SailPoint IdentityIQ

Version 8.1

Application Configuration Guide

Table of Contents

IdentityIQ Introduction

SailPoint IdentityIQ is an identity and access management solution for enterprise customers that delivers a wide variety of IAM processes-including automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. Furthermore, IdentityIQ has a flexible connectivity model that simplifies the management of applications running in the datacenter or the cloud.

Compliance Manager — IdentityIQ Compliance Manager automates access certifications, policy management, and audit reporting through a unified governance framework. This enables you to streamline compliance processes and improve the effectiveness of identity governance, all while lowering costs.

Lifecycle Manager — IdentityIQ Lifecycle Manager manages changes to access through user-friendly self-service request and password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

IdentityAI – Integrating IdentityAI within IdentityIQ enables the delivery of Predictive Identity. IdentityAI is a rule based machine learning engine using identity graph technology to provide recommendations for access review and access request decisions. With IdentityAI enabled, you can also review access history for identity cubes, create dashboards that can be customized from an administrative perspective, and view peer groups within the IdentityAI user interface.

Privileged Account Management Module — IdentityIQ Privileged Account Management module provides a standardized approach for extending critical identity governance processes and controls to highly privileged accounts, enabling IdentityIQ to be used as a central platform to govern standard and privileged accounts.

Connectors and Integration Modules — IdentityIQ offers Integration Modules that support the extended enterprise IT infrastructure. Third party provisioning and service desk integration enable multiple sources of fulfillment to access change. Service catalog integration supports a unified service request experience with integrated governance and fulfillment. Mobile device management integration mitigates risk posed by mobile devices through centralized visibility, control and automation. And IdentityIQ's IT security integration provides enhanced security with improved responsiveness and controls.

Open Identity Platform — SailPoint's Open Identity Platform lays the foundation for effective and scalable IAM within the enterprise. It establishes a common framework that centralizes identity data, captures business policy, models roles, and takes a risk-based, proactive approach to managing users and resources. The Open Identity Platform is fully extensible, providing robust analytics which transforms disparate and technical identity data into relevant business information, resource connectivity that allows organizations to directly connect IdentityIQ to applications running in the datacenter or in the cloud, and APIs and a plugin framework to allow customers and partners to extend IdentityIQ to meet a wide array of needs. An open platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications-in the datacenter and the cloud. SailPoint IdentityIQ applies consistent governance across compliance, provisioning and access management processes, maximizing investment and eliminating the need to buy and integrate multiple products.

Password Manager — IdentityIQ Password Manager delivers a simple-to-use solution for managing user passwords across cloud and on-premises applications policies from any desktop browser or mobile device. By providing intuitive self-service and delegated administration options to manage passwords while enforcing enterprise-grade password, IdentityIQ enables businesses to reduce operational costs and boost productivity.

Amazon Web Services (AWS) Governance Module — Enables organizations to extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments to provide a central point of visibility, administration, and governance across the entire enterprise. This includes policy

discovery and access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and federated access support.

SAP Governance Module — Improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures. New filtering capabilities enable more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as T-Codes and Authorization Objects.

Chapter 1: Configure Applications

For each application in your enterprise, you must define each application in your enterprise and specify the following items:

- Connection properties
- Relevant attributes,
- Target
- Aggregation rules

Application List Page

The Application List page displays all of the applications currently configured. To access this page, from the menu bar, go to **Applications -> Application Definition**. The Application List contains the following information:

Table 1—Application List Column Descriptions

Column	Description
Name	The name of the application.
Host	Host where the application resides.
Type	The application type, for example LDAP or JDBC.
Modified	The date when the application was last modified.

Use the Configure Application page to add or edit applications. Click on an existing application or click **New Application** to open the “Edit Application Page” on page 3.

Edit Application Page

Note: Do not open multiple tabs or browsers. Opening multiple tabs might overwrite changes made in the other.

Use the Edit Application page to define the applications in your enterprise. Specify the connection properties, relevant attributes, aggregation rules, and activity information for each application.

The information contained on the Configuration, Correlation, Risk, Activity Data Sources, and Unstructured Targets, Rules, Password Policy, and Tiers tabs is determined by the type of application specified on the **Application Type** drop-down list. Use these tabs to define how each application interacts with IdentityIQ.

Note: The Tiers tab is only available for Logical application types. See detailed information about configuring logical applications in the SailPoint IdentityIQ *Direct Connectors Administration and Configuration Guide*.

The Edit Application page opens to the Details page and contains the following tabs:

- "Configuration Tab" on page 6
- "Correlation Tab" on page 12
- "Accounts Tab" on page 12
- "Risk Tab" on page 13
- "Activity Data Sources Tab" on page 13
- "Unstructured Targets Tab" on page 14
- "Rules Tab" on page 15
- "Password Policy Tab" on page 15

For each application enter or edit the following information:

Note: This screen also contains any extended attributes that were configured for your deployment of IdentityIQ. The extended attributes are displayed at the bottom of the tab.

Table 2—Edit Application Page — Details Field Descriptions

Field	Description
Name	The name of the application. This is the named used to identify the application throughout the IdentityIQ application.
Owner	The owner of the application. The owner specified here is responsible for certifications and account group certifications requested on this application if no revoker is specified. Application ownership can be assigned to an individual identity or a workgroup. If the application ownership is assigned to a workgroup, all members share certification responsibilities, are assigned certification request associated with the application and all can take action on those requests.
Application Type	The application type, for example LDAP or JDBC. The **Application Type** drop-down list contains the types of application to which IdentityIQ can connect. This list will grow and change to meet the needs of IdentityIQ users.
Description	A brief description of the application. **Note: You must Save the description before changing languages to enter another description.** Use the language selector to enter description in multiple languages. The drop-down list displays any languages supported by your instance of IdentityIQ. The description displayed throughout the product is dependent on the language associated with the user's browser. If only one description is entered, that is the description used by default.
Revoker	The default IdentityIQ user or workgroup to be assigned revocation requests associated with entitlements on this application. **Note: If no user is specified in this field, all revocation requests are assigned to the to application owner by default.**

