EVIDEN

Identity and Access Management

DirX Audit

Audit Manager Guide

Version 9.0, Edition July 2025

Table of Contents

Copyright ii
Preface 1
DirX Audit Documentation Set 2
Notation Conventions 3
1. DirX Audit Manager Overview 4
2. Using the DirX Audit Manager 5
2.1. Logging In 5
2.2. About the Landing page 6
3. Using Audit Analysis 8
3.1. Navigating the Audit Analysis Main Page 8
3.2. Filtering Audit Events 9
3.3. Managing Audit Events Filter Views 10
3.4. Viewing the Audit Events Search Results 11
3.5. Using the Page Navigator 12
3.6. Viewing Audit Event Details 12
3.7. Viewing Related Audit Events 15
3.8. Exporting Audit Events 16
4. Using History 18
4.1. Navigating the History Main Page 18
4.2. Filtering History Entries 19
4.3. Managing History Entries Filter Views 20
4.4. Viewing the History Entries Search Results 20
4.5. Viewing History Entry Details 22
4.5.1. The Attributes tab 25
4.5.2. The Events tab 27
4.5.3. The Roles, Permissions, Groups and Accounts tabs 28
4.5.4. The Risks tab 30
4.5.5. The Assignment cause tab 31
4.5.6. The Overview tab 31
4.6. Exporting History Entries 33
5. Using Reports 36
5.1. Navigating the Reports Main Page 36
5.2. Creating a Report Set 37
5.2.1. Creating a Report File 39
5.2.1.1. Selecting a Report Definition 39
5.2.1.2. Setting the Report File Scope 41
5.2.1.3. Defining the Report File Name and Format 44
5.2.2. Defining the Schedule 45
5.2.3. Conditioning the Report Set Execution 45

5.2.4. Defining the E-mail Message . . . 47
5.3. Editing a Report Set . . . 47
5.4. Deleting Report Sets . . . 49
5.5. Activating and Deactivating Report Sets . . . 49
5.6. Synchronizing Report Set Updates to the DirX Audit Server . . . 50
Legal Remarks . . . 52

Preface

This manual describes the DirX Audit Manager user interface provided with DirX Audit. It consists of the following chapters:

- Chapter 1 provides an overview about the DirX Audit Manager user interface.
- Chapter 2 describes how to log in to the DirX Audit Manager and work with its main page layout.
- Chapter 3 describes how to use the DirX Audit Manager's Audit analysis.
- Chapter 4 describes how to use the DirX Audit Manager's History.
- Chapter 5 describes how to use the DirX Audit Manager's Reports.

DirX Audit Documentation Set

DirX Audit provides a powerful set of documentation that helps you configure your audit server and its applications.

The DirX Audit document set consists of the following manuals:

- *DirX Audit Introduction*. Use this book to obtain a description of DirX Audit architecture and components.
- *DirX Audit Tutorial*. Use this book to get familiar quickly with your DirX Audit installation.
- *DirX Audit Administration Guide*. Use this book to understand the basic tasks of DirX Audit connectivity administration.
- *DirX Audit Manager Classic Guide*. Use this book to obtain a description of the DirX Audit Manager Classic user interface provided with DirX Audit.
- *DirX Audit Manager Guide*. Use this book to obtain a description of the DirX Audit Manager user interface provided with DirX Audit.
- *DirX Audit Command Line Interface Guide*. Use this book to obtain a description of the command line interface provided with DirX Audit.
- *DirX Audit Customization Guide*. Use this book to customize your DirX Audit environment.
- *DirX Audit History Synchronization Guide*. Use this book to obtain information about the DirX Audit History synchronization jobs.
- *DirX Audit Best Practices*. Use this book to obtain guidelines and tips for avoiding common mistakes and improving the experience of a DirX Audit installation.
- *DirX Audit Installation Guide*. Use this book to install DirX Audit.
- *DirX Audit Migration Guide*. Use this book to migrate DirX Audit from previous versions.
- *DirX Audit Release Notes*. Use this book to understand the features and limitations of the current release.
- *DirX Audit History of Changes*. Use this book to understand the features of previous releases.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

install_path
The exact name of the root of the directory where DirX Audit programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Audit** on UNIX systems and **C:\Program Files\DirX\Audit** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

install_media
The exact path where the DirX Audit installation media is located.

1. DirX Audit Manager Overview

DirX Audit includes the DirX Audit Manager, a REST API-based web interface designed for audit administrators, auditors, and compliance and security officers. It enables users to view overviews, charts and reports based on audit trails and history snapshots stored in the DirX Audit Database.

This guide is structured as follows:

- "Using the DirX Audit Manager" explains how to log in to the interface and navigate its main layout.
- "Using Audit Analysis" describes how to evaluate audit trail with the Audit Analysis component.
- "Using History" details how to access and interpret historical snapshots through the History component.
- "Using Reports" covers how to configure report generation using the Reports component.

2. Using the DirX Audit Manager

The DirX Audit Manager is REST API-based web interface provided by DirX Audit for searching and analyzing identity audit data stored in the DirX Audit Database. It is designed for audit administrators, auditors, and compliance and security officers.

With DirX Audit Manager, you can:

- Use the Audit Analysis component to search for and display identity and access audit events stored in the DirX Audit Database. An audit event represents a single operation within a logical sequence of actions recorded in an audit message. Each audit event includes key information such as the origin (“where from”), the actor (“who”), and the affected objects (“what”), along with a summary of the operation. The Audit Analysis component presents these events in a paginated table based on search criteria you define.
- Use the History component to select and examine history entries stored in the DirX Audit Database. The History component provides detailed information about each entry, enhanced with a graphical timeline that visualizes changes and related events withing a selected time frame.
- Use the Reports component to create, edit, preview, and manage scheduled reports that offer immediate or recurring insights into audit events and history entries. Reports can combine data from all audited areas, enabling you to generate correlated views from multiple perspectives. These reports may include charts, audit event lists, and history details, all within a single or multi-document format.

The sections in this chapter explain how to log in to DirX Audit Manager and navigate its main interface.

Important: Do not use your browser’s **Back** button while working with DirX Audit Manager. Instead, use the application’s internal **Back** button or other provided navigation controls.

2.1. Logging In

To access the DirX Audit Manager, open a supported web browser. See the *DirX Audit Release Notes* for the list of supported browsers.

Enter the URL in the following format:
`https://`*`hostname:port`*`/`**`audit-manager-`***`tenantID`*

where

hostname – specifies the hostname of the machine where DirX Audit Manager is running,

port – specifies the port number used by the application container. The default is **8443** for an SSL connection and **8080** for a non-SSL connection,

tenantID – specifies the identifier of the configured tenant, for example the organization. Administrators provide this identifier to users based on their organization membership or access needs.

Example:
https://my-company.com:8443/audit-manager-71a75691-d28a-48ce-a542-6d6af7ece680

The URL opens a page listing available applications. Select Audit Manager to proceed the login page. In this page:

- enter your **Username**, typically your common name,
- enter your **Password**,
- click **Login**.

If the tenant ID and your credentials are correct, you will be directed to the DirX Audit Manager main page. Users can only access data for the assigned tenant. An auditor from one tenant cannot view data from another.

If you do not have permission to access DirX Audit Manager for the specified tenant, an error message will appear and you will be logged out.

To resolve this, you must be added to a privileged group with the appropriate permissions for the tenant. See "Managing a Multi-tenant Environment" in the *DirX Audit Administration Guide*. See "Configuring Privileged Groups" in the *DirX Audit Customization Guide* for privileged groups configuration.

2.2. About the Landing page

The DirX Audit Manager landing page provides access to all the essential tools and features needed to configure and execute your auditing tasks efficiently. The following figure illustrates the layout of the DirX Audit Manager landing page.

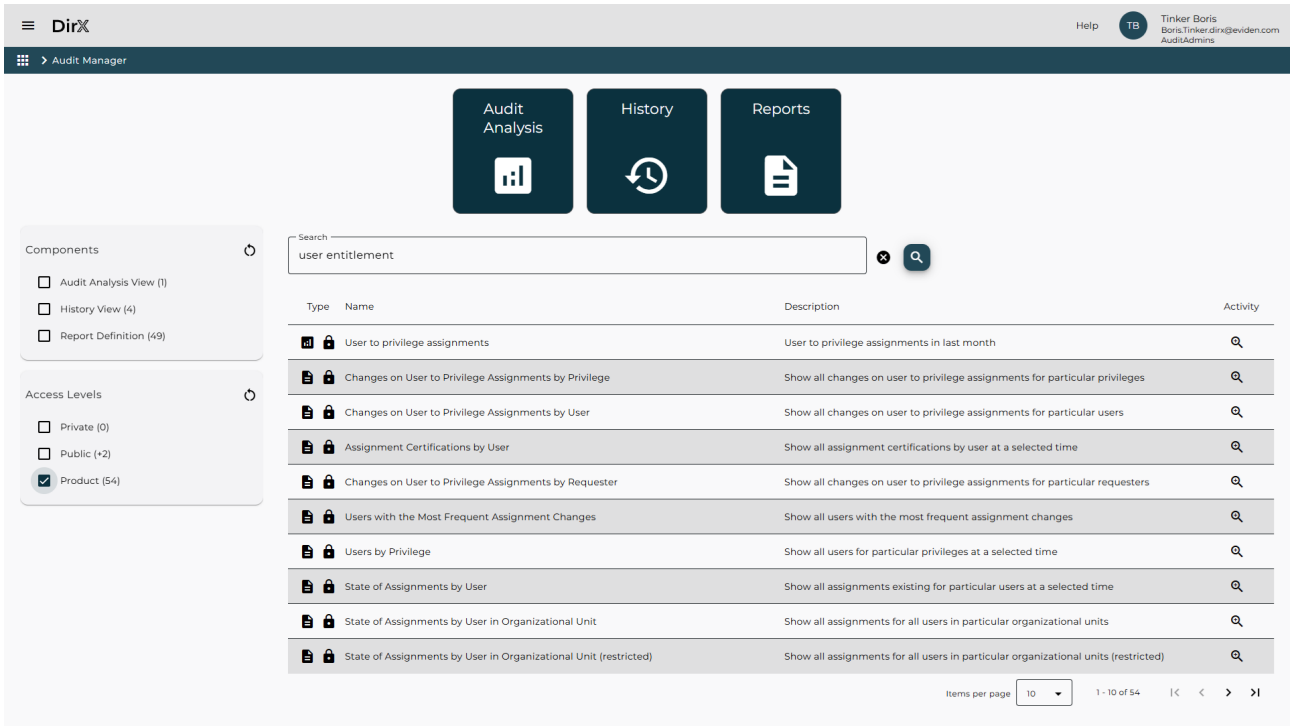


Figure 1. DirX Audit Manager Landing Page

As shown in the figure, the DirX Audit Manager main page contains the following items:

- Menu ☰ icon in the upper left corner opens a panel with several options:
  - **User identification** displays the currently logged-in user.
  - **Applications** redirects to a page listing available applications.
  - **Settings** opens the Core Settings page, where you can:
    - Select the language for the user interface.
    - Choose a theme: System, Light, or Dark.
  - **Help** opens the DirX Audit Manager documentation.
  - **About** displays version and copyright information.
  - **Logout** logs you out of the DirX Audit Manager.
- **Company logo area** displays your organization's logo.
- **Help** provides quick access to the documentation.
- **User identification** including application roles.
- **Breadcrumb navigation bar** helps you stay oriented and quickly navigate between sections without returning to the main page.
- **Audit Analysis**, **History** and **Reports** tiles allow you to access the corresponding components. The History tile is only visible if you have a valid license and it was selected during installation. Restricted auditors do not have access to Audit Analysis and History components. In such cases, only the Reports tile is available and opened by default.
- **Filter area** located on the left side allows for quick searches on configuration items in the DirX Audit Database.
- **Search results area** displays a search field and matching items in a table format. A page navigator below the table allows you to browse through multi-page results.

Users can either click a tile directly to navigate to the component or use the **Search** field on the landing page to find items based on specific filters.

For example, entering "user entitlement" will display all matching items. The search result table includes component type (Audit Analysis View, History View, Report Definition), access level (Private, Public, Product), name, and description. Component types and access levels are represented by icons in the first table column. You can further refine results using the Components and Access Levels filters on the left. To open a specific item, click the Open icon in the Activity column.

3. Using Audit Analysis

The Audit Analysis component allows you to work directly with audit events stored in the DirX Audit Database, unlike the Dashboards, which displays aggregated data from OLAP cubes.

This chapter describes how to:

- Navigate the Audit Analysis main page
- Filter audit events
- Manage audit events filter views
- View the audit events search results
- Use the page navigator
- View audit event details
- View related audit events
- Export audit events

3.1. Navigating the Audit Analysis Main Page

The layout of the Audit Analysis main page is shown in the following figure.

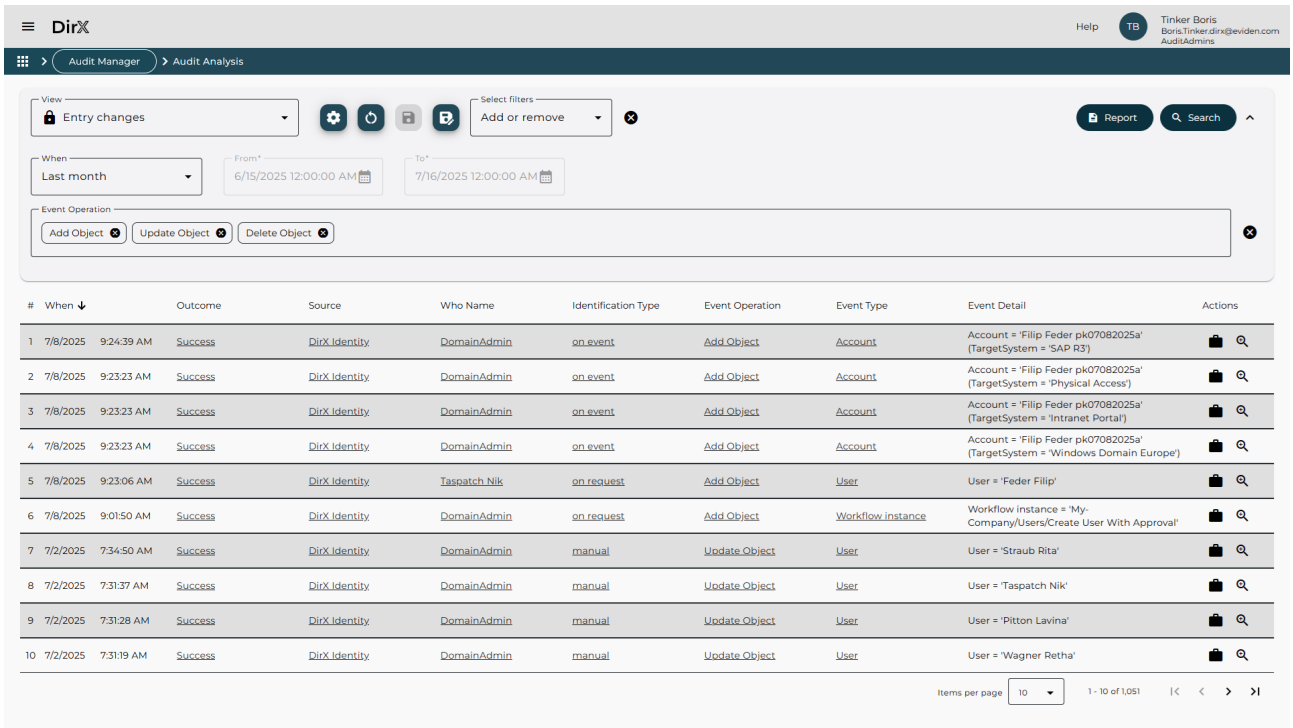


Figure 2. Audit Analysis – Main Page

As shown in the figure, the Audit Analysis page consists of two main areas:

- Filter definition area allows you to define the criteria used to search for and retrieve audit events. For details on how to use this area, see “Filtering Audit Events”.

- Search results display area presents the audit events returned by your search operation in a table format. A page navigator below the table allows you to browse through multi-page results. For more information, refer to “Viewing the Audit Events Search Results”.

3.2. Filtering Audit Events

The filter definition area allows you to define search criteria for retrieving audit events from the DirX Audit Database. You can filter events based on various attributes. To exclude an attribute from the filter, simply leave its field empty.

Start by selecting a view, which loads a predefined set of filters. The default view is **Last 24 hours (Default)**, which filters events from the last 24 hours. For more on managing views, see “Managing Audit Events Filter Views”.

The default view contains the following filter fields:

- **When** – filters audit events by time period:
  - Relative: **Previous Year**, **Previous Month**, **Month to date** and so on.
  - Absolute: **Custom Time** to define a specific range using the **From** and **To** fields. Timestamps are rounded to the nearest second. For example, to find an audit event at 4/4/2025 2:24:18.408 PM, set **To** to at least 4/4/2025 2:24:19 PM.
  - **Any time**: No time filter applied. The fields **From** and **To** are not visible in this case.
- **Event Operation** – filters by the type of operation, for example, Set Password, Add Assignment, Delete Object. Supports “Starts with” matching.
- **Event Type** – filters by the object type involved, for example, User, Account, Account to Group. Supports “Starts with” matching.

