EVIDEN

Identity and Access Management

DirX Audit

User Interface Guide

Version 7.2, Edition June 2025

Table of Contents

Preface

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

- Chapter 1 provides an overview about the DirX Audit user interface.
- Chapter 2 describes how to log in to the interface and work with its main page layout.
- Chapter 3 describes how to use the DirX Audit Manager's Dashboard view.
- Chapter 4 describes how to use the DirX Audit Manager's Audit analysis.
- Chapter 5 describes how to use the DirX Audit Manager's Reports view.
- Chapter 6 describes how to use the DirX Audit Manager's History view.
- Chapter 7 describes the command-line tools for working with the DirX Audit Database.

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\Atos\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. User Interface Guide

DirX Audit provides the following user interfaces:

- DirX Audit Manager, a Web-based interface that allows auditors, security and compliance officers and audit administrators to run different views of the audit trails stored in the DirX Audit Database.
- Command line-based DirX Audit Database tools, which allow DirX Audit administrators to archive, purge and restore audit trails in the DirX Audit Database and maintain DirX Audit Database data structures.

The chapters in this guide are organized as follows:

- "Using the DirX Audit Manager" describes how to log in to the interface and work with its main page layout.
- "Using the Dashboard View" describes how to use the DirX Audit Manager’s Dashboard view.
- "Using Audit Analysis " describes how to use the DirX Audit Manager’s Audit analysis feature.
- "Using the Reports View" describes how to use the DirX Audit Manager’s Reports view.
- "Using the History View" describes how to use the DirX Audit Manager’s History view.
- "Using the DirX Audit Tools" describes the command-line tools for working with the DirX Audit Database.

2. Using the DirX Audit Manager

The DirX Audit Manager is DirX Audit's Web-based tool for searching and analyzing identity audit information contained in the DirX Audit Database. With the DirX Audit Manager, you can:

- Use the Dashboard view to search for and display identity audit data that the DirX Audit Server has aggregated according to standard and customized identity audit key performance indicators (KPIs) in graphical charts. This view allows you to perform analysis - especially time-based trend analysis of selected KPI data - and then drill down to details as necessary.
- Use Audit analysis to search for and display identity and access audit events stored in the DirX Audit Database. An audit event records a discrete operation within a logical sequence of operations contained in an audit message. Audit event data includes the audit message with the "who", what" and "where from" information extracted from the original message and an informational summary of the operation and the objects on which it operated. The Audit analysis displays page-through tables of audit events retrieved from the DirX Audit Database according to a set of search criteria that you define.
- Use the Reports view to create, edit, preview and manage scheduled automated advanced reports which can provide an immediate or regular overview of both audit events and history entries according to the specific scope and time filtering selected by the user. Data from all audited areas can be used enabling the user to produce correlated reports from different points of view combining chart representations with relevant events lists and history record details in single or multiple report documents.
- Use the History view to select a history entry stored in the DirX Audit Database and then display the details of the entry extended by a graphical timeline representation of its changes, including a view of related events within a selected time period.

The sections in this chapter describe how to log in to DirX Audit Manager and work with its main page layout.

Please do not use the **Back** button of the browser when working with DirX Audit Manager. If you need to go back to the previous page, please use the internal application **Back** button or the **Switch to search form** button or another user interface control with this functionality.

2.1. Logging In

To log in to the DirX Audit Manager, open your Internet browser. (See the *DirX Audit Release Notes* for supported browsers.) Specify the URL of DirX Audit Manager:

https://*hostname:port*/**AuditManager/?tenant=***tenantID*

where

hostname
specifies the hostname of the machine where DirX Audit Manager is running.

port
specifies the port number of the DirX Audit Manager application server. (The default is **8080** for a non-SSL connection or **8443** for an SSL connection).

tenantID
specifies the identifier of a configured tenant (that is, the organization). The specific tenant ID should be provided to users by administrators once they configure individual tenants according to their respective organization memberships or access needs.

For example:

`https://localhost:8080/AuditManager/?tenant=71a75691-d28a-48ce-a542-6d6af7ece680`

DirX Audit Manager displays the login page. In this page:

- **Tenant** conveys the tenant name specified by the tenant ID in the URL. This field is displayed only if multi-tenancy is configured. If you have only a single tenant configured, the tenant name field is not visible.
- Enter your user identification in **Name**, typically your common name in the DirX Identity or other LDAP directory.
- Enter your corresponding password in **Password**.
- Click **Login**.

If you have supplied the correct user name and password for the correct tenant specified by the tenant ID in the URL, DirX Audit Manager directs you to its main page. An auditor of a specific tenant will not see any data of another tenant.

If you don't have the permission to use DirX Audit Manager for a specific tenant, an error message is displayed and you will be logged out. In this case, you must be added to a privileged group with the correct permission within a specific tenant. (See the section "Managing a Multi-tenant Environment" in the *DirX Audit Administration Guide*; see the section "Configuring Privileged Groups" in the *DirX Audit Customization Guide* for supported groups.)

2.2. About the Main Page Layout

The DirX Audit Manager main page presents all of the elements you need to set up and run your auditing tasks. The following figure illustrates the DirX Audit Manager main page layout.

Figure 1. DirX Audit Manager Page Layout

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

- A company logo area that displays the company's logo and its name. See the section "Customizing the User Interface Layout" in the *DirX Audit Customization Guide* for information on how to customize the logo.
- A "welcome" message that identifies the logged-in user (for example, Tinker Boris).
- The user identification with DirX Audit roles assigned to the logged-in user in the form: *UserName*@*TenantName* (roles). *TenantName* is displayed only if multi-tenancy is supported. If you have only one tenant configured, you will see only: *UserName* (roles). For more information, see the section "Accessing Components" in this guide or the section "Managing a Multi-tenant Environment" in the *DirX Audit Administration Guide*.
- A language selection area that allows you to display the page in English (EN-US or EN-GB with specific time formatting), German or French. By default, DirX Audit Manager uses the language selected in the browser. Click **US** to select English with the time formatting for USA or **GB** to select English with the time formatting for Great Britain. Click **DE** to select German or **FR** to select French. The browser then displays the page in the language you have selected.
- **Dashboard**, **Audit analysis**, **Reports** and **History** tabs. Click a tab to select the corresponding view. You can configure the default tab displayed after user login in the Core Configuration Wizard in the Manager Application dialog. Note that the Dashboard or History tabs are only displayed if you have purchased a license for them and you selected them during installation. Note that the restricted auditor has no access to the Dashboard, Audit analysis and History views; only the Reports tab is available and opened by default in this case.

- **Help** menu for displaying the DirX Audit Manager online help (this guide).
- **Logout** icon for exiting the DirX Audit Manager.
- A page footer that displays additional information like the copyright information.

2.3. Configuring DirX Audit Manager

DirX Audit Manager supplies configuration switches that allow you to control how it operates. See the *DirX Audit Customization Guide* for details.

3. Using the Dashboard View

The Dashboard view allows you to analyze identity audit data that has been aggregated according to key performance indicators (KPIs) and stored as online analytical processing (OLAP) data cubes in the DirX Audit Database. DirX Audit provides a set of pre-defined OLAP data cubes that cover the most commonly used identity audit KPIs and allows you to configure your own customized OLAP data cubes.

To view and analyze this data, you select from a set of Dashboard "components" that are displayed in tiles (or "zones") in the Dashboard main page. Each component displays one aspect of the aggregated data stored in a KPI-based data cube - for example, the total number of password changes made, by date, within the last month - in one of the available tiles. DirX Audit provides a set of standard components that you can use right away and allows you to create your own components.

This chapter describes the features of the Dashboard page and how to:

- Select and display components and control the Dashboard page layout.
- Drill down from the data in the Dashboard view to more detailed data in the events view.
- Export the data provided in a component to a file.
- Send component data in an e-mail.
- Schedule the generation of a component report.
- Select the data to be provided in a component and how it is to be displayed.
- Import component data stored in a file to the Dashboard.
- Create a new component.

3.1. About the Dashboard Main Page Layout

The Dashboard main page layout is shown in the following figure.

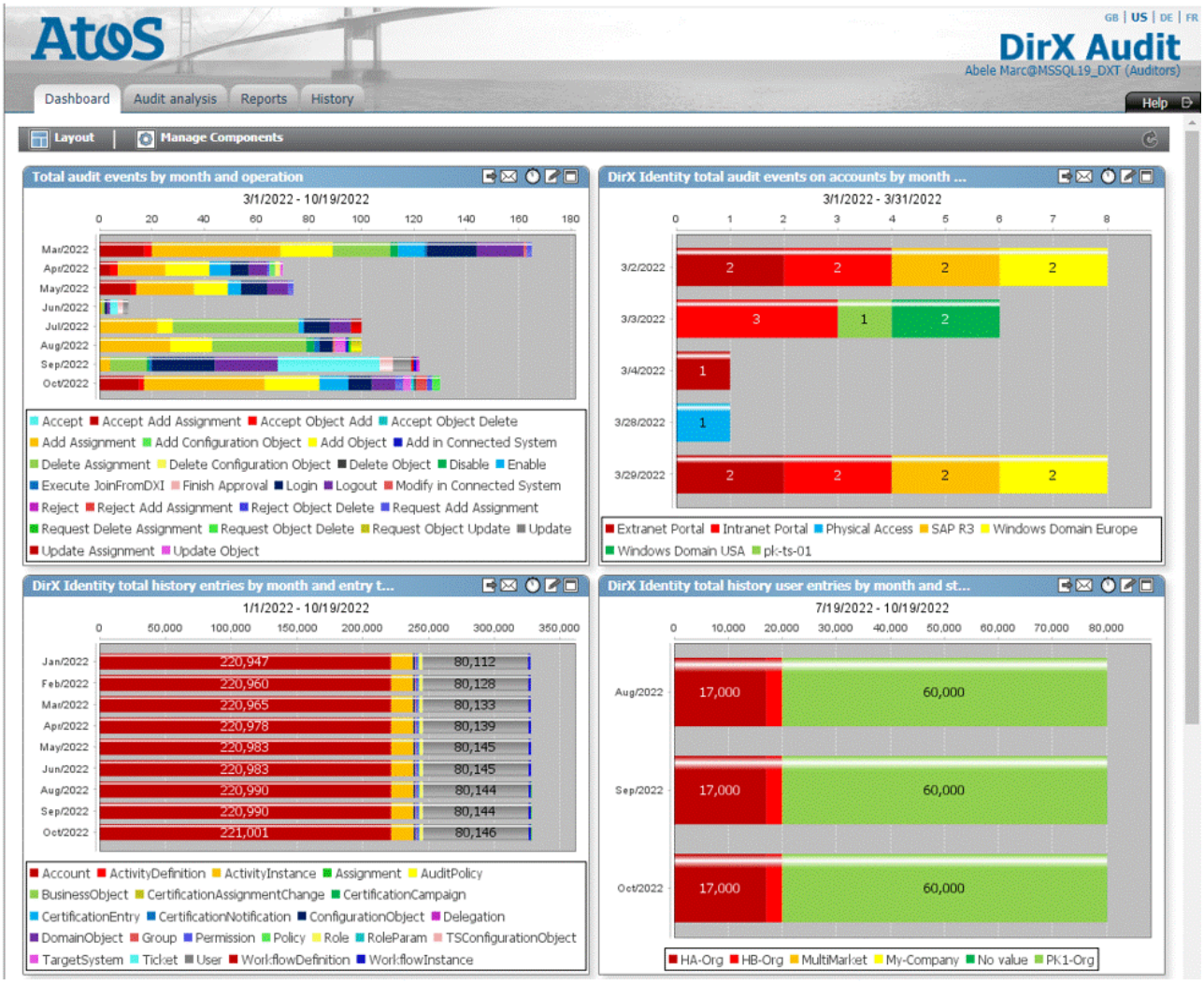


Figure 2. Dashboard View - Main Page

As shown in the figure, the Dashboard view page is composed of a toolbar and a display pane. The toolbar provides the following selections:

- **Layout** - allows you to select the components you want to display and the layout of the Dashboard. The Dashboard display pane is divided into different tiles. Each tile typically displays one component but can be empty if the number of available tiles in your layout is greater than the number of components you have selected to display. The layout selected in the previous figure allows a maximum of four components to be displayed at a time in a left-to-right, top-down display. For more information, see "Displaying Components".
- **Manage Components** - allows you to import, edit, export and delete components. For more information, see "Managing Components".
- **Refresh** - cancels any unsaved changes you have made to the Dashboard component's settings and reverts to the last saved settings. For more information, see the section "Changing a Component".

3.2. Accessing Components

The Dashboard interface defines two types of component:

- **Public** - components created by an administrator for use by the entire DirX Audit user community.
- **Private** - components created by a logged-in user for his or her private use.

The components that a user sees when he is logged in to DirX Audit Manager and the kind of access he has to these components depends upon his / her user type (role). DirX Audit Manager currently specifies several user types (roles): "audit administrator", "auditor", and "restricted auditor". Access to components for these users is as follows:

- Audit administrators can view and manage all **Public** components and their own **Private** components.
- Auditors can view and use the **Public** components but they cannot make changes to them or delete them.
- Restricted auditors have no access to Dashboard, Audit analysis and History view and they can only view and schedule Reports.
- Audit administrators and auditors can view, change and delete their own **Private** components.

Whether a user is an audit administrator, an auditor or a restricted auditor is determined by the user's membership in configurable groups in any LDAP directory (usually the source of the audit information). For example, in DirX Identity, these are two predefined groups - Auditors and AuditAdmins - that are controlled by roles. See the *DirX Audit Installation Guide* and *DirX Audit Administration Guide* for details about configuring user authentication.

3.3. Displaying Components

Use 

in the Dashboard main page to:

- Select the components you want to display in the Dashboard view's display pane.
- Change the number of tiles used to display components in the Dashboard view's display pane.

The following figure shows the Layout dialog.

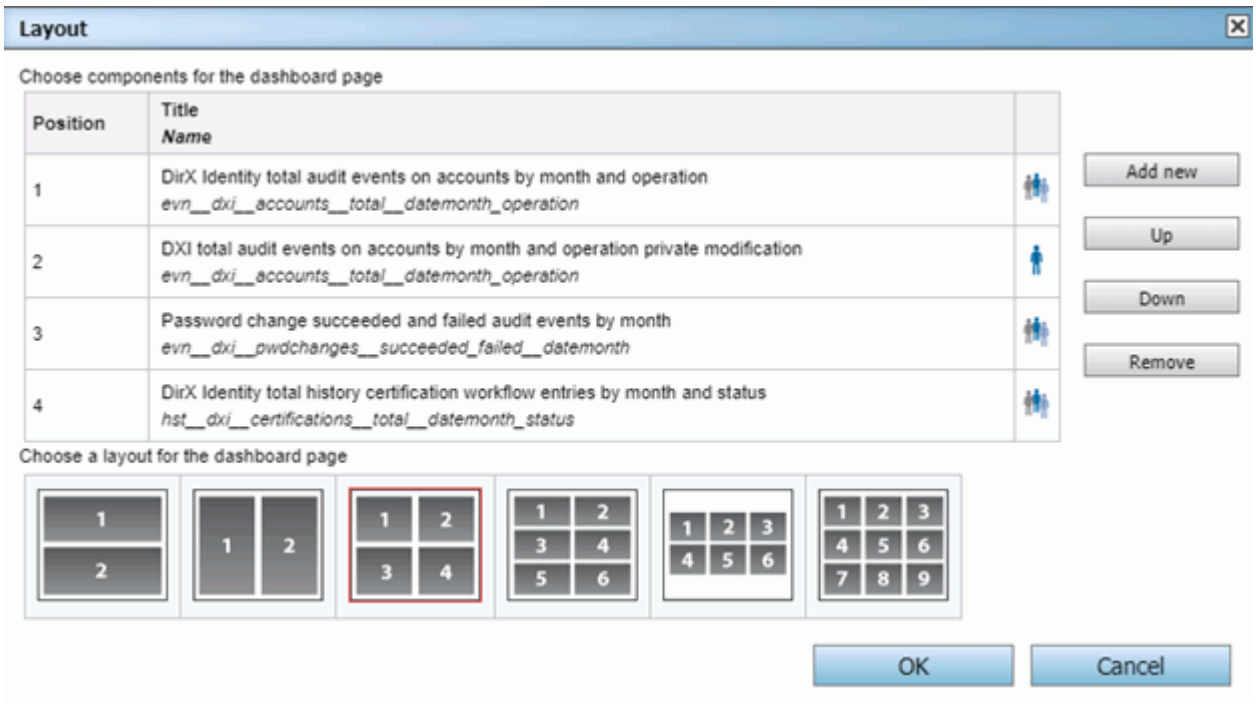


Figure 3. Dashboard View - Layout Selection Dialog

As shown in the figure, the Layout dialog provides two areas: one for selecting the components to be displayed and one for selecting the type of layout to use. The next sections explain how to use each area.

3.3.1. Selecting Components

The upper part of the Layout dialog allows you to select the components you want to display in the Dashboard view's display. The following figure shows this area:

Figure 4. Layout Dialog - Selected Components

The **Position** column indicates the tile in the display pane layout at which the named component is displayed. In this example, a four-tile layout is selected and **DirX Identity total audit events on accounts by month and operation** appears in the top left tile.

The icon in the last column of the table identifies whether the component is public or private .

To add a new component to the list, click **Add new**. The DirX Audit Manager displays two tabs: one that lists the public components available to you, and one that lists your private components:

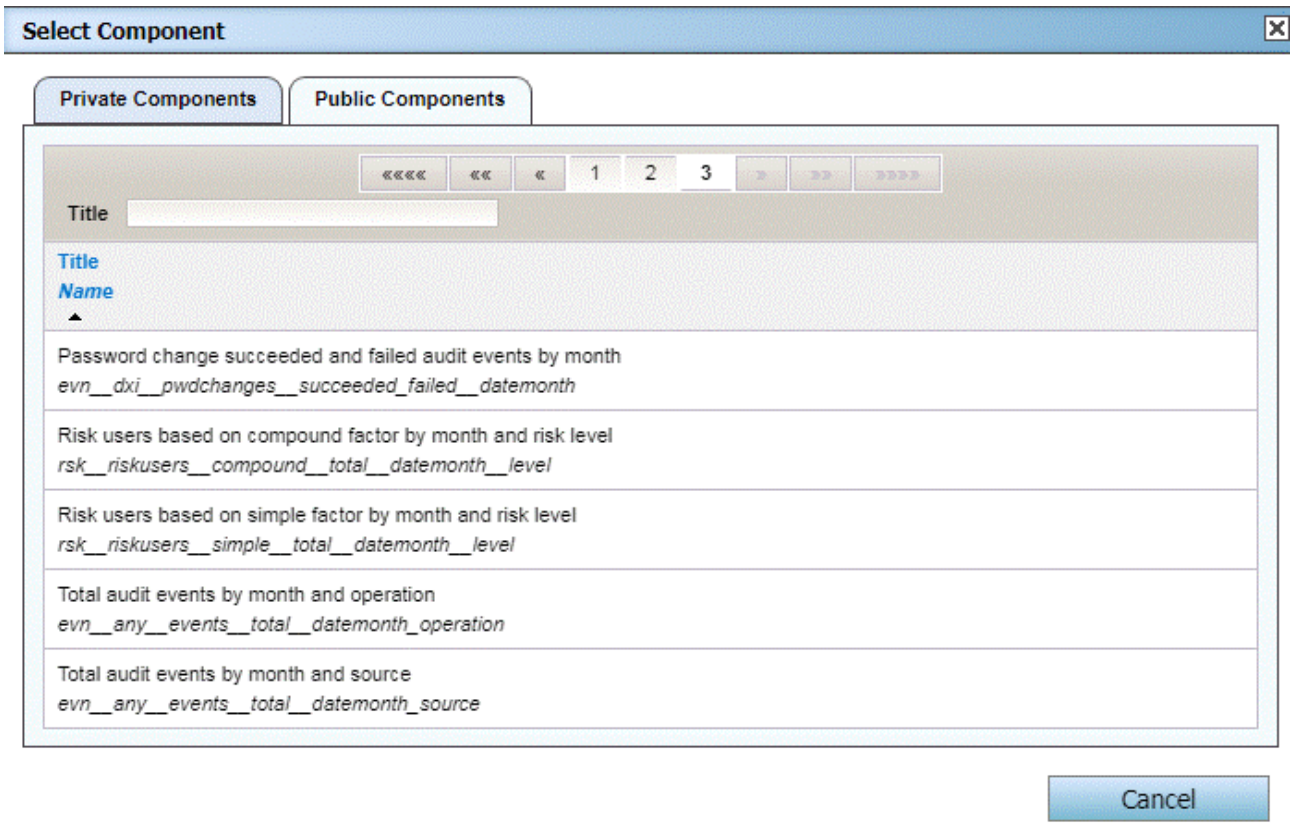


Figure 5. Layout Dialog - Add New Component

Click a tab to choose which kind of components to list. You can use the **Title** field to filter the component names. When you find a component you want to use, click it in the list to select it. The DirX Audit Manager adds the new component to the bottom of the selected components list. If there is no available zone in which to display the new component, it is shown as crossed out in the list.

To move a component to a different position in the selected components list, click the component and then click **Up** or **Down**. To delete it from the list, click **Remove**.

To exit the dialog without making any changes, click **Cancel**.

3.3.2. Controlling Component Layout

The lower part of the Layout dialog displays a selection of layouts from which you can choose, as shown in the following figure:

Figure 6. Layout Dialog - Layout Selection

To select a layout, click it. The selected layout is then highlighted in red. To confirm the selection, click **OK**. To cancel the selection and return to the Dashboard main page, click **Cancel**.

If there are more components selected than tiles available in the layout, the components that can no longer be displayed are shown crossed out in the Components Selection area. For example, suppose you are displaying six components in a six-tile layout, and then you change the layout from six tiles to two. When you click **OK**, the Components Selection dialog shows the components in positions 1 and 2 (the only available tiles in the new two-tile layout) but crosses out the components in positions 3 through 6. If you want to display different components in the available tiles, select them in the list and then click **Up** or **Down** to move them into the available tile positions (1 and 2, in this example).

3.4. Working with Components

This section describes how to work with the Dashboard's component interface, including how to:

- Maximize and restore component display
- Export component data to a file
- Send component data as an e-mail attachment
- Drill down to audit events
- Drill down to history entries
- Change component settings
- Schedule the generation of a report

3.4.1. Maximizing and Restoring Component Display

To display a single component in the entire Dashboard display, click the ▣ button in the component display. The following figure shows a maximized component.

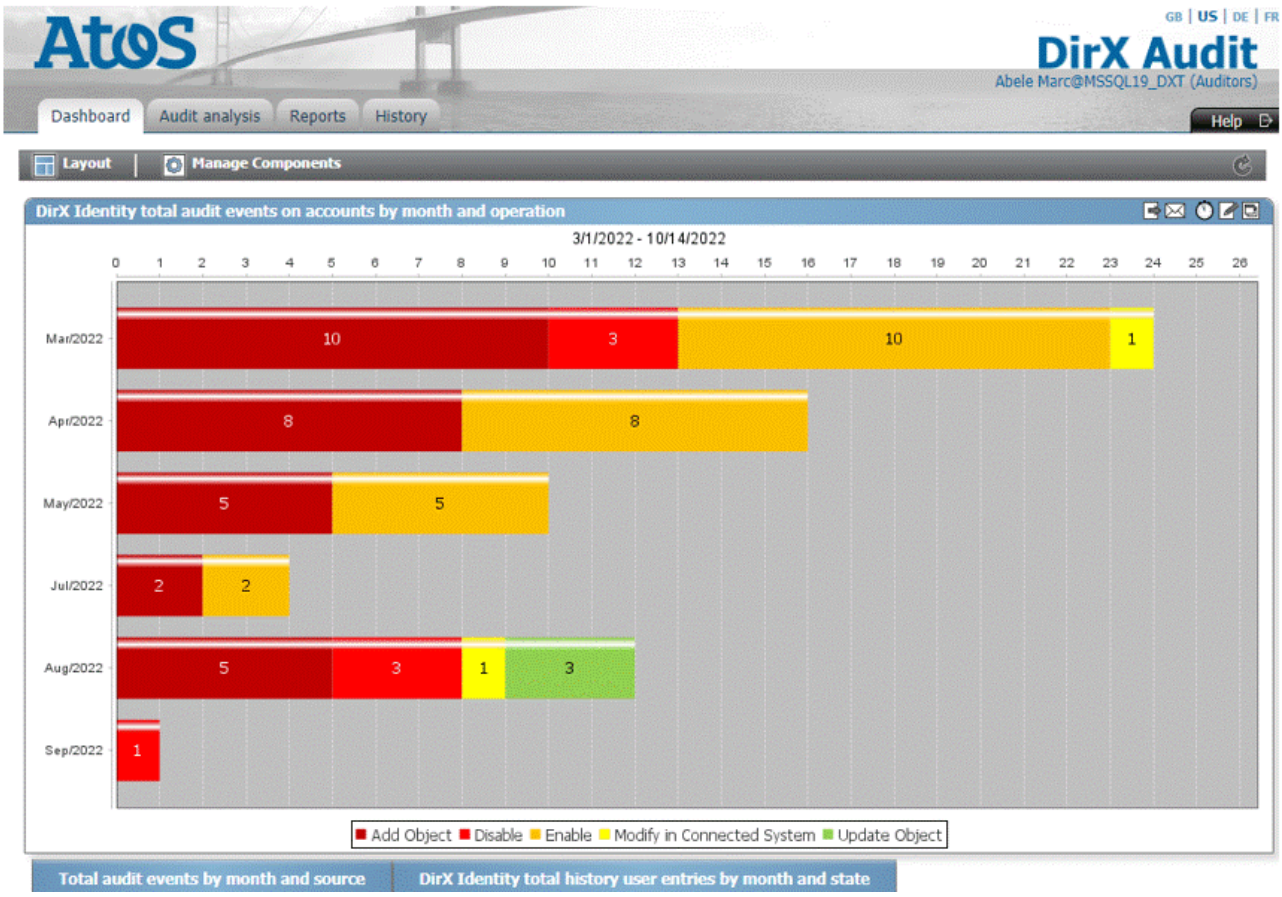


Figure 7. Maximized Component

When one component is maximized, you can display a different component by clicking its title button below the maximized component.

