**Assurance Activities Report**
**for a Target of Evaluation**

# SailPoint

# File Access Manager 8.3 SP5

## Assurance Activities Report (AAR)
## Version 1.0

August 18, 2023

Security Target (Version 1.0)

Evaluated by:

Booz | Allen | Hamilton

delivering results that endure

Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
1100 West St.
Laurel, MD  20707

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
**SailPoint Technologies, Inc.**
11120 Four Points Drive
Suite 100
Austin, TX 78726

The Author of the Security Target:
Booz Allen Hamilton
1100 West St.
Laurel, MD 20707 USA

The TOE Evaluation was sponsored by:
Booz Allen Hamilton

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

## Applicable Common Criteria Version

Common Criteria for Information Technology Security Evaluation, April 2017 Version 3.1 Revision 5

## Common Evaluation Methodology Version

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, April 2017
Version 3.1 Revision 5

# Table of Contents

1 Purpose - 1 -
2 TOE Summary Specification Assurance - 1 -
3 Operational Guidance Assurance Activities - 5 -
4 Test Assurance Activities (Test Report) - 7 -
4.1 Platforms Tested and Composition - 7 -
4.1.1 Test Configuration - 7 -
4.2 Omission Justification - 9 -
4.3 Test Cases - 9 -
4.3.1 Cryptographic Support - 9 -
4.3.2 User Data Protection - 11 -
4.3.3 Security Management - 14 -
4.3.4 Privacy - 16 -
4.3.5 Protection of the TSF - 16 -
4.3.6 Trusted Path/Channels - 23 -
5 Evaluation Activities for SARs - 24 -
6 Conclusions - 30 -
7 Glossary of Terms - 30 -

# 1 Purpose

The purpose of this document is to serve as a non-proprietary attestation that this evaluation has satisfied all of the TSS, AGD, and ATE Assurance Activities required by the Protection Profiles, Extended Packages, and/or PP-Modules to which the TOE claims exact conformance.

# 2 TOE Summary Specification Assurance

The evaluation team completed the testing of the Security Target (ST) *SailPoint File Access Manager 8.3 SP5 Security Target v1.0* and confirmed that the TOE Summary Specification (TSS) contains all Assurance Activities as specified by the *Protection Profile for Application Software Version 1.4* [APP_PP]. The evaluators were able to individually examine each SFR's TSS statements and determine that they comprised sufficient information to address each SFR claimed by the TOE as well as meet the expectations of the [APP_PP] Assurance Activities.

Through the evaluation of ASE_TSS.1-1, described in the ETR, the evaluators were able to determine that each SFR was described in enough detail to demonstrate that the TSF addresses the SFR. However, in some cases the Assurance Activities that are specified in the claimed source material instruct the evaluator to examine the TSS for a description of specific behavior to ensure that each SFR is described to an appropriate level of detail. The following is a list of each SFR, the TSS Assurance Activities specified for the SFR, and how the TSS meets the Assurance Activities. Additionally, each SFR is accompanied by the source material [APP_PP] that defines where the most up-to-date TSS Assurance Activity was defined.

**FCS_CKM_EXT.1.1 – TD0717** – "*The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the generate no asymmetric cryptographic keys selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements"*

Upon inspection of the application and its documentation, it was determined that the application does not generate asymmetric cryptographic keys. Section 6.3.1.1 has the generate no asymmetric cryptographic keys selected. Section 8.1.1 of the ST states that the TOE does not perform generation of asymmetric cryptographic keys. Therefore, this evaluation activity is considered satisfied.

**FCS_RBG_EXT.1.1** – *"If "use no DRBG functionality" is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services.*

*If "implement DRBG functionality" is selected, the evaluator shall ensure that additional FCS_RBG_EXT.2 elements are included in the ST.*

*If "invoke platform-provided DRBG functionality" is selected, the evaluator performs the following activities. The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below.*

*It should be noted that there is no expectation that the evaluators attempt to confirm that the APIs are being used correctly for the functions identified in the TSS; the activity is to list the used APIs and then do an existence check via decompilation."*

Upon inspection of the application and its documentation, it was determined that the application does not use DRBG functionality for cryptographic operations. Section 6.3.1.2 has selected use no DRBG functionality. Section 8.1.2 of the ST states the TOE does not directly invoke any DRBG functionality for any SFR related functionality. Therefore, this evaluation activity is considered satisfied.

**FCS_STO_EXT.1.1** – *"The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored."*

The evaluator examined Section 8.1.3 of the ST that states that the credentials for accessing the SQL database are stored using the Data Protection API. The TOE invokes the Windows platform to encrypt these credentials using a certificate located in the Windows Certificate Store. The TOE will then invoke the Windows platform to store the encrypted credentials.

The evaluator concludes that the TSS indicates the credentials used for accessing the SQL database, how and where they are stored, and how they are encrypted. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FDP_DAR_EXT.1.1** – *"The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the following activities cover all of the sensitive data identified in the TSS.*

*If not store any sensitive data is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test below."*

Section 8.2.1 of the ST states that the credentials for accessing the SQL database are stored using the Data Protection API, in accordance with FCS_STO_EXT.1. The TOE will invoke the Windows platform to encrypt these credentials using a certificate located in the Windows Certificate Store and then invoke the Windows platform to store the encrypted credentials. This description is consistent with the ST selection "protect sensitive data in accordance with FCS_STO_EXT.1. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FDP_DEC_EXT.1.1** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FDP_DEC_EXT.1.2** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FDP_NET_EXT.1.1** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FMT_CFG_EXT.1.1** – *"The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials."*

The evaluator examined that in Section 8.3.1 of the ST, it states that during the installation process, the administrator that performs the installation will define their own password for the TOE's main administrative account. There are no default credentials for the TOE. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FMT_CFG_EXT.1.2** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FMT_MEC_EXT.1.1** – *"The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.*

*Conditional: If "implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption" is selected, the evaluator shall ensure that the TSS identifies those options, as well as indicates where the encrypted representation of these options is stored."*

Section 8.3.2 of the ST states that the TOE maintains a set of configuration options to run in the evaluated configuration. The SFR related configuration options are stored per the mechanisms recommended by the Windows platform vendor for .NET Core applications.

**FMT_SMF.1.1** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPR_ANO_EXT.1.1** – *"The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted."*

Section 8.4.1 of the ST states that the TOE does not collect personally identifiable information (PII) for administrators or users. Therefore, there is no case in which the TOE will transmit this data over the network. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FPT_AEX_EXT.1.1** – *"The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled."*

Section 8.5.1 of the ST states that during the compilation of the TOE's software, the /NXCOMPAT flag is set to ensure that Data Execution Prevention (DEP) protections are enabled. Windows Defender Exploit Guard Exploit Protection configured on with the following enabled: Control Flow Guard (CFG), randomize memory allocations (Bottom-Up ASLR), Export Address Filtering (EAF), Import Address Filtering (IAF), and DEP. Based on the description, the evaluation activity for this SFR is considered satisfied.

**FPT_AEX_EXT.1.2 –** This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_AEX_EXT.1.3 –** This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_AEX_EXT.1.4 –** This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_AEX_EXT.1.5 –** This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_API_EXT.1.1** – *"The evaluator shall verify that the TSS lists the platform APIs used in the application."*

Section 8.5.2 of the ST states that the TOE is installed on the Windows platform and uses only supported Windows platform (.NET) APIs in order to function. Table 12 in the ST lists the .NET Core APIs used by the TOE. Because the TOE is dependent on the Windows platform (.NET Core) APIs in order to function properly and these lists were provided by the vendor, the evaluator has determined that the supported APIs listed in the ST satisfy this evaluation activity.

