational Environment's JNDI, ADSI, and JDBC installed on the local system. These trusted channels transfer TOE data, enterprise user data, and IdentityIQ administrator data to and from IT entities within the Operational Environment. When users log on to the TOE via a web GUI, a trusted path is established, and it is secured using HTTPS that is provided by Apache Tomcat using its OpenSSL module.

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

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 31 March 2023.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant to include all applicable NIAP and International interpretations through 31 March 2023.

Note that this evaluation also includes evaluation assurance activities that are defined in the claimed Protection Profile that has augmented the CEM and are not considered to be alterations to Part 3.

3.4 PP Claims

This ST claims exact compliance to the following Protection Profile:

- Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 [ESM_ICM PP]

3.5 Package Claims

The TOE claims exact compliance to a Protection Profile that is conformant with CC Part 3. The TOE claims following "architectural variations" SFRs that are defined in the appendices of the claimed PP:

- FIA_AFL.1
- FIA_SOS.1
- FTA_SSL.3
- FTA_SSL.4
- FMT_MTD.1

This does not violate the notion of exact compliance because the PP specifically indicates these as allowable 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 claims exact compliance to a Protection Profile. The ST is conformant to the claimed package.

3.7 Technical Decisions

		Changes			Analysis to this evaluation	
TD#	**Title**	**SFR**	**AA**	**Notes**	**NA**	**Reason**
TD0621	Corrections to FCS_TLS_EXT.1 in ESM PPs				X	This evaluation does not claim any FCS requirements
TD0576	FTP_ITC and FTP_TRP Updated	X	X			Wording changes in SFR and clarification in TSS.
TD0574	Update to FCS_SSH in ESM PPs				X	This evaluation does not claim any FCS requirements
TD0573	Update to FCS_COP and FCS_CKM in ESM PPs				X	This evaluation does not claim any FCS requirements
TD0079	RBG Cryptographic Transitions per NIST SP 800-131A Revision 1				X	This evaluation does not claim any FCS requirements.
TD0066	Clarification of FAU_STG_EXT.1 Requirement in ESM PPs			X		Clarification made in the TSS.
TD0055	Move FTA_TAB.1 to Selection-Based Requirement			X		FTA_TAB.1 is claimed.
TD0042	Removal of Low-level Crypto Failure Audit from PPs				X	This evaluation does not claim any FCS requirements.

Table 3-1 Technical Decisions

3.8 Conformance Claim Rationale

The ICM PP states the following: "This protection profile focuses on the aspect of ESM that is responsible for enforcing identity and credential management. Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise. They will also maintain the organizational attributes that are associated with these subjects. By providing a means for subjects to validate their identities and determining the relationship these subjects have to the enterprise, an Identity and Credential Management product is able to support enterprise accountability and access control."

The TOE is a software application that communicates with enterprise authentication stores to allow for the centralized enrollment of enterprise users which includes the issuing and maintenance of credentials, association of user accounts with identity attributes, and definition of privileges based on these associated attributes. As such, it is consistent with the definition of an identity and credential management product as stated in the ICM PP. Therefore, the conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

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

Threat	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.
T.FORGE	A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
T. INSUFFATR	An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.RAWCRED	A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the ICM PP.

Policy	Policy Definition
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Table 4-2: TOE Organization Security Policies

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 ICM PP.

Assumption	Assumption Definition
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ENROLLMENT	There will be a defined enrollment process that confirms user identity before the assignment of credentials.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.FEDERATE	Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.

Table 4-3: TOE Assumptions

Note that the TSF satisfies A.ESM by establishing a secure connection to one or more environmental identity stores that other ESM products may use for administrator identification, authentication, and/or administration. The TOE is not expected to connect directly to other ESM products to share this data; it will be shared with other ESM products through updating a data store that is in the Operational Environment of other ESM products.

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.

4.4.1 TOE Security Objectives

This section identifies the security objectives of the TOE. These objectives have been taken from the ICM PP. A subset of the optional security objectives has been included based on the set of optional SFRs that are claimed by the TSF.

Objective	Objective Definition
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.

Objective	Objective Definition
O.MANAGE	The TOE will provide Assignment Managers with the capability to manage the TSF.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTCRED	The TOE will be able to protect stored credentials.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

Table 4-4: TOE Objectives

4.4.2 Security Objectives for the Operational Environment

This section identifies the security objectives of the environment into which the TOE is expected to be deployed. These objectives have been taken from the ICM PP. A subset of the optional environmental objectives has been included based on the set of optional SFRs that are not claimed by the TSF.