Table 2—Edit Application Page — Details Field Descriptions

Field	Description
Proxy Application	Optional: Specify an application to manage accounts and provide a connector and schema settings for this application. A proxy application is an application that handles the processing (aggregation and provisioning) on behalf of your application. Here are three examples of proxy applications: —Multiplex applications: In this case you define an application and, most often, a build map rule that sorts the data out in multiple sub-applications. In that case, the sub-applications have the main application as the proxy. — Similar to the multiplex applications are the connectors for legacy identity management systems such as, BMC, Novell/NetIQ, IBM Tivoli, and Sun/Oracle Waveset. — The Cloud Gateway connector tunnels all aggregation and provisioning requests to the gateway in another network. The gateway then acts on behalf of IdentityIQ. All applications that live in the remote network need to have the cloud gateway connector set as the proxy.
Profile Class	An optional class used to associate this application with a larger set of applications for role modeling purposes. For example, you might set a profile class of XYZ on all of the applications where any user that has read account privileges should be assigned the role XYZ Account Reader. You can then create a single profile for that role instead of a separate profile for each instance of the applications. During the correlation process any user with read account privileges on any of the applications with the profile class XYZ is assigned the role XYZ Account Reader.
Scope	**Note: This field is only visible if scope is enabled.** The scope for this application. If scope is assigned, only the owner of the application or users that control the designated scope can work with this application. Objects associated with this application, for example entitlements in a certification request, are visible to a user with any or no controlled scope, but if a new object is being created, for example a certification schedule, this application does not appear on the select list unless the creator controls the scope assigned. Depending on configuration settings, objects with no scope assigned might be visible to all users with the correct capabilities.
Authoritative Application	Select if this application in an authoritative application. You can specify multiple authoritative applications. An authoritative application is a repository for employee information for your enterprise, for example a human resources application. These might not be at risk applications, but they are the data source from which the majority of the IdentityIQ Identity Cubes are built.
Case Insensitive	Use to cause case insensitive comparisons of account attribute values when evaluating provisioning policy.

Table 2—Edit Application Page — Details Field Descriptions

Field	Description
Native Change Detection	Select this option if this application should be included when IdentityIQ performs native change detection during aggregation.
Native Change Definitions:	
Native Change Operations	Select which operations are included when detecting native change. If no operations are selected, native change detection is disabled.
Attributes to Detected	Indicates which attributes are compared when accounts are modified. If the **Entitlement** option is selected, all entitlement attributes are included. If you select **User Defined**, enter the name of the attributes to compare in the **Attribute Names** box.
Maintenance: Take an application off line for maintenance	
Maintenance Enabled	This application is excluded from provisioning and aggregation during the defined maintenance period.
Maintenance Expiration	The date at which the maintenance will end. If no date is defined, this application will be in maintenance indefinitely.

After adding the application information, click **Save** to save your changes and return to the Application List page.

Configuration Tab

The information displayed on the Configuration tab changes depending on the application type specified. The tab is haste following tabs:

- "Settings Tab" on page 6
- "Schema Tab" on page 7
- "Provisioning Policies Tab" on page 9

Settings Tab

Note: The terms account group and application object are use interchangeably in this document but have the same meaning. Some application can have multiple application objects. An account group can be the name of one of those objects.

A note is displayed at the top of this tab for application configured to use credential cycling. For those applications, the credentials are stored and maintained on a Privileged Access Management (PAM) module, and verification is performed using existing hook points that support the retrieval of passwords from application credential management solutions such as, CyberArk Application Identity Manager (AIM) or BeyondTrust PowerBroker Password Safe. Refer to the SailPoint IdentityIQ *Privileged Assess Management Module Guide* for more information.

The Settings tab contains the information that IdentityIQ uses to connect and interact with the application. Each application type requires different connection information and the fields on this tab are changed accordingly.

For most application types you see account and group object types, certain application types, however, enable you to create multiple application object types, each with their own schema. These application object types are sometimes referred to as account groups and those term might be used interchangeably in discussion around this feature.

Click at the top of the page to add a new object type. This function is only available for if the application type is associate with a connector that is enable to handle multiple application object types, or multiple schema.

This button is also displayed if you recently upgraded your instance of IdentityIQ and the application type now supports multiple schemas. In that case you must add the supported application object type here and then run the Account Group Aggregation task to import the new information.

Multiple application object types can be directly correlated, for example an application object type is also an attribute in the schema of another, or they can be indirectly associated, for example they are both objects (schemas) in the same application. These objects and their associations are tracked throughout IdentityIQ and appear in place such as reports, policy violations, searches, and certifications.

If your enterprise is going to use partitioning for account aggregations, identity refreshes, and manager certification, you must enable that function here. Each application type requires different partitioning information.

This is also where you enable an application for data merging and delta aggregation.

Refer to the connector documentation for detailed information on each of the connectors.

Enter the information on this tab as required by the application type being configured. Click **Test Connection** to verify the information is correct.

Schema Tab

The Schema tab is used to define the attributes for each object type in the application being configured. Use the following fields to define attributes for use with the IdentityIQ application. The field content is dependent on the application being configured.

Refer to the connector documentation for detailed information on each of the connectors.

When initially configuring applications, click **Add New Schema Attribute** to define the attributes for each object. Most application types include a default set of schema attributes. For more dynamic application types (JBDC or DelimitedFile), schemas should be defined manually. Click **Edit** to display the Advanced Properties dialog.

The connectors for some application types enable the automatic discovery of the base schema attributes for those applications. For those application types, click **Discover Schema Attributes** to automatically populate your schema tables. After using the automatic discovery function you must designate the Identity Attribute and Display Attribute for the application.

Click **Preview** to test the respective schema configuration. A pop-up sample table displays to indicate a successful configuration. These tables automatically update when you make changes so that you can use this feature before committing your changes. Only one table can be open at one time. Failures result in an error message specifying the point of failure, for example, a file path and name.

Note: The Preview function does not apply to applications which do not support aggregation.

