IdentityIQ Identity Management

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

Contents

Identity Management **1**

Identity Warehouse Page **2**

Identity Details Page **3**

Attributes Tab 3

Entitlements Tab 3

Roles 4

Entitlements 4

Application Accounts Tab 4

Policy Tab 5

History Tab 6

View Identity History Page 7

Risk Tab 7

Activity Tab 7

User Rights Tab 8

Capabilities Access 9

Events Tab 9

Events 9

Access Requests 10

Identity Correlation **12**

Select Uncorrelated Accounts Panel 12

Select Target Identity Panel 13

How to Perform Manual Identity Correlation 14

Identity Management

Use the Identity Warehouse page to create, view and edit individual Identity Cube information. Identity Cubes are multi-dimensional data models of identity information that offer a single, logical representation of each managed user. Each Cube contains information about user attributes, entitlements, accounts, policy violations, risk scores,rights and capabilities within IdentityIQ, and historical records of user access configurations and activity.

The Identity Management area includes:

- **Identity Warehouse Page** — basic user information for every user in your organization.
- **Identity Details Page** — clicking on any identity in the Identity Warehouse page opens detailed information for that identity.
- **Identity Correlation** — manually correlate the Identity Cubes created when identity aggregation was performed on your identity authoritative sources with any user accounts discovered while performing aggregations on other applications.
- **Identity Risk Model** — configure your organization's risk model for roles, entitlements, and policy violations, and configure your risk scoring.. For information on the Identity Risk Model, see the **Risk** documentation. You can view a risk scorecard for each identity in the Identity Warehouse on the Risk Tab in the detailed view of the identity. You can also see lists of identities that fall into specific risk levels under the **Intelligence > Identity Risk Scores** menu. See the **Risk** documentation for more information.

Access to these pages is controlled by IdentityIQ Capabilities and Scope. Contact your system administrator if you need help to access to the se areas of IdentityIQ.

Identity Warehouse Page

The Identities table contains basic user information for every identity discovered during the latest aggregation process. Identities can include non-human identities, such as service accounts and bot identities, as well as users

> By default, only active identities are displayed.

> Many columns in the table can be sorted. Click the column title to sort the table by the entries in that column in ascending order. Click again to sort the table in descending order. You can also click the associated drop-down menu to sort or to add or remove columns in the table.

To **Search** for identities, enter a letter, or combination of letters into the **Filter By Identity Name** field above the list of identities. Then click the search icon (magnifying glass) to find identities that have that letter combination in their name.

The Identity Warehouse listing contains this information for each identity:

Column Name	Description
User Name	The user's account ID or login name.
First Name	Full first name of the user.
Last Name	Full last name of the user.
Manager	Name of the manager for the user.
Assigned Role Summary	A complete list of all roles assigned to the user.
Detected Role Summary	A complete list of all detected roles for the user.
Risk Score	The composite risk score for the user. Risk score is determined by numerous factors defined during configuration.
Last Refresh	The date of the last identity refresh.
Type	The type assigned to this identity, Employee, Contractor, External/Partner, RPA/Bots, or Service Accounts.
Location	The physical location of the user. For example, Chicago or Singapore.
Region	The corporate region assigned to the user. For example, Americas or Asia-Pacific.

Click any identity to display the View Identity page.

Identity Details Page

Use the View Identity page to view detailed information about each component of the Identity Cube for a selected user.

The Identity Details page contains the following option:

- Attributes Tab
- Entitlements Tab
- Application Accounts Tab
- Policy Tab
- History Tab
- Risk Tab
- Activity Tab
- User Rights Tab
- Events Tab

Attributes Tab

The Attributes tab provides the basic user identity information such as first name, last name, email, manager, and employee type..

You can also update information about the user from this tab, using these options:

Edit

Click to modify attribute values as needed. This option is restricted based on user capabilities and is not available to every user.

Manager

The manager to whom the user reports directly. Click the manager name to display the View Identity page for that user.

Change Password

Set or update a password for the user. If you want to require the user to change their password the next time they log in to IdentityIQ, select the check-box below the password confirmation field

Change Forwarding User

The forwarding user is a user or workgroup to whom work items assigned to this identity can be forwarded. You can use the **Start Forwarding** and **End Forwarding** options to set a specific time period when forwarding should occur (for example, if the user is on leave).

