IdentityIQ Advanced Analytics

Version: 8.2

Revised: June 2021

Copyright and Trademark Notices

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

Contents

Advanced Analytics Overview

Advanced analytics enable you to create specific queries based on numerous aspects of IdentityIQ. These searches can be used to determine specific areas of risk and create interesting populations of identities.

Search results can be saved for reuse or saved as reports. In some cases, you can save your results as interesting populations of identities. When you save a search as a report, you can schedule the search on an continuous basis for monitoring and tracking purposes. When you save the search criteria as a population, you can use activity monitoring and statistical reporting of identities that fit that criteria in the same way that you use them for groups.

You can access the search page from the navigation menu bar, **Intelligence -> Advanced Analytics**. Select a **Search Type** from the drop-down menu and enter the search criteria.

IdentityIQ advanced analytics is made up of the following search types:

- Identity Search — generate searches on specific attributes of the users in your enterprise.
- Advanced Search — generate ad-hoc searches using boolean operations.
- Access Review Search — generate searches based on certification criteria.
- Role Search — generate searches on the roles in your enterprise.
- Entitlement Search — generate searches on entitlements in your enterprise.
- Activity Search — generate searches on activity over specific time periods and on specific applications, identities, groups, populations or targets.
- Audit Search — generate searches for audit records for specific time periods and for specific actions, sources, and targets.
- Process Metrics Search — generates searches based on business process metrics criteria.
- Access Requests Search — generates searches for current and archived access requests.
- Syslog Search — generates searches for specific technical support related information that relates to your IdentityIQ installation.
- Account Search— generates searches based on the accounts in your enterprise. These searches can find accounts by application, display name, owner, native identity, instance or any combination of these criteria.

For search that offer the Advanced Search option, see Advanced Search.

To view your search results, see Search Results

Identity Search

Generate searches on specific attributes of the identities in your enterprise. You can use these searches to determine specific risk areas or to define interesting populations of people from multiple organizations, departments and locations.

See Identity Search Criteria

Search results can be saved for reuse or saved as reports. In some cases, you can save your results as populations of identities.

- When you save a search as a report, you can schedule the search on an continuous basis for monitoring and tracking purposes.
- When you save the search criteria as a population, you can use activity monitoring and statistical reporting of identities that fit that criteria in the same way that you use them for groups.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Identity Search Criteria

The search criteria text fields support partial text strings using a starts-with protocol. For example, if you input “ro” in the Last Name field, the search results include Thomas Rowen and Betty Roberts.

Your use search criteria is used to narrow the search results. If you do not type information in a search criteria field, all possible choices are included. For example, if you do not select an application from the **Applications** list, all applications are included.

> If the Load Saved Search panel displays, the search criteria for that search is loaded on the page. To create a new search click Clear Search.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results. For example, if you search by **First Name** John and **Last Name** Doe, the search results include only users with the character string John in their first name and Doe in their last name.

Use the **Fields to Display** panel on the right to select the identity and risk fields to display on the search results page.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Identity Search page has the following information:

Identity Attributes

Criteria	Description
Identity Attributes Identity attributes are pulled from the identity mapping information that is set during deployment and configuration. You can use full names or partial strings in the text fields. For example, “ro” in the Last Name field returns Roberts and Brown.	
Searchable Attributes Searchable Attributes are attributes you created and that are designated as Searchable when an identity is generated during deployment and configuration. For example, Department, Organization or Location.	
Last Name	Last name criteria to use in the query.
First Name	First name criteria to use in the query.
User Name	User name criteria to use in the query.
Display Name	The identity name in IdentityIQ.
Email	Email address criteria to use in the query.
Manager	Manager criteria to use in the query. The Identity search results include all users that report to managers that match the criteria in this field.
Is Inactive	Select **True** to include identities currently marked inactive or **False** to include identities that are currently active in the search results.
Is Manager	Select **True** to include identities that are marked as manager or **False** to include identities that are not marked as manager in the search results.
Type	Employee type: - Employee - Contractor - External Partner - RPA/Bots - Service Accounts
Software Version	**Only applicable to RPA/Bots** Software version associated with the Robotic Process Automation (RPA) /bots.
Administrator	**Only applicable to RPA/Bots**

