EVIDEN

Identity and Access Management

DirX Audit

Release Notes

Version 9.0, Edition July 2025

Table of Contents

Release Notes

1. General

This Release Notes file contains important information about changes and enhancements of DirX Audit 9.0 that are not described in the DirX Audit user documentation. Familiarity with the DirX Audit user documentation is recommended because it will make this Release Notes file easier to understand.

1.1. Licenses

The Product License Agreement must be accepted in order to use the DirX Audit software products. Please refer to the file **license.txt** on Windows systems or read the file license agreement with *page* resp. *more* on Unix systems.

1.2. DirX Audit Highlights

1.2.1. General Features

DirX Audit provides a platform for the central compilation and analysis of identity-based audit logs and snapshots of history entries. It includes collectors to retrieve or receive audit information from external source applications, workflows and connectors to import history entries, a database to store this information securely and the DirX Audit Manager and DirX Audit Manager Classic to evaluate the stored audit events and history entries.

DirX Audit comprises these main features:

- A set of collectors that allow importing audit messages from various sources.
- A selection of relational databases can be used for persistent storage of the audit events, history entries and configuration data.
- The audit events database schema is based on a customization of the RFC 3881 (Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications) standard.
- DirX Audit Manager and DirX Audit Manager Classic, web-based user interface components, that allow for comfortable retrieval of audit results.
- Convenient correlation of events and activities from different IAM sources in a single online user interface with Dashboard, Audit analysis and History views for different levels of analysis.
- Standard identity audit key performance indicators (KPI) that provide statistical information about audit events or history entries over a period structured into online analytical processing (OLAP) tables for fast, interactive analysis and insight into IAM operations.
- Dashboard view for analysis of KPI data, with slice and dice and drill-down to more detailed audit event or history entry information as necessary.
- Audit analysis view of audit events retrieved from the central database according to a given search filter and summarized for ease of use, providing auditors and security compliance officers with the answers to the **when**, **where**, **who**, **what** and **why** of user

access and entitlements.

- History view for searching and viewing the state of DirX Identity entries in the past, comparing their state between different points in time and checking the state of related entries. Also audit events relating to the history entry are visualized in the History view.
- Configurable report templates in the Dashboard, Audit analysis and History views for exporting selected audit data to file format.
- Management of public and private dashboard components on all attributes and over a time period.
- Statistics evaluation based on the query result.
- Display of the statistics result in various chart types.
- Automated consolidation of identity-related audit logs with transformation to a standard format, giving DirX Audit users a unified presentation and analysis of audit events from a variety of sources.
- Authentication and authorization against any Lightweight Directory Access Protocol (LDAP) directory to the DirX Audit Database.
- Secure, persistent storage of audit logs in both their original and normalized format in a central database.
- Query and report templates to make it easier to analyze audit logs. DirX Audit provides pre-configured reports based on the TIBCO JasperReports Library technology. Additionally, customers can download and use Jaspersoft Studio to customize them or create their own reports to meet specific requirements.
- Configurable Dashboard layout and chart templates to analyze audit events and history entries according to several criteria.
- Integration with archive solutions through purge/restore functionality.
- Reporting service for scheduling jobs that can regularly and automatically generate and email user defined reports according to a schedule plan. Reports can be configured in a highly flexible way.
- Persistent storage of DirX Identity history entries in a central database.
- Persistent storage of contextual audit event relations and dependencies.
- Risk assessment of users based on risk factors like the total number of active accounts, applications, group memberships, imported accounts, imported memberships, privileged accounts, and SoD exceptions. Single risk factors can be combined to overall risk.
- Support for multi-tenant installation and configuration in all system components (Manager, Manager Classic, Server, Message Broker, Tools).
- Distinction of auditor roles Audit Administrator, (common) Auditor and Restricted Auditor with only limited access rights to selected reports.

1.2.2. New Features of DirX Audit 9.0

This section lists important new features of DirX Audit 9.0 compared to DirX Audit 7.2.

See the **history-of-changes.pdf** file for a history of changes of previous DirX Audit releases.

Main features of this version are:

Manager Classic

- Apache Tomcat 11 supported.
- Generic CSV report template.

Manager

- New software component based on REST API and Angular technologies. It provides Audit Analysis, History and Reports views. The Dashboards view is planned for future releases. A new landing page provides direct access to important features.

Server

- REST API for audit events.
- REST API for history entries.
- REST API for configurable report jobs.
- Improved context calculation.
- Improved fact population.

