National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
SailPoint IdentityIQ v8.3p5

Report Number:	**CCEVS-VR-VID11520-2025**
Dated:	**February 12, 2025**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin, Senior Validator
Marybeth Panock, Lead Validator
Seada Mohammed, Lead Validator (Trainee)
The Aerospace Corporation

Common Criteria Testing Laboratory

Herbert Markle
Rachel Kovach

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of IdentityIQ v8.3p5, provided by SailPoint Technologies, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in February 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the Enterprise Security Management Identity and Credential Management Protection Profile (ICMPP).

The Target of Evaluation (TOE) is the SailPoint IdentityIQ v8.3p5. IdentityIQ is a governance-based Identity and Access Management (IAM) software solution. It integrates compliance management and provisioning in a unified solution that leverages a common identity governance framework.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the ICMPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the ICMPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the SailPoint IdentityIQ v8.3p5 Security Target, Version 1.0, January 8, 2025, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities that are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance results of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	SailPoint IdentityIQ version 8.3p5
Protection Profile	Standard Protection Profile for Enterprise Security Management Identity and Credential Management v2.1
Security Target	SailPoint IdentityIQ v8.3p5 Common Criteria Security Target, Version 1.0, January 8, 2025
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "SailPoint IdentityIQ v8.3p5" Evaluation Technical Report v1.0 January 18, 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended; CC Part 3 conformant
Sponsor	SailPoint Technologies, Inc.
Developer	Booz Allen Hamilton, Laurel, Maryland
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Daniel Faigin, The Aerospace Corporation Marybeth Panock, The Aerospace Corporation Seada Mohammed, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

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

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- 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.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- 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.
- 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.

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Standard Protection Profile for Enterprise Security Management Identity and Credential Management v2.1, 24 October 2013 to which this evaluation claimed exact compliance.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM

defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.

- The evaluation of security functionality of the product was specifically limited to the functionality specified in the claimed PP (PP_ESM_ICM_V2.1). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target; Section 6, Security Functional Requirements, and their operation with respect to the TOE is described in Section 8, TOE Summary Specification. Any other functionality provided by SailPoint IdentityIQ needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- Multifactor authentication (MFA) and Single Sign On (SSO) were not covered by the evaluation.
- Note that the functionalities listed in Section 7.1 of this document are not covered by this evaluation.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

IdentityIQ (also referred to as the TOE) is a governance-based Identity and Access Management (IAM) software solution. It integrates compliance management and provisioning in a unified solution that leverages a common identity governance framework. IdentityIQ provides a variety of IAM processes that include automated access certifications, policy management, access request and provisioning, password management and identity intelligence.

4.2 Physical Boundaries

The physical boundary of the TOE includes the IdentityIQ software that is installed on top of the Apache Tomcat application server. The evaluated configuration of the TOE includes licenses for the Lifecycle Manager portion of IdentityIQ. 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 that 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	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 18c 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 2022 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 118 or later.

Table 4-1: IT Environment Components

5 Security Policy

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.

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.

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.

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 46 out-of-the-box capabilities. The TOE also allows administrators to create or modify capabilities and assign them to users or groups of users.

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.

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.

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.

6 Documentation

The vendor provides a standard set of guidance documents that covers the core functionality of the product. These documents were used during the evaluation of the TOE:

- SailPoint IdentityIQ v8.3p5 Supplemental Administrative Guidance (AGD)
- SailPoint IdentityIQ System Configuration version 8.3
- SailPoint IdentityIQ Lifecycle Manager version 8.3
- SailPoint IdentityIQ Active Directory Connector version 8.3
- SailPoint IdentityIQ Installation Guide version 8.3
- SailPoint IdentityIQ Tasks version 8.3
- SailPoint IdentityIQ Password Management version 8.3
- SailPoint IdentityIQ Application Configuration version 8.3
- SailPoint_IdentityIQ_Capabilities.xls

These guidance documents contain the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance documents are applicable for version of IdentityIQ claimed by this evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the SailPoint IdentityIQ v8.3p5 software installed upon a general-purpose server platform, that is configured in accordance with the Common Criteria Addendum described in Section 6. The TOE includes all the code that enforces the policies identified (see Section 5).

Section 2.4 of the ST describes the TOE's physical boundary as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Authentication Store provide enterprise authentication and user data.
- Application Server for hosting the TOE software.
- Database for storage of configuration, operation, and audit data for the TOE.
- Underlying Server on which the IdentityIQ software is installed.
- Web Browser used for remote administration of the TOE.

To use the product in the evaluated configuration, the product must be configured as specified in the *SailPoint IdentityIQ v8.3p5 Supplemental Administrative Guidance v1.0* document. Refer to Section 6 for the full list of documents needed for instructions on how to place the TOE in its evaluated configuration.

7.1 Excluded from the TOE

There are optional products, components, and/or applications that 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.