Criteria	Description
	The administrator of the Robotic Process Automation (RPA) /bots.
Applications	Select the applications to include in the search. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications or type a few letters in the field to display a list of applications that begin with that letter string. Identities need to match only one of the selected items to be included in the search results
Detected Roles	Select the detected roles to include in the search. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles or type a few letters in the field to display a list of roles that begin with that letter string. For hierarchical roles, the identity is included in the search results with each role in the hierarchy not only the highest level role.
Instance	The attribute that uniquely identifies a specific subdivision of an application.
Assigned Roles	Select the assigned roles to include in the search. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles or type a few letters in the field to display a list of roles that begin with that letter string. For hierarchical roles, the identity is included in the search results with each role in the hierarchy not only the highest level role.
Workgroup	Select the workgroups to include in the search. If no workgroups are specified, all workgroups are included.
Include Assigned Role Hierarchy	Select to include roles that are inherited from the assigned roles you selected for your search.

Entitlements

Criteria	Description
Entitlement Filters Select an application, attribute name and entitlement then click **Add** to filter by your selection.	
Entitlement Metadata Filter your search to include identities with entitlements meet specific IdentityIQ-related criteria.	
Certification	**Has uncertified entitlements** — Use the drop-down list and select True or False to specify search results that include identities that have uncertified entitlements. **Has entitlements pending certification** — Use the drop-down list and select

Criteria	Description
	True or False to specify search results that include identities that have entitlements with pending certifications.
Request	**Has entitlements that were not requested** — Use the drop-down list and select True or False to specify search results include identities with entitlements that were not requested. **Has pending requests for entitlements** — Use the drop-down list and select True or False to specify search results that include identities that have entitlements with pending access requests.
Other	**Aggregation Status** — Specify if the search must include identities whose entitlements are associated with applications that are Connected or Disconnected for aggregation. **Is Assigned** — Use the drop-down list and select True or False to specify search results that include identities with entitlements were assigned and not detected.

Multi Valued Attributes

Criteria	Description
Multi-Valued Attributes: By default, IdentityIQ does not come pre-configured with any multi-valued attributes. Multi-valued attributes are created during deployment and configuration. To limit the search, add values associated with a multi-valued attribute.The search results include the member list for the selected values. Use the and/or operator to define the search criteria. For example, for multi-valued identity attributes you can search by cost center or projects that have multiple values on multiple applications. For multi-value account attributes you can use group membership for specific accounts such as payroll or strategy and planning.	
Certification Score	The sum of compensated risk scores associated with certifications.

Risk Attributes

Risk scores and compensating factors are defined when IdentityIQ is configured.

Criteria	Description
Composite Score	The total composite risk score for the identity.
Role Score	The sum of the compensated risk scores of each role assigned to this identity. To determine the compensated role risk score, compensating factors are applied to the role base risk score.
Role Score (Base)	The sum of role base risk scores. This score does not account for the compensating factors defined for role risk scoring.

Criteria	Description
Entitlement Score	The sum of the compensated risk scores of each entitlement assigned to this identity. To determine the compensated role risk score, compensating factors are applied to the entitlement base risk score.
Entitlement Score (Base)	The sum of entitlement base risk scores. This score does not account for the compensating factors defined for entitlement risk scoring.
Policy Score	The sum of compensated risk scores associated with policy violations as defined when IdentityIQ was configured. Policies do not affect identity risk scores until a violation occurs.
Certification Score	The sum of compensated risk scores associated with certifications.

Access Review Search

Use the Access Review Search page to generate searches for access review records. These searches can find access reviews by certifier, identity to be certified, access review type, access review phase, completion percentage, significant dates, tags or any combination of criteria.