To restore the display to show the selected components in their tiles, click the ▣ button.

3.4.2. Exporting Component Data

To export the aggregated audit data presented in a component into a PDF file, click the button in the component display. DirX Audit Manager creates a PDF file that you can open in a separate tab with a PDF reader or save to your local file system with your Internet browser. Here is an example of an exported component:

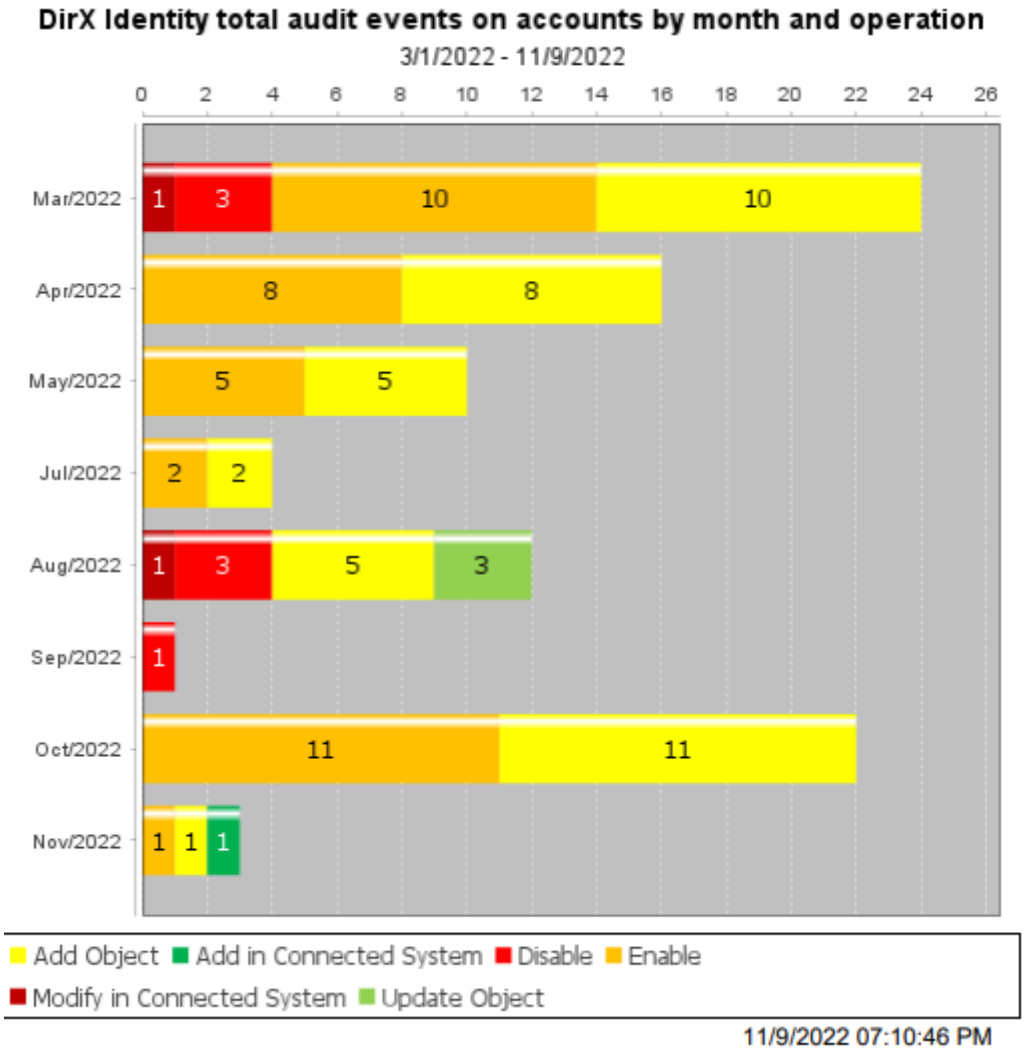


Figure 8. Exported Component Data

3.4.3. Sending Component Data in E-mail

To send the aggregated audit data presented in a component as a PDF file in an e-mail attachment, click the button in the component display. DirX Audit Manager creates a PDF file that can be enclosed in an e-mail message. Provide data for the To, Cc, Bcc, Subject and Body e-mail message fields, and then click **OK** to send the message.

This feature is only available when you have set and configured **Send emails** in the Core configuration. See the section “Common SMTP Configuration” in the *DirX Audit Installation Guide* for details.

3.4.4. Drilling Down to Audit Events

To display detailed information about the audit events indicated in a bar, line, or slice in a component display, click it. The DirX Audit Manager opens the events view and displays details about each audit event. For example, consider the **Password change succeeded and failed audit events by month** component, shown below.

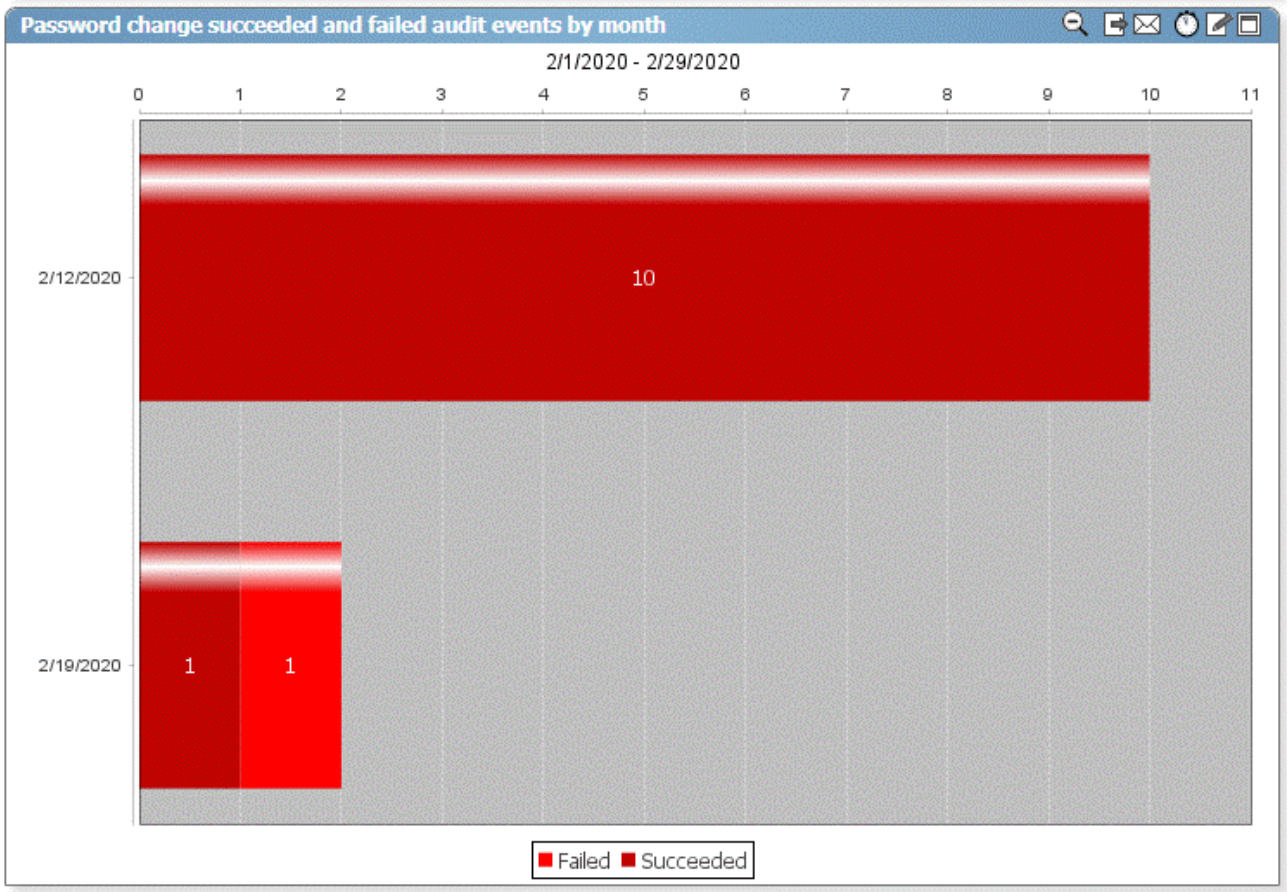
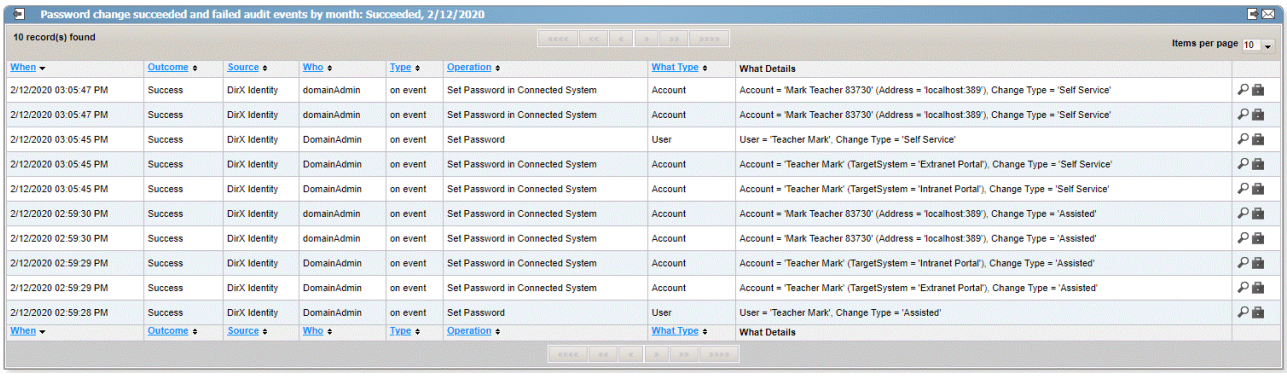


Figure 9. Password Change Events - Dashboard View

Each bar in the chart indicates the total number of password change events that occurred on a specific date. To get detailed information about the ten password change events that succeeded on 12 February 2020, click on the bar labeled **02/12/2020**. DirX Audit Manager displays the following information about these audit events:


Password change succeeded and failed audit events by month: Succeeded, 2/12/2020

10 record(s) found

Items per page 10

When	Outcome	Source	Who	Type	Operation	What Type	What Details
2/12/2020 03:05:47 PM	Success	DirX Identity	domainAdmin	on event	Set Password in Connected System	Account	Account = 'Mark Teacher 83730' (Address = 'localhost:389'), Change Type = 'Self Service'
2/12/2020 03:05:47 PM	Success	DirX Identity	domainAdmin	on event	Set Password in Connected System	Account	Account = 'Mark Teacher 83730' (Address = 'localhost:389'), Change Type = 'Self Service'
2/12/2020 03:05:45 PM	Success	DirX Identity	DomainAdmin	on event	Set Password	User	User = 'Teacher Mark', Change Type = 'Self Service'
2/12/2020 03:05:45 PM	Success	DirX Identity	DomainAdmin	on event	Set Password in Connected System	Account	Account = 'Teacher Mark' (TargetSystem = 'Extranet Portal'), Change Type = 'Self Service'
2/12/2020 03:05:45 PM	Success	DirX Identity	DomainAdmin	on event	Set Password in Connected System	Account	Account = 'Teacher Mark' (TargetSystem = 'Intranet Portal'), Change Type = 'Self Service'
2/12/2020 02:59:30 PM	Success	DirX Identity	domainAdmin	on event	Set Password in Connected System	Account	Account = 'Mark Teacher 83730' (Address = 'localhost:389'), Change Type = 'Assisted'
2/12/2020 02:59:30 PM	Success	DirX Identity	domainAdmin	on event	Set Password in Connected System	Account	Account = 'Mark Teacher 83730' (Address = 'localhost:389'), Change Type = 'Assisted'
2/12/2020 02:59:29 PM	Success	DirX Identity	DomainAdmin	on event	Set Password in Connected System	Account	Account = 'Teacher Mark' (TargetSystem = 'Intranet Portal'), Change Type = 'Assisted'
2/12/2020 02:59:29 PM	Success	DirX Identity	DomainAdmin	on event	Set Password in Connected System	Account	Account = 'Teacher Mark' (TargetSystem = 'Extranet Portal'), Change Type = 'Assisted'
2/12/2020 02:59:28 PM	Success	DirX Identity	DomainAdmin	on event	Set Password	User	User = 'Teacher Mark', Change Type = 'Assisted'
When	Outcome	Source	Who	Type	Operation	What Type	What Details

Figure 10. Password Change Events - Events View

Each row in the table provides details about each of the ten password change events. For more information on how to work with the events view, see the chapter "Using Audit Analysis", because the basic functionality is the same.

To return to the Dashboard component view, click the button.

Sometimes the total number of events displayed in a Dashboard component audit event category does not correspond to the number of events you see when you drill down on the category. This can happen when:

- The Dashboard values for the audit event category have not been calculated for recently imported audit messages; for example, for the current day, but they are already stored in the DirX Audit Database and visible with the events view. In this case, the Dashboard component displays a lower number.
- Some audit messages, including their related audit events, have been exported with the purge tool and thus cannot be shown when drilling down on the category. In this case, the Dashboard component indicates a higher number.
- The user has no privilege to view individual audit events because of the fine-grained access control policies in force. In this case, the Dashboard component indicates a higher number.

3.4.5. Drilling Down to History Entries

You can use the Dashboard charts on history entries to directly access the detailed view of related history entries. To display detailed information about the history entries indicated in a bar, line, or slice in a component display, click it. The DirX Audit Manager opens the list of history entries and displays details about each of them.

When the dimension is set to **Month**, Dashboards that display history entries will display the status for each month as of the last day of that month. Set the dimension to **Date and time** to view all values for the month. For more information about how to change the dimension, see the section "Changing Component Settings" and "Changing the Data Source".

The **DirX Identity total history approval workflow entries by month and status** component shown below has the dimension set to the value **Date and time** and shows all values in the months.

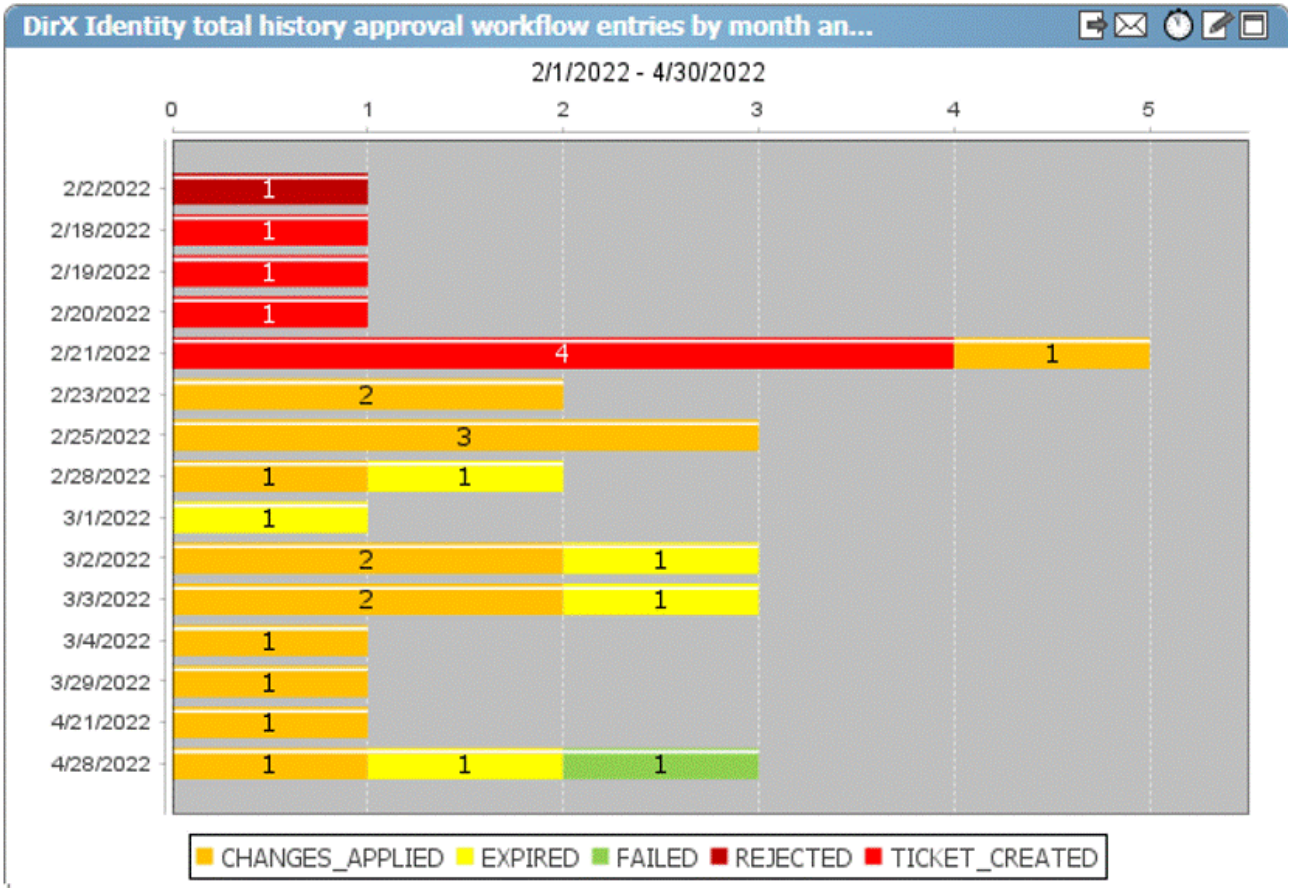


Figure 11. Component Chart with History Entries - Dashboard View

Each bar in the chart indicates the approval workflow history entries on a specific date. To get detailed information about history entries, click, for example, on the bar labeled **02/25/2022**. DirX Audit Manager displays the following information about these history entries:

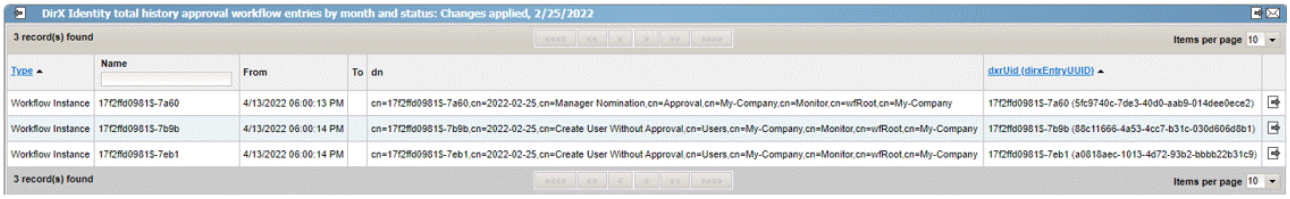


Figure 12. Component Chart with History Entries - History Entries View

To access the history entry's details, click the button in the last column of the drill down list. The History view opens.

You can sort the result list either by entry type or by the **dxrUid** (**dirxEntryUUID**) identifier. You can use the **Name** field to filter the entries by name.

To return to the Dashboard component view, click the button.

3.4.6. Changing a Component

To change the settings for a component you're displaying, click the button in the component display. This action opens the Edit component dialog for the component, where you can change the data source or the display format for the component. For more information about how to use this dialog, see the section "Changing Component Settings".

3.4.7. Scheduling Component Report Generation

To schedule the generation of a component report, click the button in the component display. This action opens the **Add a new report to a report set** dialog where you can select an existing report set or create a new one. For more information about how to configure a report, see the section "Using the Reports View".

3.5. Managing Components

The Manage Components selection in the Dashboard main page allows you to manage the components to which you have access. Only users with the audit administrator role can view and manage the public components in the Manage Components dialog. The following figure shows the Manage Components dialog.

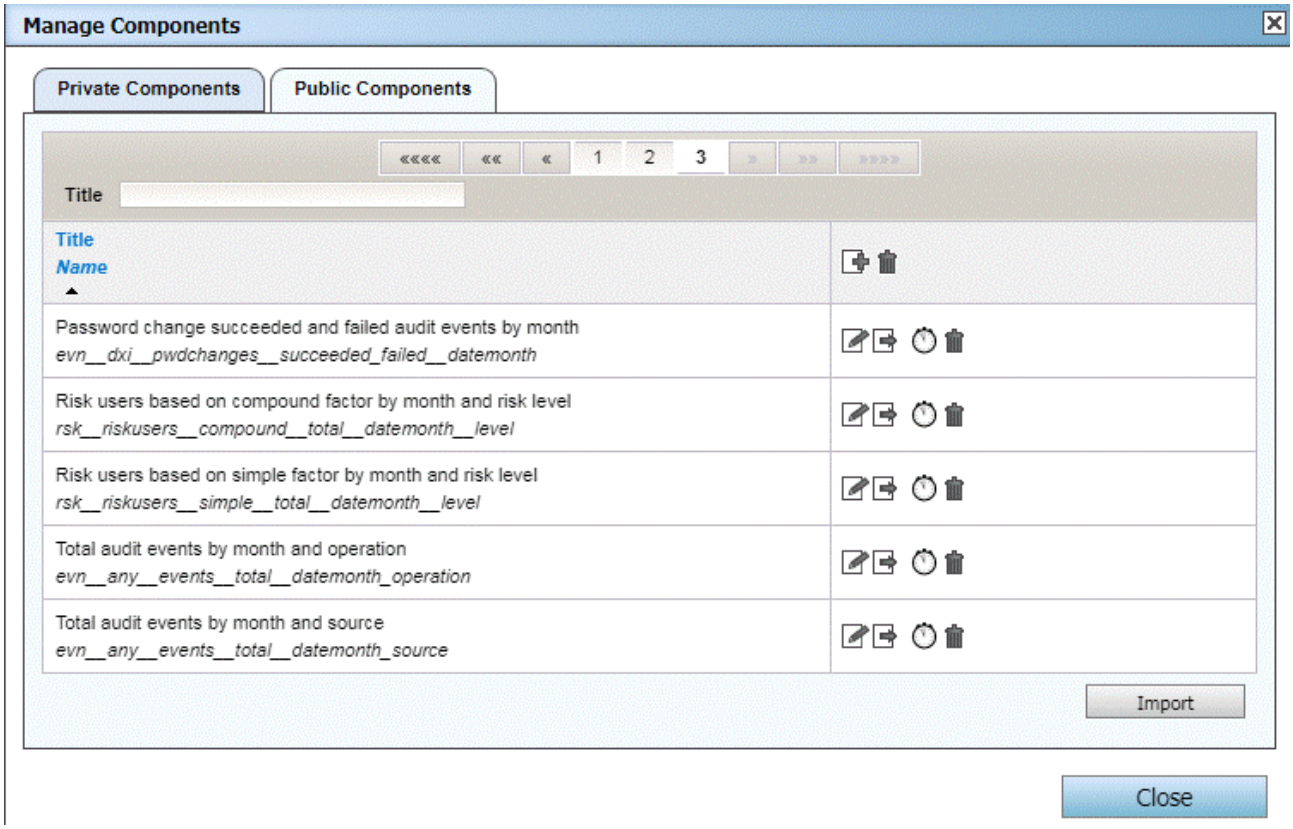


Figure 13. Managing Components

As shown in the figure, the Manage Components dialog contains: two tabs, one for managing your private components, and one for managing public components, if your DirX Audit role permits this action (see "Accessing Components" for details). If there are more components available than can be displayed in the dialog, a Page Navigator is provided for paging through the list. You can use the **Title** field to filter the component names.

From the Manage Components dialog, you can:

- Click to the right of a component in the list to change its settings. See the section "Changing Component Settings" for details.
- Click to the right of a component in the list to export its settings to the local file system as an XML file. See the section "Exporting Component Settings" for details.
- Click to the right of a component in the list to schedule a generation of a Dashboard component report.
- Click **Import** to import an XML file of component settings from the local file system. See the section "Importing Component Settings" for details.
- Click to create a new dashboard component from scratch with the Edit component dialog.
- Click to the right of a component in the list to delete it.
- Click **Close** to exit the dialog and return to the Dashboard main page.