**FPT_IDV_EXT.1.1** – *"If "other version information" is selected the evaluator shall verify that the TSS contains an explanation of the versioning methodology."*

The TOE is versioned with a "major release number, minor release number, patch number, service pack number" methodology. Section 8.5.3 of the ST states that the versioning nomenclature used by the TOE is #.#.#.#. The first number indicates the major release number and is incremented by the value of 1. The second number is the minor release number and is incremented by the value of 1. The third number represents the patch number and is incremented by the value of 1000. The fourth number represents the service pack number and is incremented by the value of 1000. This clearly explains the TOE versioning schematics; therefore, the evaluator has determined the evaluation activity is met.

**FPT_LIB_EXT.1.1 –** This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_TUD_EXT.1.1** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_TUD_EXT.1.2** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_TUD_EXT.1.3** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_TUD_EXT.1.4** – *"The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained."*

Section 8.5.5 of the ST explains that the software update packages are downloaded in the Windows Universal Application package (.APPX) format. During the build process, SailPoint digitally signs a software update package using their private key and their certificate signed by DigiCert. Once a software update package is on the system where the TOE is installed, an administrator with permission to the 'Start Installation' button via the fat client can initiate the update process. The fat client will request the platform to validate the certificate using the public key from DigiCert that is already loaded on the platform and verifies the digital signature on the software update package using the public key in the certificate. The software update process will only occur if the signature validation is successful.

The TSS clearly describes how updates are obtained and how they are signed by DigiCert during the build process. The TSS also explains the administrator permissions and actions to perform the installation and updates of the TOE. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FPT_TUD_EXT.1.5** – *"The evaluator shall verify that the TSS identifies how the application is distributed. If "with the platform" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "as an additional package" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2."*

The evaluator observed in Section 8.5.5 of the ST that the TOE administrator downloads the software installation package or software update package from SailPoint's customer portal. This is the only method for distributing the TOE software. This is consistent with the ST selection of "as an additional package to the platform OS". Therefore, the evaluation activities were performed as required by the ATE test assurance activity for FPT_TUD_EXT.2 (see Test Assurance Activities section below for details) as stated. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FPT_TUD_EXT.2.1** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_TUD_EXT.2.2** – This SFR does not contain any [APP_PP] TSS Assurance Activities.

**FPT_TUD_EXT.2.3** – *"The evaluator shall verify that the TSS identifies how the application installation package is signed by an authorized source. The definition of an authorized source must be contained in the TSS."*

Section 8.5.5 of the ST states that during the build process, SailPoint digitally signs the .MSI or .EXE file using their private key and their certificate signed by DigiCert. During the installation process, the platform will validate the certificate using the public key from DigiCert that is already loaded on the platform and verifies the digital signature on the .MSI or .EXE file using the public key in the certificate. The installation process will only occur if the signature validation is successful.

Additionally Section 8.5.5 states that each customer that is entitled to the TOE software has a username and password for accessing SailPoint's customer portal. TOE administrator downloads the software installation package or software update package from SailPoint's customer portal. This is the only method for distributing TOE software.

The TSS clearly describes how installation packages are signed by DigiCert during the build process. The TSS also explains the administrator permissions and actions to perform the installation and updates of the TOE. Based on this description, the evaluation activity for this SFR is considered satisfied.

**FTP_DIT_EXT.1.1 –** *"For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality."*

Section 8.6.1 of the ST states the TOE invokes the platform's .NET Core to encrypt the communications between the TOE and the remote Activity Monitors. The TOE calls the .NET System.ServiceModel API for this interface. All communication over this interface is protected by TLS.

The evaluator has found that this evaluation activity is satisfied because of the detailed description of each trusted path/channel that the TOE communicates with, the calls to the platform by each interface, and protocols used for protection of the communication.

# 3 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, which includes the review of the *SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria v1.0* (AGD) document and confirmed that the Operational Guidance contains all Assurance Activities as specified by the *Protection Profile for Application Software Version 1.4* [APP_PP]. The evaluators reviewed the [APP_PP] to identify the security functionality that must be discussed for the operational guidance. This is prescribed by the Assurance Activities for each SFR and the AGD SARs. The evaluators have listed below each of the SFRs defined in the [APP_PP] that have been claimed by the TOE (some SFRs are conditional or optional) as well as the AGD SAR, along with a discussion of where in the operational guidance the associated Assurance Activities material can be found. The AGD includes references to other guidance documents that must be used to properly install, configure, and operate the TOE in its evaluated configuration. The AGD and its references to other SailPoint File Access Manager guidance documents were reviewed to assess the Operational Guidance Assurance Activities. The AGD contains references to these documents in Chapter 4 and these references can also be found below:

The following references are used in this section of the document:

[1] SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria v1.0 (AGD)

[2] SailPoint File Access Manager Administrator Guide Version 8.3

[3] SailPoint File Access Manager Installation Guide Version 8.3 SP5

**FCS_CKM_EXT.1.1 – TD0717** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FCS_RBG_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FCS_STO_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FDP_DAR_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FDP_DEC_EXT.1.1** – *"The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required."*

Section 7.1 of the AGD "Access to Platform Resources" identifies that the TOE requires network connectivity for communication with web browsers for GUI access and Activity Monitor applications. The AGD as a whole supports the need and identifies the purposes that network access is required and is consistent with the SFR selection of network resources only. Therefore, this evaluation activity is considered satisfied.

**FDP_DEC_EXT.1.2** – *"The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator* *shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required."*

Section 7.1 of the AGD "Access to Platform Resources" identifies that the TOE access the Windows operating system's Active Directory component which is a sensitive data repository that contains enterprise user data. This is consistent with the SFR selection of Active Directory only. Therefore, this evaluation activity is considered satisfied.

**FDP_NET_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FMT_CFG_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FMT_CFG_EXT.1.2** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FMT_MEC_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FMT_SMF.1.1** – *"The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function."*

The following list was taken from the ST and then mapped to the AGD section that provides the instructions:

- configuration of the Active Directory to which the TOE will communicate via the fat client, [AGD Section 7.2]
- perform tasks that read data from Active Directory via the GUI and the fat client, [AGD Section 7.2]
- perform tasks that read or write data (i.e., local user credentials, configuration data, governed data) to the SQL database via the GUI and the fat client, [AGD Section 7.2]
- query the current version of the TOE via the fat client, [AGD Section 6.1]
- perform the software update process via the fat client, [AGD Section 7.3]

All management functions defined in the SFR have corresponding sections in the AGD that describe the administrative procedures. Therefore, this evaluation activity is considered satisfied.

**FPR_ANO_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_AEX_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_AEX_EXT.1.2 –** This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_AEX_EXT.1.3 –** This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_AEX_EXT.1.4 –** This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_AEX_EXT.1.5 –** This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_API_EXT.1.1 –** This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_IDV_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_LIB_EXT.1.1 –** This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_TUD_EXT.1.1** – *"The evaluator shall check to ensure the guidance includes a description of how updates are performed."*

Section 7.3 of the AGD "Secure Updates" provides instruction on performing trusted updates. Therefore, this evaluation activity is considered satisfied.

**FPT_TUD_EXT.1.2** – *"The evaluator shall verify guidance includes a description of how to query the current version of the application."*

Section 6.1 of the AGD "Query the Installed Version of the TOE" provides the instructions to verify what version of the application is being used. Therefore, this evaluation activity is considered satisfied.

