EVIDEN

Identity and Access Management

DirX Audit

Tutorial

Version 7.2, Edition June 2025

Table of Contents

Preface

This manual is a tutorial that is intended to help you understand and use the features of DirX Audit. It consists of the following chapters:

- Chapter 1 uses a step-by-step approach to describe how to work with the product. The information in this chapter is intended for any DirX Audit customer.
- Chapter 2 explains specific aspects of DirX Audit when working on data delivered by DirX Identity. The information in this chapter is intended for DirX Identity customers. The sample data results from a run through the *DirX Identity Tutorial*.
- Chapter 3 explains specific aspects of DirX Audit when working on data delivered by DirX Access. The information in this chapter is intended for DirX Access customers. The sample data results from a run through the *DirX Access Web Sample Scenario Guide* for one user.

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. Getting Started

This quick start demonstrates the most important features of DirX Audit and illustrates the typical way to work with DirX Audit in a customer environment. It consists of several nearly independent sections that describe typical DirX Audit use cases.

This quick start consists of several sections:

- How to analyze aggregated data with the DirX Audit Manager Dashboard view.
- How to analyze audit events with the DirX Audit Manager Audit analysis.
- How to analyze history entries of audit events with the DirX Audit Manager History view.
- How to set up and run DirX Audit reports with the DirX Audit Manager Reports view. For information on how to customize reports, see the *DirX Audit Customization Guide*.

After performing these quick start sections, you should be able to:

- Understand and use most of DirX Audit's powerful features.

1.1. Before You Begin

Before you can use the quick start, you must:

- Install DirX Audit and all of its selectable components on the same machine (no distributed environment). See the *DirX Audit Installation Guide* for details.
- Read about basic user interface features in the *DirX Audit User Interface Guide*.

This tutorial also assumes that you are running the DirX Identity My-Company sample domain and that you can use the My-Company users to log in to DirX Audit Manager. See the *DirX Identity Tutorial* for details about the My-Company sample domain and its users.

If you are familiar with the DirX Identity Tutorial, which is the original source of data for this tutorial, you can also follow and compare individually performed steps.

1.2. Preparing to Use the Tutorial

Before we can proceed with the tutorial, we need to perform the following tasks:

- Set up the event context calculation
- Load the sample data (events) from the DirX Identity source
- Load the sample data (events) from the DirX Access source
- Load the sample DirX Identity history data
- Calculate history data foreign keys and sample KPI tables
- Load the default Dashboard components

1.2.1. Setting up the Event Context Calculation

A context record contains data on the causing event for most audit events. In particular, it holds names of requesters and approvers in approval activities. DirX Audit Server calculates these values regularly. We need to edit the server configuration file for populating context records before loading the sample data so that the data loaded in the next steps are calculated with the correct time scope.

- Navigate to the tenant route deployment folder *install_path***/server_container/tenants/***tenantID***/deploy/routes/**.
  Copy the tenant context record calculation route XML file **route-dxt-scheduler-populatecontextrecords-***version***.xml** to a safe location outside of the tenant route deployment folder. We need to save a copy of the original file so that we can restore it later after we complete the steps to load the sample data.
- In the deployment folder, open the **route-dxt-scheduler-populatecontextrecords-***version***.xml** for editing.
- Find the **Run on configured time** trigger section and modify the **jobdatamap.arg_orphan_to** parameter. If you want to see the same results as described in this tutorial, you must calculate contexts for all tutorial data which come from 09/2022 or 10/2022. For example, if you start tutorial data calculation in 01/2023, you must set **jobdatamap.arg_orphan_to=TM-4**. Save the file.
- The calculation runs several times according to the set scheduler and maximum of results until it counts all the contexts; for our data, it takes about half an hour. If you need to speed it up, you can change the scheduler and increase the **jobdatamap.arg_max_result** parameter to a larger value to calculate contexts faster. For example, you could change it to **jobdatamap.arg_max_result=1000**.
- When you have completed your modifications to the tenant context record calculation route XML file, *move the modified file to a location outside of the tenant route deployment folder* so that it disappears from the folder. (Make sure not to overwrite the original XML file you copied in the first step). This action unregisters the original version of the file with the server.
- Now *move your modified file back into the tenant route deployment folder*. This action registers your modified file with the server so that the modifications are reflected in the job scheduling.
- You should revert the scheduled context calculation job back to the original state after all contexts have been calculated. To check that calculation is finished, check the **dirxaudit-server.log** file in *install_path***/server_container/tenants/***tenantID***/logs**.
  When you find the message **Created context for 0 audit messages. ... PopulateContextRecordsJob has finished.**, you can be sure that all contexts have already been calculated.
  Delete the modified **route-dxt-scheduler-populatecontextrecords-***version***.xml** route file in the tenant route deployment folder and then copy the original route backup file you copied and saved in the very first step back into the tenant route deployment folder. This action resets the original context calculation job settings.
- Now proceed with the next sample data loading steps.

After running the context calculation, you should see the correct contexts in the Audit analysis details view in several context-based reports and in the History details view.

1.2.2. Loading the Sample Data from the DirX Identity Source

DirX Audit comes with a pre-defined set of sample data from the DirX Identity source. This data was prepared by performing the *DirX Identity Tutorial* and it is stored in DirX Identity XML file format. To load this data into an empty (data) database, we need to:

- Navigate to the folder *install_media*/**Additions/Data/SampleData/Identity/Data** on your DirX Audit installation media.
- Copy all files named **dxi_audit_***number***.xml** and **dxi_auditTrail_***number***.xml** in this folder to the input folder you specified for DirX Audit file collector imports when you configured the collectors for your tenant; for example, **C:/dxt/input/file/***tenantID***/dxi**. Be sure to copy the files into the correct folder configured for your tenant.

In the file names above, *number* is a number assigned to the file when it was created during the DirX Identity. The suffix **_audit** distinguishes the audit messages from the JMS queue and **_auditTrail** the audit messages collected from LDAP.

The DirX Audit Server creates the input folder - for example, **dxi** - when it first starts up. If this folder does not currently exist in your installation, you can create it yourself in the input folder and then copy the files to it, or you can start the DirX Audit Server first and then copy the files.

If you do not know the path to the input folder for DirX Audit file collector imports, you can find it by looking in the Tenant Configuration Wizard tabs. For this tutorial, the relevant component is:
Server File Collector for DirX Identity Format

Search for the parameter **Input** folder. If you insert only the folder name without the full path in the Tenant Configuration Wizard; the input folder is created in the *install_path*/**server_container/tenants/***tenantID***/** folder.

- If you have not started **DirX Audit Server** service, start it now. This action triggers the file collectors to import the files in the input folder into the DirX Audit Database (we recommend importing all files). After a few minutes, the files you copied should disappear from the input folder (for example, **C:/dxt/input/file/***tenantID***/dxi**).

If your DirX Audit installation has set up the DirX Audit components like the DirX Audit Server as system services, you can start and stop the DirX Audit Server as you would any other operating system service; for example, on Windows, from the Services panel. See the subsection on installing system services in Chapter 5 of the *DirX Audit Installation Guide* for more details.

1.2.3. Loading the Sample Data from the DirX Access Source

DirX Audit also comes with a pre-defined set of sample data from the DirX Access source. To load this data into your database:

- Navigate to the folder *install_media*/**Additions/Data/SampleData/Access** on your DirX Audit installation media.
- Copy all files named **dirx_access_***number*_**sampledata.xml** in this folder to the input folder you specified for DirX Access file collector imports when you configured the collectors for the tenant; for example, **C:/dxt/input/file/***tenantID***/dxa**. Be sure to copy the files into the correct folder configured for your tenant.

The DirX Audit Server creates the input folder - for example, **dxa** - when it first starts up. If this folder does not currently exist in your installation, you can create it yourself in the input folder and then copy the files to it, or you can start the DirX Audit Server first and then copy the files.

If you do not know the path to the input folder for DirX Audit file collector imports, you can find it by looking in the Tenant Configuration Wizard tabs. For this section, the relevant component is:
Server File Collector for DirX Access Format

Search for the parameter **Input folder**. If you insert only the folder name without the full path in the Tenant Configuration Wizard; the input folder is created in the *install_path*/**server_container/tenants/***tenantID***/** folder.

- If you have not started **DirX Audit Server** service, start it now. This action triggers the file collectors to import the files in the input folder into the DirX Audit Database (we recommend importing all files). After a few seconds, the files you copied should disappear from the input folder (for example, **C:/dxt/input/file/***tenantID***/dxa**).
- When all contexts have been calculated, copy the saved ***original*** **route-***tenantID***-dxt-scheduler-populatecontextrecords-***version***.xml** back into the deployment folder. This action registers the original settings with the server and restores the scheduled context record population to its original state. You can check to see if the calculation has finished by checking the **dirxaudit-server.log** file in *install_path*/**server_container/tenants/***tenantID***/logs**, where you can find logged messages indicating that no new contexts are calculated; for example, **| ContextRecordProducer | 64 - dxt-db-persistence - 7.1.12.SNAPSHOT | UpdateContexts result: 0 failed events, 0 new contexts**.

1.2.4. Loading the Sample DirX Identity History Data

The history database is usually populated by scheduled history synchronization server jobs, synchronizing DirX Identity entries snapshots as history entries into the DirX Audit history database. To facilitate the DirX Audit tutorial environment setup without the need to configure a connection from DirX Identity and the history synchronization job, we provide a set of LDIF files that contain exported history entries.

We'll use the DB maintenance tool (described in more detail in the Tools chapter of the *User Interface Guide*) and specify the target tenant with its history database to load these prepared history entries automatically into the specified DirX Audit database:

- Navigate to the folder *install_media***/Additions/Data/SampleData/Identity/History** on your DirX Audit installation media and then copy its contents to your hard drive to the folder *install_path***/tools/db_maintenance/bin**.
- Before running the batch file, which will import the history data you have to modify it by specifying the tenant ID - i. e. the already configured tenant which includes the target history database into which the history entries will be imported. Edit the *install_path***/tools/db_maintenance/bin/dxtTutorialLdif2Histdb.bat** file and replace all occurrences of *tenantid* with the ID of your target tenant.
- Now start the command line as administrator from the Start menu and run the batch tool *install_path***/tools/db_maintenance/bin/dxtTutorialLdif2Histdb.bat**. This action automatically loads all the prepared history entries sets into the DirX Audit database specified in the connection file. There are several sets of history entries representing individual *DirX Identity Tutorial* exercises, so the loading procedure will run repeatedly in several cycles and can take up to 15 minutes to complete.
- If you're working with the Oracle database, you'll be able to see the entry attributes after running **DXT_HISTORY_VIEW_PROCEDURE**. By default, it is set to run once a day during the night. To be able to see the changes immediately, contact your database administrator to run **Procedures/DXT_HISTORY_VIEW_REFRESH** manually. As some history views are based on foreign keys, this procedure should be run after calculating history data foreign keys as described in the next step.

1.2.5. Calculating History Data Foreign Keys

After we've loaded the sample DirX Identity history entries into the history database, we also need to calculate the foreign keys. This procedure connects related entries, which results in the display of related DNs in entry attributes as links in the Manager application. By default, the DirX Audit Server calculates the keys regularly every night. However, we want the calculation to occur right now, instead of having to wait until the next day. To trigger immediate calculation, we need to edit the server configuration file to enable the predefined 30-second trigger:

- Navigate to the folder *install_path***/server_container/tenants/***tenantID***/deploy/routes/**. Copy the tenant foreign keys calculation rout XML file **route-dxt-scheduler-updatehistdb.xml** to a safe location outside of the tenant route deployment folder. We need to save a copy of the original file so that we can restore it later after we complete the steps to load the sample data.
- In the deployment folder, open the **route-dxt-scheduler-updatehistdb.xml** for editing.
- Uncomment the **Run immediately - only once** trigger section and comment out the **Run on configured time** trigger section.
- Modify 2 values - (TD-7) and (TD-30) to cover all tutorial data which come from 09/2022 or 10/2022. For example, if you start the tutorial history data foreign keys calculation in January 2023, you must set it to **TD-150** which covers 150 days into the past. Save the file.

- Next, copy the modified file to a safe location outside of the tenant route deployment folder. Delete the modified route XML file that exists in the tenant route deployment folder and then copy your saved modified version back into the folder. These steps ensure that the modified settings are reflected in the job scheduling.
- Wait five minutes to make sure that all the foreign keys have been computed. You can optionally check this in the **dirxaudit-server.log** server log file in *install_path***/server_container/tenants/***tenantID***/logs** where you can find logged messages indicating that the recalculation has already been performed and so no new foreign keys need to be added; for example, **UpdateHistoryDbJob has finished.** The visible result of this action is that when you open any history entry details page, there will be active links to other related or assigned history entries; for example, user **Alle Nicolas** with links to his assigned accounts and privileges, his organizational unit and so on.
- Revert the changes to prevent constant running of the update job: delete the modified **route-dxt-scheduler-updatehistdb.xml** route file in the tenant route deployment folder and then copy the original route backup file you copied and saved in the very first step back into the tenant route deployment folder. This action resets the original foreign key calculation job settings.

1.2.6. Calculating the Sample KPIs

DirX Audit can show KPI values in a form of chart. The aggregated source data for charts is calculated from audit events and messages and also from history entries. DirX Audit Server calculates the values regularly. For immediate calculation of the aggregated data you can use the fact population command-line tool installed as a part of DirX Audit.