Use the **Select filters** to add more filter fields. The following additional filter fields are available:

- **Source** – filters by the audit producer, for example, DirX Identity, or DirX Access. Leave empty to include all sources.
- **Event Detail** – filters by specific details, for example, a user account or target system. This field supports full-text search if enabled in the configuration. Only full words are matched. With Microsoft SQL Server as the DirX Audit Database, you can use an asterisk (*) as a wildcard.
- **Outcome** – filters by event outcome: Success, Minor Failure, Serious Failure, Major Failure.
- **Identification Type** – filters by how the operation was initiated, for example, manually, on event, on schedule, on request.
- **Who Name** – filters by the user who initiated the operation. Supports “Starts with” matching.
- **What Name** – filters by the name of the object involved, such as a user or account. Also supports “Starts with” matching.
- **UID** – filters by the unique identifier of the audit message.

- **Event Dimension** – filters by a specific audit event dimension, for example, Approval, Policy, Target system. Selecting a dimension reveals a value field.
- **Message Dimension** – filters by a specific audit message dimension, for example, Activity, Who – Organizational unit. Selecting a dimension reveals a value field.

For better readability, you can collapse the filter definition area by clicking the **Collapse** ^ icon in the upper-right corner.

For the **Source**, **Event Operation**, **Event Type**, **Outcome**, and **Identification Type** filter fields, you can either select values from a predefined list or begin typing to search for matching values. As you type, DirX Audit Manager queries the database and displays a list of matching attribute values, from which you can select.

These fields support multiple values, allowing you to add several filter criteria for a single field. To remove a value, simply click the **X** next to it. If you no longer want to use a particular filter, you can remove it entirely from the list.

In the **Event Operation**, **Event Type**, **Who Name**, and **What Name** fields, you can search using a "Starts with" comparison. For example, entering **Account** in the **Event Type** field will return events related to Account and Account to Group memberships. These fields also support multiple values. Simply type a value and press Enter to add it. To remove a value, click the **X** next to it. If you no longer wish to use the filter, you can delete it from the list.

For the **Event Dimension** and **Message Dimension** filter fields, you can select a dimension from the available list. Once a specific dimension is selected, an additional field appears where you can choose a corresponding value. If you prefer not to filter by a specific value, simply select the empty line from the list. In this case, the search will return all events that include the selected dimension, regardless of its value.

To remove all values from a specific filter field, click the **Remove all** ⊗ icon at the end of the line. This action deletes both the filter values and the filter field itself. To use the filter again, reselect it from the **Select filters** list.

To remove all filter fields from the filter definition area, click the **Remove all** ⊗ icon next to the **Select filters** dropdown. You can re-add any filters as needed from the same list.

Click **Search** to execute your query. DirX Audit Manager will populate the search results area with audit events that match your criteria. For details on working with the results table, see "Viewing the Audit Events Search Results".

You can also refine your search directly from the results: click on a value in the table to add it as a filter, then click **Search** again to update the results.

To export the search results to a file, click the **Report** button. For more information, see "Exporting Audit Events".

3.3. Managing Audit Events Filter Views

You can name and save your custom filter views to the configuration database for future use. This allows you to quickly reapply commonly used filters without redefining them each

time. Simply select a stored view from the **View** list and click **Search**.

Filter views are grouped into the following categories:

- Favorites – Views marked as favorites by the user. These appear in the View dropdown.
- Private – Views created by the user. Only the creator can edit or delete them.
- Public – Views created and managed by audit administrator. Only they can edit or delete them.
- Product – Predefined views created during the product installation.

The default view is predefined for both Audit Analysis and History. If you remove it from your Favorites, the first view in the Favorites list becomes the default.

To save a new view, click the **Save As** icon next to the View field. Provide a name, a description, and select the visibility (Public or Private). Only users with the Audit Administrator role can create public views. Other users can only save views as private. Click **Create** to save the view.

To update an existing view, click the **Save changes to the view** . Only Audit Administrators can update public views. Product views deployed during the product installation cannot be modified.

To reset all changes in the selected view, click the **Undo changes** icon.

Click the **Manage views** icon to open the view manager. Here, views are organized into Favorites, Private, Public, and Product tabs. Click the **Mark as favorite** ☆ icon in the Actions column to appear the view in the Favorites tab and the View dropdown. Click the **Remove from favorites** ★ icon in the Actions column to remove the view from the lists. In the Favorites tab, you can reorder views by dragging and dropping them.

You can also clone, edit, and delete existing views. These capabilities help tailor the filtering experience to individual or organizational needs.

3.4. Viewing the Audit Events Search Results

The search results display area presents audit events in a table format based on the criteria defined in the filter definition area.

Each search result includes the following features:

- Columns – Each column corresponds to an attribute of the audit event. You can sort the data in ascending or descending order using the sort controls in the column headers.
- Rows – Each row represents a single audit event retrieved from the DirX Audit Database.
  - Show Related Events – Click the **Show related events** icon in the **Actions** column to display a list of audit events related to the selected one. For details, see “Viewing Related Audit Events”.
  - Show Details – Click the **Show details** icon in the **Actions** column to view additional information about the audit event in a separate window. For details, see

"Viewing Audit Event Details".

- Page Navigator – Located at the bottom of the results area. It allows you to navigate through multiple pages of results. For details, see "Using the Page Navigator".

Note: If audit message data has been purged from the DirX Audit Database, some additional information or the original message may no longer be available in the Event Details window. Similarly, if related audit messages have been purged, the list of related events may be incomplete.

3.5. Using the Page Navigator

The page navigator, located at the bottom of the search results display area, allows you to control how results are displayed and navigate through multiple pages of items.

It includes the following elements:

- **Items per page** – A dropdown menu for selecting the maximum number of items displayed per page.
- Item count – Displays the total number of items found based on your search criteria.
- Navigation buttons – Use these buttons to move between pages of results:
  - **First page** |< – Jumps to the first page of results.
  - **Previous page** < – Moves to the previous page of results.
  - **Next page** > – Moves to the next page of results.
  - **Last page** >| – Jumps to the last page of results.

3.6. Viewing Audit Event Details

The results table in the Audit Analysis view displays only a subset of the available audit event data. To view the full details of an audit event, click the **Show details** icon in the **Actions** column of the corresponding row. This action opens a separate window displaying all available information related to the selected audit event. The following figure illustrates an example of the detailed audit event view.

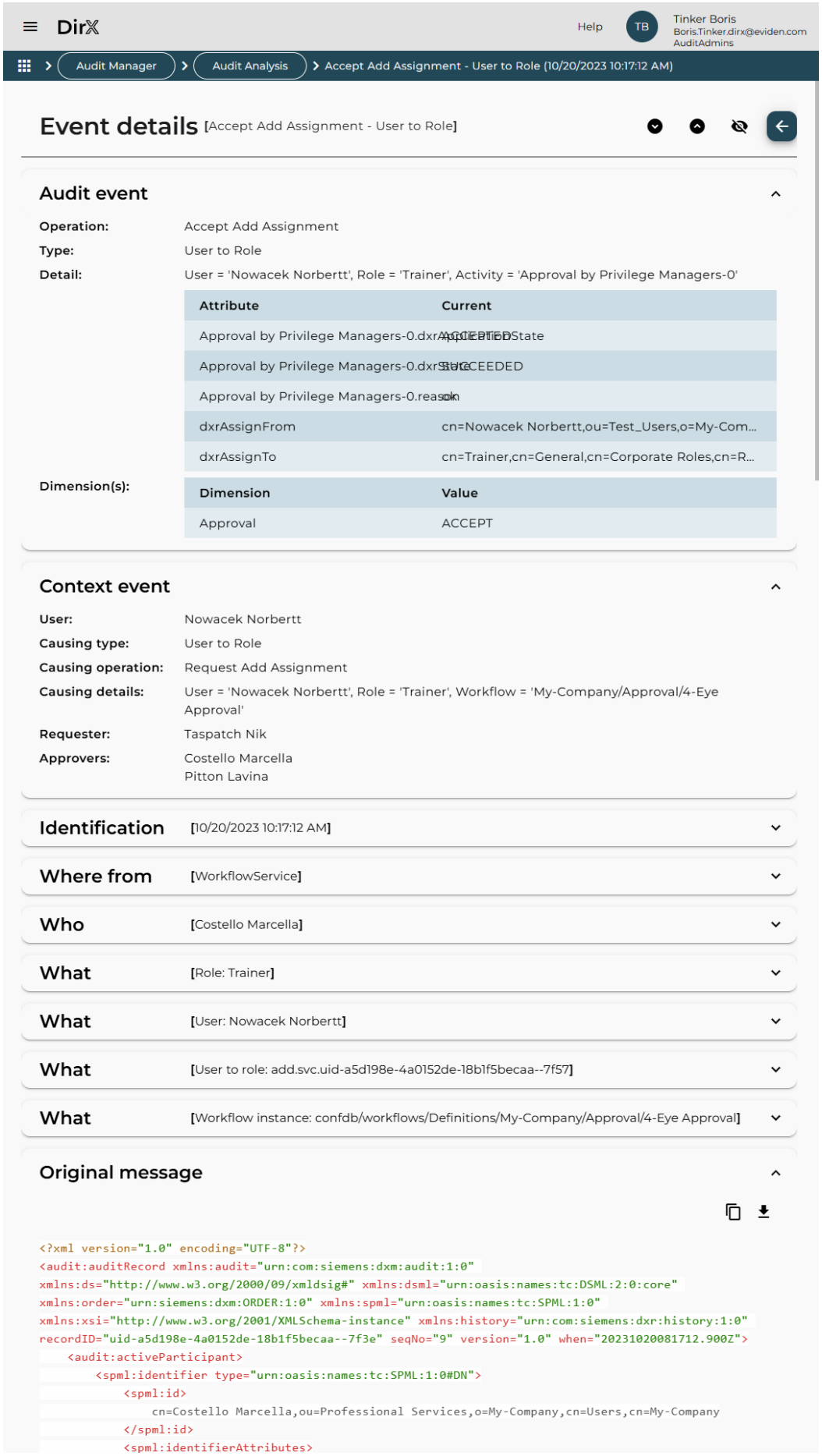


Figure 3. Audit Analysis – Event details

The detailed view includes several expandable sections, each providing specific information about the selected audit event:

- **Audit event** bar – Provides a summary of the audit event and its associated tags. Example: The event represents the approval of a role assignment (Trainer) to user **Nowacek Norbertt** by **Marcella Costello**, the role's privilege manager. This action was triggered by a DirX Identity approval workflow. The suffix in the activity name (for example, **"Activity='Approval by Privilege Managers'-0"**) indicates the approver's position in the approval sequence: -0 = first approver; -1, -2, etc. = escalation path approvers. If multiple role assignments or membership changes are involved, the summary may describe only one of them. Tags (for example, ACCEPT_REJECT) provide additional context. In this example, the value ACCEPT indicates that the request was approved.
  - **Detail** – Displays a table of attribute changes related to the event. Columns include:
    - **Attribute** – name of the changed attribute,
    - **Previous** – previous value, if applicable,
    - **Current** – new value, if applicable.
- **Context Event** – Summarizes related events, including the causing event, the requester, and the approver.
- **Identification** bar – Provides metadata about the operation, including timestamp, operation, type and category, audit message UID, outcome (success or failure), and associated audit message tags, for example, ACTIVITY with the name of the workflow activity. For more details on the database schema, refer to the *DirX Audit Administration Guide*.
- **Where from** bar – Identifies the source application or component that generated the event, for example, DirX Identity workflow service. Includes the source address and optional properties.
- **Who** bar – Identifies the user who performed the operation, for example, Marcella Costello. The Extensions area lists identifying attributes of the user.
- **What** bars – Represents an object involved in the operation: the user assigned the role, for example, **Nowacek Norbertt**, the user-to-role assignment, the workflow instance that triggered the activity.
- **Original Message** bar – Displays the original audit message received from the source system.

The **Audit Event** bar is expanded by default for readability. Click any title bar to expand or collapse its section. Use the following icons in the upper-right corner:

- **Expand all** to expand all bars.
- **Collapse all** to collapse all bars.
- **Show empty values** to show empty values.
- **Hide empty values** to hide empty values.

To return to the Audit Analysis results, click the **Back** ← icon or use the breadcrumb navigation.

Some audit events include links to related history entries, marked with the **See in history** icon. Clicking the link, for example, on **Costello Marcella**, opens the corresponding history entry for further inspection.

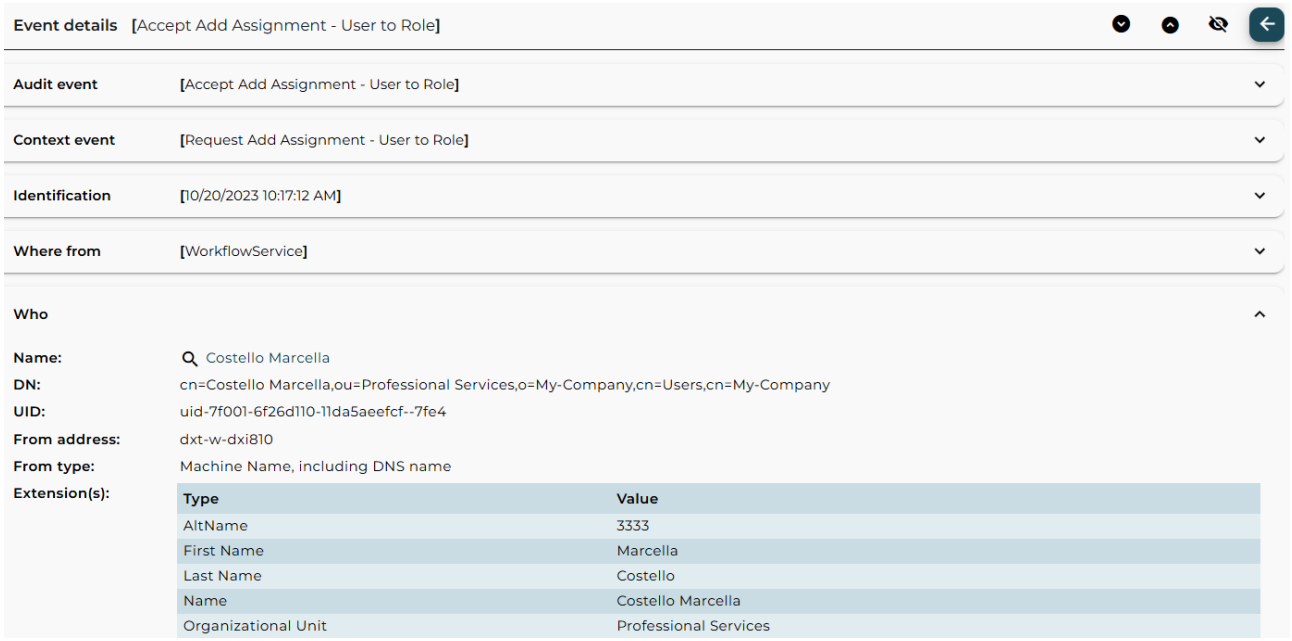


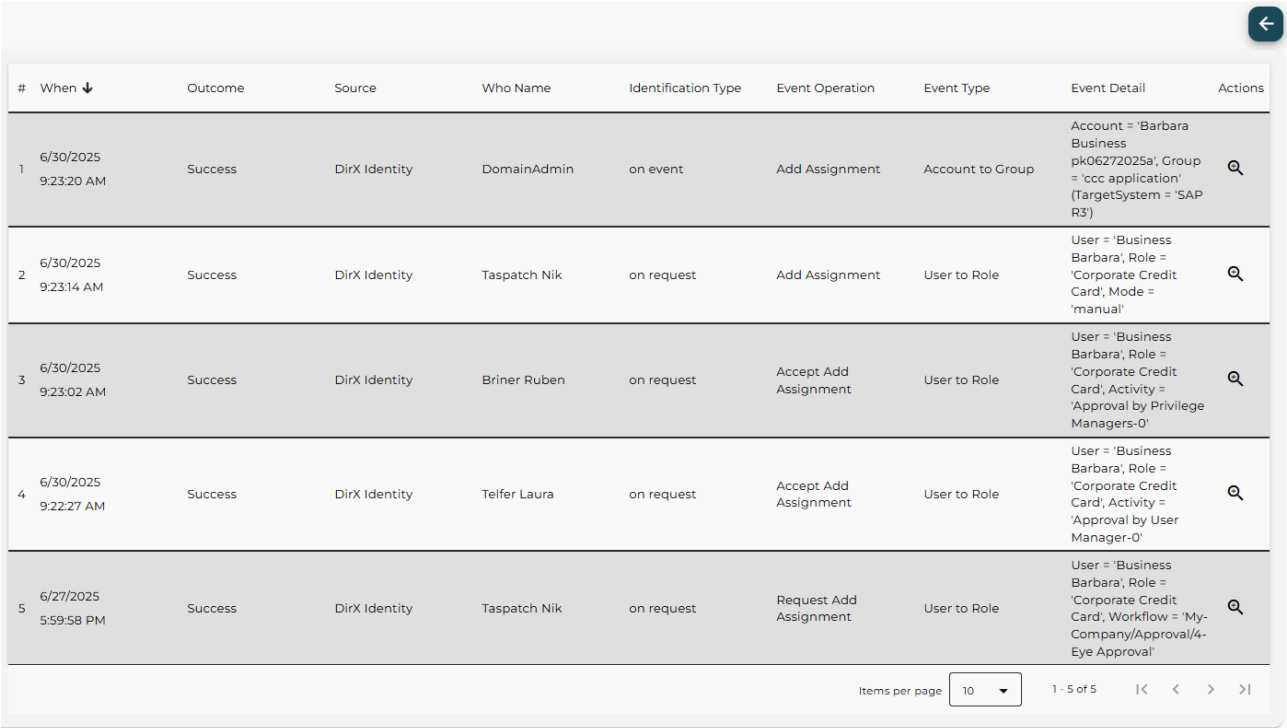
Figure 4. Audit Analysis – Events detail – Link to History Entries

3.7. Viewing Related Audit Events

To view audit events related to the selected one, click the **Show related events** icon in the **Actions** column of the results table.

