SailPoint IdentityIQ v8.0
Supplemental Administrative Guidance

Version: 1.0
April 16, 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

Contents

Table of Tables

1 Introduction

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

IdentityIQ is a software application that is used to associate an organization's computer system users with role and privilege information based on their position within the organization. This concept of correlating the attributes of an individual with permissions assigned to their account(s) on IT resources can be understood as identity management.

The evaluated configuration of IdentityIQ includes licenses for both the Compliance Manager and Lifecycle Manager portions of IdentityIQ.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating IdentityIQ version 8.0. 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 expected to be familiar with the Security Target for IdentityIQ version 8.0 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.

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 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 IdentityIQ that contain the security functions that were tested as part of the CC evaluation process.

4 References

The following documents are part of the IdentityIQ version 8.0 bookshelf. This is the standard documentation set that is provided with the product.

[1] SailPoint IdentityIQ Administration Guide version 8.0

[2] SailPoint IdentityIQ User's Guide version 8.0

[3] SailPoint IdentityIQ Direct Connectors Administration and Configuration Guide version 8.0

[4] SailPoint IdentityIQ Installation Guide version 8.0

[5] SailPoint_IdentityIQ_Capabilities.xls

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

[6] SailPoint IdentityIQ Common Criteria Security Target

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:

TOE Components

Component	Definition
IdentityIQ	The identity and credential management software application. The evaluated configuration of IdentityIQ includes licenses for both the Compliance Manager and Lifecycle Manager portions of IdentityIQ.

Table 5-1: TOE Components

Supporting Environmental Components

Component	Definition
Active Directory	Stores enterprise user data and policies for the operational environment. Also serves as an authentication store for the TOE.
Application Server	Apache Tomcat application server that is used to host the IdentityIQ software as well as the GUI.
Database	Stores a variety of configuration, operation, and audit data for the TOE. In the evaluated configuration, the TOE will use Oracle 18c for its database. The connection to the database is required in order for the TOE to function.
Server	Physical system on which the IdentityIQ software is installed. The physical system is comprised of a Microsoft Windows Server 2016 OS, Microsoft .NET Framework, Apache Tomcat Application Server and JRE.
Web Browser	The interface that is used to access the IdentityIQ Web GUI. In the evaluated configuration the GUI will be managed via Chrome, version 76.

Table 5-2: Supporting Environmental Components

6 Secure Installation and Configuration

SailPoint IdentityIQ Installation Guide [4] includes procedures for downloading the installation files directly from SailPoint. Once a customer purchases the IdentityIQ product, they are given access to the "community.sailpoint.com" site in which they are able to download the product. This download is secured using a HTTPS connection from the site.

NOTE: It is assumed that IdentityIQ is installed on hardware that is located in a secure area to prevent malicious tampering. All Administrators of IdentityIQ are considered trusted personnel and should receive proper training in order to operate the product in a secure and responsible manner.

SailPoint IdentityIQ Installation Guide [4] provides step by step instructions for installation and deployment of IdentityIQ.

NOTE: The communications described below must be secured using TLS in the evaluated configuration. IdentityIQ does not provide any cryptographic functions and is dependent on the Operational Environment to provide these services.

SailPoint communicates with remote Administrators and 3rd party ESM products via trusted paths and channels. IdentityIQ uses Apache Tomcat for secure communications to Administrators via the GUI. IdentityIQ uses connectors to be able to read/write data to 3rd party ESM products securely. SailPoint IdentityIQ Direct Connectors Administration and Configuration Guide version 8.0 [3] provides the instructions to configure IdentityIQ to use these connectors. Depending on what product IdentityIQ is communicating with, determines which configuration is needed. In the evaluated configuration, IdentityIQ reads/writes data to two instances of Active Directory. One instance uses the ADSI connector and the other uses a JNDI connector. IdentityIQ also reads/writes data to an Oracle 18c database using the JDBC connector. The connectors that are discussed are provided by the underlying Operational Environment and are not included in the scope of this evaluation.

The following actions must be performed to secure these communications in the evaluated configuration. For additional information regarding these steps, please refer to the Operational Environment component's guidance documentation.

