SailPoint IdentityIQ File Access Manager 8.1

Supplemental Administrative Guidance for Common Criteria

Version 1.0
October 21, 2020

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

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

Table of Tables

1 Introduction

The SailPoint IdentityIQ File Access Manager (FAM) 8.1 (TOE) is a software application that is installed on an operating system (OS). The Protection Profile for Application Software Version 1.3 (APP_PP) defines an application as "software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation."

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating SailPoint IdentityIQ FAM 8.1. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the Security Target for SailPoint IdentityIQ File Access Manager 8.1 and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs. The IdentityIQ 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 IdentityIQ File Access Manager 8.1 Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the SailPoint IdentityIQ File Access Manager 8.1 Security Target.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the IdentityIQ FAM product that contain the security functions that were tested as part of the CC evaluation process.

Administrator: An administrator is an individual who has permissions to modify the behavior of the TOE. This includes the individual that installs it on the underlying platform but can also include other individuals if administrator access is granted to them on the TOE's GUI or fat client.

Fat client: The portion of the TOE which allows local authentication to and administration of the TOE.

Governed Data: The data created by the IdentityIQ File Access Manager product for its primary functionality that is an abstract of information gathered from a managed resource, for example, file names and data-type tags.

GUI: The GUI is a web-based interface of the TOE that can be used to manage the TOE remotely using HTTPS.

Managed Resource: Remote system which the IdentityIQ File Access Manager product monitors to create governed data for its primary functionality.

User: An individual who has access to the TOE but is not able to manage its behavior.

4 References

The following security-relevant documents are included with the TOE. This is part of the standard documentation set that is provided with the product. Documentation that is not related to the functionality tested as part of the CC evaluation is not listed here.

[1] SailPoint IdentityIQ File Access Manager Administrator Guide, Version 8.1
[2] SailPoint IdentityIQ File Access Manager Installation Guide, Version 8.1

The following document was created in support of the IdentityIQ FAM CC evaluation:

[3] SailPoint IdentityIQ File Access Manager 8.1 Security Target, v1.0

The following document is provided by SailPoint but is for the Activity Monitor which is an operational environment component. This documentation is referenced for completeness of configuration but since the Activity Monitor is not part of the TOE, this document is not considered security-relevant.

[4] SailPoint IdentityIQ File Access Manager Windows Connector Installation Guide, Version 8.1

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims:

5.1 TOE Components

The TOE is SailPoint IdentityIQ File Access Manager (FAM) version 8.1, which is an application on an operating system. The TOE is installed on a Windows Server 2019 and utilizes several functions of the operating system to perform its operations.

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

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

Table 1: Evaluated Components of the TOE

5.2 Supporting Environmental Components

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

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

Table 2: Components of the Operational Environment

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

Table 3: Requirements for Operational Environment Components

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Platform:** The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- **Proper administrator:** The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance of the applied enterprise security policy.
- **Proper user:** The user of the application software is not willfully negligent or hostile and uses the software in compliance with the applied enterprise security policy.

6 Secure Installation and Configuration

Documentation for how to order and acquire the TOE is described under the Contact link on the SailPoint website www.sailpoint.com. Section 5.1 of this document lists the properties that are associated with the TOE. When downloading the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the software application can be verified.

Installation and first-time setup of the TOE can be accomplished by following the steps outlined below which use procedures found in [2]. The steps below will specify any options required for the CC evaluation.

TOE Installation Procedures

1. Complete all procedures under "Server Installation" in **Chapter 5: IdentityIQ File Access Manager Installation**.
2. Complete all procedures under "Creating a Database (through the Installer)" in **Chapter 5: IdentityIQ File Access Manager Installation**.
3. Complete all procedures under "Adding a Server" under "Creating the Configuration" in **Chapter 5: IdentityIQ File Access Manager Installation** and note that for procedure 2(g), do not check "Disaster Recovery" server type.
4. The procedures under "Services Configuration" and "Performing the Installation" in **Chapter 5: IdentityIQ File Access Manager Installation** have been simplified to the following steps:
    a. Specify the default selections, with the exception of the following changes:
        i. Specify the Elasticsearch Database Path as C:\Program Files\elastic_data.
        ii. Check "Central Data Classification".
            1. Specify "Service Name" → dc1
        iii. Check "Central Permissions Collection".
            1. Specify "Service Name" → pc1
    b. Click "Next".
    c. Choose "Save Configuration and Perform current Server's Installation Tasks".
    d. Click "Next".