**FPT_TUD_EXT.1.3** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_TUD_EXT.1.4** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_TUD_EXT.1.5** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_TUD_EXT.2.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FPT_TUD_EXT.2.2** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

**FTP_DIT_EXT.1.1** – This SFR does not contain any [APP_PP] AGD Assurance Activities.

# 4 Test Assurance Activities (Test Report)

The following sections demonstrate that all ATE Assurance Activities for the TOE have been met. This evidence has been presented in a manner that is consistent with the "Reporting for Evaluations Against NIAP-Approved Protection Profiles" guidance that has been provided by NIAP. Specific test steps and associated detailed results are not included in this report in order for it to remain non-proprietary. The test report is a summarized version of the test activities that were performed as part of creating the Evaluation Technical Report (ETR).

Evaluator-conducted manual testing was completed in July 2023. The evaluation team set up a test environment for the independent functional testing that allowed them to perform all test assurance activities across the SailPoint FAM over the SFR relevant interfaces.

## *4.1 Platforms Tested and Composition*

All required test assurance activities were performed against the TOE application. The TOE was installed on an Intel Xeon Gold 6230 (Cascade Lake) platform with the Windows 2019 Server Datacenter version 1809 operating system that matched the CC evaluated Windows Server 2019 (update 1809) Security Target.

The evaluation team performed testing of the TSF functionality using the TOE's two available management interfaces (local fat client, remote GUI) and the operational environment as depicted in the figure below. The full set of tests were developed to stimulate each applicable TSF relevant interface, which would fully test all combinations of the TSF relevant interfaces. The testing is consistent with the use of the interfaces defined within the ST. Thus, the testing of the interfaces was based upon testing SFR functionality related to user actions over each interface.

### 4.1.1 Test Configuration

The evaluation team configured the TOE for testing according to the *SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing activities of SailPoint File Access Manager 8.1 between April and July 2023. Testing was conducted at the Booz Allen CCTL in Laurel, MD.

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

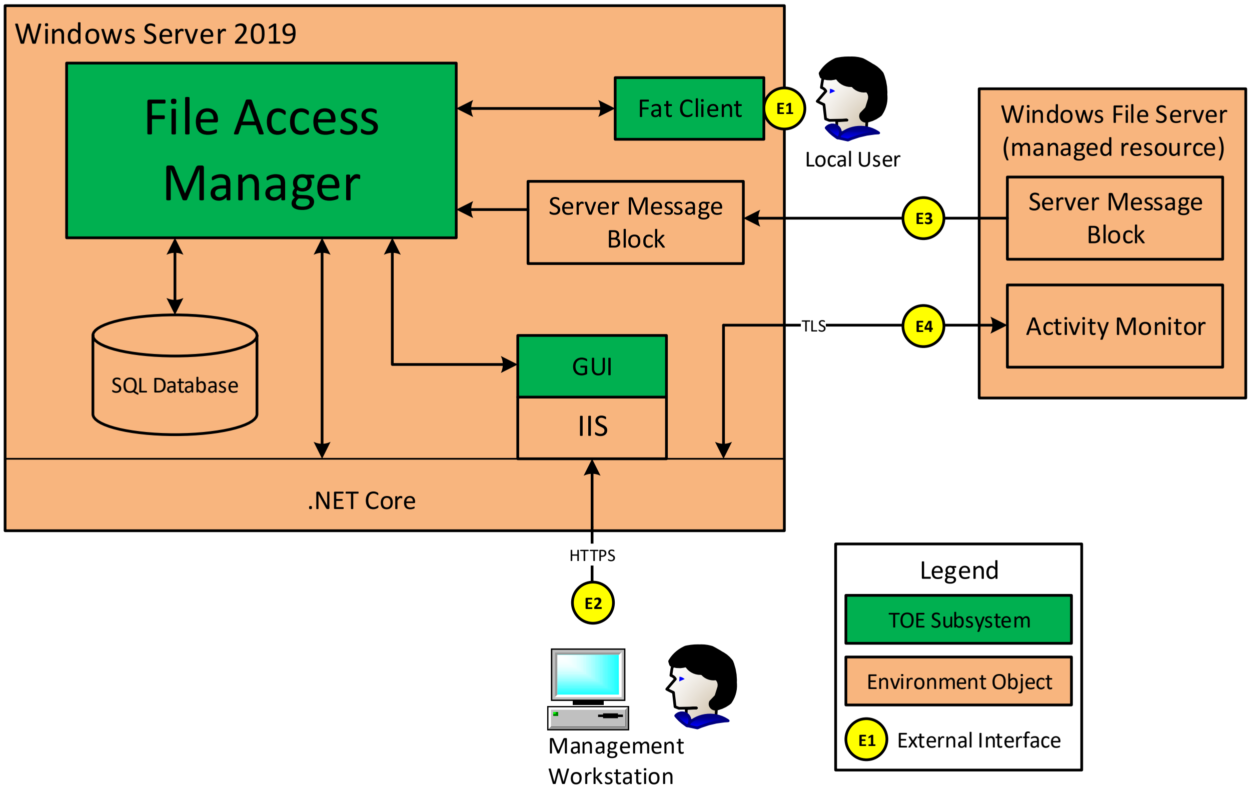

Figure 1 - Test Configuration

The TOE has the following external interfaces:

- **E1: Local User to fat client** – Accessed through the Windows operating system, this is the local interface for authentication to and administration of the TOE.
- **E2: Remote Workstation to IIS (TOE GUI)** – Accessed through a web browser on a remote general-purpose management workstation, this is the remote administration interface of the TOE. This interface is over a secure HTTPS connection (HTTPS server) which is provided by .NET Core invoked by IIS. IIS and .NET Core are components of the Windows platform. This interface is being described for completeness of the required operational environment. To be clear, this operational environment interface is out-of-scope for testing but is required in order to test the GUI TOE component, which is in-scope of the evaluation.
- **E3: Server Message Block to Server Message Block** – This is not a direct interface for the FAM product as the connection is completely handled between the instance of Windows on each managed resource and the Windows platform FAM is installed on. This interface is being described for completeness since the FAM product creates governed data based upon the information provided over this interface which can result in the invocation of or display of data through the interfaces described above. This interface is not tested as part of the evaluated configuration.
- **E4: FAM to Activity Monitor** – If an Activity Monitor is installed on a managed resource, the TOE will communicate with the Activity Monitor to collect data on the managed resource for the

FAM product's primary purpose. This interface is over a secure TLS connection (TLS server) which is provided by .NET Core component of the Windows platform.

**Tested interface summary:**

- Locally connected interface: E1
- TOE invoked network interfaces in-scope for testing: E4,
- Required Operational Environment network interfaces out-of-scope for testing: E2, E3
- TOE User interfaces tested: Fat Client and GUI

## *4.2 Omission Justification*

The TOE is a single instance of software that was installed on a Windows Server 2019 Datacenter platform and was fully tested as part of this test plan. This is the only operating system claimed in the evaluation. Successful completion of the tests is sufficient to demonstrate the appropriate behavior of the TSF.

During the evaluation, the TOE was updated to 8.3.0 SP5 as a result of SailPoint self-reporting vulnerabilities on features and functions that are outside the scope of the evaluated functionality. The lab performed an impact analyses and found that there were no impactful changes to any NDcPP testing that had been performed. It was determined that 8.3.0 and 8.3.0 SP5 are functionally equivalent. Despite this finding, the lab still performed regression testing on administrative functions to ensure that the non-SFR related functions did not impact the SFR related functions, as well as network tests, and the update tests.

## *4.3 Test Cases*

The evaluation team completed the functional testing activities within the Booz Allen laboratory environment. The evaluation team conducted a set of testing that includes all ATE Assurance Activities as specified by the *Protection Profile for Application Software Version 1.4* [APP_PP]. The evaluators reviewed the [APP_PP] to identify the security functionality that must be verified through functional testing. This is prescribed by the Assurance Activities for each SFR.