DirX Audit Manager will search for and display all related audit events on a new page. These related events may include:

- parent – causing events,
- child – dependent events,
- sibling events – other child events of the same parent,
- indirectly related events.



#	When	Outcome	Source	Who Name	Identification Type	Event Operation	Event Type	Event Detail	Actions
1	6/30/2025 9:23:20 AM	Success	DirX Identity	DomainAdmin	on event	Add Assignment	Account to Group	Account = 'Barbara Business pk06272025a', Group = 'ccc application' (TargetSystem = 'SAP R3')	
2	6/30/2025 9:23:14 AM	Success	DirX Identity	Taspatch Nik	on request	Add Assignment	User to Role	User = 'Business Barbara', Role = 'Corporate Credit Card', Mode = 'manual'	
3	6/30/2025 9:23:02 AM	Success	DirX Identity	Briner Ruben	on request	Accept Add Assignment	User to Role	User = 'Business Barbara', Role = 'Corporate Credit Card', Activity = 'Approval by Privilege Managers-0'	
4	6/30/2025 9:22:27 AM	Success	DirX Identity	Telfer Laura	on request	Accept Add Assignment	User to Role	User = 'Business Barbara', Role = 'Corporate Credit Card', Activity = 'Approval by User Manager-0'	
5	6/27/2025 5:59:58 PM	Success	DirX Identity	Taspatch Nik	on request	Request Add Assignment	User to Role	User = 'Business Barbara', Role = 'Corporate Credit Card', Workflow = 'My-Company/Approval/4-Eye Approval'	

Items per page 10 1 - 5 of 5

Figure 5. Audit Analysis – Related Audit Events

The related audit events are presented in the same format as the Audit Analysis results. To view more details about a specific related event, click the **Show details** icon. To return to the previous results list, click the **Back** ← icon in the top-right corner of the page.

Note: If audit message data has been purged from the DirX Audit Database, some additional information or the original message may no longer be available in the Event Details window. Similarly, if related audit messages have been purged, the list of related events may be incomplete.

3.8. Exporting Audit Events

To export audit events displayed in the search results table into a report-formatted file, click **Report** in the filter definition area. The **Events report** dialog appears, allowing you to configure the export settings:

- **Report definition** – Select a predefined report definition to structure the exported data.
- **Report templates** – Choose a report template that defines the layout and formatting of the report.
- **Style** – Select the visual style to apply to the report.
- **Format** – Choose the file format, such as: PDF, CSV, Microsoft Word formats (DOCX, RTF), and others.
- **Language** – Select the language for the report content.
- **Encoding** – Choose the character encoding, for example, UTF-8, Big5, EUC-JP.
- **Record limit** – Defines the number of rows to include in the report. Currently limited to the number of rows displayed on the first page of search results table.

- **Action** – Choose what to do with the report file:
  - **Download** – Save the file directly.
  - **Open** – Open the report in a new browser tab.

Click **Export** to generate the report. Click **Cancel** to close the dialog without exporting. After clicking **Export**, your browser may prompt you to open, save, or cancel the download of the report file.

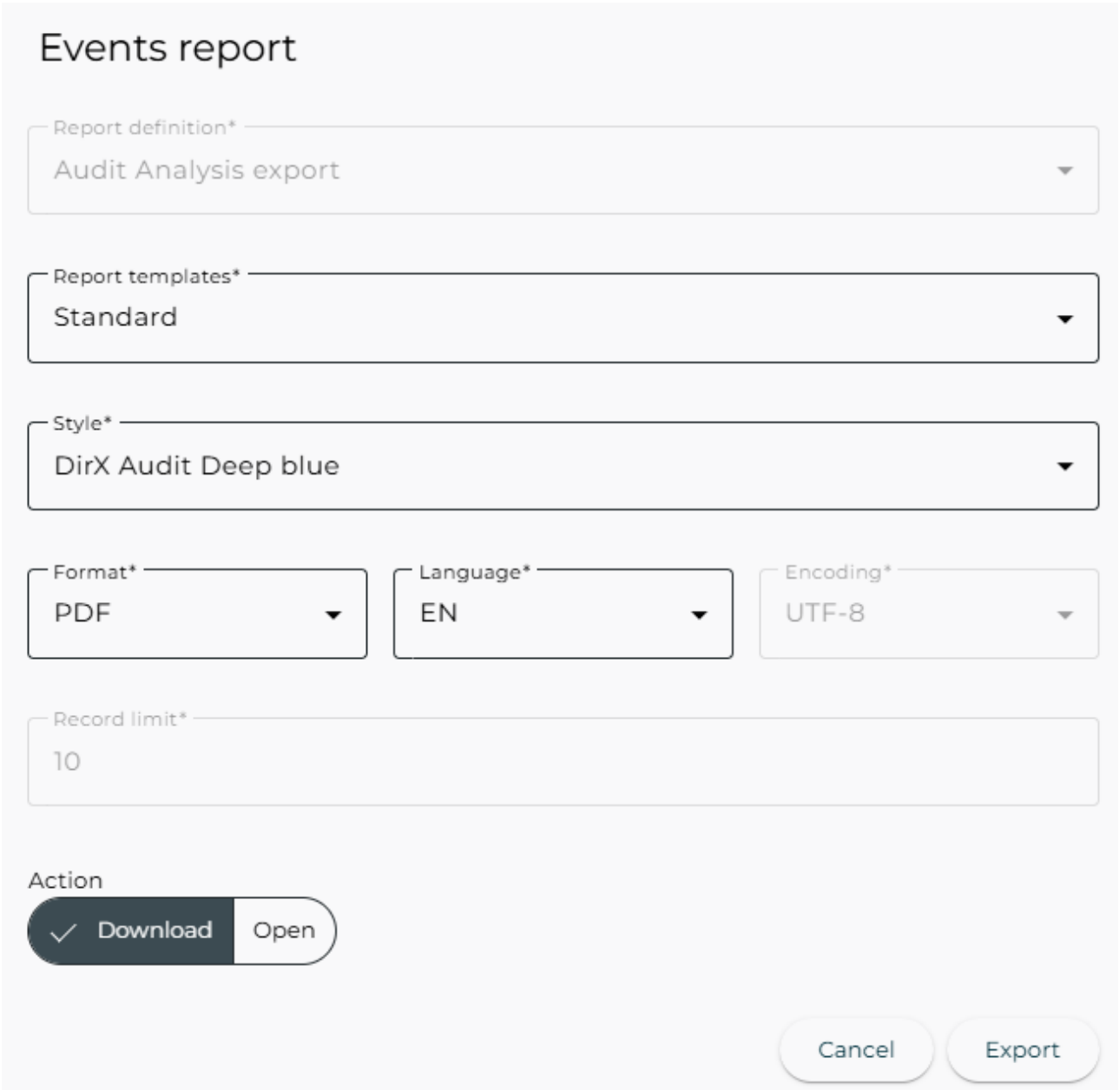


Figure 6. Audit Analysis – Events report

4. Using History

The History view is DirX Audit Manager's interface to the DirX Audit History Database. Unlike the Audit Analysis view, which focuses on audit events, the History view works directly with history entries stored in the database.

This chapter describes how to:

- Navigate the History main page
- Filter history entries
- Manage history entries filter views
- View the history entries search results
- View history entry details
- Export history entries

4.1. Navigating the History Main Page

The History page allows users to select and analyze history entries from the DirX Audit History Database for historical review and compliance tracking. The layout of the History main page is shown in the following figure:

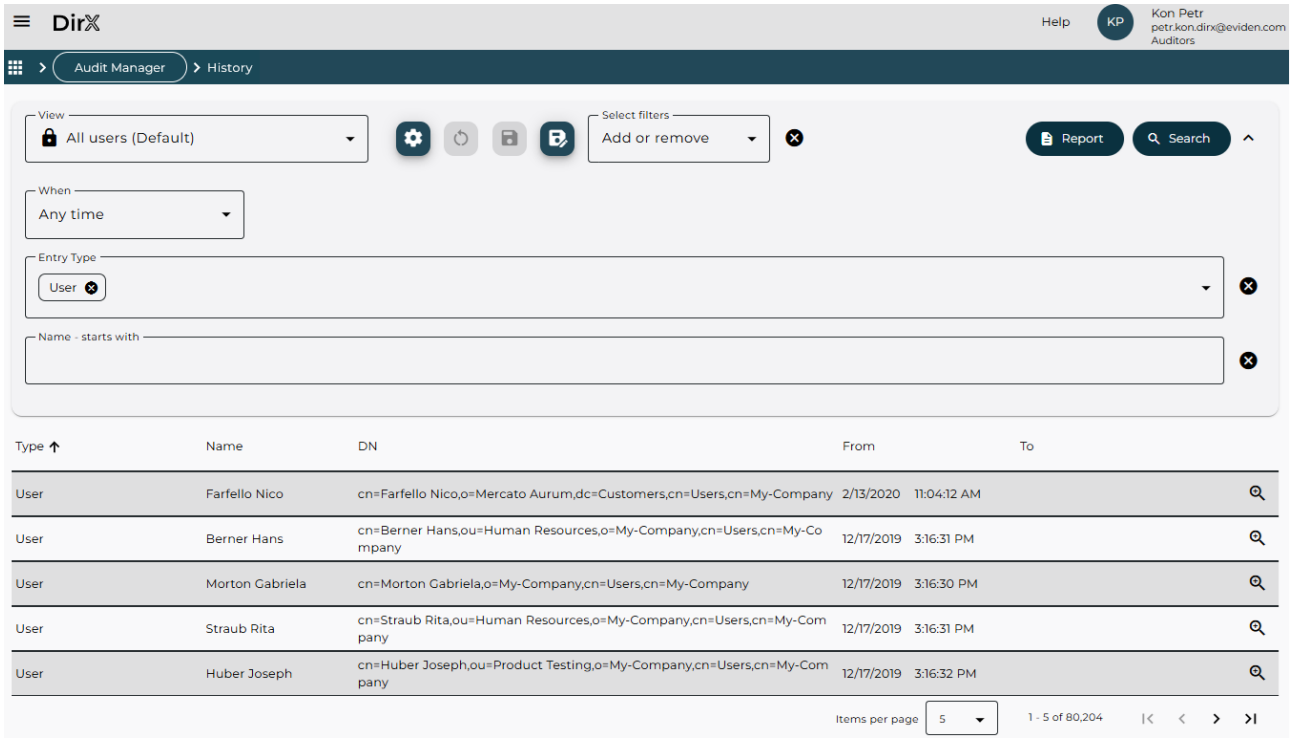


Figure 7. History – Main Page

As shown in the figure, the History page consists of two main components:

- Filter definition area allows you to define search criteria for retrieving specific history entries from the DirX Audit History Database. For detailed instructions on using this area, refer to the section "Filtering History Entries".

- Search results display area – presents the history entries returned by your search operation in a table format. A page navigator below the table enables users to browse through multiple pages of results. For details, see the section “Viewing the History Entries Search Results”.

4.2. Filtering History Entries

The Filter Definition Area allows you to define search conditions for retrieving history entries from the DirX Audit History Database. You can filter entries based on various attributes. To exclude an attribute from the filter, simply leave its field empty.

Start by selecting a view, which provides a predefined set of filters.

The default view is **All users (Default)**, where:

- **When** is set to **Any time**.
- **Entry Type** is set to **User**.

For details, see “Managing History Entries Filter Views”.

The default view includes the following filters:

- **When** – filters history entries by time period:
  - Relative: **Previous Year**, **Previous Month**, **Month to date** and so on.
  - Absolute: **Custom Time** to define a specific range using the **From** and **To** fields. Timestamps are rounded to the nearest second. For example, to find a history entry existing at 4/4/2025 2:24:18.408 PM, set **To** to at least 4/4/2025 2:24:19 PM.
  - **Any time**: No time filter applied. The fields **From** and **To** are not visible in this case.
- **Entry Type** – filters by entry type, for example, User, Role, Account, Target System.
  - Multi-value: select multiple entry types.
  - To remove all values, click the **Remove all** ⊗ icon. Then search result displays all of the types.
- Identifying attribute **Name** – filters by name prefix. You can enter one or more values. Remove values individually or clear the entire field.

Use the **Select filters** dropdown to add more filter fields:

- **Identifying Attributes** – includes **Name**, **DN**, **dirxEntryUUID**, and **dxrUID**. **Name** is selected by default. Each selected attribute adds a field for entering one or more values or prefixes.
- **Small Attributes** – filters based on specific attribute values.
  - Select an attribute name from the **Select filters** list.
  - Each selected attribute name adds a corresponding input field for entering values. These fields support multiple values, allowing you to specify more than one attribute value per attribute name.

For better readability, you can collapse the filter definition area by clicking the **Collapse** ^ icon in the upper-right corner.

Remove individual attributes using the **Remove attribute** ⊗ icon. Remove all filters using the **Remove all** ⊗ icon next to the **Select filters** dropdown.

Click **Search** to execute the query. The results will appear in the search results display area.

- Identifying Attributes: Results match entries with any of the specified values.
- Small Attributes: Results match entries that satisfy all specified attributes.
- **DN** uses an "Ends with" operator. Example: **cn=MVS,cn=TargetSystems,cn=My-Company** matches entries from the **MVS** node of target systems in the **My-Company** node.
- **Name**, **dxrUID**, and **dirxEntryUUID** use a "Starts with" operator. Example: Entering **Meeting** in **Name** returns all entries starting with **Meeting**.
- If no entries match the criteria, the message "No history entry found" is displayed.

Click **Report** to export the search results. For details, see "Exporting History Entries".

4.3. Managing History Entries Filter Views

You can name and save your custom filter views to the configuration database for future use. This allows you to quickly reapply commonly used filters without redefining them each time. Simply select a stored view from the **View** list and click **Search**.

This streamlines the search process and ensures consistency across repeated queries. Filter views are organized similarly to those in DirX Audit Manager's Audit Analysis component. For details, see "Managing Audit Events Filter Views".

You can also clone, edit, and delete existing views. These capabilities help tailor the filtering experience to individual or organizational needs.

4.4. Viewing the History Entries Search Results

After executing a search, the results are displayed based on the number of matching entries. If the search returns more than one history entry, the search results display area presents history entries in a table format.

Each search result includes the following features:

- Columns – Each column corresponds to an attribute of the audit event.
- Rows – Each row represents a single history entry retrieved from the DirX Audit Database.
- Page Navigator – Located at the bottom of the results area. It allows you to navigate through multiple pages of results. For details, see "Using the Page Navigator".

If the search returns exactly one history entry, the system bypasses the table view and directly displays the details page for that entry. For details, see "Viewing History Entry

Details”.

If no entries match the search criteria, the system displays the message: “No history entry found”.

The following figure illustrates a typical result table page:

Type	Name	DN	From	To
User	Trhlik Tonda	cn=Trhlik Tonda,cn=Users,cn=My-Company	2/28/2022 11:43:48 AM	
Ticket	Countries	cn=Countries,cn=For Object Types,cn=_Queries,cn=Internal,cn=Orders,cn=My-Company	12/17/2019 3:15:36 PM	9/23/2022 1:01:20 AM
User	Trainee SW Development	cn=Trainee SW Development,ou=Resources,o=My-Company,cn=Users,cn=My-Company	12/17/2019 3:16:32 PM	
User	Trainee HW Development	cn=Trainee HW Development,ou=Resources,o=My-Company,cn=Users,cn=My-Company	12/17/2019 3:16:32 PM	
User	Summer Sun Sona 3	cn=Summer Sun Sona,cn=Users,cn=My-Company	7/21/2020 11:52:31 AM	
User	Trhlik Tadeas	cn=Trhlik Tadeas,ou=Product Testing,o=My-Company,cn=Users,cn=My-Company	7/25/2023 12:24:39 PM	
User	Trainee Product Testing	cn=Trainee Product Testing,ou=Resources,o=My-Company,cn=Users,cn=My-Company	12/17/2019 3:16:32 PM	
Target System	PK_test_ts3	cn=PK_test_ts3,cn=TargetSystems,cn=My-Company	1/29/2021 2:27:32 PM	2/1/2021 10:51:34 AM
Certification Campaign	AB DXR Auditors role certification 2022-02-01	cn=AB DXR Auditors role certification 2022-02-01,cn=Certification Campaigns,cn=My-Company	2/1/2022 9:07:21 AM	2/4/2022 4:03:36 AM

Items per page 50 1 - 9 of 9

Figure 8. History – Search Result Table

Each row in the search results table represents a history entry and includes key identifying information and interactive features:

- **Name** and **DN** – identify the entry and reflect its location in the corresponding DirX Identity domain.
- Hovering over the DN field reveals a tooltip displaying **dxrUid** and **dirxEntryUUID**. These values can be copied for further use.

If an entry’s **Name** or **DN** was modified during the selected time period:

- The entry appears as multiple rows, each showing the state before and after the change.
- For better readability, these rows are collapsed into a single line.
- The collapsed row is marked with:
  - an exclamation mark icon,
  - a count of the related records next to the name.
- To expand a single modified entry, click the **Expand all states** icon at the end of the row.
- To expand all collapsed entries, click the **Expand all rows** icon at the top of the table.
- **From** and **To** columns indicate the entry’s lifetime:
  - **From**: When the entry was created.
  - **To**: When it was deleted or renamed.

To view detailed information about a specific entry, click the **Show Details** icon in the entry's row. This opens the details page for that history entry.