- Navigate to the folder *install_path***/tools/db_fact_population/bin**.
- Start the fact population tool by running **dxtPopulateFacts -tenantid** *tenantID*; where *tenantID* specifies the identifier of a configured tenant. For example:

```
dxtPopulateFacts -tenantid 71a75691-d28a-48ce-a542-6d6af7ece680
```

The tool populates a set of OLAP structures that contains aggregated data for presenting KPI values. It uses database connectivity settings stored in the configuration file of the specified tenant. See the section “Using the DirX Audit Tools” in the *DirX Audit User Interface Guide* for more options. See the subsection on installing system services in Chapter 5 of the *DirX Audit Installation Guide* for more details. You can also check the result of this action in the Dashboard tab in the next step. The components will display the data loaded in previous steps and computed in this step.

1.2.7. Loading the Default Dashboard Components

DirX Audit comes with a set of default Dashboard components that you can load into the DirX Audit Manager and use right away. In this preparation step, we will load these components and then select a Dashboard layout.

1.2.7.1. Loading Dashboard Components

First, we need to log in as **Tinker Boris**, because only the Audit Administrator can manage and import public components. (**Dalmar Christopher** and **Abele Marc** are Auditors, so they can only use public components but cannot manage them. They can only import the components for their private use):

- Start your Internet browser and specify the URL of DirX Audit Manager for your tenant, for example:
  `https://localhost:8443/AuditManager/login.xhtml?tenant=685a5aec-4c34-4e64-94fe-377df25f8774`.
- In **Name**, enter **Tinker Boris**.
- In **Password**, enter the password **dirx**, and then click **Login**.

Now we can import the default Dashboard components:

- Click the Dashboard tab, if it's not already selected.
- Click **Manage Components** to open the Manage Components dialog.
- Select the Public Components tab (if it's not already selected) and then click **Import**.
- In the display area of the Import dialog, click **Add**. A file selection dialog is displayed.
- Navigate to the folder *install_media*/**Additions/Data/Components**.
- Type **Ctrl+A** to select of the files in the folder *install_media*/**Additions/Data/Components** in one step and then click **Open**.
- The Import dialog display area now shows the files in the file list. Click **Upload** to upload them to the application, and then click **Import** to load them into to the Dashboard. After a few seconds, the new components are displayed under the Public Components tab.
- Click **Close**. Now we've completed the task of loading the default components into the Dashboard.
- Click **Logout** to log out of DirX Audit Manager.

1.2.7.2. Selecting a Dashboard Layout

Now we need to select a Dashboard layout in which to display the new components and select the components to be displayed:

- In **Name**, enter **Tinker Boris** to login again.
- In **Password**, enter the password **dirx**, and then click **Login**.
- Click the Dashboard tab if it's not already selected.
- Click **Layout** to open the Layout dialog.
- Select the layout that presents components in two rows and three columns, if not already selected.
- Click **Add new**, select the Public Components tab and move to the second table page to add the **DirX Identity total audit events on accounts by month and operation** component.
- Click **Add new** again to add the **Total audit events by month and source** component, again from the Public components tab, this time from the third table page.
- You can populate the layout with the other components, but you'll select specific components in subsequent tutorial steps.
- Click **OK**.

1.3. Working with the Tutorial

Once you have completed your preparation for the tutorial, you should back up the example database so that you can restore the prepared example database later on. It is also a good idea to back up your example database each time you successfully complete a quick start exercise. This way, you can retry an exercise that failed for some reason without having to return to the very first exercise.

Refer to your database product's user documentation for instructions on how to back up your data.

1.4. Logging In

Log in as Tinker Boris:

- Start your Internet browser and specify the URL of DirX Audit Manager for your tenant, for example:
  `https://localhost:8443/AuditManager/login.xhtml?tenant=685a5aec-4c34-4e64-94fe-377df25f8774`
  (See the chapter "Logging In" in the *DirX Audit User Interface Guide* for details.)
- In **Name**, enter **Tinker Boris**.
- In **Password**, enter the password **dirx**, and then click **Login**.

After a few seconds, the DirX Audit Manager displays its main page. (See "About the Main Page Layout" in the *DirX Audit User Interface Guide* for details.)

By default, DirX Audit Manager uses the language selected in the browser. Please select **GB** in the language selection area (if not selected) to see the same data results as described in this tutorial.

1.5. Analyzing Aggregated Data with the Dashboard

This exercise demonstrates the Dashboard feature of DirX Audit. We'll explore how to

- Use default Dashboard components
- Modify Dashboard components
- Create your own Dashboard components

1.5.1. Using Default Components

DirX Audit comes with a set of default components that you can use right away. We loaded these components into the Dashboard in the preparation step "Loading the Default Dashboard Components". In this exercise, we'll use some of these components.

1.5.1.1. Using the Total Audit Events by Month and Source Component

The sample database contains a set of audit events collected from DirX Access and DirX Identity.

In the Dashboard view, look at the tile that displays the **Total audit events by month and source** component. First, we need to adjust the time filter to display all the sample data:

- Click  to open the Edit component dialog.
- Click the Data tab if it's not already selected.
- In **When**, select **Any time**.
- Click **Save**.

Now the chart shows a list of months. There is a stacked bar for each of them. Pieces of the bar represent audit sources like DirX Access and DirX Identity and the total number of these operations over objects. For example, DirX Identity produced 220 audit events in September 2022 and 1012 audit events in October 2022.

- Click  to maximize the component. The component now takes over the entire Dashboard view display.
- Click on the area next to the 1012 (DirX Identity, Oct/2022) label. This action initiates a drill-down to audit events that originated in DirX Identity in October 2022. A list of audit events appears.
- Set the **Items per page** to **20**.
- Click  to return to the **Total audit events by month and source** component.

- Notice the buttons with component names that appear below the maximized **Total audit events by month and source** component. These buttons link you to the other components that you have selected for display in the Dashboard view. To switch to one of these components, you can simply click its button.
- Click to restore the component's size from maximized to original.

1.5.1.2. Using the DirX Identity Total Audit Events on Accounts by Month and Operation Component

Now analyze operations over accounts:

- Look at the component displayed in the Dashboard view. Again, we need to change the time settings:
  - Click to open the Edit component dialog.
  - Click the Data tab if it's not already selected.
  - In **When**, select **Any time**.
  - Click **Save**.
- The chart shows a list of months. There is a stacked bar for each of them. Pieces of the bar represent the following operations: Add Object, Delete Object, Disable, Enable, Update Object and the total number of these operations over account objects. For example, the Add Object operation was run 63 times in October 2022.
- Click on the area at the 63 (Add Object, Oct/2022) label to drill down to audit events that record the addition of new accounts. You can use the page navigator to browse the list of events. You can also change a number of audit events per page in the Items per page list.
- You can see that some of the accounts were created manually (**manual**) and some on event or on request.
- Click to return to the **DirX Identity total audit events on accounts by month and operation** component in the Dashboard view.

We can also use the zooming feature to view only those records within the selected time period in a more detailed time resolution:

- Click the **Oct/2022** month indicator next to the bar with the October stacked bar. You can now see only the October events bars but divided by their day time stamp. This view can be useful when you are interested in getting more detailed information on a particular time range and it allows you to quickly zoom in on it without having to change the entire component time constraint through the settings.
- Click to reset the zoom level.

1.5.2. Changing Component Settings

We may also want to change a component's settings: its data source and the style in which the data is displayed. The next exercises demonstrate how to accomplish these tasks.

1.5.2.1. Changing Component Data

First, change the time constraint of the source data:

- Choose a component you want to change; for example, the **DirX Identity total audit events on accounts by month and operation** component.
- Click to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Custom time**.
- Set **1/9/2022** to **From** and **30/9/2022** to **To**.
- Click **Save**. The chart is recalculated and the chart's subtitle indicates the time frame you just applied. You cannot see October 2022 data in this component now because it is out of the changed time scope. To adjust this:
- Click  to open the Edit component dialog again.
- Set the **Custom time** values to **1/9/2022** in **From** and **31/10/2022** in **To**.
- Click **Save**. Now all data is visible again.

In the Data tab, you can also change a component's fact table, fact and dimension sources. If you do this, don't forget to change the component's title to correspond with your new selection.

1.5.2.2. Changing the Component Style

Now modify the component's style:

- Choose a component you want to modify; for example, the **DirX Identity total audit events on accounts by month and operation** component.
- Click  to open the Edit component dialog.
- Select the **Style** tab (if it's not already selected).
- Click the drop-down arrow in **Color scheme** and then select another color option.
- Click **Save**. The chart is recalculated and a different color scheme is applied.

You can also change other style settings. Some of them are applicable only for selected component types.

1.5.3. Creating a New Component

In this exercise, you'll select an existing Dashboard component and then change it:

- In the **DirX Identity total audit events on accounts by month and operation** component, click  to open the Edit component dialog.
- Click **Save As ...**. In **Component title**, enter **Successful password changes by month**. In **Component Name**, enter **evn__dxi_pwdchanges__succeeded__datemonth** . In **Add to dashboard**, select **as new** and then click **Save**.
- If the new component is not displayed in the dashboard, open **Layout** and move your new component up in the list so that it is visible in the Dashboard.
- Click  to open the Edit component dialog again.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- In **Fact table**, select **Password changes**. In **Facts**, select, **Succeeded**. In **Dimensions**, select **Month**.
- Change the **Chart class** selection icon to  (one fact and one dimension).
- Click the **Style** tab and change the component's style to whatever you'd like to use.
- Click **Save**.

The new component shows only successful password changes on accounts and users aggregated by month. You can drill down to list corresponding audit events.

You can also export the component into an XML file and later import it back into the Dashboard.

1.6. Analyzing Audit Events with the Audit analysis

This exercise demonstrates how to use the DirX Audit Manager Audit analysis page. The Audit analysis provides a view on audit events in a user-friendly form. It extends the audit message data with three additional columns: Operation, Type and Detail. Information is digested from fields of the related audit message when the message is persisted into the DirX Audit Database. Each audit message can have no related audit events, exactly one related audit event, or more than one related audit event.

In this section, we'll demonstrate how to:

- Search for and analyze events
- Work with event search filters
- Use an advanced search
- Create an audit events report

1.6.1. Searching and Analyzing Events

We'll begin this exercise by opening the Audit analysis:

- If you are not logged in to DirX Audit Manager, follow the instructions in "Logging In".
- In the DirX Audit Manager main page, click the Audit analysis tab.
- Click **Search**.

The result is a table with 10 rows that represent audit events. The additional rows at the top and bottom of the table define column names.

1.6.1.1. Searching for an Operation

Now we'll look at all events of a specific operation; in this case, the Add Assignment operation:

- In **Source**, select **DirX Identity**.
- In **Operation**, type **Add Assignment**.
- Click **Search**.

Test this query with other operations; for example, Accept and Reject.

1.6.1.2. Analyzing the Audit Event Details

Now you can explore the details of the audit message using the Add Assignment operation:

- In a result table, select a message with **Operation = Add Assignment**.
- Click the Show Details icon 🔎.

The pop-up window with the event details opens. You can see Audit Event, Identification, What, Who, Where From and Original Message sections.

1.6.1.3. Analyzing the Related Events

You can also explore the related events using the Add Assignment operation:

- In a result table, select a message with **Operation = Add Assignment**.
- Click the Show Related Events icon 💼.

The display with the table containing audit events opens. The message for which this function is calculated is highlighted in gray. The other messages are related to the original one, which means they caused or they were caused by the original action.

1.6.2. Working with Search Filters

This exercise demonstrates how to work with event search filters: we'll use the filter definition area in Audit analysis to create a private filter, modify it and then delete it.

1.6.2.1. Creating a Private Search Filter

You can save your search criteria as a filter so that you can easily repeat common queries; here, you'll create one for the User to Role Assignment event:

- In **Source**, select **DirX Identity**.
- In **Operation**, type **Add Assignment**.
- In **What Type**, type **User to Role**.
- Click **Search** to check what your selected filtering options will display.
- Click **Save As...**.
- The **Save as ... Filter** pop-up window opens. In **Name**, type **User to Role Assignment**.
- In **Description**, type **User to role assignment from DirX Identity audit events**.
- Click **Save**.

You have just created a private filter definition that searches for User to Role Assignment events from DirX Identity. Private filters are available only to the user who created them. When you select it from **Select Filter**, the search fields are pre-filled with your saved search criteria and the search action is performed automatically.

1.6.2.2. Modifying a Search Filter

You can change the search criteria of your saved filter:

- In **Select Filter**, select **User to Role Assignment**.
- In **Who**, type **DomainAdmin**.
- Click **Save**.

Your filter definition is now changed. You can also modify the filter's name and description:

- Select Manage Filter .
- Click Edit for User to Role Assignment.
- In **Name**, type **User to role assignment by DomainAdmin**.
- In **Description**, type **User to role assignment from DirX Identity audit events caused by Domain Admin**.
- Click **Save**.

The filter's name, description and search criteria are changed.

1.6.2.3. Deleting a Search Filter

You can delete a filter in the following way:

- Select Manage Filter .
- Click Delete for **User to Role Assignment by DomainAdmin**.
- The message **Delete this filter?** is displayed. Click **OK**. The filter is deleted and removed from the list. It is also removed from the available filters in **Select Filter**.
- Click **Close** to close the pop-up window.