Message Broker

- Upgraded DirX Audit Message Broker (Apache ActiveMQ 6.1.6).

Database

- SQL Server 2022 supported.
- Database connection pooling upgraded to HikariCP.

Command Line Tools

- Improved performance of data export with deletion.
- Improved performance of purge in History entries database.
- New `purgeEnded` History DB CLI command.

Configuration Wizard

- New Look & Feel.
- DirX Audit Server service name configurable.
- DirX Audit Manager configurable.

Documentation

- DirX Audit User Interface Guide is newly split into three parts: DirX Audit Manager User Interface Guide, DirX Audit Manager Classic User Interface Guide, and DirX Audit

Command Line Interface Guide.

1.2.3. Bug Fixes

Manager Classic

- Specific whats, having no What - Detail, are not visible in Event Details.
- **Property** selection box in Advanced Search in **Audit analysis** tab is initialized only with audit event dimension names. Audit message dimension names are missing.
- The **Entry changes** report does not allow filtering by entry name prefix.
- Unable to drilldown by month dimension in dashboard components based on history entries when language is set to German or French.
- DirX Audit 7.2 cannot reestablish the connection with SQL Server.

Server

- Population of the **FCT_RSK_USERS** table is very low performable.
- Context population process of DirX Audit Server cannot process all incoming audit messages in time.
- LDAP collector fails to delete **dxrHistory** attributes on DNs with Unicode characters.
- DirX Audit 7.2 cannot reestablish the connection with SQL Server.
- 'Unable to execute the following SQL' during the context population.
- Fixed a 'failure to resume transaction' randomly occurring during orphan processing in context calculation.

Message Broker

- Message broker - critical CVE - CVE-2023-46604.

Database

- Solve backward compatibility with SQL Server 2016 - remove usage of **string_agg** function.

Command Line Tools

- Migration to 7.2 fails on makeunique command.
- **Dxtdbtool** `decompress` does not work correctly on SQL Server 2019.
- History entries export with deletion is slow.
- DirX Audit 7.2 cannot reestablish the connection with SQL Server.
- Improved performance of Data DB purge operations: cascading replaced with stored procedures.
- Improved performance of History DB purge operations: cascading replaced with stored procedures.

- SQL Server locks during scheduled purge jobs.
- Log resolved relative dates when running purge CLI tools.

Configuration Wizard

- Message broker error after reconfiguring SSL.
- Migration of discontinued DirX Identity Synchronization Workflows find all active workflows for all configured DXI domains.
- Configuration of LDAP collector - wrong URL uniqueness check.
- Next button disabled after filling all required values.
- Fix checkbox for running tenant configurator.
- Additional screens for **Scheduled Purge Jobs Configuration** are visible after uncheck this option in tenant configuration.

1.2.4. Information about Discontinued Features

DirX Audit 9.0 does no longer support these features:

- File PEP as the supported authorization method

DirX Audit 9.0 is the last version that supports the following features:

- DirX Audit Manager Classic
- Fine-grained access control for retrieving audit events from DirX Audit Database via DirX Audit Manager Classic.

1.2.5. Previous Releases

Previous DirX Audit releases:

Version	Release Date	Notes
DirX Audit 7.2	01/13/23	*)
DirX Audit 7.1 SP2	05/20/22	*)
DirX Audit 7.1 SP1	08/03/21	*)
DirX Audit 7.1	07/31/20	*)
DirX Audit 7.0 SP1	10/18/19	*)
DirX Audit 7.0	06/29/18	*)
DirX Audit 6.0	04/15/16	*)
DirX Audit 5.0	06/19/15	*)
DirX Audit 4.0	04/11/14	*)
DirX Audit V3.0B	05/17/13	*)
DirX Audit V3.0A	03/30/12	*)

Version	Release Date	Notes
DirX Audit V2.0D	12/13/11	*)
DirX Audit V2.0C	10/20/10	*)
DirX Audit V2.0B	04/30/10	*)
DirX Audit V2.0A	05/31/09	*)
DirX Audit V1.0C	01/23/09	*)
DirX Audit V1.0B	11/10/08	*)
DirX Audit V1.0A	09/12/08	*)

*) See the **history-of-changes.pdf** file for a history of changes of previous DirX Audit releases.

