IdentityIQ Access History

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

SailPoint Technologies, Inc. makes no warranty of any kind regarding these materials or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. https://www.sailpoint.com/patents

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Access History

About Access History

Access History helps organizations track the history of access for identity objects. This feature benefits:

- Auditors who need to confirm that entitlements and access were provisioned or removed as expected
- Managers who want to compare access of newly-hired employees against incumbents
- Administrators who need to generate a report to document or prove how access stands on a specific date
- Application owners who want to know how many identities have entitlements and how they were acquired

Access History extracts data. If your needs are beyond that scope and you would like to learn about using Data Extract to code custom extracts for other objects or change data formats, see **About Data Extract** in the *System Administration Guide*.

How Access History Works

History events related to Access History objects are constructed and published to the history writer API through a scheduled event or ad hoc service. You can configure how frequently Access History runs, but the default is once per day.

The Dispatch Access History task determines the set of IdentityIQ objects to extract from IdentityIQ, which are those that haven't been captured previously or have changed significantly since the last time Access History was executed.

NOTE: The initial run of Dispatch Access History extracts all identity and related objects, and it can take a long time to execute. The following runs of Dispatch Access History are faster because only changed or new objects will be extracted and processed.

Each extracted object describes all of the information about a single IdentityIQ access history object (e.g., identity, role, account, etc.). An extracted object can also reference other objects. The extracted objects are formatted into JSON and enqueued to the Access History writer service.

The writer service processes the JSON objects, persisting the information into the tables in the access history database used specifically by the Access History user interface (UI).

The Access History UI lets you search the access history database. There are also APIs that the UI can use to query against the database, processing Identity, Role, Identity Entitlements, Certifications, Identity Requests, Managed Attributes, Capabilities, Accounts, Workgroups, and Policy Violations.

The system identifies duplicates so they are not processed twice and can distinguish between initial events and change events. Unchanged objects are not processed.

Access History is disabled by default to allow you to configure it. To use this functionality, you need to complete the following:

1. Setting Up Access History Database and Tables
2. Setting Up Access History Task
3. Scheduling the Access History Task
4. Configuring Access History

Setting Up Access History Database and Tables

The database for storing Access History data is separate from the IdentityIQ database. The IdentityIQ install and upgrade scripts create separate databases for IdentityIQ and Access History data. The databases can be within the same instance for convenience, but separate database instances are recommended for production environments to avoid an impact on IdentityIQ performance. Depending on your environment setup and on the number of daily changes to your identities, the Access History database can be large, and will continue to grow.

The separate IdentityIQ Access History database is required, even when the Access History feature is disabled or is not being used. See the *IdentityIQ Install Guide*.

On the initial run, the Dispatch Access History Task gathers all the objects it needs and places them into a queue. Access History then processes them from the queue and writes them into database tables, so that on an initial fresh install or upgrade you will have a populated access history store to work with.

IdentityIQ Access History database includes the following tables:

- spt_hist_account_capture
- spt_hist_accounts
- spt_hist_assigned_roles
- spt_hist_capability
- spt_hist_capability_capture
- spt_hist_certification
- spt_hist_cert_remediation_capture
- spt_hist_detected_roles

- spt_hist_entitlement_capture
- spt_hist_entitlements
- spt_hist_identity
- spt_hist_identity_capture
- spt_hist_identity_event
- spt_hist_identity_req_capture
- spt_hist_identity_req_item_capture
- spt_hist_mattr
- spt_hist_mattr_capture
- spt_hist_mattr_event
- spt_hist_object_config_capture
- spt_hist_policy_violation_capture
- spt_hist_policy_violation_remediation_bundle_ids
- spt_hist_policy_violation_remediation_capture
- spt_hist_policy_violation_remediation_entitlements
- spt_hist_policy_violations
- spt_hist_role
- spt_hist_role_capture
- spt_hist_role_event
- spt_hist_workgroup
- spt_hist_workgroup_capture
- spt_hist_workgroup_event

Setting Up Access History Task

There is a preconfigured task named Dispatch Access History. This is a scheduled task that runs every day at midnight by default.

Alternatively, you can create your own Access History task to run on your IdentityIQ instance:

1. Navigate to **Setup > Tasks**.
2. Select the **New Task dropdown** in the upper right corner.
3. From the dropdown list, select **Access History**.
4. On the New Task screen, enter a name for your task, and add any other optional field information you would like.
5. Under Access History Options, select **AccessHistoryExportConfig** from the dropdown.

   > Note: If you are setting up multiple Access History tasks with slightly different timings, you need to provide a unique YAML for each and input a unique name here for each task that you create.