Objective	Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.

Table 4-5: TOE Operational Environment Objectives

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. The associated mappings of assumptions to environmental objectives, SFRs to TOE objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profile.

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 that requires their usage.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

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 bold text.**
- **Refinement:** allows the addition of details. *Indicated with 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.

Finally, when multiple cases are specified for the handling of TSF behavior based on the contents of a selection, only the applicable case(s) has been retained. This unambiguously defines the TSF by excluding non-applicable conditional statements. Application notes have been included in all instances of this so that all omissions are clearly identified. If an entire SFR component is non-applicable (e.g. FAU_GEN_EXT.1.3 only applies to TOE-internal audit data storage, which the TSF does not provide), the component has been retained.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Enterprise Security Management	ESM_EAU.2	Reliance on Enterprise Authentication
	ESM_EID.2	Reliance on Enterprise Identification
	ESM_ICD.1	Identity and Credential Definition
	ESM_ICT.1	Identity and Credential Transmission
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_STG_EXT.1	External Audit Trail Storage
Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_USB.1	User-Subject Binding
	FIA_SOS.1	Verification of Secrets
Security Management	FMT_MOF.1	Management of Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Specification of Security Roles

Class Name	Component Identification	Component Name
Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of Secret Key Parameters
TOE Access	FTA_TAB.1	TOE Access Banner
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
Trusted Path /Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class ESM: Enterprise Security Management

6.3.1.1 ESM_EAU.2 Reliance on Enterprise Authentication

ESM_EAU.2.1 The TSF shall rely on [[**IdentityIQ internal mechanism**], [**Active Directory**]] for subject authentication.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.3.1.2 ESM_EID.2 Reliance on Enterprise Identification

ESM_EID.2.1 The TSF shall rely on [[**IdentityIQ internal mechanism**], [**Active Directory**]] for subject identification**.**

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.3.1.3 ESM_ICD.1 Identity and Credential Definition

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [**account attributes and group attributes**].

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [**upper case letters, lower case letters, numbers, and special characters**] that include the following values [**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z 1 2 3 4 5 6 7 8 9 0 ! @ # $ % ^ & * ( )**]; and
2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and
3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2-20.

6.3.1.4 ESM_ICT.1 Identity and Credential Transmission

ESM_ICT.1.1 The TSF shall transmit [identity and credential data] to compatible and authorized Enterprise Security Management products under the following circumstances: [immediately following creation or modification of data].

6.3.2 Class FAU: Security Audit

6.3.2.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; and

b) All auditable events identified in Table *6-2* for the not specified level of audit; and

c) [**no other auditable events**].

Component	Event	Additional Information
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)

Component	Event	Additional Information
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	None
FIA_SOS.1	Identification of any changes to the defined quality metrics	The change made to the quality metric
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

Table 6-2: Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no other audit relevant information**].

6.3.2.2 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [**the Oracle database**].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.3.3 Class FIA: Identification and Authentication

6.3.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [**1-99**]] unsuccessful authentication attempts occur related to [**authentication to the GUI**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [**lock the account until an administrator configurable positive integer within 1-60 minutes has been reached, or until an administrator manually unlocks the account**].

6.3.3.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following:

a) For environmental password-based authentication, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [**upper case letters, lower case letters, numbers, and special characters**] that include the following values [**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z 1 2 3 4 5 6 7 8 9 0 ! @ # $ % ^ & * ( )**]; and

2. Minimum password length shall settable by an administrator, and support passwords of 16 characters or greater; and

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall have a maximum lifetime, configurable by an administrator; and

5. New passwords shall contain a minimum of an administrator-specified number of character changes from the previous password; and

6. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based authentication, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

6.3.3.3 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**username, principal, capabilities, rights, dynamic scopes**].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**association of a user's session and security attributes assigned to the user**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**the user's session will persist until logout and security attribute changes will be reflected upon the user's next authentication**].

6.3.4 Class FMT: Security Management

6.3.4.1 FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1 The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions: [**specified in Table 6-3**] to [**the authorized roles for each function specified in Table 6-3**].

