EVIDEN

Identity and Access Management

DirX Audit

Installation Guide

Version 9.0, Edition September 2025

Table of Contents

Preface

This manual helps you to install DirX Audit. It consists of the following chapters:

- Chapter 1 provides general information about a DirX Audit installation.
- Chapter 2 provides information about local and distributed installations.
- Chapter 3 provides information about the installation procedure.
- Chapter 4 provides information about configuring DirX Audit.
- Chapter 5 provides information on how to install the system services.
- Chapter 6 provides information on how to install the DirX Identity JMS-Audit Handler plug-in.
- Chapter 7 provides information on how to install the DirX Access File-Audit Handler plug-in.

DirX Audit Documentation Set

DirX Audit provides a powerful set of documentation that helps you configure your audit server and its applications.

The DirX Audit document set consists of the following manuals:

- *DirX Audit Introduction*. Use this book to obtain a description of DirX Audit architecture and components.
- *DirX Audit Tutorial*. Use this book to get familiar quickly with your DirX Audit installation.
- *DirX Audit Administration Guide*. Use this book to understand the basic tasks of DirX Audit connectivity administration.
- *DirX Audit Manager Classic Guide*. Use this book to obtain a description of the DirX Audit Manager Classic user interface provided with DirX Audit.
- *DirX Audit Manager Guide*. Use this book to obtain a description of the DirX Audit Manager user interface provided with DirX Audit.
- *DirX Audit Command Line Interface Guide*. Use this book to obtain a description of the command line interface provided with DirX Audit.
- *DirX Audit Customization Guide*. Use this book to customize your DirX Audit environment.
- *DirX Audit History Synchronization Guide*. Use this book to obtain information about the DirX Audit History synchronization jobs.
- *DirX Audit Best Practices*. Use this book to obtain guidelines and tips for avoiding common mistakes and improving the experience of a DirX Audit installation.
- *DirX Audit Installation Guide*. Use this book to install DirX Audit.
- *DirX Audit Migration Guide*. Use this book to migrate DirX Audit from previous versions.
- *DirX Audit Release Notes*. Use this book to understand the features and limitations of the current release.
- *DirX Audit History of Changes*. Use this book to understand the features of previous releases.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

install_path
The exact name of the root of the directory where DirX Audit programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Audit** on UNIX systems and **C:\Program Files\DirX\Audit** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

install_media
The exact path where the DirX Audit installation media is located.

1. About the DirX Audit Installation

This guide provides information about how to install and configure DirX Audit. Installing DirX Audit consists of two phases:

- Running the installation procedure, which copies the necessary files to the target file system and performs an initial deployment.
- Running the configuration procedure which configures the installed software.

New versions of DirX Audit are distributed about every year, while service packs provide intermediate updates (new features or bug fixes). Contact your support organization for the latest information about service packs.

The sections in this chapter provide general information about the installation.

1.1. Supported Relational Databases

DirX Audit can use the following relational databases:

- Microsoft SQL Server
- Oracle Database

For the supported version numbers and distributions, see the *DirX Audit Release Notes*.

You can use the Express editions (of either Microsoft SQL Server or Oracle Database), but these configurations are not recommended for production environments due to the limitations of the Express Editions.

See the chapter "Managing DirX Audit Databases" in the *DirX Audit Administration Guide* for additional information about configuring DirX Audit databases.

1.2. Supported Operating Systems

You can run the DirX Audit software on the following operating systems:

- Linux
- Microsoft Windows Server

For the supported version numbers and distributions, see the *DirX Audit Release Notes*.

DirX Audit runs in 64-bit mode.

Installing as system services is supported on the Windows platform and on Linux platforms that conform to Linux Standard Base Core 3.1 and newer.

1.3. Supported Web Browsers

The following Web browsers have been tested to ensure they work correctly with DirX Audit Manager or DirX Audit Manager Classic:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

For the supported version numbers, see the *DirX Audit Release Notes*.

1.4. Disk Space Requirements

The installation procedure requires 1.5 GB of temporary disk space. The completed DirX Audit installation requires 1.1 GB of disk space.

Additional space is required for data and log files.

1.5. Firewall Configuration Hints

The following table shows the default outgoing communication ports used by DirX Audit Managers (deployed in Apache Tomcat), DirX Audit Message Broker and DirX Audit Server. You should open these ports on firewalls on the machine where DirX Audit is installed (only if you use the corresponding component). When isolating DirX Audit Manager, DirX Audit Message Broker and DirX Audit Server behind firewalls or on secure subnets, ensure that communication between components on these ports is not interrupted.

Service	Non SSL	SSL
DirX Audit Message Broker (Apache ActiveMQ)	30666	30667
DirX Audit Message Broker Console (Apache ActiveMQ admin Web console)		30662
DirX Audit Message Broker (Apache ActiveMQ) JMX interface	30699	
DirX Audit Managers deployed in Apache Tomcat	8080	8443
DirX Audit Server JMX interface - specific port for each tenant	30091 – 30xxx	
DirX Audit Server REST API interface - specific port for each tenant		30501 – 305xx

The following table shows the default incoming TCP ports that should be opened on the other systems that DirX Audit uses (for collecting or storing audit trails; for example, LDAP and DB) (only if you use the corresponding system):

Service	Non SSL	SSL
DB access (JDBC) – SQL Server	1433	

Service	Non SSL	SSL
DB access (JDBC) – Oracle Database	1521	
LDAP server	389	636
Apache ActiveMQ broker (external – non DirX Audit)	61616	61617

Apache Tomcat is not deployed with DirX Audit and its configuration is independent of the product. The port numbers listed here are the default Apache Tomcat values. They can be modified in your deployment and real values must be checked in the Apache Tomcat configuration.

The values listed in the table for DirX Audit Message Broker are the system defaults. You can change the default values for the OpenWire connector and SSL connector, if necessary, by using the DirX Audit Core Configuration Wizard.

The values listed in the table for DirX Audit Server JMX interface are the system defaults and are specific for each configured tenant. You can change the default values by using the DirX Audit Tenant Configuration Wizard.

2. Installation Configurations

DirX Audit supports several installation environments. This section describes two typical installation configurations:

- A complete local installation on a single machine
- A sample distributed installation on several machines

2.1. Installation Prerequisites

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

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

You must also check whether the JAVA_HOME and PATH environment variables are set correctly for your operating system.

If you need to upgrade your Java VM installation later on, follow these steps:

1. Stop the Apache Tomcat (for DirX Audit Managers), DirX Audit Message Broker and DirX Audit Server services for all configured tenants.
2. Upgrade your Java VM installation with a newer version.
3. If you have extended JVM installation with additional files, for example with the **mssql-jdbc_auth-***<version>*-*<arch>***.dll** file to support integrated Windows authentication in database connectivity or your proprietary copy of the **cacerts** file, you must deploy also these files in this step.
4. Check that the JVM path reference is still valid in the following files: *install_path***/dxtrunenv.bat** (*install_path***/dxtrunenv.sh** on Linux) and *install_path***/conf/installation.ini**.
5. Start the Apache Tomcat (for DirX Audit Managers), DirX Audit Message Broker and DirX Audit Server services for all configured tenants manually.
6. Check that the services run correctly.

See the *DirX Audit Release Notes* for supported versions.

2.2. Local Installation

To install all DirX Audit components on a single machine:

1. Install and prepare the Apache Tomcat if you plan to run DirX Audit Manager or DirX Audit Manager Classic and stop the service before DirX Audit installation.
2. Run the DirX Audit installation procedure.
3. In the Choose Install Set dialog, select **All**. **Message Broker**, **Server application**, **Manager application** and **Tools** will be selected.
4. (Optional) Install Oracle Database JDBC driver.
5. Perform the DirX Audit configuration procedure. Now your system is ready to run.

2.3. Distributed Installation

You can also distribute the DirX Audit components across different machines.

If you install DirX Audit in a distributed environment, be sure to update all machines with the new DirX Audit software version. Otherwise, severe inter-operational problems could result.

An example for a high level of distribution is:

- DirX Audit Message Broker runs on machine A.
- DirX Audit Server application containers for all configured tenants and Tools reside on machine B.
- DirX Audit Manager or DirX Audit Manager Classic application container resides on machine C.

To set up this environment:

- Install the DirX Audit Message Broker on machine A:
  1. Run the installation and configuration procedure.
  2. In the Choose Install Set dialog, select **Message Broker**.
  3. Configure DirX Audit Message Broker.
- Install the DirX Audit Server application and its containers on machine B:
  1. Run the installation and configuration procedure.
  2. In the Choose Install Set dialog, select **Server** in **Install Set**. **Server application** and **Tools** are selected in the component tree.
  3. (Optional) Install Oracle Database JDBC driver.
  4. Configure DirX Audit Server for each tenant.
- Install the DirX Audit Manager or DirX Audit Manager Classic application and its container on machine C:
  1. Install and prepare the Apache Tomcat and stop the service before DirX Audit

Manager or DirX Audit Manager Classic installation.

2. Run the installation procedure.
3. In the Choose Install Set dialog, select **Manager** in **Install Set**. **Manager application** is selected in the component tree.
4. (Optional) Install Oracle Database JDBC driver.
5. Configure DirX Audit Manager or DirX Audit Manager Classic.

2.4. Apache Tomcat Installation

To run DirX Audit Manager or DirX Audit Manager Classic, you must install Apache Tomcat, which serves as the DirX Audit Manager's container, from the web site http://tomcat.apache.org. See the *DirX Audit Release Notes* for supported subversions.

The documentation assumes that Apache Tomcat is installed in the *tomcat_install_path* folder.

Make sure that the Apache Tomcat service is running under an account which has same access rights to the DirX Audit deployment as the one used for the DirX Audit installation and configuration so that the Apache Tomcat container used for the DirX Managers can access all DirX Audit resources. Typically, the service account can be the same as the one used for the product installation.

We recommend extending the Tomcat Java Options, especially when running the DirX Audit Managers and the DirX Identity Web Center using the same Tomcat installation (the following description applies to the Microsoft Windows platform):

1. Start *tomcat_install_path***bin****Tomcat***version**w.exe*.
2. Select the Java tab.
3. Set at least **2048** to **Maximum memory pool**.
4. Click **Apply** and then click **OK**.

If you are upgrading from older versions of DirX Audit, be aware that service support for running Apache Tomcat has been removed from DirX Audit Configuration Wizard. To create, configure and run Tomcat (and DirX Audit Managers), use only the service provided by Tomcat installation (as described here). For other platforms, see the Apache Tomcat documentation. If you had the service provided by DirX Audit in the old installation (service DirX Audit Manager X.Y), this service was removed during the upgrade procedure.

We strongly recommend that you run the DirX Audit Manager application via the HTTPS protocol. See the Tomcat documentation for details; for example, https://tomcat.apache.org/tomcat-11.0-doc/ssl-howto.html.

2.5. Support for Windows Authentication in Database Connectivity

If you want to use integrated Windows authentication in database connectivity, you must copy the **mssql-jdbc_auth-***<version>*-*<arch>*.**dll** file into the *jvm_install_path***\bin** folder where *jvm_install_path* represents Java Virtual Machine installation location. The dynamic-link library is distributed together with the Microsoft JDBC Driver for SQL Server.

For details on the Windows authentication in database connectivity, see the chapter "Using the Configuration Wizard for the Tenant Configuration".

2.6. Oracle Database JDBC Driver Installation

To run Oracle Database as the DirX Audit Database, you must install Oracle Database JDBC driver for the supported Java installation and your version of Oracle Database. See the *DirX Audit Release Notes* for the supported Java version.