If you have Audit Administrator rights, you can use the procedures shown here to create, modify and delete public filters visible to other users. A private filter can be used, modified and deleted only by its owner. Public filters created by the Audit Administrator can be used but not deleted by an Auditor. The Audit Administrator is permitted to delete his private filters and public filters.

1.6.3. Using an Advanced Search

Sometimes the search criteria provided in the filter definition area are not enough. If this is the case, you can use the Advanced Search section, which provides more options for querying audit events. In this exercise, you will search for self-assisted password settings:

- Delete your previous search criteria from **Operation** and **What Type** fields. The fields should be empty. You can also clear the fields by selecting the default Empty filter from the filter selection above the search criteria fields.
- Click the Advanced Search icon .
- In **Property**, select **Password self assisted**.
- In **Value**, select **Assisted**. See the section "Dimensions" in the chapter "Dashboard Data" in the *DirX Audit Administration Guide* for details.
- Click **Search**.

You can see the list of events generated by assisted password settings in the connected systems and in DirX Identity Web Center. The changes were provided by **domainAdmin** (the **Who** search criterion).

The settings in the Advanced Search section are also saved to the private search filter.

1.6.4. Creating an Audit Events Report

When you perform a search, you can use the Report function to export audit events to a file and/or send it via email:

- Use the values returned from previous exercises or provide a search according your criteria.
- Click **Report**. A pop-up window opens.
- In **Template**, select **EventMonitorAll**.
- In **Format**, select **PDF**.
- In **Encoding**, select **UTF-8**.
- In **Rows**, type **0** to export all records.
- Click **Export**.

A new tab opens that displays the list of audit events that correspond to the search criteria.

1.7. Analyzing History Data with the History View

The History view works directly with history entries stored in the DirX Audit Database. As part of preparing to run this tutorial, you loaded sample DirX Identity history data generated from running the DirX Identity tutorials into your DirX Audit History database. In this set of exercises, you'll learn how to use DirX Audit Manager's History view to explore this sample data. For details on the DirX Identity tutorials on which these exercises are based, see the *DirX Identity Tutorial*.

In this exercise, you'll learn how to:

- Generate a table of history entries
- Create a report of history entries
- Search for user history entries by name and by distinguished name
- Explore the details of a history entry

If you haven't used the History view before, we recommend reviewing the information about its basic functions presented in the chapter "Using the History View" in the *DirX Audit User Interface Guide* before continuing with this exercise.

1.7.1. Generating a Table of History Entries

To get started, you'll use the DirX Audit Manager's History view to generate a table of history entries for DirX Identity events:

- If you aren't logged in to DirX Audit Manager, follow the instructions in "Logging In".
- In the DirX Audit Manager's main page, click the History tab.
- Leave the default values in **When** (**Any time**), **Type** (**User**), and **Attribute** (**uid**) and then click **Search**.

DirX Audit Manager displays a result table below the search area that lists all of the matching entries. Each row represents one history entry that matches the search criteria. In our example, the result table shows ten users and a total of 109 users found.

1.7.2. Creating a History Report

Sometimes you may want to save your history entry result tables outside of DirX Audit Manager. To accomplish this task, you use the Report feature in DirX Audit Manager's History view to save the result table to a formatted file. To save the result table you just generated:

- In the History main page, click **Report**. A pop-up dialog appears with parameters for setting the output format.
- Leave the default values as they are, and then click **Export**. Note that the default report exports only the first 100 entries while the sample data contains 109 user entries. If you want to export all 109 entries, increase the **Rows** value or set it to **0** (which means exporting all entries without any limitation).
- In the Internet browser dialog, you can select to open the report, save it, or cancel it. Click Open to see the results.

The reporting feature demonstrated here is a simple way to export on demand the search result lists generated from your current search criteria. You can read more about this feature in the section "Exporting History Entries" in the chapter "Using the History View" in the *DirX Audit User Interface Guide*.

DirX Audit Manager's Reports view provides a more powerful, complex mechanism for generating auditing reports both on demand and according to a schedule. We'll demonstrate how to use this feature later on in this tutorial.

1.7.3. Searching for a User's History

There are several ways to search for a history entry. You can use a specific attribute and its value for searching or you can click on the Advanced Search icon and search for a history entry by its name, DN or dxrUid. We'll show you how to use two of these methods in this exercise.

1.7.3.1. Searching for a User Entry by Name

First, we'll search for a user history entry by its name. In this case, we'll search for a history entry for the user **Taspatch Nik**:

- In **Type**, select **User**.
- Click the **Advanced Search** icon  .
- In **Name**, type **Taspatch** and then click **Search**.

Because there is only one history entry in the sample database with the name **Taspatch**, DirX Audit Manager displays the details page for this entry. We'll explore the details page in more detail in a later exercise. For now, click **Switch to search form** to return to the History view main page.

1.7.3.2. Searching for a User Entry by DN

Now we'll search for **Taspatch Nik** using his distinguished name (DN):

- In **Type**, select **Any**.
- Clear **Name** in **Advanced Search**.
- In **dn**, type **cn=Taspatch Nik,ou=Global IT,o=My-Company,cn=Users,cn=My-Company**.
- Click **Search**.

Because DirX Audit Manager finds only one entry with this DN, it displays the details page for this entry. In the next exercise, we'll explore this details page.

1.7.4. Exploring History Entry Details

In "Searching for a User's History", you searched for and retrieved a unique history entry for Nik Taspatch. Because it's the only history entry for this user, DirX Audit Manager automatically displays its details page with the Attributes tab table open by default.

The timeline area shows two comparison time point markers. The first time point is the creation time and date for the user entry **Taspatch Nik**. The second time point is the current date and time.

In the timeline area, you'll see the following data for **Taspatch Nik**:

- The time at which his user entry was created.
- The number of attributes created for his user entry (55).
- The number of roles (13) and permissions (18) assigned to him.
- The number of groups to which he belongs (25).
- The number of accounts he has (3).

In the data area, the Attributes tab table shows the list of attributes and their values depending on the selected comparison time point. In our example, the two time points are automatically selected and you can see the attributes and their values at each time point. Attributes that have changed are highlighted in yellow.

The data area also shows tabs for Roles, Permissions, Groups, Accounts, Risks, Events and Assignment cause. In the Show events for row above the timeline, uncheck the Permissions checkbox. The information in the timeline area about Nik Taspatch's assigned permissions is no longer displayed.

Click **Show changes only**. Now you only see the changed values in the Attributes tab table and in the respective Roles, Groups, Accounts and Events tabs for Nik Taspatch. Now clear **Show changes only** and check the Permissions tab in **Show events for** because you'll explore the history of one of Nik Taspatch's assigned roles in the next step.

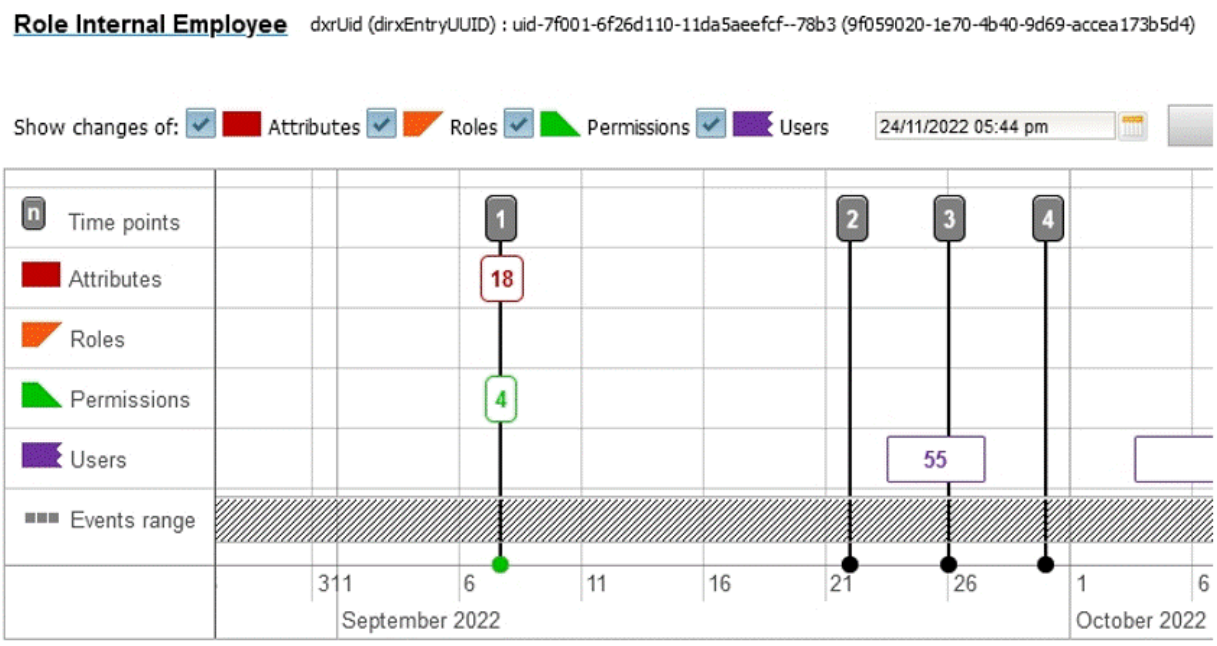
1.7.4.1. Exploring a Role's History

Now you'll explore the history of one of the roles assigned to Nik Taspatch: the **Internal Employees** role.

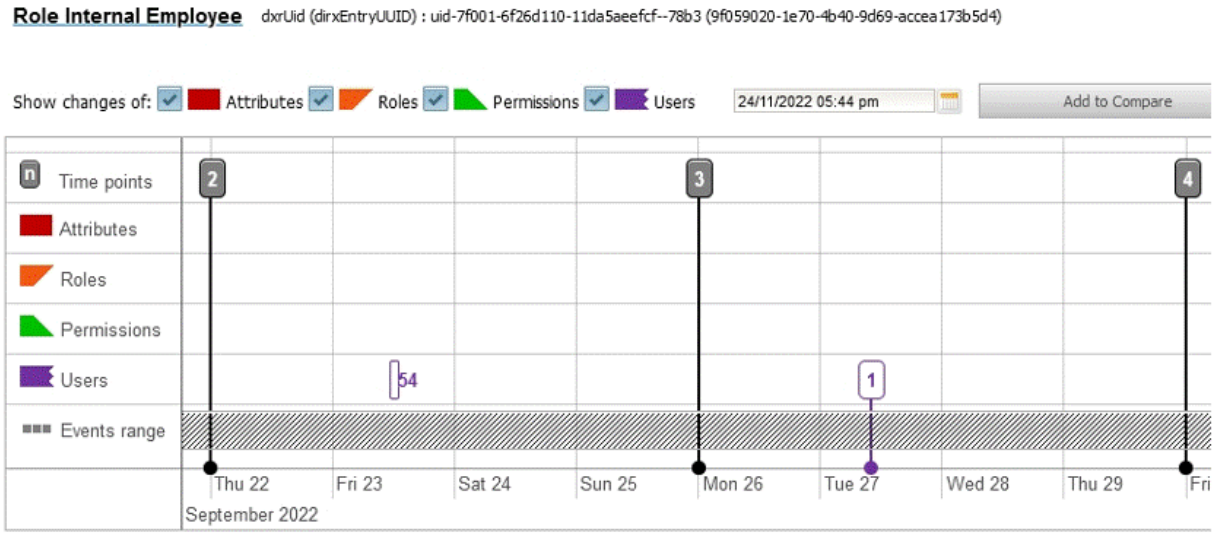
- In the data area, click the Roles tab. DirX Audit Manager displays a table with the names of the roles assigned to Nik Taspatch, the date of their validity and their assignment mode. In the table, you can see that:
  - The role **Internal Employee** has been assigned based on a rule.
  - The role **DXR User Administrator** has been assigned by inheritance from a business object.
  - The other roles have been assigned manually.
- In the **Role Name** column, click the link **Internal Employee [rule]**. This action directs you to this role's details page with the Attributes tab table open by default.
- Examine the timeline area for the **Internal Employee** role to view the event markers indicating the users that have been assigned to the role within the two comparison time points.
- Click the Users tab in the data area. DirX Audit Manager displays a table that lists the names of these assigned users. Note that the table shows 70 records about user assignment changes, the timeline shows cumulative information due to the zoom level. To view the times in milliseconds of each user-role assignment, you'll need to adjust the timeline's scale and then zoom in to the millisecond level of the original time.
- Use the zoom-in button in the details page header to expand the timeline's scale until you can see the event markers that indicate the precise time of each role assignment. Now click the Autozoom button to return to the timeline's original scale. (Note: on mouse devices that provide wheels, you can use the mouse wheel to zoom in the timeline. You can also use the wheel to scroll down to view the data area in the history detail page, but be careful that your mouse cursor is not in the timeline, or you'll zoom in the timeline instead of moving to the data area.)

Next, you'll explore the user changes step by step:

- Add three comparison time points to the timeline (by double-clicking in the time line near one of the User event markers or using the **Add to Compare** function) and then zoom into the timeline until you show the following scenario:



- Scroll down in the details page to view the table with the user names. You can see that some users do not have any time records in the first few columns because they were assigned to the role later.
- The timeline in the table shows the cumulative information about 55 user assignment changes in the time period of 23/09/2022 - 27/09/2022 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 zoom in to days. Now you can see one event 27/09/2022 and the cumulative information about 54 user assignment changes 23/09/2022. You can proceed this way up to milliseconds.