Requirement	Management Functions	Capabilities (Roles)
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	System Admin, Identity Admin, Password Admin
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	System Admin, Identity Admin, Password Admin
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	System Admin, Password Admin, Identity Admin
ESM_ICD.1	Management of credential status	System Admin, Identity Admin
ESM_ICD.1	Enrollment of users into repository	System Admin
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	System Admin, Application Admin
FAU_STG_EXT.1	Configuration of external audit storage location	System Admin
FIA_AFL.1 (optional)	Management of the threshold for unsuccessful authentication attempts Management of actions to be taken in the event of an authentication failure	System Admin, Help Desk Personnel
FIA_SOS.1 (optional)	Management of the metric used to verify secrets	System Admin, Certification Admin
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	System Admin, Identity Admin
FMT_MOF.1	Management of sets of users that can interact with security functions	System Admin
FMT_SMR.1	Management of the users that belong to a particular role	System Admin, Role Admin, IT Role Admin, Business Role Admin, Entitlement Role Admin
FTA_SSL.3 (optional)	Configuration of the inactivity period for session termination	System Admin
FTA_TAB.1	Maintenance of the banner	System Admin
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	System Admin
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	System Admin

Table 6-3: Management Functions by Role

6.3.4.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete] the [**Objects defined in Table 6-4]** to **[the role defined in Table 6-4**].

Function	Object	Role
Query	Username (own)	All users (all roles)
Query	Username (other users)	SysAdmin, Auditor, Compliance Officer, Identity Admin, Password Admin, Policy Admin
Modify	Password, Security Questions and Answers (own)	All users (all roles)
Modify	Password, Security Questions and Answers (other users)	SysAdmin
Modify	Username	SysAdmin
Delete	Username, Password, Security Questions and Answers	SysAdmin

Table 6-4: Management of TSF Data

6.3.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 The TSF shall be capable of performing the following management functions: [**management functions listed in Table 6-3**].

6.3.4.4 FMT_SMR.1 Security Management Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Application Admin, Auditor, Batch Request Admin, Business Role Admin, Certification Admin, Compliance Officer, Rule Admin, Managed Attribute Provisioning Admin, Managed Attribute Property Admin, Entitlement Role Admin, Identity Request Admin, Identity Admin, IT Role Admin, Organizational Role Admin, Password Admin, Policy Admin, Role Admin, Signoff Admin, Identity Correlation Admin, System Admin (SYSADMIN), Task Results Viewer, Webservices Executer, Workgroup Admin, Help Desk Personnel, Work Item Admin, Access Manager, Syslog Admin**].

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

6.3.5 Class FPT: Protection of the TSF

6.3.5.1 FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

6.3.5.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.6 Class FTA: TOE Access

6.3.6.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after an Authorized Administrator-configurable time interval of session inactivity**.**

6.3.6.2 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.3.6.3 FTA_TAB.1 TOE Access Banner

FTA_TAB.1.1 Before establishing a user session, the TSF shall display a configurable advisory warning message regarding unauthorized use of the TOE.

6.3.7 Class FTP: Trusted Path/Channels

6.3.7.1 FTP_ITC.1[1] Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be capable of using [TLS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **[**audit server, authentication server] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [[**enterprise user data, IdentityIQ administrator data**]].

6.3.7.2 FTP_TRP.1[2] Trusted Path

FTP_TRP.1.1 The TSF shall be capable of using [HTTPS] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and [no other types of integrity or confidentiality violations].

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

[1] TD0576
[2] TD0576

FTP_TRP.1.3	The TSF shall require the use of the trusted path for initial user authentication and execution of management functions.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the PP against which exact compliance is claimed and 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, with the exception of a corrected wording in FTP_ITC.1.3 to reflect the intent of the SFR.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are consistent with the SARs that are defined in the claimed Protection Profile.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 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.

7.1.1.2 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.

7.1.1.3 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.

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 Developer action elements:

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 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.

7.2.1.3 Evaluator action elements:

AGD_OPE.1.1E

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

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 Developer action elements:

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 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.

7.2.2.3 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.

7.3 Class ALC: Life Cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 Developer action elements:

ALC_CMC.1.1D

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

7.3.1.2 Content and presentation elements:

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 Evaluator action elements:

ALC_CMC.1.1E

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

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 Developer action elements:

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 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.

