EVIDEN

Identity and Access Management

DirX Audit 9.0

Efficient Compliance Support

Analytics and Intelligence for Identity and Access Management

The Challenge

Cost pressure is combining with increased security needs to cause enterprises and other organizations to look for new ways of optimizing their business processes. That is especially true in the observance of compliance regulations such as those stipulated in the EU's General Data Protection Regulation (GDPR) regarding the processing of personal data or in the Sarbanes Oxley Act regarding the reliability of the financial data published by enterprises. One way of providing efficient support for these efforts is to roll out an Identity and Access Management (IAM) system with analytics and intelligence support.

The sheer number and types of regulations, however, pose a challenge:

- Many different regulations exist today, and new ones are mandated all the time, requiring continuous revision of IAM controls.
- The policy for what is audited depends on the given regulation, the enterprise business model in force, and the application creating the audit trail, making it difficult to establish consistent, end-to-end audit policies.
- Different regulations require different methods of analysis and reporting.

Audit data of IAM activities need to be produced that can be used to demonstrate accountability and report on the results to demonstrate control of business processes on user access and entitlements as required by applicable regulations. On a regular basis or on demand, reports must be produced on status and history on the information in the IAM repositories - for example, the identity store in an identity management component.

The audit trails and historical data produced by IAM components can help to answer the questions that auditors ask to obtain proof of compliance. Until now, audit logs and historical data from several applications had to be analyzed to answer questions like "Who has accessed financial data in the last month?", "Who gave the users access rights for this?" and "Who approved these rights?" Different audit formats, different user identities for the same person and parallel timelines in the individual applications make such analyses very difficult and cost intensive.

Our Solution

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. DirX Audit complements the core IAM capabilities for administration, authentication, and authorization by providing means to analyze and report on IAM operations and deliver the information necessary to support IAM governance, risk management and prove compliance.

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, evaluatinging, correlating, and reviewing of identity-related events, and job management for report generation. With its analytical features, DirX Audit helps enterprises and organizations to ensure sustainable compliance and provide business intelligence for the identity and access management processes.

DirX Audit provides the functional building blocks for a centralized, secure identity analytics and intelligence solution as shown in Figure 1.

Key features include:

- Convenient correlation of events and activities from different IAM sources in a single Web-based user interface with Dashboard, Audit Analysis and History views for different levels of analysis.
- Risk assessment for identities based on a configurable set of risk factors
- Standard identity audit key performance indicators (KPI) that provide statistical information about audit events and historical identity data over a period of time structured into online analytical processing (OLAP) tables for fast, interactive analysis and insight into IAM operations.
- Dashboard view for KPI and trend analysis charts, with drill-down to more detailed event or historical identity information.
- Audit Analysis of audit events according to a given search filter and summarized for ease of use, providing auditors and security compliance officers with the answers to the "what, when, where, who and why" of user access and entitlements.
- History view for tracking changes to identity and identity-related data over time, allowing for reviewing identities in the past and point-

in-time comparisons.

- Reports view for configuring and scheduling the generation and e-mailing of reports for Dashboard, Audit Analysis and History view analyses.
- Configurable report templates for Dashboard charts, audit events and history entries for exporting selected audit and historical data to files.
- Configurable Dashboard layout and chart templates to analyze audit KPI data according to several criteria.
- Automated consolidation of identity-related audit trails with transformation to a standard format and business language, giving DirX Audit users a unified presentation and analysis of audit events from a variety of sources.
- Authentication with LDAP against directory server, with OpenID Connect,orwithKerberos.Authorization based on group memberships in the LDAP directory server.
- Persistent storage of audit trails in both their original and normalized format in a central database.
- Persistent storage of historical identity data in a central database.
- Integration with archive solutions through purge/restore functionality.
- Support of multiple tenants (DirX Identity domains).
- Extensibility to collect audit events from other applications.
- Support of organization or department auditors who see only events for their organization.

