EVIDEN

Identity and Access Management

DirX Audit

Installation Preparation Checklist

Version 9.0, Edition July 2025

Table of Contents

1. Installation Preparation Checklist

This document aims to provide a list of steps that you should check prior to installing and configuring DirX Audit to help you prepare all required materials, files, documents, data and environment. There are the following sections:

- PREPARATION - collecting system requirements, preparing the target environment
- INSTALLATION of DirX Audit and required applications
- CONFIGURATION of DirX Audit
- MAINTENANCE – operation and troubleshooting

While the first three checklists are helpful for correctly, dutifully and thoroughly preparing a one-time procedure, the maintenance checklist is meant as an ongoing upkeeping operation that should be scheduled on a regular basis.

1.1. Preparation

- ☐ *In case of an upgrade installation, backup your existing configuration files*

  in the *install_path***/conf** folder, all customer specific files and/or custom dashboard component configurations

  See:

  specific instructions in the *DirX Audit Migration Guide*

- ☐ *Install JVM*

  on each machine where DirX Audit Manager and DirX Audit Manager Classic (Apache Tomcat), DirX Audit Message Broker and DirX Audit Server are to be operated

  See:

  “Installation Prerequisites” in the *DirX Audit Installation Guide*

- ☐ *Install Apache Tomcat*

  on the machine where DirX Audit Manager and DirX Audit Manager Classic are to be operated

  See:

  “Apache Tomcat Installation” in the *DirX Audit Installation Guide*

  “Supported Apache Tomcat Installations” in the *DirX Audit Release Notes*

- ☐ *Secure Apache Tomcat*

  See:

  “Securing Apache Tomcat” in the *DirX Audit Best Practices*

- ☐ *Prepare truststores and keystores for SSL configuration*

  to secure (encrypt) data transfer

  See:

  “Establishing Secure Communication” in the *DirX Audit Best Practices*

  “Preparing Truststores and Keystores for SSL Configuration” in the *DirX Audit Installation Guide*

- ☐ *Prepare Kerberos configuration file (optional)*

  to support Windows authentication in DirX Audit Manager Classic

  See:

  “Windows Authentication Using the Kerberos Login Module” in the *DirX Audit Administration Guide*

- ☐ *Generate the keytab file and define the service principal name (optional)*

  to support DirX Audit Manager Classic SSO based on SPNEGO / Kerberos

  See:

  “Configuring SSO Web Authentication Using SPNEGO / Kerberos” in the *DirX Audit Administration Guide*

“Authentication Configuration” in the *DirX Audit Installation Guide*

- ☐ *Configure the Internet Browser for Windows SSO Authentication (optional)*

  to support DirX Audit Manager Classic SSO based on SPNEGO / Kerberos

  See:

  “Configuring the Internet Browser for Windows SSO Authentication” in the *DirX Audit Administration Guide*

- ☐ *Setup new databases or consider database backups (for each tenant)*

  up to three databases should be prepared (Config DB, Data DB, History DB)

  consider backing up the whole database or exporting relevant audit events and history entries in case of upgrading an existing installation

  See:

  “Managing DirX Audit Databases” in the *DirX Audit Administration Guide*

- ☐ *Consider the number of tenants to configure*

  See:

  “Managing a Multi-tenant Environment” in the *DirX Audit Administration Guide*

  “Using the Configuration Wizard for the Tenant Configuration” in the *DirX Audit Installation Guide*

- ☐ *Consider what data to collect and synchronize (for each tenant)*

  See:

  “Managing Audit Messages Data” and “Managing History Entries Data” in the *DirX Audit Administration Guide*

  “Controlling the Number and Size of Audit Events” and “Managing History Entries” in the *DirX Audit Best Practices*

- ☐ *Consider what collectors to use (for each tenant)*

  See:

  “Configuring DirX Audit Collectors” in the *DirX Audit Administration Guide*

  “Collectors Configuration” in the *DirX Audit Installation Guide*

- ☐ *Consider data access (audit messages only) control - authorization (for each tenant, optional)*

  See:

  “Managing Authorization PEPs” in the *DirX Audit Administration Guide*

  “Authorization Configuration” in the *DirX Audit Installation Guide*

- ☐ *Consider what scheduled jobs to execute (for each tenant)*

  See:

  “Scheduled Jobs Configuration” in the *DirX Audit Installation Guide*

- ☐ *Consider what History Synchronization jobs to schedule (for each tenant)*

  See:

DirX Audit History Synchronization Guide

”History Synchronization LDAP Configuration” and “Scheduled History Synchronization Jobs Configuration” in the *DirX Audit Installation Guide*

- ☐ *Setup LDAP groups for DirX Audit Manager and DirX Audit Manager Classic authorization (for each tenant)*

  LDAP groups representing Administrator and Auditor DirX Audit Manager and DirX Audit Manager Classic application roles