See Access Requests Search Criteria

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Access Review Search Criteria

The search criteria text fields support partial text strings using a starts-with protocol. For example, if you input “ro” in the Last Name field, the search results include Thomas Rowen and Betty Roberts.

Your use search criteria is used to narrow the search results. If you do not type information in a search criteria field, all possible choices are included. For example, if you do not select an application from the **Applications** list, all applications are included.

> If the Load Saved Search panel displays, the search criteria for that search is loaded on the page. To create a new search click Clear Search.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results. For example, if you search by **First Name** John and **Last Name** Doe, the search results include only users with the character string John in their first name and Doe in their last name.

Use the **Fields to Display** panel on the right to select the identity and risk fields to display on the search results page.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Access Review Search page has the following information:

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. These Saved Searches are only available for your use. To make searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of the current saved query.	
Run Search	Run the search with the criteria displayed on the current page. If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.
Unload the Loaded Saved Search and clear all query options.	Clear Search.
Delete Search	Delete the specified Loaded Saved Query.
Access Review Attributes:	
Name	The name that you assigned to the access review when the access review was created. The search results include all access reviews that meet a specific criteria. The search is case-insensitive. You can type the entire name or a portion of the name. For example, you can type “mycert” to include that specific name or you can type “m” to include all access reviews that begin with the letter “m.”
Certifier	The identity or workgroup that is assigned the access review request. The search results include all access reviews assigned to the value specified. Click the arrow to the right of the suggestion field to display a list of all certifiers or type a few letters in the field to display a list of identities or workgroups that begin with that letter string.
Identity	An identity in access review requests. The search results include all access reviews that have the specified identity. Click the arrow to the right of the suggestion field to display a list of all identities or type a few letters in the field to display a list of identities that begin with that letter string.
Type	Select an access review type from the drop-down list. The access review type can display additional options to filter the search.
Phase	Select an access review phase to limit the search. Review phases include Active, Challenge, Remediation, End.
Percentage Complete	Limit the search results by a percentage complete. Type a percentage in the field to the right and set the operator, greater than or less than.

Criteria	Description
Tags	Tags are assigned when access reviews are scheduled. You can use tags to classify access reviews for search and report purposes. The drop-down list has all the tags assigned to access reviews that you can access.
Filter By: **The following fields are displayed based on the Type of access review selected in the Type field. If no type is specified these fields are not displayed.**	
Manager Attributes	Specify a manager to include in your search for access review requests. Click the arrow to the right of the suggestion field to display a list of all managers or type a few letters in the field to display a list of manager names that begin with that letter string.
Group	Select a group or population to include in the search for access review requests. Note: The search results include access reviews assigned to the group or population. To display the valid options., click the arrow to the right of the Group and Value fields.
Application Attributes	Specify an application to search for access review requests. Click the arrow to the right of the suggestion field to display a list of all applications or type a few letters in the field to display a list of application names that begin with that letter string.
Role Attributes	Specify a role to search for access review requests. Click the arrow to the right of the suggestion field to display a list of all roles or type a few letters in the field to display a list of role names that begin with that letter string.
Account Group Attributes	Specify an account group and application to search for access review requests. Click the arrow to the right of the suggestion field to display a list of all account groups or applications or type a few letters in the field to display a list of account groups or applications that begin with that letter string.
Filter By: Date	
Date Type	Select an access review state for the dates specified. Review states include Created, Expiration, Signed or Finished.
Start Date	Specify a date to begin this search. For example, if you selected a type of Create, the search results include any access reviews created on or after the specified date.
End Date	Specify a date to end this search. For example, if you selected a type of Create, the search results include any access reviews created on or before the specified date.
Filter By: Signed Status	

Criteria	Description
Status	Specify access reviews by Signed or Unsigned status. Use the drop-down list to select **True or False**.
E-Signed	Specify access reviews by Electronic Signature status. Use the drop-down list to select **True or False**.
Signed By	Specify access reviews by the identity who signed off.
Fields to Display:	
Fields to Display	Specify the information displayed on the Access Review Search Results page associated with this search. The fields displayed change based on the type specified. Each field defines a column on the results table. You must select at least one field to display on the results page.