Dashboard

The Dashboard view of DirX Audit Manager presents event and historical data that the DirX Audit Server has aggregated according to the various identity audit KPIs in graphical charts. DirX Audit provides a standard set of KPIs modelled as OLAP tables to allow for fast display of important aggregated data. Using the Dashboard, auditors can perform analysis, especially time-based trend analysis of selected KPI data - for example, the total number of users created from day to day over a given period - and then drill down to details as necessary. Charts can be displayed in bar, pie, line, point or area formats, as shown in Figure 2.

The Dashboard provides KPI charts for:

- Events on accounts, account-group memberships, users, user-role assignments, password changes, password lookups, approvals, authentications, authorizations, etc. with total, succeeded and failed operations, accepted and rejected approvals
- Historical identity data with total number of entries
- which can be categorized by time (year, month, day), operations, applications, object type, auditing component, organizational unit of the user, automatic or manual assignment, etc.

Samples for analysis that can be performed by auditors are:

- How many account changes in a target system have been performed?
- How many account-group memberships have been imported from a target system?
- What is the trend in the number of high-risk users?
- How many role assignments have been approved?
- How many passwords were changed; How many of the password changes failed?
- How many identities have been managed?
- How many SoD Exceptions were detected?
- How many accounts are orphaned?
- How many access reviews have been performed?
- How many (high risk) users have not been certified last year?

An audit administrator can provide a set of public chart configurations that are readily available to all auditors. Auditors can in turn define their own private chart and Dashboard layouts and store and import these definitions to and from local files.

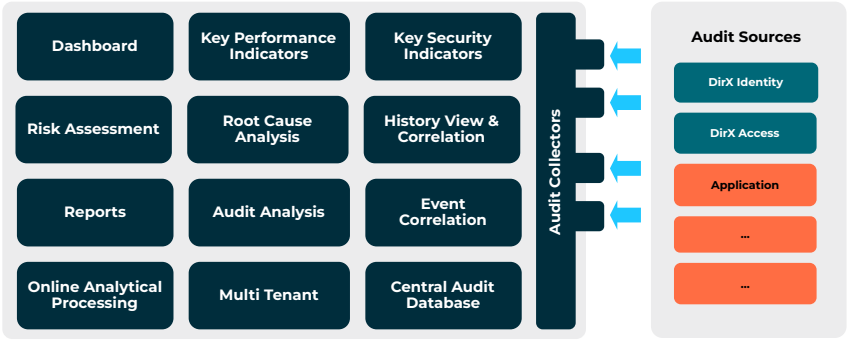

Figure 1 - DirX Audit Functionality

Audit Analysis

The Audit Analysis of DirX Audit Manager allows auditors to search for and retrieve audit events from the central DirX Audit Database according to a given search filter. The Audit Analysis works directly with audit events stored in the DirX Audit Database rather than with aggregated, OLAP-structured KPI data. An audit event extends the information in the original, detailed audit message with one or more informational summaries of the operation recorded by the message and the objects on which it operated. These summaries can help auditors to easily understand even complex operations like approval of a user-role assignment with modification of the end date and a new role parameter.

Auditors can configure the search filter according to the following parameters:

- When, From and To: relative or absolute time period - for example, last month, last year – or a specific start and end date.
- Source: the component/product that generated the audit event.
- Who: user who initiated the audit event.
- What: the name of an object that is associated with the event; for example, the name of a user, account, and role.
- Type: operation type associated with the event; that is, how the operation was initiated; for example, manually, on schedule, or on request.
- Operation: the operation associated with the event; for example, set password, add assignment, request object update, add object, delete object, login, and logout.
- What Type: the object type that is associated with the event; for example, users, accounts, account-group memberships.

- What Detail: Specific detail of an operation on an object type; for example, a specific user account or target system in a search for update operations made to accounts.

The search filter's What Detail parameter allows for filtering audit events according to specific details of events, such as:

- Role assignment of role Project Manager to user John Doe
- Request of a role assignment of role First Class with start date June 7, 2018, with 4-eye approval workflow
- Approval of the above request
- Account-to-group assignment of user John Doe to group First Class in target system Extranet Portal

The Audit Analysis displays the search results returned by running the filter in page-through tables, with more detailed information about each audit event available on request via a simple mouse click on an icon. Especially you can see the events in the same context. For example, the event which has caused a new group membership or those on the approval or the Web access requests of a user in the same DirX Access session. The search results can also be exported as a report to a file. The detailed view allows you to navigate to the History View.