3.5.1. Changing Component Settings

To change a component's settings, click the button to the right of the component in the list. This action displays the Edit component dialog, as shown in the following figure:

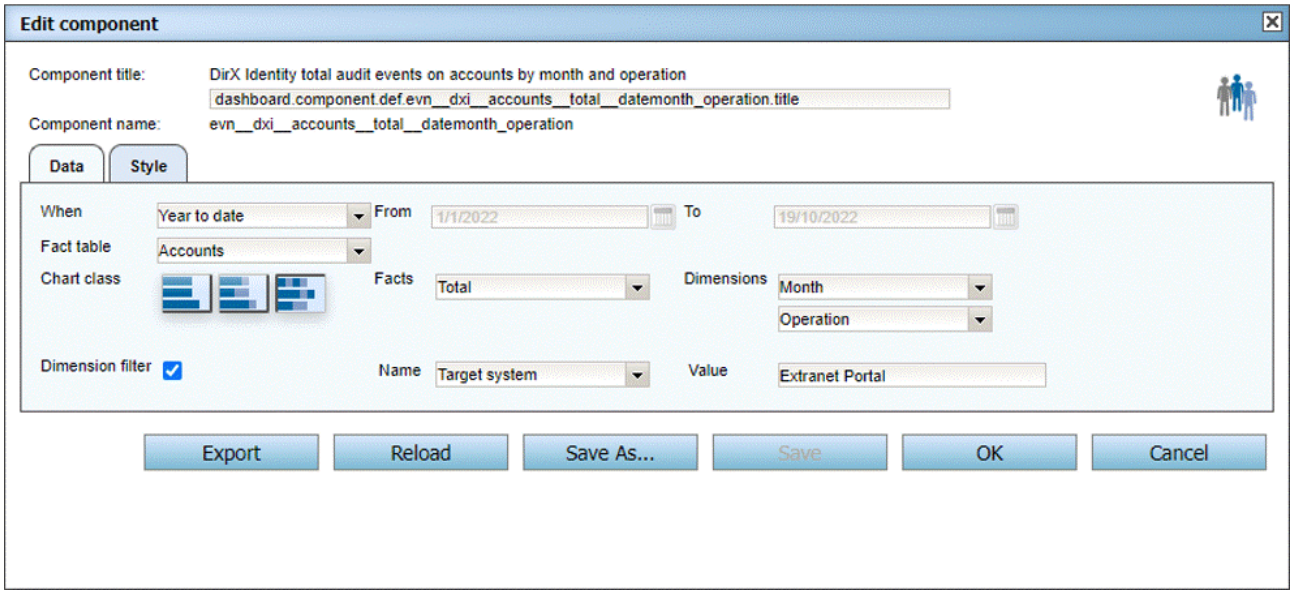


Figure 14. Manage Components - Edit Component Dialog

As shown in the figure, the Edit component dialog contains the following items:

- The component title used in its display and its key, which is used for component title localization. If the key is not found in the localization files, a proper component title cannot be displayed and the key is used as the component title.
- The component filename.
- An icon that indicates whether it is a public or private component.
- **Data** - selects the aggregated audit data to be provided by the component.
- **Style** - selects the look and feel of how the component data is displayed.
- **Export** - exports the component's definition (its XML format) to the local file system. For more information, see "Exporting Component Settings".
- **Reload** - cancels any changes you have made to the component's settings and reverts to the last saved settings.
- **Save As** - saves the component's settings to a new entry in the DirX Audit Database. For more information, see "Creating New Components".
- **Save** - saves your changes to the component's settings in the DirX Audit Database. This item is available if you have permission for this action.
- **OK** - applies the changes you have made and returns you to the Manage Components dialog.
- **Cancel** - cancels any changes you have made to the component's settings and returns you to the Manage Components dialog.

3.5.1.1. Changing the Data Source

Click the Data tab to change the source of the aggregated audit data that a component provides; that is, the OLAP data cube in the DirX Audit Database from which it retrieves the data.

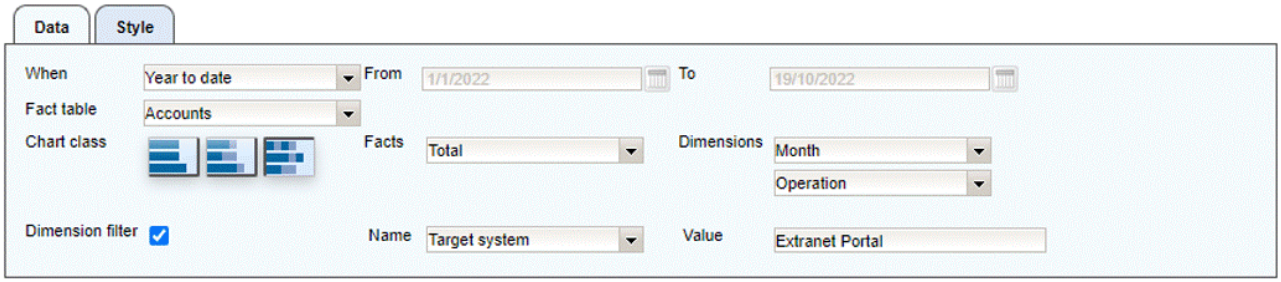


Figure 15. Component Settings - Data Tab

As shown in the figure, the Data tab provides the following items:

- **When** - filters the available data according to a specific or a relative time period; for example, within the previous year (**Previous Year**), within the previous month (**Previous Month**), within the current month (**Month to date**) and so on. Selecting **Any time** means that all the aggregated audit data contained in the specified OLAP data cube is displayed. Selecting **Custom time** allows you to set specific start and end dates with the **From** and **To** fields.

- **From** and **To** - selects the data in the time period defined by the start (**From**) and end (**To**) date.
- **Chart class** - selects a chart class, which can be one fact and one dimension, two facts and one dimension, or one fact and two dimensions. Some chart classes may be disabled for some fact tables.
- **Fact table**, **Facts and Dimensions** - specifies the OLAP data cube to be used to supply the aggregated audit data.
- **Dimension filter** - specifies an additional filter for presenting component data. When you check this box, you can select a dimension related to the selected **Fact table** from the drop-down list and then enter a string in **Value**. This filter specifies that component data is to be sliced to audit events or history entries with the specified value for the selected dimension. Only audit events or history entries matching this additional condition are reflected when data is aggregated for the Dashboard component.

Facts and Dimensions can be configured, added or removed from the list. For more information, see the section “Customizing Fact and Dimension Tables” in the *DirX Audit Customization Guide* and the section “Managing Fact and Dimension Tables” in the *DirX Audit Administration Guide*.

3.5.1.2. Zooming the Date Dimension

Click the date indicator in a chart to zoom into the view and see more detailed values for months or days. Here is an example:

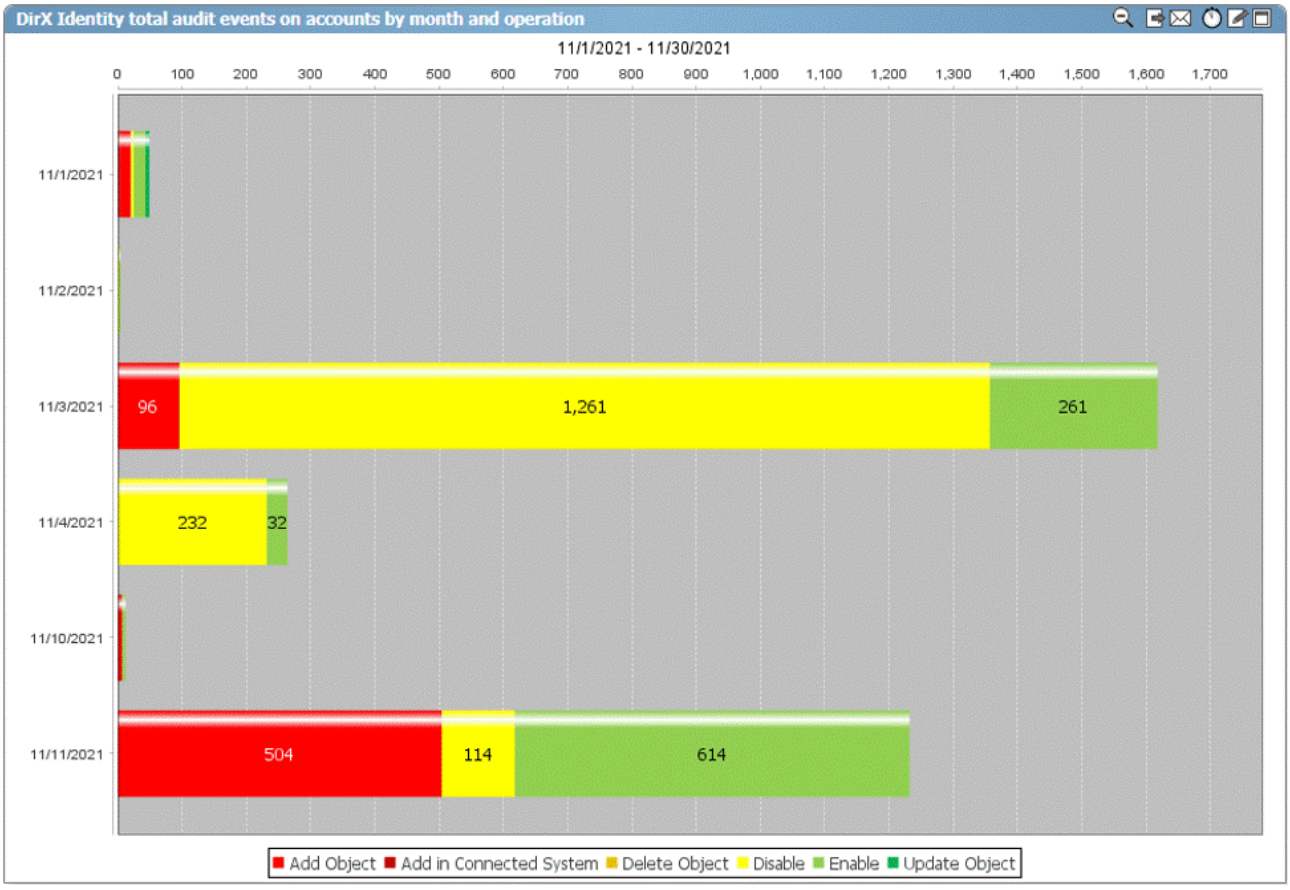


Figure 16. Zoomed-in Dates in a Chart

Click in the toolbar to zoom out of the view and back to the original settings.

3.5.1.3. Changing the Display Format

Click the Style tab to configure the look and feel of the component's data display:

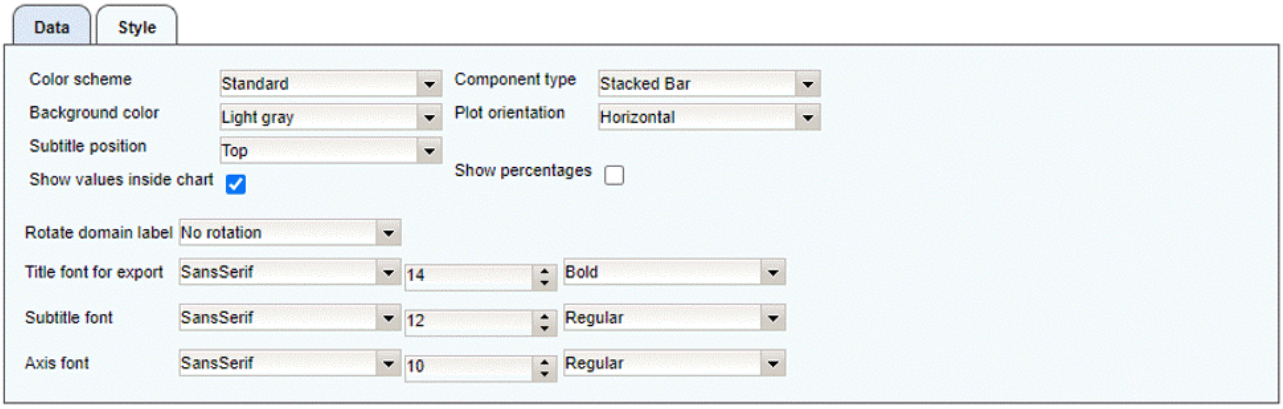


Figure 17. Edit Component - Style Tab

As shown in the figure, the Style tab provides the following items:

- **Color scheme** - selects a predefined color scheme for the component display; for example, **Ocean** or **Forest**.
- **Background color** - selects a background color for the component display.
- **Subtitle position** - selects the position at which the subtitle of the component display is to appear: above the chart (top) or below the chart (bottom). The subtitle displays the relative or specific time period you selected in the **Data** tab (if you select **Any time**, a subtitle is not displayed).
- **Show values inside chart** - show or hides the labels given on a bar, line, or slice in a component display that identify the number of audit events that occurred and the audit event category to which they belong.
- **Show percentages** - show the percentages instead of the numbers on a bar, line, or slice in a component display that identify the number of audit events that occurred and the audit event category to which they belong. This parameter is visible only for a component with the "two facts and one dimension" or "one fact and two dimensions" chart class selected.
- **Component type** - selects a display type for the component data; for example, a bar chart or a pie chart. Depending on the selected type, additional parameters may be displayed; for example, when you select a **Bar** component type, a parameter for **Plot** orientation is displayed. Components with two dimensions or two facts can use **Stacked Bar** or **Stacked Bar 3D** component types.
- **Rotate domain label** - rotates the axis value labels by 45 or 90 degrees for better readability.
- **Title font**, **Subtitle font**, and **Axis font** - selects the type face (Serif, Sans Serif, Monospace), font size (10, 12, 14...) and appearance (bold, italic ...) of the type used in the display.

3.5.1.4. Adding a Threshold

You can add a threshold to a component with the "one fact and one dimension" chart class to highlight results above the determined limit:

- In the Style tab, insert a value into **Threshold**.

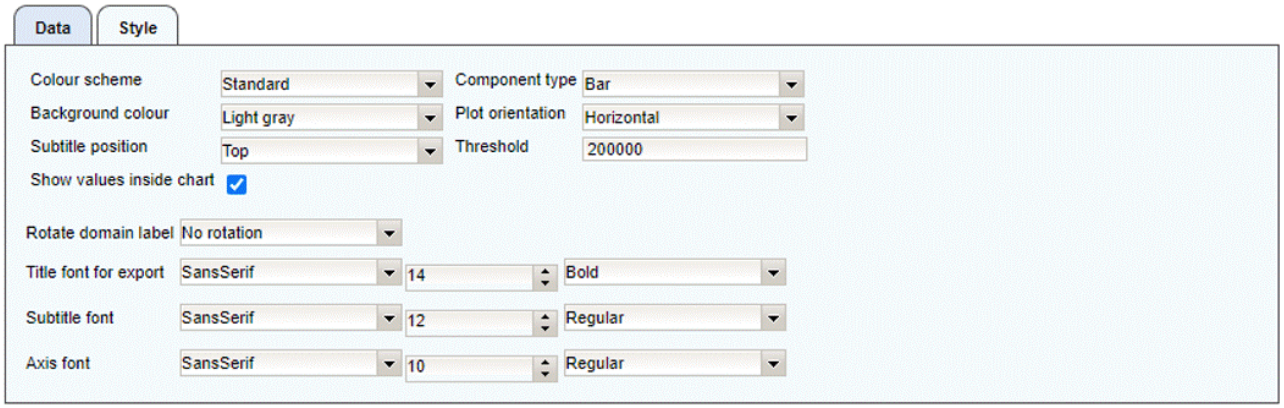


Figure 18. Edit Component Style - Threshold

When the limit conforms to the chart range, the threshold is displayed.

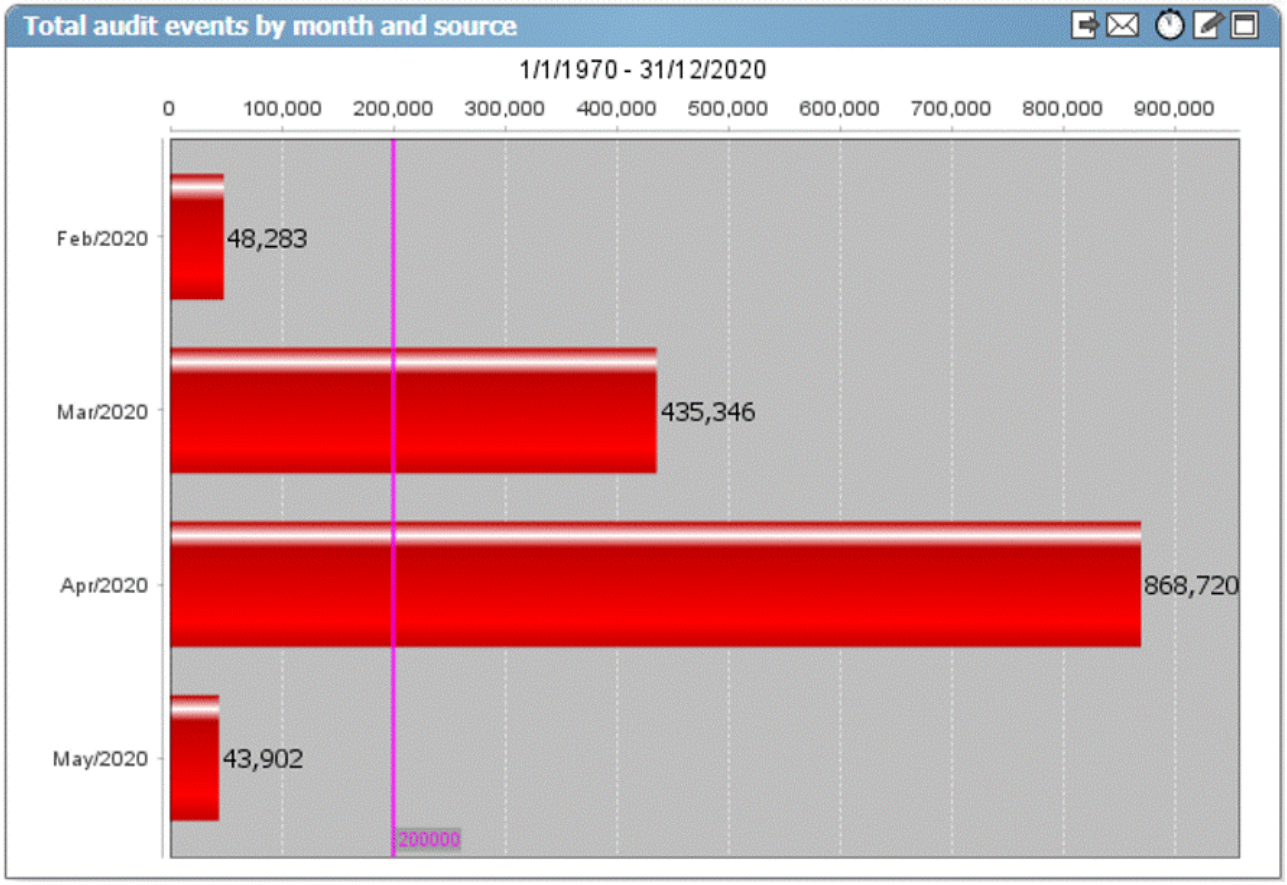


Figure 19. Edit Component Threshold - Example

3.5.2. Exporting Component Settings

To export a component's settings - its configuration data - to an XML file in the local file system, you can either:

- Click **Export** in the Edit component dialog.
- Click to the right of a component listed in the Manage Components dialog.

The following figure shows an example of an XML definition of a component's settings.

Figure 20. Exported Component Settings in XML

3.5.3. Importing Component Settings

To import component settings defined in an XML file to the Dashboard:

- Click **Import** in the Manage Components dialog.
- In the dialog displayed, click **Add**. DirX Audit Manager allows you to navigate to a file in the local file system and select it. Repeat this step for any other files you want to select for import.

- Click **Upload**. DirX Audit Manager loads the selected files into memory and checks for valid content and for any naming conflicts with other components. If it finds a conflict, it highlights the wrong component name. Rename the component and change its title. If you decide not to import a file that you have previously selected, check **Skip** to the left of the component name.
- Click **Import**. The DirX Audit Manager loads the selected and validated component(s) into the DirX Audit Database and displays it in the Manage Components dialog.

The import and export functions in the Manage Components dialog work together to allow you to export a component's settings to an XML file and then change them "offline" in the file system, and then upload them back into the Dashboard. You can also use the import function to create a new component "offline" and then import it into the Dashboard.

3.5.4. Creating New Components

You can create new components in several ways:

- You can import an XML file of component settings into the Dashboard, as described in "Importing Component Settings"
- You can use the Edit component dialog described in "Changing Component Settings" to change an existing component's settings, and then use **Save As** in that dialog to save it in the database under a different name.
- You can use  (Add new) in the Manage Components dialog described in "Managing Components". This action opens the Edit component dialog with default values for the new component. For information about customizing components, see the *DirX Audit Customization Guide*.

4. Using Audit Analysis

Audit analysis works directly with audit events stored in the DirX Audit Database as opposed to the Dashboard's display of aggregated OLAP data cubes. This chapter describes the features of the Audit analysis page and how to:

- Filter and search for audit events
- Manage audit event filters
- View the search results table returned by Audit analysis
- Use the page navigator to page through multi-paged search results
- View additional audit event details from the search results page
- Export the search results table to an external file for reporting purposes
- Send the search results table as an e-mail attachment
- Schedule the generation of a search results report

4.1. About the Audit Analysis Main Page

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

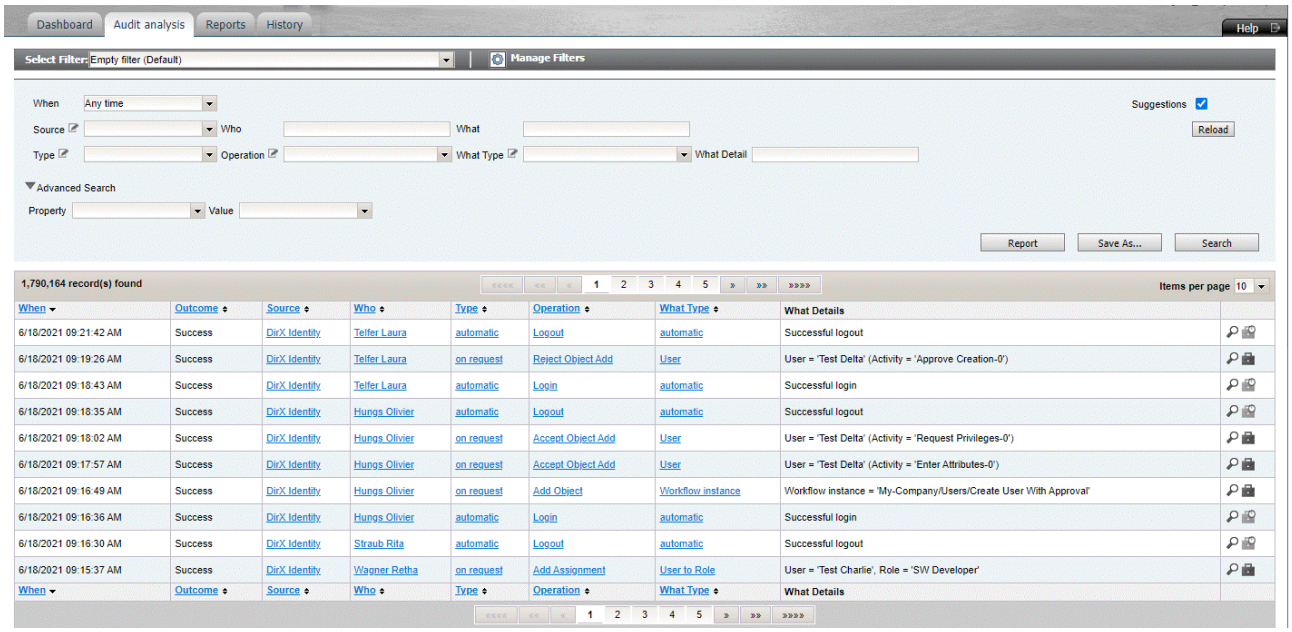


Figure 21. Audit Analysis Main Page

As shown in the figure, the Audit analysis page is composed of three elements:

- A filter definition area that allows you to define the criteria to be used to search for and retrieve audit events and run search and export operations. The section "Filtering Audit Events" describes how to use this part of the page.
- A search results display area that displays information in table format about the audit events returned by a search operation. The section "Viewing the Search Results" explains how to use this part of the page.

- A page navigator above and below the search results display that allows you to navigate through multi-page results. The section "Using the Page Navigator" describes how to use this tool.

4.2. Filtering Audit Events

The filter definition area provides fields for specifying search conditions for retrieving audit events from the DirX Audit Database. The fields in the filter definition area allow you to search for audit events according to their attributes. As shown in the figure, the filter definition area contains the attributes described below. To prevent filter criteria from being applied to an attribute, leave it empty.

- **When** - filters the audit events according to a relative or an absolute time period; for example, within the previous year (**Previous Year**), within the previous month (**Previous Month**), within the current month (**Month to date**) and so on. Selecting **Any time** means that a time period is not used as a filter. Selecting **Custom Time** allows you to set a specific start and end date in the **From** and **To** fields.
- **From** and **To** - filters the audit events according to an absolute time period defined by a start and end date.
- **Source** - filters the audit events according to the audit producer; for example, DirX Identity. If you are interested in events from all producers, select **AnySource** or leave the field empty.
- **Who** - filters the audit events according to the user who initiated the operation.
- **What** - filters the audit events according to the name of an object associated with the event; for example, users, accounts, roles, and so on.
- **Type** - filters the audit events according to the operation type associated with the event; that is, how the operation was initiated (manually, on event, on schedule, on request, and so on).
- **Operation** - filters the audit events according to the operation associated with the event; for example, Set Password, Add Assignment, Request Object Update, Add Object, Delete Object and so on.
- **What Type** - filters the audit events according to the object type associated with the event; for example, user, account, account-to-group (memberships), and so on.
- **What Detail** - filters the audit events according to a specific detail of an operation on an object type; for example, a specific user account or target system in a search for update operations made to accounts. A database full-text index is defined for this field. It searches the DirX Audit Database for all audit events whose What Detail information contains the word specified in the **What Detail** field.

The Advanced Search section contains two additional filter fields:

- **Property** - filters the audit events according to a specific audit message or audit event dimension.
- **Value** - filters the audit events according to the value of the dimension specified in **Property**.

For the **Source**, **Type**, **Operation** and **What Type** filter fields, you can choose between two component types used for value presentation: the **Selection list** component or the **Autocomplete** component. The component type is selected automatically according to the configuration. You can change the component manually by clicking  or  , or you can switch the component for all defined fields at once by clicking the **Suggestions** checkbox.

If the **Selection list** component is used, you can select one of the preselected available values from the list. Values are loaded directly from the database, cached by the DirX Audit Manager and periodically refreshed. You can manually refresh values by clicking **Reload** to be sure that you are working with actual data. For more details on customization, see the section “Customizing Audit Analysis” in the *DirX Audit Customization Guide*. Filter conditions are tagged with a "Starts with" comparison operator. For example, entering **Account** into the **What Type** field returns events associated with account and account-to-group memberships. You can also use the SQL wildcard character **%** to field input if you have not enabled the full-text search in the configuration and have no full-text index in the data DB; for example, specifying %B%der in the **What Detail** field returns all events associated with person names like **Binder** or **Bader**.

If you have enabled the full-text search in the configuration, you can search in the **What Detail** field for any string with a complete word from any place in the searched string. The percent wildcard (%) does not work for full-text functionality; however, if you are using the Microsoft SQL Server database, you can complete the searched phrase with an asterisk wildcard (*). Remember, only searching with complete words works with full-text enabled.