If an SFR is not listed, one of the following conditions applies:

- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a test Assurance Activity for a different SFR.
- The Assurance Activity for the SFR does not specify any actions related to ATE activities (e.g., FCS_CKM_EXT.1).

Note that some SFRs do not have Assurance Activities associated with them at the element level (e.g., FCS_CKM_EXT.1.1). In such cases, testing for the SFR is considered to be satisfied by completion of all Assurance Activities at the component level.

The following lists for each ATE Assurance Activity, the test objective, test instructions, test steps, and test results. Note that unless otherwise specified, the test configuration is to be in the evaluated configuration as defined by the AGD. For example, some tests require the TOE to be brought out of the evaluated configuration to temporarily disable cryptography to prove that the context of transmitted data is accurate. As part of the cleanup for each test, the TOE is returned to the evaluated configuration.

### 4.3.1 Cryptographic Support

Note: The TOE does not provide any native cryptography. All cryptography is provided by the underlying OS.

| **Test Case Number** | 001 |
|---|---|
| **SFR** | FCS_RBG_EXT.1.1 |
| **Test Objective** | If **invoke platform-provided DRBG functionality** is selected, the following tests shall be performed: |

| | |
|---|---|
| | The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API.<br>The following are the per-platform list of acceptable APIs:<br>**For Windows:** The evaluator shall verify that rand_s, RtlGenRandom, BCryptGenRandom, or CryptGenRandom API is used for classic desktop applications. The evaluator shall verify the application uses the RNGCryptoServiceProvider class or derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications. It is only required that the API is called/invoked, there is no requirement that the API be used directly. In future versions of this document, CryptGenRandom may be removed as an option as it is no longer the preferred API per vendor documentation. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | The SFR selection in the ST is “use no DRBG functionality”. Therefore, this test assurance activity does not apply. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 002 |
| **SFR** | FCS_STO_EXT.1.1 |
| **Test Objective** | For all credentials for which the application implements functionality, the evaluator shall verify credentials are encrypted according to FCS_COP.1(1) or conditioned according to FCS_CKM.1.1(1) and FCS_CKM.1(3). For all credentials for which the application invokes platform-provided functionality, the evaluator shall perform the following actions which vary per platform.<br>**For Windows:** The evaluator shall verify that all certificates are stored in the Windows Certificate Store. The evaluator shall verify that other credentials, like passwords, are stored in the Windows Credential Manager or stored using the Data Protection API (DPAPI). For Windows Universal Applications, the evaluator shall verify that the application is using the ProtectData class and storing credentials in IsolatedStorage. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Per .NET (core) framework API documentation, https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.protecteddata? |

| | |
|---|---|
| | view=netframework-4.5, DPAPI calls for encrypting and decrypting data are as follows:<br>• Encrypt: ProtectedData.Protect<br>• Decrypt: ProtectedData.Unprotect<br>Examine the source code of the TOE application for DPAPI calls:<br>a) Capture the source code containing “ProtectedData.Protect”.<br>b) Capture the source code containing “ProtectedData.Unprotect”.<br>2. Verify that the password is encrypted by opening C:\Program Files\SailPoint\NHibernate\hibernate.cfg.xml in a text editor. In the file look for the connection string used to connect to the DB. Something like this:<br>Server=SERVER_NAME,1433;initial catalog=DB_NAME;User=FAM_USER;Password=<encrypted string>;Pooling=true |
| **Test Results** | The source code search for “ProtectedData.Protect” and “ProtectedData.Unprotect” resulted in code containing these methods used to perform encryption and decryption on the SQL database credentials demonstrating DPAPI being used.<br>The .xml file showed that the password has been stored encrypted. -Pass |
| **Execution Method** | Manual |

### 4.3.2 User Data Protection

| | |
|---|---|
| **Test Case Number** | 003 |
| **SFR** | FDP_DEC_EXT.1.1 |
| **Test Objective** | **For Windows:** For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required hardware capabilities. The evaluator shall verify that the user is made aware of the required hardware capabilities when the application is first installed. This includes permissions such as ID_CAP_ISV_CAMERA, ID_CAP_LOCATION, ID_CAP_NETWORKING, ID_CAP_MICROPHONE, ID_CAP_PROXIMITY and so on. A complete list of Windows App permissions can be found at:<br>• http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx<br>For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of the required hardware resources. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Inspect the application software documentation for a list of the required hardware resources used by the TOE. |
| **Test Results** | The application software documentation (Section 7.1 of the AGD) provided a list of the required hardware resources used by the TOE, to include: network adapter. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 004 |
| **SFR** | FDP_DEC_EXT.1.2 |

| | |
|---|---|
| **Test Objective** | **For Windows:** For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required capabilities. The evaluator shall identify the required information repositories when the application is first installed. This includes permissions such as ID_CAP_CONTACTS,ID_CAP_APPOINTMENTS,ID_CAP_MEDIALIB and so on. A complete list of Windows App permissions can be found at:<br>• http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx<br>For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of sensitive information repositories it accesses. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Inspect the application software documentation for a list of the sensitive information repositories accessed by the TOE. |
| **Test Results** | The application software documentation (Section 7.1 of the AGD) provided a list of the sensitive information repositories accessed by the TOE, to include: Windows operating system's Active Directory component - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 005 |
| **SFR** | FDP_NET_EXT.1.1 |
| **Test Objective** | The evaluator shall perform the following tests:<br>**Test 1:** The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Stop the TOE services.<br>2. Begin capturing packets using Microsoft Network Monitor on the machine running the TOE to capture Activity Monitor Traffic.<br>3. Begin capturing packets using Wireshark on the machine running the TOE to capture other network traffic.<br>4. Start the TOE services.<br>5. Perform the following activities to stimulate the TOE such that the claimed network communication occurs:<br>a. From the test machine (Management Workstation), establish a connection and authenticate to the TOE application via the web UI (NOTE: This stimulates the management of the TOE via the web UI):<br>b. From the Windows File Server (Activity Monitor) machine, perform file system read/write activities on the host.<br>6. Stop capturing packets on the machine running the TOE.<br>7. Open Process Explorer and capture the PIDs of the services labeled with "SailPoint Technologies Inc 2022" under the Company Name column.<br>8. Verify that any network communications associated with the TOE application are documented in the TSS or are user-initiated. |
| **Test Results** | All network communications associated with the TOE processes are documented in the ST and/or are user initiated. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 006 |

| | |
|---|---|
| **SFR** | FDP_NET_EXT.1.1 |
| **Test Objective** | The evaluator shall perform the following tests:<br>**Test 2:** The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP). |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Ensure the TOE application is uninstalled.<br>2. Execute the following command on the underlying TOE host: `netstat -anbo`<br>3. Install the TOE application.<br>4. Run the TOE application.<br>5. Open Process Explorer and capture the PIDs of the services labeled with “SailPoint Technologies Inc 2020” under the Company Name column.<br>6. After the application initializes, execute the following command on the machine running the TOE: `netstat -anbo`<br>7. Inspect the output for any LISTENING ports associated with the TOE application by comparing the differences in netstat output from Step 2 against Step 6, in addition to the output from Step 5, as needed. |
| **Test Results** | Any ports opened by the application have been defined in the ST’s TSS section 8.2.3. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 007 |
| **SFR** | FDP_DAR_EXT.1.1 – TD0756 |
| **Test Objective** | Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.<br>If "implement functionality to encrypt sensitive data as defined in the PP-Module for File Encryption" or "protect sensitive data in accordance with FCS_STO_EXT.1" is selected the evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.<br>If **leverage platform-provided functionality** is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis.<br>**For Windows:** The Windows platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption, such as BitLocker or Encrypting File System (EFS), clear to the end user. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | The only SFR selection is “protect sensitive data in accordance with FCS_STO_EXT.1”. As such, this test assurance activity is met by testing performed in FCS_STO_EXT.1 – Test Case 002. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