History View

The History view of DirX Audit Manager allows the auditor to examine the status of identities and identity-related data at points in time in the past. The auditor can query for entries with their name and for a desired date. Alternatively, the auditor can select a who or what in the Audit Analysis and request to show this entry in the History view. Then the timeline shows the state of the entry before and after the event time.

For a selected entry, the history view shows a graphical timeline with the points in time where the entry was created, modified, and deleted. By zooming in and out the auditor can focus on the interesting time interval.

Additionally, details on the entry's attributes and relationships are displayed for selected points in time. For identities, this includes all privilege assignments, role parameters, accounts, and the risk level. For privileges, this includes all identities that have the privilege assigned. By following reference links, the auditor

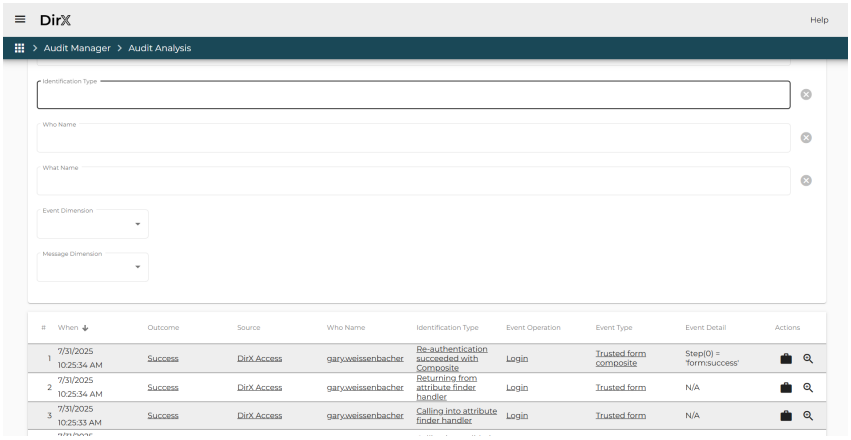

Figure 2 - DirX Audit Analysis - View, filter and analyze Events

can view related entries (for example, the details of an associated role or account).

For a selected entry, the correlated events which changed the entry or which the user has performed can also be viewed. DirX Audit also supports root cause analysis for privilege assignments as shown in figure 3.

Reports View

In the Reports view of DirX Audit Manager the auditor sets up scheduled report jobs. A report job sends an email with one or more report files. Each file can contain one or more single reports. A single report can be a Dashboard chart, a list on audit events or on snapshots of history entries. The schedule will typically be periodically, for example once per month. But the auditor can also request to send it once either at a specific date and time or as soon as possible. In the mail the auditor sets the mail recipients and a body text. The DirX Audit Server will then manage the regular production of the reports and send the e-mails to the intended recipients.

Reports can have parameters defining their scope. As they are typically generated periodically, they require the definition of a time range, for example the previous month.

Other parameters convey the set of events or entries based on attributes such as entry names, risk level, target system names, organizational units, or particular privileges.

Certain reports include a placeholder in their filter criteria, so that their result depends on the report author. For example, the report contains then only the events associated with the organizational unit of the author.

DirX Audit provides several default reports, for example

- Access requests by user, requestor or privilege
- Account and group changes in particular target systems
- Logins, especially failed logins
- Overview on orphaned, imported, or disabled accounts for all or only selected target systems
- Overview on imported, i.e., unsolicited group memberships
- High-risk users
- Overview on particular users including their accounts or roles and groups
- Unused privileges – neither assigned to a user or to a role
- Users of particular roles or groups
- Approval workflows and certification campaigns – both pending and finished
- Details on access reviews that are pending or have been performed last month
- List of users who have not been certified last year

Reports on audit events can contain information on the requestor or causing rule and on the approvers.

Based on the delivered samples administrators can customize their own reports or adapt existing ones.

Reports can be created also from other DirX Audit Manager views based on the current query results and based on pre-configured report templates. HTML and PDF are among the formats supported for output. In this case, reports can be saved to the file system for further distribution and processing.