The JDBC driver (**.jar** file only) must be copied to the following location:

- *install_path***/lib/**, where *install_path* represents the DirX Audit installation location.

2.7. Silent Installation

DirX Audit can be also installed without any interaction (silent mode). Follow these steps to create a silent setup:

- Copy the contents of the folder *install_media***/DirXAudit/***selected_platform* from the DVD to a folder on your machine.
- Customize the installation properties file **dirxaudt.properties** as described in this section.
- Start the installation program in the folder on your machine. Check for errors

The **dirxaudt.properties** file contents are as follows:

```
…
# UI mode for the installer.
# Options: SILENT, CONSOLE or GUI
# Default for Windows:
# INSTALLER_UI=GUI
# Default for Unix:
# INSTALLER_UI=CONSOLE
#
# INSTALLER_UI=<mode>
# Installation property file (this file) given for installation.
```

```
# It's used internally for checking if silent installation has this
file.
# Set to 1 to use this file. The file will be ignored if set to 0.
PROP_USE_FILE=0
#################################################################
#
# DirX Audit specific properties
#
#################################################################
# ---------------------------------------------------------------
# Only for Unix in silent installation and running as root!
# If the installation runs under root, you have to set the user name.
# DirX Audit will be installed under the account of an existing user.
# The user and group must already exist!
# Target Unix user (username or UID)
# PROP_UNIX_USER=<user>
# Target Unix user group (groupname or GID)
# PROP_UNIX_USER_GROUP=<group>
# ---------------------------------------------------------------
# Installation path
# Default for Windows:
# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$DirX Audit
# Default for Unix (installing as root):
# PROP_USER_INSTALL_DIR=$UNIX_OPT$$/$DirX_Audit
# Default for Unix (installing as normal user):
# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$DirX_Audit
#
# PROP_USER_INSTALL_DIR=<path>
# ---------------------------------------------------------------
# Program group for DirX Audit.
# Default:
# PROP_USER_SHORTCUTS=$WIN_COMMON_PROGRAMS_MENU$$/$DirX Audit
V<version>
#
# PROP_USER_SHORTCUTS=<program group>
# ---------------------------------------------------------------
# Java VM for DirX Audit.
#
# PROP_JAVA_HOME=C:\\Program Files\\Java\\jre21
# ---------------------------------------------------------------
# Selected licenses for DirX Audit
```

```
# <license>=[1 | 0]
# 1: license will be selected.
# 0: license will be not selected.
# Support for DirX Identity:
PROP_LIC_PROD_DXI=1
# Support for DirX Access:
PROP_LIC_PROD_DXA=1
# Support for Dashboard components.
PROP_LIC_COMP_Dashboard=1
# Support for History DB components.
PROP_LIC_COMP_HistoryDB=1
# ---------------------------------------------------------------
# Install features for DirX Audit
# <feature>=[1 | 0]
# 1: feature will be installed
# 0: feature will be not installed
# Message broker.
PROP_FEAT_Message_Broker=1
# Server container and server application deployment.
PROP_FEAT_Server=1
# Manager application deployment.
PROP_FEAT_Manager=1
# Tools.
PROP_FEAT_Tools=1
# ---------------------------------------------------------------
# Force Windows restart - (De)-Installation in silent mode
# Note:
# Set to YES when you want to force a reboot after (de-)installation.
#
# PROP_RESTART_NEEDED=YES
# ---------------------------------------------------------------
# Specific InstallAnywhere options for installation.
# File overwrite
# -fileOverwrite_c\:\\example_file.txt=Yes
```

To configure this file for silent installation and other customizations:

- Uncomment the `# INSTALLER_UI=<mode>` line and change it to `INSTALLER_UI=SILENT`. This step is not necessary if the installer is started with the argument -i silent (which enforces silent mode).
- Set the value `PROP_USE_FILE` to **1** if you want to use the customized values from this file.

The settings in the file will be ignored if this property value is not set to 1.

- Customize the `PROP_LIC_...` values according to the features you have licensed, specifying the **`1`** value for features you have licensed and the **`0`** value for features you have not licensed.
- Change (and uncomment) the `PROP_...` values in the section starting with `# DirX Audit specific properties` if you do not wish to use the respective default settings.
- To select a Java VM for DirX Audit that is already installed, customize and uncomment the setting for the property `PROP_JAVA_HOME` according to the inline comments shown in the file contents shown in this section.

The installation properties file must be located in the same folder as the installer and the base name (the file name that precedes the extension) must be the same as the base name of the installer binary.

Configuring a silent installation implicitly configures a subsequent silent un-installation because the UI mode you specify in the installation properties file applies to both the installer and uninstaller binaries. As a result, an uninstallation performed after a silent installation will automatically run in silent mode unless you specify a different mode with command line arguments.

2.8. Preparing Truststores and Keystores for SSL Configuration

We recommend communicating over secure channels between components and services. To set up this environment, you must supply cryptographic material stored in Java keystores and truststores for each endpoint that will communicate over a secure channel. The Configuration Wizard will ask you for these files.

The next sections explain how to prepare individual truststores and keystores (using a newly created Certificate Authority). If you have a general certification service in your company, you should use it to create the certificates instead of creating your own as described in this section. If these certificates are globally trusted by the Java JVM selected for DirX Audit (or you add your company CA certificates to this JVM default Certificate Authority (**ca**) store) you can omit creating the truststores (as no additional stores are required if your JVM already trusts your certificates).

The recommended location for all keystores and truststores is the folder *install_path***/conf/crypto/stores**.

For more information, see the section “Managing Cryptographic Material” in the *DirX Audit Administration Guide*.

2.8.1. Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration

DirX Audit allows you to configure LDAP over SSL (LDAPS) for establishing secure SSL/TLS connections to the LDAP directory server. You must prepare a truststore for this configuration and use it in the "REST Service Authentication Configuration" step for DirX Audit Manager or in the "Authentication Configuration" step for DirX Audit Manager Classic during the tenant configuration. If you are using the same LDAP server for both the authentication and LDAP collector you can create only one truststore and use it in both configurations screens (authentication and LDAP server collector).

To prepare an LDAP truststore:

- Export the DirX Directory server and Certificate Authority (CA) certificates to files.
- Import the DirX Directory server and CA certificates to the truststore.

The next sections detail these tasks.The final truststore file will be named **ldap-ts.jks.**

2.8.1.1. Exporting the DirX Directory Certificates

To export the DirX Directory certificates to files:

- Run DirX Directory Manager. In the Configuration section, select **ldapSSLConfiguration** under **LDAP Configuration Subentries**.
- Select the DirX Directory certificate and then click the disk icon **Export to PEM** to export the server certificate into a PEM file; for example, **dirx_directory.pem**.
- Edit the generated file and remove all sections containing private keys – all lines between (including) **-----BEGIN ENCRYPTED PRIVATE KEY-----** and **-----END ENCRYPTED PRIVATE KEY-----**.

If there are more certificate entries remaining in the file (there are lines between the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** lines), you need to split them into separate files and import them one by one. Typically, the exported file will contain two such entries – the first is the server certificate and the second is the CA (Certificate Authority that signed the server certificate) certificate. You need to import all of these into the truststore. For the purpose of the next example, let's assume that you have two of these separate certificates exported: one for the server certificate named **server.pem** and the CA certificate named **ca.pem**.

2.8.1.2. Importing the DirX Directory Server and CA Certificates

- Run the command prompt and navigate to the location where you have separate certificates exported.
- Import the server certificate **server.pem** into the truststore **ldap-ts.jks**. Run the following command, enter the password and then press Enter:

```
keytool -keystore ldap-ts.jks -importcert -alias dirxserver -file
```

```
server.pem
```

- Import the CA certificate **ca.pem** into the truststore **ldap-ts.jks**:

```
    keytool -keystore ldap-ts.jks -importcert -alias dirxca -file
ca.pem
```

2.8.2. Preparing the DirX Access Server Secure Connection

To set up the secure connection to DirX Access Server when a DirX Access PEP is configured in the DirX Audit authorization settings, you need to use the relevant DirX Access Server certificate and the relevant DirX Access Server CA certificate (the Certificate Authority that signed the server certificate) from the DirX Access Server. You need to create your own truststore containing the exported certificates and then use this truststore in the DirX Audit Authorization – DirX Access PEP configuration.

2.8.3. Preparing the LDAP Collector

If you set up the collector for the same LDAP server as you are using for authentication, you can use the truststore you already created or create a new one by following the steps described in the section “Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration”.

You must use the prepared truststore described in the Tenant configuration procedure’s “Server LDAP Collector for DirX Identity Format” step for establishing secure SSL/TLS connection to the server LDAP collector.

2.8.4. Preparing the Message Broker

DirX Audit allows you to configure Message Broker over SSL to establish secure SSL/TLS connections to the Broker and the Broker admin console. You must prepare a keystore and a truststore for this configuration and use them in the **Message Broker Connectivity** step in the Core configuration.

If you want to use SSL for connecting DirX Identity JMS Audit Handler to the DirX Audit Message Broker, make sure to import the CA certificate of the broker into the truststore of the Java VM running the IdS-J server. For more information, see the *DirX Identity Installation Guide*.

The keystore contains the private key for the Broker and the admin console and is used by the Broker.

The truststore contains the public certificate of the Broker and the Certificate Authority (CA) and is used by the Broker and all clients (for example, the Server JMS collectors, Identity Audit Plugin and DirX Access Audit Plugin).

To prepare the Message Broker certificates:

- Create the CA certificate in the file **dxt-ca.jks**.
- Create the Message Broker keystore in the file **broker-ks.jks**.
- Create the Message Broker truststore in the file **broker-ts.jks**.

The next sections detail these tasks.

2.8.4.1. Creating the CA Certificate

To create the CA certificate:

1. Create the keystore file **dxt-ca.jks** and then create a new CA key and certificate with the validity of 10 years (3650 days)

```
    keytool -genkeypair -keystore dxt-ca.jks -alias dxtca -keyalg RSA
-dname CN=DXTCA,O=Demo -ext bc:c -validity 3650
```

2. Export the CA certificate in the PEM format:

```
    keytool -keystore dxt-ca.jks -alias dxtca -exportcert -rfc > dxt-
ca.pem
```

2.8.4.2. Creating the Message Broker Keystore

To create the keystore:

1. Create the keystore file **broker-ks.jks** and create a new key for the Broker. The given CN should match the hostname of the machine:

```
    keytool -genkeypair -keystore broker-ks.jks -alias broker -keyalg
RSA -dname CN=server.demo.org,O=Demo
```

2. Create the certificate signing request for this certificate:

```
    keytool -keystore broker-ks.jks -certreq -alias broker >
broker.csr
```

3. Sign the prepared certificate with your CA (for the validity of 5 years) and export it into

PEM format. The specified DNS extension must match the full hostname of the machine where the broker is installed:

```
    keytool -keystore dxt-ca.jks -gencert -alias dxtca -ext
ku:c=dig,keyEncipherment,keyAgreement -ext san=dns:server.demo.org
-validity 1825 -rfc -infile broker.csr > broker.pem
```

4. Combine the CA and server certificate and import the signed certificate back to the keystore:
   Windows: `copy dxt-ca.pem+broker.pem chain.pem`
   Linux: `cat dxt-ca.pem broker.pem >chain.pem`

```
    keytool -keystore broker-ks.jks -importcert -alias broker -file
chain.pem
```

2.8.4.3. Creating the Message Broker Truststore

To create the truststore:

1. Import the CA certificate to the truststore **broker-ts.jks**:

```
    keytool -keystore broker-ts.jks -importcert -alias dxtca -file
dxt-ca.pem
```

2. Import the server certificate to the truststore:

```
    keytool -keystore broker-ts.jks -importcert -alias broker -file
broker.pem
```

2.8.5. Preparing DirX Audit Manager and DirX Audit Manager Classic

We strongly recommend that you run the DirX Audit Manager and DirX Audit Manager Classic applications via the HTTPS protocol. See the Tomcat documentation for details, for example, https://tomcat.apache.org/tomcat-11.0-doc/ssl-howto.html.

