EVIDEN

Identity and Access Management

DirX Audit

Migration Guide

Version 7.2, Edition June 2025

Table of Contents

Copyright ii
Preface 1
DirX Audit Documentation Set 2
Notation Conventions 3
1. Introduction 4
1.1. Migration from DirX Audit 7.1, 7.1 SP1, and 7.1 SP2 4
1.2. Features to be Migrated 4
1.2.1. Issues Relevant for Upgrade from 7.1 to 7.1 SP1 4
1.2.1.1. Audit Messages Database Update 4
1.2.1.2. History Entries Database Update 4
1.2.1.3. Message Broker Upgrade 4
1.2.1.4. DirX Audit Server Upgrade 4
1.2.2. Issues Relevant for Upgrade from 7.1 SP1 to 7.1 SP2 5
1.2.2.1. Audit Messages Database Update 5
1.2.2.2. History Entries Database Update 5
1.2.2.3. Message Broker Upgrade 5
1.2.2.4. DirX Audit Server Upgrade 5
1.2.3. Issues Relevant for Upgrade from 7.1 SP2 to 7.2 5
1.2.3.1. Audit Messages Database Update 5
1.2.3.2. History Entries Database Update 5
1.2.3.3. Message Broker Upgrade 6
1.2.3.4. DirX Audit Server Upgrade 6
2. Migration Procedure 7
3. Preparing the Migration 8
3.1. Archive Error Handling Data 8
3.2. Stop All Message Broker Connections 8
3.3. Archive Custom Data and Stop Services 8
3.4. Prepare the Configuration Database 8
3.5. Prepare the Audit Messages Database 8
3.6. Prepare the History Entries Database 9
3.7. Install the Java VM 9
4. Manual Migration 10
4.1. Migrating Databases from DirX Audit 7.1 to 7.1 SP1 10
4.2. Migrating Databases from DirX Audit 7.1 SP1 to 7.1 SP2 11
4.3. Migrating Databases from DirX Audit 7.1 SP2 to 7.2 11
4.4. Checking Apache Tomcat 13
4.5. Clearing Cached Internet Browser Data 13
4.6. Performing Initial Configuration 13
4.7. Starting Services 13

4.8. Update Scheduled Report Jobs 14
4.9. Update Set of Dashboard Components 14
Legal Remarks 16

Preface

This manual describes the DirX Audit migration procedure from previous versions. It consists of the following chapters:

- Chapter 1 discusses the migration process and describes the concepts.
- Chapter 2 describes the general migration procedure.
- Chapter 3 describes what must be done before you start migration.
- Chapter 4 describes how to perform additional manual migration tasks that are required to complete the migration.

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. Introduction

New customers install DirX Audit according to the *DirX Audit Installation Guide* and work with the product. Existing customers must migrate their environment.

1.1. Migration from DirX Audit 7.1, 7.1 SP1, and 7.1 SP2

Migration from DirX Audit 7.1, 7.1 SP1, and 7.1 SP2 requires you to perform preparation steps and an upgrade installation including the initial configuration and then perform the migration steps described in the next chapters.

The migration procedure consists of the audit messages database (Data DB) update and the history entries database (History DB) update. There are no modifications to the configuration database (Config DB).

1.2. Features to be Migrated

This section provides an overview of the features to be migrated and explains the underlying concepts.

1.2.1. Issues Relevant for Upgrade from 7.1 to 7.1 SP1

This section comprises all issues relevant for version 7.1 only.

1.2.1.1. Audit Messages Database Update

New indexes have been added to the DAT_AUDITMESSAGES and DAT_AUDITEVENTS tables for the SQL Server. No change for Oracle Database.

1.2.1.2. History Entries Database Update

The size of columns in several tables has been extended to be able to store strings up to 850 characters. In addition, the index structure has been improved.

1.2.1.3. Message Broker Upgrade

DirX Audit Message Broker comes with an updated version of Apache ActiveMQ.

1.2.1.4. DirX Audit Server Upgrade

No changes.

1.2.2. Issues Relevant for Upgrade from 7.1 SP1 to 7.1 SP2

This section comprises all issues relevant for version 7.1 SP1 only.

1.2.2.1. Audit Messages Database Update

No changes.

1.2.2.2. History Entries Database Update

The DIM_HST_GEN_DATETIME view has been replaced with a table to improve performance.

A new HDB_APPROVALS table has been added to provide data on approvals realized in DirX Identity.

The FCT_HST_CERTCAMPAIGNS_LIFECYCLE and HDB_CERTCAMPAIGNS_LIFECYCLE tables have been removed. All certification campaign data are provided with FCT_HST_CERTCAMPAIGNS and HDB_CERTCAMPAIGNS tables.

The FCT_HST_IMPORTED_MEMBERSHIPS table has been modified to improve performance.

Other minor improvements and fixes were also made.