Event Correlation

Context queries in the Audit Analysis view help to find related audit events for a selected event. Examples are the login operation for an access event or the role assignment that caused the addition of a user into a specific group that enables access to specific resources in a connected system.

Risk Assessment

To classify users into risk categories from low to high, risk factors for users are regularly calculated and stored according to a customizable configuration. Examples for risk factors are SoD violations, imported accounts and group memberships and total number of group memberships. These values and their weighted totals are displayed in DirX Audit Manager's History view as well as in appropriate charts and reports. Compliance managers or managers can then focus on them and try to reduce the number of high-risk users.

Security

To secure access to the DirX Audit system, DirX Audit requires that users are authenticated and that their access to DirX Audit is authorized.

Authentication and Authorization

DirX Audit users can be authenticated against any directory server using LDAP authentication, OpenID Connect or Kerberos.

DirX Audit distinguishes between the following types of users for authorizing access to DirX Audit:

- Audit administrators - can view and manage all public chart component definitions (Dashboard view) and all public filters (Events view)
- Auditors - can view and use the Dashboard public chart components and, public Events filters and view and manage their own Dashboard layout and private Dashboard charts and, public Events filters.
- Restricted auditors – can see and schedule only reports with the tag RESTRICTED, but not the Dashboard, Audit Analysis and History view. Restricted reports include placeholders as filter constraints so that the report output covers only the users of the report author's organization or organizational unit.

Note: The user's membership in configurable groups in the LDAP directory used for authentication specifies the auditor role of the user within DirX Audit. For example, in DirX Identity, there are two predefined groups - Auditors and AuditAdmins - that are controlled by roles.

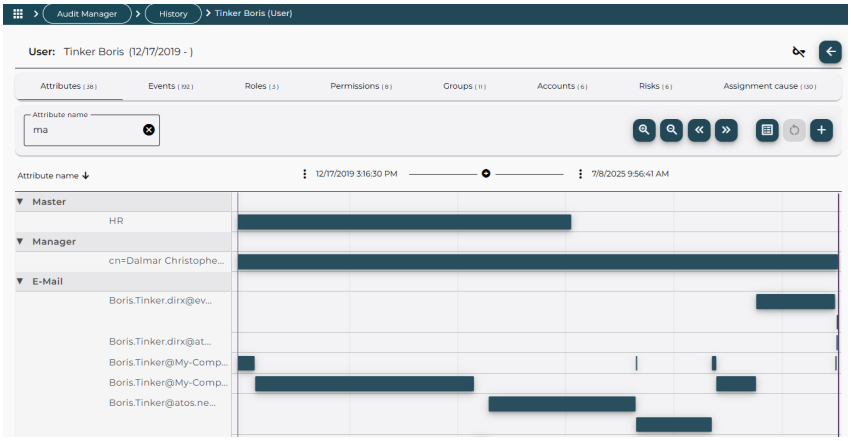

Figure 3 - DirX Audit History View - Timeline with Details

Authorization for Audit Trails

DirX Audit supports fine-grained access control for audit trails. Access policies can be defined that restrict access to trails based on trail content. As an example, auditors may only see trails associated with their organizational unit, that is, where objects of their organizational unit are changed or the actions that a member of their organizational unit has performed.

Access policies are implemented as XACML policies (eXtensible Access Control Mark-up Language) in form of obligations for the SQL queries. DirX Audit implements its own stand-alone Policy Enforcement Point (PEP) and can optionally leverage DirX Access as policy store and policy decision point (PDP). The audit administrator can configure the obligations using the DirX Access Manager. Access policies are usually applied to LDAP groups, but they can also be based on attributes of the auditor's LDAP entry.

Audit Message Transformation

Audit trails can come from different sources in native format. Transformers allow for conversion from the native format to DirX Audit's standard audit message format.

The DirX Audit enrichment functions help to extend the audit messages in the audit trail; in particular, to supply the informational summary that accompanies each audit event

Specific component enrichment operations also generate tags for each imported audit message that form the basis for populating facts and dimensions of the OLAP cubes.

Custom transformation and enrichment functions can be applied to audit messages of applications that are not supported out-of-the-box. Customers can even generate their own tags for events produced by DirX Identity and DirX Access.