6. Select **Save**, **Save & Execute**, **Cancel**, or **Refresh**.
   a. Executing the task looks at what objects are configured to be exported, applies the filter criteria and any limits that you have set and translates all of those objects into JSON documents and writes them to a JMS queue.
   b. If executed, review the Task Results, which display all the differences as well as the attribute statistics. See **Viewing Data Extract Task Results** in the *System Administration Guide*.

Scheduling the Access History Task

Schedule the Dispatch Access History task to run at a time or cadence you choose. See **Tasks Overview** and **How to Schedule a Task** in the *Tasks Guide*.

Configuring Access History

The Access History Configuration page is available under **Global Settings** for users with the appropriate rights, Access History Admin. The page allows you to edit and save the decided options.

1. Navigate to the **gear > Global Settings > Access History Configuration** page, which includes Access History Controls.

2. Make sure the **Enable Access History** checkbox is selected.

3. Enter a Destination Queue Name.

   See **Working with the Data Extract Message Broker** in the *System Administration Guide* for more information about message brokers and queues.

4. Select Save Changes or Cancel.

Additional configuration may be completed in the Debug page, where the following objects are available:

- Configuration object "SystemConfiguration"
  - accessHistoryEnabled

    Set to True to enable Access History.
- Configuration "AccessHistoryConfiguration"
  - jsonFormat

    If set to PRETTY, JSON strings are stored in an easy-to-read format.

    If set to MINIFIED, JSON strings are stored in unformatted JSON with white space removed.

    If set to ZIPPED (default), JSON strings are compressed.

    > Note: Due to space considerations, it is advisable to leave jsonFormat set to ZIPPED, unless suggested by support for troubleshooting.
  - maxAllowedPatches

    A patch capture only captures the differences from the previous capture of the object. It is useful for saving space.

    If maxAllowedPatches > 0, patch document support is enabled. This property identifies the number of patch documents that can be saved between full captures, e.g., if the value is 2, every third capture will be a full capture. This pattern can change based on the config property captureMaxAgeInDays.
  - captureMaxAgeInDays

    If a patch document is older (in days) than the number specified in captureMaxAge, a full capture will be taken regardless of the number of patch documents.

A default Extract YAMLConfig is available for Access History. If you prefer to create a custom configuration, see **Configuring Data Extraction** in the *System Administration Guide*.

Troubleshooting Access History Task Failures

If the Access History feature is not enabled, the task completes but the Task Result has a status of Warning and a banner states, "The Access History feature must be enabled in order to support history events."

If the Extract YAMLConfig is missing a message destination, the task status indicates Fail and a banner states, "Export YAMLConfig is missing a valid message destination."

If the Extract YAMLConfig contains an invalid message destination, the task status indicates Fail and a banner states, "Export YAMLConfig message destination could not be created."

If the Extract YAML Config is missing the transform configuration name, the status indicates Fail and a banner states, "No transformation configuration name was found in the Export YAMLConfig."

If the Extract YAMLConfig has a bad value for the transform configuration name, or references one that does not exist, the status indicates Fail and a banner states, "Unable to find YAMLConfig AccessHistoryImageConfig2."

If the Extract YAMLConfig is missing a value for extracted objects, the status indicates Warning and a banner states, "The selected Export YAMLConfig is missing entry for exportedObjects."

If the Transform YAMLConfig has a bad value in the extracted objects list, the status indicates Warning and a banner states, "The Transform YAMLConfig is missing imageConfigDescriptor for exportedObject [object]." Note that other extracted objects with valid values will still be processed.

If the Transform YAMLConfig is missing an entry for one of the extracted objects, the status indicates Warning and a banner states, "The Transform YAMLConfig is missing ImageConfigDescriptor for importedObject Certification."

Using the Access History UI

To see the Access History UI, you need to have the spright AccessHistoryViewIdentityHistory. The AccessHistoryExportIdentityHistory right further allows export of the selected Access History data.

1. Navigate to **Identities > Identity Access History**.
2. Search for and / or select an identity from the Identity List.
   a. The Identity List shows all identities by default. Use filters or search to narrow down the options.
   b. Display name and email are both shown for each identity so that in cases where there are duplicate display names, you can more easily select the one you want.
3. Select a capture date. By default, the most recent capture is shown for the selected identity.
4. View details in the Access Items cards, by Accounts, Entitlements, or Roles, and on the event timeline, which lists individual events affecting the identity from the capture date backwards to the beginning of Access History data capture.

   a. Select **View Profile** to view the identity attributes at the time of the capture. See View Profile.

   b. Select **Export** to export access items and / or events. See Export Access History.

Using the Identity List Search and Filters

Search allows you to find identities in the Access History database. When the search field and filter are blank, all identities are included in the identity list in alphabetical order.