### 4.3.3 Security Management

| | |
|---|---|
| **Test Case Number** | 008 |
| **SFR** | FMT_MEC_EXT.1.1 |
| **Test Objective** | If “invoke the mechanisms recommended by the platform vendor for storing and setting configuration options” is chosen, the method of testing varies per platform as follows:<br>**For Windows:** The evaluator shall determine and verify that Windows Universal Applications use either the Windows.Storage namespace, Windows.UI.ApplicationSettings namespace, or the IsolatedStorageSettings namespace for storing application specific settings. For .NET applications, the evaluator shall determine and verify that the application uses one of the locations listed in https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/ for storing application specific settings.For Classic Desktop applications, the evaluator shall run the application while monitoring it with the SysInternals tool ProcMon and make changes to its configuration. The evaluator shall verify that ProcMon logs show corresponding changes to the Windows Registry or C:\ProgramData\ directory. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | **NOTE: According to the URL provided for .NET applications in the Test Objective section of this test, the location of executable-hosted application configuration files is located in the same directory as the executable and have the following filename convention: “[ExecutableApplication.exe].config”, where “ExecutableApplication.exe” is the associated application binary.**<br>1. On the server running the TOE application, open a PowerShell window and execute the following command: `Get-ChildItem -Path 'C:\Program Files\SailPoint\' -Include *.exe,*.exe.config -Recurse`<br>2. Verify that the TOE application executable directories contain configuration files in the same directory with the following filename convention: “[ExecutableApplication.exe].config”, where “ExecutableApplication.exe” is the associated application binary. |
| **Test Results** | For any “[ExecutableApplication.exe].config” file, there is an associated “ExecutableApplication.exe” binary in the same directory. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 009 |
| **SFR** | FMT_CFG_EXT.1.1 |
| **Test Objective** | If the application uses any default credentials the evaluator shall run the following tests.<br>**Test 1:** The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | N/A – The Security Target states there are no default credentials for the TOE. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 010 |
| **SFR** | FMT_CFG_EXT.1.1 |
| **Test Objective** | If the application uses any default credentials the evaluator shall run the following tests.<br>**Test 2:** The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | N/A – The Security Target states there are no default credentials for the TOE. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 011 |
| **SFR** | FMT_CFG_EXT.1.1 |
| **Test Objective** | If the application uses any default credentials the evaluator shall run the following tests.<br>**Test 3:** The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | N/A – The Security Target states there are no default credentials for the TOE. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

<table>
<tr><td><b>Test Case Number</b></td><td>012</td></tr>
<tr><td><b>SFR</b></td><td>FMT_CFG_EXT.1.2</td></tr>
<tr><td><b>Test Objective</b></td><td>The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform.<br><b>For Windows:</b> The evaluator shall run the SysInternals tools, Process Monitor and Access Check (or tools of equivalent capability, like icacls.exe) for Classic Desktop applications to verify that files written to disk during an application's installation have the correct file permissions, such that a standard user cannot modify the application or its data files. For Windows Universal Applications the evaluator shall consider the requirement met because of the AppContainer sandbox.</td></tr>
<tr><td><b>Test Instructions</b></td><td>Execute this test per the test steps.</td></tr>
<tr><td><b>Test Steps</b></td><td>1. Inspect filesystem paths created by the installer to determine where the TOE installs its files.<br>2. Execute the command specifying the directories based on the inspection performed in Step 1. Repeat for all directories where the TOE installs it’s files.<br>Get-ChildItem '<<b><i>full path to directory</i></b>>' -Recurse | Get-Acl | Format-List | Out-File '.\TOE_file_permissions_<<b><i>directoryname</i></b>>.txt'<br>3. Verify that each file has the correct file permissions (i.e. standard users cannot modify application or data files).</td></tr>
</table>

| | |
|---|---|
| **Test Results** | Each file was found to have the correct file permissions (standard users cannot modify application or data files). For each BUILTIN\Users entries the permissions do not contain delete, write or modify capabilities. -Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 013 |
| **SFR** | FMT_SMF.1.1 |
| **Test Objective** | The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Exercise the management functions of the TOE application as described in the ST:<br>a. Configure the AD server to which the TOE will communicate, read/write data from the SQL database, and read data from the AD server via the fat client.<br>b. Perform task to read data from AD and read/write from the SQL database via the GUI:<br>c. Query the current version of TOE via the fat client:<br>d. Perform the software update process via the fat client (See Test 21 for FPT_TUD_EXT.1) |
| **Test Results** | All defined functions performed as descripted within the AGD documentation. -Pass |
| **Execution Method** | Manual |

### 4.3.4 Privacy

| | |
|---|---|
| **Test Case Number** | 014 |
| **SFR** | FPR_ANO_EXT.1.1 |
| **Test Objective** | If require user approval before executing is selected, the evaluator shall run the application and exercise the functionality responsibly for transmitting PII and verify that user approval is required before transmission of the PII. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | N/A – The Security Target states that the TOE does not collect personally identifiable information (PII). |
| **Test Results** | Pass |
| **Execution Method** | Manual |

### 4.3.5 Protection of the TSF

| | |
|---|---|
| **Test Case Number** | 015 |
| **SFR** | FPT_API_EXT.1.1 |
| **Test Objective** | The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. For each API listed in the TSS, verify that it is a documented and supported .NET Core API by searching through developer documentation on the APIs online. If the API is found to be supported and not missing or deprecated then that API is allowed. |

| | |
|---|---|
| **Test Results** | The evaluator found all of the declared APIs in the Microsoft documentation for .NET website and nuget.org website. Each API is supported and not deprecated. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 016 |
| **SFR** | FPT_AEX_EXT.1.1 |
| **Test Objective** | The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings.<br>**For Windows:** The evaluator shall run the same application on two different Windows systems and run a tool that will list all memory mapped addresses for the application. The evaluator shall then verify the two different instances share no mapping locations. The Microsoft SysInternals tool, VMMap, could be used to view memory addresses of a running application. The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application has ASLR enabled. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | **a) Memory Mapping**<br>1. Start the TOE application on the server machine.<br>2. Launch VMMAP on the server machine.<br>3. In the VMMAP instances, set the process to the TOE's executable and wait for the memory scans to complete.<br>4. Save the VMMAP results.<br>5. Repeat Steps 1-4 for each of the TOE's executables running in memory.<br>6. Perform the Steps under the "ASLR" section of this test case.<br>7. Uninstall the TOE application from the server machine.<br>8. Reboot the server machine.<br>9. Install the TOE application on the server machine.<br>10. Repeat Steps 1-6.<br>11. Compare the results from the two VMMAP scan instances and verify that the two instances share no mapping locations.<br>**b) ASLR**<br>1. Open a PowerShell window on the server machine running the TOE.<br>2. Import the module using the command.<br>3. Execute against the TOE application executables using the applicable command.<br>4. Verify the tool's output contains the statement "ASLR : True", indicating has ASLR enabled for all of the TOE application executables running in memory. |
| **Test Results** | The two instances of the TOE application did not share any memory mapping locations and that the ASLR was enabled. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 017 |
| **SFR** | FPT_AEX_EXT.1.2 |