Persistent Audit Database

Audit trails are stored securely in both their original and normalized format in the central DirX Audit Database.

Audit producers like DirX Identity can deliver their audit trails secured with a system-specific digital signature to make them tamper-proof; once they are stored in the central DirX Audit Database, these audit trails cannot be changed without compromising the signature. Audit producers like DirX Identity can also generate client-signed audit trails to provide evidence of transactions defined by IAM policies to be high-risk.

For archiving, DirX Audit supports purge and restore of the database or parts of the database in XML format.

A compression mechanism is used to reduce the size of the archived database. In addition, backup and restore can be performed using the native database tools.

To maximize the availability of aggregated audit data, the DirX Audit archiving tools support different lifetimes for audit messages, audit events and OLAP fact tables. Fact tables and their associated dimension tables have the longest lifetime, while the full audit messages with all the details have the shortest. As a result, administrators can export and delete the details of audit messages and the original messages after a

few months, but auditors can still view the charts on the aggregated data and drill down to the audit event informational summaries to understand the operations. If disk space gets short some months later, administrators can delete the summaries, but auditors can still view the charts with the aggregated data from the OLAP cubes.

Multi-Tenancy

One DirX Audit installation can support multiple tenants, for example multiple DirX Identity domains.

The DirX Identity domains can be hosted in the same or in different LDAP servers. The audit events and history snapshots of each tenant are stored in separate audit databases, where access to data of other tenants can easily be prevented.

Each tenant can configure and produce their own reports and charts based on a set of common out-of-the-box templates.

Administration

Audit administrators and auditors are typically responsible for managing queries, reports and access control. System administration tasks include:

- Managing the DirX Audit Manager
- Managing the DirX Audit Message Broker
- Managing the DirX Audit Server
- Managing databases
- Managing audit plug-ins in audit producing products (DirX Identity, DirX Access)
- Managing tenants and their respective databases and message queues

Customization and Extensibility

DirX Audit is designed to be highly customizable and extensible with regard to queries, reports, and to the display of its objects in its user interfaces. Customization features include:

- Connecting the audit data from any application to DirX Audit by transforming the native audit message format to DirX Audit's generic format and importing them using the generic DirX Audit message queue (JMS) or file collector
- Customizing the Dashboard layout and selecting KPI data from existing OLAP fact tables and controlling how it displays this data
- Adding customer specific OLAP tables for use in the Dashboard view
- Adding customer specific OLAP dimension producer components and then using these dimensions in the OLAP tables
- Customizing the default reports supplied for use in the Audit Analysis view
- Creating customer-specific reports using native SQL and placeholders
- Adding specific attribute values to predefined queries
- Defining custom queries
- Customizing table layout of query results such as column visibility
- Creating custom pages: Custom pages are Java Server Faces (JSF) pages that contain only selected GUI components from the DirX Audit Manager. Components, their composition and their layout are completely under the customizer's control
- Adding support for additional languages to DirX Audit Manager; DirX Audit Manager is delivered with two language versions: English and German
- Setting up single sign-on: HTTP header injection functionality can be used to integrate DirX Audit Manager into an existing Web access management or Web single sign- on solution