4.5. Viewing History Entry Details

The history details page provides comprehensive information about a selected history entry. It is divided into two main areas: a header area and a data area. The header area displays the entry's: type, name, identification attributes (Distinguished name, dirxEntryUUID, and dxrUid). For better readability, the header area is collapsed by default. To view identification attributes, click the **Show identifiers** icon in the upper right corner. To hide them again, click the **Hide identifiers** icon. You can copy identification attributes for further use by clicking the **Copy** icon next to each attribute.

The following figure shows an example of a history entry's details page header area.

Figure 9. History – Details Page Header Area

The following figure shows an example of a history entry's details page data area:

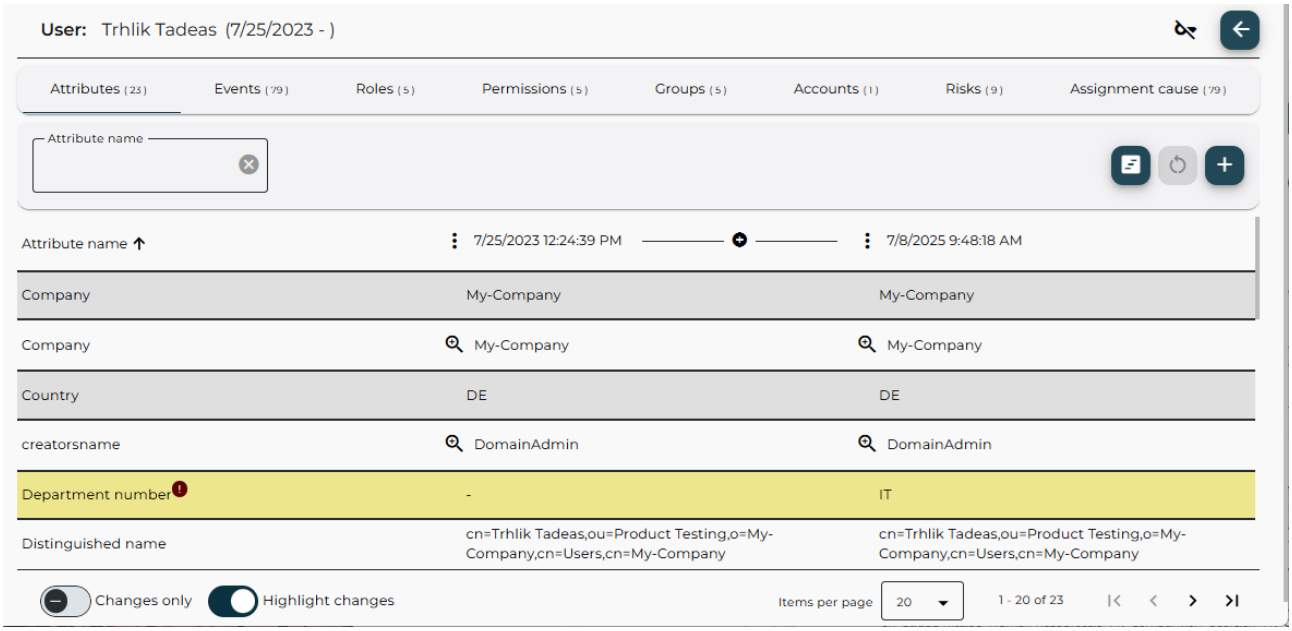


Figure 10. History – Details Page

To return to the History display area, you can:

- click the **Back** ← icon in the upper right corner, or
- use the navigation bar to jump to a different section.

The data area is organized into tabs, which vary depending on the entry type. Each tab contains a results table showing the entry's data at selected comparison time points.

- **Attributes** and **Events** tabs are common tabs available for all entry types.
- **Overview** tab is available only for the Workflow Instance, Certification Campaign and Certification Assignment Change entry types.
- **Privileges** tab is available only for the Certification Campaign entry type.
- **Roles** and **Permissions** tabs are available only for the User and Role entry types. In the latter case, the junior roles are displayed.
- **Groups** tab is available only for the User, Permission, and Target System entry types.
- **Accounts** tab is available only for the User and Target System entry types.
- **Users** tab is available only for the Role, Permission, Group, and Certification Campaign entry types.

- **Risks** and **Assignment cause** tabs are available only for the User entry type.

For entries of the User entry type, if associated Role, Permission, Group, or Account history entry is not synchronized to the DirX Audit History Database, only summary information is shown.

Some tabs offer additional filtering options to help you quickly locate specific data.

At the bottom of each table, the footer displays the total number of data items. A page navigator and items-per-page selector are also available.

You can also check **Changes only** to display only modified values. Check **Highlight changes** to visually emphasize changes with color and the exclamation mark icon.

By default, the data area includes two comparison time points: creation date, and termination date or current date, if the entry still exists. You can customize time points using the following controls:

- **Add time point** + icon – adds a new comparison column.
- **Split interval** icon – inserts a time point between two existing ones.
- **Reset time points** icon – restores the default time points.
- **Show more options** icon – opens a drop-down menu with advanced time point controls.
  - **Previous day** ‹ and **Next day** › – quickly change the selected date.
  - **Update time point** – updates the comparison time point.
  - **Remove time point** – removes the selected time point from the table.

You can switch from the table view to a graphical timeline view by clicking the **Show timeline** icon in the table header. The timeline view presents the same historical data as the table, but in a graphical format, making it easier to monitor changes over time. Attribute changes are represented as lines, showing how values evolve. Comparison time points can be added just like in the table view.

Use the navigation icons in the header to adjust the timeline display:

- **Zoom in** / **Zoom out** – adjust the scale of the timeline.
- **Backward** / **Forward** – move the timeline view backward or forward in time.
- You can also drag the timeline using your mouse for quick navigation.
- Hovering over a line displays a tooltip with the time validity of the attribute.
- Clicking on a line reveals the attribute value at that time.
- To return to the table view, click the **Show table** icon in the timeline header.

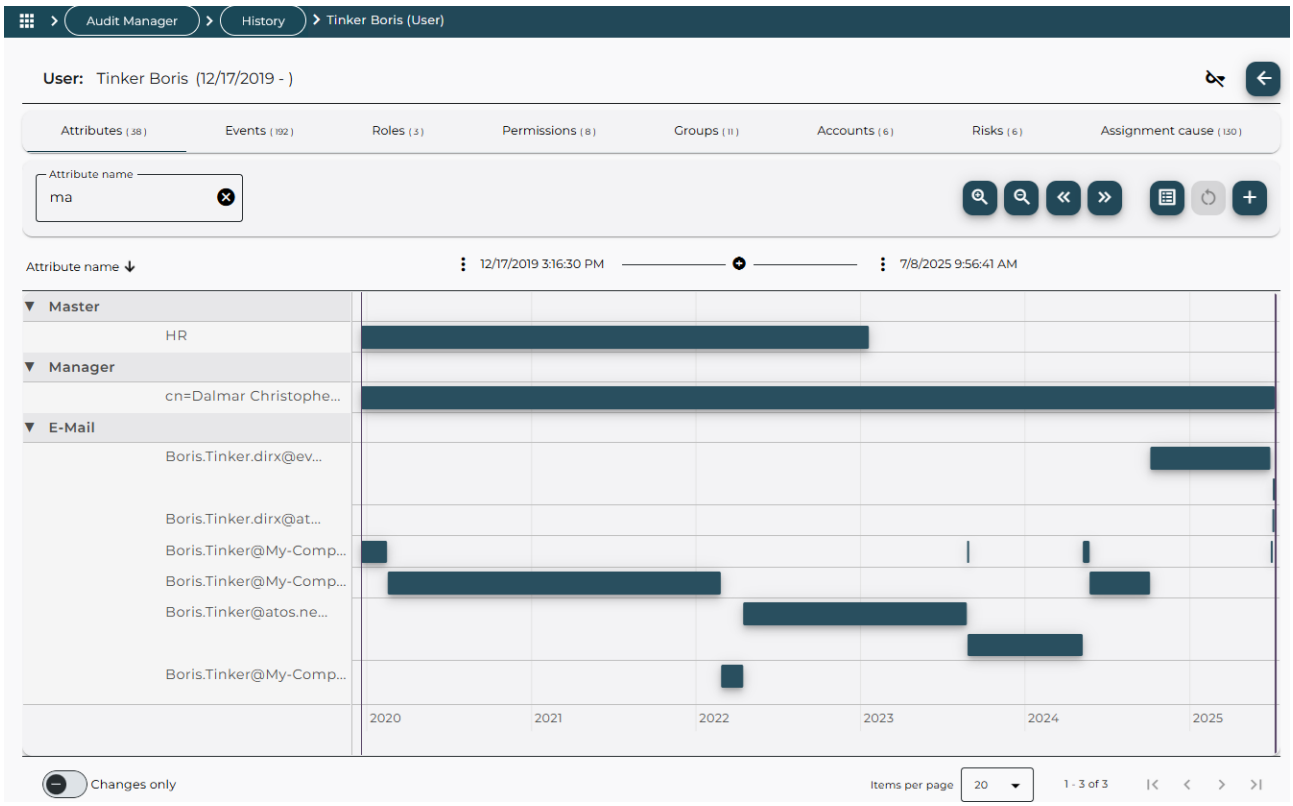


Figure 11. History – Timeline Page

4.5.1. The Attributes tab

The **Attributes** tab presents a detailed comparison of attribute values across selected time points. It is structured to enhance readability and usability, especially when dealing with large datasets. The table is divided into **Attribute name** column and one or more attribute value columns, one for each selected target date. For clarity, relative attribute names are displayed, for example **Distinguished name**. The tooltip on each name shows the technical attribute name, for example dn.

You can sort the table by **Attribute name** in ascending or descending order.

Use the **Attribute name** filter field to quickly locate specific parameters. This filter is also available in other tabs and is recommended for large datasets, for example many users in a role. Use the **Clear** ⊗ icon to reset the filter field.

Some attributes may contain a large number of values, such as: `dxrPrivilegesLink`, `dxrResolvedPrivilegesLink`, `dxrGroupMemberAdd`. To maintain readability, the number of displayed values is limited. If the total exceeds the configured maximum, the total count is shown at the end of the list and a note indicates how many values are hidden.

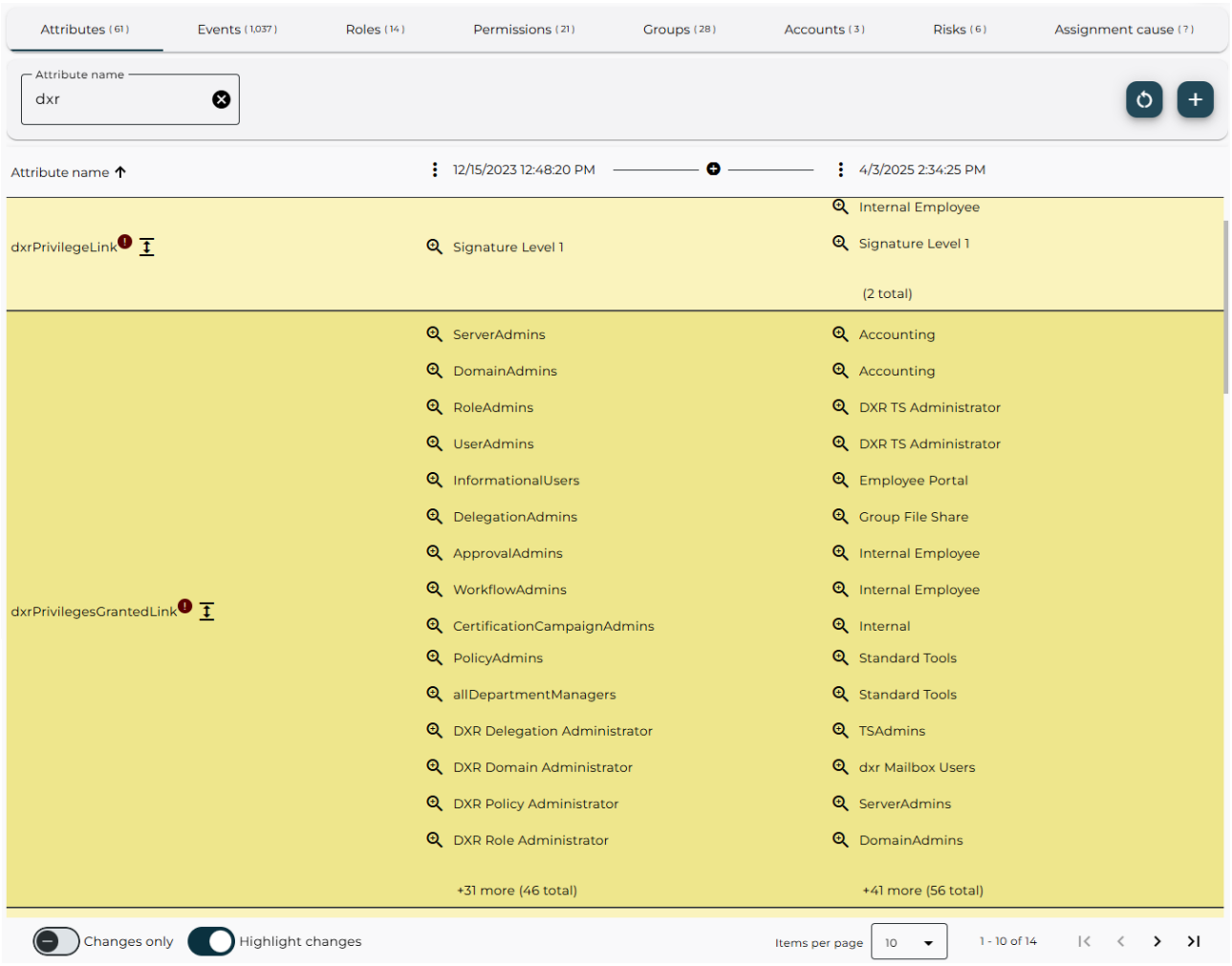


Figure 12. History – Attributes Tab with Multivalue Attributes

To view the complete list, click the **Show and compare all values** icon next to the attribute name. This opens a new window displaying all values for that attribute. A filter field is available for quickly searching within the values. The table footer shows the total number of data items, a page navigator and a drop-down menu to adjust the number of items displayed per page.

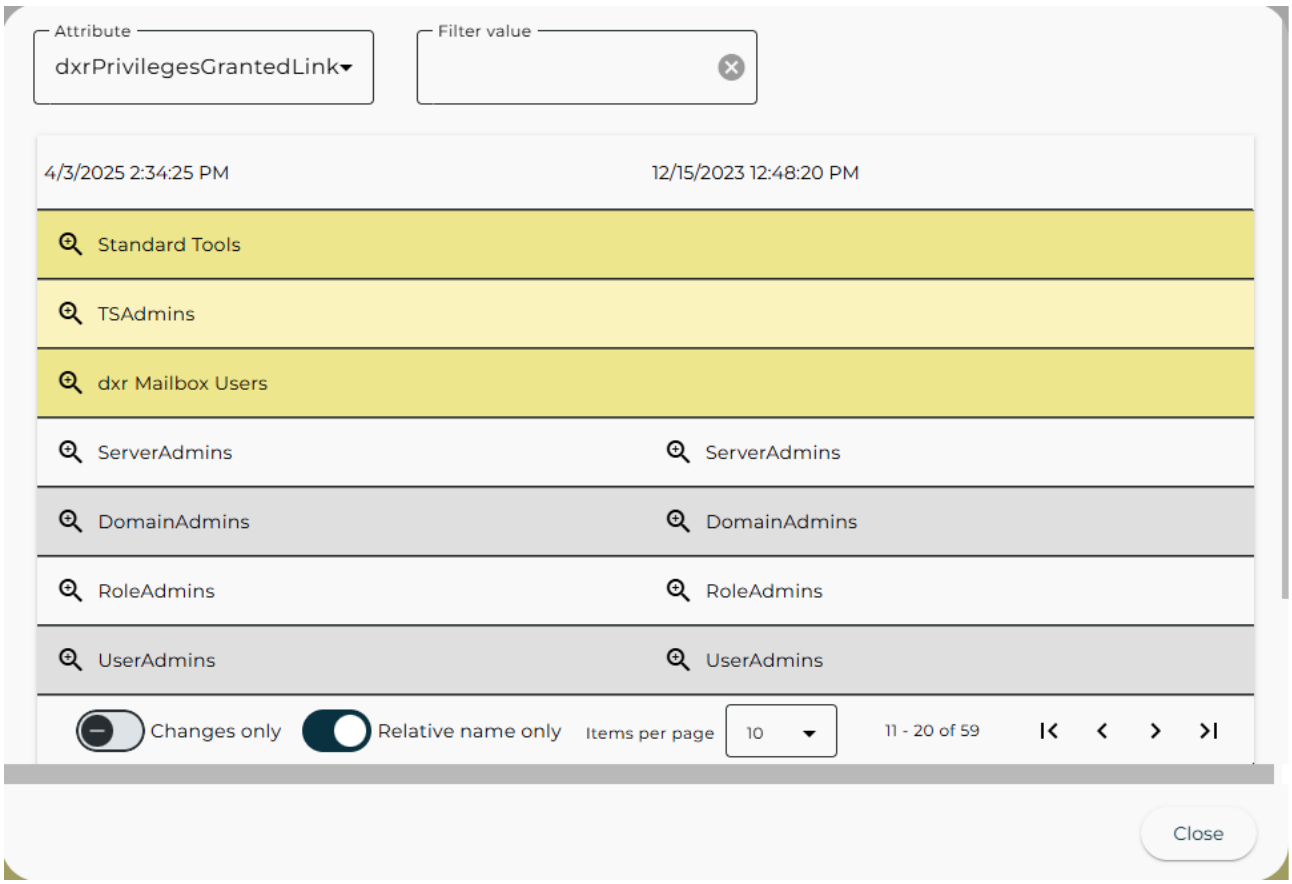


Figure 13. History – Multivalue Attributes Details

To refine your view and focus on relevant data, the Attributes tab offers several powerful filtering options:

- **Changes only** – displays only attributes with changed values across the selected time points.
- **Relative name only** – displays relative names instead of full Distinguished Names (DNs), improving readability.
- **Filter value** – searches for specific attribute values. The filter uses a “Contains” comparison operator. For example, entering “Admin” returns all values that include “Admin” in the full DN.