Table 3—Application Configuration - Schema Tab Field Descriptions

Fields	Descriptions
Native Object Type	**Note: LDAP default types are iNetOrgPerson and groupOfUniqeNames for groups.** **Note: This is a required field.** The type of object with which the attributes are associated. For example, User and Group for Active Directory LDAP or DBA_USER and DBA_ROLES for Oracle.

Table 3—Application Configuration - Schema Tab Field Descriptions

Fields	Descriptions
Identity Attribute	**Note: This is a required field.** **Note: Do not change the identity attribute on connectors with pre-defined schema.** The attribute that is used by the IdentityIQ application to identify the object.
Include Permissions	Select this function to automatically add directPermissions to the schema. This option is available for any application that has `DIRECT_PERMISSIONS` in the `featureString`, for example, Oracle, DelimitedFile, and sybase HR. With this option activated, IdentityIQ correctly pulls in permission data for identities.
Display Attribute	**Note: This is a required field.** The attribute that is used as the object name as it appears throughout the IdentityIQ application.
Instance Attribute	The attribute that uniquely identifies a specific instance of an application. **Note: Instance Attributes are not supported for Managed Attributes.**
Remediation Modifiable	Accounts that are remediation modifiable can have their values and permissions modified from the Certification Report page for the identity being certified. Specify the method of modification for this attribute: **Select** — display a select list of all possible values or permissions for this attribute. **Free text** — display a text field in which a certifier can enter any value.
Additional Group Attributes:	
Description Attribute	Used during group aggregation to indicate which of the group attributes is used to populate the corresponding ManagedAttribute description. The value set here overwrites any set during the Account Group Aggregation task.
Group Membership Attribute	The attribute that is used by the IdentityIQ application to identify the group.
Attributes:	
Name	**Note: Attribute names cannot begin with IIQ_. Attributes with names that begin with IIQ_ are considered internal, reserved attributes and are not displayed in the product.** The name of the attribute.
Description	A brief description of the attribute.
Type	The type of attribute being defined. For example, string or boolean. Select from the drop-down list.
Properties: Click Edit to open the Advanced Properties dialog to edit the attribute properties.	

Table 3—Application Configuration - Schema Tab Field Descriptions

Fields	Descriptions
Managed	Specify attributes to promoted to a first-class object in the IdentityIQ database so that they can be associated with other objects with that value, for example a description or an owner. Any attribute can become managed: department, location, title, but the most common attribute to be managed is the one holding group memberships. Managed attributes can be viewed and managed from the Entitlement Catalog page.
Entitlement	Specify attributes to be used as entitlements on this application. Attributes specified as entitlements are used by IdentityIQ as follows: — as additional entitlements during certification. — when creating profiles based on exiting users on this application. Profiles are created on the IdentityIQ Modeler and are used to create roles. — in account group certifications. — in Lifecycle Manager.
Multi-Valued	Specify attributes for which multiple values might be returned during aggregation. Attributes flagged as multi-valued are stored as a list. Even objects that have a single value for a multi-value attribute are stored as a single-item list. Multi-valued attributes are used for queries throughout the product. Before multi-valued attributes are available for use in searches, they must be mapped on the Edit Account Attribute page. Refer to the SailPoint IdentityIQ System Configuration Guide for information on how to add or edit account attributes.
Correlation Key	Specify attributes that IdentityIQ can use to correlate activity discovered in the activity logs for this application with information stored in identity cubes. For example, activity logs might contain the full name of users instead of unique account ids. Therefore, correlation between the activity discovered by an activity scan and the identity cube of the user that performed the action must key off of the user's full name. **Note: Correlation Key is only used during activity aggregation. If activity aggregation is not being used, Correlation Key should not be selected.**
Minable	Specify attributes for use during role and profile creation. When creating roles and profiles it is possible to mine applications for attributes and permissions to use in those objects rather than manually entering the values. Only attributes designated as minable are returned by those searches.
Remediation Modifiable	Attributes that are remediation modifiable can have their values and permissions modified from the Certification Report page for the identity being certified. Specify the method of modification for this attribute: **Select** — display a select list of all possible values or permissions for this attribute. **Free text** — display a text field in which a certifier can enter any value.

Provisioning Policies Tab

Provisioning Policies are used to define application object attributes that must be managed due to a Lifecycle Manager request. With a provisioning policy in place, when a role or entitlement is requested the user must input specified criteria into a generated form before the request can be completed. A policy can be attached to an IdentityIQ application object or role and is used as part of the provisioning process.

For applications that support multiple application objects, each object is displayed in a separate table containing the provisioning policies those objects support. Not all application objects support all of the provisioning policies listed below.

In order to be able to provision to a DN with a backslash (\) to an Active Directory application through the Cloud Gateway you will need to set the following properties in catalina.sh or catalina.bat on the Cloud Gateway instance:

```
    set CATALINA_OPTS=%CATALINA_OPTS%
-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true
    set CATALINA_OPTS=%CATALINA_OPTS%
-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=true
```

Setting the dependencies between applications and accounts implies ordering in provisioning.

IdentityIQ includes the following types of provisioning policies:

- Create
- Update
- Delete
- Enable Account
- Disable Account
- Unlock Account
- Change Password
- CreateGroup
- UpdateGroup

Click an existing provisioning policy or click **Add Policy** to create a new one using the Provisioning Policy Editor or to reference an existing policy. Only one of each policy types is supported.

Use the **Application Dependencies** drop-down list to create the list of applications where this application is dependent for provisioning. If no account is detected on an application where this application is dependent, an account request is added to the provisioning plan and the provision policy for this application is processed as expected.