7.3.2.3 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 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 Developer action elements:

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 Content and presentation elements:

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 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.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 Developer action elements:

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 Content and presentation elements:

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 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

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR.

8.1 Enterprise Security Management

8.1.1 ESM_EAU.2

Before allowing any other TSF-mediated action, enterprise user authentication must be performed against either the IdentityIQ's authentication mechanism or one or more environmental Active Directory servers' authentication mechanism. Both authentication mechanisms rely on username and password-based credentials for subject authentication. In the evaluated configuration, the TOE uses an Oracle 19c database that resides in the Operational Environment for its user store. When authenticating a user against the TOE's user store, the TOE will request the JRE to encrypt the user's password using AES-128 with Base64 encoding and will compare the user's username and encrypted password against the values stored in the Oracle database. The Active Directory authentication is performed via an LDAP bind request which is secured using TLS over an environmental connection via JRE's JNDI.

Every authentication source (AD server 1, AD server 2, etc., and IdentityIQ) is checked for the user's identity during authentication. All sources will be checked until the user is successfully authenticated or it is determined that the user does not exist or has failed authentication. The authentication sources are checked based upon an administratively defined order, with the IdentityIQ authentication mechanism being checked last. When a match of the user's identity credential is found, the authentication source will attempt to authenticate the user.

When a user has forgotten their password, the user can answer a series of security questions. If the user answers the questions correctly, the TSF will authenticate the user and the user may then reset their password. The answers to user security questions are also stored in the Oracle database in the AES-128 with Base64 encoding encrypted format and the TOE would similarly request the JRE to encrypt the user provided answers when comparing them to the values stored in the database.

In the event that there are multiple authentication sources with the same username, IdentityIQ will identify these occurrences and allow the administrators to perform administrative actions to correct these conflicts.

8.1.2 ESM_EID.2

See ESM_EAU.2 above.

8.1.3 ESM_ICD.1

The TOE has the ability to communicate with Active Directory to define identity and credential data for enterprise users. This communication is accomplished through the use of connectors. In the evaluated configuration, IdentityIQ will communicate with one or more instances of Active Directory utilizing the ADSI connector. The TOE will also communicate with the Oracle 19c database using JDBC. The TSF allows the management (query, change, or delete) of an enterprise user's credentials (non-IdentityIQ specific credentials) through Active Directory.

IdentityIQ connects to Active Directory servers to perform compliance checks (also known as "certifications") by reading the enforced policies and enterprise user data that is stored within Active Directory and then writes that information into its Oracle Database. The data that is collected is considered either account attributes or group attributes (a full list of attributes can be found under Schema Attributes in the SailPoint IdentityIQ Active Directory Connector version 8.3 [14]). Account attributes contain items such as display name, phone numbers and titles. Also included within the account attributes are the user's credential lifetime (i.e. password expiration) and credential status (i.e. user account is enabled, disabled, locked). While Group Attributes contain information such as group type and group scope. The TOE has the ability to read in any attribute located on Active Directory and the list of attributes collected is based upon administrative configuration.

When configured by an administrator to do so, the TOE can utilize any attributes collected by endpoint applications to manage an enterprise user's identity throughout the Operational Environment.

The TOE enrolls users in one of two ways. The TSF will perform compliance checks by reading the existing enterprise user data that is stored within the Active Directory servers and then writing that information into its Oracle database, thus enrolling the user. A user can also be created and enrolled through IdentityIQ's GUI interface by an administrator. All enterprise users are assigned the unique attribute called a 'principal' which identifies the user within IdentityIQ.

The security relevant attributes assigned to an enterprise user depend on the policies in which the administrator has defined within the TOE. The TOE defines these attributes as entitlements. The TOE is able to read any attribute configured in Active Directory. Likewise, administrators with the proper capabilities have the ability to create new attributes for enterprise users and provision them to one or more Active Directory instances.

An administrator has the ability to query the status of an enterprise user through IdentityIQ's GUI. This can be done by verifying the latest information (per last certification) stored in the Oracle Database or by requesting the Active Directory instances to provide the status. An administrator also has the ability to disable an enterprise user through IdentityIQ's GUI. IdentityIQ will immediately provision the Active Directory instances to revoke the user as well.