Some attribute values are references to other entries in the system. Click the **Show Details** icon next to a referenced value to open the history entry details for that referenced entry. This allows you to seamlessly explore related entries and understand the broader context of changes.

4.5.2. The Events tab

The **Events** tab displays all audit events related to the selected history entry.

The default filter is:

- **When** set to **Any time**,
- **Search in** set to **All**.

The filter included the following fields:

- **When** – filters audit events by time period:
  - Relative: **Previous Year**, **Previous Month**, **Month to date** and so on.
  - Absolute: **Custom Time** to define a specific range using the **From** and **To** fields. Timestamps are rounded to the nearest second. For example, to find an audit event at “4/4/2025 2:24:18.408 PM”, set **To** to at least “4/4/2025 2:24:19 PM”.
  - **Any time**: No time filter applied. The fields **From** and **To** are not visible in this case.
- **Search in** – filters events by the attribute to search in:
  - **Who**, the actor who triggered the event,
  - **What**, the object affected,
  - **All** for both **Who** and **What**.

This helps narrow down results when working with a large number of audit events.

The audit events are presented in the same format as the Audit Analysis results. To view more details about a specific related event, click the **Show details** icon. To return to the previous results list, click the **Back** ← icon in the top-right corner of the page.

Note: If audit message data has been purged from the DirX Audit Database, some additional information or the original message may no longer be available in the Event Details window. Similarly, if related audit messages have been purged, the list of related events may be incomplete.

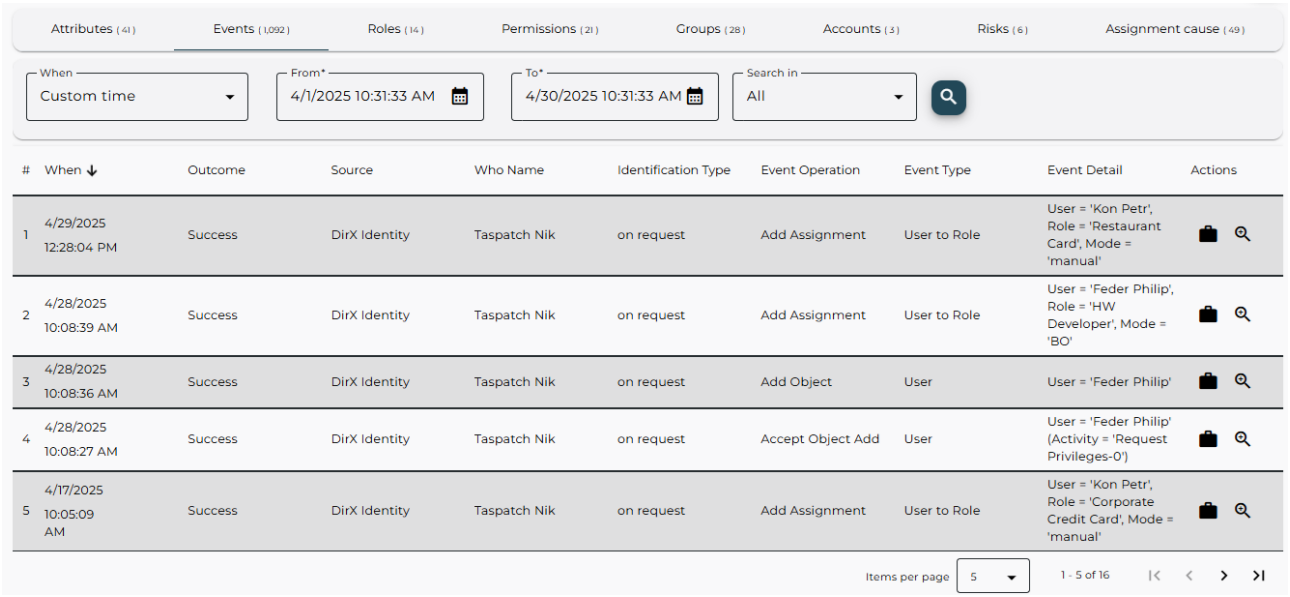


Figure 14. History – Events Tab

4.5.3. The Roles, Permissions, Groups and Accounts tabs

Roles, **Permissions**, **Groups**, and **Accounts** tabs are available for User history entries and are structured differently from the standard attribute-based tabs to better represent assignment relationships and their metadata. Each tab displays a list of assigned items: roles, permissions, groups, and accounts.

The Name column may include:

- assignment mode for privileges: rule, BO, manual, inherited,
- target system name for groups and accounts.

Each comparison time point column shows:

- whether the assignment existed at that time,
- additional assignment data such as:
  - start date and end date,
  - needs re-approval, in approval, and is inconsistent flags,
  - role parameter values for manual user to role assignments,
  - validity period, for user to privilege assignments,
  - state and connected system state for groups and accounts,
  - login name for accounts.

These tabs are analogously structured for history entries of the Role and Permission entry types.

Click the **Expand row** › icon next to an item's name to view its state and properties.

Click the **Show assignment cause** icon next to a privilege name to open the **Assignment cause** tab directly for that item.

These tabs may include filter fields to help you quickly search through large datasets, for example, many users in a role or many accounts in a target system.

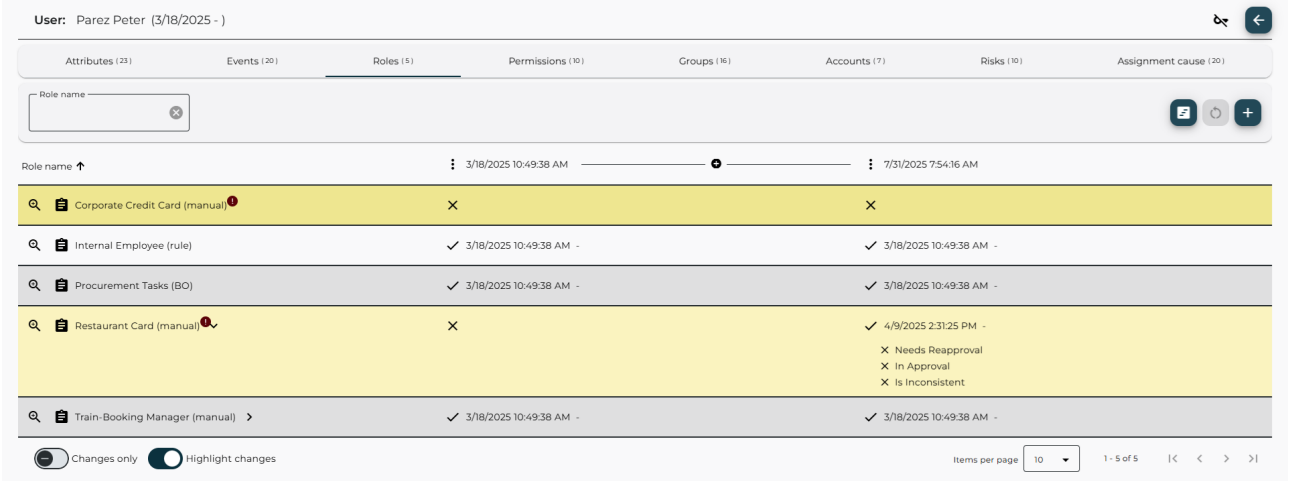


Figure 15. History – Roles

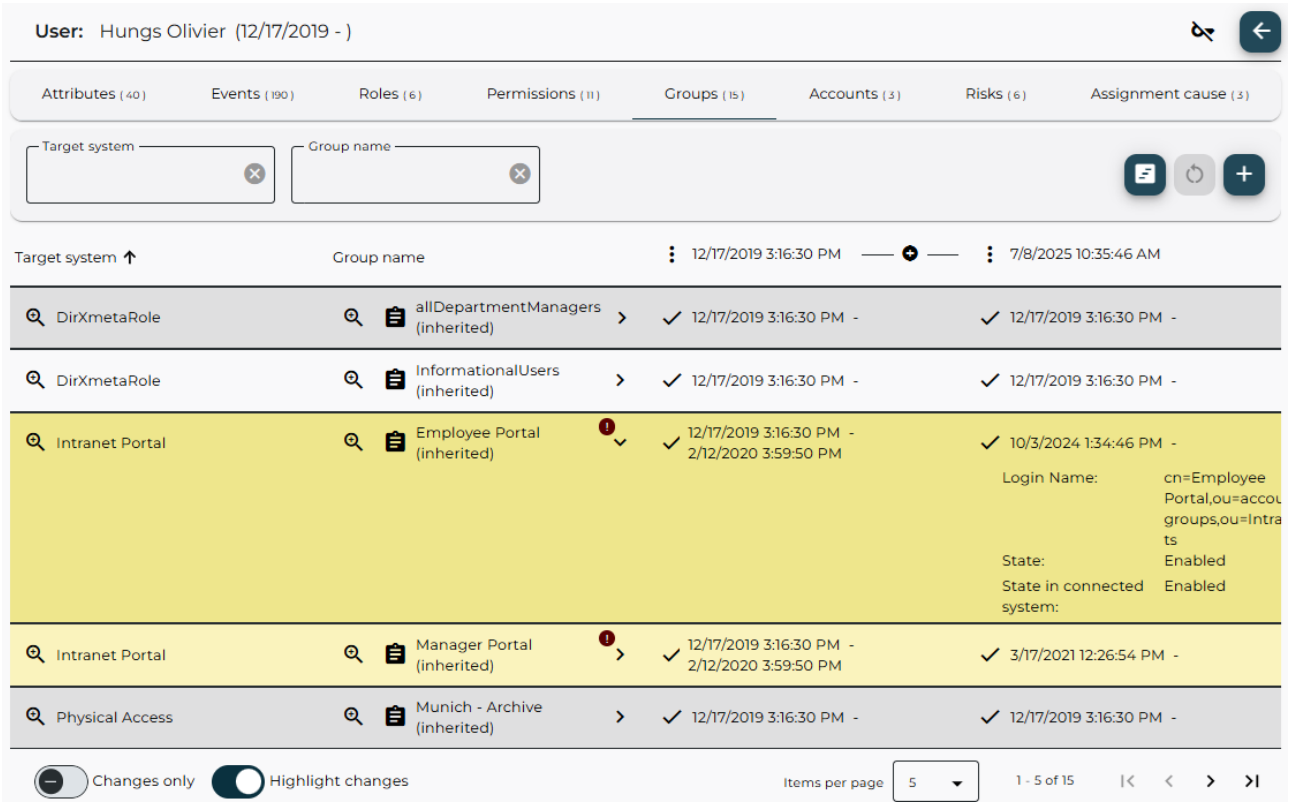


Figure 16. History – Groups

4.5.4. The Risks tab

The **Risks** tab displays user risk data derived from DirX Identity risk factors and overall risk values. These values are synchronized from the DirX Identity store into the DirX Audit Database, along with other user-related data. The tab provides insight into potential compliance or security risks associated with the user, based on predefined risk models and factors. This tab is especially useful for auditing and monitoring users with elevated access or unusual activity patterns.

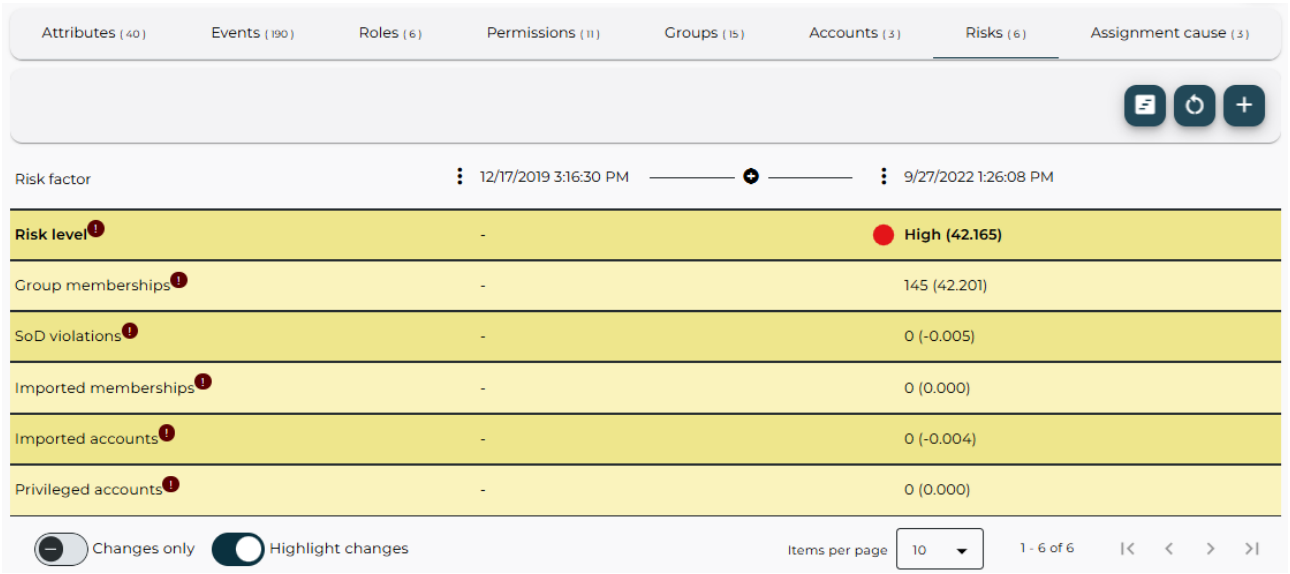


Figure 17. History – Risks

4.5.5. The Assignment cause tab

The **Assignment cause** tab displays the causing events that led to the assignment of a selected privilege. This helps trace the origin and rationale behind privilege assignments. In the last **Actions** column, click the **Show related events** icon to open a list of contextually related audit events. These events are correlated with the selected audit event to provide a broader view of the assignment context. For details, see the section "Viewing Related Audit Events".

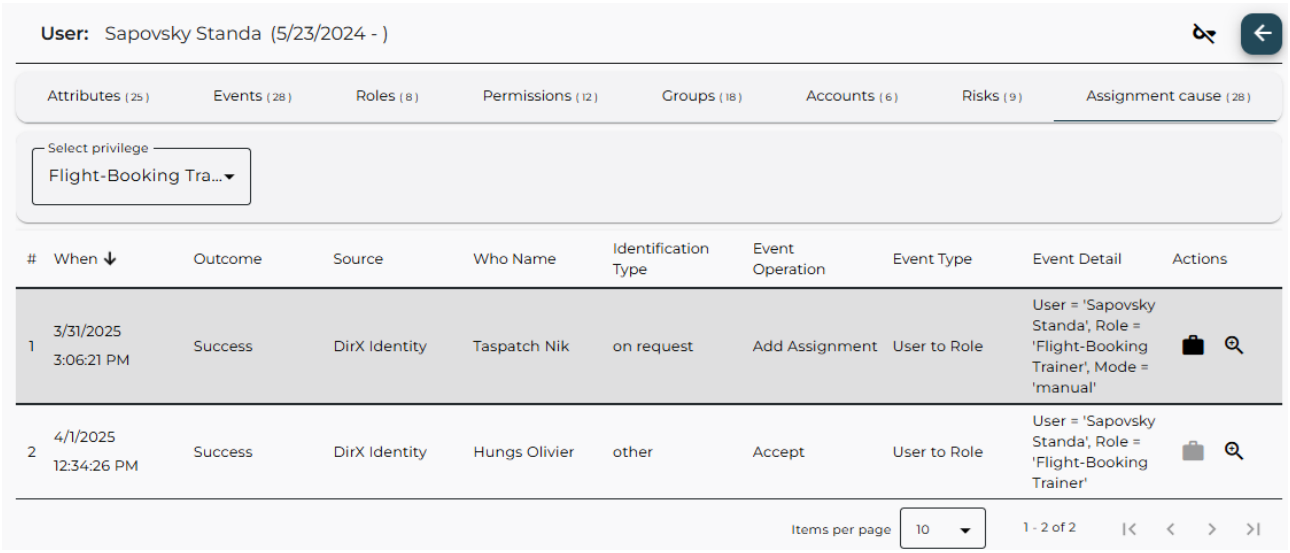


Figure 18. History – Assignment cause

While browsing the Roles, Permissions, or Groups tabs, you can directly switch to the **Assignment cause** tab for a specific privilege by clicking the **Show assignment cause** icon next to its name. This opens the **Assignment cause** tab pre–filtered for the selected privilege, streamlining your investigation.

