National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

SailPoint

File Access Manager 8.3 SP5

Report Number: CCEVS-VR-VID11352-2023

Dated: August 31, 2023

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
Fernando Guzman, ECR Team
Russell Fink, ECR Team
Robert Wojcik, ECR Team

The Aerospace Corporation and The Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Chris Rakaczky
Rachel Kovach
Evan Seiz

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary 1
2 Identification 3
3 Assumptions and Clarification of Scope 4
3.1 Assumptions 4
3.2 Threats 4
3.3 Clarification of Scope 4
4 Architectural Information 5
4.1 TOE Introduction 5
4.2 Physical Boundary 5
5 Security Policy 7
5.1.1 Cryptographic Support 7
5.1.2 User Data Protection 7
5.1.3 Security Management 7
5.1.4 Privacy 7
5.1.5 Protection of the TSF 7
5.1.6 Trusted Path/Channel 8
6 Documentation 9
7 TOE Evaluated Configuration 10
7.1 Evaluated Configuration 10
7.2 Excluded Functionality 11
8 IT Product Testing 12
8.1 Test Configuration 12
8.2 Developer Testing 14
8.3 Evaluation Team Independent Testing 14
8.4 Evaluation Team Vulnerability Testing 14
9 Results of the Evaluation 15
9.1 Evaluation of the Security Target (ASE) 16
9.2 Evaluation of the Development (ADV) 16
9.3 Evaluation of the Guidance Documents (AGD) 16

9.4 Evaluation of the Life Cycle Support Activities (ALC) 16
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 16
9.6 Vulnerability Assessment Activity (VAN) 17
9.7 Summary of Evaluation Results 17
10 Validator Comments 18
11 Annexes 19
12 Security Target 20
13 List of Acronyms 21
14 Terminology 22
15 Bibliography 23

List of Figures

Figure 1 TOE Boundary 11
Figure 2 Test Configuration 12

List of Tables

Table 1 – Evaluation Identifiers 3
Table 2 – Operational Environment Software Requirements 5
Table 3 – Evaluated Components of the Operational Environment 5
Table 4 – Public Vulnerability Search Keywords 14

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of SailPoint File Access Manager 8.3 SP5 provided by SailPoint. 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 August 2023. The information in this report is largely derived from the evaluation sensitive 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 *Protection Profile for Application Software Version 1.4* (APP_PP), October 7, 2021.

The Target of Evaluation (TOE) is the SailPoint Identity File Access Manager (FAM) version 8.3 SP5 ("SailPoint FAM") application executing on Microsoft Windows Server 2019 operating system (OS). The primary function of SailPoint FAM is to allow its users to review and manage the governed data created by SailPoint FAM for the monitoring of enterprise data stored on one or more managed resources. The governed data allows SailPoint FAM users to identify and classify data, understand on which managed resources within the network the data is stored, and understand which enterprise users have access to the data. SailPoint FAM's primary functionality of monitoring enterprise data was not evaluated, except where the product's functionality relates to the Security Functional Requirements (SFRs) included within the scope of the evaluation.

In the evaluated configuration, the Target of Evaluation (TOE) is the SailPoint File Access Manager (FAM) 8.3 SP5 ("SailPoint FAM") application is installed on a Windows Server 2019 and through APIs the TOE utilizes several functions of the operating system to perform its operations. The TOE relies on .NET Framework to function and Internet Information Services (IIS) to host its GUI web pages. The TOE communicates with the Windows operating system's Server Message Block component to receive information about data on managed resources which FAM turns into governed data. The TOE also communicates with the Windows operating system's Active Directory component which contains enterprise user data. The TOE stores all of its configuration data, TOE managed user credentials, and governed data within a separately installed SQL Database. During operation, the TOE will read and write this data to the SQL Database. In the evaluated configuration, the SQL Database resides on the same Windows Server as the TOE. The administrative interfaces include a local Fat Client for local access and a web GUI for remote access. The TOE is configured to securely communicate with the following external IT entity: Windows File Server(s).