You can use the same steps as in the section “Preparing the Message Broker” to prepare the keystore and truststore for Tomcat installation hosting the DirX Audit Manager and DirX Audit Manager Classic applications. You should use the same CA and just generate new key and certificate for the Tomcat server. The keystore and truststore files can be named **tomcat-ks.jks** and **tomcat-ts.jks** respectively.

2.8.6. Preparing DirX Audit Server

We strongly recommend that you run the services (especially REST services) provided by the DirX Audit Server application via the HTTPS protocol.

You can use the same steps as in the section “Preparing the Message Broker” to prepare the keystore and truststore for the DirX Audit Server application. You should use the same CA and just generate new key and certificate for the Tomcat server. The keystore and truststore files can be named **server-ks.jks** and **server-ts.jks** respectively. You should generate a separate set of keys and certificates for each tenant as each tenant will run its own instance of the DirX Audit Server application.

3. Installing DirX Audit

This chapter describes how to run the DirX Audit installation procedure to install the DirX Audit software on a machine and how to use the procedure to uninstall it.

3.1. Installing DirX Audit

The procedure described here installs all DirX Audit components on one machine. See the chapter "Installation Configurations" for instructions on how to create distributed installations.

3.1.1. Before You Begin

Before you begin the DirX Audit installation, be sure to read the instructions given here that apply to your target operating system.

If you plan to run DirX Audit Manager or DirX Audit Manager Classic, install and prepare the Apache Tomcat but stop the Apache Tomcat service before installation. See the section "Apache Tomcat Installation" in "Installation Configurations".

3.1.1.1. Windows Instructions

Important: The installation path must be shorter than 50 characters.If you change the default installation path, please keep in mind that the maximum length of the absolute path is 50 characters; otherwise, you may have problems deleting the deployment folder (the entire path is limited to 255 characters and the deployment uses up to 200-character-long paths).

3.1.1.2. UNIX Instructions

The login name of a UNIX user determines the default destination folder for installation. The folder is different for root and for other users:

- For root, the folder is **/opt/DirX_Audit**.
- For other users, the folder is *user_home_directory***/DirX_Audit**, where *user_home_directory* is the home directory of the specified account.

We strongly recommend that you use a separate (not root) account for DirX Audit. You must create this account before you start the DirX Audit installation.

You can choose a different user during the installation if started as root. The selected user will then be used to run the installed software and related services.

A graphical and a command-line based (console mode is the default interface) installation procedure is available. The installation procedure given in this chapter shows the graphical installation procedure. The screenshots are taken on Windows Server. The look on UNIX is slightly different. During the graphical installation mode, you can click Cancel at any time to leave the installation program. You can click Previous at any time to return to a previous dialog.

Console mode mimics the default GUI steps provided by InstallAnywhere and uses standard input and output. You do not need X Windows (X11) to run the DirX Audit installation in console mode. Console mode outputs text to the console line-by-line. It does not allow you to format, clear the screen, or position the cursor. Because the console mode information is nearly the same as the information provided in the graphical installation procedure, it is not described here.

In console mode, you must respond to each prompt to proceed to the next step in the installation. If you want to return to a previous step, type back. You can type quit at any time to cancel the console procedure.

Important: The installation path must not contain spaces, or some tools may not be able to start or may operate incorrectly. Use underscores instead of spaces in the installation path.

3.1.2. Starting the Installation

This section provides operating system-specific instructions for starting the DirX Audit installation.

3.1.2.1. Windows Instructions

To start the DirX Audit installation on Windows Server:

- Log on as administrator.
- Run **dirxaudt.exe** from the *installation_medium*/**Installation/DirXAudit/Windows** folder.

3.1.2.2. UNIX Instructions

To start the DirX Audit installation:

- Log in as a UNIX user. If you want to install DirX Audit using a different account, log in as root.
- Insert the installation medium that corresponds to your UNIX system. If the system does not mount the installation medium automatically, you must mount it manually.
- Open a shell.
- Change the working directory to the following path:
  mount_point/**Installation/DirXAudit/Linux**. In the shell, you can use the following command:
  cd *mount_point*/**Installation/DirXAudit/Linux**

- Start the installation. To run the graphical installation, type the following command:

```
sh ./dirxaudt.bin -i gui
```

- or to start a console installer from the command line, type the following command:

```
sh ./dirxaudt.bin
```

- or start the installer in the console (default) user interface (UI) mode with the following command:

```
sh ./dirxaudt.bin -i console
```

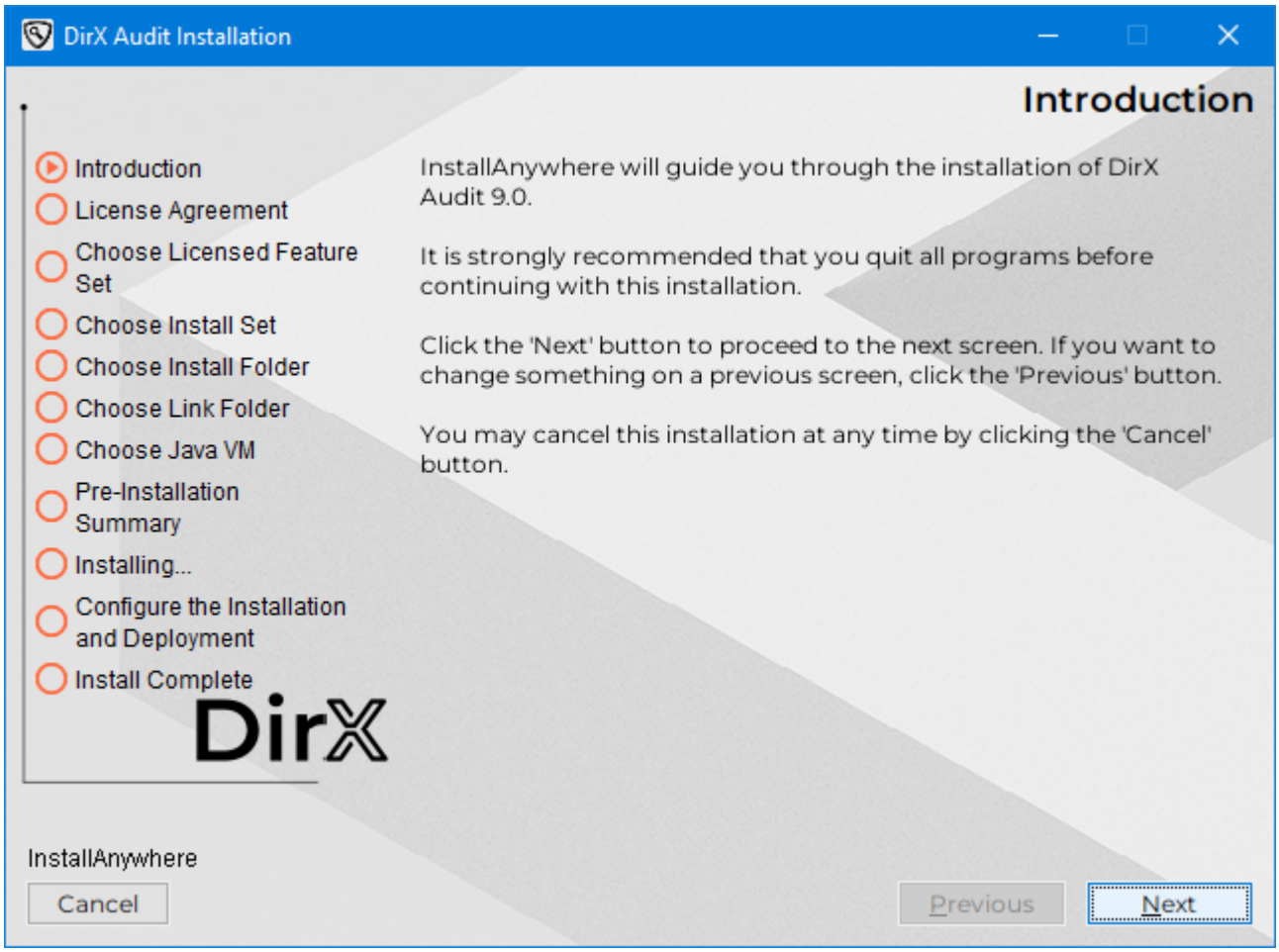
- To run the silent installation, type the following command:

```
sh ./dirxaudt.bin -i silent
```

3.1.3. Graphical Installation Procedure

This section steps through the dialogs presented by the graphical installation procedure.

3.1.3.1. Introduction



Click **Next** to go to the next dialog.

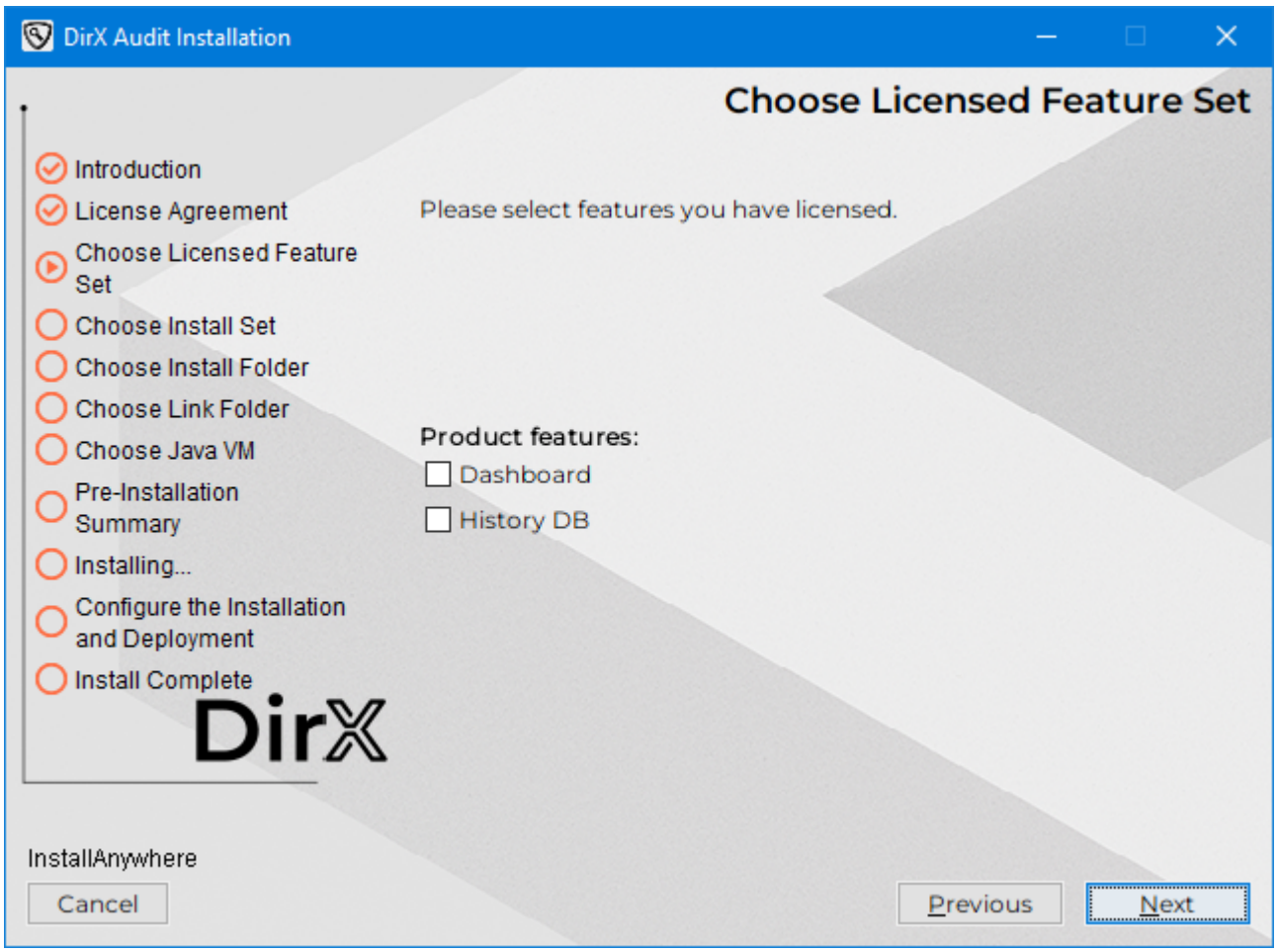
You can click **Cancel** at any time to leave the installation program. You can click **Previous** at any time to return to a previous dialog.