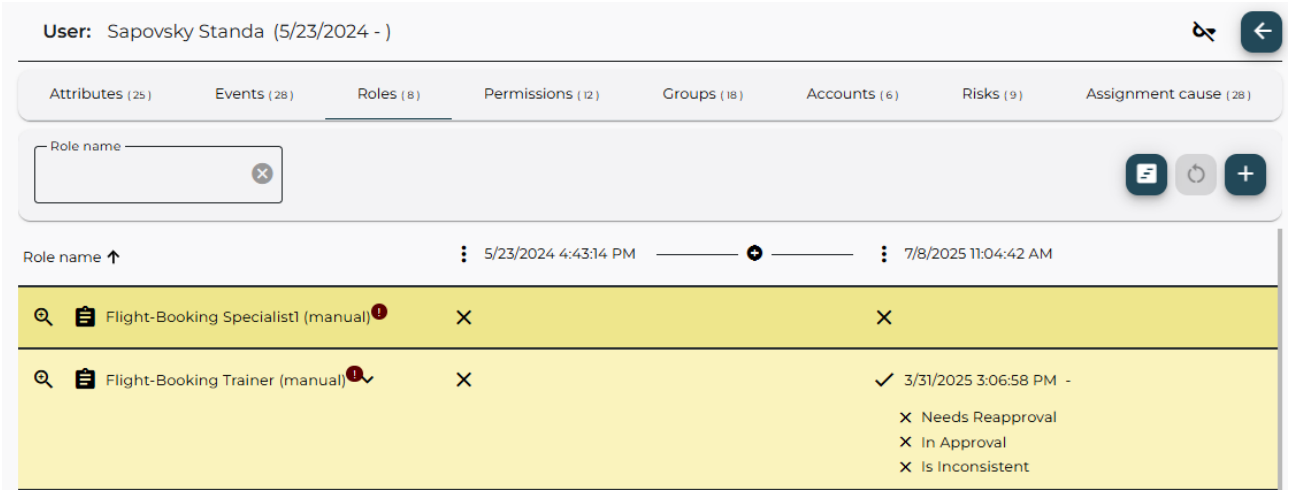


Figure 19. History – Assignment cause from privilege

4.5.6. The Overview tab

The **Overview** tab is available only for history entries of the Workflow Instance, Certification Campaign, and Certification Assignment Change history entry types. This tab serves as the default view for these entry types and provides a high-level summary of key information:

- name, (workflow) type, status, operation, subject, requester, start date, end date, and related activities for Workflow Instances,
- name, description, type, start date, end date, expiration date, owner, state, and so on for Certification Campaigns,
- start date, end date, reason, and so on for Certification Assignment Change.

This tab helps users quickly understand the context and progress of workflows and certification processes without needing to navigate through detailed attribute or event data.

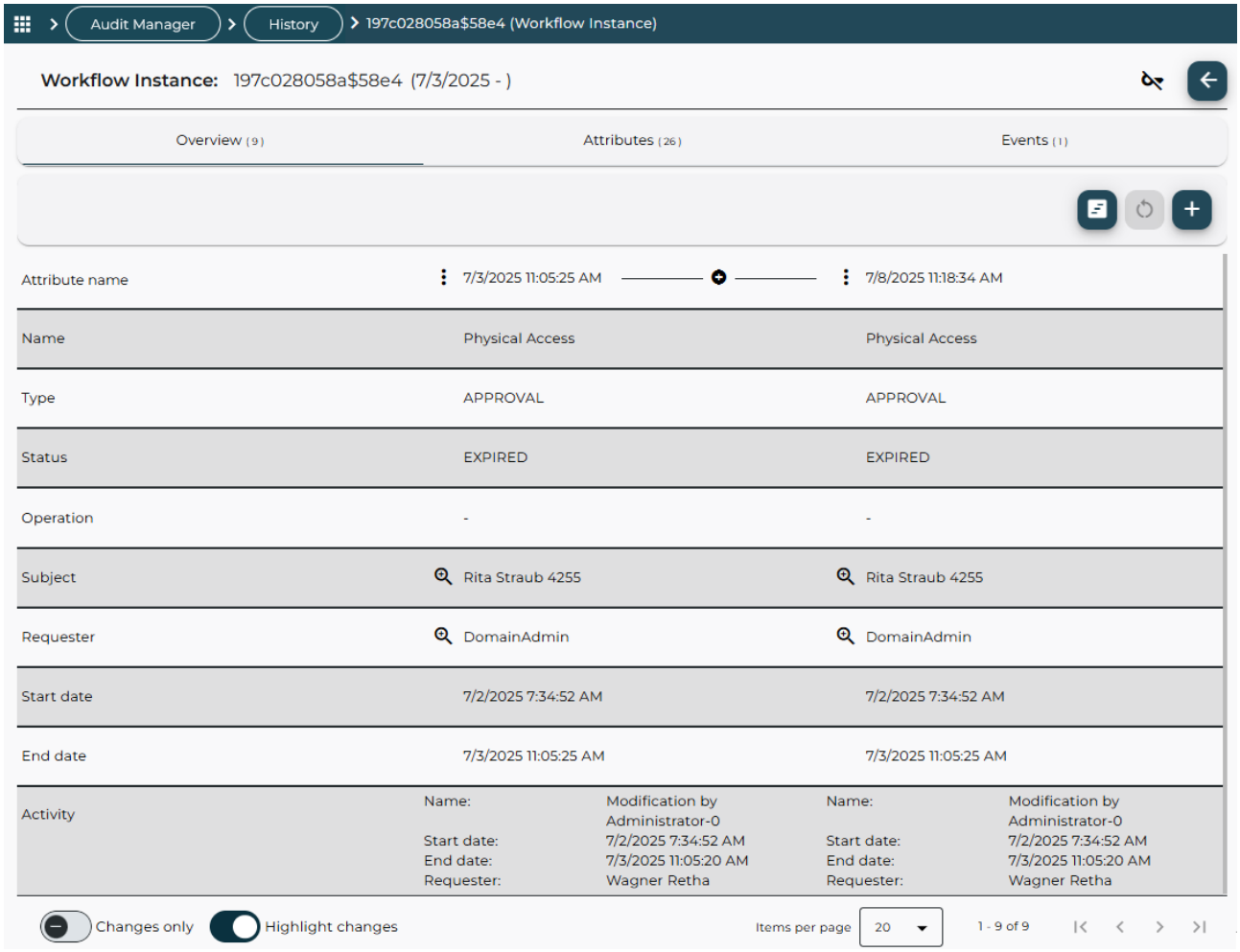


Figure 20. History – Overview for Workflow Instance

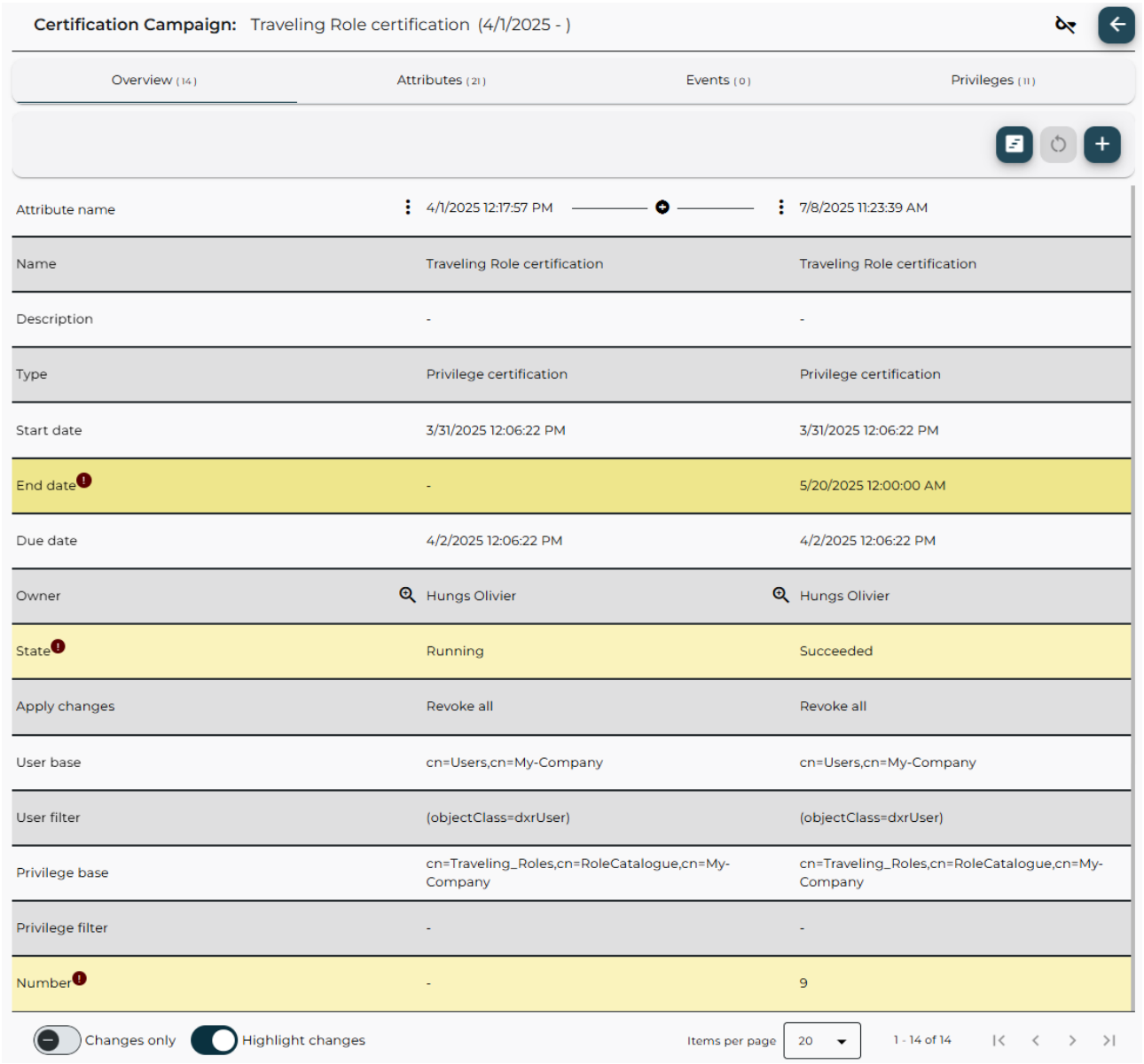


Figure 21. History – Overview for Certification Campaign

4.6. Exporting History Entries

To export history entries displayed in the search results table into a report-formatted file, click **Report** in the filter definition area. The **History entries report** dialog appears, allowing you to configure the export settings:

- **Report definition** – Select a predefined report definition to structure the exported data.
- **Report templates** – Choose a report template that defines the layout and formatting of the report.
- **Style** – Select the visual style to apply to the report.
- **Format** – Choose the file format, such as: PDF, CSV, Microsoft Word formats (DOCX, RTF), and others.
- **Language** – Select the language for the report content.

- **Encoding** – Choose the character encoding, for example, UTF-8, Big5, EUC-JP.
- **Entries limit** – Defines the number of rows to include in the report. Currently limited to the number of rows displayed on the first page of search results table.
- **Action** – Choose what to do with the report file:
  - **Download** – Save the file directly.
  - **Open** – Open the report in a new browser tab.
- **Show** – Choose whether to display **DN** (distinguished name) or **Path** in the report. The default is **DN**.
- **Create short report** – Enable this to generate a summary report. It combines multiple history entry versions, for example, same user with different DNs, into a single line. If disabled, all versions are listed individually.

Click **Export** to generate the report. Click **Cancel** to exit the dialog. After clicking **Export**, your browser may prompt you to open, save, or cancel the report file download.

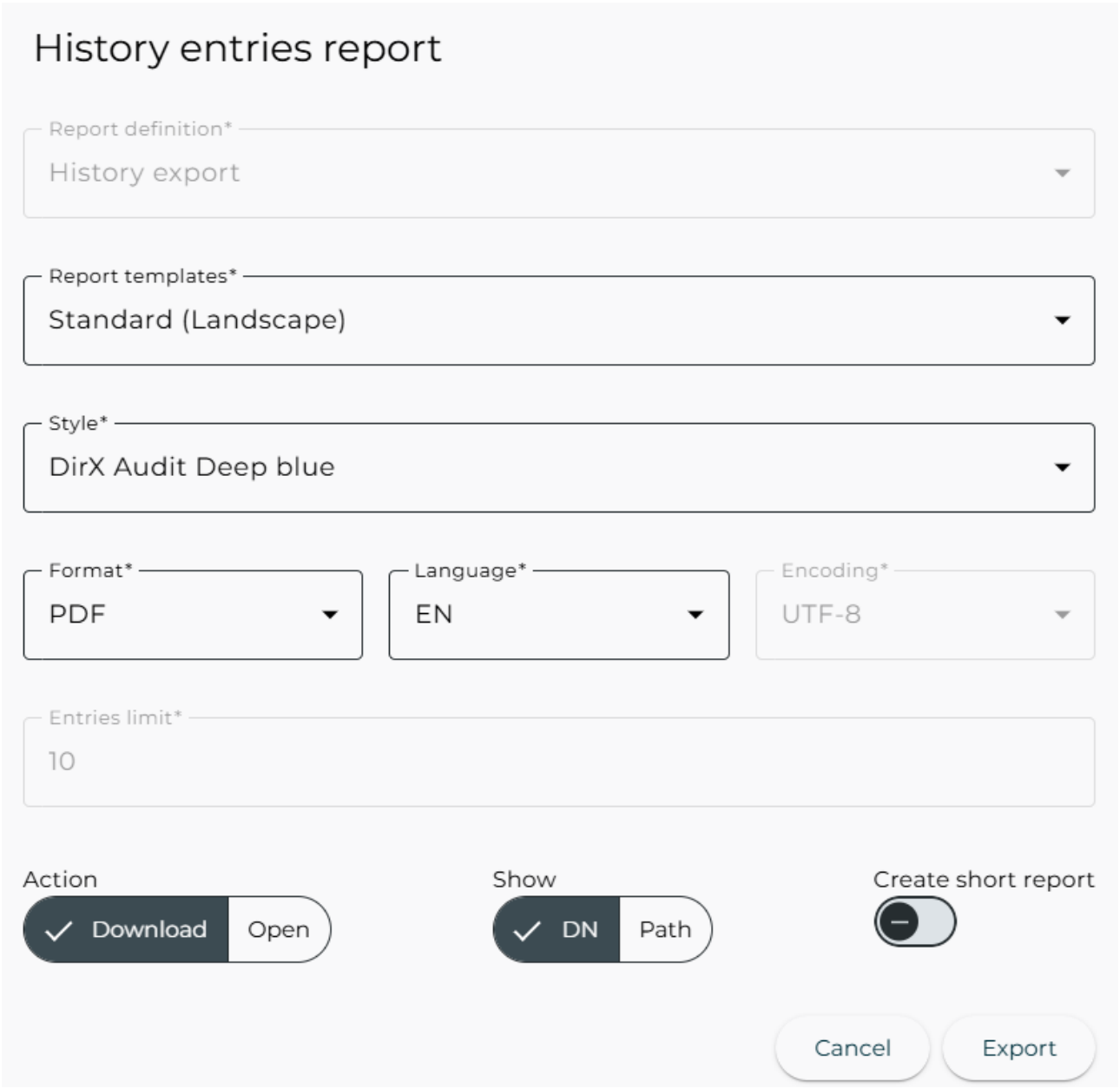


Figure 22. History – History entries report

5. Using Reports

The Reports page is a configuration interface for setting up scheduled reports. The DirX Audit Server automatically generates these reports based on a defined schedule and sends them via email to specified recipients.

A report set defines:

- one or more report files to be sent, each report file contains one or more individual reports,
- the schedule for sending the report set,
- the conditions under which the report set is generated,
- the recipients of the report set.

This chapter describes how to:

- Navigate the Reports main page
- Create a report set
- Edit a report set
- Delete a report set
- Activate and deactivate report sets
- Synchronize report set updates to the DirX Audit Server

5.1. Navigating the Reports Main Page

The Reports page consists of:

- a toolbar at the top of the page,
- a table displaying the current report set definitions.

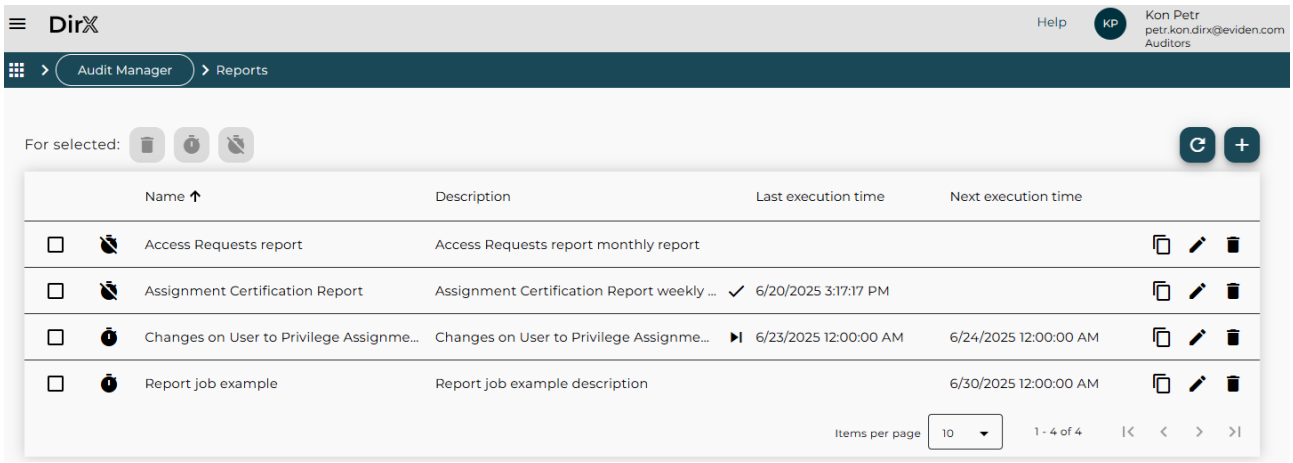


Figure 23. Reports – Main Page

The toolbar provides a set of actions for managing report sets efficiently. These are divided into actions for selected report sets and general functions.