- Check **Show changes only**. Now you can see the following information:
  - The names of the users who were assigned to the role in the process of following the exercises in the DirX Identity tutorial.
- Click the Attributes tab and then uncheck **Show changes only**.

- Now examine the value of the **dxrRoleAdmin** attribute. You'll see that **Taspatch Nik** is listed as a value. This means that Nik Taspatch was assigned to the role when it was created and that he is the role's administrator.

1.7.4.2. Exploring a User's Account History

Next we'll examine Nik Taspatch's account assignments. To return to Nik's details page from the **Internet Employee** role details page, you can either:

- Click the **Taspatch Nik** value for **dxrRoleAdmin** in the Attributes tab table (the highlighted and underlined text).
- Click the down-arrow in **Already viewed entries** in the details page header and then select the history entry for Nik Taspatch that you previously viewed.

DirX Audit Manager returns you to the details page with the Attributes tab table open by default.

Click the Accounts tab. The table shows the names of the accounts created for Nik Taspatch and the corresponding target system name.

Click the expansion arrow next to the account name **Nik Taspatch 5326** (valid for Extranet Portal target system). You can see values for account state, target system state and login name.

1.7.4.3. Exploring Related Events for a User

Now you'll look at the events related to Nik Taspatch's history entry:

- Click the Events tab.
- Check the **From** and **To** fields and the Events range bar in the timeline. The default scope of the Events range bar is three months previous to the current day. The **From** and **To** fields display these dates.
- To view the events in September and October, you need to extend the default scope. Click the Events range bar in the timeline and then move the start of the range to September 2022 and end of the range to October 2022.
- Examine the **Search in** field. If it's not already selected, select the **What** value from the list. Notice that there are no events for **What** that contain **Taspatch Nik** because there were no changes to any of the audited attributes for the user Nik Taspatch processed in the sample data from the DirX Identity tutorial run.
- Go back to the **Search in** field and then select the **Who** value from the list. Now 41 events are shown because **Taspatch Nik** was the requester and/or the workflow approver of changes for other users during the DirX Identity tutorial run. You can learn about the details of these changes by reviewing the *DirX Identity Tutorial* exercises.

You've completed the initial exercises for learning how to use the History view. You'll find more exercises on browsing audit history in the chapter "Identity Auditing".

1.8. Setting up Reports with the Reports View

DirX Audit Manager's Reports view allows you to create various reports on events and history and then send them to selected recipients as email attachments. In this section, we'll demonstrate these tasks.

To get started with this exercise:

- If you are not logged in already, follow the instructions in the "Logging In" section to log in to DirX Audit Manager.
- In the DirX Audit Manager main page, click the Reports tab.

Next, you'll learn how to:

- Work with report sets and report files
- Schedule reports for email delivery to recipients

1.8.1. Working with Report Sets

When you want to create and send a report, you need to create a report set first. A report set contains one or more report files, which are represented by separate email attachments in the generated email message. These files in turn contain one or more reports selected from the list of available reports. Note that you must restrict yourself to using PDF for your reports if you want to create a report file with multiple reports. Other formats don't support this feature.

In this exercise, you'll learn how to:

- Create a report set
- Add a report file to a report set
- Add a report to a report file

You can read more about how to work with report sets, report files and reports in the chapter "Using the Reports View" in the *DirX Audit User Interface Guide*.

1.8.1.1. Creating a Report Set

First, you'll create a new report set named **Demo report**:

- Click  to create a new report set.
- In **Name**, type **Demo report**. In **Description**, type **Demo report set with two files**. Using these fields makes it easier to identify report sets when they are displayed in the report set definitions table in the Reports view.
- Click **Save**.

The report set you just created is now listed in the report set definitions table on the Reports main page.

1.8.1.2. Adding a Single Report File to a Report Set

Now you'll add a report file that contains one report to the report set you just created:

- Click in **Demo report** in the list. This action opens the Edit report set dialog with the File tab open by default.
- Click to add a new report file. This action starts the report file creation wizard, which displays a list of available report file templates. There are two types: report files that contain only one report (identified by the and the icons in the list) and report files that contain multiple reports (identified by the icon in the list).
- You can use **Name** or **Tags** to filter the list of report file templates. Type **Event** in **Tags**. Now only the reports with the **Event** tag are displayed.
- Click on **Changes on User to Privilege Assignments by User** to select it in the list. The wizard opens the Report scope dialog, which allows you to define your report file's parameters.
- In the **When** section, select **Any time**.
- In the **Users** section, specify the users whose data you want to view. In **Identifying Attributes**, select **Name** and then click **Search**. In the list of users in the **Found** table, check the boxes next to **Bader Hans** and **Baretti Franca**, and then click **Add**. These users are now shown in the **Selected** table.
- In **Attribute Value**, type **Teacher Mark** and then click **Search**. Now check the box next to **Teacher Mark (ou: Professional Services, o: My-Company, alt: 83730)** and then click **Add**. Teacher Mark is now shown in the **Selected** table.
- You can click **Preview** to check the results of your filtering criteria. A dialog window opens, offering to open the preview PDF directly with the browser or to save it for later checking. Note that the Row limit field restricts the amount of results displayed in the Preview report. In this example, clicking **Preview** helps you to determine that there are no access requests events for **Baretti Franca** in the sample data set.
- Click **Finish** to complete the report file definition.
- Now type **Changes on User to Privilege Assignments by User - Bader Hans, Baretti Franca and Teacher Mark** in **Name**. This file name will be displayed in the email as the name of the attachment and will also be displayed in the report set File tab.
- Next, type **User to Privilege Assignments by 3 users, pdf file format** in **Description**.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- Click **Save** to save your changes to the **Demo report** report set.

1.8.1.3. Adding a Multi-Report File to a Report Set

In this exercise, you'll add another report file to your report set. This report file contains two reports, which will be collated into one email attachment later on.

- Click in **Demo report** in the list. This action opens the Edit report set dialog with the File tab open by default.
- Click to add a new report file.
- Use **Name** to filter the list of report file templates: type **Logins** in **Name**. Now only the reports that contain **Logins** in their names are displayed.
- Click on the **Total Sum of Logins** report in the list to select it.
- In **When**, select **Custom time From 01/09/2022 To 31/10/2022**.
- In the **Source** section, define the source for the data you want to see. In **Identifying Attributes**, select **Name** and then click **Search**. In the **Found** table, check the box next to **DirX Identity** and then click **Add**. DirX Identity is added to the **Selected** table.
- Click **Next report**. This action allows you to insert another report into the file.
- Clear **Tags**. In **Name**, replace **Logins** with **Assignments**. You now see only those reports whose names contain assignments.
- Click **State of Assignments by User** to select it in the list.
- In the **When** section, select **End of Previous Month**.
- In the **Users** section, define the source for the data you want to see. In **Identifying Attributes**, select **cn** and then click **Search**. The **Found** table displays a long list of users.
- In **Attribute Value**, type **Abele** and then select **Abele Marc** from the list. Now click **Search**. You can see **Abele Marc** in the **Found** table. Check the box next to the entry and then click **Add**. This user is added to the **Selected** table.
- In **Attribute Value**, type **Teacher Mark** and then follow the same procedure as with Abele Marc to add **Teacher Mark** to the **Selected** table. Now search for **Berner Hans** and **Taspatch Nik** and then add them to the **Selected** table.
- Click **Finish** to create the report file with two reports.
- In **Name**, type **File combines two reports in one attachment**.
- In **Description**, type **Logins for DirX Identity, Assignments by user for Abele Marc, Teacher Mark, Berner Hans and Taspatch Nik**.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list. You can see two different reports under the file you just added, which means that these two reports will be collated in one email attachment.
- Click **Save**.

1.8.2. Sending a Report Set

Next, we'll demonstrate how to schedule and send a report set. You'll learn how to:

- Schedule a report set for immediate delivery
- Activate a report set so that it runs
- Schedule a report set for generation and delivery

1.8.2.1. Scheduling the Report Set for Immediate Delivery

We want to send the reports in our report set right away so that we can review them, so we'll set up a schedule for sending the report set immediately:

- Click  in the **Demo report** set row to open it for editing.
- Click the **Schedule** tab and then select **As soon as possible**.
- Check **No end time**. (When this box is not checked, you can define an end date after which the report is no longer sent.)
- Click the **Send to** tab and then enter your email address in **To**.
- In **Subject**, type **Demo report set**.
- Type the message text in **Body**. For example, **Report set generated from DirX Audit.** The attachment contains two files. In the file **Changes on User to Privilege Assignments by User - Bader Hans, Baretti Franca and Teacher Mark** there is a report **Changes on User to Privilege Assignments by User**. In the file named **File combines two reports in one attachment** there are **Logins** and **Assignments by user.**

  You can also leave the **Body** empty. The report status and description are then automatically added to the email message.
- Click **Save**.

1.8.2.2. Activating the Report Set

Even when a report set is planned to be sent and email fields are populated, the report set will not be processed if it's in the inactive state. In this exercise, you'll switch your **Demo report** set to the active status to send it right away:

- An inactive report is identified by the icon in the first column of report set list. Click the inactive icon for the **Demo report** set to activate it.
- The icon changes to  to indicate that synchronization is operating. After the DirX Audit Server processes the changes, the icon changes to  to mark the report set as active.
- If you set up the SMTP email server correctly during DirX Audit configuration, you will receive the email with the report attachment. For the **As soon as possible** scheduling option, the report is sent only once after each editing and saving.

1.8.2.3. Scheduling the Report Set for Regular Delivery

As an auditor, you probably want to generate and send your reports on a regular basis; for example, at the end of each month.

To be able to see variable data, choose a dynamic time definition in the **When** report scope for the reports in a report set, and then set the report schedule to run regularly. This section shows how to make these changes for the **Demo report** set we created earlier in this exercise. First, you'll edit the report set and change the scope for the reports it contains:

- Click in the **Demo report** row to open the report set for editing. You'll see two report files. One of them is the multi-report file named **File combines two reports in one attachment** with two reports listed underneath it. Click next to **Total Sum of Logins** to open it for editing. In the report scope dialog, change **When** to **Previous Month**. Click **OK**.
- Perform the same steps for the other report file **Changes on User to Privilege Assignments by User - Bader Hans, Baretti Franca and Teacher Mark** to change the **When** scope to **Previous Month** for the report it contains.

Next, edit the report set and schedule it to run on a regular basis:

- Click the Schedule tab and then select **Recurring**.
- In **Start date**, select today's date. Set **Time to run** for five minutes from now.
- Uncheck **No end time** and then set **End date** for one month from today. The email and report will not be generated after this date.
- Set **Frequency** to **Monthly**.
- Select today's date in **Day of month** so that you'll see the generated email immediately.
- Click **Save**.

After the DirX Audit Server synchronizes these changes, you can see that your report has the active status and that the **Next start date** column contains a date and time.

We've now finished the introductory exercises for how to view and manage reports with DirX Audit Manager. The exercises in "Identity Auditing" demonstrate more report features and describe individual report content.

2. Identity Auditing

This chapter provides an introduction to auditing with DirX Identity as the source of audit messages. You don’t need to set up a running DirX Identity installation. Instead, we’ll work with sample data content that was produced by performing a complete run through the DirX Identity tutorial and which we loaded and set up in "Preparing to Use the Tutorial".

The sections in this chapter will take you through a set of common Identity auditing use cases. You need to have a working knowledge of DirX Identity in order to understand this section.

2.1. Analyzing a User Self Registration

In the exercises described in the section "User Self Registration" in the *DirX Identity Tutorial*, the following tasks were performed:

- Customer self registration of Farfello Nico
- Assignment to the Customer Newsletter and Hardware Beta Programs services
- Approval of the user creation request by Klarmann Bruno
- Approval of the Hardware Beta Programs request by Briner Ruben

This section shows you how to analyze DirX Identity user entries created by the self registration process. It describes how to:

- Analyze a user creation
- Analyze user to privilege assignments

In these exercises, we’ll use DirX Audit to answer the questions from an auditor’s point of view: Do we have any new users? When were they created and by whom? What privileges were they assigned and who approved the assignments?

2.1.1. Examining a User Creation

Typically, you perform a user creation in DirX Identity via a request workflow. All data is collected during the workflow steps and kept as orders at the workflow instance. The activity ApplyChange of such a workflow creates the user entry in the Identity Store. The operation AddObject creates a new object (User, Account, Workflow instance) in the LDAP directory.

In this section, we’ll examine a user creation that results from a self registration from the Dashboard and Audit analysis views and see how the new user and its attributes are displayed in the History view.

2.1.1.1. Examining a User Creation with the Dashboard

First, we'll examine the user creation for **Farfello Nico** from the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Add the **Total audit events by month and operation** component to the Dashboard using the Layout settings.
- Examine the **Total audit events by month and operation** component. It contains aggregated data for Add Assignment, Add Object and other operations.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**, select the **What – Type** dimension and then enter **User** in **Value**.
- Click **OK**. The chart is recalculated.
- Drill down to audit events of the Add Object operation for September 2022.
- In the **Type** column, you will find audit events created **on request**. The value for **Farfello Nico** came from the user self registration.
- Click  to return to the Dashboard view.