7.1.1 Not Installed

There are several components, or optional products, that can be used with the TOE but are not included in the evaluated configuration and are 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.

7.1.2 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.

7.1.3 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: AIServices Admin, Alert Admin, Access Manager, Assign or Detect Role Admin – DEMODATA, Batch Request Admin, CAM Admin, Certification Admin, Container Role Admin – DEMODATA, FAM Admin, Form Admin, Full Access Admin Console, Identity Correlation Admin, Identity Request Admin, Managed Attribute Provisioning Admin, Managed Attribute Property Admin, Organizational Role Admin, PAM Admin, PAM Viewer, Plugin Admin, Rapid Setup

Admin, Rapid Setup Birthright Role Admin, Rapid Setup Configuration Admin, Rapid Setup Configuration Viewer, Rapid Setup Identity Operations Admin, Rapid Setup Viewer, Rule Admin, SCIM Executor, Signoff Admin, Syslog Admin, Task Results Viewer, View Admin Console, Work Item Admin, Workgroup 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.

Additional Authentication Mechanisms — Multifactor authentication (MFA) and Single Sign On (SSO) were not covered by the evaluation.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Evaluation Technical Report for a Target of Evaluation SailPoint IdentityIQ v8.3p5 Evaluation Technical Report v1.0* dated January 18, 2025, which is not publically available.

8.1 Test Configuration

The evaluation team installed and configured the TOE according to the SailPoint IdentityIQ v 8.3p5 Supplemental Administrative Guidance v1.0 document for testing.

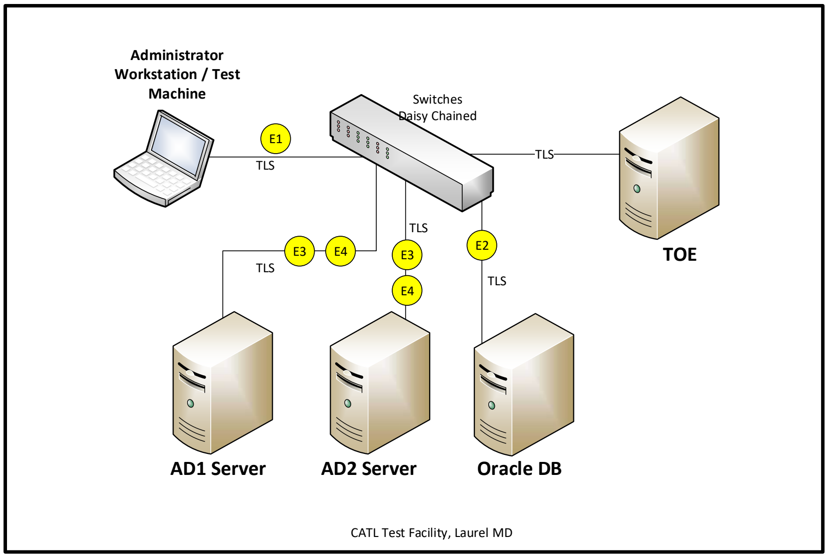

Figure 1: SailPoint IdentityIQ Testbed Network Diagram

El: All management activities are completed through the web browser that connects to the Administrative GUI. This channel is secured using HTTPS that is provided by the environmental Apache Tomcat.
E2: 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. This connection is secured using a TLS protected channel between the environmental JRE’s JDBC and the Oracle database.
E3: 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.
E4: 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 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 TOE was installed on a Windows 2022 Server 10.0.20348 Build 20348 running Apache Tomcat v9.0 and JDK 17 as its Java Runtime Environment. All devices were connected on the same LAN using daisy chained Cisco switches.

The TOE was configured to communicate with the following environment components:

Function Performed	IP Address / Subnet Mask	MAC Address	Timing Source	Version of OS software / firmware	Version of Tools
Active Directory instance 01 (E3, E4)	Ethernet0: 192.168.2.210	Ethernet0: 00-50-56-88-4C-1A	Hardware backed clock Primary domain controller	Microsoft Windows Server 2019 / Version 1809 (OS Build 17763.1490)	Nmap v7.9.5
Active Directory instance 02 (E3, E4)	Ethernet0: 192.168.2.211	Ethernet0: 00-50-56-88-3B-F1	Hardware backed clock Primary domain controller	Microsoft Windows Server 2019 / Version 1809 (OS Build 17763.1217)	Wireshark v4.2.2
Database (E2)	Ethernet0: 192.168.2.212	Ethernet0: 00:50:56:88:0B:C2	NTP: SP-IDIQ-AD1.spcc.local	Microsoft Windows Server 2019 / Version 1809 (OS Build 17763.1217) Oracle (19C) 19.3.0.0.0	Wireshark v4.2.2
Management Workstation (E1)	Ethernet0: 192.168.2.99	Ethernet0: 00-50-56-88-EA-10	Manually Set and verified	Microsoft Windows 10 Enterprise / 10.0.19045 N/A Build 19045	Wireshark v4.2.2 Google Chrome v122.0.6261.129 Zenmap v7.95 OWASP Zap v2.16.0

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the (ESM ICM PP). The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. A description of the test configurations and the test tools may be found in Section 4 of that report.