1.2.2.3. Message Broker Upgrade

DirX Audit Message Broker comes with an updated version of Apache ActiveMQ.

1.2.2.4. DirX Audit Server Upgrade

DirX Audit Server has been updated with available fixes.

1.2.3. Issues Relevant for Upgrade from 7.1 SP2 to 7.2

This section comprises all issues relevant for version 7.1 SP2 only.

1.2.3.1. Audit Messages Database Update

The database behavior when DAT_AUDITEVENTS records are deleted has been modified for both SQL Server and Oracle Database.

1.2.3.2. History Entries Database Update

Since DirX Audit 7.2, user-to-privilege assignments are synchronized the same way as other entry types. Consequently, the HST_ASSIGNMENTS_IN_TIME table has been removed from the database schema and all its original data will be migrated during the manual migration process. In addition, the HST_ROLEPARAMS_IN_TIME table has been modified to reflect these changes.

The FCT_HST_IMPORTED_MEMBERSHIPS view has been replaced with the table of the same name to improve performance.

The FCT_RSK_COMPOUND_USERS view and RSK_COMPOUND_STATISTICS, RSK_COMPOUND_SCORES, RSK_STATISTICS, RSK_SCORES, RSK_COMPOUND_FACTOR_WEIGHTS, RSK_COMPOUND_FACTORS, RSK_FACTORS, and RSK_LEVELS tables have been removed as DirX Audit risks have been deprecated and only DirX Identity risk data is available.

The HST_ENTRIES table has been modified, the DIRX_ENTRY_UUID column is considered mandatory and unique.

The HST_LDAP_ATTRS table has been extended with a new column TYPE_NAME.

A new HDB_ASSIGNMENTS view has been added to provide data on assignments.

The HDB_ENTRY_OBJECTS view has been removed.

The HDB_ENTRY_ATTRIBUTES, HDB_USER_ROLES, HDB_USER_PERMISSIONS, HDB_USER_GROUPS, HDB_USER_ACCOUNTS, HDB_ROLE_ROLES, HDB_ROLE_PERMISSIONS, and HDB_PERMISSION_GROUPS views have been modified to improve performance.

The HDB_USER_PRIVILEGES view has been added.

Other minor improvements and fixes were also made.

1.2.3.3. Message Broker Upgrade

DirX Audit Message Broker comes with an updated version of Apache ActiveMQ.

1.2.3.4. DirX Audit Server Upgrade

Since the current version, DirX Audit Server is based on Spring Boot technology which has replaced previously-used Apache Karaf technology.

2. Migration Procedure

The general migration procedure is to:

1. Perform the **preparation steps** described in the "Preparing the Migration" section of this document.
2. **Install DirX Audit 7. 2**. DirX Audit 7.1 or DirX Audit 7.1 SP1 or DirX Audit 7.1 SP2 is uninstalled in this step. For details about installation, see the chapter "Installing DirX Audit" in the *DirX Audit Installation Guide*.
3. Perform the manual migration steps described in the "Manual Migration" section of this document.
4. **Configure DirX Audit**. Use the Configuration Wizard for this step and perform both the complete initial Core configuration and the Tenant configuration for each of your tenants. For details, see the "Configuring DirX Audit" section in the *DirX Audit Installation Guide*.
5. Test all DirX Audit components thoroughly to be sure that everything works well.

3. Preparing the Migration

The following step is necessary to prepare the migration:

- Back up the DirX Audit configuration database (Config DB), audit messages database (Data DB) and history entries database (History DB) to be able to reset to the starting point if something goes wrong.

Depending on the features you used, you need to perform the steps described in the next sections.

3.1. Archive Error Handling Data

Archive the DirX Audit Server error handling folder for each of your tenants and keep it empty before starting a new version of the DirX Audit product.

3.2. Stop All Message Broker Connections

Apache ActiveMQ will be upgraded during the DirX Audit 7. 2 installation, so users should make sure that all Message Broker connections have been stopped and that there are no pending messages waiting in individual queues.

3.3. Archive Custom Data and Stop Services

We strongly recommend backing up all configuration- or customer-specific files, especially for the DirX Audit Server configuration, added to the installation folder manually before performing the upgrade. The DirX Audit Server will be upgraded and its structure, configuration files and libraries will change completely.

Stop the DirX Audit services manually, including the Apache Tomcat service if it was used to start the DirX Audit Manager.

3.4. Prepare the Configuration Database

You can use the same configuration database (Config DB) as for DirX Audit 7.1, DirX Audit 7.1 SP1, and DirX Audit 7.1 SP2.

3.5. Prepare the Audit Messages Database

You can use the same audit messages database (Data DB) as for DirX Audit 7.1, DirX Audit 7.1 SP1, and DirX Audit 7.1 SP2. The audit messages database schema will be updated during the migration process.