The 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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the APP_PP. 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 APP_PP 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 File Access Manager 8.3 SP5 Security Target v1.0*, dated July 07, 2023, 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, which are interpretation of Common Methodology for Information Technology Security Evaluation – Evaluation Methodology (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 Compliant 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 result 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 File Access Manager 8.3 SP5
Protection Profile	Protection Profile for Application Software Version 1.4 [APP_PP], including all applicable NIAP Technical Decisions and Policy Letters
Security Target	SailPoint File Access Manager 8.3 SP5 Security Target Version 1.0 dated July 7, 2023
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "SailPoint File Access Manager 8.3 SP5" Evaluation Technical Report Version 1.0 dated August 18, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	SailPoint Technologies, Inc.
Developer	SailPoint Technologies, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Daniel Faigin, Marybeth Panock, Fernando Guzman, Russell Fink, Robert Wojcik

3 Assumptions and Clarification of Scope

3.1 Assumptions

The assumptions are drawn directly from the APP_PP.

3.2 Threats

The threats are drawn directly from the APP_PP.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. 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 *Protection Profile for Application Software Version 1.4*, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the APP_PP are claimed by the TOE and documented in the ST.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- 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 security functionality 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product, including the primary advertised functionality of the product, which allows its users to review and manage the governed data created by FAM for the monitoring of enterprise data stored on one or more managed resources, was not assessed as part of this evaluation. Only the functionality discussed in Section 5 of this report was assessed. All other functionality provided by the product needs to be assessed separately and this report makes no statement about correctness of operation for that functionality. Section 7.2 of this document, and Section 2.3 "Excluded from the TOE" of the ST, provide the details of features that are part of the purchased product but were not included in the evaluation.

4 Architectural Information

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

4.1 TOE Introduction

The TOE type for SailPoint FAM 8.3 SP5 is Application Software. The Protection Profile for Application Software [APP_PP] specifies several use cases that conformant TOEs may implement. In particular the TOE supports:

Use Case 2, Content Consumption, is defined as follows: "The application allows a user to consume content, retrieving it from either local or remote storage."

> SailPoint FAM 8.3 SP5 meets the expectations of Use Case 2 because it implements content consumption by allowing its users to review and manage governed data created by SailPoint FAM for the monitoring of enterprise data stored on one or more managed resources.

4.2 Physical Boundary

SailPoint FAM 8.3 SP5 is a software-only TOE and therefore its physical boundary is its software. The TOE does not include the hardware or operating system of the system on which it is installed. It also does not include the third-party software which is required for the TOE to run. The following table lists the 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.

Table 2 – Operational Environment Software Requirements

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

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

Table 3 – Evaluated Components of the Operational Environment

Component	Definition
Activity Monitor	A SailPoint software application which optionally can be installed on a Windows File Server (managed resource) to collect additional information to create governed data for the FAM product's primary functionality. Although this software is produced by the same vendor as the TOE, the Activity Monitor is not part of the TOE and is not required for FAM to perform its primary functionality.
Host Server	Physical system on which the FAM software is installed.
Host Platform	The Microsoft Windows Server 2019 Datacenter (version 1809) operating

	system on which the FAM software is installed. This includes the required Windows Server components: Internet Information Services (IIS), .NET Core (.NET), Active Directory, and Server Message Block (SMB).
SQL Database	Stores a variety of configuration, operation, and governed data for the FAM product. The connection to the SQL database is required in order for the TOE to function.
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE remotely via a web browser. Note that the fat client can also be used to administer the TOE locally.
Windows File Server(s)	One or more Windows Servers which the FAM product monitors as a managed resource to create governed data for its primary functionality. Each Windows Server may optionally have an Activity Monitor installed on it to collect additional data for the FAM product's primary functionality.

5 Security Policy

5.1.1 Cryptographic Support

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

5.1.2 User Data Protection

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

- respond to TLS connection requests from an Activity Monitor to receive managed resource data.

5.1.3 Security Management

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

5.1.4 Privacy

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

5.1.5 Protection of the TSF

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

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

5.1.6 Trusted Path/Channel

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

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria – v1.0, July 07, 2023
- SailPoint File Access Manager Administrator Guide Version: 8.3 Revised: March 30, 2022
- SailPoint File Access Manager Installation Guide Version: 8.3 SP5 Revised: June 30, 2023
- SailPoint IdentityIQ Version: 8.3.0.5000 File Access Manager v8.3 Service Pack 5 Deployment Guide