Role Search

Use the Role Search page to generate searches based on the roles in your enterprise. These searches can find roles by name, owner, type, or status. You can also search for roles by the number of users to whom they are assigned, manually or through role assignment rules, the number of entitlements they contain, their risk score weight, their association to other roles, the last time they were assigned or certified, or any combination of that criteria.

See Role Search Criteria

For example, you can identify roles that were created but are not being used by searching for setting **Detected Total** and **Assigned Total** to less than one (1).

> The Refresh Role Indexes task must have run at least once before a roles search will yield results.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on an on-going basis for monitoring and tracking purposes. See the **Reports** documentation.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Role Search Criteria

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Role Search page has the following information:

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you have saved to reuse at a later time. These Saved Searches are only available for your use.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	Run the search with the criteria displayed on the current page. If you have modified the criteria of the Loaded Saved Search, the search used the modified criteria.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Role Attributes:	
Name	Enter a role name to include in the search. Entering a string of characters returns all roles with that string in their name that your controlled scopes enable you to view. For example, if you enter admin the search results include information for the roles System Administrator, SysAdmin, and Administrative Assistant.
Display Name	Enter a display name to include in the search. Entering a string of characters returns all roles with that string in their display name that your controlled scopes enable you to view. For example, if you enter System Administrator the search results include information for the display name System Administrator.
Owner	Enter the role owner to include in the search. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Type	Select the role type to include in your search. For example, IT, Organizational, or Business. Role types are defined for your enterprise during the role modeling process.
Status	Select the Enabled/Disabled status of the roles to include in the search.
Classification	Classifications can identify roles as potentially allowing access to sensitive, protected, or otherwise significant data. Choose any classifications to include in the search.
Detected Total	Specify an upper or lower limit for the number of identities that have this role detected that should be included in the search results.

Criteria	Description
	Detected roles are roles that are automatically assigned to identities based on the entitlements to which they have access. For example, to search for roles that were not detected by any identity during correlation, select Less Than from the drop-down list and type 1 in the empty field. The search results include all roles that were not automatically assigned to at least one identity.
Assigned Total	Specify an upper or lower limit for the number of identities that have this role assigned that should be included in the search results. Assigned roles are roles that were manually assigned to an identity by a user with role assignment authority or through a role assignment rule. For example, to search for roles that were not assigned to any identity, select Less Than from the drop-down list and type 1 in the empty field. The search results include all roles that were not manually assigned to at least one identity.
Entitlement Total	Specify an upper or lower limit for the number of entitlement a role can have. For example, if you select Less Than and type 3, the search results include roles that contain two (2), one (1), or zero (0) entitlements.
Risk Score Weight	Specify an upper or lower limit for risk score weight assigned to a role for it to be included in the search results. For example, you can specify a Greater Than value to search for high-risk roles, or you can specify a Less Than value to search for roles that were created with a risk score weight that is too low for their type. In the second example, if your enterprise has a policy that requires that all IT-type roles have a risk score weight of 100, you can select IT from the **Type** drop-down list, select Less Than from the **Risk Score Weight** drop-down list, and type 100 in the empty field to return all IT-type roles with a risk score weight less than 100.
Associated To Another Role	Include roles that are associated with at least one other role or roles that are NOT associated with any other role. **True** — include roles that are associated with at least one other role. **False** — include roles that are NOT associated with any other roles.
Effective Access	Limit the search to the specific effective access list. Effective Access is any indirect access that was granted through another object. For example a nested group, an unstructured target, or another role.
Filter By: Date	
Date Type	Select a state to associate with the specified dates:

Criteria	Description
	Last Membership Certification — the date when the last role membership certification was performed. **Last Composition Certification** — the date when the last role composition certification was performed. **Last Assigned** — the date when the role was last assigned to an identity.
Start Date	Specify a beginning date for this search. The search results include information pertaining to any action performed on or after the specified date.
End Date	Specify an end date for this search. The search results include information pertaining to any action performed on or before the specified date.
Fields to Display:	
Fields to Display	Specify the information displayed on the Role Search Results page associated with this search. Each field defines a column on the results table. You must select at least one field to display on the results page.