IdentityIQ uses the Lifecycle Manager to manage environmental user's passwords that are stored in the Active Directory servers that it manages. This is accomplished over the Active Directory ADSI connector (via interface E4) when the PASSWORD feature is enabled. A separate password policy can be defined for each instance of Active Directory. The "identity filter" can also be used to define multiple policies within a single instance of Active Directory by applying the policy only to the identities within the filter. IdentityIQ enforces these password policies only if the user changes their password via IdentityIQ directly. The TOE will not enforce the password policy if the password is changed in the environment.

Password-based credentials can be configured to include upper case and lower-case letters, numbers and special characters. In the evaluated configuration, the minimum password length supported is 16 characters and can be configured to be greater than 16 characters. If a user has an existing password that does not meet the password policy, the TOE will enforce the password policy at the time of the next password change. The TSF is capable of enforcing composition rules for the configuration of strong passwords. For example, "Minimum number of lowercase letters" or "Minimum number of special

characters" can be configured by an administrator. Administrators can also configure the password history length. The password history length is the number of past passwords that cannot be reused.

Non-password-based credentials do not apply to the TOE.

8.1.4 ESM_ICT.1

IdentityIQ provisions the enterprise user identity and credential data to one or more instances of Active Directory based upon the configuration of the administrator. Provisioning occurs immediately following the creation or modification of the data by an administrator through IdentityIQ. Provisioning occurs through the use of a provisioning form that allows an administrator to define the AD user's credentials and account attributes. Once the administrator completes the form, provisioning of the data automatically occurs. If an Active Directory instance is not responsive or unavailable when a change is supposed to occur, the Administrator will see an error when attempting to provision data. The TOE will perform a configurable number of retries at a configurable rate until the AD becomes available, or the Administrator will have to repeat the process to update or create the user data in the identity store.

8.2 Security Audit

8.2.1 FAU_GEN.1:

The TSF generates audit records when auditable events occur. The auditable events that are logged are described in Table 6-2. These audit records are written to the Oracle 19c database that resides in the Operational Environment. Auditing needs to be configured for each of the types of events listed in the table. The actions that trigger the events can be performed by a user with the SYSADMIN capability, thus, a SYSADMIN user has the ability to start and stop the audit functions for particular events.

For each auditable event, the date, time, type, subject identity, and outcome of the event is logged.

8.2.2 FAU_STG_EXT.1:

The TOE generates audit data for events and writes them to the Oracle 19c database. IdentityIQ does not store any audit data locally. If the connection to the Oracle database is severed, no management functions can be performed or audited during the outage. Once the connection is re-established management functionality and auditing resumes automatically. No user has the ability to delete or modify the audit data that resides in the Operational Environment via the TOE. The TOE does not provide any interface or mechanism to complete such actions. The transmission of data is protected using TLS via the JRE's JDBC that is provided by the Operational Environment.

8.3 Identification and Authentication

8.3.1 FIA_AFL.1:

The TOE provides the ability to discourage brute force authentication attempts by providing authentication failure handling for the GUI. Administrators can configure the number of unsuccessful attempts to any selection within 1-99. The default setting is five.

Once the administrator defined value has been met the user will be locked out until an administrator manually unlocks the account or until an administrator configurable positive integer within 1-60 minutes has been reached.

IdentityIQ also has the ability to identify and grant users the 'protected users' privilege and these users cannot be locked out. In the out-of-the-box configuration, the SYSADMIN capability is granted this privilege. In the evaluated configuration, the SYSADMIN capability will have this privilege removed and no other user/capability will be granted it. This is done by configuring the field 'Enable Protected User Lockout'.

8.3.2 FIA_SOS.1:

Password-based credentials can be configured to include upper and lower-case letters, numbers and special characters. To prevent users from using similar password consecutively, password changes are also required to have a minimum number of character changes from the previous password. This is configurable within the password policy by configuring the “Minimum number of characters by position” and the “Case sensitive check” settings. In the evaluated configuration, the minimum password length supported is 16 characters and can be configured to be a maximum of 300 characters. IdentityIQ administrators with the proper capabilities are also capable of enforcing users to configure passwords to meet composition rules. For example, “Minimum lowercase letters” or “Minimum special characters” can be administratively configured.

The password history length can also be administratively configured. The password history specifies the number of previous passwords in password history to check against for uniqueness to prevent the re-use of the same passwords.