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is the SailPoint File Access Manager (FAM) 8.3 SP5 ("SailPoint FAM") application executing on a Windows OS. In the evaluated configuration, SailPoint FAM 8.3 SP5 is installed on a Windows Server 2019 and through APIs the TOE utilizes several functions of the operating system to perform its operations. the TOE relies on .NET Framework to function and IIS to host its GUI web pages. The TOE communicates with the Windows operating system's Server Message Block component to receive information about data on managed resources which FAM turns into governed data. The TOE also communicates with the Windows operating system's Active Directory component which contains enterprise user data. The TOE stores all of its configuration data, TOE managed user credentials, and governed data within a separately installed SQL Database. During operation, the TOE will read and write this data to the SQL Database. In the evaluated configuration, the SQL Database resides on the same Windows Server as the TOE. The administrative interfaces include a local Fat Client for local access and a web GUI for remote access. The TOE is configured to securely communicate with the following external IT entity: Windows File Server(s).

Section 4.2 describes the TOE's physical configuration 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:

- Host Server
- Host Platform (IIS, .Net Core (.NET), Active Directory, and Server Message Block (SMB)
- Management Workstation
- Windows File Server(s)

To use the product in the evaluated configuration, the product must be configured as specified in the *SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria Version 1.0, July 07, 2023*, document.