Entitlements Tab

The Entitlement tab lists all of the roles and entitlements for the selected user.

You can use **Advanced Search** for both roles and entitlements, to find access based on a variety of criteria, such as how it was assigned, whether is has been requested or is pending approval, and whether it has been certified.

The entitlements tab includes this information:

Roles

A list of roles that were detected or assigned to the user manually or through role assignment rules. **Assigned roles** are typically business-type roles that model how users are grouped by business function, including functional hierarchies, project teams, or geographic location. **Detected roles** are roles that are detected by IdentityIQ during the aggregation and correlation processes based on the entitlements assigned to an identity.

If an activation or deactivation date is defined for the role it is displayed in a message box below the role name.

Name — name of the role. Click the name to view detailed information about the role.

Description — brief description of the role.

Classifications — if the role has a classification that categorizes it as potentially allowing access to sensitive, protected, or otherwise significant data, an icon is shown to flag the classification

Assigned By — the user that assigned this role to the identity.

Allowed By — the assigned roles that permit a user to have this role, either directly or indirectly. A direct permission is one in which the assigned role is a member of the permitted role. An indirect permission is one in which the assigned role is on the permitted list for the assigned role.

Acquired — how the role was acquired.

Application — the application associated with the role.

Account Name — the application account the role is mapped to.

Entitlements

A list of the applications that have entitlements to which the identity has access. Click the entitlement or application name to view the entitlement details, if available.

When an information icon is displayed, you can hover over it to view more details.

If the entitlement has a classification that categorizes it as potentially allowing access to sensitive, protected, or otherwise significant data, an icon is shown to flag the classification

Select **Show only additional entitlements** to limit the list to entitlements that are not included in a role assigned to the user.

> If any of the roles or entitlements displaying has elevated access, they will have the Elevated Access icon next to the name or entitlement.

Application Accounts Tab

The Applications Accounts tab lists account information for all of the applications to which the user has some level of access.

Column Name	Description
Application	The name of the applications to which the user has some level of access. Click on an application name to view detailed information.
Account Name	The simple name used to identify the user on the application.
Status	Values can include: **Disabled** - the account has been disabled by an admin at some point. **Locked** - the user is locked out after too many password attempts. **Active** - the account is not disabled or locked.
Last Refresh	Date on which the user identity information was last refreshed.

To remove the link between the identity and the application in IdentityIQ, select an account in the table and click **Delete**. This action does not affect the user's account or entitlements on the application.

To transfer the account to a different identity, select an account and click **Move Account**. On the Select Account Owner dialog, select an existing identity from the list or create a new identity. To select an existing identity enter the first few letters of the identity name to display a suggestion list, or click the arrow next to the field to display a list of all identities to which you have access.

Policy Tab

The Policy tab shows policy violations for the user. The table contains the policy and rules that are violated.

Policies are composed of rules used to enforce your organization's policies. For example, a separation of duty rule might be defined that disallows a single user from having roles that enable them to both request and approve purchase orders.

For more information about policy violations, see the **Policies** documentation.

The Policy tab includes the following information:

Column Name	Description
Detected	The date when the policy violation was detected.
Policy	The policy that is violated.
Policy Violation Owner	The owner of the policy. The owner is assigned during the policy definition process.
Rule	The specific rule that is being broken to cause the violation in the policy. Click a rule to display the following rule information: **Policy Description** — brief description of the violation as defined with the policy. **Policy Violation Owner** — the owner of the policy with which you are in violation. **Rule Description** — brief description of the rule from the rule definition page.

Column Name	Description
	Compensating Control — any compensating controls associated with this rule. **Correction Advice** — advice on how to correct the violation as entered when the rule was created.
Summary	The reason for the violation.

History Tab

The History tab provides a history of user data. Tracking identity scores over time enables you to identity patterns or trends in the activity of a selected user.