The Provisioning Policy Editor panel contains the following information:

Table 4—Application Configuration - Provisioning Policy Editor Field Descriptions

Field Name	Description
Name	The name of your provisioning policy.
Description	A brief description of the provisioning policy.
Owner	The owner of the provisioning policy. This is determined by selecting from the following: None — no owner is assigned to this provisioning policy. Application Owner — identity assigned as owner of the application in which the provisioning policy resides. Role Owner — identity assigned as owner of the role in which the provisioning policy resides. Rule — use a rule to determine the owner of this provisioning policy. Script — use a script to determine the owner of this provisioning policy

Table 4—Application Configuration - Provisioning Policy Editor Field Descriptions

Field Name	Description
Edit Provisioning Policy Fields Panel Use the Edit Provisioning Policy Fields panel to customize the look and function of the form fields generated from the provisioning policy.	
Name	The name of the field.
Display Name	The name displayed for the field in the form generated by the provisioning policy.
Help Text	The text you wish to appear when hovering the mouse over the help icon.
Type	Select the type of field from the drop-down list. Choose from the following: Boolean — true or false values field Date — calendar date field Integer — only numerical values field Long — similar to integer but is used for large numerical values Identity — specific identity in IdentityIQ field Secret — hidden text field String — text field
Multi Valued	Choose this to have more than one selectable value in this field of the generated form. Click the plus sign to add another value.
Read Only	Determine how the read only value is derived: Value — value based on the selection from the drop-down list Rule — value is based on a specified rule Script — value is determined by the execution of a script
Hidden	Determine how the hidden value is derived: Value — value based on the selection from the drop-down list Rule — value is based on a specified rule Script — value is determined by the execution of a script
Owner	The owner of this provisioning policy field. This is determined by selecting from the following: None — no owner is assigned to this provisioning policy. Application Owner — identity assigned as owner of the application in which the provisioning policy resides. Role Owner — identity assigned as owner of the role in which the provisioning policy resides. Rule — use a rule to determine the owner of this provisioning policy. Script — use a script to determine the owner of this provisioning policy
Required	Choose whether or not to have the completion of this field a requirement for submitting the form.
Review Required	Choose whether or not to require the person who is approving the workflow item to approve this field.
Refresh Form on Change	Select this option to have the form associated with this policy refresh to reflex changes to this policy.
Display Only	Set this field as display only.
Authoritative	Boolean that specifies whether the field value should completely replace the current value rather than be merged with it; applicable only for multi-valued attributes

Table 4—Application Configuration - Provisioning Policy Editor Field Descriptions

Field Name	Description
Value	Determine how the value is derived. Select from the following: Literal — value is based on the information you provide Rule — value is based on a specified rule Script — value is determined by the execution of a script
Validation	Gives the ability to specify a script or rule for validating the user's value. For example, a script that validates that a password is 8 characters or longer.

Correlation Tab

Use the correlation tab to configure how application accounts are assigned to identities within IdentityIQ using account and identity information.

To configure Account Correlation you can select an existing correlation configuration from the list or create a new configuration using the correlation wizard. The correlation wizard walks you through both attribute and condition based correlation.

In the manager correlation section, configure how assigned managers should be resolved to identities using existing information.

- **Attribute Based Correlation** — use attributes of the application's account to find identities based on attribute values stored on Identity objects. This is how accounts are typically correlated to Identities. For example, you can correlate the application's account attribute “mail” with an identity's attribute “email”.
- **Condition Based Correlation** — assigns application accounts to existing identities by defining attribute conditions. Service and Administrator accounts might be handled using condition based correlation. For example, the root account on Unix typically does not have any identifying attributes that can help when trying correlate it to an existing identity. In cases where the account owner is known because they are the application owner, a direct mapping can be used.

To configure Manager Correlation you must select two attributes, the Application Attribute and the Identity Attribute.

- **Application Attribute** — the name of the applications account attribute that holds the reference to the manager.
- **Identity Attribute** — the name of the identity attribute to use when searching for managers.

For example, if the application has an attribute `managerEmail` with the value set as the email address of the manager of every user with an account on the application, and you have an identity attribute `email` configured within IdentityIQ with the value set as the email address for every identity cube, you would correlate the application attribute `managerEmail` with the identity attribute `email` to perform manager correlation.

Accounts Tab

The Accounts Tab list the following information for the selected account:

- Account ID
- Account Name
- Status
- Last Refresh
- Identity Name

Click the down -arrow next to an account name to view detail about the account, such as the last login time and date.

Risk Tab

The application Risk tab provides a current application risk score and a detailed view of the raw and compensated risk score for each category used to derive that score. This page also provides a list of the top composite score contributors providing further information on how the score was derived and providing clues on the areas of highest risk. These scores are based on the latest information discovered by IdentityIQ.

IdentityIQ uses a combination of base access risk and compensated scoring to determine the overall application risk scores, or composite risk score, used throughout the application.

All scores are calculated by first determining the percentage of accounts that have the qualities tested by the component score. For example, if 10 out of 100 accounts are flagged as service accounts, then the raw percentage is ten percent (.10). This number is then multiplied by a sensitivity value which can be used to increase or decrease the impact of the original percentage. The default sensitivity value is 5 making the adjusted percentage fifty percent (.50). This final percentage is then applied to the score range of 1000 resulting in a component score of 500.

After the component score is calculated a weight, or compensating factor, is applied to each component score to determine the amount each contributes to the overall risk score for the application. For example, a few violator accounts might increase risk more than many inactive accounts.

Service, Inactive, and Privileged component scores look for links that have a configured attribute. For example, the component `service` with a configured value `true`.

The Dormant Account score looks for a configured attribute that is expected to have a date value, for example `lastLogin`. This algorithm has an argument, `daysTillDormant`, that defaults to thirty (30). If the last login date is more than thirty (30) days prior to the current date, the account is considered dormant and is factored into the risk score.

The Risky Account score looks for links whose owning identity has a composite risk score greater than a configured threshold. The default threshold is five hundred (500).

The Violator Account score looks for links whose owning identity has a number of policy violations greater than a configured threshold. The default threshold is ten (10).

Activity Data Sources Tab

The Activity Data Source tab is used to configure the data sources from which activity information is collected. The information collected from these sources is normalized and then stored by IdentityIQ and used to monitor activity information for users and applications. Activity information is collected and correlated using the Activity

Aggregation task. Activity information displayed on the or returned by activity searches is based on the information stored by IdentityIQ since the last aggregation and correlation tasks were run.

The Activity Data Sources table contains the following information:

Table 5—Application Configuration - Activity Data Source Tab Table Descriptions

Column	Description
Name	A descriptive name for the activity data source from which the activity data is collected.
Type	The activity data source type, for example JDBC Collector, Log File, CEF Log File or Windows Event Log Collector.
Modified	The date when the activity data source was last modified.