Although we'll use the History view later in this section to examine the history data for Farfello Nico, you can access it directly from the Dashboard, too:

- In the drill-down table you just generated, click 🔎 to open the **Event Details**.
- Expand the **What [User : Farfello Nico]** row and then click the blue underlined **Farfello Nico** link. This action takes you directly to the selected history entry, which is Farfello Nico in this case.

2.1.1.2. Examining a User Creation with the Audit analysis

To analyze the user creation of **Farfello Nico** with the Audit analysis:

- Select the Audit analysis tab in the DirX Audit Manager main page.
- In **Source**, select **DirX Identity**.
- In **Type**, select **on request**.
- In **Operation**, select **Add Object**.
- In **What type**, select **User**.
- Click **Search**. You will find audit events in the result list. These users were created as new ones in the DirX Identity tutorial. You will find an audit event for **Farfello Nico** at the end (she was created as the first new user).

2.1.1.3. Examining a User Creation in the History View

Now we'll view the new user **Farfello Nico** and her attributes with the History view:

- Click the History tab in the DirX Audit Manager main page.
- In **Type**, select **User**.
- Click the **Advanced Search** icon  .
- In **Name**, type **Farfello**.
- Click **Search**. Because only one user with the name **Farfello** is found, the Attribute tab on the details page for this user is displayed. Here you can view the history of changes for **Farfello Nico**.
- Scroll down to the Attributes tab table. You can see the date and time of user creation which is also where the first time point is placed in the timeline. Further down, you can check the user attributes. The user **Farfello Nico** and her attributes were not changed during the life-cycle. Check the type of user with the **employeeType** attribute. **Farfello Nico** is a customer from **Mercato Aurum Rome**.
- Click the Roles tab. You can see four roles assigned to the user **Farfello Nico**. Roles **Customer Newsletter** and **Hardware Beta Programs** were assigned by manual selection of the role. **Platinum Customer** and **Silver Customer** were assigned based on the rule for the customers.
- Click the Permissions tab and then click  next to the permission name to expand the values in the permission name column. You can see that all permissions are inherited from roles and consistent. None of them requires re-approval. You can check the same items for Group assignments.
- Click the Accounts tab and then expand the values in the account name column. **Farfello Nico** has only one active account (in the **Extranet Portal**) as a customer.
- Click the Events tab. In **From**, set **1/9/2022**. In **To**, type or select **31/10/2022**. In **Search in**, choose **Who**. You can see two (2) audit events caused by a direct action of Nico Farfello, that is two (2) login messages from Web Center. You can also see that these two events originate only after the user creation when Ms. Farfello received a mail with the news that she could log in, which is what she did.
- Now choose **What** in **Search in**. You can see a list of five (5) audit events related to Nico Farfello's user creation and privilege assignments.

2.1.2. Studying User to Privilege Assignments

Assigning privileges enables the user to access specific resources in connected systems. In this section, we will show several ways to evaluate privilege assignments and how to create a **Users by Privilege** report.

2.1.2.1. Studying User Privilege Assignments with the Dashboard

To study user privilege assignments in the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **Total audit events by month and operation** component. It contains aggregated data for Add Assignment, Add JoinFromDXI, Add JoinToDXI, Add Object and other operations.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**, select the **What – Type** dimension and then enter **User to Role** in **Value**.
- Click **OK**. The chart is recalculated.
- Drill down to audit events of the Add Assignment operation for September 2022. Change **Items per page** to **50**. Order the table by the **When** column in ascending order.
- You will find several audit events on assigning privileges the users **Farfello Nico** and **Teacher Mark**. In the **What Details** column, you can check which roles were assigned.
- Click  to return to the Dashboard view.

2.1.2.2. Studying User Privilege Assignments with the Audit analysis

To study user privilege assignments with the Audit analysis:

- Select the Audit analysis tab in the DirX Audit Manager main page.
- In **Source**, select **DirX Identity**.
- In **Operation**, select **Add Assignment**.
- In **What**, enter **Farfello Nico**.
- Click **Search**. You should receive four (4) audit events in the result list on assigning Farfello Nico to several roles.

2.1.2.3. Studying User Privilege Assignments with Reports

In this exercise, we'll create a report set that contains two reports for analyzing user-privilege assignments. First, you'll create a report that shows the users assigned to specific privileges, and then you'll create a report that shows the privileges of a specific user.

To create a **Users by Privilege** report:

- Click the Reports tab in the DirX Audit Manager main page.
- Add a new Report set and fill in the report set's **Name** and **Description**.
- Click  to add a new report file.

- Either browse through the list of available reports or use name completion (start typing a part of the report name) or tag filtering (tag History, User or Privilege) to display the **Users by privilege** report. Click on it in the list to select it. The Report scope dialog opens for you to define the parameters of the report.

  Note that the report tag set always includes either History or Events tags indicating the report source data. Events reports are based on the data database and provide an audit trail on performed changes and updates, while history-based reports help the auditor understand and compare different states of inspected history entries in selected points in time.
- In the **When** section, select **Custom time point** and leave the default (current) value in **Date**.
- In the Privileges section, define the attribute filter: in **Identifying Attributes**, choose **cn**, in **Attribute Value**, type **Customer Newsletter** and then click **Search**. The **Found** table displays the resulting privileges. Check **Customer Newsletter Group**, **Customer Newsletter Permission**, **Customer Newsletter Role** to select them and then click **Add**. All of the selected privileges are added to the **Selected** table.
- You can use the **Preview** feature to quickly check whether the filtering criteria you have just configured actually deliver the expected results. Note that the Row limit field restricts the number of results displayed in the Preview report. You can open the preview PDF in the browser or save it for later examination.
- Click **Finish** to stop adding new reports to the file.
- Enter the report file name in **File Name** and a description of it in **Description** and then check that **PDF** is selected in **Format**.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the Schedule tab, choose **As soon as possible**.
- In the Send to tab, enter your email address in **To**. You can also fill in the message **Subject** and **Body**.
- Click the checkbox next to Active to activate the report set. The icon in the top right corner changes to ⏻.
- Click **Save** to save your changes to the report set and run the report. You should receive the report as an email attachment. Open it and check the users assigned to the **Customer Newsletter** group, permissions and role.

You can also create a report that shows all of the privileges assigned to a selected user. Now we'll add this kind of report to the report set we just created:

- In the Reports tab, open the report set you just created for editing.
- Click ➕ to add a new report file.
- In the list of available reports, click on **Changes on User to Privilege Assignments by User** in the list to select it.
- In the **When** section in the report scope dialog, select **Any time**.
- In the **Users** section, select **Last Name** in **Identifying Attributes** and **Farfello** in **Attribute Value** and then click **Search**.

- Check **Farfello Nico** and then click **Add** to move this user to the **Selected** table.
- Click **Finish**. Enter the report file name in **Name** and then click **Save**. You should receive an email with two report files. In the second report, you can see all of the privileges assigned to **Farfello Nico**.

2.2. Analyzing the Addition of a New User

In the exercises described in the section "Adding a New User" in the *DirX Identity Tutorial*, the following tasks were performed:

- The user **Teacher Mark** was created as a contractor.
- The user **Teacher Mark** was manually assigned the **Trainer** privilege.
- The user **Teacher Mark**'s password was reset.
- The user **Teacher Mark**'s privilege assignments were approved.
- The user **Teacher Mark** was added to a project.
- The user **Teacher Mark** was assigned some privileges based on rules.
- The user **Teacher Mark** was assigned the **Internal Employee** role.

The user **Teacher Mark** was also assigned the **Test Tasks** privilege for a limited period of time because of later changes initiated in the DirX Identity tutorial.

This section shows you how to analyze this DirX Identity user entry data. It describes how to:

- Examine a user creation
- Analyze a user to privilege assignment

Here, auditors want to answer the same questions as for the previous case concerning new users. They also want to know: Were there any new or modified project assignments and what was their root cause? Were there any password changes and with what outcome?

2.2.1. Examining the User Creation

One way of creating a new user in DirX Identity is with Web Center, which is controlled by a request workflow. All data is collected during the workflow steps and is kept as orders at the workflow instance. The ApplyChange operation of this kind of workflow creates the user entry in the Identity Store. The operation AddObject creates a new object (User, Account, Workflow instance) in the directory or database.

In this section, we'll investigate the user creation for **Teacher Mark** with the Dashboard view and Audit analysis and see how the new user and its attributes are displayed in the History view.

2.2.1.1. Examining the User Creation in the Dashboard

To examine Mark Teacher's user creation from the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **Total audit events by month and operation** component.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**, select the **What – Type** dimension and then enter **User** in **Value**.
- Click **OK**. The chart is recalculated.
- Drill down to audit events of the Add Object operation for September 2022. Order the table by the **When** column in ascending order. You can see the list of all newly created users. The second one is **Teacher Mark** (check the column **What Details** User='Teacher Mark').
- When you open the details of this event, you can find out in the **Who** section that it was **Taspatch Nik** who performed this action. The **Context Event** section shows that the cause was the **Add WorkflowService** event.
- Close the details window and then click  to return to the Dashboard view.

2.2.1.2. Examining the User Creation in the Audit analysis

To analyze Mark Teacher's user creation with the Audit analysis:

- Select the Audit analysis tab in the DirX Audit Manager main page.
- In **Source**, select **DirX Identity**.
- In **Type**, select **on request**.
- In **Operation**, select **Add Object**.
- In **What type**, select **User**.
- Click **Search** and then order the table by the **When** column in ascending order. You can see the list of users created on request: the first one is **Farfello Nico** and the second one is **Teacher Mark**. The others are users and personas from other tutorial steps and will be explained in the later sections of this tutorial.
- Click the context event icon  for one of the events. You can see a chain of messages connected to the customer self registration process. The list of contextually related events can be also accessed from a dashboard drilldown list of events we explored in the previous exercise.

2.2.1.3. Examining the User Creation in the History View

To view the new user **Teacher Mark** and his attributes in the History view:

- Click the History tab in the DirX Audit Manager main page.
- In **Type**, select **User**.
- Click the **Advanced Search** icon .
- In **Name**, type **Teacher Mark**.
- Click **Search**. Because only one user with the name **Teacher Mark** is found, the Attribute tab on the details page for this user is opened. You can see the history of changes for this user. Because Teacher Mark changed from the **Contractor** role to the **Internal Employee** role, you can see the attribute changes marked in the timeline (if you see only one timeline with cumulative information you must zoom in to the day level) and in the attributes table below.
- Double-click in the timeline near 18 October to add another comparison time point marker.
- Check **Show changes only**.
- Browse the Roles, Permissions, Groups and Accounts tabs and explore the changes described in the section "Adding a New User" in the *DirX Identity Tutorial*.
- On the Events tab, set **From** to **1/9/2022** and **To** to **31/10/2022** and then examine the events messages for **Teacher Mark**.

2.2.1.4. Examining the User Creation with Reports

Now we'll examine Teacher Mark's user creation events by creating some reports:

- Click the Reports tab in the DirX Audit Manager main page.
- Add a new Report set and fill in the report set's **Name** and **Description**.
- Click to add a new report file.
- Either browse through the list of available reports or use name completion (start typing a part of the report name) or tag filtering (tag History) to display the **Users in Organizational Unit** report. Click on it in the list to select it. The Report scope dialog opens to define the parameters of the report.
- The report is created for one date. Select the current date by selecting **Custom time point**.
- In the **Organizational Units** section, select **ou** in **Identifying Attributes** and **Professional Services** in **Attribute Value**. Click **Search**.
- Select **Professional Services** and click **Add**. The name is added to the **Selected** table.
- Click **Finish** to stop adding new reports to the file. Enter the report file name in **File name** and select the format (PDF is preferred).
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the **Schedule** tab, set its schedule to run **As soon as possible** and check **No end time**.
- In the **Send to** tab, enter your email address.

- Activate the report and then save it.

Open the report attachment in the email you received. It shows all of the users from the **Professional Services** business unit. You can check their roles, permissions and accounts. The state is taken from the date set in the **When** section. For this example, it was the state of the last synchronization.

You can also run the report with its date set to a point in the past to view the user status and assignments that correspond to that time point in the history:

- Go back to the Reports tab.
- Click in the display of the report set you just created to open it for editing.
- Click in the **Users in Organizational Unit** row to edit this report's scope.
- In **When**, select **Custom time point** and change the date to **4/10/2022**.
- Click **OK** and then click **Save**.

Once you receive the second report, you can check the report date in the header section and examine the assignments of **Teacher Mark**. The FS Professional Services and Software Tests groups are now missing because they were only assigned later - on 4/10/2022 and 11/10/2022 respectively. This report now presents all users and their assignments as they were on the selected date 4/10/2022.

If you want to see all created users and the data related to their creation, use the **Contextually Related Changes for the Selected Causing Operation and Type** report:

- In the Reports tab, add a new report set and fill in the report set's **Name** and **Description**.
- Click to add a new report file.
- Click on **Contextually Related Changes for the Selected Causing Operation and Type** in the list of available reports.
- In the **When** section, select **Custom time** and then set the interval **From** to **1/9/2022 01:00 AM** and **To** to **27/9/2022 01:00 AM**.
- In the **Operation** section, select **Add Object**
- In the **Type** section, select **User**.
- Click **Finish** to stop adding new reports to the file. Enter the report file name in **File name** and then select the format (PDF is preferred).
- Click **OK**. The report file is inserted into the report set and it is displayed in the file list.
- In the **Schedule** tab, set the report set schedule to run **As soon as possible**, check **No end time** then and enter your email address in the **Send to** tab.
- Activate the report set and then save it.