The History tab contains the following information:

Column Name	Description
Identity Snapshots	
Snapshot Date	The dates of the identity snapshots. Click on a snapshot date from the table to view details about attributes, roles, entitlements, and application accounts in the View Identity History page. Snapshots are generated when a certification is run, and when the **Maintain identity histories** option is used in the identity refresh task. The frequency with which snapshots are generated is set in **gear > Global Settings > IdentityIQ Configuration** on the **Identities** tab. See the **System Configuration** documentation for more information.
Roles	A list of the IT roles assigned to this user. The snapshot does not display Business roles.
Identity Certification History	
Decision	Displays an icon that indicates the decision made on the certification. Options include Approved, Revoked, Allowed Exception, or Delegated. For detailed descriptions of decisions, see the **Certifications** documentation
Type	The type of certification. For example, Role or Additional Entitlement.
Description	Brief description of the certification.
Application	The application to which the certification applies.
Account Name	The account name to which the certification applies.
Actor	The person who signed off on the certification.
Date	The date when the certification decision was made.
Comments	Any comments entered during the decision phase of the certification.

Click any row in the Identity Certification History panel to see an overview of that specific portion's certification history.

View Identity History Page

The View Identity History page contains user information from the specific date and time listed on the top of the page.

The View Identity History page contains four tabs:

- **Attributes** — the identity attributes.
- **Roles** — roles assigned to this user and all of the associated entitlements.
- **Extra Entitlements** — all entitlements assigned to this user that are not part of a role assigned to the user.
- **Application Accounts** — all applications on which this user has an active account, along with the account name, and the user's full identity.

Risk Tab

The Identity Risk Tab provides a current composite identity risk score with a list of the raw and compensated risk score for each category used to derive the composite score. This page also provides a list of the top composite score contributors which provide further information on how the score was derived. This information helps to provide clues on the areas of highest risk. These scores are based on the latest information discovered.

IdentityIQ uses a combination of base access risk and compensated scoring to determine the overall Identity Risk Scores, or Composite Risk Score, used throughout the application.

Base access risk score is a measure of inherent user access risk. Base risk scores are set on each role, entitlement, and policy defined. This type of score ranges from 0 (lowest risk) to 1000 (highest risk).

A series of compensating factors are applied to each base risk score to calculate compensated scores. These compensated scores are then weighted using a maximum contribution percentage and combined to form an overall Composite Risk Score for each user.

The compensating factors and weighted values enable you to identify high risk users based on more than the roles they are assigned in your enterprise.

For more information about risk modeling in IdentityIQ, see the **Risk** documentation.

Activity Tab

The View Identity Activity tab provides a list of all applications that have activity monitoring enabled and to which a user has access, including the roles associated with those applications and the activities performed.

The Recent Activities table initially lists the last ten (10) actions performed. Click **See All Activities** to include all of the activities stored by IdentityIQ on the table.

From this tab you can also enable activity monitoring for this user on specific applications that do not have activity monitoring enabled at the role level.

> Changes made to activity monitoring do not appear until identity aggregation is performed from the task page, or a scheduled identity aggregation takes place.

To enable activity monitoring for this user on the associated applications and roles, select the **Activity Monitoring** check-box next to the Activities Settings table.

To display additional activity information in the Activity Details panel, click an activity entry in the Recent Activities list.

The View Identity Activity tab contains the following information:

Column	Description
Activity Settings:	
Activity Monitoring Checkbox	Enable activity monitoring for this user on the specified application. If this box is not active, activity monitoring is already enabled at the role level or the application does not allow activity monitoring.
Applications	The list of applications to which this user has some level of access.
Activity Enabled Roles	The list of roles that are all of the following: • assigned to this user • associated with the application • have activity monitoring enabled Activity monitoring is enabled when roles are defined.
Recent Activities:	
Date	The date on which the activity occurred.
Action	The activity performed on the application. For example, Login, Update, Delete.
Target	The specific part of the application that was targeted by the activity. For example, the name of a particular database that was updated.
Application	The application on which the activity was performed.
Result	The result of the activity. For example, Success or Failure.

User Rights Tab

The User Rights tab enables you to set the capabilities and define controlled scope for the user. Capabilities determine which features in IdentityIQ the user can access.

> The scope feature MUST be enabled in order for the scope information to display.