Apache Tomcat:

1. Add a signed certificate to a keystore
2. Modify the Apache Tomcat's server.xml file by performing the following actions:
    a. Add the keystore location and password
    b. Specify the TLS port 8443 for HTTPS communication
    c. Comment out the non-TLS port to prevent non-TLS access

NOTE: The default setting for Apache Tomcat is to use port 8080 for all requests. An enterprise administrator must configure Apache Tomcat 9.0 to redirect any request to port 8443 in order to invoke HTTPS using OpenSSL.

JRE:

1. Set the Unlimited Strength Policy (By default, this setting is already configured in JDK 11. If it is not, follow the instructions below.)

a. Set the unlimited policy in the <jre_home>/lib/security/java.security file.
b. Search for the #crypto.policy=unlimited and remove the # character to uncomment it.

NOTE: The vendor recommends updating all drivers in order to ensure encrypted communications.

.NET Framework:

The desired libraries are used by default, no additional configuration is necessary.

Active Directory TLS communication:

1. Generate signed certificates on the Domain using MMC (Note: For an existing environment using Active Directory this activity has likely already occurred and this action will not need to be performed)
2. Copy the signed Active Directory certificate to the servers running IdentityIQ and IQService
3. Import the certificate into the JDK keystore on the server hosting IdentityIQ
4. Imported the certificate using MMC on the server(s) hosting the IQService (in the evaluated configuration this will be the same server(s) as the Active Directory Domain Controller instances being managed by IdentityIQ)
5. Enable Use SSL flag on your Active Directory application in IdentityIQ

Oracle database TLS communication:

1. Generate signed certificates on the server using Oracle Wallet (Note: For an existing environment using Oracle database this activity has likely already occurred and this action will not need to be performed)
2. Copy the signed Oracle database certificate to the server running IdentityIQ
3. Import the certificate into the JDK keystore
4. Configure iiq.properties to use a TLS database URL for the connection

6.1 Evaluated Configuration

6.1.1 Connectors

SailPoint communicates with 3rd party ESM products via trusted channels and paths. IdentityIQ uses connectors to be able to read/write data to these products. SailPoint IdentityIQ Direct Connectors Administration and Configuration Guide version 8.0 [3] provides the instructions to configure IdentityIQ to use these connectors. Depending on what product IdentityIQ is communicating with, determines which configuration is needed. In the evaluated configuration, IdentityIQ reads/writes data to two instances of Active Directory. The connector used by IdentityIQ depends on the action being performed; the ADSI connector is used for compliance or provisioning events and the JNDI connector is used for IdentityIQ authentication requests. IdentityIQ also reads/writes data to an Oracle 18c database using the JDBC connector. The connectors that are discussed are provided by the underlying Operational Environment and are not included in the scope of this evaluation.

NOTE: The communications described above are secured using TLS. IdentityIQ does not provide any cryptographic functions and is dependent on the Operational Environment to provide these services.

6.1.2 Password Policy

In order to meet the requirements for FIA_SOS.1, an Administrator must configure the password policy in IdentityIQ. By default, the special characters that are allowable in the password policy do not meet the requirement. Chapter 35 in the SailPoint IdentityIQ Administration Guide version 8.0 [1] discusses the procedures to change the password policy for users of the TOE to meet the requirements. Section 7.4.1 of this document discusses more about the specific requirements of the password policy.

6.1.3 Generating Encryption Key

By default, IdentityIQ contains a hard-coded encryption key that it supplies to the JRE for encryption of user passwords before it sends them to the database. In the evaluated configuration, this key will not be used. A new key must be generated and stored in the OE's keystore. First, set the keystore to an alternate location by editing the "iiq.properties" file. Uncomment the keyStore.file and keyStore.passwordFile parameters and set them equal to the path of the location of the new keystore that was set in the "iiq properties" file as described in the previous step. Next, to generate a new encryption key, run iiq console with the keystore command. To do this, navigate to the WEB-INF/bin folder and issue the following command: "iiq keystore". From here, issue the "addKey" command and select 'y' when asked to confirm. **NOTE:** This creates a key generation call to JRE. IdentityIQ does not perform any key generation. All application servers must be restarted for the change to take effect. Once this is done, IdentityIQ will automatically use the newly generated key for encrypting user passwords.

6.2 Aggregation of Data from Active Directory

In order for IdentityIQ to read data such as enterprise user information from the Active Directory, the IdentityIQ SYSAdmin must perform an Account Aggregation. This aggregation is performed as a Task. Chapter 19 in the IdentityIQ Administration Guide [1] describes each type of aggregation that can be performed. It also goes into detail of the different options when performing these tasks.