| | |
|---|---|
| **Test Objective** | The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform.<br>**For Windows:** The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application passes the NXCheck. The evaluator may also ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled for the application. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Launch the TOE application.<br>2. Using the Process Explorer, obtain the list of SailPoint FAM related processes as a result of performing Step 1.<br>3. Open a PowerShell window.<br>4. Execute the command to import the security tool module.<br>5. Execute the command for each TOE application executable file determined from Step 2.<br>6. Verify that the tool output from Step 3 contains the statement "DEP : True", indicating that the /NXCOMPAT flag was used during compilation. |
| **Test Results** | The tool output indicated the required "DEP : True" and confirmed that the /NXCOMPAT flag was used during compilation on all TOE application executables. - Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 018 |
| **SFR** | FPT_AEX_EXT.1.3 |
| **Test Objective** | The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests:<br>**For Windows:** If the OS platform supports Windows Defender Exploit Guard (Windows 10 version 1709 or later), then the evaluator shall ensure that the application can run successfully with Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The following link describes how to enable Exploit Protection, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/customize-exploit-protection. If the OS platform supports the Enhanced Mitigation Experience Toolkit (EMET) which can be installed on Windows 10 version 1703 and earlier, then the evaluator shall ensure that the application can run successfully with EMET configured with the following minimum mitigations enabled; Memory Protection Check, Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), and Data Execution Prevention (DEP). |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Start TOE.<br>2. Using Process Explorer, obtain the list of SailPoint FAM related processes as a result of performing Step 1. (before restart PID list)<br>3. Stop TOE.<br>4. Set the CFG, Bottom-Up ASLR, EAF, IAF, and DEP protections.<br>5. Restart the TOE application services.<br>6. Using Process Explorer, obtain the list of SailPoint FAM related processes as a result of performing Step 6  (after restart PID list)<br>7. Verify all the same processes are running after restart (output of step 7) as were running before (output of step 3) |

| | |
|---|---|
| | 8. Execute the `Get-ProcessMitigation -id [PID]` powershell command to verify the configuration in Step 2 for each process identifier (PID) of the TOE application services:<br>9. Verify that the TOE application runs successfully with the new Windows Defender Exploit Guard Protection configuration.<br>a. Authenticate to the TOE fat client and perform functions such as a health check and reading AD configurations. |
| **Test Results** | The CFG, Bottom-Up ASLR, EAF, IAF, and DEP protections were enabled for each TOE application service and the TOE application runs successfully. -PASS |
| **Execution Method** | Manual |

| **Test Case Number** | 019 |
|---|---|
| **SFR** | FPT_AEX_EXT.1.4 |
| **Test Objective** | The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform:<br><br>**For Windows:** For Windows Universal Applications the evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox). For Windows Desktop Applications the evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Inventory and calculate the hashes of every file in the TOE application executable directories.<br>2. Run the TOE application.<br>a. Search for any method to export reports to TOE file system.<br>b. If a means is discovered: Generate reports and tasks.<br>3. Re-inventory and calculate the hashes of every file in the TOE application executable directories.<br>4. Note where, if any, user-modifiable files are written (indicative of a file hash difference or addition of new file).<br>5. Verify that there are no executable files stored in the same directories to which the application wrote, if any, user-modifiable files. |
| **Test Results** | It was found that no method was available to export reports to the filesystem. There were no executable files stored in the same directories to which the application wrote user-modifiable files. -Pass |
| **Execution Method** | Manual |

| **Test Case Number** | 020 |
|---|---|
| **SFR** | FPT_AEX_EXT.1.5 |
| **Test Objective** | The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present.<br><br>**For Windows:** Applications that run as Managed Code in the .NET Framework do not require these stack protections. Applications developed in Object Pascal using the Delphi IDE compiled with RangeChecking enabled comply with this element. For other code, the evaluator shall review the TSS and verify that the /GS flag was used during compilation. The evaluator shall run a tool like, BinScope, that can verify the correct usage of /GS. |

| | |
|---|---|
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | N/A – Per the Security Target TSS, the TOE's software runs as Managed Code in the .NET Core, and therefore no additional stack-based buffer overflow protection needs to be enabled. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 021 |
| **SFR** | FPT_TUD_EXT.1.1 |
| **Test Objective** | The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | **If update is NOT available:**<br>This requirement is considered to be met.<br>**If update is available:**<br>Install update steps:<br>1. From the local machine where the TOE is installed, launch the TOE fat client.<br>2. Authenticate to the TOE fat client.<br>3. Validate version operating (before)<br>4. Following the AGD, perform the steps to upgrade the TOE.<br>5. Launch the TOE fat client.<br>6. Verify version is upgraded to the expected version on the Fat Client (after)<br>NOTE: A failed update to the TOE’s software version will result in a failure state under the “Upgrades & Patches” tab as well as an error icon (a red X icon) associated with that software update. A successful update to the TOE’s software version will result in a successful state under the “Upgrades & Patches” tab associated with that software update. |
| **Test Results** | The TOE successfully updated without error and reported the new version. -Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 022 |
| **SFR** | FPT_TUD_EXT.1.2 |
| **Test Objective** | The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Query the current version of the TOE application:<br>a. From the local machine, launch the TOE fat client.<br>b. Authenticate to the TOE fat client.<br>c. Observe the client version output in the lower right corner of the TOE fat client.<br>2. Verify that the queried version matches that of the documented and installed version. |
| **Test Results** | The queried version of the TOE matched that of the documented and installed version. -Pass |

| | |
|---|---|
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 023 |
| **SFR** | FPT_TUD_EXT.1.3 |
| **Test Objective** | The evaluator shall verify that the application's executable files are not changed by the application. For all other platforms, the evaluator shall perform the following test:<br>**Test 1:** For all other platforms: The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Ensure the TOE is not installed on the system.<br>2. Execute the command on the system via an Administrator Command Prompt to inventory the file system.<br>3. Install the TOE on the system.<br>4. Execute the command on the system via an Administrator Command Prompt to inventory the file system.<br>5. Examine the two filesystem output files for differences between the filesystem before and after the installation of the TOE to determine where the TOE writes its executable files.<br>6. Calculate and save the hashes of the TOE files.<br>7. Launch the TOE fat client application.<br>8. Exercise all features of the TOE application as described in the ST:<br>a. Configure the AD servers to which the TOE will communicate:<br>b. Perform task to read data from AD server and SQL database:<br>c. Query the current version of TOE:<br>d. Do not perform the software update process if update is available:<br>**i. NOTE: This was omitted as it would result in the TOE application software updating to a different version of the TOE software, resulting in new binary executables.**<br>9. Calculate and save the hashes of the TOE files.<br>10. Compare the calculated hashes from the hashes_TOE_executables_before_execution.csv and hashes_TOE_executables_after_execution.csv files to confirm that the hash values for each file did not change. |
| **Test Results** | The calculated hash for each TOE executable did not change between the “before” and “after” execution of the TOE . -Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 024 |
| **SFR** | FPT_TUD_EXT.2.1 – TD0628 |
| **Test Objective** | If a container image is claimed the evaluator shall verify that application updates are distributed as container images.<br>If the format of the platform-supported package manager is claimed, |

| | |
|---|---|
| | the evaluator shall verify that application updates are distributed in the format supported by the platform. This varies per platform:<br><br>**For Windows:** The evaluator shall ensure that the application is packaged in the standard Windows Installer (.MSI) format, the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process, or the Windows Universal Application package (.APPX) format. See https://msdn.microsoft.com/en-us/library/ms537364(v=vs.85).aspx for details regarding Authenticode signing.<br><br>NOTE: An .APPX file is nothing more than a .zip file. SailPoint  saves the .APPX formatted zip file with a .wbxpkg suffix. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Open each TOE installer file (ServerInstaller.msi and ClientInstaller_x64.msi) in a hex editor.<br>2. Verify that the following byte sequence (.msi file signature) occurs at the beginning of each file:<br>`D0 CF 11 E0 A1 B1 1A E1`<br>3. Open the update package File_Access_Manager_v8.3.0.5000.wbxpkg in a hex editor.<br>4. Verify that the following byte sequence occurs at the begin of the update package:<br>`50 4b 03 04`<br>5. Rename the File_Access_Manager_v8.3.0.5000.wbxpkg to add a .zip extension.<br>6. Open the .zip file<br>7. Verify that there is an AppxSignature.p7x file within package.<br>8. Right click on filename and select properties and then the Digital Signature Tab.<br>9. Verify that the SailPoint Technologies Inc is the name of the signer. |
| **Test Results** | The TOE installer files (ServerInstaller.msi and ClientInstaller_x64.msi) contain the .msi file signature byte sequence.<br><br>The TOE update files (Service Pack 5: File_Access_Manager_v8.3.0.5000.wbxpkg) contained the .APPX (.zip) file signature byte sequence and the AppxSignature.p7x file. The signature file had SailPoint Technologies Inc as the name of the signer. -Pass |
| **Execution Method** | Manual |