5. Complete all procedures under **Chapter 6: IdentityIQ File Access Manager Website SSL**.
    a. After procedure 7 and before procedure 8, click on the http/80 binding.
    b. Click “Remove”.
    c. Continue with procedure 8.
6. Complete all procedures under **Chapter 7: Administrative Client Installation**.
7. Once installation is completed, launch the File Access Manager client (fat client).
8. Click “Yes, Let’s get started”.
9. Click “OK”.
10. Click “Next”.
11. Configure the Authentication Store Connection by specifying the Active Directory details.
    a. Specify the Domain DNS name, Domain NetBios, Port, and check “SSL”.
    b. Specify the Username, Password, and then click “Synchronize Domains”.
    c. Click “Test” then “Save”.
    d. Click “Next” and then “Finish”.
12. Click “New” > “Application”.
13. Specify Application Type → “Windows File Server (Agent) and then click “Next”.
14. Specify the General Details fields.
    a. Click on “Create new Container” and specify its name.
    b. Specify the Identity Collector.
15. Click “Next”.
16. Specify the Configuration.
    a. Specify the Central Permission Collection Service.
    b. Check “Enable Data Classification”.
    c. Specify the Central Data Classification Service.
17. Click “Next”.
18. Specify the Configuration.
    a. Specify the “Excluded Users” to include “Local System”.
19. Click “Next”.
20. Specify the Data Enrichment Connector from the Available list to the Current list.
21. Click “Next”.
22. Specify the Permission Collector Scheduling.
    a. Check “Create a Schedule?”.
    b. Specify the Name and Schedule fields.
23. Click “Next”.
24. Specify the Crawler.
    a. Check “Create a Schedule?”.
    b. Specify the Name and Schedule fields.
25. Click “Next”.
26. Specify the Data Classification.
    a. Check “Create a Schedule?”.
    b. Specify the Name and Schedule fields.
    c. Check “Active?”.
27. Click “Next”.
28. Skip “Access Fulfillment” and click “Next”.
29. Click “Finish”.

Configure the TOE (fat client) to use Active Directory authentication

30. Through the fat client, click "Configuration" > "Manage File Access Manager Permissions" > "Users".
31. Click "New".
    a. Specify the Active Directory username and click "Is AD User?".
    b. Assign all the available roles to the user.
    c. Click "Save".

Activity Monitor Installation

NOTE: The steps below are those that are required to configure the Activity Monitor for its use with the TOE. Additional information on configuring the Activity Monitor for IdentityIQ FAM's primary purpose can be found within [4] but this functionality was not assessed as part of the CC evaluation.

32. On the Activity Monitor server, launch the "Collector Installation Manager" installer.
33. Specify the parameters to connect to IdentityIQ File Access Manager.
34. Click "OK" on the Unknown server information dialog box.
35. Specify the Application and click "Add" and then click "Next".
36. Once installation completes click "Exit".

Secure Configuration

37. Complete all procedures under "Post Installation Configuration" in **Chapter 8: Recommended Secured Deployment**.

NOTE: The administrator must restart all the TOE's services or reboot the server for the secure configuration procedures to take effect.

NOTE: Due to C:\Program Files being the installation directory, the Windows platform will protect the TOE's binaries and data files from modification by unprivileged users. No further configuration is needed.

6.1 Query the Installed Version of the TOE

The software version of the TOE is always displayed after the administrator authenticates to the TOE via the fat client. Post installation or software update, the administrator will need to verify that the TOE version installed was the version expected. This is accomplished by performing the following steps:

1. From the local machine where the TOE is installed, launch the TOE fat client.
2. Authenticate to the TOE fat client.
3. Observe the client version output in the lower right corner of the TOE fat client and verify this is the expected version of the TOE.

6.2 Cryptographic Configuration Notice

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 administrator installing the TOE is expected to perform all of the operations in Section 6 of this document to configure the underlying Windows platform's cryptographic services.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

7 Secure Management of the TOE

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. Note that this information is largely derived from [1] but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the IdentityIQ FAM product, including functions that may be beyond the scope of this evaluation.

7.1 Access to Platform Resources

During operation of the TOE, access to the underlying Windows platform is limited to use of network connectivity hardware for communication with web browsers for GUI access, the SQL database, the LDAP server(s), and Activity Monitor application(s). The network connectivity is required for the TOE security functions and the primary purpose of the IdentityIQ FAM product. Additional information regarding these communications can be found in [1] under "Inter-service Communication" in **Chapter 2: Application Capabilities and Architecture**.