7 Secure Management of IdentityIQ

Table 6-3 in the SailPoint IdentityIQ Common Criteria Security Target [6] describes the management functions and the capability (role) that is able to perform them. All management functions described are performed using the Web GUI. In the evaluated configuration, the path for the management of the product is protected using HTTPS that is provided by the Operational Environments Apache Tomcat with OpenSSL module.

7.1 Authenticating to IdentityIQ

Users must authenticate to IdentityIQ in order to perform any management functions. Users must authenticate to IdentityIQ via Active Directory or the local data store that resides in the Oracle Database. When authenticating a user against the TOE's user store, the TOE will request the JRE to encrypt the user's password using AES-128 with Base64 encoding and will compare the user's username and

encrypted password against the values stored in the Oracle database. The Active Directory authentication is performed via an LDAP bind request which is secured using TLS over an environmental connection via JRE's JNDI.

1. After the TOE has been successfully installed, open Google Chrome v76 web browser and enter the correct URL. The URL may look something like this: https://localhost:8443/identityiq

2. The IdentityIQ login page will appear. Enter the default username and password.

   Username: spadmin

   Password: admin.

NOTE: The default password should be changed immediately after initial login.

Once a user authenticates to IdentityIQ, a user session is created in memory that contains the authenticated username, principal, and the capabilities, rights and dynamic scopes that are associated with the user's principal.

7.2 User Lockout

Pages 17-18 of the SailPoint IdentityIQ Administration Guide [1] discuss the authentication failure handling settings that includes, the number of times a user can attempt authentication before being locked out and number of minutes the user will be locked out.

1. In the Homepage, click on "Cog" symbol at the top right of the screen then select "Global Settings".
2. Select Login Configuration link on the left side of the page.
3. Under the Login Setting tab, click the check the Enable Authorization Lockout box.
4. Here the Admin can set:
   a. Number of Unsuccessful Login Attempts before Lockout. (Default=5).
   b. Number of Minutes a User will be locked out due to unsuccessful Login. (Default=60)
5. Click Save to save the changes that were made.

NOTE: Regardless of the Number of minutes a user will be locked out, a SYSAdmin or an Admin with the Help Desk capability may unlock an account at any time.

7.3 Managing Identities

7.3.1 Create/Edit/Query Identities

Chapter 32 of the SailPoint IdentityIQ User's Guide version 8.0 [2] discusses how to create, view, and modify identity and credential data.

Under the Manage Identity section of the Homepage, there are options to create, edit, and view identities.

To create a new identity in IdentityIQ, use the Create Identity tab. The data fields are based on the fields defined as standard and/or searchable attributes in the IdentityIQ configuration.

1. From the Homepage, under the "Manage Identity" section select "Create Identity".
2. Fill out the page with the user information.

NOTE: Username, First name, and Last name are required to be filled in.

3. Click submit to save the identity.

To edit identities, follow the same procedures, except click on "Edit Identity". Depending on the rights your Identity has, you may be able to edit the Identities of other users as well as your own.

NOTE: Only a SYSAdmin or the Manager of an Identity has the ability to delete an Identity.

1. From the Homepage, select "Identities" then from the menu select "Identity Warehouse" and select the Identity you would like to add/remove the capability.
2. Select the "User Rights" tab.
3. Choose which Capability you would like to add/remove. If multiple capabilities are desired, use the "Control" button to select more than one capability.

IdentityIQ will provision this data with the Operational Environment's Active Directory and/or Oracle Database immediately following creation or modification of data. These intervals can be set by the SYSAdmin by following the instructions below.

1. From the homepage, Click on the "Cog" symbol at the top right of the screen then select "Global Settings".
2. Scroll down to the "Lifecycle Manager" and select the "Identity Provisioning Policies" link.

To edit an account that is associated with the Identity, navigate to the Account Management tab. Here you can create, manage, and delete accounts. (Manage accounts include enabling, disabling and unlocking accounts). Refer to Chapter 32 of the SailPoint IdentityIQ User's Guide version 8.0 [2] for more information.