To run the search, click **Search**. DirX Audit Manager populates the search results area with the audit events retrieved according to your search criteria; for more information on how to use this table, see "Viewing the Search Results".

When you enter values into filter fields, DirX Audit Manager searches the database and returns a list of matching attribute values and the number of times they occur in the database. You can simply select a value from this list and click **Search**.

Click **Report** if you want to write the search results to a file; for more information, see "Exporting Audit Event Data".

4.3. Managing Audit Event Filters

You can name and save your filters into the configuration database for future use. Later, you can simply select a stored filter from a list and use it without the need to define it all over again.

Click **Save As ...** to save a new filter to a specified name. You can also provide a description and the visibility. Check the Public option for public filters. Keep it unchecked for private filters. This action is only visible to users with the Audit Administrator role.

Click **Save** to update an existing filter.

You can select an existing filter from a list and then click **Search** to receive results.

Click **Manage Filters** to show all available filters organized in the Private and Public tabs. You can drop an existing filter into this view.

4.4. Viewing the Search Results

The search results display area displays information in table format about the audit events returned by a search operation. In a search results table returned on a search:

- The page navigator is displayed at the top and bottom of the search results area. See the section "Using the Page Navigator" for details.
- Each row represents one audit event returned from the DirX Audit Database according to the search criteria specified in the filter definition area.
- Each column represents an attribute of an audit event. You can use the sort controls on a column to sort the column’s entries in ascending or descending order.
- The icon in the last column on the right allows you to display additional information about the audit event in a separate window. See the section "Viewing Audit Event Details" for more information.
- The icon in the last column on the right allows you to display a list of other events that correlate to a selected audit event. See the section "Viewing Related Audit Events" for more information.

Note that you may not see all additional information or the original message related to the audit event in the Event Details window when you purge this audit message data from the DirX Audit Database. You also may not see a complete list of related audit events that correlate with the selected audit event when you purge these complete audit messages, including message additions and the original message from the DirX Audit Database.

4.5. Using the Page Navigator

The page navigator is displayed above and below the search results display area and contains the following items:

- Information about the number of items found.
- Buttons for moving between pages:

«««« - displays the first page.

»»»» - displays the last page.

»» - performs a fast forward step.

«« - performs a fast rewind step.

» - displays the next page.

« - displays the previous page.

- A drop-down menu 10 in the upper navigator for changing the maximum number of items displayed per page.

4.6. Viewing Audit Event Details

The results table in Audit analysis displays only a subset of the available audit data. To view all the information, click the 🔎 icon in the last column on the right for the audit event. The following figure shows an example.

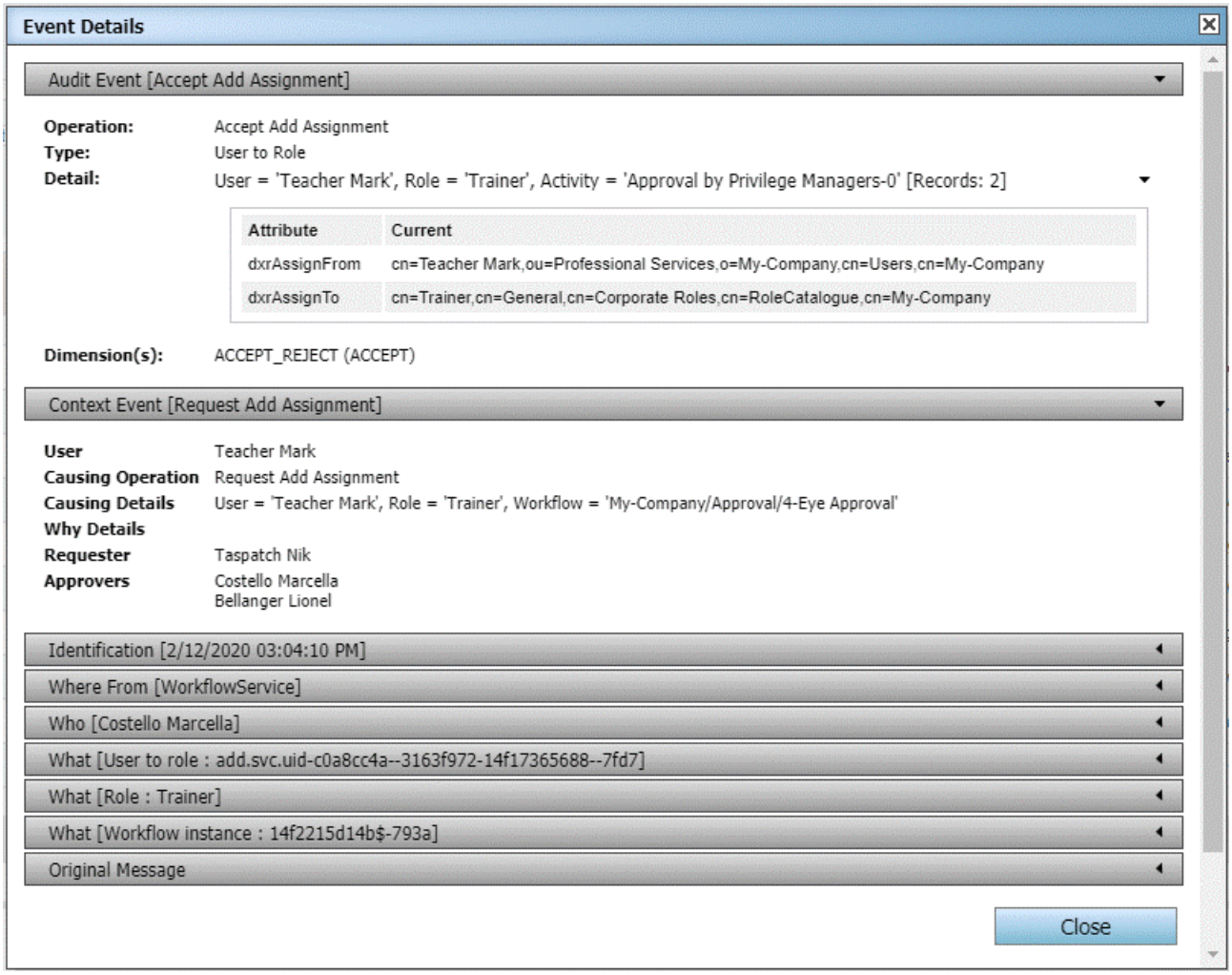


Figure 22. Event Detail Summary

As shown in the example:

- The **Audit Event** bar provides a summary of the audit event and the tags that are attached to it. In this example, the operation is an approval of the assignment of a role "Trainer" to a user **Teacher Mark** by the manager of the role ("Privilege Manager", who is the user **Costello Marcella**) that was generated by a DirX Identity approval workflow activity. The zero suffix in "**Activity='Approval by Privilege Managers'-0**" indicates that Marcella Costello is the first approver calculated in an approval process. Activity names with incremental suffixes (for example, 1, 2, 3) indicate approvers in an approval escalation path. If there are, for example, several role assignments or several membership changes in a **What** element that represents a group or an account, the summary describes just one of the role assignments or the account-group memberships. A tag for this event is ACCEPT_REJECT; in this example, the value ACCEPT tells us that the request was approved.

- The **Detail:** section in the Audit Event bar provides a table that lists the attribute changes. Generally, it formats the “Detail(s)” section of a “What” object in the Audit Event Detail view. The table contains an **Attribute** column and **Previous** and/or **Current** columns depending on the type of operation. The **Attribute** column specifies the names of the changed attributes and the other columns define the previous and/or current value of the attributes. The Detail section is collapsible using the triangle icon on the right. For better readability, the section with the table is expanded by default. If the configured maximum number of attributes is exceeded, the section is automatically collapsed. For more details on customizing the maximum value, see the section “Customizing Audit Analysis” in the *DirX Audit Customization Guide*.
- The **Identification** bar provides more information about the operation, such as when it occurred, its type, the UID of the audit message and the message that caused it, the operation category, and whether or not the operation was successful. It also shows the tags that are attached to the audit message; in this example, it is the tag ACTIVITY with the name of the activity within the approval workflow. See the chapter in the *DirX Audit Administration Guide* that describes the database schema for details.
- The **Where From** bar identifies the application or component within the producing product suite that generated the audit event (the DirX Identity workflow service, in this example), its address and an optional list of other associated properties.
- The **Who** bar identifies, for this example, the approver of the assignment (Marcella Costello, who is the privilege manager for the **Trainer** role). The Extensions area shows the list of identifying attributes of the user (label and value).
- Each **What** bar identifies an object that participated in the operation. In this example, they identify the user who was assigned the **Trainer** role (**Teacher Mark**), the user-to-role assignment and the workflow instance that generated the activity. The Extensions area shows the list of identifying attributes for the What object, and the Detail(s) area shows the list of modified attributes: modify operation, attribute name and value.
- The **Original Message** bar contains the original message delivered from the audit source.
- The **Context Event** bar provides a summary of related audit events. It contains information on the causing event and who requested and approved the operation.

The **Context Event** and **Audit Event** bars are expanded by default. Click on the bars to show and hide the details.

The events details also contain history entry links, which you can use to access the related history entry and view its details. These links are highlighted in blue. In the following example, **Trainer** and **Costello Marcella** represent links to history entries.

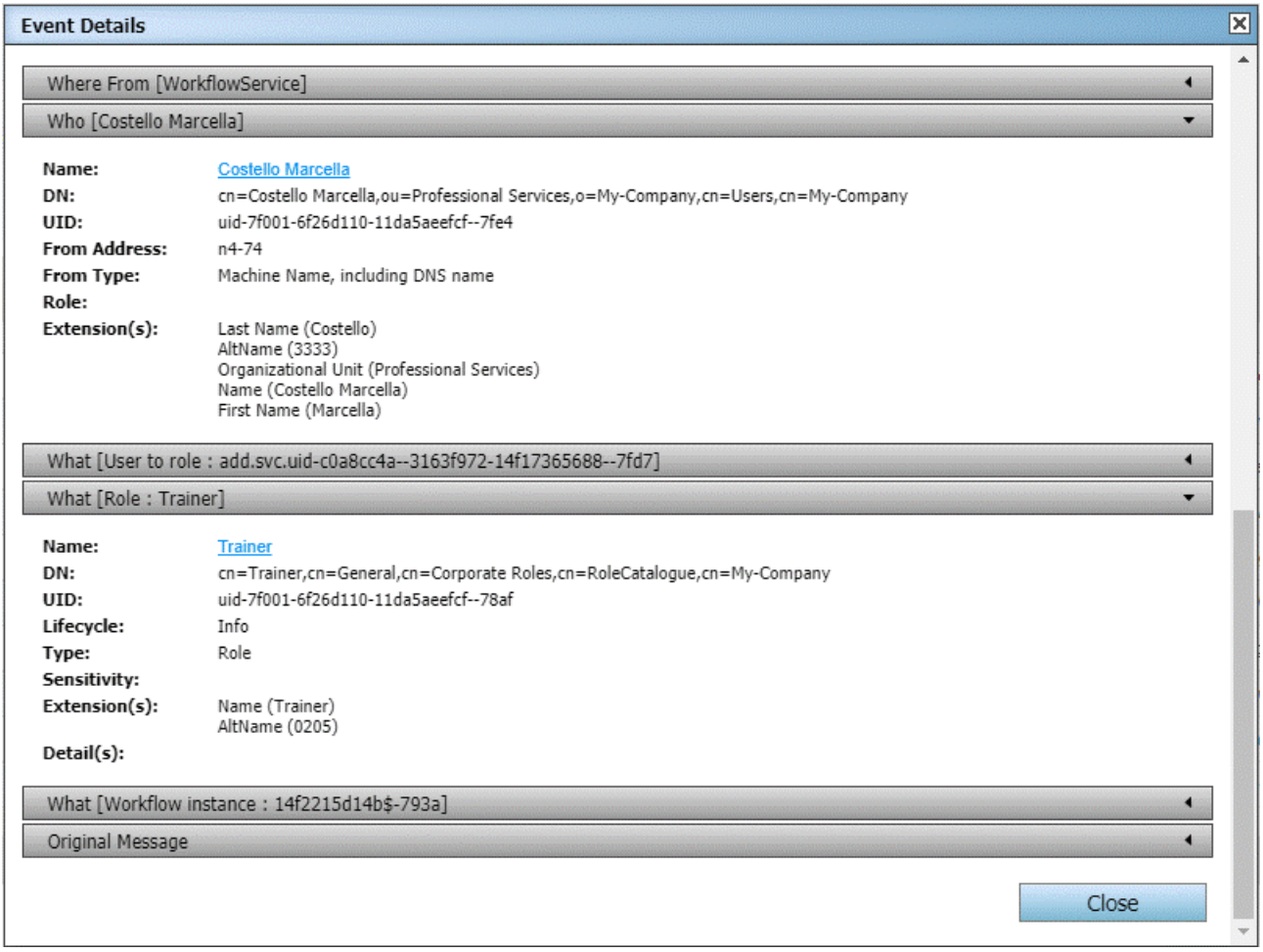
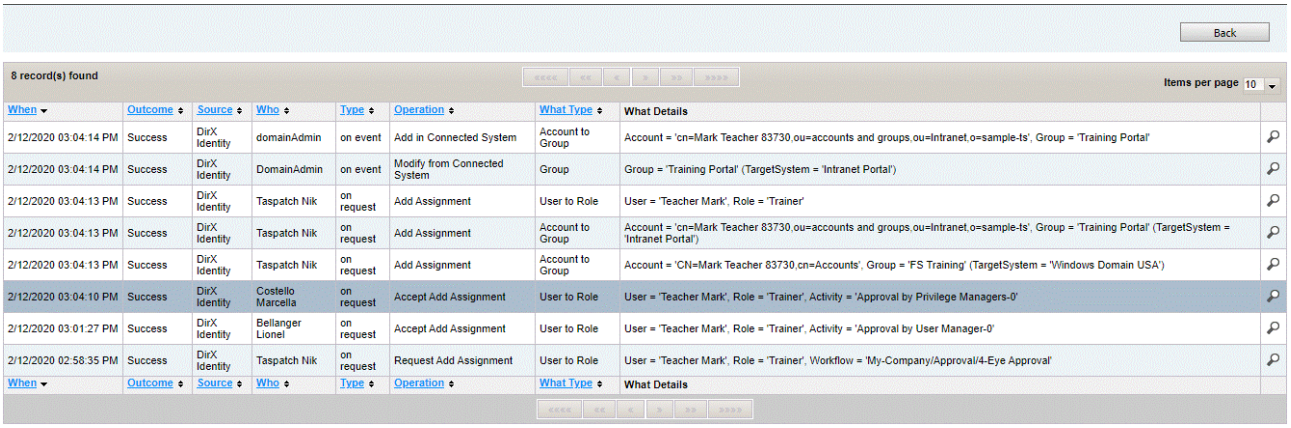


Figure 23. Events Detail - Links to History Entries

Note that you may not see all additional information or the original message related to the audit event in the Event Details window when you purge this audit message data from the DirX Audit Database.

4.7. Viewing Related Audit Events

To view the other audit events that are related to a selected event, click . DirX Audit Manager searches for all audit events that are related to the selected event and presents them in a new page, as shown in the following example:



When	Outcome	Source	Who	Type	Operation	What Type	What Details
2/12/2020 03:04:14 PM	Success	DirX Identity	domainAdmin	on event	Add in Connected System	Account to Group	Account = 'cn=Mark Teacher 83730,ou=accounts and groups,ou=Intranet,o=sample-ts', Group = 'Training Portal'
2/12/2020 03:04:14 PM	Success	DirX Identity	DomainAdmin	on event	Modify from Connected System	Group	Group = 'Training Portal' (TargetSystem = 'Intranet Portal')
2/12/2020 03:04:13 PM	Success	DirX Identity	Taspatch Nik	on request	Add Assignment	User to Role	User = 'Teacher Mark', Role = 'Trainer'
2/12/2020 03:04:13 PM	Success	DirX Identity	Taspatch Nik	on request	Add Assignment	Account to Group	Account = 'cn=Mark Teacher 83730,ou=accounts and groups,ou=Intranet,o=sample-ts', Group = 'Training Portal' (TargetSystem = 'Intranet Portal')
2/12/2020 03:04:13 PM	Success	DirX Identity	Taspatch Nik	on request	Add Assignment	Account to Group	Account = 'CN=Mark Teacher 83730,cn=Accounts', Group = 'FS Training' (TargetSystem = 'Windows Domain USA')
2/12/2020 03:04:10 PM	Success	DirX Identity	Costello Marcella	on request	Accept Add Assignment	User to Role	User = 'Teacher Mark', Role = 'Trainer', Activity = 'Approval by Privilege Managers-0'
2/12/2020 03:01:27 PM	Success	DirX Identity	Bellanger Lionel	on request	Accept Add Assignment	User to Role	User = 'Teacher Mark', Role = 'Trainer', Activity = 'Approval by User Manager-0'
2/12/2020 02:58:35 PM	Success	DirX Identity	Taspatch Nik	on request	Request Add Assignment	User to Role	User = 'Teacher Mark', Role = 'Trainer', Workflow = 'My-Company/Approval/4-Eye Approval'

Figure 24. Related Audit Events

Related audit events include the parent (or causing) events, the child, the sibling events (children of the same parent) and all other indirectly-related events. They are presented in the same way as the Audit analysis. Click 🔎 to view additional information about the selected audit event. To return to the previous result list, click **Back** at the top right of the page.

Note that you may not see a complete list of related audit events that correlate with the selected audit event when you purge these complete audit messages, including message additions and the original message from the DirX Audit Database.

4.8. Exporting Audit Event Data

To export the audit event data presented in a search result table to a report-formatted file, click **Report** in the filter definition area. The DirX Audit Manager displays the **Report Events** dialog that allows you to set the output format for the file as follows:

- **Template** - selects the report template to be used for the file.
  DirX Audit Manager converts the information in the search result table to the format specified in this field.
  Report templates are stored in the folder *install_path***/conf/reports**.
- **Format** - selects the file format to be used; for example, PDF, CSV, Microsoft Word formats (DOCX, RTF), and so on.
- **Encoding** - selects the type of character encoding to be used; for example, UTF-8, Big5, EUC-JP, and so on.
- **Rows** - the number of rows presented in a search result table used for the exported report. For a **0** value, all audit event data presented in a search result table are exported.

Click **Export** to continue the export procedure or click **Cancel** to dismiss it.

When you click **Export**, the Internet browser running the DirX Audit Manager may display a dialog that prompts you to open the report file, save it, or cancel the operation.

4.9. Sending Search Results in E-mail

To send the audit event data as a report attached to an e-mail message, click **Report** in the filter definition area. The DirX Audit Manager displays a dialog that allows you to set the output format for the file. See the section “Exporting Audit Event Data” for information on the settings in this dialog.

Click **Send** to continue the procedure or click **Cancel** to dismiss it.

When you click **Send**, a new dialog opens. Provide data for the **To**, **Cc**, **Bcc**, **Subject** and **Body** e-mail message fields. Click **OK** to send the message.

4.10. Scheduling Search Result Report Generation

To schedule a report generation, select a filter from a filter list (see "Managing Audit Event Filters"), and then click **Report** in the filter definition area. DirX Audit Manager displays a dialog that allows you to set the output format for the file. See “Exporting Audit Event Data” for information on how to make the settings.

If you want to schedule report generation for audit event data searched without using an existing filter, you first must use **Save As** to save your setting as a new filter.

Click **Schedule** to continue the procedure or click **Cancel** to dismiss it.

When you click **Schedule**, the **Add a new report to a report set** dialog opens, where you can add a report to an existing report set or create a new one. For more information about how to configure reports and report sets, see the section "Using the Reports View".

5. Using the Reports View

The Reports view tab is a configuration area for setting up scheduled reports. The DirX Audit Server generates these reports automatically on the specified schedule and e-mails them to the specified recipients. A report set specifies one or more report files to be sent, the schedule for when to send them, and who is to receive them. Each report file contains one or more individual reports.

This chapter describes the Reports view main page layout and how to:

- Create reports, report files and report sets
- Edit reports, report files and report sets
- Delete reports, report files and report sets
- Activate and deactivate report sets
- Synchronize report set updates to the DirX Audit Server

It also contains a reference to the reports overview and samples.

5.1. About the Reports View Main Page

The Reports view main page is shown in the following figure:

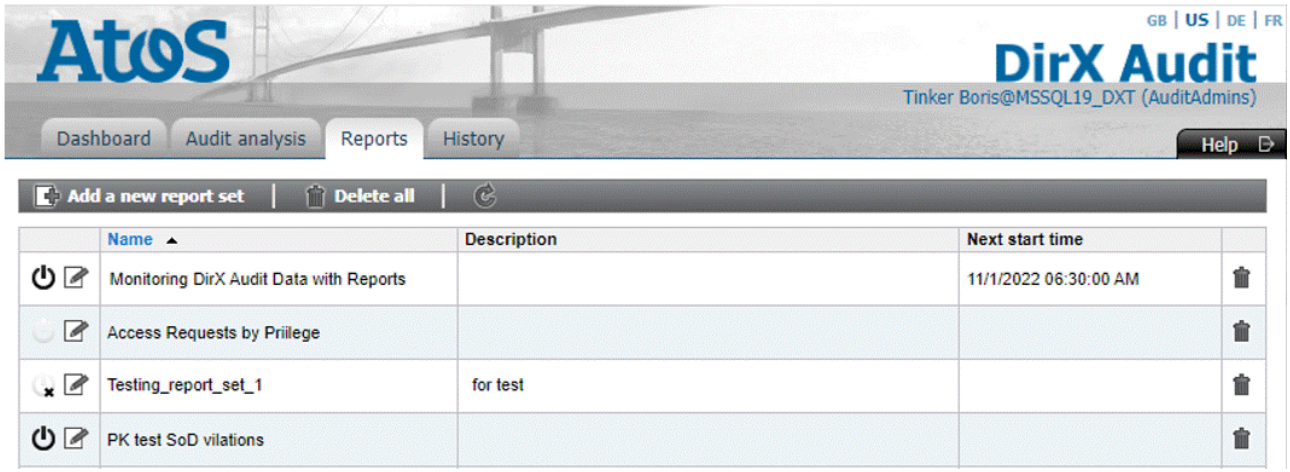


Figure 25. Reports View - Main Page

As shown in the figure, the Reports view consists of a toolbar at the top of the page and a table showing the current report set definitions. The toolbar provides the following selections:

- **Add a new report set** - allows you to create a new report set definition from scratch.
- **Delete all** - allows you to delete all report set definitions from the table and the database.
- - refresh the list of report sets.

The table consists of report set definitions listed by their names, their descriptions and the next time they will start up. You can perform the following actions here:

- Click in a report set in the list to deactivate it. Click or to activate it. The icon indicates that it cannot be activated until its schedule is changed.
- Click in a report set in the list to edit it.
- Click in a report set in the list to remove it.

The next sections provide more information about the operations in the Reports view. Note that users with the RestrictedAuditors role can see only the Reports view in the DirX Audit Manager and only use report templates with the Restricted tag described in this section.

5.2. Creating a Report Set

To create a new report set from scratch, click the **Add a new report set** button. This action displays the **Edit report set** dialog, as shown in the following figure:

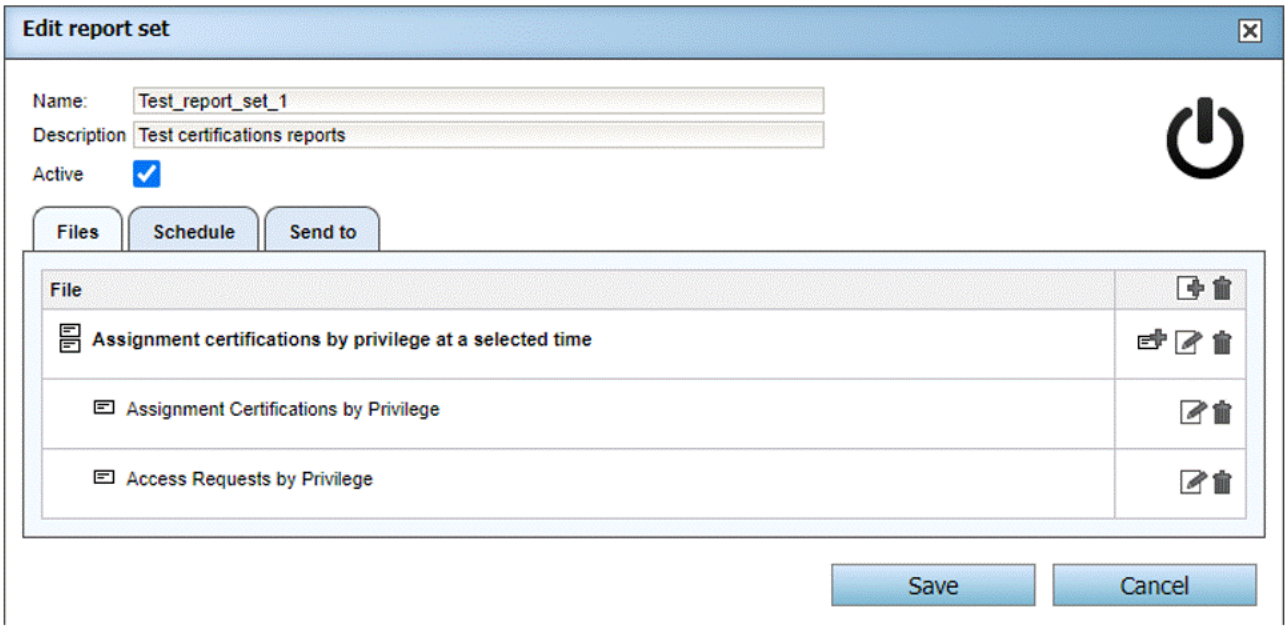


Figure 26. Reports View - Edit Report Set

The **Edit report set** dialog contains the following items:

- **Name** - provides a name for the report set.
- **Description** - provides a description for the report set.
- **Active** - activates or deactivates the report set. The or icon appears based on the selection.
- **Files** - specifies the report files to be sent in the e-mail and the reports contained in each file.
- **Schedule** - defines when to generate the reports.
- **Send to** - specifies the e-mail data to be used when e-mailing the report (sender, recipients, message text).