3.1.3.2. License Agreement

Setup displays a License Agreement dialog.

Read the licensing information. Select **I accept the terms of the License Agreement** if you agree, and then click **Next**.

3.1.3.3. Choose Licensed Feature Set

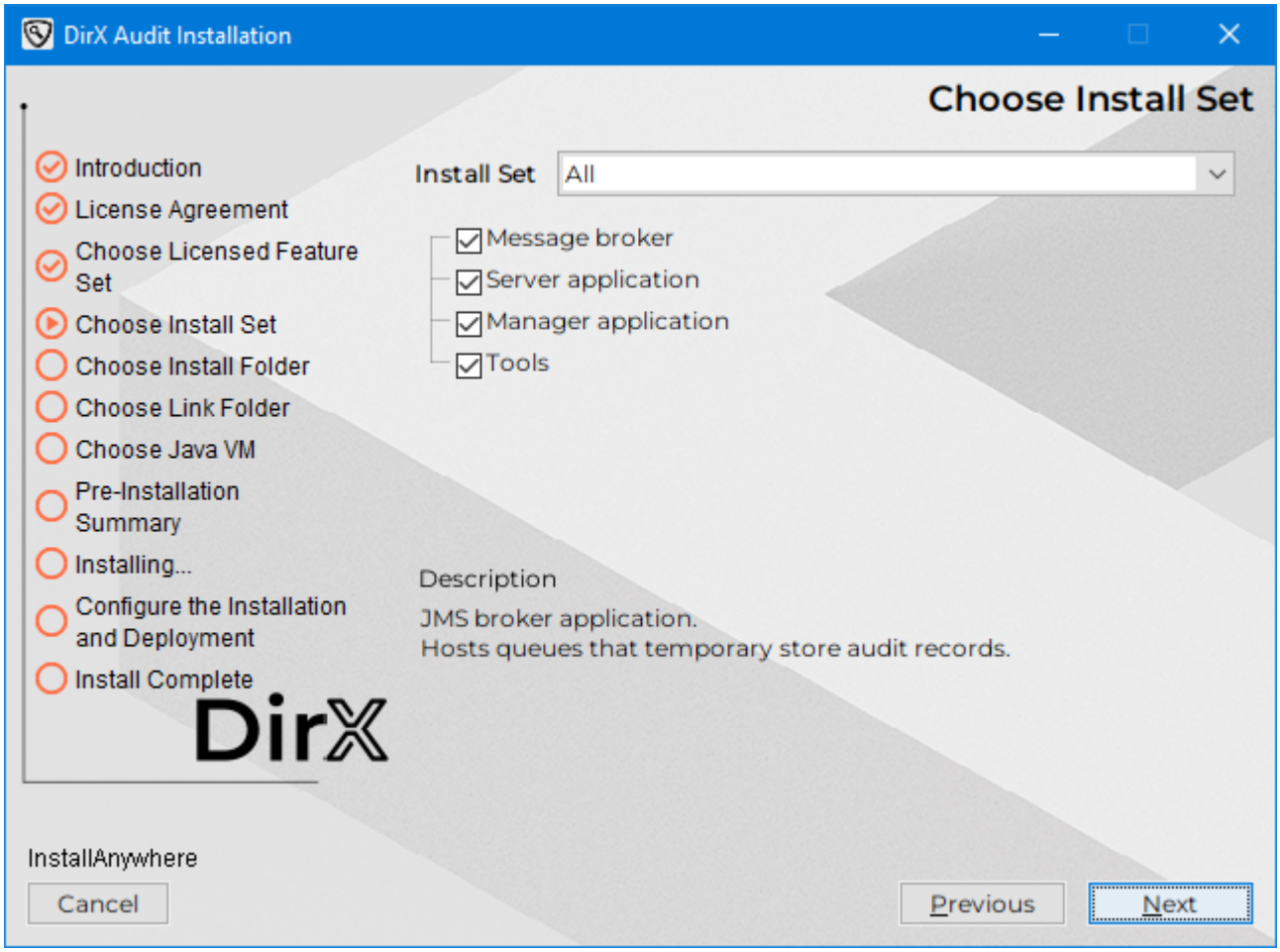


Setup displays a Choose Licensed Feature Set dialog. Audit Analysis and Reports are “core” features, they are always enabled and are not licensed separately.

In **Product features**, you can select the features you are licensed for:
Dashboard - Enables DirX Audit’s dashboard feature.
History DB - Enables DirX Audit’s History DB feature.

Make your selection and then click **Next** to go to the next dialog.

3.1.3.4. Choose Install Set



Setup displays a Choose Install Set dialog. In **Install Set**, you can select:

All - Installs all DirX Audit components on this machine.

Message Broker - Installs only DirX Audit Message Broker.

Server - Installs only DirX Audit Server application container and tools.

Manager - Installs only DirX Audit Manager and DirX Audit Manager Classic application deployment.

Custom - Allows you to define the set of components you would like to install on this machine.

The components visible in the tree that you can select are:

- Message broker (DirX Audit Message Broker). You must select this component if you need to collect audit messages through JMS queues (for example, DirX Identity workflow audit messages).
- Server application. You must select this component if you want to run the DirX Audit Server.
- Manager applications. The DirX Audit Manager and DirX Audit Manager Classic application container, the Apache Tomcat installation is required.
- Tools. Additional tools for DirX Audit (for example, database export, import, purge and maintenance utilities). Tools are installed together with DirX Audit Server application container because they are used for the maintenance and migration process.

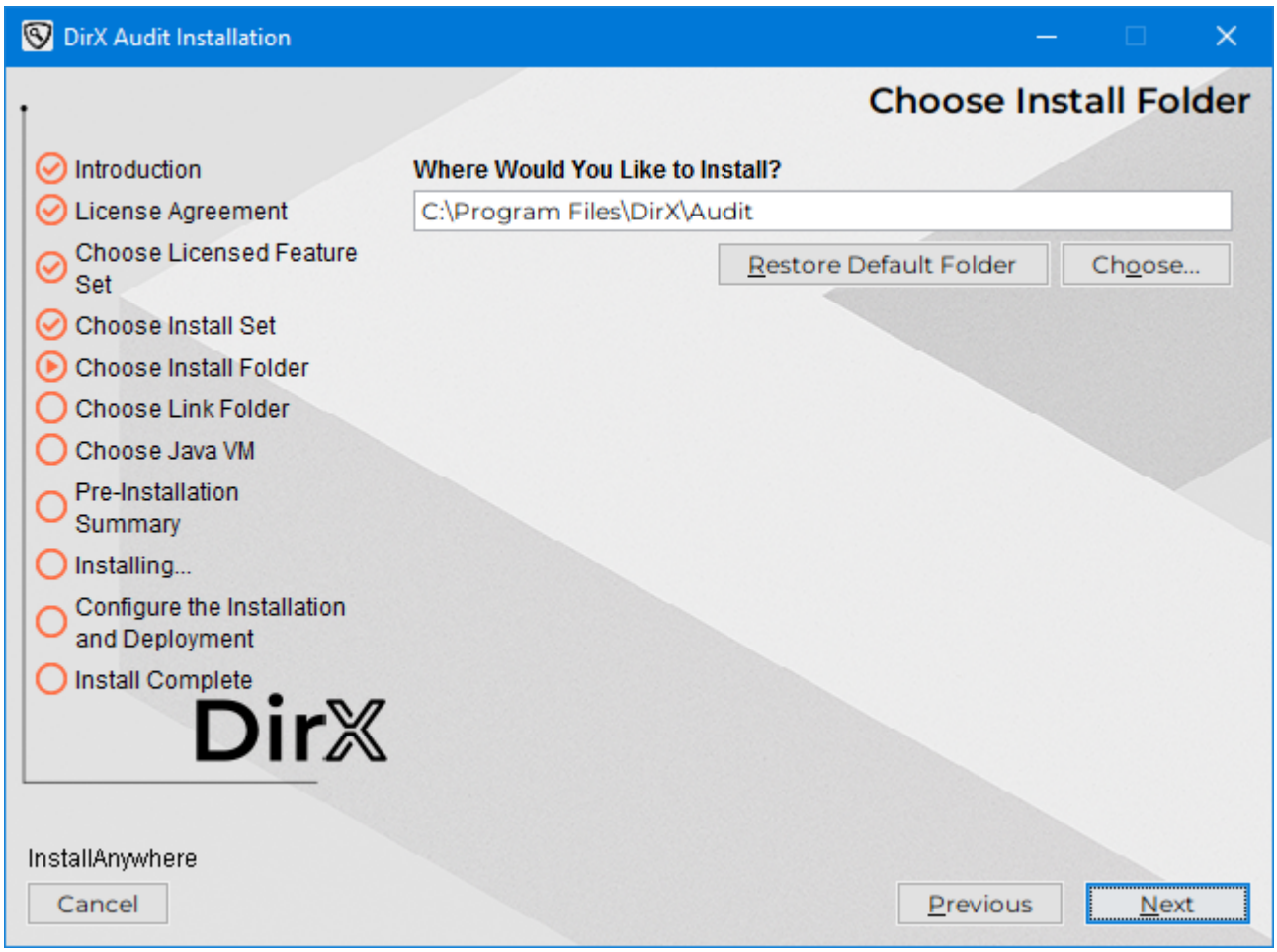
Make your selection and then click **Next** to go to the next dialog.

3.1.3.5. Choose Target User Account

Setup displays a Choose Target User Account dialog. This step is applied only when installing on the UNIX platform.

Make your selection and then click **Next** to go to the next dialog.