1.3. Supported Platforms

DirX Audit 9.0 is available on the following platforms:

PC (Intel)

- Microsoft Windows Server 2019 (x86-64)
- Microsoft Windows Server 2022 (x86-64)
- Microsoft Windows Server 2025 (x86-64)

UNIX

- Red Hat Enterprise Linux 8 AP (x86-64)
- Red Hat Enterprise Linux 9 AP (x86-64)
- SUSE Linux Enterprise Server 12 (x86-64)
- SUSE Linux Enterprise Server 15 (x86-64)

Virtual Machine Support:

- VMWare ESXi, in combination with the guest operating systems listed above and that are supported by VMWare ESXi.

Clients run also on Windows 11.

Note: You can install DirX Audit completely on Windows 11 for non-productive use (demos or PoCs). Do not use this configuration for productive use.

1.4. Java Requirements for DirX Audit

DirX Audit requires a customer-supplied Java SE installation. No embedded Java environment comes with DirX Audit. It is customer’s responsibility to download and install any Java SE security patches in time.

As described in the DirX Audit Installation Guide these are the options regarding the Java environment:

- The product must be an implementation of the Java Platform, Standard Edition (Java SE).
- The related version number must be 21.0.xx.
- It must be a 64-bit distribution.

Supported Java product is for example:

- OpenJDK 21

For details regarding said installation options, see the chapter “Installation Prerequisites” in “Installation Configurations” in the DirX Audit Installation Guide.

1.5. Supported Apache Tomcat Installations

DirX Audit Manager supports these Apache Tomcat versions running with Java SE 21:

- Apache Tomcat 11 version 11.0.9 or higher

Use Java SE 21 with the latest security patches installed. It is customer’s responsibility to download and install any Java SE security patches in time.

Please check that the Apache Tomcat service executes under the Local System account in Windows Server. Otherwise, there can be issues with importing and exporting data in DirX Audit Manager Classic.

Please consider also additional steps to secure Apache Tomcat beyond the default installation. As the Apache Tomcat installation comes with a default username / password for the Apache Tomcat administrator we strongly recommend considering additional measures to secure the Apache Tomcat web container by following the guidelines in https://tomcat.apache.org/tomcat-11.0-doc/security-howto.html.

1.6. Supported Databases

Product

- Microsoft SQL Server 2019
- Microsoft SQL Server 2022
- Oracle Database 19c

1.7. Supported JMS Messaging Servers

DirX Audit supports the following JMS messaging server:

- Apache ActiveMQ 6.1.6 message broker (included in the installation)

If you consider upgrading the message broker, please contact the DirX support unit.

1.8. Supported integration container

DirX Audit supports the following applications runtime:

- Spring Boot 3.4.6 (included in the installation)

If you consider upgrading the integration container, please contact the DirX support unit.

1.9. Delivery Packages

This section provides information about DirX Audit delivery packages on the distribution media. It contains:

- Additions
  - A set of predefined dashboard components in **\Additions\Data\Components**.
  - Sample DirX Identity and DirX Access audit message data stored in XML files and DirX Identity history snapshots stored in LDIF files in **\Additions\Data\SampleData**.
  - Sample Java code for Digest Producer and Tag Producer in **\Additions\Data\SampleJava**.
  - Sample authorization policies in **\Additions\Data\SamplePolicies**.
  - A set of generated sample reports in the PDF format partly based on the DirX Identity sample domain data in **\Additions\Data\SampleReports**.
  - XML schema for DirX Audit messages, dashboard components and report definitions in **\Additions\Schemas\DirXAudit**.
  - SQL scripts for creation of tables and their indexes and views in **\Additions\Scripts**. Subfolder **common\adm** contains useful queries which for example give an overview on indexes or allow to query history entries with given or duplicate dxrUid.
- Documentation
  - for DirX Audit
- Installation
  - DirX Audit 9.0 installers for all supported platforms.
- Resources
  - modified sources of Mozilla LDAP SDK.
  - sources for other third-party software that require source delivery.

1.9.1. Distribution Media

Software packages for all platforms are usually distributed on DVDs. All platforms are delivered together on one DVD.

In addition to the distribution medium, you must purchase separate product licenses in

order to use the software packages.

Please contact your local sales representative for details on product licenses.

1.9.2. Resources

Each DVD ships with modified sources of the:

- Mozilla LDAP Java SDK 4.18 (see also: http://www.mozilla.org). You can find them - along with a brief documentation of the modifications - in the folder Resources of the DVD.