| | |
|---|---|
| **Test Case Number** | 025 |
| **SFR** | FPT_TUD_EXT.2.2 – TD0664 |
| **Test Objective** | **For All Other Platforms:** The evaluator shall record the path of every file on the entire filesystem prior to installation of the application, and then install and run the application. Afterwards, the evaluator shall then uninstall the application, and compare the resulting filesystem to the initial record to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Ensure the TOE is not installed on the system.<br>2. Execute the command on the system via an Administrator Command Prompt to inventory the file system.<br>3. Install the TOE on the system.<br>4. Launch the TOE application.<br>5. Uninstall the TOE application. |

| | |
|---|---|
| | 6. Execute the command on the system via an Administrator Command Prompt to inventory the file system.<br>7. Examine the two filesystem output files for differences between the filesystem before the installation of the TOE and after the uninstallation of the TOE to verify that no files, other than configuration, output and audit/log files have been added to the filesystem. |
| **Test Results** | No files, other than configuration, output, and audit/log files were left on the file system. -Pass |
| **Execution Method** | Manual |

| **Test Case Number** | 026 |
|---|---|
| **SFR** | FPT_LIB_EXT.1.1 |
| **Test Objective** | The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Execute the command in a PowerShell window to survey the installation directories for third-party dynamic libraries.<br>2. Verify that only the third-party libraries returned from the command executed in Step 1 are listed in the Security Target. |
| **Test Results** | Only the documented third-party libraries were returned from the command executed in Step 1. -Pass |
| **Execution Method** | Manual |

| **Test Case Number** | 027 |
|---|---|
| **SFR** | FPT_IDV_EXT.1.1 |
| **Test Objective** | The evaluator shall install the application, then check for the / existence of version information. If SWID tags is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | The TOE does not use SWID tags. Refer to FPT_TUD_EXT.1.2 – Test Case 022 for querying the version of the TOE application. |
| **Test Results** | Pass |
| **Execution Method** | Manual |

### 4.3.6 Trusted Path/Channels

| **Test Case Number** | 028 |
|---|---|
| **SFR** | FTP_DIT_EXT.1.1 |
| **Test Objective** | The evaluator shall perform the following tests.<br>**Test 1:** The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Begin capturing packets on the server running the TOE application.<br>2. Exercise the TOE application to stimulate connections to the following remote systems: |

| | |
|---|---|
| | a. From the Windows File Server (Activity Monitor) machine, perform file system read/write activities on the host.<br>3. Stop capturing packets on the server running the TOE application.<br>4. Inspect the packet capture and verify that the traffic is encrypted with TLS for the TOE to remote Activity Monitor server channels. |
| **Test Results** | The communication channels were found to be encrypted with TLS. -Pass |
| **Execution Method** | Manual |

| **Test Case Number** | 029 |
|---|---|
| **SFR** | FTP_DIT_EXT.1.1 |
| **Test Objective** | The evaluator shall perform the following tests.<br>**Test 2:** The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | This is tested as part of FTP_DIT_EXT.1.1 – Test Case 028. |
| **Test Results** | No sensitive data was transmitted in the clear as the data was encrypted with TLS. - Pass |
| **Execution Method** | Manual |

| **Test Case Number** | 030 |
|---|---|
| **SFR** | FTP_DIT_EXT.1.1 |
| **Test Objective** | The evaluator shall perform the following tests.<br>**Test 3:** The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found. |
| **Test Instructions** | Execute this test per the test steps. |
| **Test Steps** | 1. Inspect the TSS to determine if user credentials are transmitted.<br>2. Specify and/or identify the TOE fat client password: [REDACTED]<br>3. Capture packets from the TOE application.<br>4. Authenticate to the TOE fat client.<br>5. Stop capturing packets from the TOE application.<br>6. Perform a string search for "[REDACTED]" and verify that no results are returned. |
| **Test Results** | The search for the password returned no results. -Pass |
| **Execution Method** | Manual |

# 5 Evaluation Activities for SARs

This section addresses assurance activities that are defined in the *Protection Profile for Application Software Version 1.4* [APP_PP] that correspond with Security Assurance Requirements.

**ADV_FSP.1** – *"There are no specific evaluation activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5.1 Security Functional Requirements, and other activities described for*

*AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other evaluation activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided."*

A separate functional specification was not provided by the vendor; instead, the relevant information is Section 1.3 of the ST. This section provides a labeled figure of the TOE interfaces and describes the purpose and method of use for each security relevant TSFI by enumerating all security relevant interfaces, including those used for remote administration of the TOE and where the TOE communicates with an external IT entity in the operational environment.

The evaluation team reviewed the ST and found that it describes the following security relevant interfaces:

The TOE has the following external interfaces:

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

The purpose of each TSFI is understood based on the descriptions presented in the ST. In addition to this, the mapping between logical TSFIs and physical interfaces to the application are consistent with the evaluation team's understanding of what each TSFI is used for. Therefore, this evaluation activity is considered satisfied.

**AGD_OPE.1** – *"Some of the contents of the operational guidance will be verified by the evaluation activities in Section 5.1 Security Functional Requirements and evaluation of the TOE according to the [CEM]. The following additional information is also required.*

*If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.*

Section 6.2 clearly states that the TOE invokes the OS for all cryptographic operations: The TOE invokes the underlying Windows platform to perform all cryptographic services including DRBG functionality, TLS/HTTPS trusted communications, and sensitive data encryption storage.

*The documentation must describe the process for verifying updates to the TOE by verifying a digital signature – this may be done by the TOE or the underlying platform.*

*The evaluator shall verify that this process includes the following steps:*

- *Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).*

- *Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities."*

Section 7.3 of the AGD "Secure Updates" provides instruction on performing trusted updates. The description includes how and when the update is digital signed, obtaining the update from vendor portal, who can and how to initiate an update, when the signature is validated by the TOE during the installation process, result in failure of installation if digital signature is found to be invalid, and how the version is displayed after successful installation. The description clearly indicates that the administrator function of initiating the update is after the package has been placed on the TOE host system. Based on the detailed description, this evaluation activity is considered satisfied.

Additionally, Section 2 of the AGD "Intended Audience: describes the scope of the evaluation and what functionality is and is not covered. The AGD states that, "The FAM product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the SailPoint File Access Manager 8.3 SP5 Security Target was not evaluated and should be exercised at the user's risk."

This evaluation activity is considered satisfied as all of the required descriptions were found in the AGD.

**AGD_PRE.1** – *"As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST."*

The AGD document covers the installation and configuration of the TOE application on the Windows Server 2019 (version 1809) platform in Section 5.1. This is the only platform the TOE was tested and the ST claimed. Based on the agreement of platforms being defined in the AGD and ST this activity is considered satisfied.

**ALC_CMC.1** – *"The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product."*

The evaluation team verified that the Security Target (ST), TOE, and Supplemental Administrative Guidance (AGD) were labeled consistently to correctly identify the operational environment and TOE software versions in the CC evaluation.