- **Save** - stores the report set definition.
- **Cancel** - cancels the operation.

To create a new report set in the Edit report set dialog:

- Enter a **Name** and **Description** for the report set.
- Use the Files tab to create one or more report files and add them to the report set. See the section "Creating a Report File" for details.
- Select the Schedule tab to define the schedule for the report set. See the section "Defining the Schedule" for more details.
- Select the Send to tab to define the recipients and other options for the e-mailed reports. See the section "Defining the E-mail Message" for details.
- Click **Save** to store the new report set definition.

5.2.1. Creating a Report File

To create a new report file for a report set, click  in the Files tab header in the Edit report set dialog. This action starts a wizard that lets you add one or more reports to the report file and set the file's name and format. For each report to be added, you first select a report template from a list of existing templates and then edit the scope and output format to your requirements. The next sections describe these steps in more detail.

Note that multiple reports can be combined into one file only when the file format is PDF. Legacy reports – reports that have been created with versions of DirX Audit up to DirX Audit 4.0 – cannot be combined with other reports and will always be sent as separate files.

5.2.1.1. Selecting a Report Template

The report file creation wizard's Report selection dialog lets you select a report template from a list of existing templates. The following figure shows an example of this dialog:

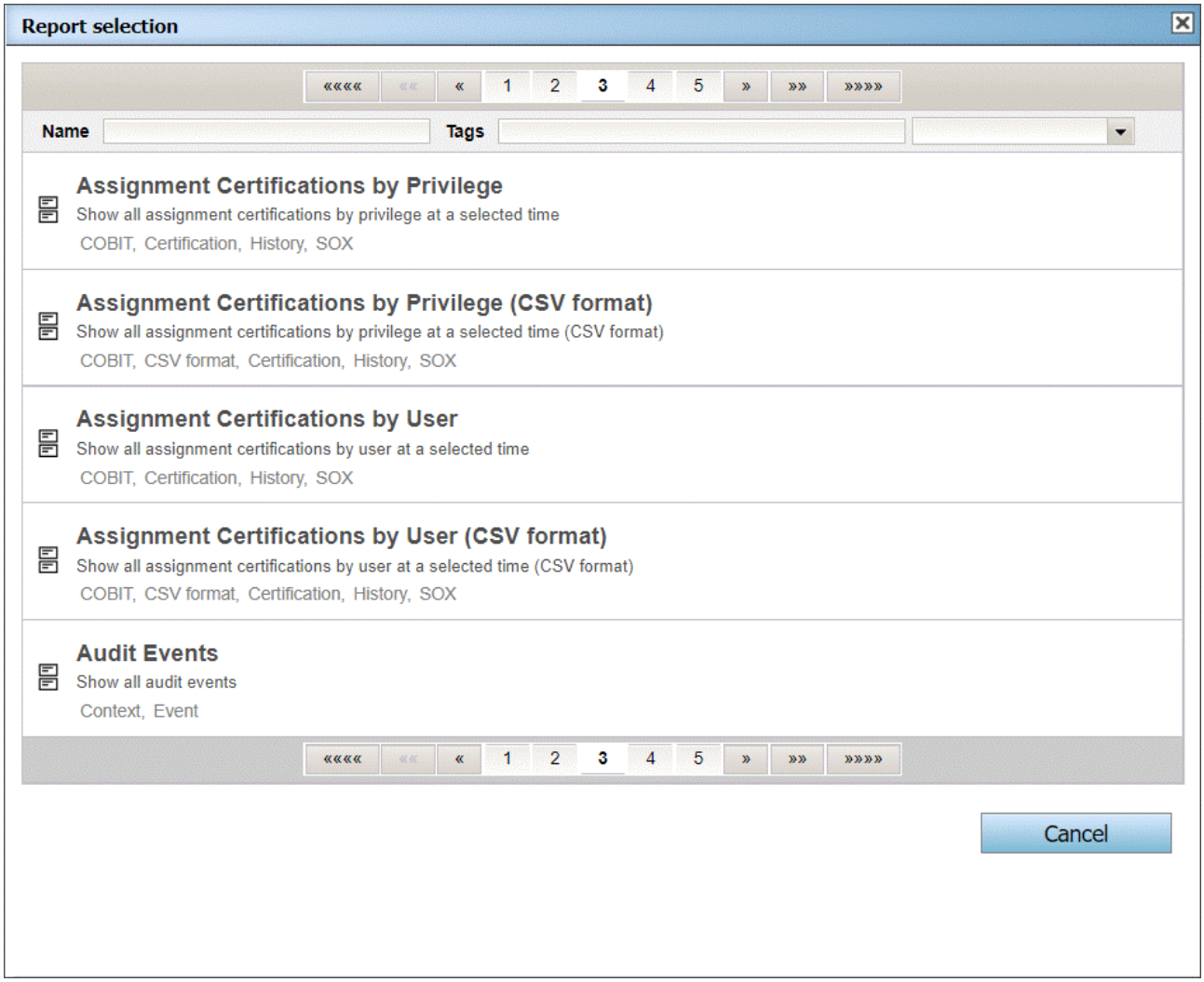


Figure 27. Reports View - Report Selection Dialog

Each item in the list shows the name of the report template, its description and the list of tags associated with it. Use the page navigator at the top and bottom of the dialog window to page through the list. The section "Using the Page Navigator" in the chapter "Using Audit Analysis" describes how to use this tool.

Use the **Name** and **Tags** fields to filter the list of existing report templates by name or by a tag:

- To search for a report by name, type a string into **Name**. The list of existing report templates is refreshed to display all reports whose names contain the string.
- To search for a report by tag, click the down arrow to the right of **Tags** to display the tags associated with at least one of the existing reports and then select one or more tags. Clicking on one of the tags shown in the report definitions also adds the tag to the list. You can find reports created in versions of DirX Audit prior to V5.0 by using the tag **Legacy**. Some report names or configuration options may vary in new versions. The list

of existing report templates is refreshed to display the reports that contain at least one of the selected tags. Note that the matching reports need not contain all of the given tags. DirX Audit 7.0 adds the Restricted tag, which is visible in the list of tags only for users with the AuditAdmins role. Users with the RestrictedAuditors role can see and use only reports with this tag.

To select a report template from the list, click it. This action opens a new Report scope dialog for setting the scope and the output format for the selected report.

Click **Cancel** to cancel report template selection and return to the Edit report set dialog.

5.2.1.2. Setting the Scope and Output Format

The report file creation wizard's Report scope dialog lets you customize the scope of a report template you select in the Report selection dialog. A report's scope specifies the set of objects on which it reports and depends on the configuration of the report template.

A scope is composed of different variables; for example, a time range. Each section in the dialog allows you to define a particular variable. Some definitions are mandatory, while others are optional, depending on the report template configuration. You'll need to define a time range in the **When** section for the events or entries in which you are interested. Usually, you'll select **Previous Month** to get the events of the previous month - for example, the events that occurred in April when the report is run in May. The other options are the same as in the Audit analysis tab: previous day, week or year, week / month / year to date, last hour / 24 hours, today, custom time (you set fixed start and end date and time) and all (any time). See the section "Filtering Audit Events" in the chapter "Using Audit Analysis" for details.

In some cases, you will need to define a time point in the **When** section for history entries. Usually, you'll select **End of Previous Month** to get the state of the history entry at the end of the previous month. The other options are **End of Previous Day** and **End of Previous Week**.

Other sections in the scope definition dialog let you select:

- A list of entries (such as a list of users, privileges, or target systems) in which you are interested
- A list of filter attributes for entries that match the filter (for example, a list of organizational units)

A scope definition dialog may also provide check boxes for specifying, for example, whether or not:

- To produce short or long output. Long output contains more properties of an event or entry output. Short output formats typically give the most important information on an event or an entry within one line while long output formats use three or four lines per event or entry.
- To include only orphaned, imported or disabled accounts.
- To include only failed events; for example, only failed logins.

If you don’t provide a definition for an optional variable, the set of matching events or entries is unrestricted.

To select a list of users, privileges, target systems, organizational units or other similar items:

- In **Identifying Attributes**, click the down arrow to display a list of existing attribute names - for example, Name, First Name, Last Name for a user, Name and AltName for a privilege - and then select one from the list.
- Enter a string into **Attribute Value** and then click **Search**.

The list of matching entries is displayed in the **Found** table. Select one or more entries and then click **Add** to add them to the list of selected entries in the **Selected** table. If you want to remove some entries you previously added from the **Selected** table, select them in the **Selected** table and then click **Remove**; you can also click **Clear** to remove all entries from the **Selected** table.

A scope definition dialog may also provide the **Pseudonymize** checkbox for specifying whether or not to show sensitive user data in the report.

The **Record limit** field lets you limit the number of records for the final report; **0** means unlimited.

The following figure shows an example of this dialog. It is intended to select a list of users. They are searched by the identifying attribute Last Name. You can also filter the users search here. The **Found** table displays five users. The **Selected** table currently lists two users that have already been selected and added.

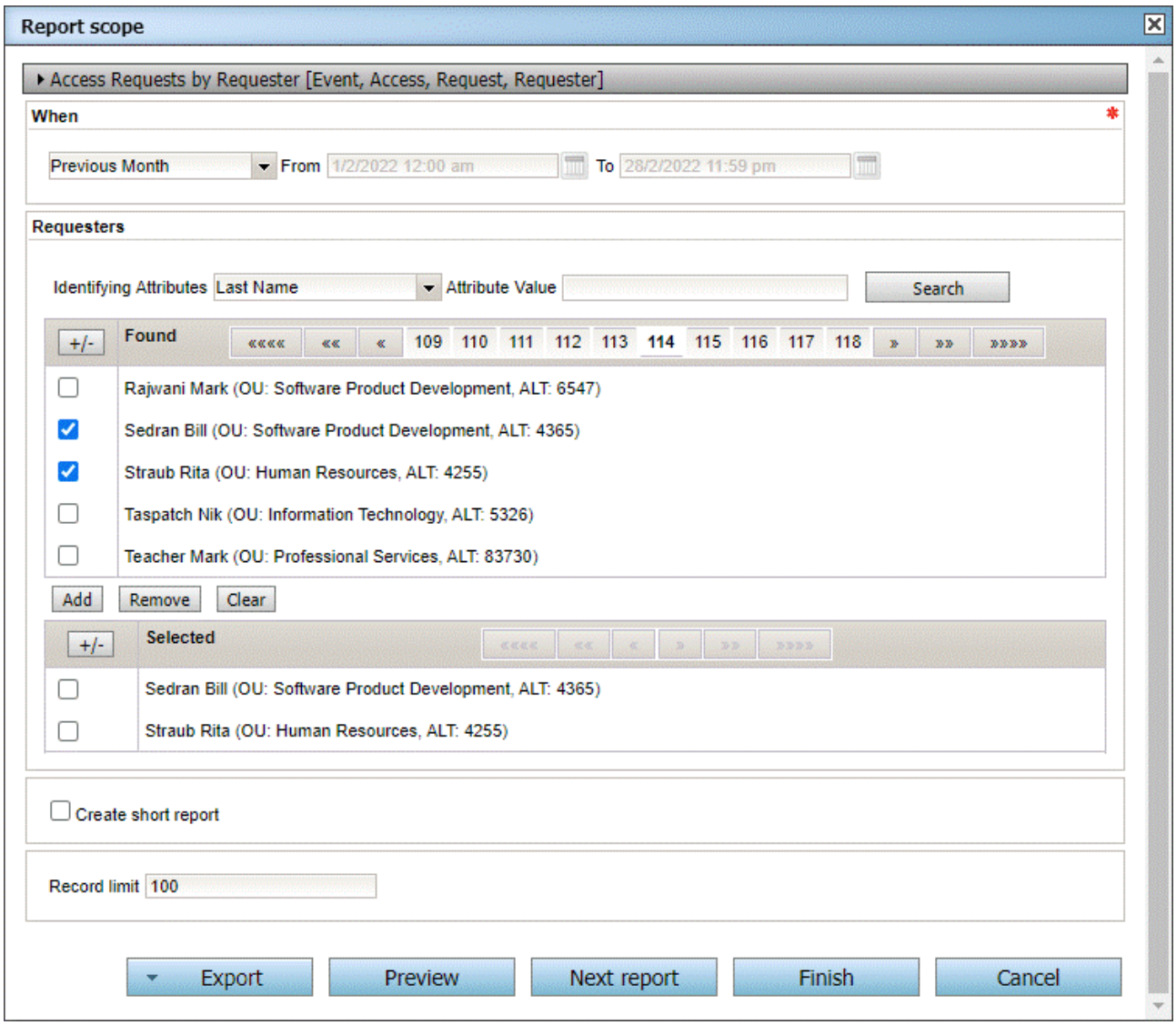


Figure 28. Reports View - Report Scope Definition Dialog

Click **Export** to export the final report. You can select between PDF and formats such as DOCX, HTML, and XLSX. Note that the **Record limit** field restricts the number of results.

Click **Preview** to see the first few pages of the report in a new browser tab. Note that the **Record limit** field restricts the number of results displayed in the Preview report.

Click **Next Report** to add another report to the same report file.

Click **Finish** when you have completed the scope definition for the final report to be added to the report file and you don't want to add another report to the same file. The wizard opens a new dialog to define the report file's name and format.

Click **Cancel** to discard your changes and return to the Report selection dialog.

5.2.1.3. Defining the File Name and Format

The report file creation wizard's Edit file dialog allows you to enter the report file's name and its description and to specify its file format. The following figures show examples of this dialog:

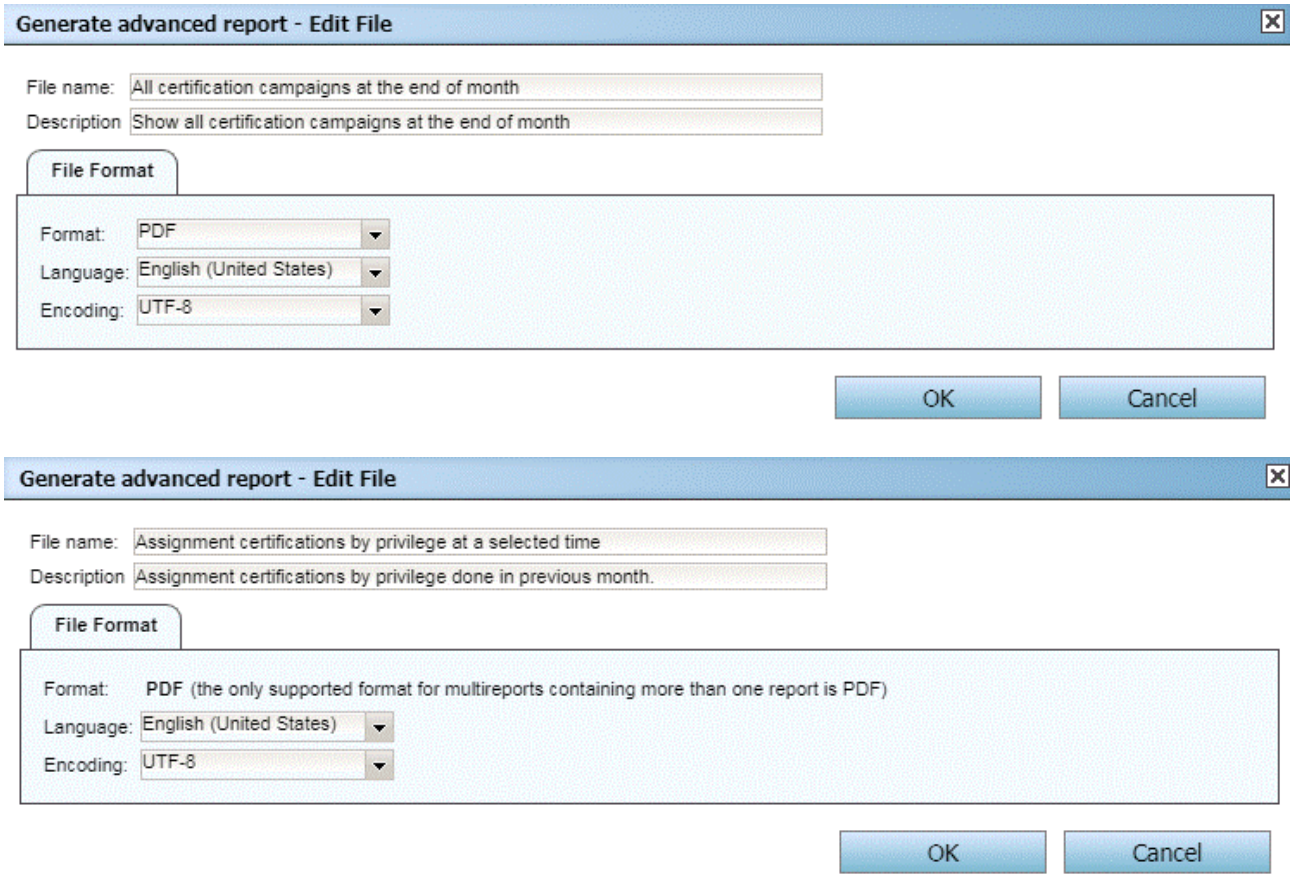


Figure 29. Reports View - Report File Name and Format Definition Dialog

In the File Format tab, you can set:

- **Format** - the output format. You can select between PDF and formats such as DOCX, HTML, and XLSX. Note that only PDF format allows for combining multiple reports in the same file.
- **Language** - the language to use for localized reports. Selections are German, French, English (United States) and English (United Kingdom).
- **Encoding** - the character encoding to be used for report production.

Click **OK** to save the report file definition in the report set and return to the Reports view main dialog.

5.2.2. Defining the Schedule

Use the Schedule tab in the Edit report set dialog to set up the schedule for when the report files are to be produced for the report set. You can select from **Simple**, **Recurring**, **Expert** and **As soon as possible** configurations.

The **Simple** configuration contains only the date and time at which the report set should be run.

The **Recurring** configuration provides user controls to run the report set repeatedly on a daily, weekly or monthly basis. Specify the **Start date** and optionally the **End date** of the report and the time to run it. Select days of week for the weekly frequency and day of month for the monthly frequency.

The **Expert** configuration is based on a **cron** expression. Specify the **Start date** and optionally the **End date** of the report, and then define the **cron** expression. For a detailed tutorial on **cron** expressions, see the following 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 3:01am, use the following expression:

```
0 1 3 * * ?
```

When you select **As soon as possible**, the DirX Audit Server produces and sends the report set as soon as it reads it. In cases where the server is not running, you can limit the time period. If the server reads the request after the set end date, it will silently ignore it.

Note that you can also use the schedule feature in the Dashboard view and Audit analysis to schedule reports of Dashboard components and event filters.

5.2.3. Defining the E-mail Message

Use the Send to tab in the Edit report set dialog to provide the data for the **To**, **Cc**, **Bcc**, **Subject** and **Body** e-mail message fields. You can specify multiple e-mail addresses by separating each one with a comma (,).

5.3. Editing a Report Set

To edit a report set, click  in the selected report set in the table of the Reports view main page. This action opens the Edit report set dialog. See the section "Creating a Report Set" for a general description of this dialog.

When you open a report set for editing, select the Files tab if it's not already selected. It lists the report files included in the report set (identified by the  icon for multireports or the  icon for single reports) and shows the individual reports included in each report file (identified by the  icon).

To change the name or format of a report file included in the report set, click in the column to the right of the report file listed in the Files tab. This action opens the report file creation wizard's Edit file dialog. See the section "Defining the File Name and Format" for details.

To change the template or the scope of a report included in a report file, click in the column to the right of the report listed underneath the file report line in the Files tab. This action opens the report file creation wizard's Report scope dialog. See the sections "Selecting a Report Template" and "Setting the Scope and Output Format" for details.

To add a new report to a report file included in the report set, click in the column to the right of the report file listed in the Files tab. This action opens the report file creation wizard's Report selection dialog.

Use the Schedule tab to change the report set schedule. See the section "Defining the Schedule" for details.

Use the Send to tab to change the e-mail information. See the section "Defining the E-mail Message" for details.

5.4. Deleting Reports and Report Sets

You can delete a single report set or all report sets from the Reports view table:

- To remove a single report set from the table, click in the corresponding row.
- To remove all report sets, click **Delete all** in the table header.

To remove a report from a report file in a report set, click in the corresponding row for the report of the Edit report set dialog's File tab.

5.5. Activating and Deactivating Report Sets

To activate or deactivate a report set, you can either:

- Click or in the first column for the report definition in the report set table.
- Check or uncheck the **Active** checkbox in the Edit report set dialog to activate or deactivate the report set. The or icon appears based on the selection.

The icon in a report set definition indicates that it cannot be activated until its schedule is changed.

5.6. Synchronizing Report Set Updates to the DirX Audit Server

Every change you make in the **Reports** view must be synchronized to the DirX Audit Server. The synchronization process runs automatically on the DirX Audit Server, which checks the changes on every specified time interval. Synchronization of a recently changed report set is indicated with ⇄ in the first column of the report set list. The synchronization is usually finished in few seconds. If it does not finish in a minute, check whether the DirX Audit Server service is running.

5.7. About the Reports Overview

The reports overview file is intended to help you find the right report for your data. The reports overview provides a list of reports, divided into groups, including all tags and descriptions. It specifies source data and provided output, the DirX Audit version in which the respective report was introduced, and links the reports to the configuration files in the *install_path*/**conf/report-definitions/** folder and to the sample report files provided in the *install_media*/**Additions/Data/SampleReports** folder where the reports overview file is also stored.

6. Using the History View

The History view is DirX Audit Manager's interface to the DirX Audit History Database. The History view works directly with history entries stored in the DirX Audit Database. This chapter describes the features of the History view and how to:

- Select a history entry
- Show a history entry's details
- Export history entries

6.1. Selecting a History Entry

The History view's main page allows you to select an entry in the DirX Audit History Database for historical analysis. The History view main page is shown in the following figure:

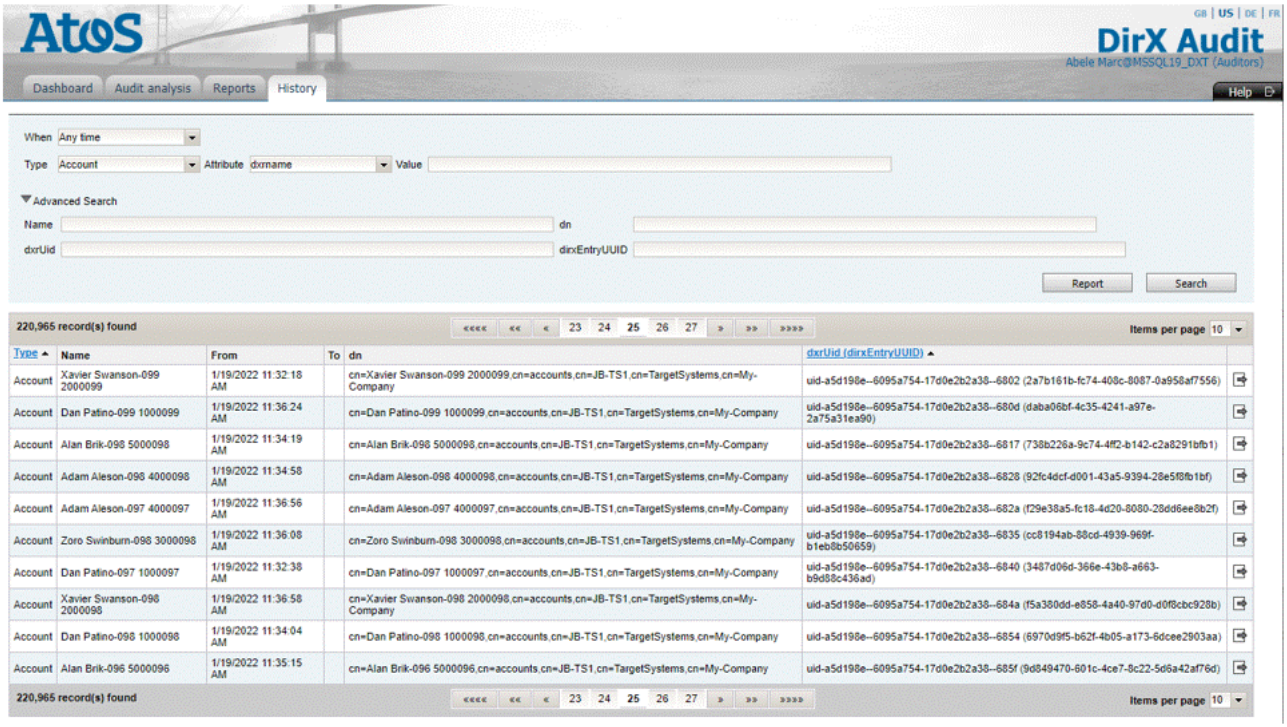


Figure 30. History View - Main Page

To select a history entry:

- Set a relative or absolute period in **When**; for example, within the previous year (**Previous Year**), within the previous month (**Previous Month**), within the current month (**Month to date**) and so on. Selecting **Any time** means that all of the history entries are displayed. Selecting **Custom time** allows you to set specific start and end dates with the **From** and **To** fields.
- Select an entry type in **Type**. Selecting **ANY** displays all of the types.
- Select a history object attribute in **Attribute** and enter its value in **Value** to filter the history entries with specific attribute value. To prevent filter criteria from being applied to an attribute, leave the **Value** field empty.

- Optionally expand the **Advanced Search** area (click the arrow on the left) and then enter the entry's name or its prefix in **Name** or its distinguished name in **dn**. You can enter the entry's unique identifier or its prefix in **dxrUid** or **dirxEntryUUID**. If you don't provide it, the set of matching entries is unrestricted.
- Click Search to find entries that existed in the period specified in **When** and match the other conditions too.