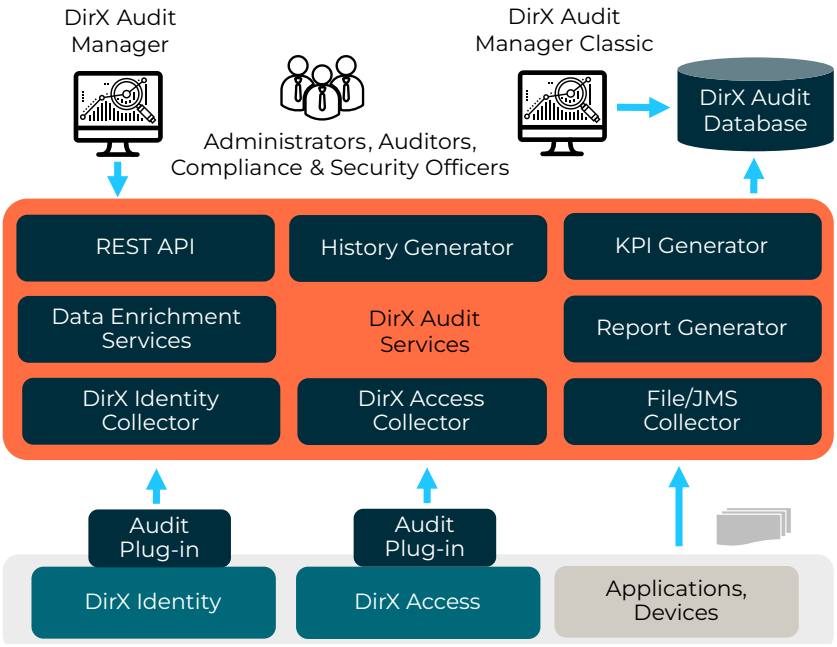

Figure 4 - DirX Audit Architecture

DirX Audit Architecture

DirX Audit components provide the basic machinery for analyzing, correlating, and storing audit data.

These components include:

- DirX Audit Server, a central server that collects, transforms, enriches, and writes the audit trails to the DirX Audit Database.
- DirX Audit Database, which provides central, secure, persistent storage for audit trails from different audit trail producers, derived OLAP data and for DirX Identity history entries.
- DirX Audit Manager, a Web-based user interface to the DirX Audit Database for auditors, security and compliance officers, audit administrators, and users.
- Command-line archive tools, which allow audit administrators to archive and restore audit trails in the DirX Audit Database and maintain DirX Audit Database data.
- Periodic history data synchronization of DirX Identity entries into the central DirX Audit Database.

Figure 4 presents the DirX Audit architecture and its integration points in existing applications from a high-level component standpoint.

DirX Audit Server

DirX Audit Server is the central server that hosts several types of services:

- Collectors retrieve the audit trails from their respective sources and then pass them to services in the DirX Audit Server for transformation, enrichment, and storage. DirX

Audit collector types can be distinguished according to their technology and the format of the audit trails they are able to consume. They can retrieve audit trails from JMS queues in the DirX Audit Message Broker, from files or from an LDAP directory server. DirX Audit's generic JMS and file collectors can be used to connect any application to DirX Audit. In this case, the audit message needs to be compatible to the generic format used by DirX Audit and a custom digest producer needs to be deployed to extend the message with a business summary.

- Data enrichment services that translate the audit trails to business-friendly format and attach tags to the audit trails that can be used for KPIs.
- Post-processing jobs aggregate the data from the OLTP tables and their tags into OLAP (KPI) cubes. They build the basis for charts and reports.
- The History Generator maintains the relationships between historical entries and extends the entries with derived attributes to support richer and faster reports and KPIs.
- The KPI generator creates and populates the OLAP cubes (fact tables along with their dimensions) based on a customizable configuration that describes a filter for the audit events or history entries to be aggregated in a fact table, the dimensions, and the requested facts. These tables are the basis for the graphical charts presented in the DirX Audit Manager's Dashboard view.
- The Report Generator evaluates the report definitions and produces the requested reports according to their schedules.

DirX Audit Database

The DirX Audit store is a relational database that works with popular SQL relational database servers such as Microsoft SQL Server and Oracle Database. The database is used for persistent storage of configuration, event and history data.

DirX Audit Manager

DirX Audit Manager provides a single, central Web-based interface that offers different views of the audit trails and historical identity data stored in the DirX Audit Database. In addition, it provides:

- Convenient correlation of events and activities from different IAM sources in a single user interface with Dashboard and Audit Analysis views for different levels of analysis.
- Point-in-time analysis of identity and identity- related data that has been synchronized from a DirX Identity domain into history entries in the DirX Audit History Database.
- Setup and scheduling of automatic report generation for audit data and historical data analyses.
- Public and private analysis tools with different levels of access, such as public and private Dashboard components and public and private events filters.
- Preconfigured items such as OLAP cubes and Dashboard components to help jumpstart audit and compliance efforts. These items can be customized to specific requirements.