Field Name	Description
User Capabilities	The SailPoint capabilities available. The capabilities currently assigned to the user are highlighted on the list. Contact your support representative for a full list of the Capabilities available. Use the Ctrl and Shift keys to select multiple capabilities.
Assigned Scope	The scope the identity belongs to.
Can Access Assigned Scope	Select this option to enable the identity to have access to the scope to which they are assigned. If this field is set to False, the user will not have access to objects within the scope to which they are assigned. If the field is set to Use System

Field Name	Description
	Default (<value>), the user's access is based on the value of the setting defined in the Global Settings for IdentityIQ.
Authorized Scopes	The scopes the user has access to. If scopes are active, identities can only see objects that are within the scopes they have access to. Assign scopes to the identity using the field at the top of the Authorized Scopes list box. • Click the arrow to the right of the field to display a list of all scopes defined. • Enter a few letters in the field to display a list of all scopes that start with that letter string. Depending on configuration, objects with no scope assigned might be visible to all users with the correct capabilities.
Workgroups	The workgroups to which this identity belongs
Indirect Rights	IdentityIQ capabilities assigned to a workgroup to which this user belongs. Workgroup members automatically have the capabilities and scopes assigned to the workgroup.

Capabilities Access

The capabilities an identity is assigned dictates which tools, pages, or tabs are accessible within IdentityIQ. A complete list of IdentityIQ default capabilities and their associated features is available on Compass.

> System Administrator has access to all IdentityIQ features including Global Settings, and Debug.

Events Tab

The Events tab enables you to view events that are scheduled for the user as well as detailed access request history.

The Events tab includes two sections - Events and Access Requests.

Events

The Events list has two sections:

- Future Events shows scheduled role sunrise and sunset events.
- Past Events shows Identity Triggers and role sunrise/sunsets events that have been executed.

Select event and click **Delete** to cancel that event and remove the schedule from the list.

Field Name	Description
Created On	The date when the event schedule was created.
Created By	The identity that scheduled the event.

Field Name	Description
Due On	The date when the event is scheduled to occur.
Summary	A brief summary of the event that is pulled from the business process with which it is associated.

Access Requests

Click on a item in the list to display detailed information about requested items and any pending actions that still need to be taken on that request. From the detailed history panel you can navigate further into the request to expand the details view, review the actual access request, and send messages to owners of the request reminding them that their action is required.

Click the **X** icon to cancel a request.

To search for specific access requests, click **Search** to expand the search criteria. Specify the search criteria and click **Search**. To clear the criteria for a new search, click **Reset**.

Column Name	Description
Access Request ID	Identification number assigned to the access request.
Priority	Specifies the priority level to which the access request was designated.
Type	The type of access request.
Description	The a brief description of the access request.
Requester	The name of the user who assigned this work item to you.
Requestee	The name of the user who was assigned this access request.
Request Date	The date the request was made.
Current Step	Status of the request. Status levels include: **Pending** — Request was received but no action has taken place. **Approved** — Request was approved. Additional action may be needed to complete the request. **Rejected** — Request was denied. **Completed** — All actions required for this access request have been fulfilled. **Cancelled** — Request was cancelled. **Completed Pending Verification** — The manual action for this request was completed, however the verification procedure has yet to have been run.
Completion Date	The date when the work item was completed.
Execution Status	Status of the request execution. Status levels include: **Executing** — The request is going through the business process and has not completed.

Column Name	Description
	Verifying — The request has finished the business process and is waiting for the Provisioning Scanner to verify it. **Terminated** — The request was terminated before it was completed. **Completed** — The request was completed and verified.

Identity Correlation

Use the Identity Correlation page to maintain the IdentityIQ Identity Cubes which contain information about an individual user's entitlements, activity and associated business context. Identity Cubes are created when identity aggregation is performed on your identity authoritative source. An example of an identity authoritative source is a human resources application that is the main repository for employee information and the data source that is used to build most Identity Cubes.

> If user accounts are discovered on at-risk applications that do not correlate to the IdentityIQ identities that were created based on the employee information in your identity authoritative sources, it may indicate a risk situation that needs to be addressed.

Because each Identity Cube is associated with an identity authoritative source, it provides a single representation of each managed identity and associated user accounts. However, user accounts on applications may not correlate to IdentityIQ identities. Some examples include the following:

- An employee who no longer works for your enterprise. They were removed from the human resources application, however, their account was not removed from every application to which they had access.
- Mismatched or redundant accounts. Accounts that were created on different applications at different times or by different administrators using variations of the employee's name; Tom Jones, Thomas Jones, and tjones.

To display detailed information about the account or identity, click an account ID or name. The details panels for an account and an identity can be open at the same time for comparison before you perform a merge.