1.10. User Documentation

1.10.1. DirX Audit User Manuals

The following manuals are available in PDF format of Adobe:

Manual	File
DirX Audit Installation Guide	installation-guide.pdf
DirX Audit Migration Guide	migration-guide.pdf
DirX Audit Introduction	introduction.pdf
DirX Audit Tutorial	tutorial.pdf
DirX Audit Administration Guide	administration-guide.pdf
DirX Audit Manager Classic Guide	audit-manager-classic-guide.pdf
DirX Audit Manager Guide	audit-manager-guide.pdf
DirX Audit Command Line Interface Guide	command-line-interface-guide.pdf
DirX Audit Customization Guide	customization-guide.pdf
DirX Audit Best Practices	best-practices.pdf
DirX Audit History Synchronization Guide	history-synchronization-guide.pdf
DirX Audit Installation Preparation Checklist	installation-preparation-checklist.pdf

You need Adobe Acrobat Reader (or a similar PDF viewer) to view PDF files. For a free copy of Adobe Acrobat Reader please refer to

http://www.adobe.com/prodindex/acrobat/readstep.html

or to

http://www.adobe.com

On Windows systems, files with the suffix ***.txt** or **.pdf** can be opened by double-clicking them.

The setup also provides each document.

1.10.2. DirX Audit Online Help

All manuals are also available as Web Help projects available in https://docs.dirx.solutions/dirx-audit-docs/latest/index.html.

Make sure that the browser is configured to allow ActiveX controls and plugins and considers ActiveX scripts as safe.

1.10.3. Third Party Documentation

Third party software is delivered with its documentation.

1.11. Hardware Requirements

This section provides information about hardware requirements.

Per default you can run DirX Audit on a single machine.

For better performance we recommend separating the database to a second machine.

For optimum performance you can distribute all components (Manager / Manager Classic, Message Broker, Server and Database) on separate machines.

1.11.1. RAM

At least 8 GB RAM is recommended for DirX Audit.

1.11.2. Disk Space

The installation requires temporarily 2.0 GB of disk space. The complete DirX Audit installation requires 1.5 GB of disk space.

For data and log files additional space is required.

At least 10.0 GB of free disk space is recommended for DirX Audit.

1.12. Software Requirements

DirX Audit 9.0 requires:

- See the DirX Audit Installation Guide file for more information.

The DirX Audit Manager supports these types of browsers:

- Microsoft Edge 138.0 (64-bit) or newer
- Mozilla Firefox 128.12.0esr (64-bit) or newer
- Google Chrome 138.0 (64-bit) or newer

For JasperReports design use TIBCO Jaspersoft Studio, but set JasperReports 6.19.0 in

Window / Preferences / Jaspersoft Studio / Compatibility / Version.

DirX Access:

If you plan to use fine-grained access control with access policies maintained by DirX Access Server, you need to deploy DirX Access V8.10 or DirX Access V9.0 or DirX Access V9.1.

1.13. Browser settings

Set the Internet Options:

- Set Scripting / Active scripting to Enable (in Control Panel / Internet Options / Security / Internet / Custom level) otherwise some DirX Audit Manager Classic functions cannot be used, for example Dashboard - Manage Components – Import
- Check the settings of Local intranet and Trusted sites, address of DirX Audit Manager Classic should be there (Control Panel / Internet Options / Security / Sites)

1.14. Restrictions

DirX Audit has the following restrictions.

1.14.1. Audit message size

There is a limit on the maximal size of the input audit message that DirX Audit Server can handle. This limit cannot be explicitly calculated because it depends on the configured environment and form of the input. In general, the size of the incoming audit message should not exceed several megabytes in original form.

For example, adding a new group with 100,000 members in DirX Identity can produce such huge messages.

DirX Audit Server stores these messages into error storage.

If all available free memory is exhausted, the DirX Audit Server can even crash. You can manually assign more memory to the DirX Audit Server container or process this input manually.

See also Known Issues section for detail on specific collectors.

1.14.2. Data not updated immediately

In some cases, the data is not updated immediately. For example, DB maintenance tool purges history entry data, but it is still visible in DirX Audit Manager in the History view. The reason is that the purged data is removed from the primary table, but DirX Audit Manager presents data originated in database materialized views. These views must be refreshed to reflect the change in the primary table. It is usually done automatically on a daily basis.

2. Compatibility

This chapter notifies about compatibility issues compared to the previous DirX Audit version.