For the **Attribute** filter, the **Selection list** component is used and you can select one of the preselected available values from the list. The attribute list is loaded directly from the database (default) or from the configuration file according to your configuration. For more details on customizations, see the section "Customizing the History View" in the *DirX Audit Customization Guide*.

Filter conditions of the DN search in the advanced search mode use an "Ends with" comparison operator. This facilitates searching for history entries from the same company or organizational unit; that is, entries having the same final part of their DN attribute value. For example, entering the dn filter value of **"cn=MVS,cn=TargetSystems,cn=My-Company"** results in searching only for history entries from the **MVS** node of target systems in the **My-Company** node.

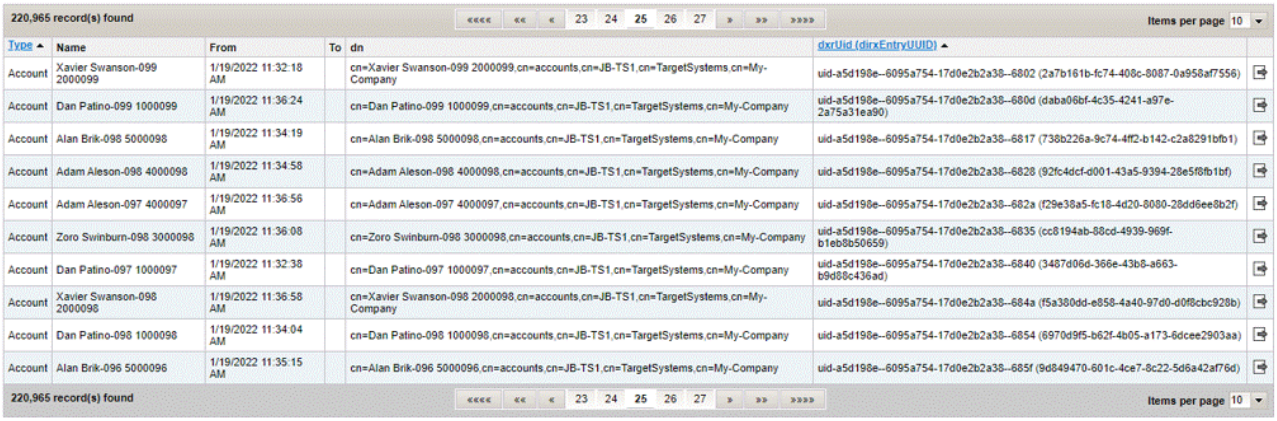
Filter conditions for **Value**, **Name**, **dxrUid** and **dirxEntryUUID** use a "Starts with" comparison operator. For example, entering "Meeting" into the **Name** field returns all meeting room entries. You can also use the SQL wildcard character **%** to field input. For example, searching for the value of "%Munich" of the "cn" attribute will find also entries with Munich in the middle of their name such as Parking Place Munich or Access to Munich - Data Center.

If the search operation does not find any history entries that match the search criteria, it displays a message.

If the search operation finds exactly one history entry, it displays this entry's details page, as described in "Showing a History Entry's Details".

If the search operation finds more than one history entry, it displays a result table that lists all of the matching entries. The table header and footer show the total number of matching entries and provide a table page navigator and a drop-down menu for changing the maximum number of items displayed per page.

The following figure shows a result table page:



220,965 record(s) found — «« « 23 24 25 26 27 » »» — Items per page 10

Type	Name	From	To	dn	dxrUid (dirxEntryUUID)
Account	Xavier Swanson-099 2000099	1/19/2022 11:32:18 AM		cn=Xavier Swanson-099 2000099,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--6802 (2a7b161b-fc74-408c-8087-0a958af7556)
Account	Dan Patino-099 1000099	1/19/2022 11:36:24 AM		cn=Dan Patino-099 1000099,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--680d (daba06bf-4c35-4241-a97e-2a75a31ea90)
Account	Alan Brik-098 5000098	1/19/2022 11:34:19 AM		cn=Alan Brik-098 5000098,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--6817 (738b226a-9c74-4ff2-b142-c2a8291bfb1)
Account	Adam Aleson-098 4000098	1/19/2022 11:34:58 AM		cn=Adam Aleson-098 4000098,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--6828 (92fc4dcf-d001-43a5-9394-28e5f8fb1bf)
Account	Adam Aleson-097 4000097	1/19/2022 11:36:56 AM		cn=Adam Aleson-097 4000097,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--682a (f29e38a5-fc18-4d20-8080-28dd6ee8b2f)
Account	Zoro Swinburn-098 3000098	1/19/2022 11:36:08 AM		cn=Zoro Swinburn-098 3000098,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--6835 (cc8194ab-88cd-4939-969f-b1eb8b50659)
Account	Dan Patino-097 1000097	1/19/2022 11:32:38 AM		cn=Dan Patino-097 1000097,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--6840 (3487d06d-366e-43b8-a663-b9d88c436ad)
Account	Xavier Swanson-098 2000098	1/19/2022 11:36:58 AM		cn=Xavier Swanson-098 2000098,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--684a (f5a380dd-e858-4a40-97d0-d0f8cbc928b)
Account	Dan Patino-098 1000098	1/19/2022 11:34:04 AM		cn=Dan Patino-098 1000098,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--6854 (6970d9f5-b62f-4b05-a173-6dcee2903aa)
Account	Alan Brik-096 5000096	1/19/2022 11:35:15 AM		cn=Alan Brik-096 5000096,cn=accounts,cn=JB-TS1,cn=TargetSystems,cn=My-Company	uid-a5d198e--6095a754-17d0e2b2a38--685f (9d849470-601c-4ce7-8c22-5d6a42af76d)

220,965 record(s) found — «« « 23 24 25 26 27 » »» — Items per page 10

Figure 31. History View - Result Table

Each history entry listed in the result table is identified with its **Name**, **dn** and **dxrUid** (**dirxEntryUUID**) attributes, whose values correspond to the entry's data in the related DirX Identity domain. If an entry's **Name** or **dn** has been modified during the selected time period, the entry row is duplicated and each row result contains history data that existed before and after the modification.

The **From** and **To** columns indicate the entry's lifetime: when it was created to when it was deleted or renamed.

You can sort the result table according to the **Type** and **dxrUid** (**dirxEntryUUID**) values in ascending or descending order.

To examine the data for an entry in the table, click in its row. The details page for the entry opens.

6.2. Showing a History Entry’s Details

The history details page provides detailed information about a selected history entry. The following figure shows an example of a history entry’s details page:

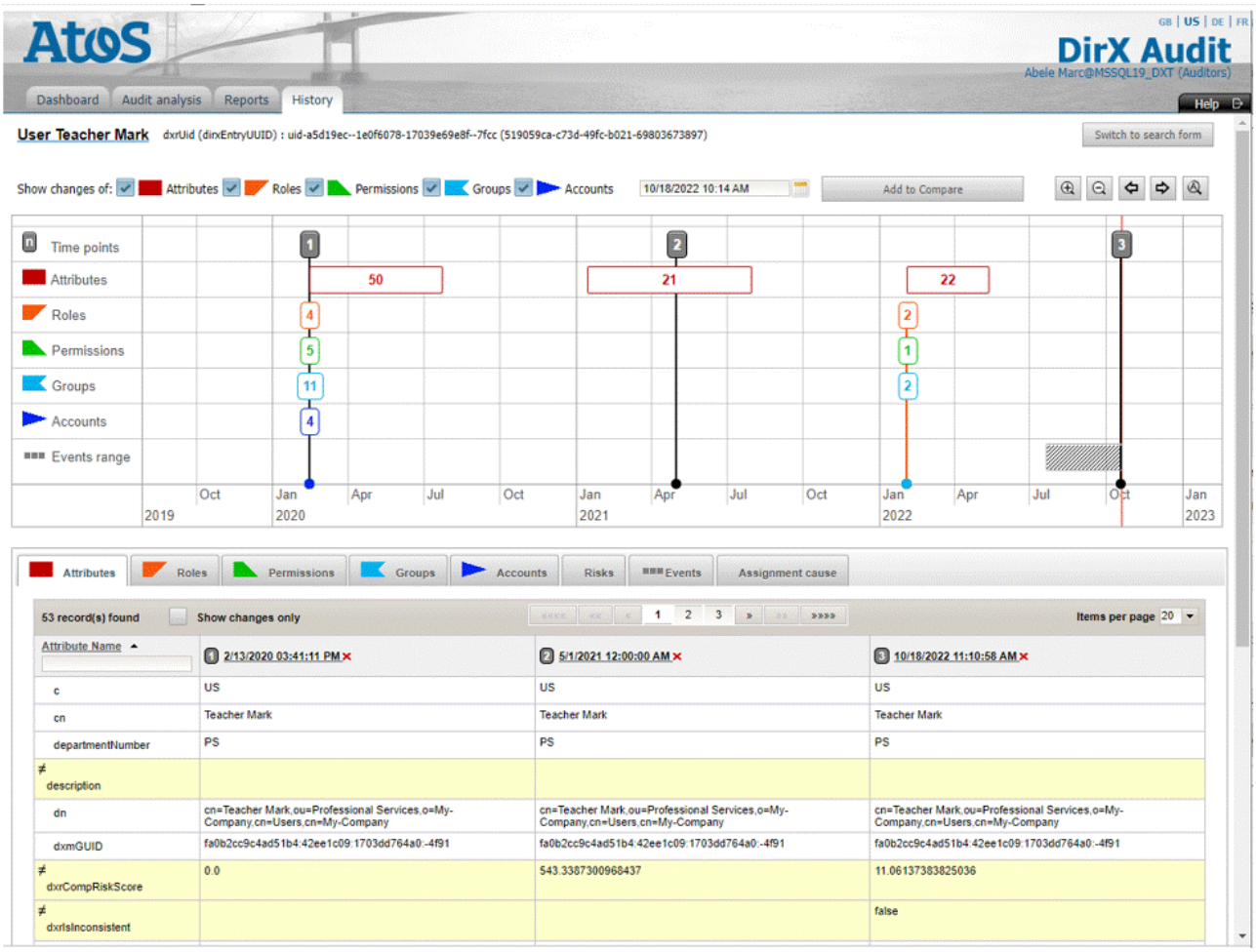


Figure 32. History View - Details Page

As shown in the figure, the history details page is composed of a header area, a timeline area, and a data area.

The header area identifies the entry’s type and name and provides controls for:

- Setting target time points (dates and times) for comparing entry history data at different points in time.
- Selecting the type of history entry data to be displayed in the timeline.
- Returning to the history search results page.

The timeline area is composed of a calendar grid that displays:

- Comparison time point markers, which show the comparison time points indicated by the values supplied in the **When** parameter for the search (**Previous Month**, custom time and so on) and any new comparison time points you create. If you select **Any time** for the search, the **from** value of this history entry is used as the first time point. These markers are numbered sequentially and are shaded in gray. For example,  indicates the first time point in the timeline.
- Change markers, which show time points at which entry data was created or modified. Change markers indicate the number of items affected by the creation or modification operation and are outlined in color. A change marker's color corresponds to the item's type, as specified in the **Show changes of** fields and the left-most column of the timeline grid. For example,  indicates two attribute changes.

Note that the timeline area shows the cumulative information about history entry data changes because the zoom level is set to months. To view the times in more detail, you'll need to adjust the timeline's scale and then zoom in to days. You can proceed this way up to milliseconds.

The data area contains one or more tabs, depending on the entry type. Each tab provides a results table that shows the history entry's data at each selected comparison time point. When user type entries are displayed, any privilege or account history entry types that are not synchronized to the DirX Audit History Database will show only summary information (common name and its DN) in the result table. Some tabs contain additional filtering options for faster searching in parameters. The table header and footer show the total number of data items and provide a table page navigator and a drop-down menu for changing the maximum number of items displayed per page.

From the header area, you can:

- Check and uncheck the **Show changes of** fields to select the types of data items associated with the entry to be shown in the timeline and data areas; for example, Attributes, Roles, Permissions, Groups or Accounts. The available fields depend on the entry type.
- Enter a target date and time and then click **Add to Compare** to add a new comparison time point to the timeline and data areas. This action adds a new comparison time point marker to the timeline area and a new column with the new comparison time point and the resulting data to each tab in the data area.
- Check **Show changes only** to restrict the results displayed in data area tabs to changed values only; otherwise, all data is presented. Rows that contain changes are highlighted.

In the timeline area, you can:

- Use the zoom in/out buttons to increase or decrease the timeline scale.
- Use the left- and right-arrow buttons to move the timeline forward or back. You can also click in the timeline and then use your mouse to drag it forward or back.
- Use the icon to reset the timeline area's boundaries so that all comparison time point markers and change markers are displayed.
- Double-click in the timeline area to create a new comparison time point. This action has the same result as using **Add to Compare**.
- Select a comparison time point and then drag and drop it to another part of the timeline area. This action recalculates the column in the data area that corresponds to the adjusted time point.
- Associate a comparison time point with a change marker by clicking on the change marker and then clicking the button that appears to the left of the icon. (Note that the button does not appear if a comparison time point is already associated with the change marker). This action adds a comparison time point that corresponds to the change related to the selected change marker to the timeline area and the data area.

The data area presents the history entry's data in two or more tabs depending on the entry type:

- The Attributes and Events tabs are presented for every entry type.
- The Overview tab is available for Workflow Instances, Certification Campaign and Certification Assignment Change history entry types.
- The User history entry's data is extended with Roles, Permissions, Groups, Accounts, Risks and Assignment cause tabs.
- The Role history entry's data is extended with (Junior) Roles, Permissions and Users tabs.
- The Permission history entry's data is extended with Groups and Users tabs.
- The Group history entry's data is extended with the Users tab.
- The Certification Campaign entry's data is extended with either the Users or Privileges tab.

In the data area, you can delete a comparison time point by clicking the button in its column head. This action removes the column from the table and removes the time point marker from the timeline area. The comparison time point date can be changed either by moving the point in the timeline or by clicking it in the data area and entering a new time value.

The Attributes tab table is divided into the **Attribute Name** column and one or more attribute value columns for each target date. You can sort the table data according to the attribute name in ascending or descending order. You can use the filter field in the **Attribute Name** column for faster searching in parameters. The same filter field is available in other tabs and it is recommended that you use it for searching instead of browsing through pages in case you have a large amount of data, such as many users in one role. You can then use the cross icon to clear the filter field.

Some multivalue attributes contain a large number of values; for example, the **dxrGroupMemberAdd** attribute. For better readability, the number of displayed values is limited. If the count of attribute values exceeds the configured maximum, the total number of values is displayed in red.

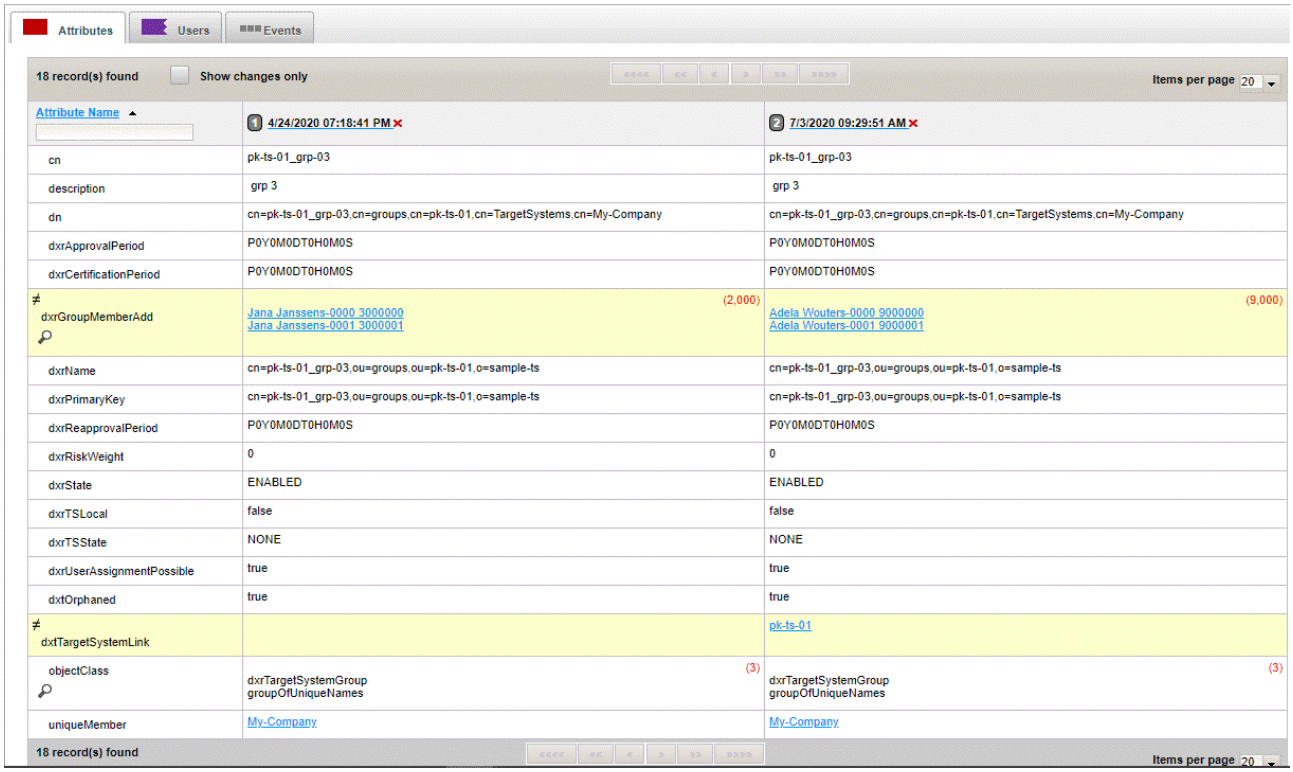


Figure 33. History View - Attributes Tab with Multivalue Attributes

To see all values, click 🔎 (Show Detail) near the attribute name. A new window opens showing the complete results. In this window, you can use the filter for faster searching in values; the table header and footer show the total number of data items and provide a table page navigator and a drop-down menu for changing the maximum number of items displayed per page. For more details on customizing the maximum value, see the section “Customizing the History View” in the *DirX Audit Customization Guide*.

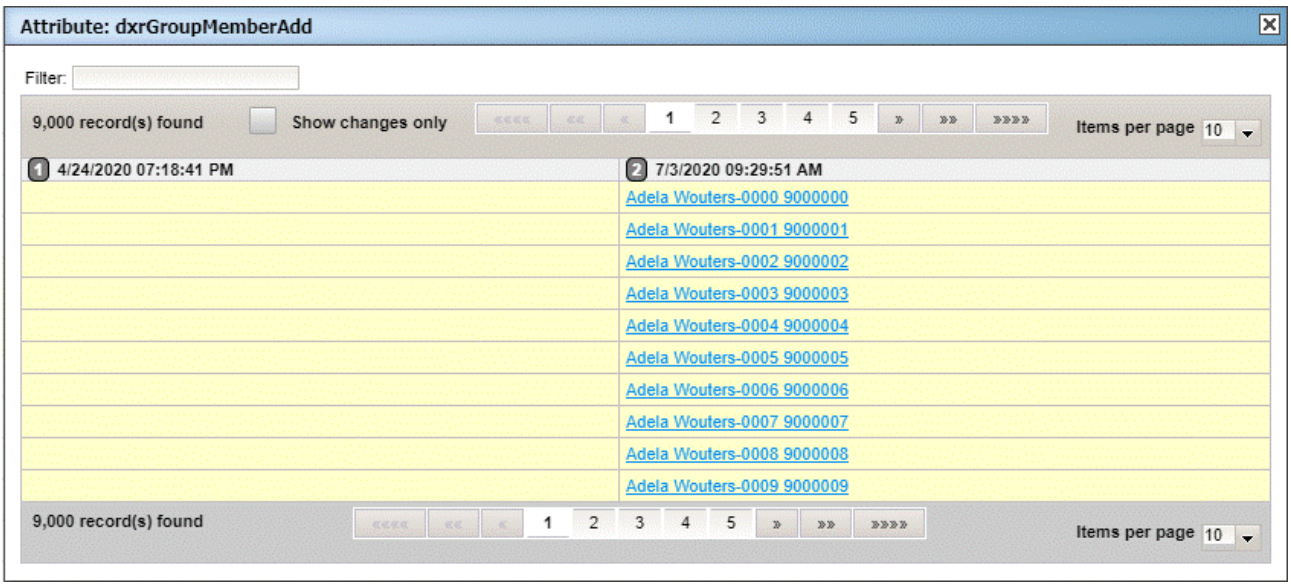


Figure 34. History View - Multivalue Attributes Details

Some attribute values represent references to other entries. You can click the value to get history entry's data for the referenced entry. You can then use the **Already Viewed Entries** selection box in the page header to get to the previous entry.

The Roles, Permissions and Groups tabs are organized in a different way. The name column also contains the assignment mode: rule, BO, manual and inherited. For groups, it is also extended with the target system name. Each comparison time point column indicates whether or not the entry (user, role or permission) to privilege assignment existed and contains additional assignment data such as start date, end date, needs re-approval flag, in approval flag and is inconsistent flag for all assignment type and role parameter values for manual user-to-role assignment. For user-to-privilege assignments, the time period for which the assignment is valid is also shown in the table cell.

The Accounts tab is similar to the other Groups tabs. The name column also contains the target system name and each comparison time point column indicates whether or not the user's account existed. Account state and target system state are also shown here.

The individual items in these tabs can be expanded by clicking ▶ next to their names to display their state and properties.

The Risks tab provides user risk data based on 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 data.

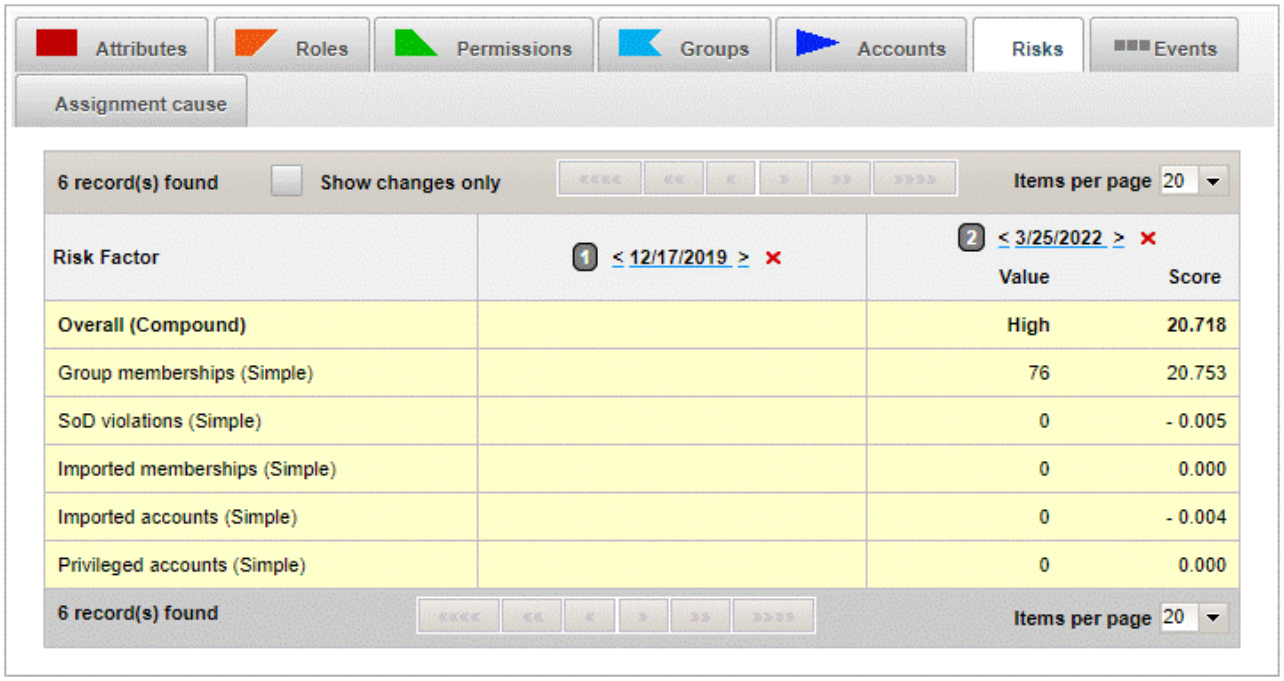


Figure 35. History View Details - Risks Tab

The Events tab displays events related to the selected history entry. The events are displayed in the time period defined either by the Events range bar in the timeline or by specifying the initial **From** and final **To** dates in the Events area below the timeline.