Entitlement Search

Use the Entitlement Search page to generate searches based on the entitlements or application object types in your enterprise. These searches can find application objects by attribute, owner, value, application, type, target, rights, annotation or any combination of that criteria.

See Entitlement Search Criteria

Search results can be saved as reports for reuse. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See the **Reports** documentation.

Entitlement searches that are saved as identity searches are only available from the Identity Search page. If you save an entitlement search as an identity search, the filters are converted to work on identity pages. The new search results include the identities that are in associated with the application objects for the original search.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Entitlement Search Criteria

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, all application object types are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Entitlement Search page has the following information:

Criteria	Description
Saved Searches:	
Search Name	These Saved Searches are only available for your use. The names of past searches that you saved to reuse at a later time.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search. Run the search with the criteria that is displayed on the current page.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Account Group Attributes:	
Attribute	Type the name of an attribute to include in the search.
Owner	Type the entitlement owner to include in the search. Click the arrow to the right of the suggestion field to display a list of all possible owners or type a few letters in the field to display a list of possible owners that begin with that letter string.
Value	The value assigned to the attribute on an application.
Application	Select the applications to include in the search for entitlements. If nothing is selected, all application are included.
Type	Select the application object type to include in the search. If no application is specified all application object types from all applications are included in this list. If no application object types are specified, all are included in the search.
Classification	Classifications can identify entitlements as potentially allowing access to sensitive, protected, or otherwise significant data. Choose any classifications to include in the search.
Effective Access	Limit the search to the specific effective access list. Effective Access is any indirect access that was granted through another object. For example a nested group, an unstructured target, or another role.
Target	The specific target on an application to include in the search. Use the target filter to narrow the search results based on a specific application.
Rights	The rights associated with an entitlement on the target attribute. For example, create, read, update, delete, execute.

Criteria	Description
Annotation	The annotation field is an open field that you can use to add information to help describe permissions.
Searchable Attributes: The extensible entitlement attributes marked as searchable in the entitlements catalog.	
Fields to Display:	
Fields to Display	Specify the information displayed on the Entitlement Search Results page associated with this search. Each field defines a column on the results table. You must select at least one field to display on the results page.

Activity Search

Use the Activity Search panel to generate searches for activity information on applications and targets, by specific identities and population, over specific time periods. These searches can determine risk areas and track activity on sensitive applications in your enterprise.

See Activity Search Criteria

Search results can be saved as reports for reuse. When you save a search as a report, you can schedule the search on an on-going basis for monitoring and tracking purposes. See the **Reports** documentation.

Activity Search Criteria

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not enter information or make a selection in a search criteria field, all possible choices are included. For example, if you do not select an application from the **Applications** list, all application configured to work with IdentityIQ are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Activity Search tab has the following information:

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved for reuse. These Saved Searches are only available for your use. To make searches available to IdentityIQ users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	Run the search with the criteria displayed on the current page. If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Activity Attributes:	
Type of Time Span:	
Time Period	If you want to filter by **Time Period**, select one or more time periods from the list. The definition for each time period is specified when IdentityIQ is configured.
Date of Activity	If you want to filter by **Date of Activity**, type the start and end dates for the search.