7.3.2 Assign/Remove Capabilities from Identities

IdentityIQ is a role-based product. The SYSAdmin and Role Admins are able to assign capabilities to users. Capabilities in IdentityIQ are synonymous with Common Criteria's definition of roles. SailPoint IdentityIQ Capabilities.xls [5] describes every out-of-the-box capability and the rights that are associated with those capabilities.

7.4 Password Management

Password Management for IdentityIQ and applications within the managed Operational Environment is discussed in detail within the IdentityIQ Administration Guide [1]. Chapter 34 specifically discusses application password management and Chapter 35 discusses IdentityIQ password management.

7.4.1 Password Policies

The chapters referenced above include implementing password policies and defining the special characters that are allowed to be used. However, in the evaluated configuration the following rules are used for password complexity:

1. Passwords can be composed of any subset of upper case and lower-case letters, numbers, and the following special characters !,@,#,$,%,^,&,*,(,).
2. The minimum password length is 16 characters.

The password policy also contains rules listed below:

1. Password history shall be set by an Administrator.
2. Passwords shall have a maximum lifetime. (Expiration)
3. Passwords shall have a mix of the characters listed above.

There is not a specific setting that these have to be configured as. However, it is required that these policies be configured. Follow the instructions in the chapters of the guidance listed above to configure these policies.

7.4.2 Changing Passwords

Depending on the password policies that are implemented, passwords can be changed by the user. Below are instructions for changing a password.

NOTE: This is required after the initial login of the Administrator.

1. Click the Identities --> Identity Warehouse.
2. Click on the username. In this case the username would be “spadmin”
3. Click change password to display the password information.
4. Change and confirm the password and click save.

7.5 Login Banner

IdentityIQ is able to show a banner on the login page prior to authentication. In order to be Common Criteria compliant, this banner must be configurable by the SYSAdmin. The login banner can be configured by the SYSAdmin by modifying the login.xhtml file.

The login.xhtml file is located outside of the IdentityIQ normal user interface. This file’s directory location is <sphome>/identityiq/login.xhtml. The login.xhtml file must be modified using an editor, Notepad++ is recommended. The code below should be added to the file in a location that does not modify the existing code and the recommended location is line 213.

```
<div style="border: 1px #CCCCCC solid; padding: 5px; margin: 20px auto 0 auto; color:
#037DA1; width: 475px; max-width: 475px; max-height: 80px; overflow-y: scroll;">
TEXT
</div>
```

The text between “div” will appear on the login page before authentication occurs.

7.6 Session Termination

7.6.1 Admin Logout

Any user/Administrator can terminate their own GUI session by simply clicking the logout button at the top left of the page. This will end the session and bring the user back to the login page.

7.6.2 Termination from Inactivity

IdentityIQ is configurable to timeout after inactivity. The SYSAdmin can configure the timeout value for inactivity of a user’s GUI session by modifying the “web.xml” file. Once this time limit is reached, IdentityIQ will logout of the user’s session and return to the login page.

The web.xml file is located outside of the IdentityIQ normal user interface. This file's directory location is <sphome>/identityiq/WEB-INF/web.xml. The web.xml file must be modified using an editor, Notepad++ is recommended. The portion of the "web.xml" file that needs to be modified is:

<session-config> <session-timeout>30</session-timeout></session-config>.

The timeout value is set in minutes and by default is set to 30 minutes. In the evaluated configuration, the timeout value must be set between 1 and 60 minutes.

8 Auditing

In order to be compliant with Common Criteria, IdentityIQ must audit the events in the table below. All of the management functions that will produce an audit record are performed via the Web GUI.

Administrators can configure what is audited by the following steps:

1. From the homepage, click on the "Cog" symbol at the top right of the screen then select "Global Settings".
2. Scroll down and click on "Audit Configuration"

This page contains tabs with actions that can be selected/deselected for auditing.

Table 8-1 below lists each auditable event required by the ESM_ICM Protection Profile as they apply to each Security Functional Requirement. The 'Additional Information' column of Table 8-1 includes a list of audit information required to be provided in the event's audit record addition to: date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Table 8-2 lists an example and description of each required audit event that IdentityIQ produces.