Right-click a data source and select **Edit** or click **New Activity Data Source** to access the Activity Data Source Configuration page.

Right-click a data source and select **Delete** to remove an activity data source.

See “Activity Data Source Configuration” on page 21.

Unstructured Targets Tab

Unstructured target information is used to define unstructured data sources from which the connector is to extract data. Unstructured data is any data that is stored in a format that is not easily readable by a machine. For example, information contained in an Excel spread sheet, the body of an email, a Microsoft Word document, or an HTML file is considered unstructured data. Unstructured targets pose a number of challenges for IdentityIQ connectors, because not only is the data stored in a format that is hard to extract from, the systems and directory structures in which the files reside are often difficult to access.

The most common unstructured data type supported by IdentityIQ is an operating system’s file system permissions.

This target collector requires a the IdentityIQ Service to be installed on a machine that has visibility to the directory or share to include in the target scan. Refer to the IdentityIQ *Installation Guide* for information on installing and registering the IQService.

The unstructured targets defined on this tab are used by the Target Aggregation task to correlate targets with permissions assigned to identities and account groups for use in certifications.

Each of the Target Source Types require unique details or attributes for their configuration, but share some basic information.

The Unstructured Targets tab contains the following basic information for each of the Target Source Types:

Table 6—Application Configuration - Unstructured Targets Tab Field Descriptions

Field	Description
Name	The name of this unstructured target configuration.
Description	A brief description of this configuration.

Table 6—Application Configuration - Unstructured Targets Tab Field Descriptions

Field	Description
Rules: Specify the rules used to transform and correlate the targets. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**	
Creation Rule	The rule used to determine how the unstructured data extracted from data source is transformed into data that can be read by IdentityIQ.
Correlation Rule	The rule used to determine how to correlate account information from the application with identity cubes in IdentityIQ.
Provisioning Action	The provisioning action used to pass information to the affected applications.

Rules Tab

These are the rules that can be customized to handle the complexity of the data being extracted. Rules are specific to connectors and are used throughout the product. You can write more than one of each type and select the rule to use from drop-down lists.

A file containing an example of each rule type is included in the IdentityIQ installation package. The examplerules.xml file is located in the IdentityIQ_*HOME*/WEB-INF/config directory.

The rules in this table apply to all applications and are called by the aggregation process. A correlation rule is only required if there is more than one application and a correlation configuration has not been defined.

The delimited file connector has rules that are specific to its implementation; buildMapRule, mergeMapsRule, and mapToResourceObject Rule.

Password Policy Tab

Use the password policy tab to select and create password policies which apply to specified applications.

The password policy panel contains the following:

Table 7—Application Configuration - Password Policy Field Descriptions

Field Name	Description
Name	The name of your password policy.
Description	A brief description of the password policy.

Click an existing password policy to edit it or click **Create New Policy** to configure one from scratch.

Table 8—Application Configuration - Password Policy Editor Field Descriptions

Field Name	Description
Password Policy Name	The name of your password policy.
Password Policy Description	A brief description of the password policy.

Table 8—Application Configuration - Password Policy Editor Field Descriptions

Field Name	Description
Minimum number of characters	Input the minimum number of characters required for a valid password.
Maximum number of characters	Input the maximum number of characters required for a valid password.
Minimum number of letters	Input the minimum number of letters required for a valid password.
Minimum number of character type constraints to meet	The minimum number of character types (digits, upper case, lower case, special) required for a valid password.
Minimum number of digits	Input the maximum number of numerical digits required for a valid password.
Minimum number of uppercase letters	Input the minimum number of uppercase letters required for a valid password.
Minimum number of lowercase letters	Input the minimum number of lowercase letters required for a valid password.
Minimum number of special characters	Input the minimum number of special characters required for a valid password.
Number of repeated characters allowed	The maximum number of consecutive repeated characters allowed in a valid password. For example, if this option is set to 2, “cloudd” and “cclooud” is valid, but “clouddd”, “cloooud” and “cccloud” are invalid. For “cclooudd” invalid password, the following error message is displayed: Password should not contain more than 2 occurrence(s) of the repeated characters. For “Clouddd” invalid password, the following error message is displayed: Password should not contain more than 2 consecutive repeated characters.
	The maximum number of occurrences of repeat characters allowed in a valid password. For example, if this option is set to 1, “happy123” is valid, but “happy123dd” and “happpy123” are not.
Password history length	The number of past passwords that cannot be used again.
Triviality check against old password	Ensure that the shorter of the old and new password is not a substring of the other. Both passwords are changed to upper case prior to the check.
Minimum number of characters by position	The minimum number of unique characters by position the new password. Can be used to ensure that not just the first or last character is being changed. Select **Case sensitive check** to ensure that more than just the case is changing in the new password.

Table 8—Application Configuration - Password Policy Editor Field Descriptions

Field Name	Description
Validate passwords against the password dictionary	Select do disallow the use of any password defined in the password dictionary. The password dictionary is a configurable list of terms unavailable for use as passwords. The `passwordDictionary.xml` file located in IdentityIQ/`WEB-INF/config/`.
Validate passwords against the identity's list of attributes	Select to disallow the use of Identity attribute values as passwords.
Validate password against the account's display name	Select to disallow the use of the account's display name as the password (exact match by default). Enter a **Minimum word length** to define the minimum length of a substring of the account's display name allowed in the password.
Validate password against account ID	Select to disallow the use of the account's ID as the password (exact match by default). Enter a **Minimum word length** to define the minimum length of a substring of the display name of the account allowed in the password.
Validate passwords against the identity's account attributes	Select to disallow the use of Identity link attribute values as passwords. Enter a **Minimum word length** to define the minimum length of a substring of the account's ID allowed in the password.
Configure Password Filter	Select a filter that selects the identities to which this password policy applies. Select from the following filters: All — all identities have this password policy applied Match List — only identities whose criteria match that specified in the list. The criteria is configured using the tools provided. Add identity attributes, application attributes and application permissions. Customize further by creating attribute groups to which this password policy applies. **Note: If Is Null is selected, the associated value text box is disabled. When the is null match is processed, the term matches users on the chosen application who have a null value for that attribute/permission.** Filter — use an XML filter or compound filter to determine the identities to which this password policy applies. Script — use a BeanShell script to determine the identities to which this password policy applies. Rule — use a rule to determine the identities to which this password policy applies. Population — select a population to which this password policy applies.