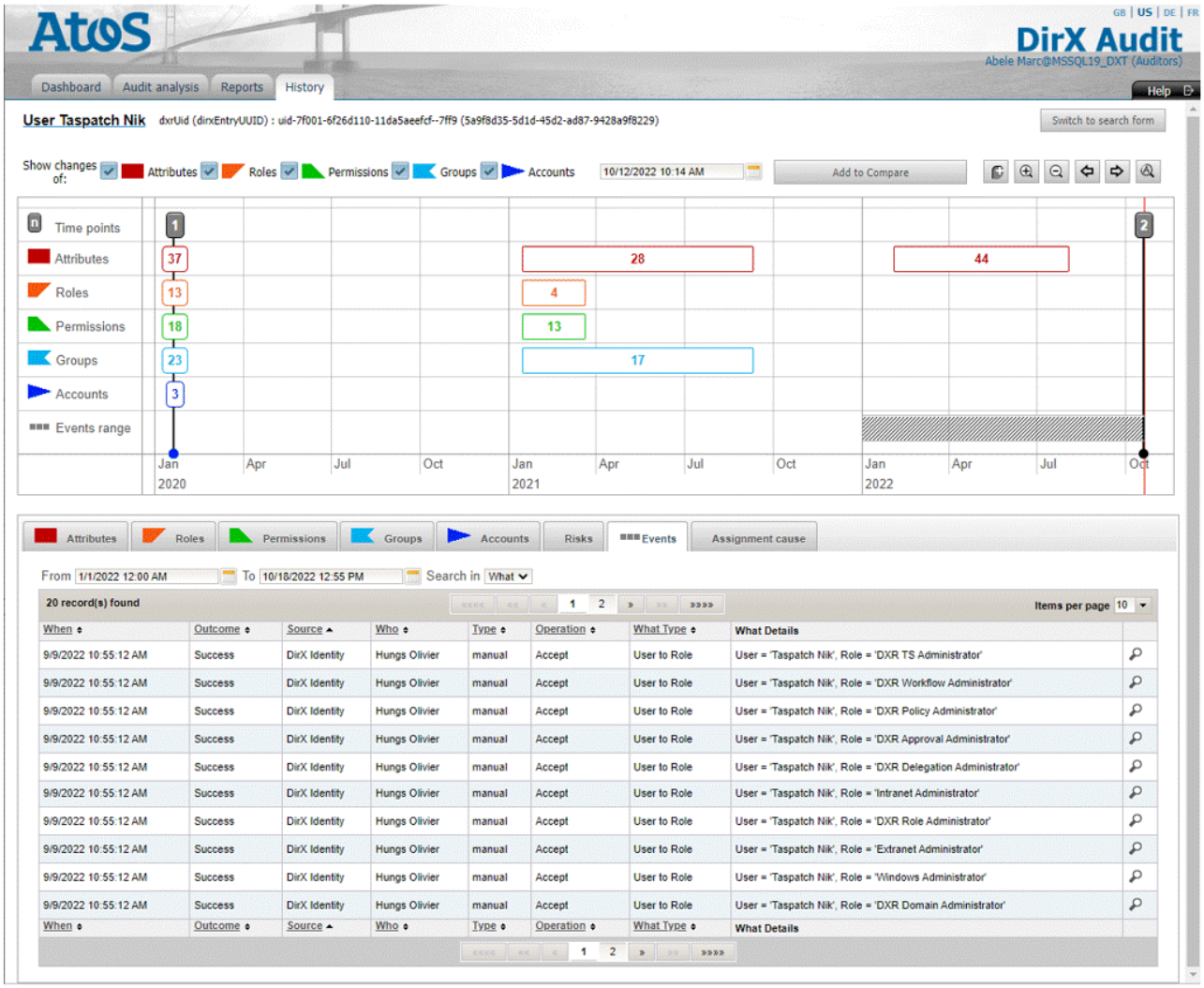


Figure 36. History View Details - Events Tab

The Assignment cause tab (located next to the Events tab under the timeline) displays causing events for the selected privilege. To view contextually-related events in an expanded list, click ▶ in front of the event date. This tab offers a useful correlated data search for the original event that triggered the selected role, permission or group assignment. You can use the selection box to select the privileges. You can also choose a privilege in individual Roles, Permissions and Groups tabs by clicking  next to the corresponding privilege name. This action automatically switches the view to the Assignment cause tab.

The Overview tab is available for workflow instances, Certification Campaign and Certification assignment change history entry types. The Overview tab is displayed as these entries' default tab. This tab provides an overview of important workflow information such as status, result, requestor and approvers and related activities for workflows; type, owner, status and certification entries for certifications.

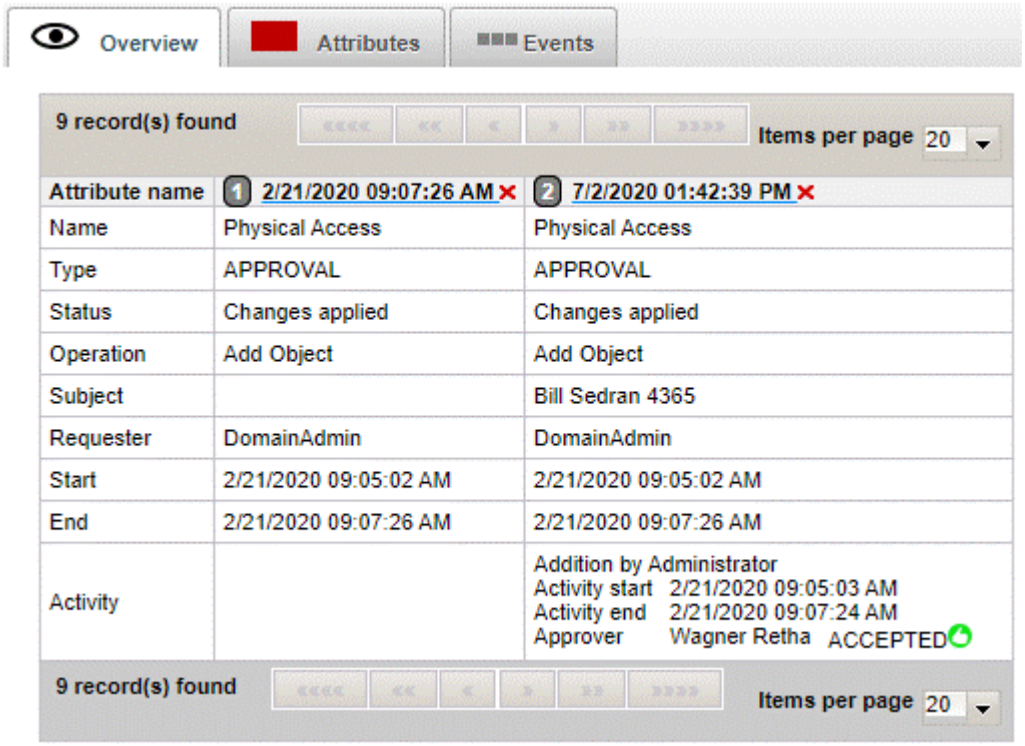


Figure 37. History View Details - Workflow Instance Overview Tab

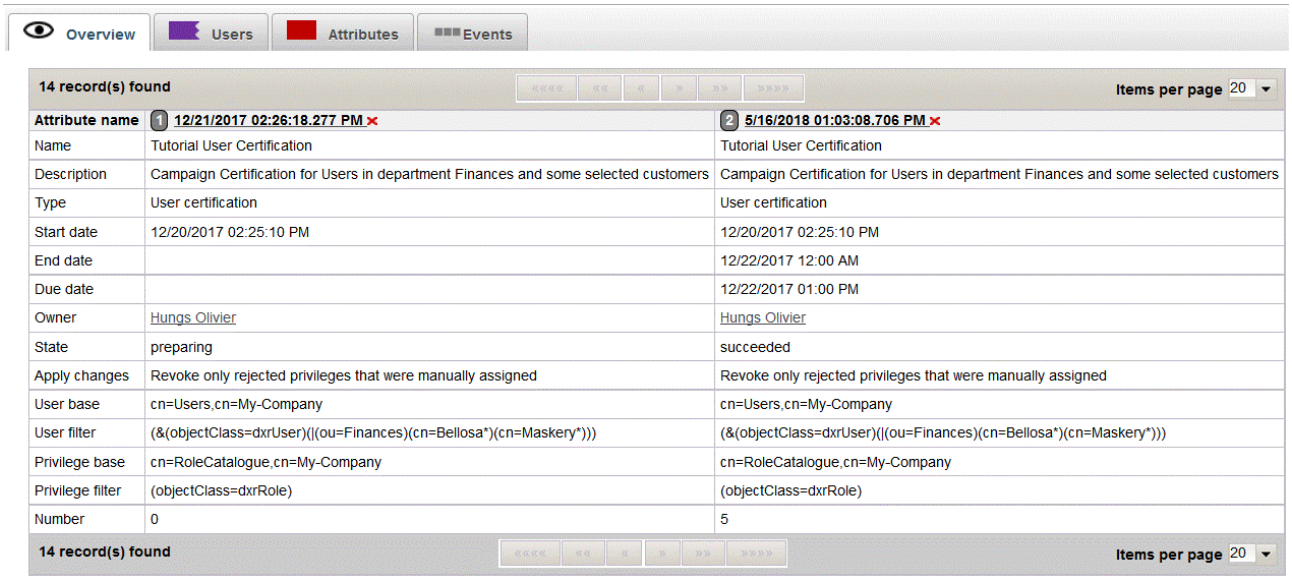


Figure 38. History View Details - Certification Campaign Overview Tab

6.3. Exporting History Entries

To export the history entries presented in a search result table to a report-formatted file, click **Report** in the filter definition area. The DirX Audit Manager displays a dialog that allows you to set the output format for the file as follows:

- **Template** - selects the report template to be used for the file.
- **Format** - selects the file format to be used; for example, PDF, CSV, Microsoft Word formats (DOCX, RTF), and so on.
- **Encoding** - selects the type of character encoding to be used; for example, UTF-8, Big5, EUC-JP, and so on.
- **Rows** - the number of rows presented in a search result table used for exported report. For value **0** all history entry data presented in a search result table are exported.

Click **Export** to continue the export procedure or click **Cancel** to dismiss it.

When you click **Export**, the Internet browser running the DirX Audit Manager may display a dialog that prompts you to open the report file, save it, or cancel the operation.

7. Using the DirX Audit Tools

DirX Audit provides the following database maintenance tools:

- A tool to maintain a database containing audit messages and history entries (DB maintenance)
- A tool to populate fact tables

The DB maintenance tool has the following modes:

- Export: Exports audit messages from the DirX Audit Data Database to XML files and exports history entries data from the DirX Audit History Database to JSON files. The audit messages can either be deleted or kept in the DirX Audit Data Database after export. The history entries data that was ended can either be deleted or kept in the DirX Audit History Database after export.
- Import: Imports audit messages from XML files to the DirX Audit Data Database. The XML files can be either deleted or kept in the file system after import.
- Extend: Extends audit messages in the DirX Audit Data Database with audit events and dimensions.
- Compress: Compresses original messages in the DirX Audit Data Database.
- Purge: Purges audit messages data and history entries data from the DirX Audit Database.
- Remove duplicate: Removes duplicate history entries with the same dirxEntryUUID or DN or duplicate history entries linked to the same logical entry.
- Compute context: computes missing contexts for audit events within the specified time interval.

The following sections provide information about these tools.

7.1. General Information

This section provides information common to all the DirX Audit tools, including:

- Usage prerequisites
- Installation location
- Common syntax and options

7.1.1. Usage Prerequisites

The DirX Audit tools have the following prerequisites:

- A command shell (the Windows command prompt or a UNIX shell) must be available to run the tools.
- The Java Virtual Machine (JVM) must be set up correctly. You must use the same JVM version that the other DirX Audit components use. If the tool is installed from the DirX Audit installer, the correct JVM will be used automatically. When the tool is installed from a standalone package, you must set the system path to contain the **bin** folder of the JVM and set the **JAVA_HOME** system environment variable to point to the JVM folder.

7.1.2. Installation Location

The DirX Audit tools are located in sub-folders of the folder:

*install_path***/tools/***tool_identifier*

where

tool_identifier corresponds to the tool as follows:
db_maintenance indicates the DB maintenance tool.
db_fact_population indicates the fact population tool.

The sub-folder **bin** contains the binary of the tool.

The names of the binaries are:

- For the DB maintenance tool:
  dxtdbtool.bat on Windows and **dxtdbtool.sh** on UNIX. It is referred to as **dxtdbtool** for the rest of this chapter.
  dxthistdbtool.bat on Windows and **dxthistdbtool.sh** on UNIX. It is referred to as **dxthistdbtool** for the rest of this chapter.
- For the fact population tool:
  dxtPopulateFacts.bat on Windows and **dxtPopulateFacts.sh** on Unix. It is referred as **dxtPopulateFacts** for the rest of this chapter.

7.1.3. Common Syntax

The general usage of the tools is:

tool_name command [*options*]

where

tool_name
is either **dxtdbtool** or **dxthistdbtool** for the DB maintenance tool or **dxtPopulateFacts** for the fact population tool.

command
is one of the following keywords:

- **export** or **import** or **extend** or **compress** or **purge** for **dxtdbtool**
- **purge** or **export** or **remdup** for **dxthistdbtool**
- no command for **dxtPopulateFacts**

options
is a list of common and command specific options. (See the following sections for details.)

If a value contains a SPACE character enclose the value in double quotes (**"**).

You can always run the utility without any argument (not **dxtPopulateFacts**) to get the usage help information and examples.

7.1.4. Common Options

All DirX Audit tools recognize the following options:

-debug
Creates a debug log.

-debugMemory
Displays more detailed memory allocation information.

-silent
Suppresses the user confirmation dialog for performing a given action. By default, you must confirm (by entering **yes**) that you really want to perform an action. This option allows you to bypass the confirmation dialog.

-simulate
Shows the results of an action without actually performing the action.

-tenantid *tenantID*
Specifies the tenant whose configuration file is accessed to acquire database credentials. The *tenantID* specifies the identifier of a configured tenant.

-transize *tranSize*
Specifies the transaction size used during an operation. A larger size will increase performance, but will require larger transaction log files.

-types *type*[**,***type*]...
Specifies a list of comma-separated history entry types to which the operation is restricted. All types are used, if none is specified.

The tenant ID is used to obtain the database credentials of the specific tenant. The credentials are acquired from the tenant configuration file, properly configured by the Configuration Wizard. If only one tenant is configured, the **-tenantid** option can be omitted from the command line and the configuration file of this tenant is used automatically. If more than one tenant is configured, the **-tenantid** option needs to be specified on the command line.

7.1.5. LDAP Connection Parameters

Some DirX Audit tools require the following LDAP connection parameters:

-ldapbase *ldapBase*
LDAP node used as a search base.

-ldapconfig *ldapConfigFile*
LDAP connection properties file. It contains all mentioned required LDAP parameters. You can find the **ldap.properties** file example in the *install_path***/tools/db_maintenance/doc/samples**.

-ldapdomain *ldapDomain*
LDAP domain DN. It will be prepended before the *ldapBase* node.

-ldapfilter *ldapFilter*
Search filter applied to the LDAP search.

-ldaphost *ldapHost*
LDAP host used to establish an LDAP connection.

-ldappassword *ldapPassword*
LDAP connection password.

-ldapport *ldapPort*
Port on which the LDAP connection will be established.

-ldapscope *ldapScope*
Scope of the LDAP search.

-ldapuser *ldapUser*
LDAP user used to establish an LDAP connection.

7.2. Maintaining Audit Messages

This section describes how to use the DB maintenance tool to maintain DirX Audit messages.

7.2.1. Export Audit Trail

To export audit messages from the DirX Audit Data Database to XML files, execute the following command:

dxtdbtool export *common_options*
-dstdir *folder_name*
[**-delete**]
[**-from** *date_time | function*]
[**-recsperfile** *number*]
[**-recsperquery** *number*]
[**-to** *date_time | function*]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-dstdir *folder_name*
Specifies the destination folder for the XML files containing the exported audit messages.

-delete
Specifies that the audit messages are to be deleted from the DirX Audit Data Database after export.

-from *date_time | function*
Specifies that only audit messages created after the specified date and time (inclusive) or by the specified function are exported.

-recsperfile *number*
Specifies the maximum number of audit messages to be written to the XML files.
The default value is **500**.

-recsperquery *number*
Specifies the maximum number of audit messages per database query. The value can affect command processing on the database-server side. A low value can increase the total processing time because of frequent network communication and more actions to be processed. On the other hand, a high value can require more database server resources and command processing can fail when these resources are not sufficient.
The default value is **500**. Decrease this number if the export fails.

-to *date_time | function*
Specifies that only audit messages created up to the specified date and time (exclusive) or by the specified function are exported.

The format for the value of *date_time* is *yyyy.MM.dd_HH.mm.ss_z* . See the Java documentation for the SimpleDateFormat class for details and examples.

You can use the following functions in **-from** and **-to** options:

- Beginning functions (which return the beginning of a unit): **$bhour(***parameter***)**, **$bday(***parameter***)**, **$bweek(***parameter***)**, **$bmonth(***parameter***)**, **$byear(***parameter***)**
- End functions (which return the end of a unit): **$ehour(***parameter***)**, **$eday(***parameter***)**, **$eweek(***parameter***)**, **$emonth(***parameter***)**, **$eyear(***parameter***)**
- Other: **$now()**

The *parameter* argument is a required integer value, where:

- Zero (0) represents the current moment. For example, **$bday(0)** returns the beginning of this day.
- A negative number represents a moment before the current date and time value. For example, **$emonth(-1)** returns the end of the previous month.
- A positive number represents a moment after the current date and time value. For example, **$byear(3)** returns the beginning of a year in three years.

Note that audit messages usually use UTC zone in the audit message **Identification - When** field.

If the **-delete** option has been specified and an error occurs during export or the tool is interrupted, it can resume work: simply re-run the tool with exactly the same arguments.

7.2.1.1. Exported Message Structure and Format

The exported audit messages are stored in the file system as XML files. The files that contain exported messages are compressed. The audit messages are split into separate files using the audit message event date and given options according to the following rules:

- A new folder structure *yyyy/MM* is created in the destination folder (option **-dstdir**) for each file set if it does not exist yet; for example: the folder **2010/01** will contain messages from January 2010.
- The **-recsperfile** option specifies the maximum number of audit messages in a file.
- One file contains audit messages from one day. (The audit message **Identification - When** field is used.)

The file containing exported audit messages has the following name and path:

*yyyy/MM***/dxtdata_***yyyyMMdd_HHmm-HHmm***_tot***records_count_index***.xml.zip**

Here is an example: `2001/12/dxtdata_20011217_0930-0930_tot1_0.xml.zip`

An additional file with the same base name and suffix **.info.xml** is created for each exported messages file. This file contains information about the exported messages.

7.2.1.2. Export Examples

In the following example, all messages from January 2009 are exported. The export process deletes the exported messages from the DirX Audit Data Database. It stores the data into the folder **./data/audit_export/**. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**. Please make sure that you use the "simple plain hyphen" **-** in the command line.

```
dxtdbtool export -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -dstdir
./data/audit_export -from 2009.01.01_00.00.00_UTC -to
2009.02.01_00.00.00_UTC -delete
```

In the following example, all messages from January 2009 are exported. The export process deletes the exported messages from the DirX Audit Data Database. It stores the data into the folder **./data/audit_export/**. The connection data are stored in the configuration file of the only configured tenant:

```
dxtdbtool export -dstdir ./data/audit_export -from 2009.01.01_00.00.00_UTC
-to 2009.02.01_00.00.00_UTC -delete
```

In the following example, all messages older than 12 months are exported. The export process deletes the exported messages from the DirX Audit Data Database. It stores the data in the folder **./data/audit_export/**. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxtdbtool export -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -dstdir
./data/audit_export -to $bday(-365) -delete
```

In the next example, all messages are exported. The export process does not delete the exported messages from the DirX Audit Data Database. It stores the data in the folder **./data/audit_export**. The database connection data are taken from the stored configuration file of the only configured tenant (set in the Configuration Wizard). The export operation starts immediately (because the **-silent** option is used; see the section "Common Options" for details):

```
dxtdbtool export -dstdir ./data/audit_export -silent
```

7.2.2. Import Audit Trail

To import audit messages from XML files to the DirX Audit Data Database, execute the following command:

dxtdbtool import *common_options*
-src *path*
[**-delete** | **-dstdir** *folder_name*]
[**-recursive**]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-src *path*
Specifies the source file or folder. You can also use a folder containing data previously exported with **dxtdbtool export** saved as **dxtdata_***xxx***.xml.zip**.

-delete
Specifies that the XML files are deleted after import.

-dstdir *folder_name*
Specifies the destination folder to which the XML files are moved after import.

-recursive
Specifies that the XML files in all sub-folders are imported.

The options **-delete** and **-dstdir** are mutually exclusive. You can specify only one of them. After a successful import, the source file is either deleted from the file system (if **-delete** was specified) or moved from the source folder into destination folder (if **-dstdir** was specified).

The option **-src** can be either a path to a file or a folder. If it is a folder, only the files in this folder are processed unless the **-recursive** option was specified (all sub-folders and files are processed in this case).

The import operation expects the files to be in the same format and syntax as generated by the export operation; that is, in the form of archive files.

If an error occurs during the import process or the tool is interrupted, it can resume the import: simply re-run the tool with exactly the same arguments.

You can also use the DirX Audit file collector component of the DirX Audit Server to import the messages from the XML files into the DirX Audit Data Database. However, you must unzip all audit message files before you copy them into the collector's input folder. Do not copy the information files there. Only the audit message files should be copied to this folder. See the section "Server File Collector for DirX Audit Format" in the *DirX Audit Installation Guide* for the configuration details.

7.2.2.1. Import Examples

In the following example, the audit messages are imported from the folder **./data/audit** to the DirX Audit Data Database. All connection settings are taken from the stored tenant configuration file. After import, the files are moved to the **./data/audit/archive**. Please make sure that you use the "simple plain hyphen" **-** in the command line.

```
dxtdbtool import -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -src
./data/audit -dstdir ./data/audit/archive -recursive
```

In the next example, the audit messages are imported from the folder **./data/audit** to the DirX Audit Data Database. The connection data are stored in the configuration file of the only configured tenant. After import, the files are deleted:

```
dxtdbtool import -src ./data/audit -delete -recursive
```

In the next example, the audit messages from the file/archive **./data/audit/file.xml.zip** are imported to the DirX Audit Data Database. The connection settings are taken from the stored configuration file of the only configured tenant. After import, the file is moved to the folder **./data/audit_backup**:

```
dxtdbtool import -src ./data/audit/file.xml.zip -dstdir ./data/audit_backup
```

7.2.3. Extend Audit Messages

To extend audit messages in the DirX Audit Data Database with audit events and dimensions, execute the following command:

dxtdbtool extend *common_options*
[**-from** *date_time*]
[**-recsperquery** *number*]
[**-to** *date_time*]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-from *date_time*
Specifies that only audit messages created after the specified date and time (inclusive) are extended.

-recsperquery *number*
Specifies the maximum number of audit messages per database query. The value can affect command processing on the database-server side. A low value can increase the total processing time because of frequent network communication and more actions to be processed. On the other hand, a high value can require more database server resources and command processing can fail when these resources are not sufficient. The default value is **500**. Decrease this number if the command fails.

-to *date_time*
Specifies that only audit messages created up to the specified date and time (exclusive) are extended.

The format for the value of *date_time* is *yyyy.MM.dd_HH.mm.ss_***z**. See the Java documentation for the SimpleDateFormat class for details and examples.

Note that audit messages usually use UTC zone in the audit message **Identification - When** field.

Extending audit messages is not usually necessary, especially if you use the import tool. It is only necessary in specific cases and is then indicated in the appropriate places; in the *DirX Audit Release Notes*, for example.

7.2.3.1. Extend Examples

In the following example, all messages are extended. The connection data are stored in the configuration file of the tenant with the ID **4f753e1d-d0de-4aef-bb22-caace7342e99**. Make sure that you use the "simple plain hyphen" **-** in the command line.

```
dxtdbtool extend -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
```

In the next example, all messages from January 2019 are extended. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxtdbtool extend -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -from
2019.01.01_00.00.00_UTC -to 2019.02.01_00.00.00_UTC
```

In the next example, all messages are extended. The connection data are stored in the configuration file of the only configured tenant:

```
dxtdbtool extend
```

7.2.4. Compress Original Message

Original messages can be optionally stored together with audit messages. In DirX Audit 7.0 SP1 and earlier versions, they were saved as text. As of DirX Audit 7.1, they can be saved in a compressed form, which can significantly reduce the database size.

The original message in the text form is saved in the ORIGINALMESSAGE column of the DAT_ORIGINALMESSAGES table. The original message in the compressed form is saved in the ORIGINALMESSAGE_COMPRESS column of the same table.

The command compresses the original message text data and stores it in the compressed form. It removes the text data from the table. When the command is completed, the table's clustered index is rebuilt. Data space should be significantly reduced. The table size should be reduced to about 20 % of its previous size.

To compress original messages in the DirX Audit Data Database, execute the following command:

dxtdbtool compress *common_options*
[**-from** *date_time*]
[**-recsperquery** *number*]
[**-to** *date_time*]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-from *date_time*
Specifies that only audit messages created after the specified date and time (inclusive) are compressed.

-recsperquery *number*
Specifies the maximum number of audit messages per database query. The value can affect command processing on the database-server side. A low value can increase the total processing time because of frequent network communication and more actions to be processed. On the other hand, a high value can require more database server resources and command processing can fail when these resources are not sufficient. The default value is **500**. Decrease this number if the command fails.

-to *date_time*
Specifies that only audit messages created up to the specified date and time (exclusive) are compressed.

The format for the value of *date_time* is *yyyy.MM.dd_HH.mm.ss_***z**. See the Java documentation for the SimpleDateFormat class for details and examples.

Note that audit messages usually use UTC zone in the audit message **Identification - When** field.