Criteria	Description
	Start Date — include information on activity that occurred on or after this date in the search results. **End Date** — include information on activity that occurred on or before this date in the search results. You can type the date manually or click the "..." icon to select a date from the calendar.
Actions:	
Action	The action that was performed For example, login or create. Use the Shift and Ctrl keys to select multiple list items. Identities need to match only one of the selected items to be included in the search results.
Applications:	
Source Application	Select the applications to include in the search. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications or type a few letters in the field to display a list of applications that begin with that letter string. Identities need to match only one of the selected items to be included in the search results.
Type of Target:	
Category	If you want to filter by **Category**, select the category to search from the drop-down list. The **Category** drop-down has all of the activity target categories defined on the Activity Target Categories page. Activity Target Categories are groups of targets from one or more applications. The **Target** list has all of the targets included in the selected category. This field is read only.
Targets	If you want to filter by **Targets**, specify the target that was acted upon. For example, a machine name for a login or a file name for a create action.
Identities or Interesting Populations:	
Identities	The name of the user or workgroup that requested the action. Entering the first letter or letters, of a name displays a selection list of users or workgroups with names that have that letter string or click the arrow to the right of the field to display all names.
Interesting Population	The population of identities to include in the search. The **Interesting Populations** drop-down list has the populations created based on the results of Identity Searches. The list has only the populations that you created or that their creator designated as public.
Activity Results:	
Result	The result of the action, **Failure** or **Success**.

Criteria	Description
Fields to Display:	
Activity Fields	Specify the information displayed on the Advanced Activity Search Results page. Each field defines a column on the results table. You must select at least one field to display on the results page.

Audit Search

Use the Audit Search tab to generate searches for audit records for specific time periods and for specific actions, sources, and targets. These searches can find and track events. The information included in the audit logs is different than application activity because the events in the audit log are not associated with an application or data source and may not be associated with a specific identity.

See Audit Search Criteria

Before the audit logs collect any data to use in an audit search, IdentityIQ must be configured for auditing. Because collecting and storing event information in the audit logs can impact performance, a system administrator must specify the general actions and class actions to audit.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on an on-going basis for monitoring and tracking purposes. See the **Reports** documentation.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Audit Search Criteria

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Audit Search tab has the following information:

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. These Saved Searches are only available for your use. To make searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	Run the search with the criteria displayed on the current page. If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Audit Attributes:	
Action	The action that was performed, for example, login, delete or signoff.
Source	The string that identifies the source of the event. The source is generally the name of an Identity object. The source can also be a less specific name such as, “scheduler” or “system.” When the event occurs during an interactive session with the IdentityIQ Web application, identity names are used. When background tasks or anonymous requests are not run for a specific identity, abstract names are used.
Application	Type manually or use the drop-down list to select an audited application.
Instance	Type manually or use the drop-down list to select an instance of a specified audited application.
Attribute Name	Type manually or use the drop-down list to select an audited attribute name.
Attribute Value	Type manually or use the drop-down list to select a value of a specific audited attribute.
Target	The object that was acted upon. For example, a machine name for a login or a file name for a create action.
Account Name	Type manually or use the drop-down list to select an audited account name.
Filter by Date:	
Start Date	Include information on events that occurred on or after this date in the search results. You can type the date manually or click the **“...”** icon to select a date from the calendar.
End Date	Include information on events that occurred on or before this date in the search res-

Criteria	Description
	ults. You can type the date manually or click the **"..."** icon to select a date from the calendar.
Fields to Display	Specify the information displayed on the Audit Search Results page associated with this search. Each field defines a column on the results table.. You must select at least one field to display on the results page.

Process Metrics Search

Use the Process Metrics Search page to generate searches on the business process metrics in your enterprise. These searches provide visibility to the detailed metrics that monitored processes and process steps generate. These searches help administrators create, manage, and monitor the identity business processes in IdentityIQ.

See Process Metrics Search Criteria

For example, you can determine the amount of time to run a defined business process and identity failures in the monitored steps of that process.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See the **Reports** documentation.

Process Metrics Search Criteria

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Process Metrics Search page has the following information:

Criteria	Description
Name	Type the name or select a business process from the drop-down list.
Participants	Select one or more participants to include in your search.
Result Status	Select All, Success or Fail from the drop-down list.
Filter by Active Dates	Include a start or end date to limit your search results. Click the Start Date check box and select a date. Click the End Date check box and select a date.
Filter by Execution Time	Use one of the following filtering methods to limit your search results based on the process run times: **Average or Maximum —** Select Average or Maximum to display the average or maximum of all execution times. **Execution time greater than —** enter a minimum time unit as a baseline to start your search. **Time Unit** — select from minutes, hours or days

Access Requests Search

Use the Access Requests Search page to generate searches on specific attributes of the access requests made in your enterprise.