SecurityIQ Type Application

SecurityIQ enables enterprises to discover and govern access to sensitive data and better address the security threat to unstructured data. As a key component of SailPoint's Identity Governance strategy organizations can take a comprehensive approach to govern access across all users, applications and data with enhanced visibility while reducing risk.

Use SecurityIQ to:

- Identify and govern access to exposed sensitive data found within cloud and on-premises file stores.
- Enable business users to manage access to data they know best; alleviating IT burden and over-permissioned access.
- Leverage a comprehensive identity governance solution that extends to unstructured data throughout the enterprise.

Create a new application of type SecurityIQ. By default, this application will start with an alert schema, as well as unstructured and associations schemas. The unstructured and associations schemas are used to define the makeup the Target and TargetAssociation respectively.

Attributes/Configuration:

Defined schemas on the configuration tab. If an alert schema is defined, this will include the configuration needed to set up the Alerts. If the Unstructured schema is defined, this will include the configuration needed to set up the Target/Target Permissions.

Connection Settings:

Database URL - The jdbc connection URL for the SecurityIQ database.

Driver Class - The JDBC Driver class to use for the connection.

UserName - The database user name

Password - Password for the configured user name

Schema - Schema used for the SIQ DB.

General Settings:

Referenced Applications - This is a list of applications to which the given permission are correlated. The target permissions are correlated to either a Link or ManagedAttribute belonging to one of the applications in the list.

Aggregate Inherited - True to aggregate inherited permissions. If set to true, the dataset will be much larger. If false, only the top level permissions are aggregated, and inheritance is assumed as defined on the native source.

TargetHosts - The List of SIQ Business Application Monitors from which to aggregate permissions.

Target Host Paths - This is a CSV of Paths from which to aggregate. This aggregation starts at the given root paths, and discovers all permissions under these paths. If not specified, all target/target permissions for the specified BAM are aggregated.

Rules:

The rules tab within the Application Definition user interface enables the defining of rules for given object types. The Application level rules and schema level rules, for schemas that allow them, are shown with the ability to select/edit (based off of correct capabilities) the given rules. The unstructured schema support Correlation/Creation/Customization/Refresh rules on the schema level.

Creation rules for unstructured schema will be of **Rule Type** TargetCreation

Refresh rules for unstructured schema will be of **Rule Type** TargetRefresh

Correlation rules for unstructured schema will be of **Rule Type** TargetCorrelation

Customization rules for unstructured schema will be of **Rule Type** ResourceObjectCustomization

The unstructured/assocations schema AttributeDefinitions are used to define the columns to include in the query.

Application Re-configuration

The application re-configuration option enables you to change the application type without losing history associated with the application or having to create a new application. For example, if you first deployed your instance of IdentityIQ using a flat file connection, but now want to use some of the more advance features, such as provisioning. The type defines the way in which IdentityIQ connects to the application.

Application types that have the same value format for identity and group attributes in the original and re-configure target are best suited for re-configuration.

The following application types can be re-configured:

Note: Even in the following scenarios, there might be some connectors that do not re-configure correctly. See "Application Re-configuration Considerations" on page 20.

- Delimited file to the corresponding direct connector (Delimited File to Active Directory - Direct)
- JDBC connector to corresponding direct connector (JDBC to Oracle Applications - Direct)
- Agent based connector to direct connector (Active Directory - Full to Active Directory - Direct)
- To a rewritten connector for better performance or more functional support (Google Apps - Direct)

Application Re-configuration Considerations

Take the following points into consideration before deciding to re-configure an application.

- Do the identity attribute of account and group in the original application match the identity attribute of account and group in the re-configured application?

For example:

  - Two application types (Delimited File and Active Directory – Direct) use distinguishedName as the identity attribute of account, and use the same identity attribute for group. Since both of these applications refer to the same identity attribute of both account and group, they would be good candidates for re-configuration.
  - Two application types (Oracle Application – FULL and Oracle Application – Direct) use different identity attributes for account, USER_ID in one and USER_NAME in the other and, USER_ID and USER_NAME differ in format. These are not good candidates for re-configuration.

- If there are special attributes (native identity, managed attribute, entitlement) that split into multiple attributes in the new application type, re-configuration is not recommended.
  - Profiles in SAP –Full refer to both profiles and groups in the managed system, where as in SAP-Direct, profile refers to profiles and group refers to the groups in the managed system. These are not good candidates for re-configuration.

Before Application Re-configuration

Perform the following actions before you begin the re-configuration process:

- Backup the application xml and application type specific customizations such as rules and business processes.
- Plan the attribute mapping of the original and new applications for accounts and group schema. If there are attributes in the original application type that are not in the re-configured application type, you might lose some configuration and historical data.
- Check the provisioning policies of the target application and decide which policy to use, the policy from the original application type or the policy from the re-configured application type.

How to Re-configure an Application

Note: While re-configuring an application the target application must have a static schema and not a dynamic schema like JDBC or DelimitedFile connectors. There is the button named Discover Schemas to generate the schema.

1. Go to **Applications -> Application Definition** and select an application.
2. On the Application Configuration page, click the **Reconfigure** button to display the Select New Application Type dialog.

3. Select an application type from the **New Application Type** drop-down list and click **Save**.
4. Confirm your selection to go to the Application Configuration page in edit mode.
   The tabs that contain information requiring attention are marked with an red asterisk.
5. Go to the Attributes tab and enter the valid configuration attribute settings and test the connection.
6. Go to the Schema Mapping tab and map the Previous Schema Attributes to the New Application Type Schema Attributes for the Account and Group.
   Use the **Add Missing Attributes** and **Keep Extra Attributes** options to select to add missing attributes from the old (original) application type to the new application type, and to keep attributes that are on the new application type but were not on the original application type.
7. Go to the Provisioning Policy tab and select the provisioning policy to use for the re-configured application. It is recommended that you use the policy that corresponds to the application type of the newly re-configured application. You can use a different policy, but you must manually edit that policy to match the changes made during the re-configuration process.
8. Save the re-configured application.