1. Select the **filter icon** next to the search field to open the Identity Filters panel.

2. Filter By Identity, By Role, and / or By Entitlement. (Entitlement filter will include only Managed Attributes.) Combine filters to more easily find what you need. For example, you might choose to search by both Identity and Role. Note that filtering on permissions is not supported.

   a. Select the dropdown arrows to select filter criteria options.

   b. For **Identity**, select from attributes that have been configured for your implementation such as Manager, Is Manager (set the value to true or false), Is Active, and Identity Type.

   > Note: An identity is included in the filter results if the filter value has been true for that identity either now or at any time in the past since the beginning of Access History.

   c. For Role and Entitlement, select from the three-way toggle to view **All** (all roles or entitlements the identity has ever had), **Current** (roles or entitlements that the identity currently has), or **Previous** (roles or entitlements that the identity previously had but does not have now).

   d. For **Entitlements**, first select the application, then the attribute, then the value.

3. Select the **Apply** button to apply your selection(s) or the **Clear** button to clear values from the filter fields. You may also select **Cancel** to close the dialog without applying changes to the filters.

   > Note: If you have already applied filters, then reopen the filter dialog and make changes to those filters, Cancel will discard those changes but the existing filters will still apply.

—OR—

1. In the **search** field, begin entering a name or email.

   a. The search and filter capabilities are a "starts with" incremental search in which suggested values are filtered in real time as letters are entered.

   b. Search by display name, first name, last name, or email. Select **X** to clear values from the search field.

   c. If nothing matches the value you enter, the identity list is empty.

   > Note: Because a person's name may change over time, you may search using any of their names and it will bring up all results associated with that historical identity. For example, a person's name of origin and their married or changed name may both appear in a list, but selecting either one displays information for the same identity.

2. The Identity List displays all potential matches.

   a. At the bottom of the identity list, Of Total shows the total number of identities matching your entered criteria. Select **Show Next 20** to display more matches.

3. Select an identity to view its detailed information on the right side of the screen. Only one identity can be selected at a time.

Selecting a Capture Date

Choose a date on the calendar or timeline for the selected identity to view data about a specific identity capture.

Use the timeline carousel to select an access change event.

1. Use the toggle above the timeline to scroll by month or day.

2. Use the capture selector or arrows to the right and left of the timeline to scroll chronologically backwards and forwards.

   a. The capture selector above the Month / Day toggle navigates backwards and forwards one capture at a time.

   b. The arrows to the right and left of the timeline scroll backwards or forwards one week when in Day mode or one year when in Month mode.

3. Select a date on the carousel to see information about a specific identity capture.

   a. The filled blue dot indicates the day or month of the currently selected capture.

   b. Empty circles indicate one or more captures on that day. Select the circle to see a list and select a specific capture.

   c. Gray dots indicate that there was no identity capture on that day and the date may not be selected.

Alternately, you can use the date field or date picker to see an identity's state on a given date.

1. Enter a date in the date field or select the **calendar icon** on the upper right side of the timeline to open the date picker.
   a. Select a date from the calendar. A dot under a calendar date indicates that there are captures for that date.
   b. The selected date displays next to the calendar icon.
2. If there was an access change on the selected date, the latest capture data is shown.
3. If there was no access change on the selected date, a pop-up message states that no capture events occurred on this date and asks if you want to view the closest prior capture.
   a. Select **Yes** to view information for the closest prior capture.
   b. Select **No** to dismiss the pop-up message.

When a date is selected either on the date carousel or using the date picker, the Access Items tiles and Event Timeline below update to show data for the selected identity on the selected date. A timestamp above the date carousel displays the capture date for the information displayed below.

Access Items Tiles

The Access Items panel displays tiles with the identity's counts of Total Access Items, Accounts, Entitlements, and Roles. Selecting the Accounts, Entitlements, or Roles tile displays a table with more information about items of that type. To close the detail table, select **Go back to event timeline**.

Use the Search field above the Entitlements and Roles tables to search items in each table. Search results include matches in any column. To clear the search, select **Clear Search** next to the search field.

For Entitlements, you can select the **Show only additional entitlements** checkbox to filter out entitlements that were gained because of role assignments.

Table columns may be configured from the options below. Those marked with an asterisk are sortable.

Accounts:

- Application *
- Account ID *
- Status (Active/Locked/Disabled)

Roles:

- Name *
- Description
- Classifications (multivalued – select the icon to see the classifications list)
- Elevated access (Boolean)
- Assigned by (identity)
- Allowed by (role)
- Acquired (assigned / detected)
- Role type (business, IT, etc.)
- Application (multivalued)
- Account name (multivalued)

> Note: Blue icons indicate elevated access. If a Role has a sunrise and / or sunset date, it displays here.

Entitlements:

- Attribute *
- Entitlement (value)
- Classifications (multivalued)
- Elevated access (Boolean)
- Application *
- Account name

> Note: Red triangle icons indicate that an entitlement has been disconnected. If an Entitlement has a sunrise and / or sunset date, it displays here.