You should receive an email with the report file. Open the attachment. You can see the user creations for **Teacher Mark** and **Farfello Nico** and related events. The filter Add Object + User is applied to the initial and related events so that's why the chain starts with the workflow event (which is the initial event).

Note that if you don't restrict the date and create the report using **Any time**, you'll obtain the overview of all users created during the DirX Identity tutorial run.

2.2.2. Analyzing User to Privilege Assignments

Assigning privileges enables a user to access specific resources in connected systems. In this section, you'll learn several ways to evaluate privilege assignments and learn how to create reports to analyze the privilege assignments made with the "Adding a New User" DirX Identity tutorial.

2.2.2.1. Analyzing User Privilege Assignments with the Dashboard

To analyze user privilege assignments from the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if it's not already selected.
- Examine the **Total audit events by month and operation** component.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**, select the **What – Type** dimension and then enter **User to Role** in **Value**.
- Click **OK**. The chart is recalculated.
- Drill down to audit events of the Add Assignment operation for September 2022. Change **Items per page** to **50**. Order the table by the **When** column in ascending order.
- You will find several audit events on assigning privileges to the users **Farfello Nico** and **Teacher Mark**. You can view the details of these audit events with the  and  icons. In the **What Details** column, you can see which role was assigned.
- Click  to return to the Dashboard view.

2.2.2.2. Analyzing User Privilege Assignments with the Audit analysis

To analyze user privilege assignments with the Audit analysis:

- Select the Audit analysis tab in the DirX Audit Manager main page.
- In **Source**, select **DirX Identity**.
- In **Operation**, select **Add Assignment**.
- In **What**, enter **Teacher Mark**.
- Click **Search**. You should receive seven (7) audit events in the result list on assigning Mark Teacher to several privileges.

2.2.2.3. Analyzing User Privilege Assignments with Reports

Now you'll examine the user privilege assignments from the Reports view:

- In the Reports tab, choose and then open one of the report sets you created in other exercises for editing.
- Click  to add a new report file.
- Click on **Changes on User to Privilege Assignments by Privilege** in the list of available reports to select it.
- In the **When** section, select **Any time**.
- In the **Privileges** section, select **Name** in **Identifying Attributes** and **Test Tasks** in **Attribute Value**. Click **Search**.
- Check the **Test Tasks** permission and role and then click **Add** to copy them to the **Selected** table.
- Now type **Sales Tasks** in **Attribute Value**. Click **Search**.
- Check both the **Sales Tasks** permission and role and then click **Add** to copy them to the **Selected** table.
- Click **Finish**, enter the report name in **File name**, select the format and then click **Save**.

When you receive the report, you'll see an overview of all users to whom the **Test Tasks** and **Sales Tasks** privileges were assigned.

2.3. Checking Imported Users

In the exercises described in the sections "Importing Identities" and "Changing the Workflow Configuration" in the *DirX Identity Tutorial*, the following tasks were performed:

- Importing nine users from the **New-HR** domain (Gross Berta, Dyson Mark, Hoegeli Michel, Huber Fritz, Binder Horst, Banzoi Miriam, Bader Hans, Karrer Antonie, Berchtold Max)
- Adding these users to the **Product Testing** organizational unit
- Assigning **Internal Employee** and **Test Tasks** roles
- Assigning the **Signature Level 1** permission by the rule
- Assigning **Intranet Portal**, **MVS**, **Signatures** and **Windows Domain Europe** target systems groups
- Creating accounts in the **Intranet Portal**, **MVS** and **Windows Domain Europe** target systems
- Changing the **Description** and **Manager** attributes for users imported from **New-HR**

This section shows you how to analyze the DirX Identity data created by these tasks. It describes how to:

- Examine a role with Audit analysis
- View the attributes changes of a user with the History view

- View accounts with the Dashboard
- View the accounts created in target systems with reports

In this case, an auditor might be curious about the following items: What users were imported from the connected system and which privileges were they assigned afterwards? You can see that the first password setting was assisted after the initial insertion of Teacher. The second audit event was initiated from a self-service password change.

2.3.1. Examining a Role

You can check which of the audited events relate to a specific role. Let's see what happened with the **Test Tasks** role. First, we'll analyze it with Audit analysis:

- In the DirX Audit Manager main page, click the Audit analysis tab.
- In **Source**, select **DirX Identity**.
- In **What Detail**, enter **Test Tasks** (or **%Test Tasks%** if you have not enabled full text search in the Configuration Wizard).
- Click **Search**. You can see the list of users assigned to the **Test Tasks** role. You can change **Items per page** to **50** to view all of them at once.
- To see the complete chain of user creation and assignment to the role, click  on one of the imported users to view the related events; for example, **Gross Berta**.
- Check the message **Add Object, User = 'Gross Berta'**. You can see that this user was created on schedule (**Type** column), which means that an automatic procedure created the user. In our case, it was the import workflow for **New-HR**.

2.3.2. Reviewing User Attribute Changes

Now we'll use the History view to analyze the user attributes changes:

- In the DirX Audit Manager main page, click the History tab.
- In **Type**, select **User**.
- Click the **Advanced Search** icon  .
- In **Name**, enter one of the **New-HR users**; for example, **Banzoi Miriam**.
- Click **Search**. Because only one user with the name **Banzoi** was found, the details page for this user is displayed with the Attributes tab table open by default. Now you can see the history of changes for this user.
- Check **Show changes only** to display only those attributes where a change has occurred in the displayed time range. You can see that the **Manager** and four (4) risk attributes were changed.
- To identify the **New-HR** source, uncheck **Show changes only** and look at the **dxmOprMaster** attribute. You can use the search field in the Attribute Name column to find this parameter quickly.
- Click the **Switch to search form** button to return to the Search page. Now check the other **New-HR** users, like **Karrer Antonie**, **Binder Horst** and so on.

2.3.3. Exploring the Accounts

Users can use a Dashboard component to analyze the accounts creation in the target systems. In this step, you'll create a new Dashboard component. Later on in this session, you'll use this component as a template, change the Fact table and save it under a new name to assign it to a report.

- In the DirX Audit Manager main page, select the Dashboard tab.
- Click  in the **Total audit events by month and operation** component toolbar to open the Edit component dialog.
- Click the **Data** tab if it is not already selected.
- In **When**, select **Custom time** and then set **From** to **1/9/2022** and **To** to **30/9/2022**.
- In **Fact Table**, select **Memberships**.
- Set **Facts** to **Succeeded**.
- Set **Dimensions** to **Day** and **Target System**.
- Check the Dimension filter, select **Operation** in **Name** and enter **Add Assignment** in **Value**.
- Click **Save as ...**.
- In the pop-up window, enter the **Component title** as **Accounts to group by target system created in September 2022**. In **Component name**, enter **accounts_to_group_by_target_system**.
- Uncheck **Public** to prevent others from using your component and leave **Add to dashboard** checked with **instead of existing** selected.
- Click **Save**. The saved chart and modified Dashboard component are displayed. You can see how many accounts were created and in which target system. Drill down individual parts of the bar to see details about the accounts.

2.3.4. Examining the Account-Group Memberships

Now we'll analyze the account-group memberships for the imported users with reports.

First, we'll create a report that provides an overview of the accounts created in the target systems:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set, name it **Accounts by Target Systems** and add a description for it.
- Add a new report file and select **Changes on Account to Group Memberships by Target System**.
- The Report scope dialog opens for you to define the parameters of the report. In the **When** section, select **Custom time** and set **From** to **1/9/2022** and **To** to **30/9/2022**.
- In the **Target Systems** section, you can define the sources that act as filtering elements for the events for which you want to see data. In **Identifying Attributes**, choose **Target System** and then click **Search**.

- All of the available target systems are displayed in two pages. On each page, click +/- to select all of the available target systems and then click **Add** to move them to the **Selected** table. Navigate to the next page and then repeat this step.
- Make sure you change the default **Record limit** value from **100** to **0** (indicating there is no limit) to include all memberships in the report. Leaving the default value means that you will receive an incomplete/limited report.
- Click **Finish** to stop adding new reports to the file. Name the report file **Accounts in target systems for September 2022** and leave PDF selected as the format.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the **Schedule** tab, set the report set schedule to run **As soon as possible**, check **No end time** and then enter your email address in the **Send to** tab.
- Activate the report and then click **Save**.

Open the report attachment in the email you receive. You'll see a list with the newly created accounts sorted by target systems.

You can enhance this report by adding the **Accounts by target system created in September 2022** component to the end of the report. We'll perform this task next:

- In the DirX Audit Manager main page, click the Reports tab.
- Click to edit the **Accounts by Target Systems** report set.
- Add a report to the report file with the name **Accounts in target systems state for September 2022** by clicking  next to the report name.
- The report selection dialog opens. Select **Generate dashboard chart** from the list.
- In the **Data source** tab select **accounts_to_group_by_target_system**.
- Click **Finish**. Remember that having two reports in one file is allowed only for report files in PDF format. Click **Save**.
- Open the report attachment you received in the latest email. First, there is a list of accounts in the target systems as in the previous example and at the end, you can find the chart with the overview of accounts by days in September 2022.

2.4. Analyzing Imported Accounts

In the exercises described in the section "Setting up a New Target System" in the *DirX Identity Tutorial*, the following tasks were performed:

- Loading the accounts and groups from the **New-LDAP** target system to the Identity Store
- Creating a new **Firmware Tests** permission
- Creating a new **Firmware Tests** role
- Assigning the **Firmware Tests** role
- Deleting the unassigned accounts (**Derksen Konrad**)

This exercise shows you how to analyze the DirX Identity accounts, permissions and roles created by performing these tasks. It describes how to:

- Check the imported account-to-group memberships with a target system report
- Examine a permission creation with the Audit analysis and the Dashboard
- Examine a role creation with the Audit analysis and the Dashboard
- Study users assigned to a role with the Dashboard and the History view
- Explore a specific connected system's provisioning activities

These steps will help to answer the following auditor's questions: What provisioning activities were performed in the new target system? Are there any new imported accounts in any of the monitored target systems? What was changed for the Firmware Tests permission and role? To which users was the Firmware Tests role assigned?

2.4.1. Examining Permission Creation

In this part of the exercise, we'll examine the permission creation events associated with the imported accounts.

First, we'll do it with Audit analysis:

- In the DirX Audit Manager main page, select the Audit analysis tab.
- In **Source**, select **DirX Identity**.
- In **What**, enter **Firmware Tests**.
- Click **Search**.
- Change **Items per page** to **20**. Order the table by the **When** column in ascending order.

You can see audit events with the **Add Assignment** operation for three (3) users from the **New-LDAP** target system. You can also see the **Add Assignments User to Role** operation for the same three of these users. You can also see the **Delete Assignment Account to Group** operation for two users (Derksen Konrad and Zeller Andreas) and several **Firmware Tests** group updates.

Next, we'll do it with the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **DirX Identity total history entries by month and entry type** component. This component provides an overview of all history entries sorted by entry types and their total numbers changing over time.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**.
- In **Name**, select **Entry type**.

- In **Value**, enter **Permission**.
- Click **OK**. The chart is recalculated.
- You can now see the number of permissions for individual months. You can also drill down to the permission list to view all permissions active in the given time period, including the new ones.
- Click to return to the Dashboard view.

2.4.2. Examining a Role Creation

During the DirX Identity tutorial, a validation workflow from the **New-LDAP** target system is started that imports the **Firmware Tests** group. Later on, a permission and a role are created and the group is linked to the permission. Let's view these actions in Audit analysis.

First, we'll use Audit analysis to analyze the privilege hierarchy:

- In the DirX Audit Manager main page, select the Audit analysis tab.
- In **Source**, select **DirX Identity**.
- In **What**, enter **Firmware Tests**.
- In **What Type**, enter **Role**.
- Click **Search**.

You can see just one **Firmware Test** role which was created manually.

Now let's examine the role creation with the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab.
- Examine the **DirX Identity total history entries by month and entry type** component.
- Click to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**.
- In **Name**, select **Entry type**.
- In **Value**, enter **Role**.
- Click **OK**. The chart is recalculated.
- You can now see the number of roles for individual months and their increase in October 2022. Drill down to October 2022 and look at the end of the list. Here you can see the **Firmware Test** role created on 5/10/2022.
- Click to return to the Dashboard view.

2.4.3. Studying the Users Assigned to a Role

In this part of the exercise, we'll examine the users assigned to the **Firmware Test** role.

First, we'll examine it with the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab if not already selected.
- Examine the **DirX Identity user to privilege assignment total audit events by month and activity** component.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Change first field **Dimensions** to **Day**.
- Change the second field **Dimensions** to **What-Type**.
- Check **Dimension filter**.
- In **Name**, select **Operation**.
- In **Value**, enter **Add Assignment**.
- Click **OK**. The chart is recalculated.
- Drill down to the **User to Role** assignments on 5/10/2022. You can see three (3) users assigned to the **Firmware Tests** role. Drill down to the **User to Role** assignments on 11/10/2022 and there is one user assigned to the **Manager** role.