Actions for selected report sets:

- **Delete selected** – removes the selected report sets from both the table and the configuration database.
- **Activate selected** – enables scheduled report generation for the selected report sets.
- **Deactivate selected** – pauses scheduled execution for the selected report sets.

General Functions:

- **Reload** – refreshes the definitions and statuses of all report sets stored in the configuration database.
- **Add a report set** – opens a form to create a new report set from scratch.

The report set table displays a list of report set definitions, including the following columns:

- Name – the name of the report set.
- Description – a brief description of the report set.
- Last execution time – the date and time, and result of the most recent report run.
- Next execution time – the scheduled date and time for the next report run.

You can perform the following actions directly in the table:

- Select / Unselect – Use the checkbox in the first column to select or unselect report sets. This is useful for applying toolbar functions to multiple selected report sets at once.
- **Activate report** / **Deactivate report** – Use the corresponding icons to enable or pause scheduled execution for a specific report set.
- **Clone**, **Edit**, or **Delete** – Duplicate, modify, or remove an existing report set.

In the **Last execution time** column, the result of the last report run is indicated by an icon:

- **Success** – The report was generated successfully.
- **Skipped** – The report conditions were not met, and the report was not generated.

Users with the Restricted Auditor application role have limited access:

- They can only view the **Reports** component within the DirX Audit Manager.
- They are restricted to using report templates tagged with Restricted, as described later in this section.

5.2. Creating a Report Set

To define a new report set, click the **Add a report set** icon in the toolbar. This action opens the **Add a report set** dialog, as illustrated in the following figure:

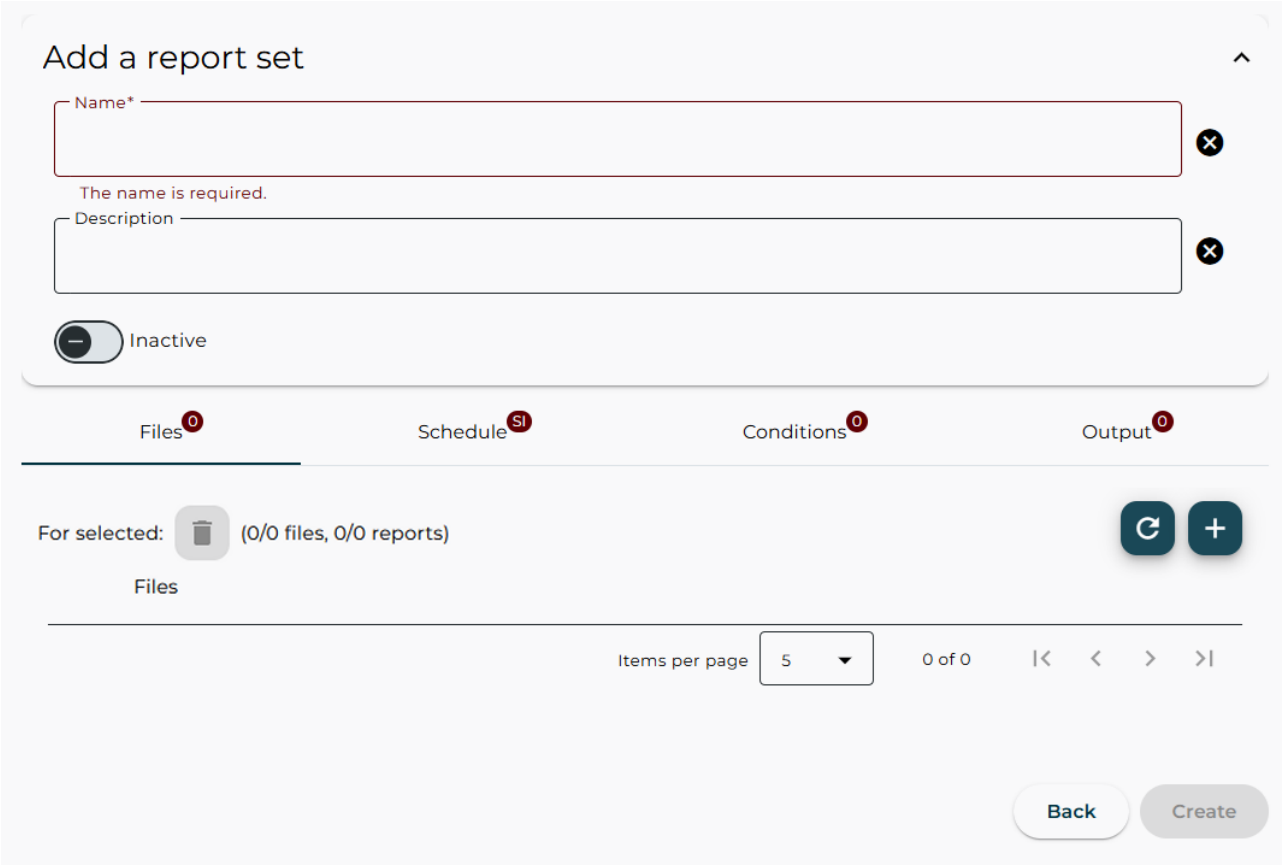


Figure 24. Reports – Add a report set

The **Add a report set** dialog allows you to define a new report set. It contains the following fields and configuration tabs:

- **Name** – a name for the report set. This is a mandatory field.
- **Description** – a brief description of the report set.
- **Active / Inactive** checkbox – select to activate or deactivate the report set.
- **Files** tab – specifies the report files to be sent via e-mail and the reports included in each file.
- **Schedule** tab – defines when the reports should be generated.
- **Conditions** tab – configures the conditions under which the report will be generated.
- **Output** tab – specifies the e-mail settings for sending the generated report (sender, recipients, message content).
- **Back** – cancels the operation and closes the dialog.
- **Create** – saves the report set definition.

To create a new report set using the dialog:

1. Enter a **Name** and **Description** for the report set.
2. Open the **Files** tab to define one or more report files and add them to the report set. For details, see "Creating a Report File".
3. Open the **Schedule** tab to define when the report set should be executed.

For details, see "Defining the Schedule".

4. Open the **Conditions** tab to configure the conditions for report generation.
   For details, see "Conditioning the Report Set Execution".
5. Open the **Output** tab to define the e-mail recipients and message content.
   For details, see "Defining the E-mail Message".
6. Click **Create** to save the new report set definition.

5.2.1. Creating a Report File

To create a new report file for a report set, click the **Add a new report file** + icon in the **Files** tab header of the **Add a report set** dialog for new report sets or the **Edit the report set** dialog for existing report sets.

This action opens the **Add a new report file** dialog, where you can:

- Add one or more reports to the report file.
- Set the file's name and format.
- Select a report definition.
- Configure the scope and output format for each report.

The following sections describe these steps in more detail:

- "Defining the Report File Name and Format"
- "Selecting a Report Definition"
- "Setting the Report File Scope"

Use the **Reload** ↻ icon in the **Files** tab header to refresh the report set definition stored in the configuration database.

5.2.1.1. Selecting a Report Definition

The selection dialog allows you to choose a report definition from a list of existing templates. The following figure shows an example of this dialog:

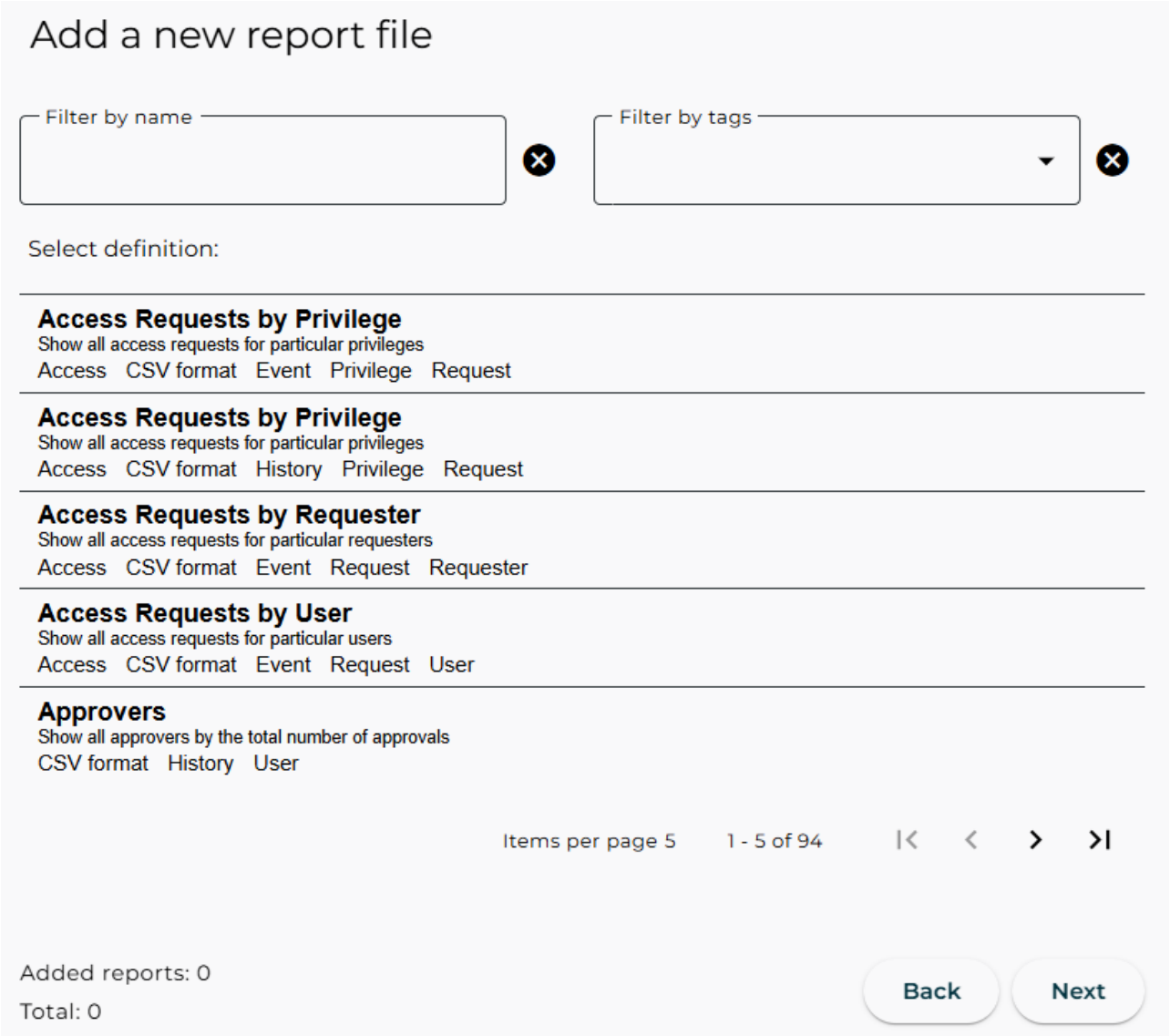


Figure 25. Reports – Add a report set – Select definition

Each item in the list displays the report definition's name, description, and associated tags. Use the page navigator at the bottom of the dialog to browse through the list.

Use the **Filter by name** and **Filter by tags** fields to narrow down the list:

- To search by name, enter a string in the **Filter by name** field. The list updates to show all report definitions whose names contain the entered string.
- To search by tag, click in the **Filter by tags** field to display available tags and select one or more. You can also click a tag shown in the report definitions list to add it to the filter. The list updates to show only report definitions that match:
  - **All** selected tags, or
  - **Any** selected tag.

Note: Some report definitions include the **Restricted** tag. Users with the **Restricted Auditor** application role can only view and use reports with this tag.

To select a report definition, click it. This opens a dialog for configuring the scope and

output format of the selected report.

Click **Back** to cancel the selection and return to the previous dialog.

5.2.1.2. Setting the Report File Scope

The report file scope dialog allows you to provide input parameter values required for the report definition selected in the **Report Definition Selection** dialog.

At the top of the dialog, the name, description, and tags of the report definition are displayed followed by a list of available templates. Some reports offer multiple templates, allowing you to choose the one that best fits your needs. The selected template determines which sections are shown in the scope definition dialog. For example, if you select a **Spreadsheet (CSV)** template, the **Select columns** section is displayed, allowing you to choose which columns will be included in the resulting report. On the other hand, the **Create short report** checkbox is not available when a CSV template is selected.

In the **Style** section, you can choose a predefined color scheme for the generated report to match your visual preferences or organizational standards.

Some input parameter values are mandatory, while others are optional, depending on the report definition.

In the **When** section, define the time range or time point for the report:

- **Time range options** for audit events or history entries:
  - Previous day, Previous week, Previous month, Previous year
  - Week to date, Month to date, Year to date
  - Last hour, Last 24 hours, Last 7 days, Last 30 days, Last month, Last 3 months
  - Today
  - Custom time – fixed start and end date and time
  - Any time
- **Time point options** for history entries:
  - End of previous day, End of previous week, End of previous month, End of previous year
  - Custom time point

Other sections in the dialog allow you to configure the following:

- A list of entries, such as users, privileges, target systems.
- Filter attributes, such as organizational units and organizations.

If no value is specified for an optional variable, the report will include all matching entries.

Additional options may be available as checkboxes:

- Create short or regular output. Short output shows key information in one line. Regular

output uses multiple lines per entry.

- Include only orphaned, imported, or disabled accounts.
- Include only failed events, such as failed logins.

The **Pseudonymize** option determines whether sensitive user data is displayed in the report.

The **Record limit** parameter allows you to restrict the number of records in the final report. A value of **0** means no limit.

The following figure shows an example of the dialog used to select a list of requesters, filtered by the identifying attribute Last Name.

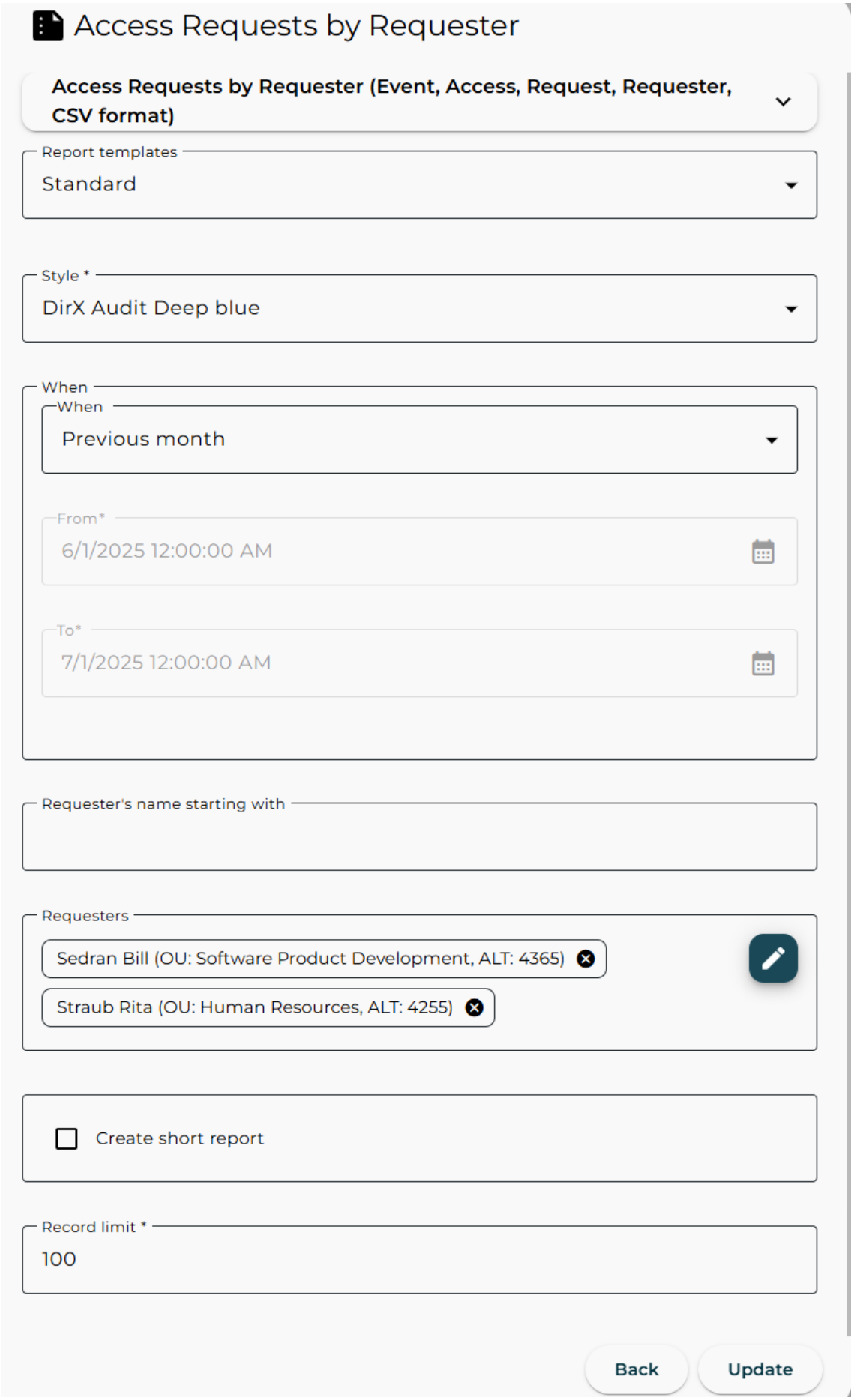


Figure 26. Reports – Report File Scope

Click **Back** to cancel the report file scope definition and return to the previous dialog. Click **Create** to save the report file scope definition and add the report to the report file.

Once a report is added, a summary is displayed. You can continue adding more reports to the same report file. The footer of the dialog shows the number of reports added and the total number of reports in the file.

Click **Next** when you have finished defining the scope for all reports you want to include in the report file. You will then proceed to define the report file name and format.