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

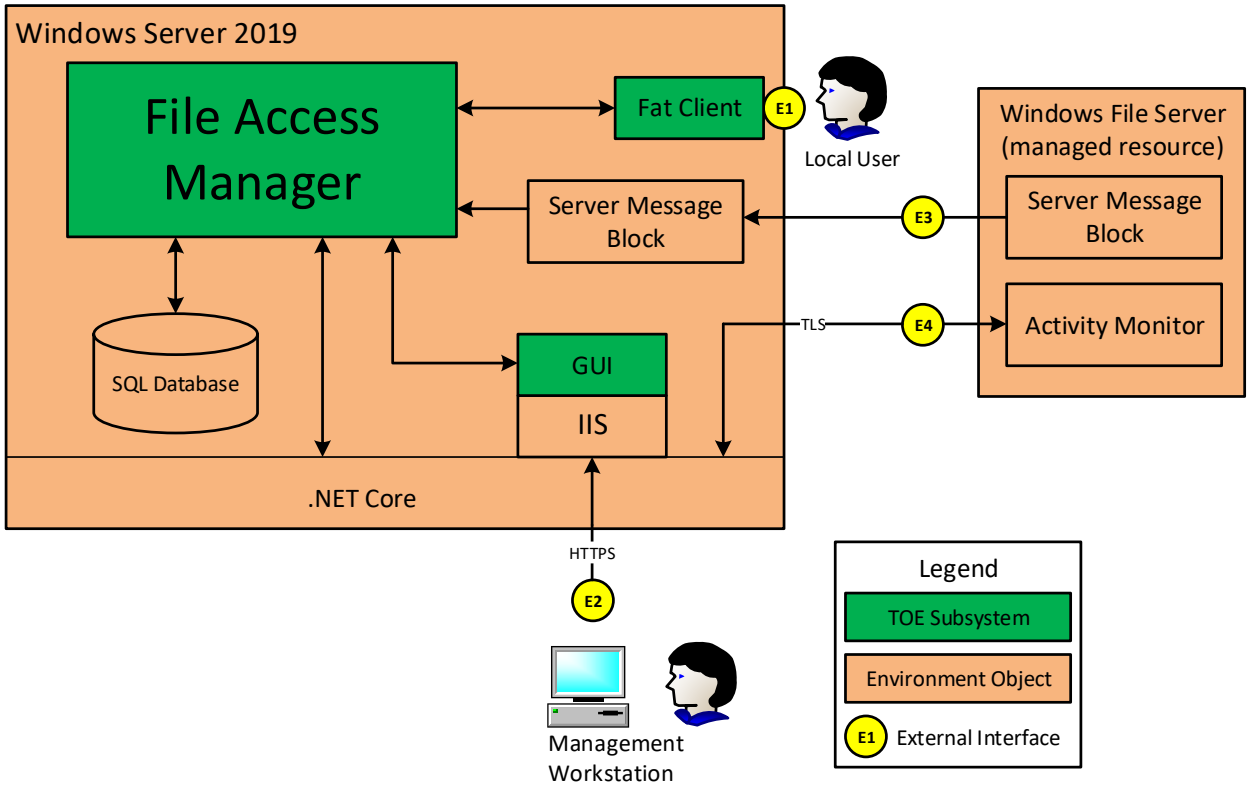

Figure 1 TOE Boundary

7.2 Excluded Functionality

The Security Target identifies the optional products, components, and/or applications that can be integrated with the TOE but are not included in the evaluated configuration. These items 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. For this product, there are no optional components that are omitted from the installation process, nor are there any excluded components, applications, and or functionality that are installed and require a separate license for activation. However, the TOE does include a number of functions that are outside the scope of the claimed Protection Profile. These functions are not part of the TSF because there are no SFRs that apply to them. This includes FAM's primary functionality which allows its users to review and manage the governed data created by FAM for the monitoring of enterprise data stored on one or more managed resources. The governed data allows FAM users to identify and classify data, understand on which managed resources within the network the data is stored, and which enterprise users have access to the data.

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 *Assurance Activity Report for a Target of Evaluation "SailPoint File Access Manager 8.3 SP5" Assurance Activities Report v1.0, August 18, 2023*.

8.1 Test Configuration

The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network.

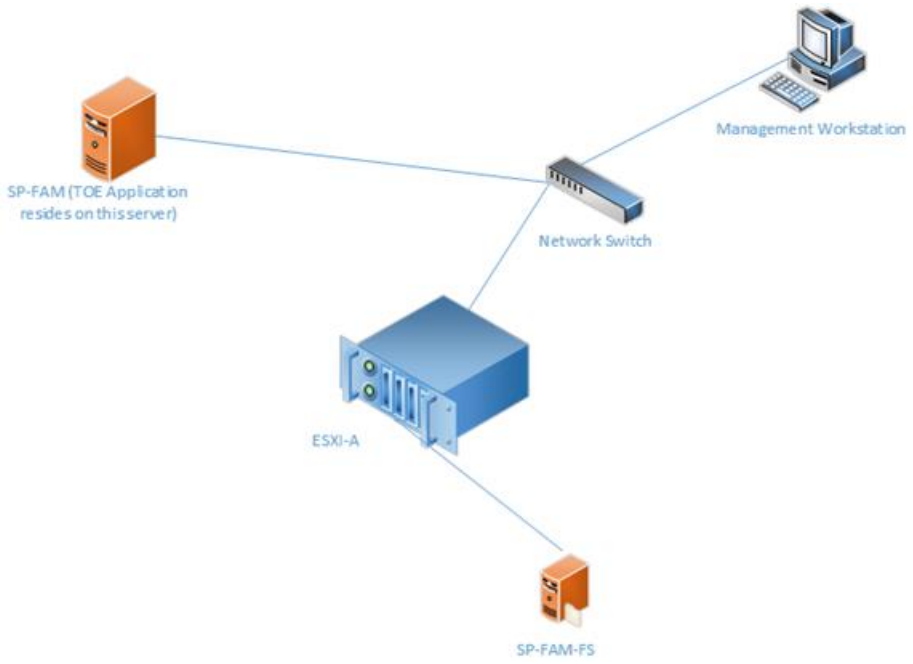

Figure 2 Test Configuration

Device Name	Function Performed	Protocols Used	Version of OS software / firmware	Version of Tools
SP-FAM	Physical server on which TOE is resident. AD Server Database	TLS	Windows Server 2019 Datacenter Version 1809	Wireshark version 3.6.8 Microsoft Network Monitor version 3.4.2350.0 VMmap 3.26

	Server			PESecurity PowerShell module to examine the Windows Binary https://github.com/NetSPI/PESecurity - version #None given Author: Eric Gruber 2014, NetSPI, Updated: Alex Verboon July 28.2017, added Control Flow Guard information.
ESXI-A	ESXi host that serves SP-FAM-FS servers	N/A	Hypervisor: VMware ESXi, 6.5.0, 7526125	N/A
SP-FAM-FS	File Server / Activity Monitor	TLS	Windows Server 2019 Version 1809	Wireshark version 3.6.8 Microsoft Network Monitor version 3.4.2350.0
2 Test Machines	Management Workstation	HTTPS		Wireshark version 3.6.8 Microsoft Network Monitor version 3.4.2350.0
Cisco Catalyst WS-C Switch, WS-C3560X-24P-L	Network Switch	N/A	Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3	N/A

8.2 Developer Testing

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

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the APP_PP 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 were 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. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the APP_PP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Table 4 – Public Vulnerability Search Keywords