The TOE does not access any sensitive data repository provided by the underlying Windows platform.

7.2 User Management

Configuration of the LDAP server(s) to which the TOE will communicate via the fat client

Performing this management function has been described in Section 6 of this document under Configure the TOE (fat client) to use Active Directory authentication.

Perform tasks that read data from LDAP server(s) via the fat client

This management function is accomplished by launching the fat client and having the administrator enter their username and password which correspond to an Active Directory user account.

Perform tasks that read data from LDAP server(s) via the GUI

1. Authenticate to the TOE via the GUI.
2. Navigate to "Settings" > "Task Management" > "Tasks".
3. Check "Synchronize Identity Collector" and choose "Re-run".

Perform tasks that read or write data (i.e. configuration data) to the SQL database via the fat client

Performing this management function has been described in Section 6 of this document under Configure the TOE (fat client) to use Active Directory authentication.

Perform tasks that read or write data (i.e. governed data) to the SQL database via the GUI

1. Authenticate to the TOE via the GUI.
2. Navigate to "Settings" > "Task Management" > "Tasks".
3. Check "Synchronize Identity Collector" and choose "Re-run".

Query the current version of the TOE via the fat client

Performing this management function has been described in Section 6.1 of this document.

Perform the software update process via the fat client

Performing this management function has been described in Section 7.3 of this document.

7.3 Secure Updates

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

Each customer that is entitled to the TOE software has a username and password for accessing the SailPoint customer portal. Connections to the SailPoint customer portal are protected using HTTPS. SailPoint's customer portal contains a full list of all versions of the product that are currently still supported. The TOE administrator downloads the software installation package or software update package from SailPoint's customer portal.

Software update packages are in the Windows Universal Application package (.APPX) format. During the build process, SailPoint digitally signs a software update package using their private key and their certificate signed by DigiCert. Once a software update package is on the system where the TOE is installed, any administrator account with permission to the 'Start Installation' button via the fat client can initiate the update process following the steps below:

1. From the local machine where the TOE is installed, launch the TOE fat client.
2. Authenticate to the TOE fat client.
3. Choose "Upgrades & Patches".
4. Choose "Load New Package".
5. Select the software update package file.
6. Choose "Upload Package".
    a. During this step, the fat client will request the platform to validate the certificate using the public key from DigiCert that is already loaded on the platform and verifies the digital signature on the software update package using the public key in the certificate. If signature validation is successful, the remaining update steps can be performed, and the administrator can click the 'Start Installation' button to initiate the update. If the validation of the digital signature fails, the remaining update steps cannot be performed, an error will be generated and the 'Start Installation' button will not be displayed.
7. After the package has finished uploading, click "Save".
8. Double click on the available update package.
9. Click the "Start Installation" button.
10. Confirm the installation by choosing "Yes".
11. Periodically choose "Refresh" to query the status of the update.
12. Once the update has finished, close the TOE fat client.
13. Launch the TOE fat client.
14. At the prompt to update the TOE, choose "Yes".
15. Follow the installer wizard to complete the installation of the TOE software update.

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.

The software version of the TOE is always displayed after the administrator authenticates to the TOE via the fat client. Refer to Section 6.1 of this document for verifying the current version of the TOE after an update is performed.

7.4 Uninstall IdentityIQ FAM

The TOE's uninstallation process results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events. The administrator will execute the uninstall through the TOE's installers which will stop and remove all services and will then begin removing files related to the application. The administrator will then use the platform's uninstall application program to complete the TOE's uninstall. The steps for uninstalling the TOE can be found in [2] under **Chapter 10: Uninstalling IdentityIQ File Access Manager**.

8 Operational Modes

The TOE does not have operational modes. When the TOE is first installed, it is considered to be in its evaluated operational mode, provided the steps in Section 6 of this document have been accomplished. Once these steps have been completed, the TOE is considered to be in its operational mode and configured to perform the security functions as described in the Security Target.

There is no separate error mode or other degraded mode of operation. If IdentityIQ FAM fails, the admin will need to restart all the TOE's services or the host platform will need to be rebooted. If the TOE has been corrupted or the application has failed such that restarting the service and rebooting will not resolve the issue, an administrator will need to contact SailPoint support per the guidance in Section 9.

9 Additional Support

SailPoint provides technical support for its products through their 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.