2.1. Database Schema

Config Database

- New tables for storing the newly created component DirX Audit Manager configuration data: CFG_ITEMS, CFG_ITEMS_CLOB, CFG_ITEMS_BLOB, CFG_ITEMS_REPORT.

Data Database (Audit events)

- Multiple changes on fact and dimension tables.
- Dropped delete triggers on audit message tables.
- New message dimension type for representing certification campaigns.

History Database (History entries)

- Multiple changes on fact and dimension tables.
- New indexes on the HST_SMALL_ATTRS_IN_TIME table.
- Removed on delete cascade on history entry OLTP and OLAP tables.

2.2. Dashboard Components

There are 2 new dashboard components for Audit Manager Classic in DirX Audit 9.0 compared to DirX Audit 7.2 - **DirX Identity created and deleted user attribute values by month** and **User creation succeeded audit events by datetime and operation**. These 2 components have to be manually imported if you want to use them. See the section “Update Set of Dashboard Components” in “Manual Migration” in Migration Guide for required steps to update the available set of dashboard components when you upgrade from previous versions.

2.3. Report Templates

Modified report templates

- There are several modified report templates with extensions and improvements.

See the section “Update Scheduled Report Jobs” in “Manual Migration” in the Migration Guide for required steps to update scheduled report jobs when you upgrade from previous versions.

3. Installation

Follow the DirX Audit Installation Guide.

Upgrade installation is supported only from DirX Audit 7.1, DirX Audit 7.1 SP1, DirX Audit 7.1 SP2 and DirX Audit 7.2. Please see DirX Audit Migration Guide for all required steps.

When upgrading from previous DirX Audit versions (DirX Audit 7.0 SP1 or earlier), it must be fully uninstalled, and DirX Audit 9.0 must be installed from scratch.

When the installer is started in the silent mode it runs in the background. If you need to wait for it to finish (for example in an automated script) you can achieve it by calling the installer in a separate script or by instructing the command shell to wait for the process to finish – on Windows by calling with START /WAIT, for example:

```
START /WAIT dirxaudt.exe [-i silent]
```

4. Documentation Changes

This chapter contains the latest documentation updates that are not contained in the official documentation on the installation media.

There is no documentation update that is not contained in the official documentation on the installation media.

5. Known Issues

This chapter contains already known issues.

5.1. General Issues

5.1.1. Services on Linux do not behave correctly

Description: Services do not behave correctly, for example graphics are incomplete and DirX Audit Manager does not work correctly.

Solution: Check permissions on installed and created files and folders. Run all DirX Audit services on Linux platforms under root account if the problem still exists.

5.1.2. System services do not start on Linux

Description: There are at least two system services typically installed and automatically started in default installations: DirX Audit Message Broker and one or more DirX Audit Server tenant services. The DirX Audit services on Linux might not start correctly after they have been stopped unexpectedly before, for example if process or system crashed or on power failure. The reason is that several files containing PIDs of the running processes are not deleted in such cases.

Solution: To fix the problem you must follow these steps.

Check if the related processes are not running, for example using **ps** command - check for **java** and **wrapper** binaries pointing to or referencing the DirX Audit installation path.

Remove the following PID files if existing for the selected service that does not start:

DirX Audit Message Broker service:
install_path/**message_broker/bin/service/dirx-audit-messagebroker.pid**

DirX Audit Server services:
install_path/**server_container/tenants/***tenant_id*/**bin/dirx-audit-server-*tenant_id*.pid**

Start the relevant services.

5.2. Installation and Configuration

5.2.1. SSL configuration for DirX Audit Message Broker

Description: DirX Audit Message Broker does not start if SSL listener is enabled and the SSL broker was not configured correctly. SSL configuration must be prepared manually.

Solution: Do not enable SSL connector on DirX Audit Message Broker configuration page unless the SSL support is configured properly. See DirX Audit and Apache ActiveMQ documentation for the SSL configuration procedure.

5.2.2. Silent update or upgrade installation on Linux as root does not work correctly

Description: Update or upgrade installation on Linux under root does not preserve the selected target user (that was selected to run the applications in previous installation). All installed files are owned by root and the target user and groups values are missing the configuration file.

Solution: Perform the update or upgrade installation on Linux as root in either console or GUI mode. You need to manually correct the installation if a silent update or upgrade installation has been already performed. Execute the following steps to fix the installation in that case:

- Stop all DirX Audit services if already started.
- Change ownership of the installation folder (recursively all files and folders) to the target user and group.
- Edit the file *install_path*/**conf/installation.ini** and add or edit the following two properties (replace the user and group with correct user and group names):
  `install.unix_user=`***user***
  `install.unix_user_gid=`***group***
- Perform the complete configuration (core and all tenants) again.