3.1.3.6. Choose Install Folder



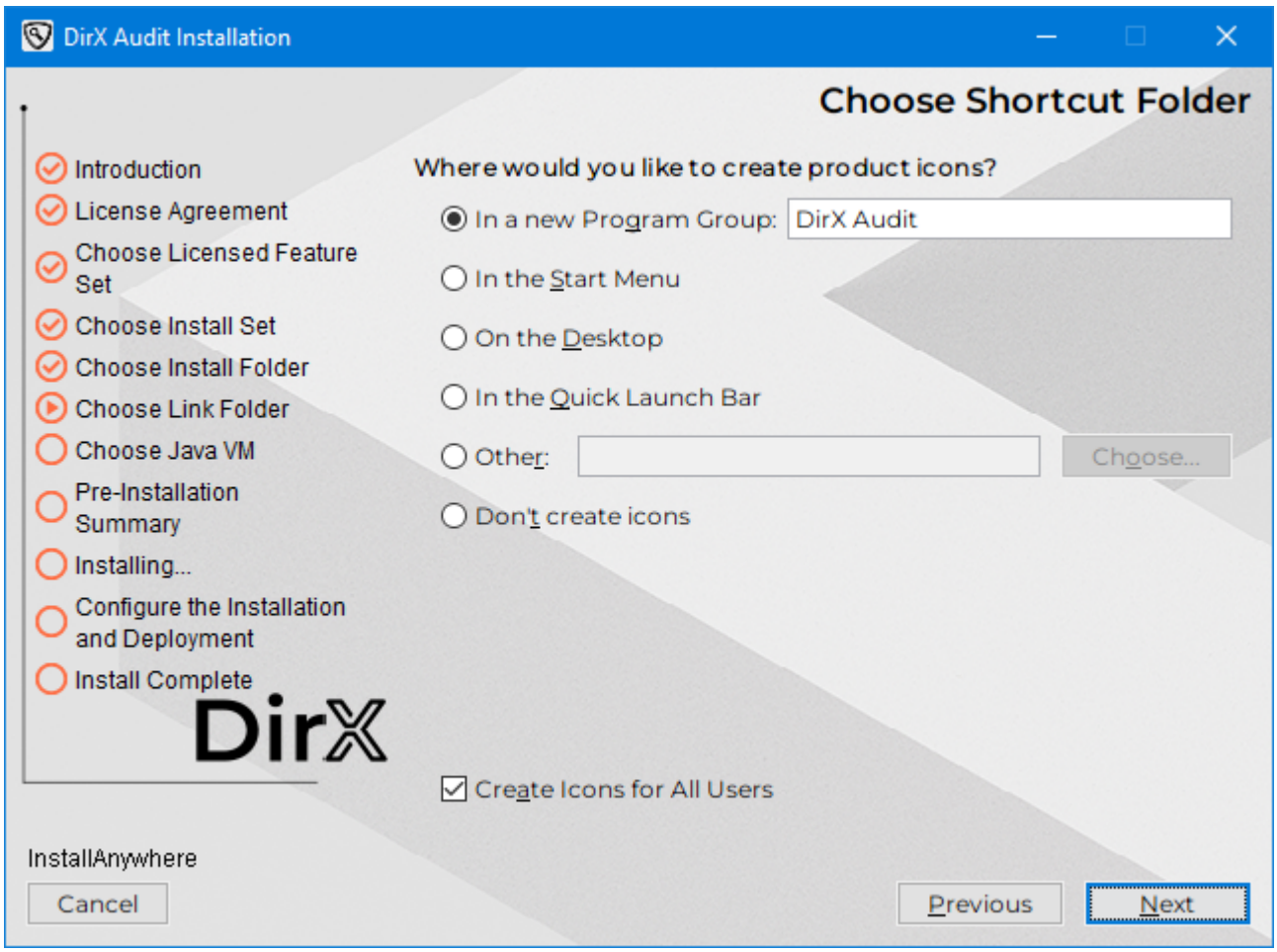
The setup tries to detect the correct installation path for DirX Audit if it is already installed on the machine. In such case, this dialog will be skipped entirely, and the installation will proceed using the existing installation path for DirX Audit. However, if DirX Audit is installed but the installation path wasn't detected properly, please select the correct folder manually. A default installation path is provided if installing for the first time. The default installation folder on Windows is **Program Files\DirX\Audit**.
Program Files contains the fully-qualified name of the folder defined by Windows to store applications.

See the section "Before You Begin" in "Installing DirX Audit" for the Linux default installation folders.

In this dialog, you can:

- Click **Next** to select the default location.
- Click **Choose ...** to select another installation folder, and then click **Next**.
- Click **Restore Default Folde**r to select the default installation folder, and then click **Next**.

3.1.3.7. Choose Shortcut Folder

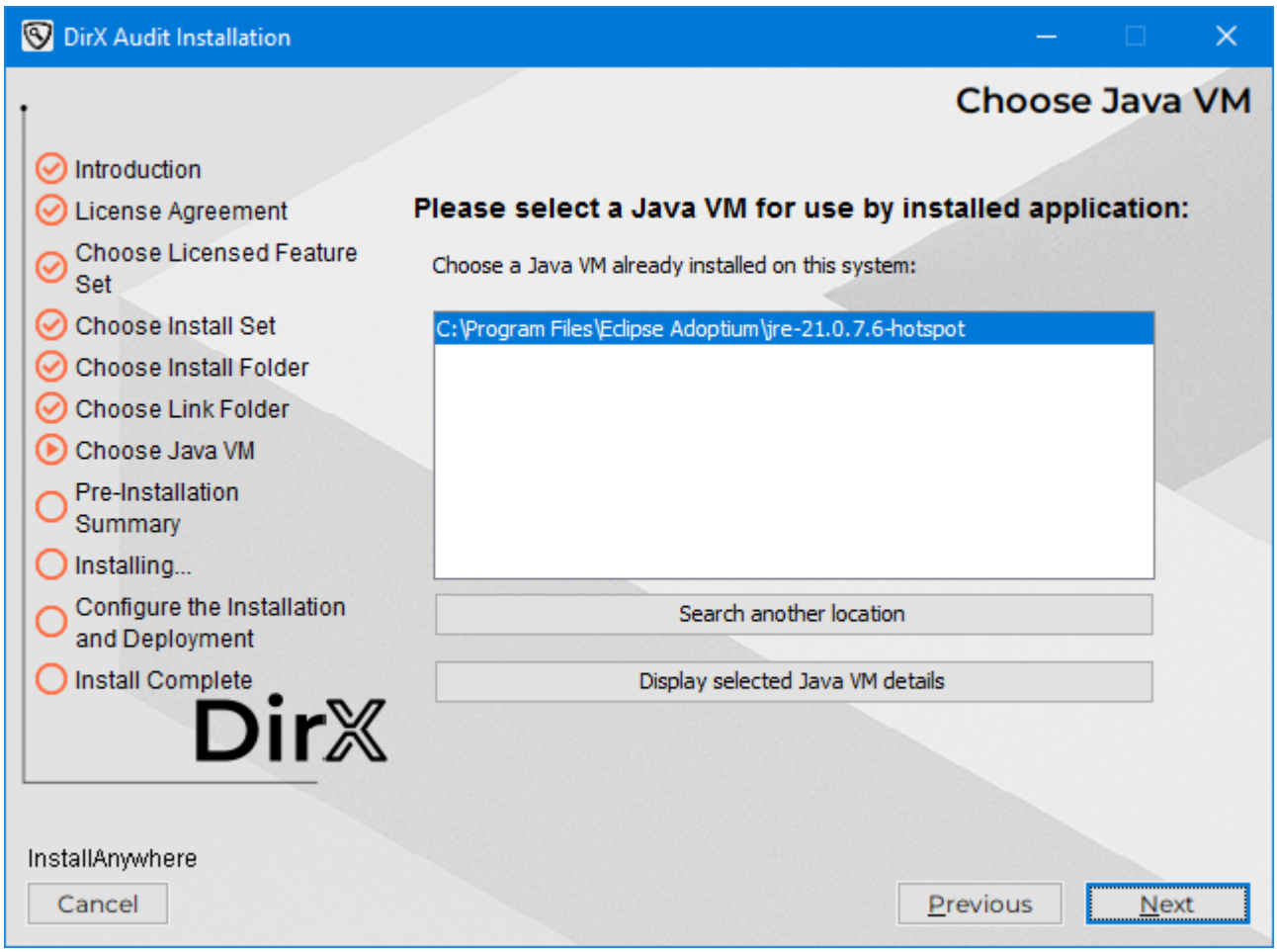


The Choose Shortcut Folder dialog allows you to select a program group for DirX Audit. The default program group is **DirX Audit**. In this dialog, you can (on Windows):

- Click **Next** to select the default program group.
- Click **In a new Program Group** (or **In an existing Program Group**) and select a program group. Click **Next**.
- Click **In the Start Menu** and then click **Next**.
- Click **On the Desktop** and then click **Next**.
- Click **In the Quick Launch Bar** and then click **Next**.
- Click **Other** and then **Choose ...** to select another program group. Click **Next**.
- Click **Don't create icons** and then click **Next**.

You can also uncheck the **Create Icons for All Users** checkbox.

3.1.3.8. Choose Java VM



Setup tries to detect Java VMs installed on the machine.

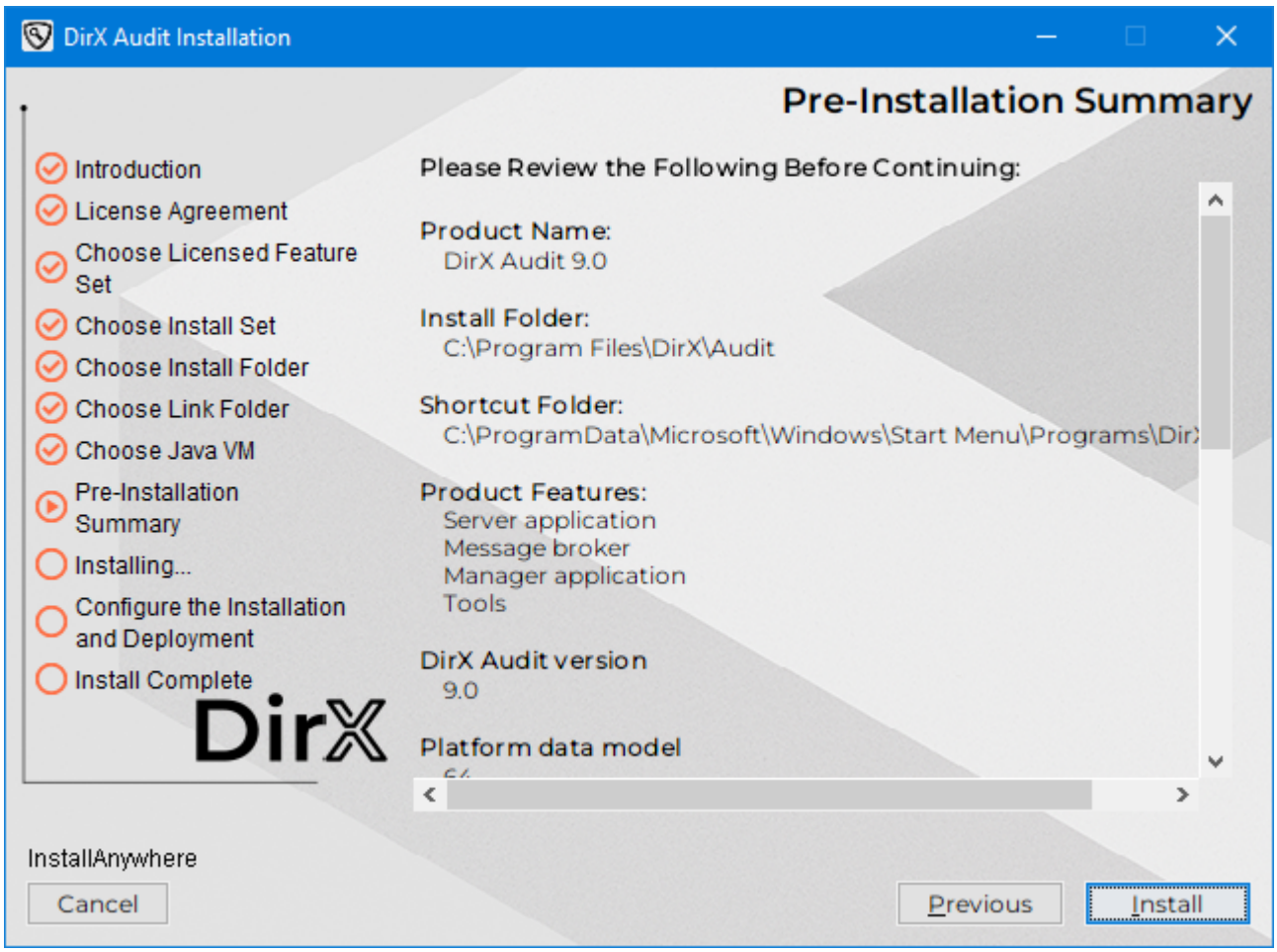
In this dialog, you can:

- Select Java VMs installed on the machine in the **Choose a Java VM already installed on this system** window.
- Click **Search another location** to select a Java VM which is not listed in the dialog.
- Click **Display selected Java VM details** to view details of the selected Java VM.