See Access Requests Search Criteria.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See the **Reports** documentation.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Access Requests Search Criteria

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See the **Reports** documentation.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Access Request Search page has the following information:

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time.

Criteria	Description
	These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Search:	
Run Search	Run the search with the criteria displayed on the current page. If you modify the criteria of the Loaded Saved Search, the modified criteria is used for the search.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Access Request Attributes:	
Access Request ID	Identification number designated for individual requests.
Requestor	Name of the identity that made the request.
Requestee	Name of the identity for who made the request
Is Verified	Attribute was verified through the provisioning process.
Application	The application that is part of the access request.
Instance	The instance of the application that is part of the access request.
Operation	Type of operator used to fulfill request. For example, Add is an operation used in Request Roles and Lock is an action of a Certification.
Completion Status	The current state of a completed access request.
Priority	The priority assigned to the access request.
Request Type	The type of business process associated with the access request.
Approval State	The current state of the access request in the Approval phase.
Provisioning State	The current state of the access request in the Provisioning phase.
Reason	Indicates if an item was added (expanded) or filtered from the original request. For example, a role requires an entitlement or an entitlement requires and account. The compilation process adds or removes any required items in the provisioning process.
State	The current state of the access request.
Filter by: Date	
Request Date	Use the drop-down list to select from Request Date, Completion Date or Verified Date and select a Start Date and End Date.

Criteria	Description
Fields to Display	Select the columns to display in your search results.

Syslog Search

Use the Syslog Search page to generate searches on specific technical support information that relates to your IdentityIQ installation.

See Syslog Search Criteria

> This tab is used primarily to determine specific support information that SailPoint IdentityIQ support engineers can use for troubleshooting issues.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuing basis for monitoring and tracking purposes. See the **Reports** documentation.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Syslog Search Criteria

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Syslog Search page has the following information:

Criteria	Description
Current Search:	
Run Search	Run the search with the criteria displayed on the current page.
Clear Search	Clear all query options.
Syslog Attributes:	
Incident Code	The ID associated with the logged exception. If the exception can be viewed in the UI, the ID is at the end of the message. The Incident Code assists help desk

Criteria	Description
	personnel to locate the exact exception.
Server	Name of the server running the code where exception was encountered. This information is helpful in clustered environments.
Level	Indicates the level of the logged exception. SailPoint supports logging WARN, ERROR and FATAL to the IdentityIQ database. Lower levels are logged using log4j if configured, but are not saved to the Syslog table in the database.
Username	User who was performing the action when the exception was encountered and logged. The username can be an individual user or a system.
Classname	Class in which the exception was encountered.
Message	The message included in the exception.
Line	The line of code executed when exception occurred.
Thread Name	The thread of code executed when the exception was encountered.
Filter by Date	
Start Date	Include information on events that occurred on or after this date in the search results. You can type the date manually or click the **"..."** icon to select a date from the calendar.
End Date	Include information on events that occurred on or before this date in the search results. You can type the date manually or click the **"..."** icon to select a date from the calendar.
Fields to Display Specify the information displayed on the Syslog Search Results page associated with this search. Each field defines a column on the results table. You must select at least one field to display on the results page.	

Account Search

Use the Account Search page to generate searches based on the accounts in your enterprise. These searches can find accounts by application, display name, owner, native identity, instance or any combination of these criteria.

See Account Search Criteria

When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See the **Reports** documentation.

Use **Advanced Search** to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your Identity Cubes, you can create multiple filters and then group and layer them using And \ Or operations.

See Advanced Search.

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Field	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.
Loaded Saved Search:	
The name and description of your current saved query.	

Account Search Criteria

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included.

For example, if you do not provide an application in the Application field, all application's accounts are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search. See Search Results.