Password lifetime can be configured for manually set passwords and generated passwords. This option allows the administrator to set a specific number of days before the password is expired. Once this limit has been reached, the user is required to change the password the next time they log on to IdentityIQ.

Non-password-based credentials do not apply to the TOE.

8.3.3 FIA_USB.1:

After a user authenticates to the TOE, the TOE creates a user session in memory that contains the authenticated username, the user’s principal, and the capabilities, rights, and dynamic scopes that have been associated with that user’s principal. The "username" is the credential identified by the authentication source (IdentityIQ or Active Directory in the evaluated configuration). The "principal" is the credential utilized by IdentityIQ to authorize user activity. The "username" and "principal" will be the same if the user is authenticated by IdentityIQ but may differ depending on deployment of a third-party authentication source.

This user session is also associated with J2EE session identifier maintained by Apache Tomcat which hosts IdentityIQ's GUI. The principal is the unique identifier that IdentityIQ uses for a user throughout the enterprise. An authenticated username within the user store (Active Directory or IdentityIQ) will be assigned to the user’s principal. The principal is then used to query the Oracle database for the capabilities, rights and dynamic scope for that user. The dynamic scope defines the GUI webpages to which the user has access. Capabilities and rights are discussed in more depth in section 8.4.1.

User actions are authorized against the user session stored in IdentityIQ's memory. A user's session will not be updated to include any changes to their security attributes while they are authenticated to IdentityIQ. Instead, changes made to a user's security attributes will be reflected upon the user's next authentication attempt.

8.4 Security Management

8.4.1 FMT_MOF.1:

The ability for a user to perform a function on an object through IdentityIQ is dependent on the capabilities, rights, and scope associated with the user. Roles in the context of IdentityIQ are the combination of "capabilities" and "rights". The "capabilities" control the components within the product to which a user has access. The "rights" are actions that the user can perform on the target attribute and are assigned to capabilities. Examples of rights include create, read, update, delete, execute. The "scope" defines the objects to which a user has access. IdentityIQ will query the Oracle database for data based on user actions and will only provide the user access to data objects within their assigned scope. Scope is referred to in two ways, Assigned scope and Controlled scope. Assigned scope is the scope assigned to an identity or object manually, automatically, or through aggregation and correlation. Controlled scopes refer to the scopes to which an identity has access. A user can only see objects that are within their controlled scopes, that were created, or that have no scope assigned. Controlled scope is hierarchical. If a user controls a parent scope they control any child scopes contained within.

The System Admin has full access to objects and every right within IdentityIQ. This is the only default capability that has this access. Refer to Table 6-3 for the modification of TOE data by the defined capabilities within the context of this ST.

8.4.2 FMT_MTD.1:

Table 6-4 describes the ability to query, modify and delete usernames, passwords and Security Questions/Answers. Any authenticated user has the ability to query their own username as well as modify their own password and Security Questions/Answers. SysAdmin, Auditor, Compliance Officer, Identity Admin, Password Admin, and Policy Admin have the ability to query usernames of other user accounts. Only the SysAdmin has the ability to modify, and delete usernames, passwords, and Security Questions/Answers for the full set of user accounts. Oracle Database 19c is the repository that the TOE utilizes for authentication data. Secure communications to and from the repository are secured with TLS using JDBC which is provided by the JRE and is part of the Operational Environment.

8.4.3 FMT_SMF.1:

For each of the security functions that are defined as part of the TSF, the TOE provides administrators with the capability to manage the function. Additionally, provisioning occurs automatically once the initial configuration of the TOE has been completed. For instance, the transmission/provisioning of user data to the environment occurs immediately following the creation or modification of the data by an Administrator. The transmission of data is sent through a secure channel protected by TLS. Table 6-3 lists all of the management functions for each requirement.

8.4.4 FMT_SMR.1:

Roles in the context of IdentityIQ are the combination of "capabilities" and "rights". The TOE allows the administrators, as defined in Table 6-3 under FMT_SMR.1, to assign users to capabilities. IdentityIQ has 27 evaluated out-of-the-box capabilities (capabilities, in this instance are synonymous with the protection profile's definition of roles.). These capabilities already have rights assigned to them. Admins with the proper capability can modify any out-of-the-box capability by adding or removing the rights assigned thus creating a custom capability. Administrators also have the ability to delete capabilities. The System Admin is a unique capability as it has all of the rights that are available already assigned. Refer to AGD documentation, specifically, SailPoint_IdentityIQ_Capabilities.xls [18] for a complete list of out-of-the-box capabilities and the rights that are assigned to them.