If you don't see any Java VM installed on your machine, make sure you have an appropriate Java VM installed and also check whether the JAVA_HOME and PATH environment variables are set correctly for your operating system. See the *DirX Audit Release Notes* for supported versions.

Make your selection and then click **Next** to go to the next dialog.

3.1.3.9. Pre-Installation Summary



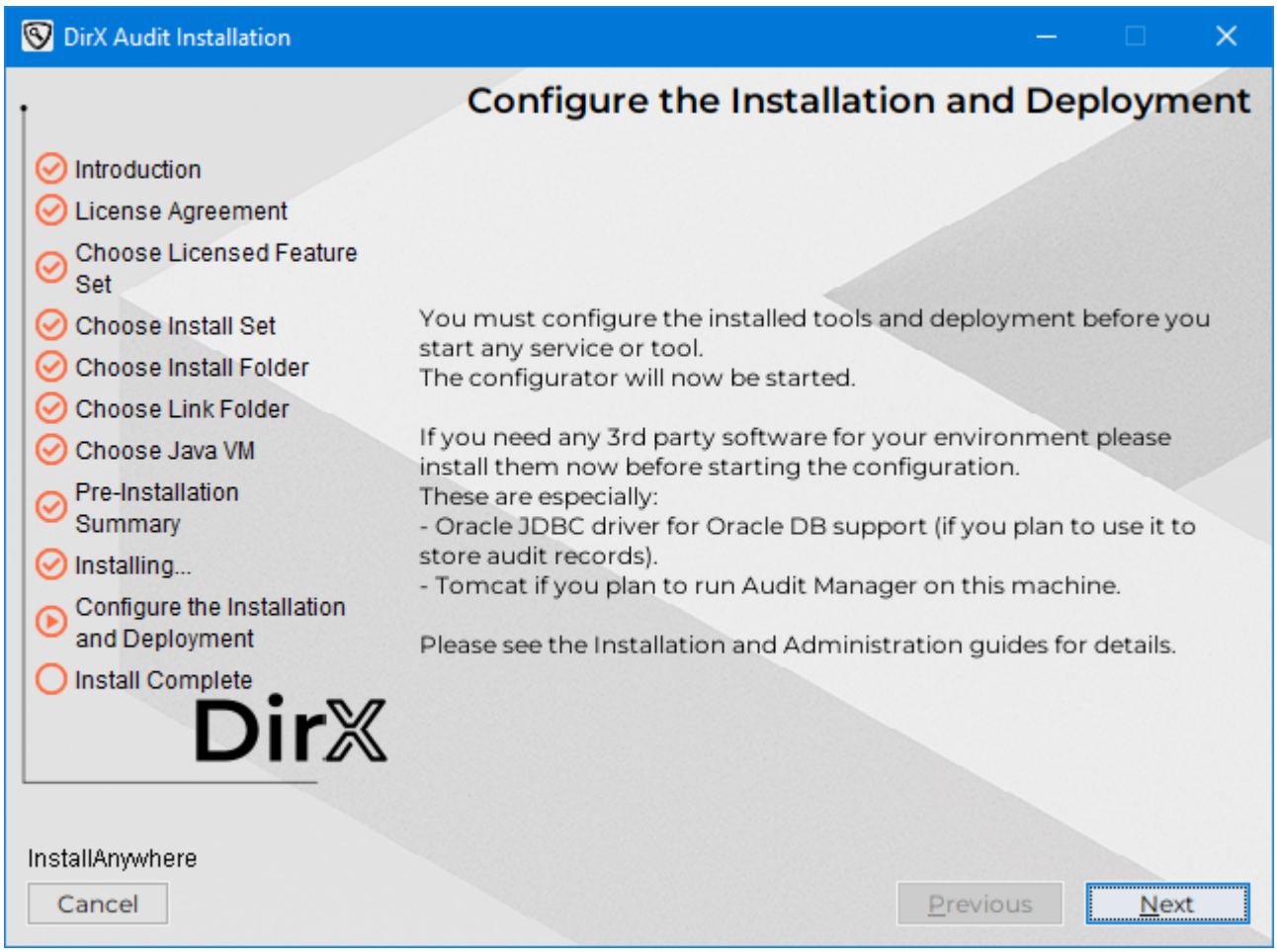
Setup displays the installation selections you have made and asks you to review them.

- Click **Previous** to change any settings you have made. Otherwise, click **Install**.

3.1.3.10. Installing DirX Audit

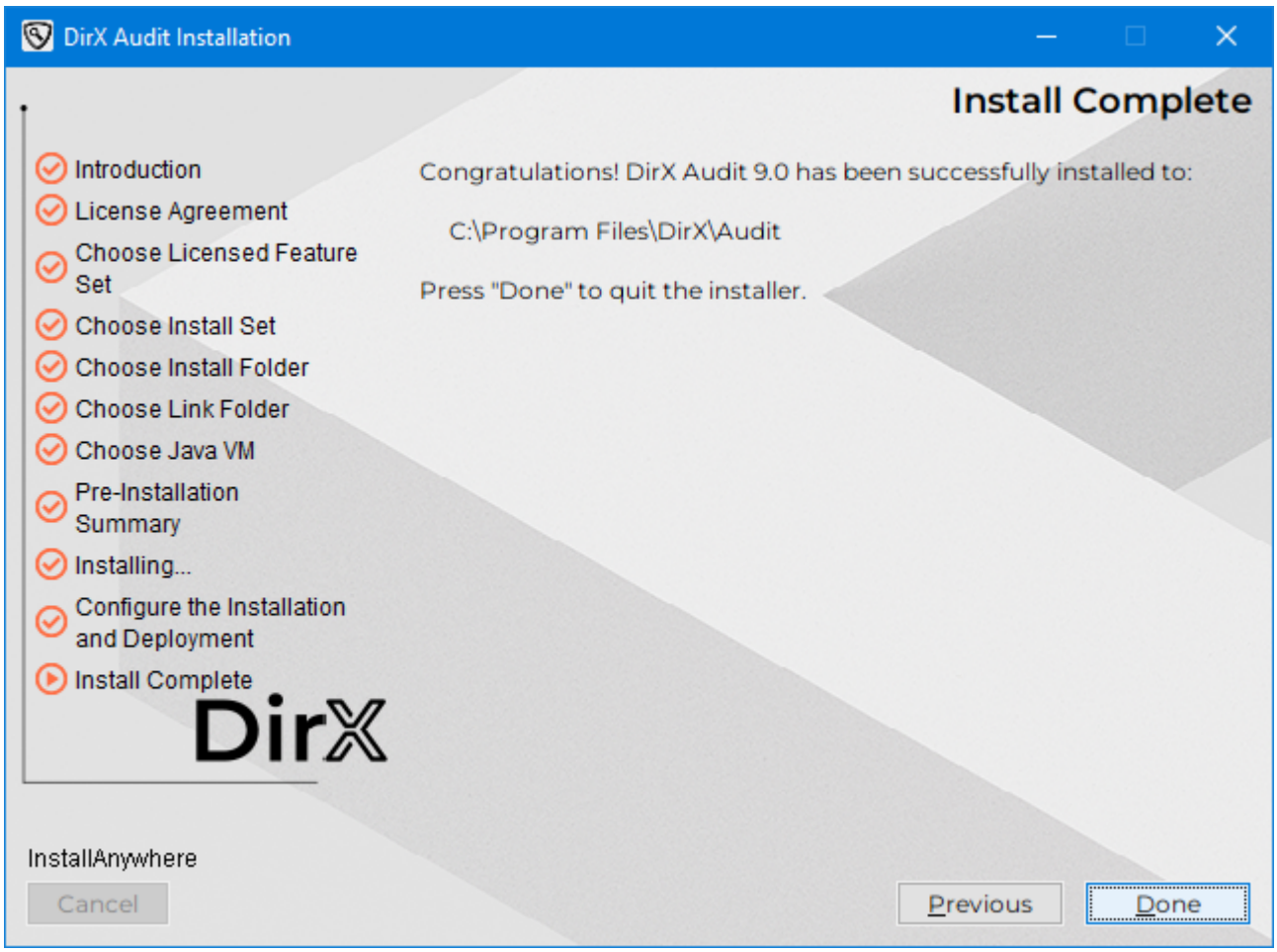
Setup displays the Installing DirX Audit dialog.

3.1.3.11. Configure the Installation and Deployment



The installation procedure displays a window with requirements that must be met before you can proceed with configuring the tools and deployment. Check the requirements and then click **Next** to start the DirX Audit Configuration Wizard. See the chapter "Configuring DirX Audit" for instructions on how to use the DirX Audit Configuration Wizard. When the wizard completes, the installation and configuration process completes.

3.1.3.12. Install Complete



Setup displays the Install Complete dialog. If you are installing DirX Audit and no errors have occurred, click **Done** to quit the installer.

3.2. Uninstalling DirX Audit

This section describes how to uninstall DirX Audit on Windows and UNIX systems.

3.2.1. Starting Uninstallation

To start the uninstallation procedure, perform these steps:

3.2.1.1. Windows Instructions

On your computer, open Programs/apps and Features.

Scroll down to **DirX Audit 9.0**, click it and then select **Uninstall**.