Keyword	Description
SailPoint	This is a generic term for searching for known vulnerabilities for the overall company that authored the TOE product.
IdentityIQ	This is a generic term for searching for known vulnerabilities for the overall product line that authored the TOE product. The SailPoint File Access Manager is no longer referred to by this name. However, IdentityIQ remained as a key word for the search for completeness.
File Access Manager	This is a generic term for searching for known vulnerabilities for the specific product type.
Elasticsearch (5.1.1)	Third party component that comes with FAM.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated August 12, 2023). The following public vulnerability sources were searched:

a) NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search

b) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php

c) US-CERT: http://www.kb.cert.org/vuls/html/search

d) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories

e) Offensive Security Exploit Database: https://www.exploit-db.com/

f) 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. Testing that was conducted under the functional testing that would have been duplication of a vulnerability tests were not re-run. This left one remaining exploit to further explore: malicious binary.

The team tested the following areas:

- Virus Scan

  This test scans the TOE binary with a virus scanner using the most current virus definitions against the application files and then the evaluator verifies that no files are flagged as malicious.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

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 5 and CEM version 3.1 rev 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP.

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.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

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 SailPoint File Access Manager 8.3 SP5 product that is 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 APP_PP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. 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. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP related to the examination of the information contained in the TOE Summary Specification.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. 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 APP_PP related to the examination of the information contained in the operational guidance documents.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and the extended assurance requirement ALC_TSU_EXT.1 defined in the APP_PP. The evaluation team found that the TOE was identified, and a method of timely updates was described.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the APP_PP 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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and validated that the vendor fixed all findings with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the APP_PP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

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.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria Version 1.0, July 07, 2023*, document. No other product versions or platforms were evaluated, and no security claims are made for them.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product, including the primary advertised functionality of the product, which allows its users to review and manage the governed data created by FAM for the monitoring of enterprise data stored on one or more managed resources, was not assessed as part of this evaluation. Only the functionality discussed in Section 5 of this report was assessed. All other functionality provided by the product needs to be assessed separately and this report makes no statement about correctness of operation for that functionality. Section 7.2 of this document, and Section 2.3 “Excluded from the TOE” of the ST, provide the details of features that are part of the purchased product but were not included in the evaluation.

Consumers employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

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 File Access Manager 8.3 SP5 Security Target v1.0*, dated July 07, 2023.

13 List of Acronyms

Acronym	Definition
AA	Assurance Activity
API	Application Programing Interface
ASLR	Address Space Layout Randomization
CC	Common Criteria
CFG	Control Flow Guard
CVSS	Common Vulnerability Scoring System
DEP	Data Execution Prevention
DRBG	Deterministic Random Bit Generator
EAF	Export Address Filtering
FAM	File Access Manager
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAF	Import Address Filtering
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OSP	Organizational Security Policy
PII	Personally Identifiable Information
PP	Protection Profile
NIAP	National Information Assurance Partnership
RBG	Random Bit Generator
SFR	Security Functional Requirement
SAR	Security Assurance Requirement
SQL	Structured Query Language
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
WCF	Windows Communication Foundation

14 Terminology

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

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5.
4. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology (CEM), dated April 2017, version 3.1, Revision 5.
5. Protection Profile for Application Software, Version 1.4, dated Oct 7, 2021.
6. SailPoint File Access Manager 8.3 SP5 Security Target v1.0, dated July 7, 2023 (ST).
7. Assurance Activity Report for a Target of Evaluation "SailPoint File Access Manager 8.3 SP5" Assurance Activities Report v1.0, dated August 18, 2023. (AAR)
8. Evaluation Technical Report for a Target of Evaluation SailPoint File Access Manager 8.3 SP5 Version 1. 0 , August 18, 2023 (ETR)
9. SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria Version 1.0, dated July 7, 2023 (AGD).
10. SailPoint File Access Manager Administrator Guide Version: 8.3 Revised: March 30, 2022
11. SailPoint File Access Manager Installation Guide Version: 8.3 SP5 Revised: June 30, 2023
12. SailPoint IdentityIQ Version: 8.3.0.5000 File Access Manager v8.3 Service Pack 5 Deployment Guide
13. SailPoint File Access Manager 8.3 SP5 Vulnerability Analysis Version: 1.1 Aug 12, 2023
14. SailPoint File Access Manager 8.3 SP5 Test Plan v1.0 July 07, 2023
15. Proprietary_SailPoint_FAM_AppPPv1.4_Test_Matrix