The test team's approach was to test the security mechanisms of the SailPoint IdentityIQ software by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in the relevant design documentation (e.g., ST and AGD) in terms of the claims on the TOE that can be tested through the external interface. The “SailPoint IdentityIQ v8.3p5 Security Target v1.0” (ST), “SailPoint IdentityIQ v8.3p5 Supplemental Administrative Guidance v1.0” (AGD), the “SailPoint IdentityIQ ATE Test Matrix Results” (Test Matrix), and “SailPoint IdentityIQ v8.3p5 Test Procedures” (Test Plan) were used to demonstrate test coverage of all SFR testing assurance activities as defined by the ICMPP for all security relevant TOE external interfaces. TOE external interfaces that will be determined to be security relevant are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements will be determined to be appropriate to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
SailPoint	This is a generic term for searching for known SailPoint IdentityIQ vulnerabilities.
IdentityIQ	This is a generic term for searching for known SailPoint IdentityIQ vulnerabilities.
Identity Credential Management	This is a generic term for searching for known SailPoint IdentityIQ vulnerabilities.
ICM	This is a generic term for searching for known SailPoint IdentityIQ vulnerabilities.
Libraries	Advanced searches were used when available in order to correctly identify the owner of the library. This list is considered Vendor proprietary is not reproduced here.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources was updated on February 7, 2025. The following public vulnerability sources were searched:

- NIST National Vulnerabilities Database: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ or https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

All search activities were conducted prior to the execution of the vulnerability testing activities.

The team tested the following areas:

In this test, the evaluators inspected network traffic captures to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Web Interface Vulnerability Identification
  OWASP ZAP is a web application vulnerability assessment tool suite. ZAP looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure.

- Malicious Code Scanning
  Malicious code scanning was conducted to ensure the TOE software had no malicious code introduced by the Vendor. Malicious code scanning actively searches for and identifies harmful code within computer systems, applications, or files, which can prevent data breaches, system disruptions, and other security threats by allowing for the removal or mitigation of malicious code before it can cause damage. The TOE software was scanned using Microsoft Windows Defender and MalwareBytes.

The TOE successfully prevented any attempts of subverting its security.

The results from the penetration testing showed that there were no vulnerabilities that could be leveraged by a malicious user when installed according to the SailPoint IdentityIQ v8.3p5 Supplemental Administrative Guidance for Common Criteria Version 1.0 [AGD]. There are currently no known discovered issues that could affect the security posture of a deployed system.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Evaluation Activities specified in the ICMPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the ICMPP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit specified in the ICMPP. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit specified in the ICMPP. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the ICMPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit specified in the ICMPP, as well as the Assurance Activities specified for ALC_CMC.1 and ALC_CMS.1. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit specified in the ICMPP. The evaluation team ran the set of tests specified by the Assurance Activities in the ICMPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the ICMPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit specified in the ICMPP. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The evaluation team performed/updated a public search for vulnerabilities on February 7, 2025, available information at nvd.nist.gov and www.cvedetails.com. The following search terms were used:

- SailPoint
- IdentityIQ
- Identity and Credential Management
- ICM
- Libraries

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the ICMPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the ICMPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

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 identity and password management security functionality as defined by the claimed Security Functional Requirements (SFRs) in the ST. Other functionalities included in the product, including Multifactor authentication (MFA) and Single Sign On (SSO), were not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *SailPoint IdentityIQ v8.3p5 Supplemental Administrative Guidance v1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is "SailPoint IdentityIQ v8.3p5 Security Target v1.0", *January 8, 2025*.

13 List of Acronyms

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

14 Terminology

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

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24, 2013.
6. SailPoint IdentityIQ v8.3p5 Security Target, Version 1.0, January 08, 2025.
7. Evaluation Technical Report for a Target of Evaluation SailPoint IdentityIQ v8.3p5 Version 1.0, February 08, 2025.
8. Assurance Activities Report for a Target of Evaluation SailPoint IdentityIQ v8.3p5 Version 1.0, February 08, 2025.
9. SailPoint IdentityIQ v8.3p5 Test Procedures Version 1.0 December 11, 2024.
10. SailPoint IdentityIQ v8.3p5 Vulnerability Analysis, Version 1.0 February 07, 2025.
11. SailPoint IdentityIQ v8.3p5 Supplemental Administrative Guidance v1.0, December 18, 2024
12. SailPoint IdentityIQ Administration Guide version 8.3.
13. SailPoint IdentityIQ User’s Guide version 8.3.
14. SailPoint IdentityIQ Active Directory Connectors Guide version 8.3.
15. SailPoint IdentityIQ Installation Guide version 8.3.
16. SailPoint_IdentityIQ_Capabilities.xls.