5.2.3. The installation and uninstallation not started correctly on some newer Windows systems

Description: The installation and uninstallation are not started correctly on some newer Windows systems. After executing the installer an error window with title "Fatal Application Error" is displayed containing text "This Application has Unexpectedly Quit". If details are expanded the following text is displayed on top: "Flexeraaw2$aaa: Windows DLL failed to load".

Solution: This is a known issue in the software used for creating the installer. To fix it a new environment variable must be set to force the compatiblity with older Windows for Java applications:

```
JAVA_TOOL_OPTIONS="-Dos.name=Windows 7"
```

This variable can be set either globally for the user (via Control Panel) or only on a command-line before starting the installer (*SET JAVA_TOOL_OPTIONS="-Dos.name=Windows 7"*).

After this variable is set and applied the installer starts correctly.

5.2.4. Configuration Wizard for Tenants indicates invalid Config DB schema on Oracle Database

Description: Configuration Wizard for Tenants indicates invalid Config DB schema on Oracle Database. The warning complains about the column ITEM_UUID in the CFG_ITEMS table and its data type.

Solution: The warning can be ignored. The column is of the RAW(16) data type on Oracle Database, which is equivalent to the BINARY(16) data type on other database platforms. The column is used for storing UUIDs in a binary format.

5.3. DirX Audit Server

5.3.1. DirX Audit Server freezes during Error Handling

Description: DirX Audit Server might stop processing audit messages if an already stored error message (due to a database disconnection) fails to persist again due to a different problem.

Solution: Stop the DirX Audit Server service, move the stored error messages to a different folder, clear the error storage folder (delete it) and start the DirX Audit Server service again. The moved error messages can then be processed later by the file collectors after investigating and resolving the reason leading to the persistence error.

5.3.2. DirX Audit Server stops to deliver scheduled reports

Description: DirX Audit Server might stop sending generated reports due to a different problem.

Solution: Restart the DirX Audit Server service.

5.3.3. Collectors, scheduled jobs or fact population not started

Description: Collectors and the scheduler for jobs and fact population run within the same server container (running under DirX Audit Server service). Under some rare conditions it can happen that either collectors or scheduler (for jobs and fact population) do not start correctly, while the other one is started and runs. Fact population is enabled only when Dashboard feature is licensed.

Solution: Stop DirX Audit Server service if started. Start DirX Audit Server service. Wait approximately two minutes and check if both collectors and the scheduler (including fact population when enabled) service components were initialized and started correctly.

If this procedure does not help, repeat it.

5.3.4. InputStreamZippedJarVisitor warnings in the DirX Audit Server log file

Description: DirX Audit Server occasionally records an InputStreamZippedJarVisitor warning.

Solution: This record does not indicate any dysfunction. You can ignore its occurrence in the dirxaudit-server.log file.

5.3.5. DirX Audit Server DB connectivity is not refreshed when DB configuration is modified with the Tenant Configuration Wizard

Description: In certain cases, when DirX Audit Server service is running and a tenant's DB configuration is modified with the Tenant Configuration Wizard, DirX Audit Server DB connectivity is not refreshed and uses the original DB connection settings.

Solution: When DB configuration is modified with the Tenant Configuration Wizard, include also the Collectors Configuration in the performed steps to force DirX Audit Server to refresh the DB connectivity.

5.3.6. SQL scripts are not executed when any of their predecessors fails

Description: When DirX Audit Server executes a list of SQL scripts and any of them is terminated with an exception, the execution of the rest of scripts is not started.

5.3.7. DirX Audit Server service does not start when database server is not available

Description: DirX Audit Server service does not start due to database connection errors. Server log contains usually the following errors in this case:

```
com.zaxxer.hikari.pool.HikariPool$PoolInitializationException: Failed
to initialize pool: The TCP/IP connection to the host ... has failed
…
org.springframework.beans.factory.UnsatisfiedDependencyException:
Error creating bean with name 'reportController'
```

Solution: Make sure that the database server is running and the configured authentication is correct. Start the DirX Audit Server services again.

5.3.8. Running the history update job on an empty database for the first time logs an error message mentioning a missing DIM table

Description: When running the history update job on an empty database for the first time an error message is logged mentioning a missing DIM table.