3.2.1.2. UNIX Instructions

- Log in as a UNIX user that has sufficient permissions for uninstallation (the same user that installed it or root).
- Type **cd** *install_path*/**Uninstaller**, for example: *user_home_directory*/**DirX_Audit/Uninstaller**
- To use the graphical uninstallation, type:

```
sh ./Uninstall_DirX_Audit -i gui
```

- or to use the console uninstallation, type:

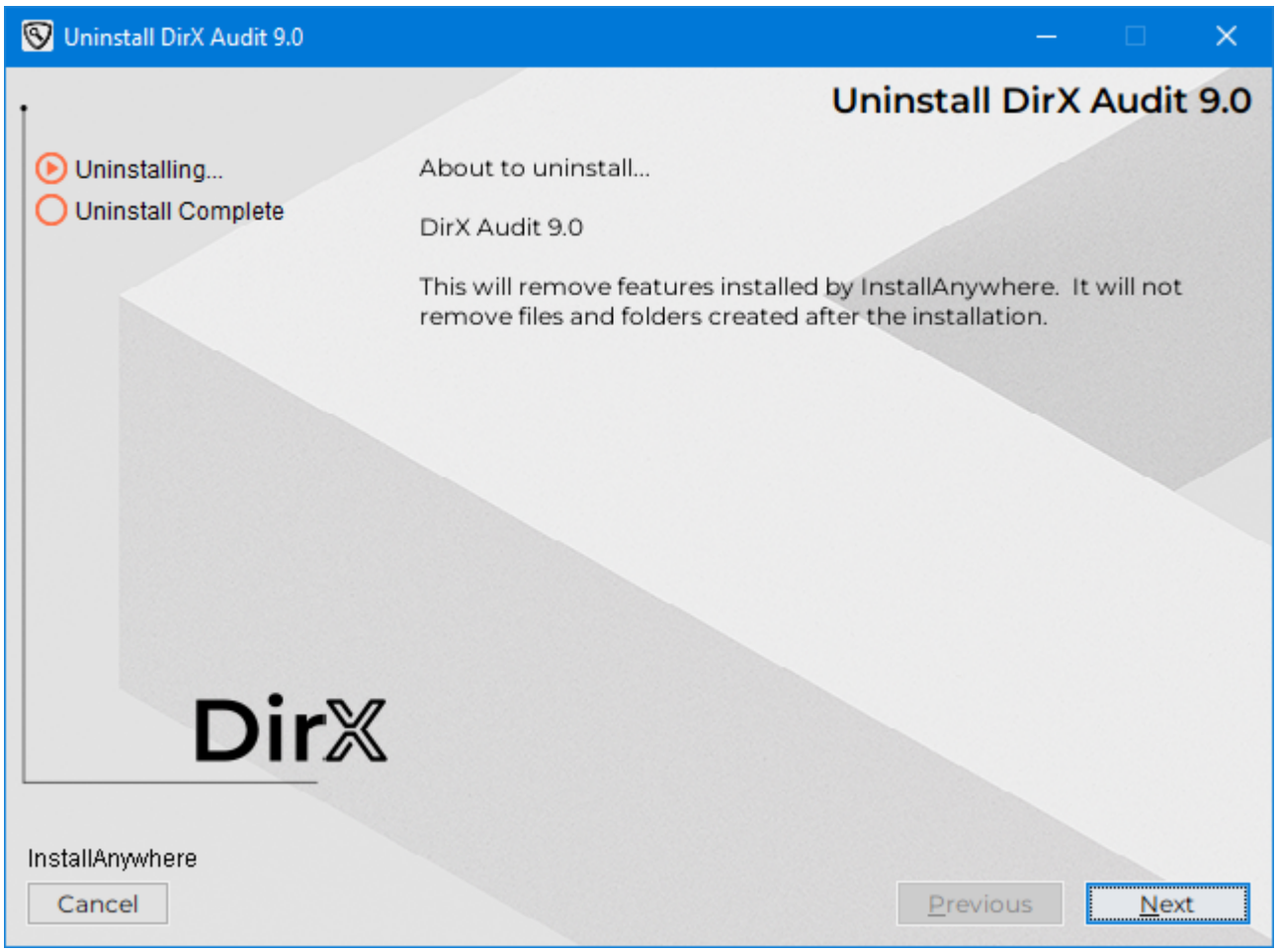
```
sh ./Uninstall_DirX_Audit –i console
```

The uninstallation starts and displays the Uninstall DirX Audit dialog.

3.2.2. Graphical Uninstallation Procedure

This section steps through the dialogs presented by the graphical installation procedure.

3.2.2.1. Uninstall DirX Audit

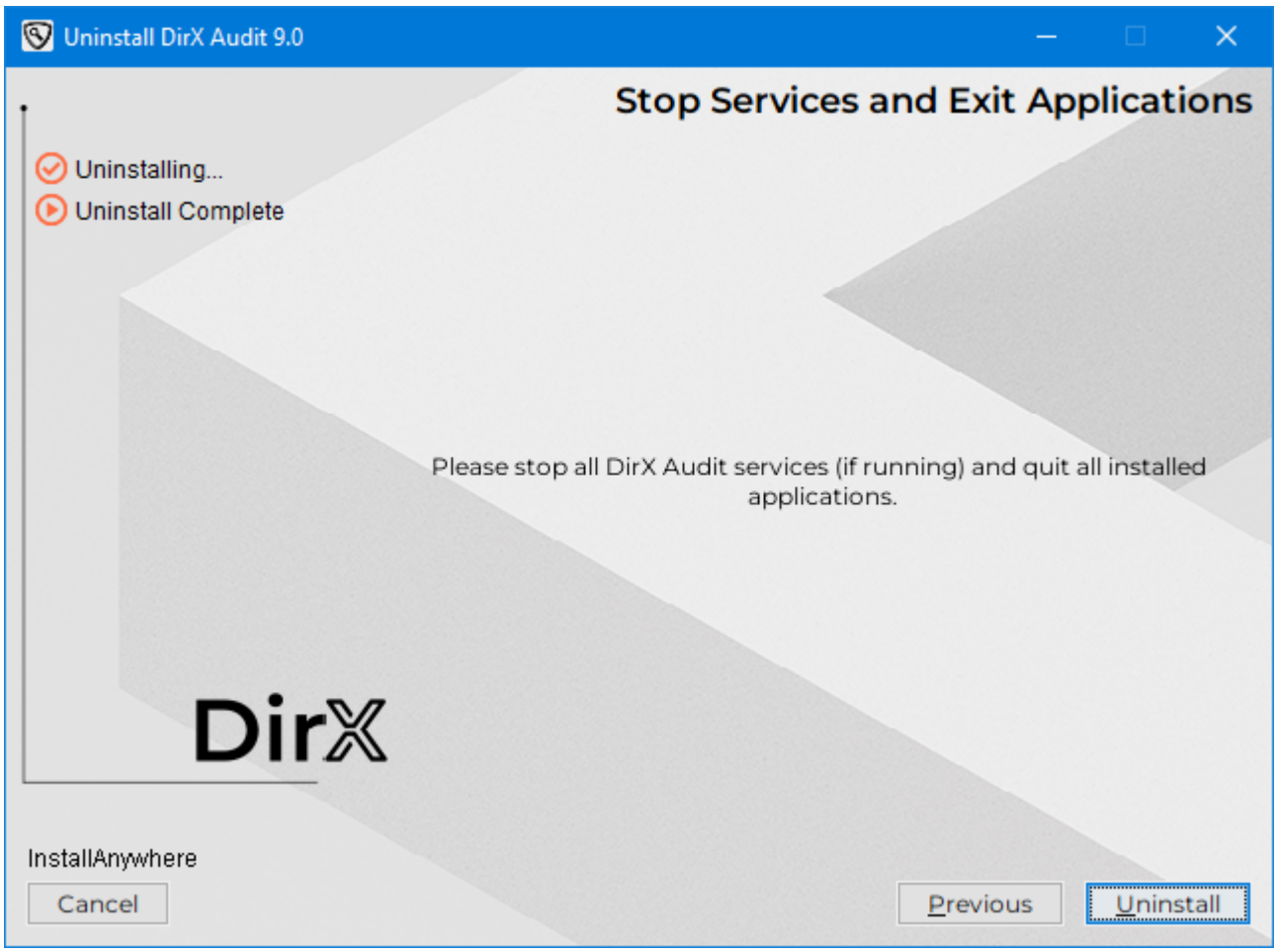


Setup displays an Uninstall DirX Audit dialog.

Click **Next** to go to the next dialog.

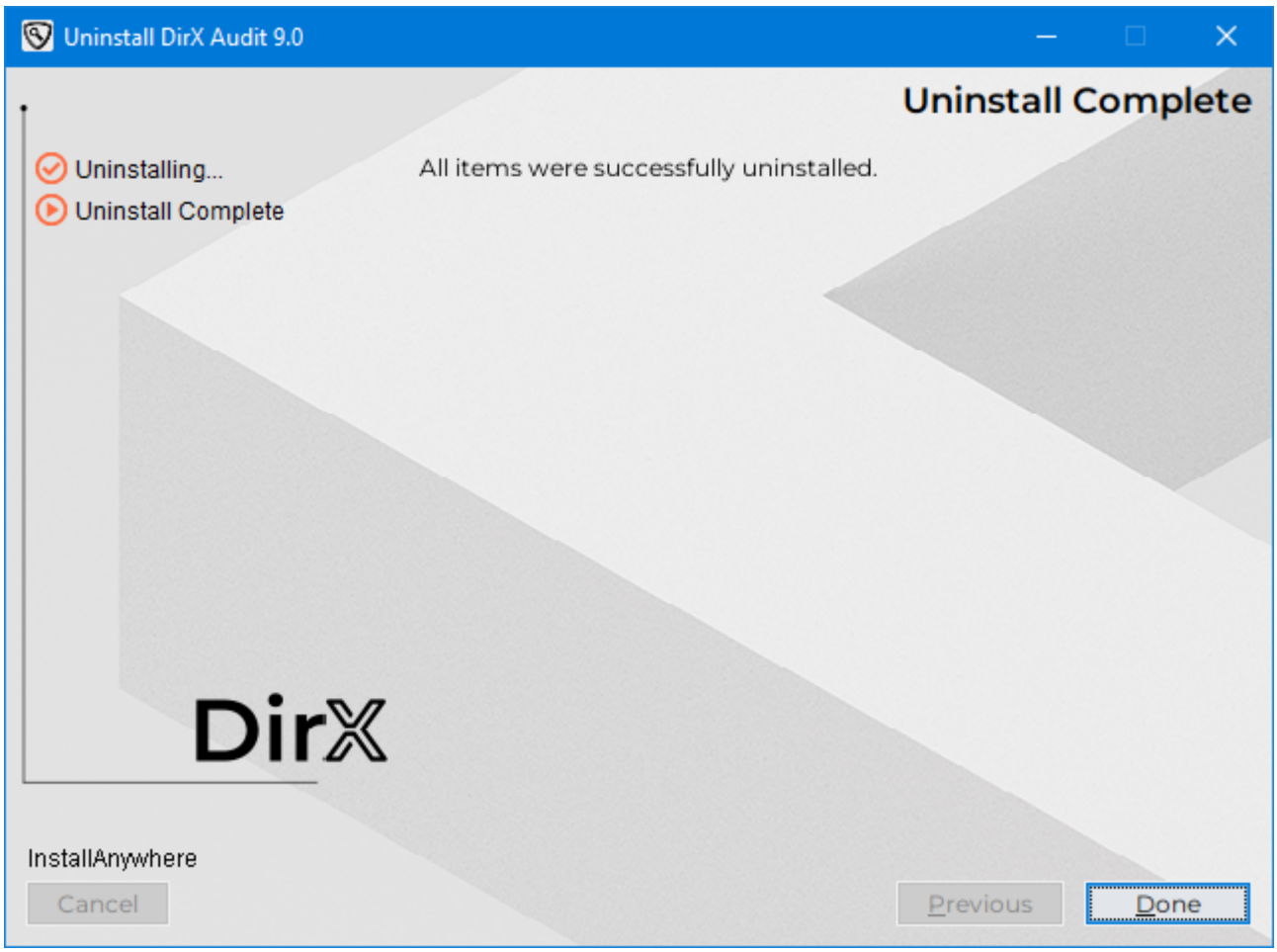
you can click **Cancel** at any time to leave the uninstallation program. You can click **Previous** at any time to return to a previous dialog.

3.2.2.2. Stop Services and Exit Applications



Setup displays a Stop Services and Exit Applications warning dialog.
Stop all DirX Audit services including the Apache Tomcat service used to start the DirX Audit Managers and quit all installed applications. Click **Uninstall** to start uninstalling DirX Audit.

3.2.2.3. Uninstall Complete



Setup displays the Uninstall Complete dialog.
If you are uninstalling DirX Audit and no errors have occurred, click **Done** to quit the installer.
If the installer requires a restart, make sure to restart the system so that you completely uninstall all components and services.

3.2.3. Uninstalling Apache Tomcat

To uninstall Apache Tomcat, use the tools provided with your operating system.

4. Configuring DirX Audit

This chapter describes how to configure DirX Audit with the Configuration Wizard.
You can use this wizard to:

- Perform a complete initial configuration, which includes the Core configuration and the Tenant configuration.
- Perform a reconfiguration at any time.
- Run the silent configuration.
- Configure LDAP over SSL (LDAPS).