3.6. Prepare the History Entries Database

You can use the same history entries database (History DB) as for DirX Audit 7.1, DirX Audit 7.1 SP1, and DirX Audit 7.1 SP2. The history entries database schema will be updated during the migration process.

3.7. Install the Java VM

The Java Virtual Machine (Java VM, JVM) is required for the DirX Audit installation. The installation will not start without Java VM installed; instead, it displays an error message indicating that a valid Java VM is missing.

When the installation runs, it prompts you to identify the folder in which the Java VM is installed. Make sure you have an appropriate Java VM installed.

You must also check whether the JAVA_HOME and PATH environment variables are set correctly for your operating system. See the *DirX Audit Release Notes* for supported versions.

If you store your keys in the **cacerts** file, make a backup copy before starting the installation and have it available with the Java VM used for DirX Audit.

4. Manual Migration

This chapter assumes that the DirX Audit 7.2 upgrade installation has successfully started. If you are upgrading from DirX Audit 7.1 or 7.1 SP1 or 7.1 SP2, the Installation Wizard displays the dialog “Manual Migration Steps” with information that you are upgrading from an older version and must execute the manual steps described in this chapter.

At this stage, perform all the relevant steps described in this chapter to update your environment to the new DirX Audit version.

When you are migrating from an older DirX Audit version, you must proceed step by step from the oldest version as described in the following sections. We also suggest consulting the *DirX Audit Migration Guide* for each respective version (available at the Atos support portal) for a more detailed description of changes and updates, including more items than just the list of migration scripts. When migrating from DirX Audit 7.1, you can continue with the section “Migrating Databases from DirX Audit 7.1 to 7.1 SP1”. When migrating from DirX Audit 7.1 SP1, you can continue with the section “Migrating Databases from DirX Audit 7.1 SP1 to 7.1 SP2”. When migrating from DirX Audit 7.1 SP2, you can continue with the section “Migrating Databases from DirX Audit 7.1 SP2 to 7. 2”.

4.1. Migrating Databases from DirX Audit 7.1 to 7.1 SP1

Migrating the databases to DirX Audit 7.1 SP1 consists of migrating the audit messages database schema (Data DB) and the history entries database schema (History DB) for each tenant.

DirX Audit 7.1 SP1 can function with the same audit messages and history entries databases from the previous version, but some database objects must be altered.

- Migrate the audit messages database schema - run the following SQL scripts in your audit messages database (Data DB) server console.

  For SQL Server:
  install_media/**Additions/Scripts/MSSQL/migrate_data_71_71SP1.sql**

  For Oracle Database:
  No action is required.

- Migrate the history entries database schema - run the following SQL scripts in your history entries database (History DB) server console.

  For SQL Server:
  install_media/**Additions/Scripts/MSSQL/migrate_history_71_71SP1.sql**

  For Oracle Database:
  install_media/**Additions/Scripts/Oracle/migrate_history_71_71SP1.sql**

Continue with the steps described in the section “Migrating Databases from DirX Audit 7.1 SP1 to 7.1 SP2”.

4.2. Migrating Databases from DirX Audit 7.1 SP1 to 7.1 SP2

Migrating the databases to DirX Audit 7.1 SP2 consists of migrating only the history entries database schema (History DB) for each tenant.

DirX Audit 7.1 SP2 can function with the history entries database from the previous version, but some database objects must be altered.

- Migrate the history entries database schema - run the following SQL scripts in your history entries database (History DB) server console.

  For SQL Server:
  install_media/**Additions/Scripts/MSSQL/migrate_history_71SP1_71SP2.sql**

  For Oracle Database:
  install_media/**Additions/Scripts/Oracle/migrate_history_71SP1_71SP2.sql**

Continue with the steps described in the section “Migrating Databases from DirX Audit 7.1 SP2 to 7.2”.

4.3. Migrating Databases from DirX Audit 7.1 SP2 to 7.2

Migrating the databases to DirX Audit 7.2 consists of migrating the audit messages database schema (Data DB) and the history entries database schema (History DB) for each tenant.

DirX Audit 7.2 can function with the same audit messages and history entries databases from the previous version, but some database objects must be altered. The migration must be done in several phases.

- Migrate the audit messages database schema - run the following SQL scripts in your audit messages database (Data DB) server console.

  For SQL Server:
  install_media/**Additions/Scripts/MSSQL/migrate_data_71SP2_72.sql**

  For Oracle Database:
  install_media/**Additions/Scripts/Oracle/migrate_data_71SP2_72.sql**

- Begin the migration of the history entries database schema - run the following SQL scripts in your history entries database (History DB) server console.