Solution: Run the fact population job. When the history update job runs next time there are no more error messages.

5.4. DirX Audit Manager Classic and DirX Audit Manager

5.4.1. Audit analysis: Sorting for the What Details (Manager Classic) / Event Detail (Manager) column not supported

Description: Sorting in the Audit analysis view for the What Details (Manager Classic) / Event Detail (Manager) column is not implemented.

5.4.2. Audit analysis: Low performance with 'contains' and ‘ends with’ condition (Manager Classic)

Description: To avoid poor performance during query execution in the Audit analysis view, do not use the 'contains' and ‘ends with’ operators with wildcards (%, _) in the Audit analysis view. Use other conditions as there are 'equals' or 'starts with' alternatives in the Audit analysis view (constant prefix).

In the Audit analysis view you can use the ‘contains’ operator in the query in case you prepare the database for it. It is necessary to create the full text catalogue and full text index over the data database. If you check the flag **Use full-text search** in the Tenant Configuration Wizard, the catalogue and index on the DETAIL column of the DAT_AUDITEVENTS table is created automatically.

5.4.3. Dashboard component title format not reflected (Manager Classic)

Description: The user can set dashboard component title’s font, size, and style, but the settings are not reflected. The reason is that the component’s title is shown only in the component’s header and not in the chart area in the Dashboard view. The font, size and style settings are applied only when exporting the component into a document with the Export function.

5.4.4. Reports do not work on Linux

Description: A report is not created and sent or is not correctly displayed. The problem might be caused by using a font that is not available on the system, for example Microsoft core true-type fonts.

Solution: Check used fonts in the report template and use either generic types like Serif or Sans-Serif or install the required font, for example Microsoft core true-type fonts.

5.4.5. Scheduled report is not delivered (Manager Classic)

Description: A dashboard component, an event report or a context event report can be attached to a scheduled report in a job definition. When you or some other user in a case of public dashboard components and Audit analysis view filters delete the object referenced in your job, you are not notified about the modification and the job is not running anymore.

Solution: Be careful what dashboard components you use in jobs. Prefer private dashboard components and Audit analysis view filters where you have full control. When your job is not run and reports delivered, check definition of the attached dashboard components.

5.4.6. Report is not generated when Oracle Database is used (Manager Classic)

Description: A dashboard component report or an event report is not generated when run directly from DirX Audit Manager and Oracle Database is used as a data store.

Solution: Run the requested report as a scheduled job in near future.

5.4.7. Audit analysis / History: Different total numbers of events could be displayed in the Audit analysis view and the History view in results

Description: Different total numbers of events could be displayed in the Audit analysis view and in the History view for the same time range and corresponding filters. This stems from the fact that History view search is based on the entry's dxrUid matches while the Audit analysis view search is based on the entry's name searching.

5.4.8. Authentication fails with many groups in LDAP

Description: When many groups are to be compared for a user's membership, the authentication fails for exceeded limits.

Solution: Create LDAP groups used for DirX Audit application role mapping in a separate subfolder with a restricted search base.

5.4.9. Windows username and password authentication can be executed on an unintended domain (Manager Classic)

Description: When DirX Audit Manager can access more domain controllers, the user identity could be authenticated with a different domain than the intended one. This could lead to a misuse of a user identity.

Solution: Restrict the list of key distribution centers in the Kerberos **krb5.conf** / **krb5.ini** file to intended domains only and disable the DNS lookup of key distribution centers (KDC).

```
# krb5.ini / krb5.conf
[libdefaults]
dns_lookup_kdc = false
…
[realms]
my-company.com = {
  kdc = ads.my-company.com:88
}
[domain_realm]
my-company.com = MY-COMPANY.COM
.my-company.com = MY-COMPANY.COM
```

5.4.10. Audit events not having an available dimension value are not considered in an aggregation by this dimension (Manager Classic)

Description: Audit events not having an available (N/A) dimension value are not considered in an aggregation by this dimension. A dashboard component chart does not contain data of such audit events.

5.4.11. Changes performed in the “Generate dashboard chart – Edit report settings“ component are not saved (Manager Classic)

Description: If the dashboard report is scheduled using the **Schedule** icon in the Dashboard component, the changed report settings for the scheduled report are not saved.

Solution: Create a report set from the **Reports** tab using the **Add a new report set** link and use the **Generate dashboard chart** component.