Section 1.2 of the ST states in the TOE Reference that, "the TOE is SailPoint File Access Manager (FAM) 8.3 SP5, which is an application on an operating system." Section 5.1 of the AGD states that the TOE is the SailPoint File Access Manager (FAM) 8.3 SP5, that includes the TOE components described in Table 1 of the AGD. Table 1 of the AGD lists the TOE components, which matches the TOE components listed in Section 2.1 of the ST. Finally, the product web site, https://www.sailpoint.com/solutions/file-access-manager, contains identifying product information including datasheets and a description of "File Access Manager." The ST states in the TOE Overview that, "the TOE is the SailPoint File Access Manager (FAM) version 8.3 SP5 application, referred to as FAM or TOE from this point forward. FAM's primary functionality is to allow its users to review and manage the governed data created by FAM for monitoring 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 understand which enterprise users have access to the data. 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."

All of this information as stated above provides sufficient context to accurately identify the TOE as such in the ST, AGD, and vendor web site. Therefore, this evaluation activity is considered satisfied.

**ALC_CMS.1** – *"The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the evaluation activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in-depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation.*

*The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification."*

The evaluation team confirmed the TOE had a unique identifier under ALC_CMC.1, which is the SailPoint File Access Manager (FAM) version 8.3 SP5. This included a review of the TSF vendor's website to determine that the identifier was enough to distinguish the TOE from other products from the TSF vendor. The evaluation team also reviewed the following documentation provided by the vendor and confirmed that this identifier was consistently used to reference the TOE:

- SailPoint File Access Manager 8.3 SP5 Security Target, Version 1.0
- SailPoint File Access Manager 8.3 SP5 Supplemental Administrative Guidance for Common Criteria, Version 1.0
- SailPoint File Access Manager Administrator Guide, Version 8.3
- SailPoint File Access Manager Installation Guide, Version 8.3 SP5

Section 8.5.1 of the TSS in the ST states that during the compilation of the TOE's software, the /NXCOMPAT flag is set to ensure that Data Execution Prevention (DEP) protections are enabled. The TOE's software runs as Managed Code in the .NET framework, and therefore no additional stack-based buffer overflow protection needs to be enabled. The TOE will operate on Windows Server 2019 with the security features of Windows Defender Exploit Guard Exploit Protection configured on, with the following enabled: Control Flow Guard (CFG), randomize memory allocations (Bottom-Up ASLR), Export Address Filtering (EAF), Import Address Filtering (IAF), and DEP. The TOE also does not allocate any memory region with both write and execute permissions or write user-modifiable files to directories that contain executable files. This ensures that protections are enabled against vulnerabilities, therefore the evaluation team has determined this evaluation activity has been satisfied.

**ALC_TSU_EXT.1 –** *"The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the*

*TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described."*

The evaluator examined Section 8.5.5.1 of the ST that SailPoint has defined a Product Vulnerability Management Policy for their operations which applies to all of their product lines, including the entire FAM product. SailPoint continuously performs security assessments of FAM for vulnerabilities by performing internal testing as well as contracting third party security verification organizations.

*"The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days."*

Section 8.5.5.1 of the ST clearly states when a potential vulnerability is discovered or reported, SailPoint will perform an internal verification to confirm that a vulnerability is present in FAM. SailPoint will then develop a mitigation to address the vulnerability which can either be a configuration change to FAM or the development of a software update package. The mitigation will be relayed to customers by providing a security notification on the SailPoint support site along with information regarding the mitigation. SailPoint's support team also provide their customers emails which can contain updates regarding security notifications. Mitigations which require configuration changes to FAM will have the steps defined within the security notification. Mitigations which require software updates will result in a software update package being created and released.

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

*"The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website."*

Section 8.5.5.1 of the ST describes that customers can report security issues by opening a support case through SailPoint's support website: https://support.sailpoint.com/. The support website is protected with HTTPS and requires customers to enter their email address and password associated with their SailPoint customer account.

The evaluator has determined that the TSS demonstrates that the vendor's timely security update process is sufficient to create and deploy updates, provide vulnerability updates in a timely manner, and provide a mechanism to report security issues. In conclusion, these evaluation activities have been satisfied.

**ATE_IND.1** – *"The evaluator shall prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. The test plan covers all of the testing actions contained in the [CEM] and the body of this PP's evaluation activities.*

*While it is not necessary to have one test case per test listed in an evaluation activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no effect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is* *necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform.*

*This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (e.g SSH). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results.*

*The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result."*

The evaluation team created a Detailed Test Report (DTR) to address all aspects of this requirement. The DTR is made up of the proprietary *SailPoint File Access Manager 8.3 SP5 Test Plan* and the *Proprietary_SailPoint_FAM_AppPPv1.4_Test_Matrix.xlsx.* The DTR discusses the test facility, environment, configuration, test tools, equivalency argument, test cases, test procedures, expected results, identification of evidence collected, and analysis of test results. The evaluator's test environment diagram is located in section entitled Test Environment of *SailPoint File Access Manager 8.3 SP5 Test Plan* document. Section 4 of this document presents a public releasable summary of the testing activity per SFR accomplished during testing. Therefore, this assurance activity is considered satisfied.

**AVA_VAN.1 –** *"The evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses.*

*The evaluator documents the sources consulted and the vulnerabilities found in the report.*

*For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.*

***For Windows, Linux, macOS and Solaris:*** *The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious."*

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:

| 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. |

| Keyword | Description |
|---|---|
| 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. |
| Third-Party Libraries | Third party libraries listed in the ST for FPT_LIB_EXT.1 |

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
e) SecurITeam Exploit Search: www.securiteam.com
f) Tenable Network Security http://nessus.org/plugins/index.php?view=search
g) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
h) Offensive Security Exploit Database: https://www.exploit-db.com/
i) Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

A public vulnerability search was also conducted on the vendor provided third-party libraries list. The Library search conducted only used the NVD, CVE, Tipping Point, Zero Day database.

Upon the completion of the vulnerability analysis research, the team identified that IND testing had sufficiently tested most areas of concern. These areas included port scan, protocol analysis, ASLR use, full disk encryption, and access (permissions). All but malicious binary was covered.

Therefore, the team tested the following areas:

- Virus/Malware Scan
  - Perform a virus scan on software as required by the App PP assurance activity requirements.

NOTE: During the evaluation, the TOE was updated to 8.3.0 SP5 as a result of SailPoint self-reporting vulnerabilities on features and functions that are outside the scope of the evaluated functionality. The lab performed an impact analyses and found that there were no impactful changes to any NDcPP testing that had been performed. It was determined that 8.3.0 and 8.3.0 SP5 are functionally equivalent. Despite this finding, the lab still performed regression testing on administrative functions to ensure that the non-SFR related functions did not impact the SFR related functions, as well as network tests, and the update tests.

The evaluation team determined that no residual vulnerabilities exist, with the updated version, that are exploitable by attackers with Basic Attack Potential. Therefore, this assurance activity is considered satisfied.

# 6 Conclusions

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The overall verdict for this evaluation is: Pass.

# 7 Glossary of Terms

| Acronym | Definition |
|---|---|
| **AA** | Assurance Activity |
| **API** | Application Programing Interface |

| | |
|---|---|
| **ASLR** | Address Space Layout Randomization |
| **CA** | Certification Authority |
| **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 |
| **EKU** | extendedKeyUsage |
| **FAM** | File Access Manager |
| **gRPC** | grpc Remote Procedure Call |
| **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 |
| **OCSP** | Online Certificate Status 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 |

**Table 7-1: Acronyms**

| 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. |

**Table 7-2: Terminology**