The Account Search page has the following information:

Criteria	Description
Saved Searches:	
Search Name	The name of the past searches that you saved to reuse at a later time. These saved searches are only available for your use.
Loaded Saved Search:	

Criteria	Description
The name and description of your current saved query.	
Run Search	Run the search with the criteria that is displayed on the current page. If you have modified the criteria of the Loaded Saved Search, the modified criteria are used for the search.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Account Attributes:	
Application	Select the application to include in the search for accounts.
Display Name	Enter the Display name of account to include in the search.
Owner	If you want to filter by owner, select the owner to search from the drop-down list.
Instance	Select the instance to include in the search for accounts.
Native Identity	Select the native identity to include in the search for accounts.
Locked	Select True to search on only locked accounts or False to search on only unlocked accounts. If neither is specified, all accounts are included.
Diabled	Select True to search on only disabled accounts or False to search on only enabled accounts. If neither is specified, all accounts are included.
Searchable Attributes:	
Select True or False to include or exclude the following in your search: • Inactive Account • Service Account • Privileged Account	
Fields to Display Specify the information displayed on the Account Search Results page associated with this search. Each field defines a column on the results table. You must select at least one field to display on the results page.	

Advanced Search

Click **Advanced Search** to access the Advanced Search panel.

> Running a filter on more than one multi-value attribute with an OR condition generates a query that is unable to use the indexes and might impact performance.

Use the Advanced Search to create detailed, multi-layered filters. To create complex queries define multiple filters and then group and layer them using the Search Type operations.

After you enter the search criteria, click **Run Search**. The search results display.

The Advance Search has the following information:

Criteria	Description
Add A Filter:	
Field	A filter characteristic associated with the search type. The drop-down list has all of the categories available.
Search Type	The qualifier associated with the attribute value. For example, “equals” or “is like.” The choices in this drop-down list are based on the Field specified.
Value	The value of the attribute.
Filter(s):	
Operations	The drop-down list that have the And/Or values that control the inter-action of the filters included in the query. The drop-down list is not visible unless two or more filters are created.
Group Selected	Group multiple filters in the Filters list to create layers or sub-filters in the query.
Ungroup Selected	Ungroup grouped filters to edit the query.
Remove Selected	Remove the selected filter or sub-filter. If you select grouped filters and click this button, all filters in the group are removed from the query. To remove one filter from a grouped bundle, you must first ungroup the filters.
view/edit filter source	Open a text box that enables you to view and edit a string view of the query. If you type invalid query code the green check mark is replaced with a red exclamation point.
Fields to Display: Specify the information to display on the Search Results page. Each field defines a column on the results table. See Search Results. You must select at least one field to display on the results page.	

Search Results

The columns in the table are based on the **Fields to Display** list. From the results you can export your search results to file and save the search criteria for future use.

Click **Refine Search** to return to the search criteria page.

From Identity Search results you can use **Schedule Certification** to schedule certifications for any or all listed identities. Identity certifications are sent to the managers of identities that warrant special attention. These additional certifications do not replace regularly scheduled certification requests.

Result Options

> Result Options are dependent on the search type.

Use the **Result Options** drop-down list to:

- **Save Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save Search As Report** — searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis.
- **Save Search As Identity Search —** searches that are saved as identity searches are only available from the Identity Search page. If you save an account group search as an identity search, the filters are converted to work on identity pages. The new search results include the identities that are associated with the entitlements from the original search.
- **Save Identities as Population** — save the search as an interesting population of identities to use in activity monitoring and statistical reporting in similar way groups are used.
- **Show Entitlements** — display the entitlement information for all of the identities included in the list. The entitlements are separated into tables based on applications. To display a list of all users who are assigned the entitlement, click a value in any of the tables.
  The Percent of Population column displays the number of identities assigned to the specified attribute value on the application. The search results are displayed as a percentage and are based on the identities that have an account on the application.

Export Searches

Use the buttons on the top of the table to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf, Microsoft Excel, or ArcSight CEF Flat File format.