5.2.1.3. Defining the Report File Name and Format

Enter a **Name** and **Description** for your report file, and specify its file format. The following options are available:

- **Format** – defines the output format of the report file. You can choose from formats such as PDF, DOCX, HTML, or XLSX. Note: If you combine multiple reports into a single report file, only the PDF format is supported. In this case, PDF is automatically selected and cannot be changed.
- **Language** – specifies the language for localized reports. Available options are English and German.
- **Encoding** – sets the character encoding for report generation. If only one encoding is supported, it is preselected and cannot be modified.

Click **Create** to generate the report file and continue configuring your report set.

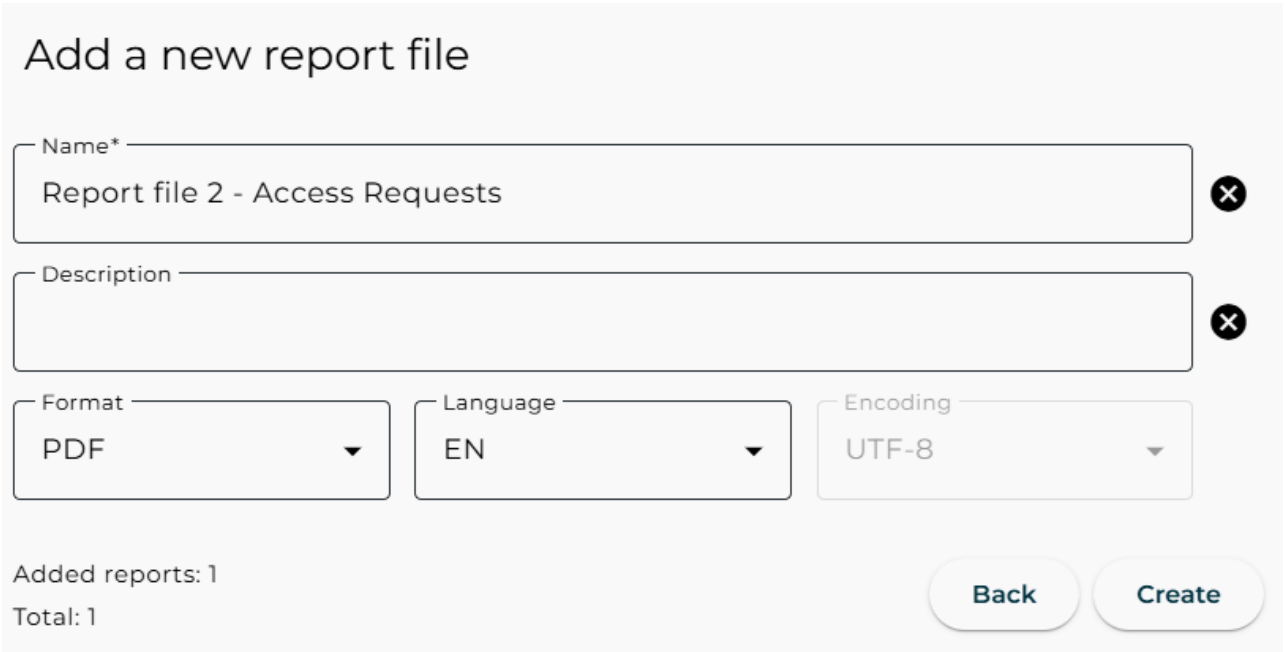


Figure 27. Reports – Add a new report file

To add additional report files to the report set, use the **Add a new report file** + icon in the Files tab of the Add a report set dialog.

Once all report files are defined, proceed with the **Schedule**, **Conditions**, and **Output** tabs to complete the report set configuration.

5.2.2. Defining the Schedule

Use the **Schedule** tab in the **Add a report set** dialog for a new report set or in the **Edit the report set** dialog for an existing report set to configure when the report files should be generated. You can choose from the following scheduling options:

- **Simple** – runs the report set once at a specified date and time.
- **Recurring** – allows the report set to run repeatedly on a daily, weekly, or monthly basis:
  - Specify a **Start date** and, optionally, an **End date**.
  - If no end date is set, the schedule continues indefinitely.
  - For weekly schedules, select the days of the week.
  - For monthly schedules, select a specific day or choose **Last day of month**.
- **Expert** – uses a cron expression to define a custom schedule.
  - Specify a **Start date** and, optionally, an **End date**.
  - Enter a valid **cron** expression to define the schedule.
    For guidance, refer to the CronTrigger tutorial:
    https://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/tutorial-lesson-06.html
    For example, to run a report daily at 3:01 AM, use: `0 1 3 * * ?`
- **As Soon As Possible** – executes the report set immediately after it is read by the DirX Audit Server.
  - If the DirX Audit Server is not running, you can limit the execution window using the End date. If the request is read after the end date, it will be silently ignored.

Once the schedule is defined, proceed with the **Conditions** and **Output** tabs to complete the report set configuration.

5.2.3. Conditioning the Report Set Execution

The **Conditions** tab allows you to configure conditions that determine whether a report set should be generated at the scheduled time. These conditions are evaluated by the DirX Audit Server when the report schedule is triggered. If configured conditions are met, the report set is generated and sent; otherwise, it is skipped.

To use conditions:

- Activate the **Conditions** toggle.
- Click the **Add condition** icon to define a new condition.
  Note: You can only add conditions if at least one indicator is marked as a favorite. If no indicators are marked, the Add condition icon will be disabled.

Click the **Settings** ⚙ icon to view all available indicators, organized under the **Favorites**, **Public**, and **Product** tabs.

- To mark an indicator as a favorite, click the **Mark as favorite** ☆ icon in the **Actions** column of the **Public** or **Product** tab.

- Marked indicators appear in the **Favorites** tab and become available in the **Add condition** dialog.
- To remove a favorite, click the **Remove from favorites** ★ icon.
- You can reorder indicators in the **Favorites** tab using drag and drop.

For more information on creating public indicators and customizing them, see the *DirX Audit Customization Guide*.

Click the **Add condition** + icon to open the condition editor: to select and add an indicator that will be evaluated to run the report.

- **Indicator** – Select a favorite indicator.
- **Operator** – Choose a comparison operator such as **Greater than**, **Less or Equal to**, **Not equal to**.
- **Value** – Enter the value to compare against.

Click **Create** to save the condition, or **Back** to cancel.

Example: Generate the report only if the number of added groups in the last 30 days is greater than or equal to 5.

Figure 28. Reports – Add a new report file – Add condition

You can define multiple conditions for a report set. Use the **Mode** setting to control how they are evaluated:

- **All** – All conditions must be met.
- **Any** – At least one condition must be met. Conditions are evaluated sequentially. Once one is satisfied, the rest are skipped.

You can reorder conditions using drag and drop.

Note: Conditions do not need to be directly related to the report content. For example, you can trigger a report on failed logins based on a condition involving deleted user accounts.

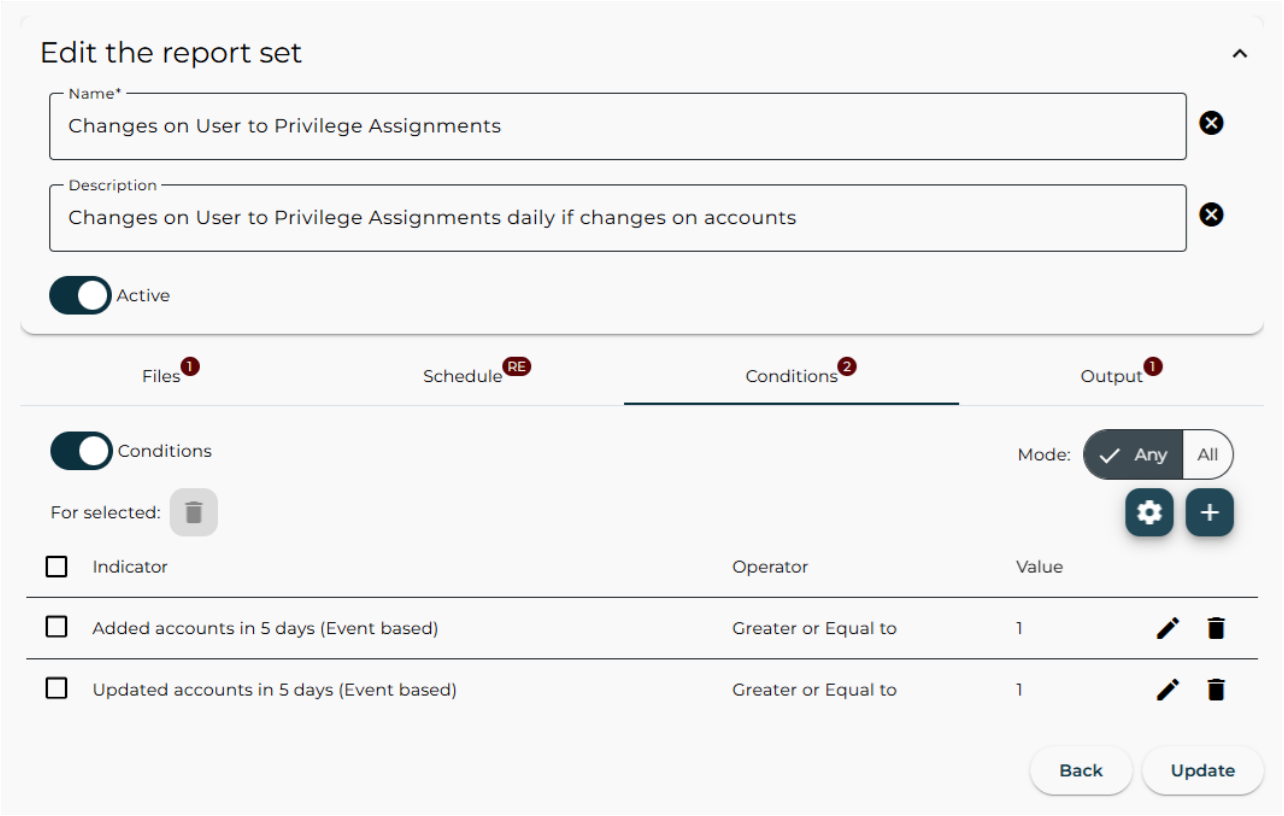


Figure 29. Reports – Edit the report set – Conditions

Once the conditions are defined, proceed with the **Output** tab to complete the report set configuration.

5.2.4. Defining the E-mail Message

Use the **Output** tab in the **Add a report set** dialog for new report sets or the **Edit the report set** dialog for existing report sets to configure the e-mail settings used to deliver the generated report.

- Enter a valid e-mail address in the **To** field and press Enter.
- The **CC** and **BCC** fields are also available.
- You can add multiple addresses to each field.
- At least one valid e-mail address is required.
- To remove an address, simply delete it from the list.

Once your report set is completed:

- Click **Create** to save the report set to the configuration database.
- To activate the report set, click the **Activate report** icon in the report set definitions table.

5.3. Editing a Report Set

To edit an existing report set, click the **Edit** icon in the row of the desired report set in

the table displaying all report sets. This opens the **Edit the report set** dialog:

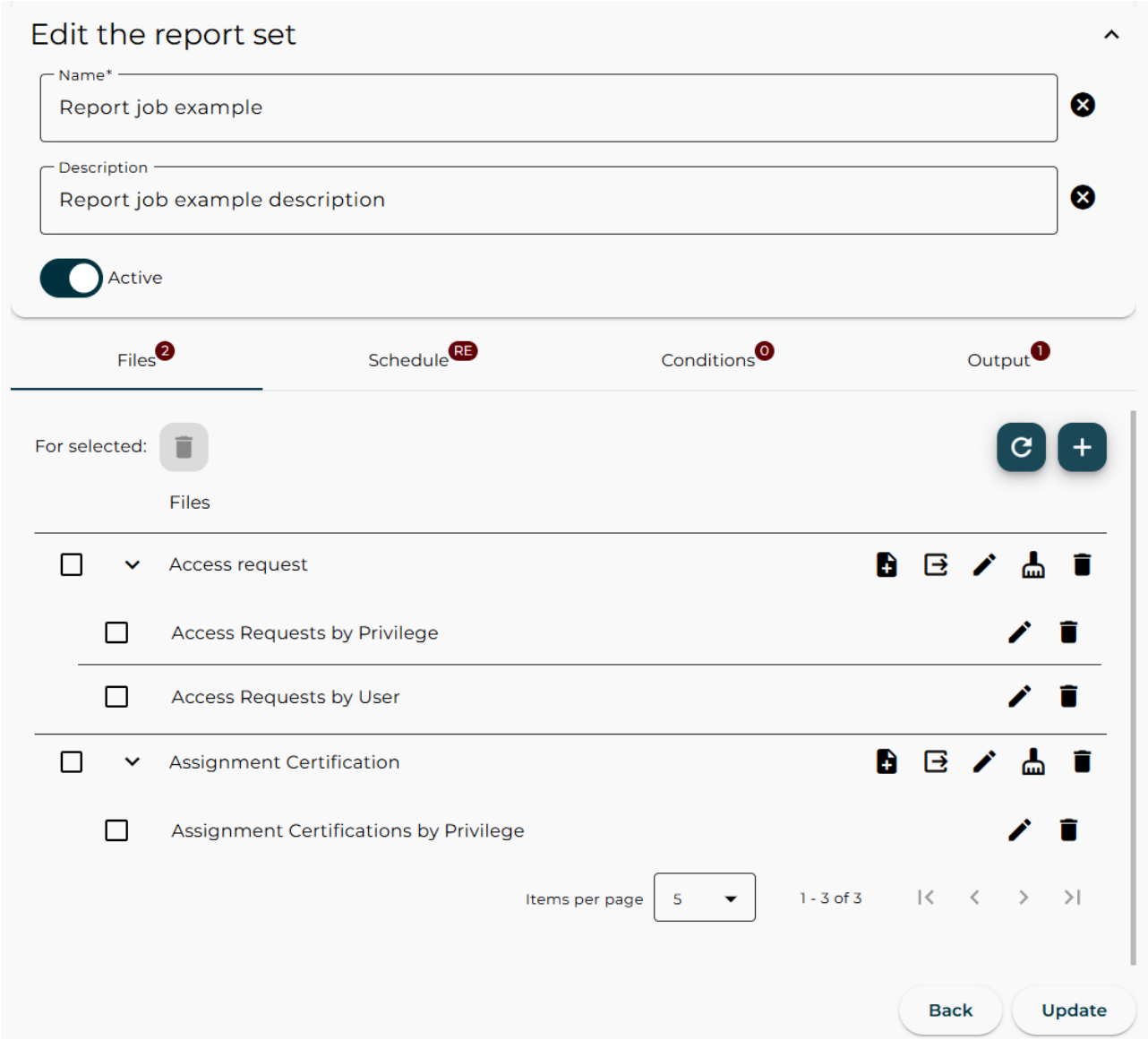


Figure 30. Reports – Edit the report set

In the **Files** tab, you can view and manage the report files included in the report set, along with the individual reports within each report file.

Managing the report files list:

- To refresh the report files list, click the **Reload** icon in the **Files** tab header.
- To add a new report file to the edited report set, click the **Add a new report file** + icon. For details, see "Creating a Report File".

Managing report files:

- To add a report to a report file, click the **Add reports** icon next to the desired report file to open the **Add reports** dialog. For details, see "Selecting a Report Definition".
- To export a report file, click the **Export** icon. This is useful for previewing the report file before scheduling the report set.

- To edit report file properties, click the **Edit** icon to open the **Edit the report file** dialog. For details, see "Defining the Report File Name and Format".
- To clear all reports from a report file, click **Clear** icon.
- To delete a report file, click the **Delete** icon.

Managing reports within a report file:

- To edit report properties, click the **Edit report** icon next to the desired report listed under a report file. For details, see "Setting the Report File Scope".
- To delete a report from a report file, click the **Delete report** icon.

Managing the report set:

- To reconfigure the report set schedule, use the **Schedule** tab. See "Defining the Schedule".
- To reconfigure the report set conditions, use the **Conditions** tab. See "Conditioning the Report Set Execution".
- To reconfigure the report set output, use the **Output** tab. See "Defining the E-mail Message".
- You can also change the report set's name, description, and active/inactive status.

5.4. Deleting Report Sets

You can delete a single report set, multiple selected report sets, or all report sets from the table displaying all report sets:

- To delete a single report set, click the **Delete** icon in the corresponding row.
- To delete multiple report sets, select the checkboxes in the first column for the report sets you want to remove, then click the **Delete selected** icon in the toolbar.

To delete a report file from a report set or remove a report from a report file, click the **Edit** icon in the row of the selected report set and continue in the **Edit the report set** dialog. For details, see "Editing a Report Set".

5.5. Activating and Deactivating Report Sets

You can activate or deactivate a report set in the following way:

- Open the **Edit the report set** dialog and use the **Active / Inactive** toggle.

You can activate or deactivate a single report set, multiple selected report sets, or all report sets from the table displaying all report sets:

- To activate or deactivate a single report set, click the **Activate report** or **Deactivate report** icon in the corresponding row of the report set in the report sets table.
- To activate or deactivate multiple report sets, select the checkboxes in the first column for the report sets you want to remove, then click the **Activate selected** or

Deactivate selected icon in the toolbar.

5.6. Synchronizing Report Set Updates to the DirX Audit Server

Any changes made in the **Reports** component must be synchronized with the DirX Audit Server.

This synchronization is handled automatically by the DirX Audit Server, which checks for updates at regular intervals. The process typically completes within a few seconds.

If synchronization does not complete within one minute, verify with the application administrator that the DirX Audit Server service is running.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.