8.5 Protection of the TSF

8.5.1 FPT_APW_EXT.1:

Users of the TOE are required to authenticate to IdentityIQ with a username and password. IdentityIQ does not store the password credential locally nor does the TOE provide any mechanism for users to read plaintext passwords. IdentityIQ's user store is an environmental Oracle 19c database. The TOE requests the JRE to encrypt the user's password using AES-128 with Base64 encoding to protect IdentityIQ passwords before being stored in the Oracle database.

8.5.2 FPT_SKP_EXT.1:

In the evaluated configuration, IdentityIQ does not store or have access to any pre-shared keys, symmetric keys, or private keys. IdentityIQ does have a symmetric key which is hardcoded into the TOE's software, which can be provided to the JRE for encrypting and decrypting IdentityIQ managed user passwords and answers to user security questions. However, in the evaluated configuration, the TOE's installer will import a unique symmetric key into the JRE's keystore for this purpose. The Operational Environment JRE would then use this unique symmetric key to encrypt and decrypt this user data using AES-128 with Base64 encoding before storing it in the Oracle database. IdentityIQ does not provide any interface to read the hardcoded key nor any key stored in the JRE keystore.

8.6 TOE Access

8.6.1 FTA_SSL.3:

IdentityIQ has the ability to terminate a user's remote administrative GUI session if the session is inactive for a specific period of time as configured by the System Admin that installs the TOE. The default timeout setting is 30 minutes. For the System Admin to configure inactivity timeout value, they would need to modify the web.xml file. The value can be set between 1 and 60 minutes.

8.6.2 FTA_SSL.4:

Any user can terminate his or her remote session using the logout button displayed within the GUI session.

8.6.3 FTA_TAB.1:

The TOE displays a warning message on the GUI's login page prior to allowing any user authentication to the TOE. This requires the System Admin that installs the TOE to modify the login page (login.xhtml) to include the warning message.

8.7 Trusted Path/Channels

8.7.1 FTP_ITC.1:

IdentityIQ connects to Active Directory in order to perform authentication of enterprise users and administrative users to IdentityIQ. This connection occurs over a TLS protected channel between the environmental JRE's JNDI and the environmental Active Directory server.

IdentityIQ also connects to Active Directory servers to perform compliance checks (also known as "certifications") by reading the enforced policies and enterprise user data that is stored within Active Directory as well as to perform provisioning by writing updates to this data on the Active Directory. This connection occurs over a TLS protected channel between the Microsoft .NET Framework's ADSI connector and the Active Directory server in the Operational Environment.

IdentityIQ connects to the Oracle Database to store policy data, enterprise user data and IdentityIQ administrator data. This connection occurs over a TLS protected channel between the environmental JRE's JDBC and the environmental Oracle database.

In all cases, the encryption is provided by the Operational Environment using the following FIPS 140-2 certified cryptographic modules:

- RSA BSAFE Crypto-J JSAFE and JCE) are used for the JNDI and JDBC connections (Database version: Oracle 19c, Java Platform: Oracle JDK 11).
- Microsoft Windows Cryptographic Primitives Library (CNG.SYS) is used for the ADSI connection (Windows Server 2016 Active Directory)

IdentityIQ initiates all communication via the trusted channel. The environmental JREs JNDI and the environmental Active Directory server channel is initiated on a per authentication request. The environmental Microsoft .NET Framework's ADSI and the environmental Active Directory server channel is initiated on a compliance or provisioning event basis which can occur immediately after administrative action. The environmental JRE's JDBC and the environmental Oracle Database channel is initiated as part of IdentityIQ's start-up process and is a continuous connection since IdentityIQ cannot operate without the TOE data stored in the Oracle database. If the connection is severed, IdentityIQ will re-establish the connection.

8.7.2 FTP_TRP.1:

IdentityIQ provides a GUI for remote administration. The GUI communication is protected by HTTPS through an environmental Apache Tomcat 9.0 with the OpenSSL FIPS Object Module.

Users initiate access to the GUI by directing their web browser to https://hostserver:8443/identityiq using Chrome, version 110 (or later). This trusted path is used for all remote administration.