After Application Re-configuration

Check the re-configured application for the following when the process is complete:

- Attributes that were not mapped might become not work and the values not get populated.
  - Unmapped attributes affect configurations, for example, policy or business roles, and context based historical data, for example viewing certification history, that is based on a population that relies on the attribute.
  - Related populations might not be populated with identities.
  - Pending provisioning operations that contain that attribute might fail.
  - Verify other place that use the attribute, such as identity mapping, account mapping, roles, policies, and policy violations.
- Verify the application definition for unwanted entries like build map rules or provisioning rules still exist.
- Perform account and account group aggregation.
- Perform refresh identity cube.
- Perform prune identity cube.

Activity Data Source Configuration

Use the Activity Data Source Configuration page to add or edit activity data sources. Activity collectors access activity data sources such as event or audit logs, collect the activity information that is to be monitored, and transform that data into a format that can be read by IdentityIQ. These Activity Data Sources are use for all activity aggregation and reporting.

Changes made on this page are not committed until a save is performed on the application with which they are associated. For example, if you add or delete a data source on this page and click **Save**, you do not see that change reflected on the application until you click **Save** on the application page and commit the change.

For each activity data source enter or edit the following:

- The general data source information in Table 9, “Configure Application Page Field Descriptions.
- Activity target information found on the Activity Target tab for each source type, see “Activity Targets” on page 22.
- The unique connection and query setting for each activity data source type.
  - “JDBC Collector Settings” on page 23
  - “Windows Event Log Collector Settings” on page 23
  - “Log File Collector Settings” on page 24
  - “RACF Audit Log Collector” on page 25
  - “CEF Log File” on page 26

Table 9—Configure Application Page Field Descriptions

Field	Description
Name	A short, descriptive name for the activity data source.
Description	A brief description of the activity data source.
Transformation Rule	The transformation rule required to convert the data collected from the data source into a format that can be used by IdentityIQ. **Note: Click the “...” icon to launch the Rule Editor to make changes to your rules if needed.**
Correlation Rule	The correlation rule that should be used to correlate the activity data collected with identities. **Note: Click the “...” icon to launch the Rule Editor to make changes to your rules if needed.**
Activity Data Source Type	The type of data source from which the activity is being collected. The **Activity Data Source Type** drop-down list contains the types of data source from which activity information can be collected. This list will grow and change to meet the needs of IdentityIQ users. **Note: When “CEF Log File” is selected from the drop down list, the “Transformation Rule” and “Correlation Rule” fields are displayed with the following respective values:** **- Transformation Rule: CEFTransformRule** **- Correlation Rule: CEFActivityCorrelation**

Activity Targets

The Activity Targets tab is used to specify targets within this data source for use in activity searches. A target is a specific object within a data source that is acted upon. For example, a target might be a machine name for a login action, or a file name for a create action.

The targets specified here are used to populate lists on the Activity Search page. These targets can be grouped with targets specified on other applications to create categories of targets. For example, if you have inventory applications at three different locations and a procurement database on each, you can set each procurement database as a target, create a Procurement category, and then collect activity for all three procurement databases using a single activity search.

See “Activity Targets” on page 22.

On the Activity Targets tab you can add activity targets for the data source with which you are working. Type the name of the activity target in the field at the bottom of the list and click **Add Activity Target**. To remove activity targets, use the selection boxes on the left of the table and click **Delete**.

JDBC Collector Settings

JDBC Connection Settings

IdentityIQ uses the connection settings to access the activity data source.

Table 10—Application Configuration - JDBC Collector Connection Settings

Field	Description
Connection User	A valid JDBC user with access to the data source being accessed by this collector.
Connection Password	The password associated with the Connection User if a password is required. The password is encrypted and is not displayed with the activity data source information.
Database URL	The full url to the activity data source. For example, `jdbc:mysql://localhost/db`
JDBC Driver	The driver class of the activity data source. For example, `com.mysql.jdbc.Driver`

Query Settings

The query settings are used to control the activity information that is collected when an Activity Aggregation task is run.

Table 11—Application Configuration - JDBC Collector Query Settings

Field	Description
SQL Statement	The SQL statement used to query activity from the database.
Condition Builder	Transforms the data mapped in the rule selected as the Position Builder into a SQL statement used by subsequent queries to determine start position.
Position Builder	Rule that converts the last row in the result set returned by the query into a configuration map that is persisted into the IdentityIQ database. The data that is mapped in this rule is used by the condition builder to create a SQL statement used in future queries to determine the start location. This enables IdentityIQ to perform scheduled activity aggregations without having to scan entire data sets with each subsequent aggregation.

Windows Event Log Collector Settings

Note: Before you can use the Windows Event Log Collector, the IQService must be installed and registered. Refer to your Installation Guide for information on installing and registering the IQService.

Event Log Settings

IdentityIQ uses the connection settings to access the activity data source and the query settings to control the activity information that is collected when an Activity Aggregation task is run.

Table 12—Application Configuration - Windows Event Log Collector Settings

Field	Description
User	Valid Windows user name with access to the event log containing the activity data.
Password	The password associated with the user specified.
IQ Service Host	The host name where the IQ service is running.
IQ Service Port	The listening port of the IQ service.
Event Log Server	The server where the activity data source resides.
Query String	The MQL query use to specify the activity data to collect during the activity aggregation.
Block Size	The number of events to retrieve with each activity aggregation performed on this activity data source.

Log File Collector Settings

Transport Settings

The transportation settings are used to access the server where the log file containing the activity data resides.

Table 13—Application Configuration - Log File Collector Transportation Settings

Field	Description
Transport Type — depending on the transport type selected you will see the following:	
local	If the log file containing the activity data is on the same server as IdentityIQ, no further connection-type information is required.
ftp	FTP User — a valid user name with authentication access to the FTP host. FTP Password — the password associated with the FTP user. FTP Host — the host where the log file resides.
scp	SCP User —a valid user name with authentication access to the SCP host. SCP Password — the password associated with the SCP user. SCP Host — the host where the log file resides. SCP Private Key — the private key that is used to encrypt the collected data.