Component	Event	Additional Information
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_GEN.1	Start-up and shutdown of the audit functions	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached

FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	None
FIA_SOS.1	Identification of any changes to the defined quality metrics	The change made to the quality metric
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

Table 8-1: Auditable Events

Component	Audit Record Example(s)	Notes
ESM_EAU.2	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Login Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Login Failure Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname	This example shows a successful authentication for Example_User. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system
ESM_ICD.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Create Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname Application: IIQ Account Name: admin2 Attribute Value: name = 'admin2'; inactive = 'false	This example shows the record that is generated when a user account is created, which creates identity and credential data. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system Account Name – Subject Created/modified Attribute Value – Attributes that were modified
ESM_ICD.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Entitlement Added	This example shows the record that is generated when a user's account is

	Source: Example_User Application: Active Directory - XYZ Account Name: CN=Example_CN, OU=Example_OU, DC=Example_DC1, DC=Example_DC2, DC=Example_DC3 Attribute Name: memberOf Attribute Value: CN=Example_Group_Name, OU=Example_OU, DC=Example_DC1, DC=Example_DC2, DC=Example_DC3	modified to add an entitlement. Example_User is the user who added the entitlement. The values in Account Name determine which user account receives the entitlement. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Application – Destination of Transmission Account Name – Subject Created/modified Attribute Name – Type of attribute that was modified Attribute Value – Attributes that were modified
ESM_ICT.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: audit_action_PasswordsRequestStart Source: The Administrator Target: Example_User Application: Active Directory Name Account Name: CN=Example_CN, OU=Example_OU, DC=Example_DC1, DC=Example_DC2, DC=Example_DC3 Attribute Name: password	When data are transmitted to external entities, the destination can be represented in either the Account Name or Application fields. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Target – Subject created/modified Application – Destination of Transmission Account Name – Subject created/modified Attribute Name – Type of attribute that was modified
FAU_GEN.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: AuditConfigChange Source: Example_User Attribute Name: op Attribute Value: update Attributes: Access Request Started - From (enabled: true;) to (enabled: false;) Accounts Request Started - From (enabled: true;) to (enabled: false;) Allow Exception on Violation - From (enabled: true;) to (enabled: false;) Approve Line Item - From (enabled: true;) to (enabled: false;) Approve Work Item - From (enabled: true;) to (enabled: false;)	This example shows the shutdown of the auditing within IdentityIQ. The startup of auditing is the same format but will show the attributes "From (enabled:false) to (enabled:true)" Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Attribute Name –Attribute that was modified Attribute Value – Identifies type of action made to attribute Attributes – Changes that were made
FAU_STG_EXT.1	N/A	Technical Query 911 recognizes that there are no audit records generated for the establishment and disestablishment of communications with the audit server.

		IdentityIQ must be connected to the Oracle database for all operation. The Oracle database also holds all audit logs. Thus, there is no way for the TOE to make an audit record for this action, because disestablishment and establishment of this channel is synonymous with operation of the TOE. It can be concluded that a connection to the audit server is established when IdentityIQ starts up and that the connection is torn down once IdentityIQ shuts down.
FIA_AFL.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Identity Locked Source: SailPointContextRequestFilter Client Host: IP address or hostname Server Host: IP address or hostname Target: The Administrator Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Unlock Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname Target: Example_User Account Name: CN=Example_CN, OU=Example_OU, DC=Example_DC1, DC=Example_DC2, DC=Example_DC3	The first audit log shows an example user lock and the second shows an example user unlock. Date – Date and Time of event Action – Type of event/Outcome and Action taken when threshold is reached Source – Subject Identity Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system Target – Destination of transmission Account Name - Subject Created/modified
FIA_SOS.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Password Policy Changed Source: Example_User Attribute Name: op Attribute Value: update Attributes: Maximum number of characters - Changed from (300) to (80)	This audit log is generated when the password policy is changed. The Attributes field lists all the changes made to the policy. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Attribute Name –Attribute that was modified Attribute Value – Identifies type of action made to attribute Attributes – Changes that were made
FIA_SOS.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: PasswordChangeFailure Source: Example_User_A Target: Example_User_B Date: MM/DD/YYYY HH:MM:SS AM/PM Action: change Source: Example_User_A Target: Example_User_B Attribute Value	The first audit log is generated upon rejection of a tested secret. Example_User_A is the user who attempted to change the password. Example_User_B is the owner of the password. The second audit log is generated upon successful acceptance of a tested secret. Example_User_A is the user who changed