Now let's analyze all users assigned to the Firmware Tests role with Audit analysis from where we will move to the History view, directly to the Firmware Tests entry details view:

- In the DirX Audit Manager main page, select the Audit analysis tab.
- In **Source**, select **DirX Identity**.
- In **What**, enter **Firmware Tests**.
- In **What Type**, enter **User to Role**.
- Click **Search**. We can see three **Add Assignment** events for the users **Binder**, **Dyson** and **Karrer**. This view gives us the opportunity to see the details of the assignment operations and move directly to the History view.
- Open the details of any one of the three events.
- Expand the **What [Role : Firmware Tests]** by clicking the gray bar in the details pop-up.
- Click the underlined link **Firmware Tests**.
- The History tab with the Attribute tab table opens for the **Firmware Tests** role. In the data area, click the Users tab. You can see the list of assigned users and their assignment validity.

2.4.4. Exploring Connected System Provisioning

In this part of the exercise, you'll inspect all of the provisioning activities that have occurred on a specific connected system; in this case, the **New-LDAP** target system:

- First, you'll examine the target system from the Dashboard view
- Next, you'll examine the accounts created in the target system from the Reports view

2.4.4.1. Exploring the Connected System from the Dashboard

First, you will check a specific connected or target system with the Dashboard.

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **DirX Identity total audit events on accounts by month and operation** component. It contains aggregated data from different operations.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Check **Dimension filter**.
- In **Name**, select **Target System**.
- In **Value**, enter **New-LDAP**.
- Click **OK**. The chart is recalculated.
- You can see the overview of operations performed on the **New-LDAP** connected system. Drill down to the **Add Object** section and you can see the list of accounts imported from the connected system.
- Click  to return to the Dashboard view.

2.4.4.2. Exploring the Target System Accounts with Reports

Now we'll generate a report that shows the accounts that were created in the **New-LDAP** target system:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set and give it a name (in **Name**) and a description (in **Description**).
- Add a new report file and select **State of Accounts by Target System** from the list of available reports.
- The Report scope dialog opens for you to define the parameters of the report. In the **When** section, select **Custom time point** and leave the default date.
- In the **Target Systems** section, you can define the sources that act as filtering elements for the events for which you want to see data. In **Identifying Attributes**, choose **cn** and then click **Search**. All available target systems are displayed. Check **New-LDAP** to select it and then click **Add**. The target system is added to the **Selected** table.
- Click **Finish** to stop adding new reports to the file. Name the report file and select the format.

- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the **Schedule** tab, set the report set's schedule to run **As soon as possible** and check **No end time**.
- In the **Send to** tab, enter your email address.
- Activate the report and then click **Save**.

Open the report attachment in the email you receive. You can see all of the accounts that have been imported to the **New-LDAP** target system with all of their status changes shown as individual entries.

2.5. Auditing SoD Violations

In the exercises described in the section "Applying SoD Policies" in the *DirX Identity Tutorial*, the following tasks were performed:

- SoD checking was activated.
- A SoD policy was activated.
- A conflicting privilege was assigned to the user **Pitton Lavina**.

This exercise shows you how to analyze a breach of a SoD policy and how to audit the assignment of SoD violations in DirX Identity. It describes how to:

- Check the SoD violation with the Dashboard view
- Use the Reports view to create a SoD violation overview report

This exercise answers the following auditor questions: Did any user assignment break the configured Segregation of Duties rules? Which report can provide a regular overview of SoD violations?

2.5.1. Analyzing a SoD Violation with the Dashboard View

Let's first examine the SoD violation with the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **DirX Identity total history SoD violation entries by month** component. This component is based on history data.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Click **OK**. The chart is recalculated. You can see an SoD exception that occurred in October 2022.
- Drill down to October 2022. In the **Name** column, you'll find the name **Pitton Lavina** as the user who has incurred an SoD violation. In **dn**, you can see the rule that was violated: the user was assigned both the **Contractor** and **Manager** roles, which is against the SoD policies defined in the **My-Company** scenario.

2.5.2. Analyzing SoD Violations with Reports

Next, we'll use a context report to set up and generate an overview of SoD violations. A context report allows you to filter the events and their context and display just the filtered operations. To create the context report with the appropriate filter settings for generating the SoD exception overview:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set and then name it and describe it in **Name** and **Description**.
- Add a new report file and then select **Risk Users by Simple Risk** from the list of available reports.
- The Report scope dialog opens for you to define the report's parameters. In the **When** section, select **End of Previous Day**.
- Leave the **Attribute** fields as they are.
- In the **Risk factor** section, select **SoD violations**
- Uncheck **Create short report**.
- Set **Record limit** to **0**.
- Click **Finish** to stop adding new reports to the file. Name the report file and select the format.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the **Schedule** tab, set the report set's schedule to run **As soon as possible** and check **No end time**.
- In the **Send to** tab, enter your email address.
- Activate the report and then click **Save**.

In the email attachment you receive, check the overview of all users based on their SoD violations risk level. In the DirX Identity tutorial exercise, only one rule was broken. In the report, you can check the initiator (author) of the exception and the rule (this information is taken from context).

2.6. Exploring Certification Campaigns

In the exercises described in the sections "Certifying a Role" and "Certifying a User" in the *DirX Identity Tutorial*, the following tasks were performed:

- Creating and running a role certification on the **Trainer** role
- Creating and running a user certification on two specific users

This section shows you how to analyze a certification campaign for re-approving a privilege or a user. It describes how to:

- Analyze the certification campaign status in the Dashboard view
- Set up and run one of the reports that identify available certification campaigns

In this exercise, the auditor will inspect the audited certifications and ask: How many certification campaigns took place? With what results? Who were the approvers? Are there still any unfinished certification campaigns?

2.6.1. Exploring Certification Campaign Status with the Dashboard

First, you'll use the Dashboard view to examine certification campaign status:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine two cpmponents: the **DirX Identity total history certification campaign entries by month and state** and **DirX Identity total history certification campaign entries by month and lifecycle state**.
- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.
- Click **OK**. The chart is recalculated. Both certification campaigns are now displayed according to their statuses.
- Drill down to the chart bar for October 2022 in both charts. You can see that the drill down results are the same.
- Click the **Tutorial Privilege Certification** link and study the History details page with the campaign data.
- Then return to the Dashboard tab and click the **Tutorial User Certification** link.
- The certification campaign's history details page is displayed with the Overview tab table open by default, where you can view the details for the campaign. You can check the privileges' names, the certification campaigns end and start dates and the certification result - results are displayed in the **Tutorial User Certification** history details page.

2.6.2. Examining Certification Campaigns with Reports

Now we'll set up and run a report that identifies certification campaigns:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set and then name it and describe it in **Name** and **Description**.
- Add a new report file and then select **Certification Campaigns** from the list of available reports.
- The Report scope dialog opens for you to define the report's parameters. In the **When** section, select **Any time**. Choose the empty selection option in both the Type and State selection boxes to take all certification campaigns into account.
- Click **Finish** to stop adding new reports to the file. Name the report file and select the format.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.

- In the **Schedule** tab, set the report set's schedule to run **As soon as possible** and check **No end time**.
- In the **Send to** tab, enter your email address.
- Activate the report and then click **Save**.

Open the report attachment in the email you receive. You can see both available certification campaigns overview and you can check the accepted and rejected users of the respective privileges.

2.7. Investigating an Assignment of Physical Access

In the exercise described in the section "Using Manual Provisioning" in the *DirX Identity Tutorial*, the physical access to **Munich-Archive** was assigned to the user **Sedran Bill**. This section shows you how to analyze physical access assignment. It describes how to:

- Analyze a manual privilege to user assignment in the History view
- Set up and run a report on user-to-privilege assignment

In this exercise, the auditor is curious about: What privileges were assigned to Sedran Bill and when? What was the reason for the assignment? To which users was the Munich – Archive role assigned?

2.7.1. Investigating the Physical Access Assignment with the History View

First, we'll look at the manual privilege-to-user assignment in the History view:

- In the DirX Audit Manager main page, click the History tab.
- In **Type**, select **User**.
- Click the **Advanced Search** icon .
- In **Name**, enter **Sedran Bill**.
- Click **Search**. There are two results available. Choose the first one, not the functional user entry.
- The details page with the Attributes tab table opens for **Sedran Bill**.
- On the Accounts tab, you can see that the Physical Access account for **Sedran Bill** was created.
- Click the Roles tab and check that the **Munich – Archive** role was assigned manually.
- Now click next to the **Munich – Archive** role name to find the reason for the manual assignment. This action opens the Assignment cause tab, which displays audit events that caused the selected privilege.
- The Assignment cause tab shows that the Request Add assignment was the causing event. Click next to it to expand the related events to view the entire chain of events leading to the assignment of the privilege. You can also view other privileges causes, but the events for other privileges are not a part of the sample data set so you will not see any causing messages for other privileges of **Sedran Bill**.

- Click the Events tab next to the Risks tab. Set **From** to **1/9/2022** and **To** to **31/10/2022**.
- You can see one event: **Add Assignment** of **Sedran Bill** to the role.
- We can also view all events triggered by **Sedran Bill**. To do this step, switch the **Search in** selection box to **Who**.
- Now you can see six events where **Sedran Bill** is the requester (initiator).

2.7.2. Investigating the Physical Access Assignment with Reports

Now we'll set up and generate a report that shows the user-to-privilege assignment:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set and gives it a name (in **Name**) and a description (in **Description**).
- Add a new report file and select **Changes on User to Privilege Assignments by Privilege** from the list of available reports.
- The Report scope dialog opens for you to define the parameters of the report. In the **When** section, select **Any time**.
- In the **Privileges** section, select **Name** in **Identifying Attributes**, select **Munich - Archive** in **Attribute Value** and then click Search. Check **Munich - Archive** and then click **Add** to move the attribute to the **Selected** table.
- Click **Finish** to stop adding new reports to the file. Name the report file and select the format.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the Schedule tab, set the report set's schedule to run **As soon as possible** and check **No end time**.
- In the **Send** to tab, enter your email address.
- Activate the report and then click **Save**.

Open the report attachment in the email you receive. You can see the list of users assigned to the selected privilege. In our example, only **Sedran Bill** is assigned. You can also check when the assignment was created, its outcome and the type of assignment.

2.8. Auditing Tickets

In the exercise described in the section "Working with Internal Tickets" in the *DirX Identity Tutorial*, a ticket for user attributes changes was created. The following change was processed:

- Changing the **Title** attribute for Leo Kubalke with an internal ticket.

In this section, you'll learn how to use DirX Audit Manager to examine these tickets, including how to:

- View audit events for a ticket in Audit analysis
- Check the user modifications generated by the ticket in the History view

In this exercise, the auditor will want to know: What changes were triggered by tickets and when?

2.8.1. Auditing Tickets with the Audit analysis

To analyze the tickets with the Audit analysis:

- In the DirX Audit Manager main page, select the Audit analysis tab.
- In **Source**, select **DirX Identity**.
- In **What Detail**, enter **Ticket** (or **%Ticket%** if you have not enabled full text search in the Configuration Wizard).
- Click **Search**. You can see two ticket audit events for Leo Kubalke. However, even when you click **Show detail**, you can't identify the attribute change that was made by the ticket. To obtain this data, we'll continue the analysis of these attribute changes with the History view.

2.8.2. Auditing Ticket-Generated Attribute Changes with the History View

Now we'll use the History view to look at the user modifications made as a result of the ticket initiation:

- In the DirX Audit Manager main page, click the History tab. Alternatively, we could have used the link tin the ticket event details to directly open the History details page of the user Kubalke.
- In **Type**, select **User**.
- Click the **Advanced Search** icon  .
- In **Name**, enter **Kubalke**.
- **C**lick **Search**. Because only one user with the name **Kubalke** was found, the details page for this user is opened and the Attributes tab table is displayed.
- Change the comparison time point marker associated with the first column of data:

  click on the date in the column header marked as  . Now change the date to **25/10/2022 12:00 AM**.
- Check **Show changes only** to display only those attributes that changed in the time range you selected. You can see, apart from several changed risk attributes, also the line where the **Title** attribute changed from empty to **Dr**.

2.9. Analyzing Personas and Functional Users

In the exercises described in the sections "Managing Personas" and "Managing Functional Users" in the *DirX Identity Tutorial*, the following tasks were performed:

- A new user **Smith John** was created.
- Two personas for **Smith John** were created with the suffix **Psn** and **EN-7716 P** by the user **Taspatch Nik**.
- A new functional user **Trainee for the Human Resources department** was created for the user **Berner Hans**.

In this section, you'll use DirX Audit Manager's History view to examine these changes. You'll learn how to:

- Analyze a persona with the History view
- Analyze a functional user with the History view

This exercise will answer the auditor questions: What is the status of the persona created for **Smith John**? What properties does the functional user **Trainee** for the **Human Resources department** have?