Event Timeline

The event timeline lets you scroll through a reverse chronological list of all changes to access that occurred up to and including the selected capture date and time. There are also governance event cards for added or removed entitlements, roles, or identity attributes with additional information about what caused the access or identity attribute change.

The most recent 20 events are displayed. Select the **Show Next 20** button to see more.

List elements include:

- **Event icon** - green + indicates add, red - indicates remove, blue gavel indicates governance events, and left / right arrows indicate an identity status change, identity attribute change, or account attribute change
- **Event type** - types of events include:
  - Changed account
  - Added account
  - Removed account
  - Removed entitlement
  - Added entitlement
  - Removed detected role
  - Added detected role
  - Removed assigned role
  - Added assigned role
  - Changed identity
  - Changed identity status
  - Deleted identity
  - Discovered identity

  - Governance event - Access Request, Certification, or Policy Violation
  - Mitigated policy violation
- **Event timestamp** - date and time the event was recorded in the Access History database
- **Type-specific fields or details** - configure columns to select which type-specific fields you want to display

Event Timeline Timestamp

The timestamp on an event in the Events Timeline is the date that the Access History task was launched, which fetched the objects that led to event detection. It is not the date and time that the event occurred. Therefore, events in the Access History database may have a later event date and time than the time at which the access change occurred in IdentityIQ. See Setting Up Access History Task.

> Note: Not every object captured in the Access History database results in a new identity capture being created. Changes to objects in the IdentityIQ database other than identity objects - such as, for example, changes to existing Accounts, Roles, or Entitlements that affect the identity - do NOT trigger a new capture. However, when a new capture is triggered by a change to the Identity, such as an added or removed Entitlement or Role, or a change to an identity attribute, the events for changes to the non-identity objects will be included in that capture.
>
> Therefore, it is possible to retrieve the latest capture for an identity in Access History, and for there to be some related events (the ones that in and of themselves don't trigger a capture) that are not yet included because those events were recorded after the latest identity capture was created.
>
> This is a transitory situation, and no events will be lost. They will show up when the next identity capture is generated. It's also possible that even recent identity-related changes may not be included in the latest capture, if the Dispatch Access History task has not been run since they occurred.

Filtering Events

Select the **filter icon** at the upper right side of the event timeline to filter events by:

- Access Items – Accounts, Entitlements, Roles
  - Use the three-way toggle to indicate whether you want to view All, Added, or Removed access items
- Governance Events – Access Requests, Certifications, Policy Violations
- Other Events – Identity Attribute Changes, Identity Status Changes, Account Attribute Changes

Select the **Apply** button to apply your selection(s) or the **Clear** button to clear values from the search fields. You may also select **Cancel** to close the dialog without applying changes to the filters.

> Note: If you have already applied filters, then reopen the filter dialog and make changes to those filters, Cancel will discard those changes but the existing filters will still apply.

View Profile

Select the **View Profile** button at the upper right side of the screen to see identity attributes for a selected identity as of the selected capture date, such as email, type, cost center, employee ID, department, job title, location, region, region owner, and location owner.

If you want View Profile to include extended attributes that your organization has configured, be sure to specify these in the Object configuration. See **Configuring Data Extraction** in the *System Administration Guide*.

Export Access History

Export Access History results to a CSV file for each type of item exported. The files are zipped together in a file whose name includes the identity name and date of the capture.

1. In Access History, select the identity for which you want to export information.
2. Select the **Export** button.
3. In the Create Export File window, select the Access Item types you would like to export – for example, Accounts, Entitlements, or Roles.

   > Note: The Search features in the Entitlement and Roles tables do not operate as filters for the Export feature. The entire table will be exported if the user requests an export, regardless of whether search has been used and the Entitlements or Roles table filtered.

4. Decide whether you want to also export the contents of the Event Timeline and select **Yes** or **No**.

   > Note: If you have filtered the Event Timeline, only the filtered events will be exported. A warning is provided, telling you how many events will be exported.

5. Select **Generate**.
6. A zip file with all of the exported CSV files can be found in your downloads.

Running Access History from the IdentityIQ Console

If you want to start IdentityIQ console standalone (without ever starting your app server) and perform accesshistory commands with it, then you need to start as follows:

```
iiq console -e MessageBus,AccessHistoryWriter -j
```

This will start the message bus broker service as well as the AccessHistoryWriter service, which reads and processes export events from the message bus.

> Note: MessageBus should not be included if a remote ActiveMQ broker is configured.

> Note: accessHistory console commands are only available after Access History is enabled.

Console Commands that do not Support Access History

The following console commands do not support Access History objects:

- checkin
- delete
- rollback
- rename
- import
- lock
- unlock