  See:

  “Authentication Configuration” in the *DirX Audit Installation Guide*

  “Configuring LDAP Authentication” and “Managing Application Roles” in the *DirX Audit Administration Guide*

  “Managing Group Search” and “Slow Authentication Due to Many Groups” in the *DirX Audit Best Practices*

- ☐ *Configure firewalls*

  See:

  “Firewall Configuration Hints” in the *DirX Audit Installation Guide*

- ☐ *Install and configure message broker (optional - when a custom message broker is used)*

  See:

  “Server JMS Collector for DirX Identity Format”, “Server JMS Collector for DirX Access Format” and “Server JMS Collector for DirX Audit Format” in the *DirX Audit Installation Guide*

- ☐ *Prepare the silent installation & configuration files (optional)*

  See:

  “Silent Installation” and “Using Silent Configuration” in the *DirX Audit Installation Guide*

1.2. Installation

- ☐ *Deploy mssql-jdbc_auth-<version>-<arch>.dll file (optional)*

  to support the integrated Windows authentication in the database connectivity

  See:

  “Installation Prerequisites” and “Support for Windows Authentication in Database Connectivity” in the *DirX Audit Installation Guide*

- ☐ *Install DirX Audit*

  See:

  “Installing DirX Audit” in the *DirX Audit Installation Guide*

- ☐ *Deploy Oracle Database JDBC driver (optional)*

  See:

  “Oracle Database JDBC Driver Installation” in the *DirX Audit Installation Guide*

- ☐ *Install DirX Identity JMS Audit Plug-in Handler (optional)*

  provided with DirX Identity (both the plugin and the documentation)

  See:

  “Installing the JMS-Audit Handler” in the DirX Identity Installation Guide

- ☐ *Install DirX Access JMS Audit Plug-in Handler (optional)*

  to be downloaded from the IAM Support Portal (both the plugin and the documentation), ensure that the version matching both DirX Audit and DirX Access is selected

1.3. Configuration

- ☐ *Perform core configuration*

  validate and test settings where provided

  See:

  “Using the Configuration Wizard for the Core Configuration” in the *DirX Audit Installation Guide*

- ☐ *Perform tenant configuration for each tenant*

  validate and test settings where provided

  See:

  “Using the Configuration Wizard for the Tenant Configuration” in the *DirX Audit Installation Guide*

- ☐ *Configure DirX Identity JMS Audit Plug-in Handler (optional)*

  to be configured in the DirX Identity Manager

  See:

  “Configuring the JMS-Audit Handler” in the DirX Identity Installation Guide

- ☐ *Configure DirX Access JMS Audit Plug-in Handler (optional)*

  to be configured locally at the machine where DirX Access is deployed (the documentation is provided with the plugin package available at the IAM Support Portal)

1.4. Maintenance

- ☐ *Update JVM*

  for security reasons, update software when required or recommended

  See:

  “Installation Prerequisites” in the *DirX Audit Installation Guide*

- ☐ *Update Apache Tomcat*

  for security reasons, update software when required or recommended

  See:

  “Supported Apache Tomcat Installations” in the *DirX Audit Release Notes*

- ☐ *Update message broker (optional, when custom message broker used)*

  for security reasons, update software when required or recommended

- ☐ *Manage Cryptographic Material*

  update keys before their expiration

  See:

  “Managing Cryptographic Material” in the *DirX Audit Administration Guide*

- ☐ *Check the Error Logs*

  See:

  “Log Files” in the *DirX Audit Best Practices*

  “Configuring Logging” in the *DirX Audit Administration Guide*

- ☐ *Monitor DirX Audit Databases*

  See:

  “Check the Audit Database Size”, “Maintain Database Indexes” and “Remove Old Data” in the *DirX Audit Best Practices*

  “Using the DirX Audit Tools” in the *DirX Audit Command Line Interface Guide*

  “Tuning Database Performance” in the *DirX Audit Administration Guide*

- ☐ *Monitor system services - Apache Tomcat / DirX Audit Manager container*

  See:

  “Running the DirX Audit Manager Service” in the *DirX Audit Administration Guide*

  “Common Managers Container Configuration” in the *DirX Audit Installation Guide*

- ☐ *Monitor system services - DirX Audit Message Broker*

  See:

  “Monitoring the Message Broker” in the *DirX Audit Administration Guide*

  “Message Broker System Service” in the *DirX Audit Installation Guide*

- ☐ *Monitor system services - DirX Audit Server*

  See:

“Running the DirX Audit Server Service” in the *DirX Audit Administration Guide*

“Application Container Configuration” in the *DirX Audit Installation Guide*

“Check for Audit Message Import Errors” in the *DirX Audit Best Practices*

☐ *Monitor DirX Audit with JMX*

See:

“Monitoring DirX Audit with JMX” in the *DirX Audit Administration Guide*

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.