Log File Settings

The log file settings are used to define the query used to collect the activity data.

Table 14—Application Configuration - Log File Collector Log File Settings

Field	Description
File Name	The name of the log file containing the activity data.

Table 14—Application Configuration - Log File Collector Log File Settings

Field	Description
Lines to Skip	The number of lines to skip before starting the scan for activity information.
Filter Nulls	Skip lines that don't conform to the defined format.
Multi-lined Data	A single record in this file spans multiple rows.
Regular Expression	A regular expression groups that can be used to tokenize each record in the file.

Log Fields

The log field settings are used to create the log fields based on the column headings in the log file.

Table 15—Application Configuration - Log File Collector Log Fields

Field	Description
Name	The name of the log field to create based on a column name from the log file.
Trim Value	Remove white space around the column name before creating the log field.
Drop Nulls	If the column by this name is null, ignore this record. For example, if the user field is null, then the record cannot be correlated to a IdentityIQ identity and, therefore, cannot be used by IdentityIQ.

RACF Audit Log Collector

Transport Settings

The transportation settings are used to access the server where the log file containing the activity data resides.

Table 16—Application Configuration - RACF Audit Log Collector Transportation Settings

Field	Description
Transport Type — depending on the transport type selected you will see the following:	
local	If the log file containing the activity data is on the same server as IdentityIQ, no further connection-type information is required.
ftp	FTP User — a valid user name with authentication access to the FTP host. FTP Password — the password associated with the FTP user. FTP Host — the host where the log file resides.
scp	SCP User —a valid user name with authentication access to the SCP host. SCP Password — the password associated with the SCP user. SCP Host — the host where the log file resides. SCP Private Key — the private key that is used to encrypt the collected data.

Log File Settings

The log file settings are used to define the query used to collect the activity data.

Table 17—Application Configuration - RACF Audit Log Collector Log File Settings

Field	Description
File Name	The name of the log file containing the activity data.
Lines to Skip	The number of lines to skip before starting the scan for activity information.
Filter Nulls	Skip lines that don't conform to the defined format.

CEF Log File

Transport Settings

The transportation settings are used to access the server where the log file containing the activity data resides.

Table 18—Application Configuration - CEF Log File Transport Settings

Field	Description
Transport Type — depending on the transport type selected you will see the following:	
local	If the CEF log file containing the activity data is on the same server as IdentityIQ, no further connection-type information is required.
ftp	FTP User — a valid user name with authentication access to the FTP host. FTP Password — the password associated with the FTP user. FTP Host — the host where the log file resides.
scp	SCP User —a valid user name with authentication access to the SCP host. SCP Password — the password associated with the SCP user. SCP Host — the host where the log file resides. SCP Private Key — the private key that is used to encrypt the collected data.

Log File Settings

The log file settings are used to define the query used to collect the activity data.

Table 19—Application Configuration - CEF Log File Settings

Field	Description
File Name	The name of the CEF log file containing the activity data.
Lines to Skip	The number of lines to skip before starting the scan for activity information.
Filter Nulls	Skip lines that do not conform to the defined format.
Multi-lined Data	A single record in this file spans multiple rows.
Regular Expression	A regular expression groups that can be used to tokenize each record in the file. The format of CEF Log File. For example, (\w\w\w\s\d\d\s\d\d:\d\d:\d\d)\s(.*)CEF:(.*)|(.*)|(.*)|(.*)|(.*)|(.*)|(.*)|(.*)(.*)

Log Fields

The log field settings are used to create the log fields based on the column headings in the log file.

Table 20—Application Configuration - CEF Log Fields

Field	Description
Name	The name of the CEF log field to create based on a column name from the CEF log file.
Trim Value	Remove white space around the column name before creating the CEF log field.
Drop Nulls	If the column by this name is null, ignore this record. For example, if the user field is null, then the record cannot be correlated to a IdentityIQ identity and, therefore, cannot be used by IdentityIQ.

IdentityIQ uses connectors to extract data and transform it into a format it can read. A connector is a Java class that extends the IdentityIQ `AbstractConnector` class and implements the IdentityIQ Connector interface. Connectors provide the means by which IdentityIQ communicates with targeted platforms, applications and systems. Each application type requires different information to create and maintain a connection. For detailed connector information refer to the connector documentation delivered with IdentityIQ.

Native Change Detection Configuration

IdentityIQ can be configured to detect native changes on applications with which it communicates during the aggregation process and launch business processes accordingly. Native changes are, changes made directly to an account on an application that were not processed as part of an IdentityIQ request.

Once enabled, aggregation will start detecting changes (while filtering IIQ requested items) and storing them with other Life Cycle Events on the identity. If you make native changes you will see them being stored on the Identity object.

To configure IdentityIQ to detect native changes during aggregation, do the following:

Note: For Native Change Detection to operate you must have both a life cycle event defined and the application enabled.

1. Run an aggregation to obtain the baseline information for the application.
2. Configure a Native Change life cycle event on the Life Cycle Events page.
   There are two life cycle change events included with IdentityIQ and you can configure your own as needed:

   Lifecycle Event - Email manager for all native changes:

   Sends a formatted email to the manager describing the changes detected.

   Lifecycle Event - Manager Approval for all native changes:

   Generates an approval work item for each change detected. Any items rejected are undone/reversed and provisioned. This business process also creates an access request within IdentityIQ so that once the changes are made they will be visible from the Access Request page.
3. Go to **Applications -> Application Definition** and select an application.
4. Select Native Change Detection on the Application Configuration page.
5. Define the operations to include when detecting native changes - **Create**, **Modify**, **Delete**.

6. Define the attributes to compare when detecting native changes:
   Entitlements: All entitlement attributes
   User Defined: Manually enter the names of the attributes to compare.
7. Run or schedule aggregations to detect and store any changes.
8. Run an Identity Refresh task with the Process Events option enabled to trigger the life cycle events for any changes detected since the last time the events were processed.