	Value1: password Value2: set	the password. Example_User_B is the user whose password was changed. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Target – Destination of transmission
FMT_MOF.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: AuditConfigChange Source: Example_User Attribute Name: op Attribute Value: update Attributes: Access Request Started - From (enabled: true;) to (enabled: false;) Approve Work Item - From (enabled: true;) to (enabled: false;)	Audit logs are generated for all modifications of management by the TOE. The Action field determines the configuration that was performed. An example of the management function for FAU_GEN.1 is shown, which is the configuration of auditable events. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Attribute Name –Attribute that was modified Attribute Value – Identifies type of action made to attribute Attributes – Changes that were made
FMT_SMF.1	N/A	Audit logs are generated for all management functions performed by the TOE. The Action field determines the function that was performed. See other entries in this table for examples.
FTA_SSL.3	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Session Timeout Source: unknown Client Host: IP address or hostname Server Host: IP address or hostname Target: Example_User	The audit log generated for session timeout has the format shown. Note that the source is listed as unknown when a timeout occurs to inactivity. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system Target – Destination of transmission
FTA_SSL.4	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Logout Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname	The audit log format for logging out is shown. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity

		Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system
FTP_ITC.1	**Aggregation from Active Directory** Name: Name Type: Account Aggregation Started By: Example_UserA Started: MM/DD/YYYY HH:MM:SS AM/PM Completed: MM/DD/YYYY HH:MM:SS AM/PM Host: IP address or hostname Status: Success Applications Scanned: Active Directory Name **Transmitting User Data to Active Directory** Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Delete Source: Example_UserA Client Host: IP address or hostname Server Host: IP address or hostname Target: Example_User Application: Active Directory Name Account Name: CN= Example_UserB Common Name, OU= Example_UserB Organizational Unit, DC= Example_UserB Domain Component **Successful Authentication via Active Directory** Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Login Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname Attribute Value1: Active Directory Name Value 2: Example_User **Oracle Database** Refer to FAU_STG_EXT.1 and Technical Query 911.	Audit logs are generated for trusted channel connections to Active Directory. The audit records are slightly different depending on the purpose for connecting to the Active Directory instance. **Aggregation from Active Directory** Name – Name of event Type – Type of event Started By – Subject Identity Started – Date and Time of event started Completed – Date and Time of event completed Host – IP address or hostname of IdentityIQ system (Identity of the initiator of the trusted channel) Status – Outcome Applications Scanned – Active Directory instance scanned (Identity of the target of the trusted channel) **Transmitting User Data to Active Directory** Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system (Identity of the initiator of the trusted channel) Target – identity for sent account data Application – Active Directory instance being transmitted to (Identity of the target of the trusted channel) Account Name – Account data for target **Successful Authentication via Active Directory** Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity Client Host – IP address or hostname of

		initiating system Server Host – IP address or hostname of receiving system (Identity of the initiator of the trusted channel) Attribute Value1: Active Directory instance being authenticated against (Identity of the target of the trusted channel) Value 2 – identity being authenticated
FTP_TRP.1	Date: MM/DD/YYYY HH:MM:SS AM/PM Action: Event Source: Example_User Client Host: IP address or hostname Server Host: IP address or hostname Attribute Value1: Active Directory Name (if applicable) Value 2: Example_User (if applicable)	This example shows an attempted use of the trusted path. Date – Date and Time of event Action – Type of event/Outcome Source – Subject Identity (Identification of user associated with all trusted path functions) Client Host – IP address or hostname of initiating system Server Host – IP address or hostname of receiving system Attribute Value1: Active Directory instance being authenticated against Value 2 – identity being authenticated

Table 8-2: Examples of Audit Records

8.1 Audit Storage

Chapter 15 of the SailPoint IdentityIQ Direct Connectors Administration and Configuration Guide [3] discusses how to configure the JDBC connector in order to be able to connect IdentityIQ to the Oracle 18c database that is implemented as part of the evaluated configuration. This connection enables IdentityIQ to read and write user and audit data to the database over a secure channel that uses TLS via the JRE's JDBC.

IdentityIQ does not provide a user interface to the database where the audit records are stored. Therefore, these records cannot be modified or deleted from the TOE. In the evaluated configuration, the connection to this database is established once the TOE is running. The TOE cannot operate without this connection established. If the connection is severed, then the TOE will re-establish the connection automatically.