With its intuitive user interface and its access to normalized, centralized audit data, DirX Audit Manager simplifies and expedites the laborious, expensive, and time-consuming process of sifting through obscurely formatted audit trails generated by many different applications and allows for examining an identity's state at different points in time.

DirX Audit Manager provides for both public and private dashboard and query management and provides a set of pre-configured OLAP cubes, dashboard chart components, queries, reports, and statistics to help jump-start audit and compliance efforts. Pre-configured reports, statistics and charts can be customized to specific requirements or created from scratch with add-on tools like Jaspersoft Studio.

DirX Audit History Synchronization jobs

The History Data is synchronized by the DirX Audit History Synchronization jobs. They regularly export snapshots of important DirX Identity entries like users, groups, accounts, roles, permissions and their assignment, together with time validity information. This data is then imported into the central DirX Audit History Database where it is analyzed and processed.

The DirX Audit History Synchronization jobs are running as scheduled tasks on the DirX Audit Server.

Reliability and High Availability

Reliability and high availability of data storage relies on the features of the database used.

DirX Audit can also handle a temporarily unavailable database with automatic recovery.

Supported Standards

DirX Audit components support several standards for connectivity, authentication and authorization, storage, and data formatting:

- The DirX Audit Server is implemented as a set of Apache Camel components, endpoints and routes running as a Spring Boot application.
- The DirX Audit Server uses Java Messaging Service (JMS) for the collection of audit trails.
- The DirX Audit Server uses the public domain components of the Java Management Extension (JMX) for DirX Audit Server monitoring.
- The DirX Audit Manager uses Lightweight Directory Access Protocol (LDAP) for user authentication and authorization to the DirX Audit Database.
- The DirX Audit Manager uses XACML (eXtensible Access Control Markup Language) policies for user authorization to the DirX Audit Database.
- The DirX Audit Manager is a Java Server Faces (JSF)-based Web application.

The DirX Audit Database uses Structured Query Language (SQL) for internal audit data management and retrieval.

System Requirements

Hardware

- Intel server platform for Microsoft Windows Server
- Red Hat Enterprise Linux,
- SUSE Linux Enterprise Server

Memory Requirements:

Main memory: minimum 8 GB

Disk Space: minimum 10 GB plus disk space for data

Software

DirX Audit as a Java application is supported on the following platforms with latest patches / service packs for the selected platform:

- Microsoft Windows Server 2019, 2022 and 2025 (x86-64)
- Red Hat Enterprise Linux Server 8 and 9 (x86-64)
- SUSE Linux Enterprise Server 12 and 15 (x86-64)
- Java SE 21 (LTS) / OpenJDK
- Apache Tomcat 11.0

Virtual Machine Support:

VMWare ESXi, in combination with guest operating systems listed above that are supported by VMWare ESXi

Supported databases:

DirX Audit supports the following databases:

- Microsoft SQL Server Enterprise or Standard Edition 2019 and 2022
- Oracle Database 19c

Browser support for the DirX Audit Manager

- Microsoft Edge 138.0 or newer
- Mozilla Firefox 128.12.0ESR (Extended Support Release)
- Google Chrome 138.0 or newer

DirX Audit Manager

DirX Audit Manager requires installation of Apache Tomcat 11.0 with latest patches/service packs.

DirX Audit Event Collectors

- Collector for DirX Identity supports DirX Identity 8.10 or higher
- Collectors for DirX Access supports DirX Access 9.1 or higher

Report template creation:

- Requires Jaspersoft Studio 6.5.1 or newer

User interface

- English
- German
- French
  (Audit Manager Classic only)

Documentation

- Release Notes

Manuals and Use Case documents are provided in English.

Manuals

- Installation Guide
- Migration Guide
- Introduction
- Tutorial
- Administration Guide
- User Interface Guides:
  - Audit Manager Classic
  - Audit Manager
  - Command Line Interface
- Customization Guide
- History Synchronization Guide
- Best Practices

Manuals are published on docs.dirx.solutions and delivered in PDF and html format.

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. With its analytical features, DirX Audit helps enterprises and organizations to ensure sustainable compliance and provide business intelligence for the risk-based identity and access management processes.

Connect with us

eviden.com