Accounts that are manually assigned to identities from this page can be reassigned if necessary from the identity Application Accounts tab. See Application Accounts Tab.

Use the Correlated column of the Select Target Identity panel to manually change the correlation status of specific accounts.

The Identity Correlation page is divided into two panels:

- Select Uncorrelated Accounts — a list of the accounts on a specific application that are not correlated with an account detected on an authoritative source. See Select Uncorrelated Accounts Panel .
- Select Target Identity — a list of all accounts detected on all applications monitored by IdentityIQ. See Select Target Identity Panel.

Make selections in each panel to perform manual correlation. See How to Perform Manual Identity Correlation.

Select Uncorrelated Accounts Panel

The Select Uncorrelated Accounts panel displays a list of the accounts on a specific application that are not correlated with an account detected on an authoritative source. From this list you can select accounts to merge with identities.

Select an application from the **Search** drop-down list or enter the first few letters of an application name and make a selection from the suggest box to populate the table. Use the filtering options to reduce the number of accounts displayed at one time.

Use the Included Account Types filter to exclude specific account types from the uncorrelated list. For example, certain account types such as Service or Privileged accounts may never be assigned to specific users and, therefore, should

never be correlated with a specific Identity Cube. To exclude a specific account type from the uncorrelated accounts list, click **Included Account Types** and clear the check-box associated with that account type on the drop-down list.

Click an Account ID to display detailed account information.

The Select Uncorrelated Accounts panel contains the ID and user name associated with the account and the date the account was created, along with the following options:

> The columns on this page can be configured and may display differently in your enterprise.

Column	Description
Account ID	Unique identifier associated with the account
Account Name	Name associated with the account.
Create Date	The date when the account was created.
Inactive Account	Inactive accounts have a value of true. This column can be used for account type filtering.
Last login	The date when the account was last accessed.
Service Account	Mark accounts as service accounts if appropriate. This column can be used for account type filtering.
Privileged Account	Privileged accounts have a value of true. This column can be used for account type filtering.

Select Target Identity Panel

The Select Target Identity panel contains a list of all accounts detected on all applications that IdentityIQ monitors. From this list you can select an identity with which to merge the uncorrelated accounts on the selected application.

Use the filtering options to display specific identities or click the filter icon to display every identity in IdentityIQ. Enter a letter string and click the search icon to search by user name or click **Advanced Search** for more options.

Click a Name to display detailed information about the selected identity.

The Select Target Identity panel contains the a variety of information about the identity, including the following:

> The columns on this page can be configured and may display differently in your enterprise.

Column	Description
Correlated	> This column is read only. Making changes here does not change the state of the account. The correlation status of the identity. Accounts marked as correlated no longer display on the uncorrelated accounts list or reports.

Column	Description
Manager	Manager listed for this identity.
Email	Full email address.
Inactive	Current status of the identity account, active or inactive.
Last Refresh	The date when the last identity refresh was performed on this identity cube.
Advanced Search Options:	
Standard Attributes:	
Standard attributes include name, username, email, and manager fields. Enter a letter string in any of these fields to return a list of identities that have a matching string in that identity attribute value. For example, typing st in the first name field returns Steve and Hester.	
Inactive	**True** - only show active identities **False** - only show inactive identities
Correlated	**True** - only show correlated identities **False** - only show uncorrelated identities
Searchable Attributes: Searchable attributes are defined during configuration and vary for each installation of the product.	

How to Perform Manual Identity Correlation

To perform identity correlation complete the following steps:

1. Click **Identities > Identity Correlation**.
2. Choose which application to correlate identities for: select an application from the **Search** drop-down list or enter the first few letters of an application name and make a selection from the suggest box to populate the table. This table contains a list of the accounts on a specific application that are not correlated with an account detected on an authoritative source.
3. Select the accounts to merge with identities that were created during the aggregation of your authoritative sources.
4. In **Select Target Identity**, select an identity to merge with the uncorrelated accounts selected in step 3. Use the filtering options to display specific identities or click the filter icon to display every identity in IdentityIQ. Enter a letter string and click the search icon to search by user name or click **Advanced Search** for more options.
5. Select an identity account to merge with the accounts selected in the **Select Uncorrelated Accounts** panel.
6. Click **Perform Merge** to perform the merge for these identities.

   The merge removes the accounts from the **Select Uncorrelated Accounts** table.