5.4.12. Dashboard is not rendered when referencing legacy dashboard component (Manager Classic)

Description: When the dashboard is referencing one of the obsolete 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), it is not rendered.

Solution: Remove the components in the Manage Components list, disconnect and re-connect to the application and remove the component reference from the dashboard configuration.

5.4.13. Dashboard indicates that the dashboard component is not available (Manager Classic)

Description: The dashboard indicates that the referenced dashboard component is not available.

Solution: Remove the dashboard component reference from the dashboard configuration in the Layout dialog.

5.5. Reports

5.5.1. Big report in the text format (txt) and plain template is not generated

Description: Huge reports configured for text format (TXT) and using plain template are not generated. An exception ArrayIndexOutOfBoundsException is logged into the log file.

Solution: Set a smaller number of rows or change the output format (use for example csv or rtf).

5.5.2. Picklist shows also records without a UID

Description: The picklist in the report configuration dialog can contain also records that are not stored with a UID in the database. These records are not transferred to the **Selected** section.

Solution: Configure your Identity Store thoroughly to prevent operations on records without providing their UID.

5.5.3. Picklist duplicates records for objects with different combination of descriptive attributes

Description: When an object is present in the database with more combinations of values of descriptive attribute, more records for the same object are shown in the picklist's **Found** section of the report configuration dialog. Only one of them is transferred to the **Selected** section.

5.5.4. Unlocalized selection of history entry types

Description: There is an unlocalized selection of history entry type in the **History Entries by Entry Type** report scope configuration screen.

5.5.5. Overview charts are not included in HTML format reports

Description: Several reports contain an overview chart. But it is not included when the HTML format is used.

Solution: Use an alternative report format like PDF.

5.5.6. Report job execution and preview fails (Manager Classic)

Description: Execution of report jobs referencing legacy report templates or dashboard components fails.

Solution: Reconfigure the legacy report in the report set. Remove the dashboard component reference from the report set.

5.5.7. Warnings in the DirX Audit Server log file when generating report in XLS format

Description: DirX Audit Server records warnings when setting DocumentSummaryInformation, SummaryInformation and codepage property in generated XLS file.

Solution: These records do not indicate any dysfunction. You can ignore its occurrence in the dirxaudit-server.log file.

5.6. Collectors

5.6.1. DirX Identity: Huge audit messages

Description: DirX Identity can produce huge audit messages. An example is the creation of a new target system group with 100,000 members. This results in one huge audit message. You should avoid producing this type of messages.

Solution: Define account-side memberships in all target systems that shall be audited on the DirX Identity side. If this is not possible remove temporarily the relevant member attributes from the audit policy.

5.6.2. Valid audit messages data is considered invalid when it is a part of a set containing also invalid audit messages data

Description: When several collected audit messages have invalid xml structure, for example for a missing element attribute, the whole set, by default 10 audit messages, is directed to the **250-nonrecoverable-xml** subfolder. No audit message of the set is persisted.

Solution: You can prevent this behavior by specifying the **send_count = 1** in the tenant's **configuration.cfg** file in the specific LDAP or File collector section.

For example, navigate to the *install_path***conf****tenants***tenantid***configuration.cfg** file and extend the following section with the configuration parameter **send_count** value set to 1.

```
[server.apps.collector.file.dxi]
…
send_count = 1
```

5.6.3. Missing What – Lifecycle value in most DirX Identity audit messages

Description: The What – Lifecycle field is empty for most DirX Identity audit messages. It is not filled by intention as no corresponding data is provided by DirX Identity.

5.7. Fact Population

5.7.1. Very slow fact population for history entries and Oracle Database

Description: The fact population on the History DB deployed at the Oracle Database has low performance.

Solution: Carefully schedule the fact population out of common business hours.

5.7.2. Population of fact tables on history entries can be restricted only with the VALIDFROM input parameter.

Description: The fact population SQL scripts for the history entries support only the VALIDFROM input parameter. There is no support for the VALIDTO input parameter.

5.8. History Synchronization

5.8.1. Distinguished name value could not be synchronized by modify jobs in some specific cases

Description: When a referenced entry is moved in the directory structure, this is not reflected as a modification of the referencing entry and the **modifyTimestamp** attribute value is not changed for the referencing entry by DirX Directory. If there is no other modification in the referencing entry, the change is not recognized with a **modify** job, as **modifyTimestamp** value is not updated, and the new distinguished name value is not synchronized.

Solution: Execute also **delete** jobs on a regular basis.

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.