  For SQL Server:
  install_media/**Additions/Scripts/MSSQL/migrate_history_71SP2_72_part1.sql**

  For Oracle Database:
  install_media/**Additions/Scripts/Oracle/migrate_history_71SP2_72_part1.sql**

- Clean up the DirX Identity domain and optionally the history entries database – remove duplicate LDAP entries with the **dxthistdbtool** command line tool and its **ldapremdup** command by following the steps described in the section “Remove Duplicate LDAP Entries” in the *DirX Audit User Interface Guide*. You may want to synchronize the changes made in the DirX Identity domain to the DirX Audit History Database. In this case, the following extension to the existing SQL Server JDBC connection string in the tenant configuration (*install_path*/**conf/tenants/***tenantID*/**configuration.cfg**) could be required if you do not use a secure connection to your SQL database: **encrypt=false**.

  Example:

```
dxthistdbtool ldapremdup
 -ldapconfig ldap.properties
 -tenantid 6bc24196-327d-441c-8d66-3633ee6b887b
 -synctohistdb
```

- Clean up the history entries database – ensure there are unique history entries in the DirX Audit History Database with unique and non-missing **dirxEntryUUID** values with the **dxthistdbtool** command line tool and its **makeunique** command by following the steps described in the section “Make History Entries Unique” in the *DirX Audit User Interface Guide*.

  Example:

```
dxthistdbtool makeunique
 -ldapconfig ldap.properties
 -tenantid 6bc24196-327d-441c-8d66-3633ee6b887b
 -csvfile duplicates.csv
```

- Finish the migration of the history entries database schema - run the following SQL scripts in your history entries database (History DB) server console.

  For SQL Server:
  install_media/**Additions/Scripts/MSSQL/migrate_history_71SP2_72_part2.sql**

  For Oracle Database:
  install_media/**Additions/Scripts/Oracle/migrate_history_71SP2_72_part2.sql**

Next, continue with the steps described in the next sections.

4.4. Checking Apache Tomcat

To run DirX Audit Manager, you must install Apache Tomcat, which serves as the DirX Audit Manager's container, if it is not already installed. For the supported version numbers, see the *DirX Audit Release Notes*. Alternatively, you can stop the running Apache Tomcat service and then remove the folder *tomcat_install_path***/work/Catalina/localhost/AuditManager**.

4.5. Clearing Cached Internet Browser Data

We recommend that you remove the cached web content data, cookies and site data from your internet browser. This step is mandatory for Firefox, where you can find it in browser Tools → Settings → Privacy & Security → Clear Data.

4.6. Performing Initial Configuration

Now you can start the initial Core and Tenant configuration for each of your tenants by clicking **Next** in the Installation Wizard.

DirX Identity Synchronization Workflows are discontinued in DirX Audit 7.2 and replaced with History Synchronization based on LDAP. The existing workflows are migrated during the initial tenant configuration. For more details, see "Discontinued DirX Identity Synchronization Workflows Migration Connectivity Configuration" in the *DirX Audit Installation Guide*.

During DirX Audit configuration, an automatic procedure runs and performs migration steps. However, you must also perform some of the migration steps later as separate tasks, as described in the next sections.

For more information about the configuration process, see the section "Configuring DirX Audit" in the *DirX Audit Installation Guide*.

When the Configuration Wizard completes, finish the installation: Click **Done** to quit the installer.

4.7. Starting Services

At this point, you have DirX Audit 7.2 installed and at least one tenant configured on your system. Now start the DirX Audit services, if not already started, in this order:

1. DirX Audit Message Broker
2. DirX Audit Server *tenant_display_name* (a separate instance of DirX Audit Server is created for every tenant)
3. The Apache Tomcat service where you deployed DirX Audit Manager

4.8. Update Scheduled Report Jobs

Remove all *Generate dashboard chart* reports in your existing/scheduled report sets referring to the following legacy Dashboard components:

- Risk users based on compound factor by month and risk level
- Risk users based on simple factor by month and risk level
- DirX Identity total history certification campaign entries by month and lifecycle state

This step must be performed by all users that have these scheduled report jobs.

Update all report configurations for modified report templates. Several report templates have been updated. If they are included in a scheduled report job, this may require a manual configuration review – this means opening each individual report in a report set and resaving its configuration.

4.9. Update Set of Dashboard Components

Remove the following private and public legacy Dashboard components:

- Risk users based on compound factor by month and risk level
- Risk users based on simple factor by month and risk level
- DirX Identity total history certification campaign entries by month and lifecycle state

and remove all custom components based on the same templates or based on these fact tables:

- FCT_RSK_COMPOUND_USERS
- FCT_RSK_USERS
- FCT_HST_CERTCAMPAIGNS_LIFECYCLE

in the **Manage Components** list. These components cannot be used anymore. This step must be performed by all users that have these Dashboard components in their lists.

DirX Product Suite

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

DirX Identity

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

DirX Directory

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

DirX Access

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

DirX Audit

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

For more information: support.dirx.solutions/about

Legal remarks

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