7.2.4.1. Compress Examples

In the following example, all original messages are compressed. The connection data are stored in the configuration file of the tenant with the ID **4f753e1d-d0de-4aef-bb22-caace7342e99**. Make sure that you use the "simple plain hyphen" **-** in the command line.

```
dxtdbtool compress -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
```

In the next example, all messages from January 2019 are compressed. The connection data are stored in the configuration file of the tenant with the ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxtdbtool compress -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -from
2019.01.01_00.00.00_UTC -to 2019.02.01_00.00.00_UTC
```

In the next example, all messages are compressed. The connection data are stored in the configuration file of the only configured tenant:

```
dxtdbtool compress
```

7.2.5. Purge Audit Messages Data

To purge audit messages data from the DirX Audit Data Database, execute the following command:

dxtdbtool purge *common_options*
-scope {**DAT_AUDITMESSAGES** | **DAT_AUDITMESSAGES_ADDITIONS** | **DAT_ORIGINALMESSAGES**}
-filter *file_path*
[**-paramsfile** *file_path*]
[**-params** *key*[**.DATETIME]=***value*[,*key*[**.DATETIME]=***value*]...]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-scope {**DAT_AUDITMESSAGES** | **DAT_AUDITMESSAGE_ADDITIONS** | **DAT_ORIGINALMESSAGES**}
Specifies the scope of the audit message data to be purged with a table name:

- **DAT_AUDITMESSAGES** deletes complete audit messages including message additions and original messages.
- **DAT_AUDITMESSAGE_ADDITIONS** deletes only message additions and original messages, but it keeps **DAT_AUDITMESSAGES** content.
- **DAT_ORIGINALMESSAGES** deletes only original messages.

-filter *file_path*
Specifies a path to the file containing a SQL select statement that provides a list of primary keys of the scope database object to be purged.
This can be a **DAT_AUDITMESSAGES** or a **DAT_AUDITMESSAGE_ADDITIONS** or a **DAT_ORIGINALMESSAGES** table.
The select statement can contain several parameters in the format **${***key***}**.
These parameters are replaced at execution time with the provided values.

-paramsfile *file_path*
Specifies a path to the file containing a list of SQL select statement parameters and their values in the format *key***=***value* for common types and *key***.DATETIME=***value* for the date and time type. The **-paramsfile** parameter can be omitted when no SQL select statement parameter is used or when only inline parameters are provided. When a parameter key is used both in the file and inline, the inline value takes precedence.

-params *key*[**.DATETIME]=***value*[,*key*[**.DATETIME]=***value*]...
Represents a set of SQL select statement parameter key – value pairs. Optionally, the parameter can be of date and time data type.

The format for the value of *date_time* is **yyyy.MM.dd_HH.mm.ss_z**. See the Java documentation for the SimpleDateFormat class for details and examples.

You can use the same functions as described in the section“Export Audit Trail” to specify values of date and time parameters (dateparam).

Note that audit messages usually use UTC zone in the audit message **Identification - When** field.

7.2.5.1. Purge Audit Data Examples

In the following example, original messages are removed. The connection data are stored in the configuration file of the tenant with the ID **4f753e1d-d0de-4aef-bb22-caace7342e99**. Make sure that you use the "simple plain hyphen" **-** in the command line.

```
dxtdbtool purge
-tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-scope DAT_ORIGINALMESSAGES
-filter om.sql
-params “IDENTIFICATION_SOURCE=DirX Identity”,
IDENTIFICATION_OUTCOME=0,
WHEN_FROM.DATETIME=$bmonth(-6),
WHEN_TO.DATETIME=$bmonth(-5)
```

The same result can be achieved with a parameter file:

```
dxtdbtool purge
-tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-scope DAT_ORIGINALMESSAGES
-filter om.sql
-paramsfile om_params.properties
```

The content of the **om.sql** file can look like this:

```
select
DAT_ORIGINALMESSAGES.DAT_ORIGINALMESSAGES_ID
from
DAT_AUDITMESSAGES
join DAT_AUDITMESSAGE_ADDITIONS on
 DAT_AUDITMESSAGE_ADDITIONS.DAT_AUDITMESSAGES_ID =
  DAT_AUDITMESSAGES.DAT_AUDITMESSAGES_ID
join DAT_ORIGINALMESSAGES on
 DAT_ORIGINALMESSAGES.DAT_AUDITMESSAGE_ADDITIONS_ID =
  DAT_AUDITMESSAGE_ADDITIONS.DAT_AUDITMESSAGE_ADDITIONS_ID
where
DAT_AUDITMESSAGES.IDENTIFICATION_SOURCE =
 '${IDENTIFICATION_SOURCE}'
 and DAT_AUDITMESSAGES.IDENTIFICATION_OUTCOME =
 ${IDENTIFICATION_OUTCOME}
 and DAT_AUDITMESSAGES.IDENTIFICATION_WHEN >= ${WHEN_FROM}
 and DAT_AUDITMESSAGES.IDENTIFICATION_WHEN < ${WHEN_TO}
```

And the content of the **om_params.properties** file can look like this:

```
IDENTIFICATION_SOURCE=DirX Identity
IDENTIFICATION_OUTCOME=0
WHEN_FROM.DATETIME=$bmonth(-6)
WHEN_TO.DATETIME=$bmonth(-5)
```

7.2.6. Compute Audit Event Context

These options allows computing missing audit events context data independently from the similar server job.

To generate missing audit events context in the DirX Audit Data Database, execute the following command:

dxtdbtool computeContext *common_options*
[**-from** *date_time*]
[**-to** *date_time*]

7.2.6.1. Compute Audit Event Context Examples

In the following example, missing context records will be generated for events from January 2009 till March 2009:

```
dxtdbtool computeContext -from 2009.01.01_00.00.00_UTC -to
2009.04.01_00.00.00_UTC
```

7.3. Maintaining History Entries

This section describes how to use the DB maintenance tool to maintain history entries.

7.3.1. Purge History Entries Data

The DB maintenance tool can delete history entries data from the DirX Audit History Database that have already ended. Specifically, it can remove rows of the following tables according to their VALID_TO column value:

- HST_ENTRIES_IN_TIME
- HST_SMALL_ATTRS_IN_TIME
- HST_LINK_ATTRS_IN_TIME
- HST_LARGE_ATTRS_IN_TIME
- HST_ASSIGNMENTS_IN_TIME
- HST_ROLEPARAMS_IN_TIME
- HDB_SMALL_DATTRS_IN_TIME
- HDB_LINK_DATTRS_IN_TIME
- HDB_MANUAL_ASSIGNMENTS

To purge history entries data from the DirX Audit History Database, execute the following command:

dxthistdbtool purge *common_options*
-endedbefore *date_time* | *function*]
[**-endedafter** *date_time* | *function*]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-endedbefore *date_time* | *function*
Specifies that only history entries data ended before the specified date and time (exclusive) or by the specified function are deleted.

-endedafter *date_time* | *function*
Specifies that only history entries data ended after the specified date and time (inclusive) or by the specified function are deleted.

The format for the value of *date_time* is *yyyy.MM.dd_HH.mm.ss_z*. See the Java documentation for the SimpleDateFormat class for details and examples.

You can use any of the functions described in the section "Export Audit Trail" in the **-from** and **-to** options.

7.3.1.1. Purge History Data Examples

In the following example, all history entries data ended in January 2019 are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**. Make sure that you use the “simple plain hyphen” **-** in the command line.

```
dxthistdbtool purge -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-endedafter 2019.01.01_00.00.00_UTC -endedbefore 2019.02.01_00.00.00_UTC
```

In the next example, all history entries data ended in January 2019 are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the only configured tenant:

```
dxthistdbtool purge -endedafter 2019.01.01_00.00.00_UTC -endedbefore
2019.02.01_00.00.00_UTC
```

In the next example, all history entries data ended before 6 months (end of months) are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purge -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-endedbefore $bmonth(-5)
```

In this example, all history entries data ended before the end of the last year are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purge -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-endedbefore $byear()
```

In the next example, all history entries data ended during the previous month are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purge -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-endedafter $bmonth(-1) -endedbefore $bmonth()
```

In the next example, all history entries data ended before today are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the tenant with **ID 4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purge -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-endedbefore $bday()
```

In the last example, all ended history entries data are deleted. The purge process deletes the history entries data from the DirX Audit History Database. The connection data are stored in the configuration file of the only configured tenant. The purge process starts immediately because the **-silent** option is used; see the section "Common Options" for details:

```
dxthistdbtool purge -silent
```

7.3.2. Purge Orphaned History Entries

Purging history entries data using the **purge** tool can leave so-called “orphaned” entries. Orphaned entries are entries that have no corresponding attributes. Purging those orphans can be performed by executing the following command:

dxthistdbtool purgeorphans *common_options*
[**-forcedelete]**

where

common_options
Specifies the common options. See the section "Common Options" for details.

-forcedelete In case of data inconsistencies in the database, some orphaned entries can have lingering attributes which fail the purge. This flag forces the deletion of orphaned entries together with any would-be lingering attributes.

7.3.2.1. Purge Orphaned History Entries Examples

In the following example, all orphaned history entries are purged from the database. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purgeorphans -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
```

In the next example, all orphaned history entries are purged from the database. In case of any lingering attributes linked to the orphans cause by database inconsistencies, the orphans are purged along with the lingering attributes. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purgeorphans -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-forcedelete
```

7.3.3. Purge Ended History Entries

Another approach to purging history entries is by purging ended entries. Ended entries are identified as entries, that have no valid attributes. As opposed to the **purge** tool, which only purged the ended attributes of entries, this approach purges the entire entries along with their attributes. Purging ended entries can be performed by executing the following command:

dxthistdbtool purgeended *common_options*
-endedbefore *date_time | function*

where

common_options
Specifies the common options. See the section "Common Options" for details.

-endedbefore *date_time | function*
Purge ended history entries whose validity ended before this date and time (exclusive).

7.3.3.1. Purge Ended History Entries Examples

In the following example, all ended history entries are purged from the database. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purgeended -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
```

In the next example, all ended history entries, whose last validity ended before the specified date and time. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool purgeended -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-endedbefore $bmonth(-1)
```

7.3.4. Export History Entries

To export history entries data from the DirX Audit History Database to JSON files, execute the following command:

dxthistdbtool export *common_options*
-dstdir *folder_name*
[**-delete**]
[**-includestarted**]
[**-endedafter** *date_time* | *function*]
[**-endedbefore** *date_time* | *function*]
[**-entsperfile** *number*]
[**-nouidlist**]
[**-noorphans**]
[**-keepentries**]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-dstdir *folder_name*
Specifies the destination folder for the JSON files containing the exported history entries data.

-delete
Specifies that the history entries data that were ended in given date-time range are to be purged from the DirX Audit History Database after export. A date and time range must be defined at least by the -**endedbefore** option. The default is not to delete history entries data. Started entries and attributes that have not ended are not affected.

-includestarted
Includes history entries data that were started in the given date and time range into the export process. The default exports only ended history entries data in the given date and time range.

-endedafter *date_time* | *function*
Exports only those history entries data ended after the specified date and time (inclusive) or by the specified function.

-endedbefore *date_time* | *function*
Exports only those history entries data ended up to the specified date and time (exclusive) or by the specified function.

-entsperfile *number*
Specifies the maximum number of history entries represented by JSON files to be written to the ZIP files. The default value is 500.

-nouidlist
Specifies that lists of entries identifiers will not be created. The default is to create such a list for every type folder.

-noorphans
Specifies that assignments without references to link attributes will not be exported. The default is to export such assignments into a separate folder.

-keepentries
Specifies that history entries will be kept even if they do not have any existing entries in time. The default is to delete such entries. This option only affects the **-delete** option.

The format for the value of *date_time* is *yyyy.MM.dd_HH.mm.ss_z*. See the Java documentation for the SimpleDateFormat class for details and examples.

7.3.4.1. Exported Entries Structure and Format

The exported history entries data are stored in the file system as JSON files. These files are compressed by the number specified in the **-entsperfile** option. The folder structure is as follows:

- A new folder structure **dxthistory_***yyyyMMddHHmmss/type* is created in the destination folder (option **-dstdir**) for each exported entry type; for example, the folder **`dxthistory_20220911093110/Account`** will contain all history entries data according to the given date and time range. Date and time in the name of top folder is the timestamp of the time at which the export started.
- The **-entsperfile** option specifies the maximum number of history entries in ZIP file.

The file containing exported history entries data has the following name and path structure:

dxthistory_*yyyyMMddHHmmss/type/type_count_range***.zip**

Here is an example:

```
dxthistory_20220911093110/Account/Account_000000001_000000500.zip
```

Each type folder contains a **dxruid_list.txt** file, which contains a list of entries identifiers for a specific type.

The additional files **export_info.txt**, **domain.properties**, **parameters.properties**, **export_result_success** or **export_result_error** are created in the folder **dxthistory_***yyyyMMddHHmmss*. When the **-delete** option is used, additional files such as **purge_info.txt**, **purge_result_success** or **purge_result_error** are also created. The **info** file contains information about the amount of exported/purged data and the operation's duration. After the export is finished, the common **result_success** or **result_error** is created.

7.3.4.2. History Export Examples

In the following example, all history entries data that ended in January 2009 are exported. The export process purges exported history entries data from the DirX Audit History Database. It stores the data into the folder **./data/history_export/**. The connection data are stored in the configuration file of the tenant with **ID 4f753e1d-d0de-4aef-bb22-caace7342e99**. Please make sure that you use the "simple plain hyphen" - in the command line.

```
dxthistdbtool export -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -dstdir
./data/history_export -endedafter 2009.01.01_00.00.00_UTC -endedbefore
2009.02.01_00.00.00_UTC -delete
```

In the next example, all history entries data that ended in January 2009 are exported. The export process purges exported history entries data from the DirX Audit History Database. It stores the data into the folder **./data/history_export/**. The connection data are stored in the configuration file of the only configured tenant:

```
dxthistdbtool export -dstdir ./data/history_export -endedafter
2009.01.01_00.00.00_UTC -endedbefore 2009.02.01_00.00.00_UTC -delete
```

In this example, all history entries data that ended previous month are exported. The export process purges exported history entries data from the DirX Audit History Database. It stores the data into the folder **./data/history_export/**. The connection data are stored in the configuration file of the only configured tenant:

```
dxthistdbtool export -dstdir ./data/history_export -endedafter $bmonth(-1)
-endedbefore $bmonth() -delete
```

In the following example, all history entries data that started or ended up to now are exported. It stores the data into the folder **./data/history_export/**. The connection data are stored in the configuration file of the only configured tenant:

```
dxthistdbtool export -dstdir ./data/history_export -includestarted
```

In the next example, Account and User history entries data that ended up to one year ago are exported. The export process purges the exported history entries data from the DirX Audit History Database. It stores the data in the folder **./data/history_export/**. The connection data are stored in the configuration file of the tenant with ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:

```
dxthistdbtool export -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -dstdir
./data/history_export -endedbefore $bday(-365) -types “Account,User” -delete
```

In the last example, all history entries data that have started or ended up to now are exported. The export process does not purge the exported history entries data from the DirX Audit History Database. It stores the data in the folder **./data/history_export/**. The database connection data are taken from the stored configuration file of the only configured tenant (set in the Configuration Wizard). The export operation starts immediately (because the **-silent** option is used; see the section "Common Options" for details):

```
dxthistdbtool export -dstdir ./data/history_export -includestarted -silent
```

7.3.5. Remove Duplicate History Entries

To remove duplicate history entries data from the DirX Audit History Database, execute the following command:

dxthistdbtool remdup *common_options*
-searchby {**ENTRY** | **DIRX_ENTRY_UUID** | **DN**}

where

common_options
Specifies the common options. See the section "Common Options" for details.

-searchby {**ENTRY** | **DIRX_ENTRY_UUID** | **DN**}
Specifies whether the duplicate entries should be identified by entry, dirxEntryUUID (default) or DN:

- **ENTRY** - Finds logical entries with multiple current history entries and ends all HST_ENTRIES_IN_TIME records associated to the same logical entry except the last created one.
- **DIRX_ENTRY_UUID** - Finds history entries with duplicate dirxEntryUUID values and ends the associated HST_ENTRIES_IN_TIME records except the last created one.
- **DN** - Finds history entries with multiple HST_ENTRIES_IN_TIME records that are not ended and ends all records associated to each entry except the last created one.

7.3.5.1. Remove Duplicate History Entries Examples

In this example, the tool finds all history entries linked to the same logical entry and ends all associated history entry records except the last one created of the only configured tenant.

```
dxthistdbtool remdup -searchby ENTRY
```

In the next example, the tool finds all history entries with duplicate dirxEntryUUID values and ends associated history entry records except the last one created. The connection data are stored in the configuration file of the tenant with ID **fb7b2fc2-a7e2-4d9b-aea9-c002426d74c0**.

```
dxthistdbtool remdup -tenantid fb7b2fc2-a7e2-4d9b-aea9-c002426d74c0
-searchby DIRX_ENTRY_UUID
```

In this example, the tool finds all history entries with multiple records having the identical DN value that are not ended and ends all records associated to each entry except the last one created of the only configured tenant.

```
dxthistdbtool remdup -searchby DN
```

7.3.6. Remove Duplicate LDAP Entries

To remove entries with duplicate dirxEntryUUID attributes from LDAP, and optionally synchronize the changes made in LDAP to the DirX Audit History Database, execute the following command:

dxthistdbtool ldapremdup *common_options ldap_parameters*
[**-filluuid**]
[**-showonly**]
[**-synctohistdb**]

where

common_options
Specifies the common options. See the section "Common Options" for details.

ldap_parameters
Specifies LDAP connection parameters. See the section "LDAP Connection Parameters" for details.

-filluuid
If entries with missing dirxEntryUUID attribute are found, they will have new values generated. By default, they are ignored.

-showonly
Only shows the empty or duplicated values for dirxEntryUUID attribute and DN values of corresponding entries.

-synctohistdb
Synchronize the changes made in LDAP to DirX Audit History Database. Therefore, if a duplicate dirxEntryUUID is changed in LDAP, the same action occurs in the DirX Audit History Database if the corresponding entry exists. Entries in LDAP and DirX Audit History Database are determined to be corresponding if they match either on dirxEntryUUID/DN or dirxEntryUUID/dxrUID value pairs.

7.3.6.1. Remove Duplicate LDAP Entries Examples

In this example, entries with duplicate dirxEntryUUID values are retrieved from LDAP. Duplicate dirxEntryUUIDs have new values generated in LDAP. Entries with missing dirxEntryUUID values are skipped. This is the default behavior when no options are selected.

```
dxthistdbtool ldapremdup -ldapconfig ldap.properties
```

In this example, the tool searches LDAP for entries with duplicate or missing dirxEntryUUID values and prints them out. No modifications are made.

```
dxthistdbtool ldapremdup -ldapconfig ldap.properties -showonly
```

In the next example, the behavior in LDAP stays the same as in the default case (the first example); however, the changes made in LDAP are synchronized to the DirX Audit History Database for any matching entries.

```
dxthistdbtool ldapremdup -ldapconfig ldap.properties -synctohistdb
```

In the following example, the tool searches for and solves duplicated dirxEntryUUIDs and searches for missing dirxEntryUUIDs. If LDAP entries with missing dirxEntryUUID values are found, a new dirxEntryUUID value is generated for them in LDAP.

```
dxthistdbtool ldapremdup -ldapconfig ldap.properties -filluuid
```

7.3.7. Fill Missing dirxEntryUUID Values of History Entries

To generate new unique values for missing dirxEntryUUID attributes of history entries in DirX Audit History Database, execute the following command. No modifications are made in LDAP.

dxthistdbtool filluuid *common_options ldap_parameters*

where

common_options
Specifies the common options. See the section "Common Options" for details.

ldap_parameters
Specifies LDAP connection parameters. See the section "LDAP Connection Parameters" for details. If an entry with a missing dirxEntryUUID value is found in the DirX Audit History Database, the tool searches LDAP for a matching entry and if possible, uses this dirxEntryUUID value in DirX Audit History Database.

7.3.7.1. Fill Missing dirxEntryUUID Values of History Entries Examples

In this example, the tool looks for entries with missing dirxEntryUUID values in the DirX Audit History Database (either NULL or an empty string). For every entry with a missing value, the tool searches LDAP for a matching entry and if possible, uses its dirxEntryUUID value. If no matching entry is found, a new unique value is generated with a special prefix in the DirX Audit History Database (No modifications are made in LDAP).

```
dxthistdbtool filluuid -ldapconfig ldap.properties
```

7.3.8. Make History Entries Unique

To ensure unique history entries in DirX Audit History Database (with unique and non-missing dirxEntryUUID values), execute the following command:

dxthistdbtool makeunique *common_options ldap_parameters*
[**-purge**]
[**-csvfile** *csvFile*]

where

common_options
Specifies the common options. See the section "Common Options" for details.

ldap_parameters
Specifies LDAP connection parameters. See the section "LDAP Connection Parameters" for details.

-purge
Resolve exact duplicates (same on all attributes) by purging all extra entries. For example in case of three exact duplicates, two will be purged from the DirX Audit History Database, and only one will remain (the one with the smallest ENTRY_ID will usually remain).

-csvfile *csvFile*
Output digests (summaries) of duplicate entries found in the DirX Audit History Database. This parameter can be used in combination with the **-simulate** option to check what entries would be modified without actually making changes in the DirX Audit History Database.

7.3.8.1. Make History Entries Unique Examples

In this example, the tool finds entries with duplicate dirxEntryUUID values in the DirX Audit History Database and generates new unique values. Entries with missing dirxEntryUUID values are resolved by internally calling the “filluuid” command. This is the default behavior.

```
dxthistdbtool makeunique -ldapconfig ldap.properties
```

In this example, the tool first finds entries that are exact duplicates of each other (the same on every attribute), and purges all extra duplicate entries from the DirX Audit History Database. After this operation, the tool continues with the default behavior.

```
dxthistdbtool makeunique -ldapconfig ldap.properties -purge
```

In this example, the tool performs the operations described in the first example (the default behavior) and also outputs digests (summaries) of all duplicate entries found in the DirX Audit History Database to the specified CSV file.

```
dxthistdbtool makeunique -ldapconfig ldap.properties -csvfile duplicates.csv
```

In this example, the tool makes no modifications to the DirX Audit History Database nor LDAP. It only outputs digests of all found duplicate entries into the specified CSV file.

```
dxthistdbtool makeunique -ldapconfig ldap.properties -simulate -csvfile
duplicates.csv
```

7.3.9. Import LDIF into DirX Audit History Database

To import LDAP entries from an LDIF file into the DirX Audit History Database, execute the following command:

dxthistdbtool importldif *common_options files*

where

common_options
Specifies the common options. See the section "Common Options" for details.

files
List of LDIF files to be imported into the DirX Audit History Database. Separate the filenames with a SPACE character. You can also specify directory names and use wildcard characters like *****. Each LDIF file must contain a single entry type. The entry type is extracted from the filename. For example: **account.ldif** imports entries of entry type **Account**. A prefix delimited by an underscore (_) can also be used. For example: **test_account.ldif** also imports entries of entry type **Account**.

7.3.9.1. Import LDIF into DirX Audit History Database Examples

In this example, the tool imports LDAP entries of entry type **User** from LDIF **user.ldif** and **Account** from LDIF **account.ldif** into the DirX Audit History Database. No changes to LDAP are made.

```
dxthistdbtool importldif user.ldif account.ldif
```

In this example, the tool imports all files inside the directory **/ldifs** with the extension **.ldif** into the DirX Audit History Database. The individual LDIF file names are used as entry types. No changes to LDAP are made.

```
dxthistdbtool importldif ./ldifs/*.ldif
```

7.4. Populate Fact Tables

The tool **db_fact_population** populates fact tables in the DirX Audit Data or History Database. In day-to-day operations, the fact tables are filled regularly by the fact population component hosted on the DirX Audit Server. It calculates the facts for the last *n* days. The number of days and the schedule are configurable. See the chapter “Managing Fact and Dimension Tables” in the *DirX Audit Administration Guide* for more information. The fact population has two parts - Java based population and script-based population.

There are cases where periodic fact population is not enough; for example:

- After migrating to a new DirX Audit version, when you want to create facts in the new configuration for the audit messages that have already been written beforehand.
- You have exported old audit messages to files, re-imported them and want to have facts for them.

For this purpose, DirX Audit provides the **db_fact_population** command-line tool. It accepts a start and an end date and calculates the facts for this time range.

Note that the tool creates the fact and dimension tables according to the configuration when necessary. It also adds fact and dimension columns to existing tables when missing. But it doesn’t delete existing columns from tables when they are removed from the configuration.

To populate fact tables in the DirX Audit Database, execute the following command:

dxtPopulateFacts *common_options*
[**-disableData**]
[**-disableHistory**]
[**-disableSqlScripts**]
[**-endDate** *yyyy.mm.dd*]
[**-startDate** *yyyy.mm.dd*]
[**-param VALIDFROM=***RELDATE*]

where

common_options
Specifies the common options. See the section "Common Options" for details.

-disableData
Prevents the fact population operation for the DirX Audit Data Database from being initiated.

-disableHistory
Prevents the fact population operation for the DirX Audit History Database from being initiated.

-disableSqlScripts
Prevents the script-based fact population from being initiated.

-**endDate**
Specifies the end of the time range for which the facts are to be populated using Java based population, including the end day. If it is missing, facts are calculated until the latest audit message.

-**startDate**
Specifies the beginning of the time range for which the facts are to be populated using Java based population. If it is missing, facts are calculated starting with the oldest audit message.

-param VALIDFROM=*RELDATE*
Specifies the beginning of the time range for which the facts are to be populated using the script-based population. The *RELDATE* argument must be a relative date expression. If it is missing, the default value is **%REL_DATE_FROM(TD-5)%**.

If both **-disableHistory** and **-disableData** options are used, no operation is performed.

7.4.1. Fact Table Population Examples

If you want to generate facts for all the audit messages in the tenant database (using Java based population; the default value **%REL_DATE_FROM(TD-5)%** limits the script based population), omit the start and end date as shown in the following command. Please make sure that you use the "simple plain hyphen" **-** in the command line.

```
dxtPopulateFacts -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
```

This example assumes that DirX Audit is installed and configured for multi-tenancy and you want to start fact population for a specific tenant. The connection data for the DirX Audit Data Database, DirX Audit History Database and localization of the configuration files for the fact and dimension tables are stored in the tenant configuration.

The next example calculates all the facts until the end of year 2011 (for Java-based population). The connection data and path to the fact configuration files are taken from the configuration file of the only configured tenant (stored configuration) and it starts without prompting the user to confirm the DirX Audit Data and History Databases to be updated (because the **-silent** option is used; see the section "Common Options" for details):

```
dxtPopulateFacts -endDate 2011.12.31 -silent
```

The next example calculates the facts from January 1st until the end of March 2015 (for Java-based population). The connection data for the databases and localization of the configuration files are taken from the tenant configuration. Only the DirX Audit History Database is populated and the user is prompted to confirm the database to be updated (because the **-silent** option is not used; see the section "Common Options" for details):

```
dxtPopulateFacts -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99 -startDate
2015.01.01 -endDate 2015.03.31 -disableData
```

The next example calculates the facts for all the audit messages only in the DirX Audit Data Database. The connection data for the databases and localization of the configuration files are taken from the tenant configuration.

```
dxtPopulateFacts -tenantid 4f753e1d-d0de-4aef-bb22-caace7342e99
-disableHistory
```

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.