2.9.1. Analyzing Personas with the History View

DirX Audit Manager displays a persona as a user with specific attributes. To search the History database for the personas created for the user **Smith John**:

- In the DirX Audit Manager main page, click the History tab. Alternatively, you can click **Switch to search form** to return to the Search page if you are proceeding directly from the previous exercise with the History view.
- In **Type**, select **User**.
- Click the Advanced Search icon  .
- In **Name**, select **Smith**.
- Click **Search**. Three users are found with the name **Smith**. The users marked as **Psn** and **EN-7716 P** are personas. These suffixes were defined when the personas were created as part of the DirX Identity tutorial exercise.
- Click  to open the details page for **Smith John Psn**.
- In the Attributes tab, navigate to the second page of the attributes table. Here you can identify the persona object by the **objectClass** attribute value **dxrPersona**. The user for whom the persona was created is displayed as the value of the **owner** attribute.

2.9.2. Assessing Functional Users with the History View

You can analyze a functional user in the History view in much the same way as you did it for a persona:

- In the DirX Audit Manager main page, click the History tab. Alternatively, you can click **Switch to search form** to return to the Search page if you are proceeding directly from the previous exercise with the History view.
- In **Type**, select **User**.
- Click the Advanced Search icon .
- In **Name**, select **Trainee**.
- Click **Search**. Four users are found with the name **Trainee**. All of them are functional users.
- To verify your finding, click to open the details page for one of these users.
- In the Attributes tab, you can identify the functional user object by the **objectClass** attribute value **dxrFunctionalUser**.

2.10. Observing Web Center Logins

During the course of following the DirX Identity tutorial exercises, several different users logged in and out of the DirX Identity Web Center application. These events are logged and stored in the DirX Audit database.

This exercise demonstrates how to use DirX Audit Manager to audit these logins. You'll learn how to:

- View login activity with the Dashboard view and with Audit analysis
- Set up and run reports that show information about separate login actions and an overview of succeeded and failed logins

In this exercise, the auditor will want to know: How many logins into the audited DirX Identity Web Center application were there? Who logged in and when? How many login failures were there? Do users mostly log out manually or are they logged out due to the session timeout? What authentication types are used for logging in?

2.10.1. Observing Login Activity with the Dashboard View

To view the logins and logouts overview in the Dashboard view:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **Authentication succeeded and failed audit events by month** component.
- Click to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- In **When**, select **Any time**.

- Click **OK**. The chart is recalculated. You can see aggregation logins per month and divided into succeeded and failed.

Next, change the component's dimensions to view the data aggregated by day:

- Click  to open the Edit component dialog.
- Click the **Data** tab if it's not already selected.
- Change **Dimensions** to **Day**.
- Click **OK**. The chart is recalculated.

Now drill down into the data so that you can see the user name and the **What details** column:

- Drill down to the Failed logins for 24/10/2022. There is a list of two (2) failed logins where the **What detail** column contains the text **The user credentials could not be validated by DirX Identity**. These messages originated from the situation when the authentication server was not online.
- Click  to return to the Dashboard view.

2.10.2. Observing Login Activity with the Audit analysis

Both the Dashboard component and the Audit analysis provide overviews of both login and logout events. We can also use the Audit analysis to analyze authentication events:

- In the DirX Audit Manager main page, select the Audit analysis tab.
- In **Source**, select **DirX Identity**.
- In **Operation**, select **Login**.
- Click **Search**. You can see login events from various users, both successful and failed.
- In **Operation**, select **Logout** and then click **Search**. In the list, you can see all recorded logout actions, all of which were successful. All the sample logouts originate from manually logging out when performing the DirX Identity tutorial exercises.

You can also use Audit analysis to view both login and logout operations together:

- In **Operation**, you must click on the **Switch to text input** button next to the Operation and then type **Log** and ignore the Login and Logout suggestions.
- Click **Search**. You now have the complete list of all login and logout actions.
- Change **Items per page** to **20** to get more events into one page.
- You can order the events according to **When**, **Operation**, **Outcome** or **Who** by clicking the respective column header.

2.10.3. Observing Login Activity with Reports

We'll use two different reports to view the Identity Web Center application login activity generated by running the DirX Identity tutorial exercises. The first report with the **Failed only** option can provide a regular overview of login failures.

First, we'll set up and run the logins report:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set and then name it and describe it in **Name** and **Description**.
- Add a new report file and then select **Total Sum of Logins** from the list of available reports.
- The Report scope dialog opens for you to define the report's parameters. In the **When** section, select **Any time**.
- In the **Source** section, select **Name** in **Identifying Attributes** and then click **Search**. Check **DirX Identity** and then click **Add** to copy it to the **Selected** table.
- Leave the default **Failed only** option checked.
- Click **Finish** to stop adding new reports to the file. Name the report file and select the format.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.:
- In the Schedule tab, set the report set's schedule to run **As soon as possible** and check **No end time**.
- In the Send to tab, enter your email address.
- Activate the report and then click **Save**.

Open the report attachment in the email you receive. You can see a list of failed logins grouped by users since we left the default **Failed only** option checked.

Now we'll set up and run the **Total Sum of Logins by Date and Authentication Type** report:

- In the DirX Audit Manager main page, click the Reports tab.
- Either edit the report set you just created create a new one.
- Add a new report file and then select **Total Sum of Logins by Date and Authentication Type** from the list of available reports.
- The Report scope dialog opens for you to define the report's parameters. In the **When** section, select **Any time**.
- In the **Source** section, select **Name** in **Identifying Attributes** and then click **Search**. Check **DirX Identity** and then click **Add** to copy it to the **Selected** section.
- Click **Finish** to stop adding new reports to the file. Name the report file and select the format.
- Click **OK**. The report file is inserted into the report set and is displayed in the file list.
- In the Schedule tab, set the report set's schedule to run **As soon as possible** and check **No end time**

- In the Send to tab, enter your email address.
- Activate the report and then click **Save**.

Open the report attachment in the email you receive. You can see a list of logins grouped by days. There are only manual logins originating from Identity Web Center. At the end of the report, there is a chart with a graphical representation of logins per day and the respective authentication type.

You can also try other login reports; for example, **Total sum of logins by authentication method** and **Total sum of logins by authentication method type** both in the "by day" and "by month" version.

3. Access Auditing

This chapter provides an introduction to auditing with DirX Access as the source of audit messages. You don't need to set up a running DirX Access installation. Instead, we'll work with sample data content that was produced by performing a run through the DirX Access tutorial.

The sections in this chapter will take you through a set of common Access auditing use cases. You need to have a working knowledge of DirX Access in order to understand this section.

3.1. About DirX Access Components

DirX Access consists of a set of components that can deliver audit information. You configure the level of audit information to be delivered in the DirX Access environment (for details, see the DirX Access documentation). The most important DirX Access components with regard to producing audit information include:

- Authentication Service - validates authentication credentials and creates internal subject representations.
- Authorization Service - performs authorization (decision making, subject attribute finder, policy finder).
- Configuration Service - manages persistent configuration objects.
- FederationService - issues SAML tokens.
- PolicyService - manages persistent authorization policies (policy making).
- SSO Service - manages SSO token representation of internal subjects.
- User Service - manages persistent user data.

3.2. Analyzing Access Actions

In these exercises, we'll demonstrate how to analyze information about various user sessions using the Dashboard, Audit analysis, and Report views.

3.2.1. Exploring the Access Audit Trail with the Dashboard

To analyze access actions with the Dashboard:

- In the DirX Audit Manager main page, select the Dashboard tab, if not already selected.
- Examine the **Authentication succeeded and failed audit events by month** component.
- Click  to open the Edit component dialog.
- Click the Data tab if it's not already selected.
- In **When**, select **Any time**.
- Click **OK**. The chart is recalculated. It contains aggregated data for authentication actions from all sources; that is, for DirX Access and DirX Identity in our case.

- Drill down to audit events of the **Failed** authentication action in October 2022. Order the result table by the **When** column in ascending order. We can see several unsuccessful authentication events from various users with different authentication methods. You can use this dashboard component to quickly access a list of failed authentications for a selected period.
- Click to return to the Dashboard view.

Now we'll examine the Authorization succeeded and failed audit events by month component in the same way:

- Click to open the Edit component dialog.
- Click the Data tab if it's not already selected.
- In **When**, select **Any time**.
- Click **OK**. The chart is recalculated.
- Drill down to Succeeded authorization audit events in October 2022. Order the result table by the **When** column in ascending order. The sample messages visible in the drill down represent a collection of AuthorizationServiceDecisionMaking events from the PDP (Policy Decision Point), both Permit and Not Applicable decisions. The Deny decisions are included in the Failed bar of the chart (so they are not visible in the current drill down view).
- Click to return to the Dashboard view.

If you want to see authentication according to the method used to authenticate, you can use the **Authentication total audit events by month and authentication method** component:

- Click to open the Edit component dialog.
- Click the Data tab if it's not already selected.
- In **When**, select **Any time**.
- Click **OK**. The chart is recalculated. This component provides an overview of all authentication methods used in the selected period, which can be useful for identifying the methods most commonly used to authenticate or possibly some exceptional or rarely used methods. There are a number of samples, ranging from Basic and Form to RFC, OAuth and X509 authentications.

3.2.2. Analyzing Access Actions with the Audit analysis

In this exercise, we'll analyze who accessed the audited applications with the Audit analysis:

- Select the Audit analysis tab in the DirX Audit Manager main page.
- In **Source**, select **DirX Access**.
- In **Operation**, enter **Login**.
- Click **Search**. You'll receive 14 audit events in the result table.
- Order the result table by the **When** column in ascending order.

Now we'll use Audit analysis to examine some decisions that the **AuthorizationServiceDecisionMaking** component has made:

- In **Source**, select **DirX Access**.
- For **Operation**, use the **Autocomplete** component for the filter field and enter **Authorization**. You can change the component for value presentation manually by clicking  or  . Note that the autocomplete feature adds suggestion for all available authorization messages: Authorization - Deny, Authorization - Not applicable, Authorization - Permit.
- Click **Search**. You'll receive 10 audit events in the result table. Let's examine one of the messages with the Permit decision in more detail.
- Order the result table by the **Operation** column in ascending order. You'll see some messages with the result **Permit** in the **Operation** column, some with the result **Deny** and others with the result **Not Applicable**. Analyze one of the messages with the result **Permit**.
- Click the Show Details icon to display details of one of the messages with the **Authorization - Permit** operation.
- Expand the **What** area where you can see the resource that the user tried to access.
- The information about the user is stored in the **Who** field.
- Close the details pop-up window.

3.2.2.1. Evaluating Related/Session Events

Next, we'll explore how to display all events from one user session. All of these actions were triggered by the same user in between their logging in and out:

- In **Source**, select **DirX Access**.
- In **Operation**, enter **Login**.
- In **Who**, enter **Willa Sy**.
- Click **Search**. Five login events for **Willa Sy** are displayed.
- Click the Show Related Events icon for the login event with the **InitAuthnForm** in **What Type**. This action retrieves all related events: events which were stored for the same user within the same session; that is, a list of messages with the same subject identifier. Order the result table by the **When** column in ascending order. You will first see the login, then an authorization event, a failed login, and also a logout event.
- Click **Back**.

Tutorial sample data contains related messages only for some events. Other events are taken from different sessions, which means that when you click the Show Related Events icon for other events, only the related session event may or may not be displayed.

3.2.2.2. Exporting Audit Event Data

When you perform a search with Audit analysis, you can export the resulting audit events to a file and/or send it via email. Let's run a report on the results of the search you just ran:

- In the filter definition area, click **Report**. A pop-up dialog opens.
- In **Template**, select **EventMonitorAll**.
- In **Format**, select **PDF**.
- In **Encoding**, select **UTF-8**.
- In **Rows**, type **0** to export all records.
- Click **Export**.

A new tab opens with the list of audit events that correspond to the search criteria.

3.2.3. Reviewing Access Activities with Reports

Finally, we'll create a logins report, which is useful for providing a regular overview of access activities for each user:

- In the DirX Audit Manager main page, click the Reports tab.
- Add a new report set and then name it and describe it in **Name** and **Description**.
- Add a new report file. Enter the **Login** tag in **Tags** or select this tag from the list. This action filters the list of reports to display only the seven login reports.
- Select the **Total Sum of Logins** report from the list of reports by clicking on the name in the list.
- The Report scope dialog opens for you to define the report's parameters. In the **When** section, select **Any time**.
- In the **Source** section, select **Name** in **Identifying Attributes** and then click **Search**. Check **DirX Access** and then click **Add** to copy it to the **Selected** table.
- Uncheck **Failed only** to be able to view both successful and failed logins.
- Click **Finish** to stop adding new reports to the file. Name the report file **Logins by user** and select **PDF** in **Format**.
- Click **OK**.
- In the Schedule tab, set the report set's schedule to run **As soon as possible** and check **No end time**.
- In the **Send** to tab, enter your email address.
- Activate the report and then click **Save**.

Open the attachment in the email you receive and examine the report.

There are six other login reports available: Total sum of logins by date / month and authentication type / authentication method / authentication method type. Try running one or more of these reports (creating, adding, defining and saving them based on the steps you just ran through) to receive more detailed information on logins from the point of view of your selection.

You can notice a difference in event numbers if you compare any login report with the Dashboard chart on authentications. The reason is that the Dashboard chart includes both login and logout events, while reports contain only login events. By default, the Dashboard chart also contains both DirX Identity and DirX Access logins (although you can filter this by using the **Dimension** filter in the respective Dashboard component). We filtered only DirX Access logins for our **Total Sum of Logins** report.

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

EVIDEN

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.