The section "Post-Configuration Tasks" in this chapter provides information about additional post-configuration and preparatory tasks that are not handled by the configuration process. Perform these tasks after the configuration process is finished.

UNIX Instructions:
To run DirX Audit Configuration Wizard, a graphical interface or graphical display must be available either locally or remotely. The Configuration Wizard cannot run in a console mode.

Run the Configuration Wizard under the same user as the installation.

4.1. Starting the Configuration Wizard

This section provides information about starting the Configuration Wizard.

Make sure you have installed the Oracle Database JDBC driver to run Oracle Database as the DirX Audit database before you start the configuration process.

4.1.1. Initial Configuration

This section describes how to start the installation process on Windows and UNIX systems.

4.1.1.1. Windows Instructions

On Windows, the installation process starts the Configuration Wizard automatically. If the Configuration Wizard does not start automatically, start it manually with the command:
install_path`\configurator\bin\configuration.bat`

You must run the command as Administrator. The command starts the Core Configuration Wizard, after which the Tenant Configuration Wizard follows. You must configure at least one tenant.

4.1.1.2. UNIX Instructions

On UNIX, the GUI installation process starts the Configuration Wizard automatically. If the Configuration Wizard does not start automatically or you used the console mode, run the script:
install_path`/configurator/bin/configuration.sh`

Make sure you run the command with an account that has sufficient read and write rights for the DirX Audit installation folder.

4.1.2. Re-configuration

You can start the Configuration Wizard at any time to modify your configuration.

4.1.2.1. Windows Instructions

To run the Core configuration on Windows, select **All Programs** → **DirX Audit** → **Configurator – Core** from the Start menu or run the command:
install_path`\configurator\bin\configuration.bat`

To run the Tenant configuration on Windows, select **All Programs** → **DirX Audit** → **Configurator – Tenant** from the Start menu or run the command:
install_path`\configurator\bin\configuration.bat tenant`

You must run these commands as Administrator.

4.1.2.2. UNIX Instructions

To run the Core configuration on UNIX, run the command:
install_path`/configurator/bin/configuration.sh`

To run the Tenant configuration on UNIX, run the command:
install_path`/configurator/bin/configuration.sh tenant`

Make sure that you run these commands with an account that has sufficient read and write rights for the DirX Audit installation folder.

4.1.3. Un-configuration

Uninstalling DirX Audit automatically performs the un-configuration.

4.2. Using the Configuration Wizard for the Core Configuration

This section provides information about the tasks that the DirX Audit Configuration Wizard performs.

The Configuration Wizard displays the configuration tasks to be performed on the left-hand side of each dialog. The number of tasks displayed depends on the configuration options you select during the process in the wizard.

The Configuration Wizard highlights the current task in orange, completed tasks in blue and outstanding tasks in gray. It also identifies the current task in a heading on the right-side of the dialog. The right side of the dialog displays all information and fields for configuration input.
Mandatory input fields are displayed in red.

A label at the bottom indicates the source from which the settings on a page are loaded: Installation, Last saved, or Defaults. When specifying input values, you can use the following buttons (if enabled) to load persistent (saved) values:

- **Installation** – Loads the values that the current installation uses.
- **Last saved** – Loads the values saved in the last configuration. The Configuration Wizard saves the entered values when you click **Cancel** and confirm to save the modifications.
- **Defaults** – Loads the default values.

The bottom of the dialog provides the following navigation buttons:

- **Previous** – Steps backward; for example, to control or correct values that you've already specified. The Configuration Wizard checks and saves the specified values in this step. If you have set an incorrect mandatory value, you may need to change it before you can go back.
- **Next** – Steps forward. The Configuration Wizard saves the specified values. The Configuration Wizard checks and saves the specified values in this step. If you have set the wrong mandatory value, you may need to change it before you can go forward. When all parameter settings are complete, the Configuration Wizard starts the configuration process.
- **Finish** – Exits the configuration process.
- **Cancel** – Cancels the Configuration Wizard.
- **Help** – Provides additional help information if available. It opens the help section in a web browser, which you can choose from the list accessed by clicking the icon next to the help button.

After startup, the Configuration Wizard displays a welcome dialog.

DirX Audit provides two user interfaces: DirX Audit Manager (Angular / REST based) and DirX Audit Manager Classic (legacy application). When the phrase "Audit Managers" is used anywhere in the guide, it is meant that the configuration process is common to both

interfaces.

4.2.1. Welcome to the DirX Audit Configuration Wizard

This page welcomes you to the DirX Audit Configuration Wizard.

Click **Next** to specify the configuration options.

4.2.2. Configuration Options

In the Configuration Options dialog, you can select the following options:

- Common Audit Configuration:
  - **Common Audit Configuration** – Configure common settings for Audit Managers and Audit Server.
- Audit Message Broker:
  - **Audit Message Broker Configuration** – Configure the JMS message broker (Apache ActiveMQ).
- Common Audit Managers Configuration:
  - **Audit Managers Container Configuration** – Configure the application container (Apache Tomcat) for running the DirX Audit Managers application.
- Audit Manager Classic:
  - **Audit Manager Classic Application Configuration** – Configure the DirX Audit Manager Classic application.
  - **Audit Manager Classic Authentication Configuration** – Configure the SSO settings.
- Audit Server:
  - **Scheduled Jobs Configuration** – Configure the basic options for scheduling the DirX Audit Server jobs.

Check the components you want to configure and then click **Next**. The Configuration Wizard calculates all of the necessary tasks given your selections and then displays them on the left-hand side of the next dialog.

When you perform the initial configuration, the Configuration Wizard requires that you configure all components.

Related Topics: “Starting the Configuration Wizard”

4.2.3. Common Configuration

In the Common Configuration dialog, specify the components you want to configure:

- **Persistence configuration** – Configure general persistence settings.
- **SMTP configuration** – Configure emailing services.

This section allows you to configure common components for all tenants (organizations). Later, you can set up the specific tenant components like databases, authorization, and the server job configuration.

When you perform the initial configuration, the Configuration Wizard requires that you configure all components.

Related Topics: "Starting the Configuration Wizard"

4.2.4. Common Persistence Configuration

In the Common Persistence Configuration dialog, specify the following parameters:

- **Folder for persistent files** – The full pathname to the folder for storing reports generated by users and user configuration.

Related Topics: "Starting the Configuration Wizard"

4.2.5. Common SMTP Configuration

In the Common SMTP Configuration dialog, specify the email settings:

- **Send emails** – Whether (checked) or not (unchecked) the email notifications and scheduled reports are provided.
  - **SMTP Server host** – The host name of the SMTP server.
  - **Secure connection** – The cryptographic protocol for the connection. Use the drop-down list to make your selection.
  - **SMTP Server port** – The port of the SMTP server.
  - **Default from email address** – The email address from which the email will be sent by default.
- **Authenticate** – Whether (checked) or not (unchecked) the email sender is authenticated.
  - **Authentication type** – The authentication type, if **Authenticate** is checked. Use the drop-down list to make your selection.
  - **Authentication username** – The user name.
  - **Authentication user password** – The user's password. The password is saved in the configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password.
- **Test connection** – Click to test the SMTP server connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on.

Related Topics: “Starting the Configuration Wizard”

4.2.6. Message Broker

In the Message Broker dialog, specify the components you want to configure:

- **Message Broker connectivity configuration** – Configure the message broker connectivity.
- **Message Broker system service configuration** – Configure the message broker system service.
- **Message Broker administrative credentials configuration** – Configure the message broker internal technical accounts.

Note that when you perform the initial configuration, the Configuration Wizard requires that you configure all components.

Related Topics: “Starting the Configuration Wizard”

4.2.7. Message Broker Connectivity

Use this dialog to specify the message broker connectors. We recommend communicating over secure channels between components and services. The message broker console is provided only over a secure channel and you must supply cryptographic material stored in Java keystores and truststores for this communication. The recommended location for all keystores and truststores is the folder *install_path***/conf/crypto/stores**.

In the Message Broker Connectivity dialog, specify the following parameters:

- **Enable SSL** – Whether (checked) or not (unchecked) to enable using secure (SSL) connection globally. Includes secure connection to ActiveMQ console and JMS message broker. Communication over secure channels between components and services is recommended.
- **Enable OpenWire connector** – The default transport for receiving audit messages over JMS. This field must be enabled if you don’t use SSL so that the OpenWire connector is used for local client connection.
- **OpenWire connector URI** – The JMS message broker listen URI, in the format **tcp://***host* **:***port*, where *host* specifies the server name or IP address of the interfaces to which the server is to bind (listen on) and *port* specifies the server port number. The default host value is **0.0.0.0**, which configures the server to listen on all available network interfaces. Be careful when setting specific IP addresses or host names; for example, remember that the locally-installed Audit Server JMS collector will most likely use the loop-back interface. The default port value is **30666**.
- **Enable SSL connector** – Whether (checked) or not (unchecked) to enable the connector using secured (SSL) connection.

- **SSL connector URI** – The JMS message broker listen URI, in the format **ssl://***host***:***port*, where *host* specifies the server name and *port* specifies the server port number. See the OpenWire connector URI format description for information about specifying the host value. The default port value is **30667**.
- **Local client (connector) URI** – The local client connection URI, in the format **tcp://***localhost***:***port*, where *localhost* specifies your local server name and *port* specifies the server port number. The default port value depends on previous selection (**30666** or **30667** for SSL). If the OpenWire connector is enabled, the default port for loop-back interface is used. The Configuration Wizard uses this URI as default value for the first Server JMS Collector configuration in the Tenant configuration.
- **Remote client (connector) URI** – The remote client connection URI, in the format **tcp://***host***:***port* or **ssl://***host***:***port*, where *host* specifies your server name and *port* specifies the server port number. The default port value depends on previous selection (**30666** or **30667** for SSL).
- **Keystore location** – The path to the keystore which will be used for secure connection. Click the Open file browser button at the end of the line to find your location. If you followed our example for keystore preparation and you saved the created keystore to the default location, the keystore location should be: *install_path***/conf/crypto/stores/broker-ks.jks**.
  For more information, see the section “Preparing Truststores and Keystores for SSL Configuration” → “Preparing the Message Broker” in this guide.
- **Keystore password** – The valid password for your keystore. Click the button at the end of the password field to view the password.
- **Truststore location** – The path to the truststore which will be used for secure connection. Click the Open file browser button at the end of the line to find your location. If you followed our example for truststore preparation and you saved created truststore to the default location, the location should be: *install_path***/conf/crypto/stores/broker-ts.jks**.
  For more information, see the section “Preparing Truststores and Keystores for SSL Configuration” → “Preparing the Message Broker” in this guide.
  If it is missing, the standard Java KeyStore (JKS) is assumed.
- **Truststore password** – The valid password for your truststore. Click the button at the end of the password field to view the password.
- **Message repository** – the folder where the queue data and messages will be stored.

Once you click **Next**, the Configuration Wizard checks the Message Broker connectivity. If invalid values are provided or some configuration is missing, an error message is displayed and you cannot continue with the configuration process until you supply valid values. If you do not use the recommended secure connections, a warning message is displayed, but you can continue with the configuration.

Related Topics:
“Starting the Configuration Wizard”
“Preparing Truststores and Keystores for SSL Configuration”

4.2.8. Message Broker System Service

In the Message Broker System Service dialog, you set the system service configuration.

The dialog window may be different for Windows and for UNIX.

Specify the following parameters:

- **(Re-)Install system service support** – Whether (checked) or not (unchecked) to install or re-install support for running as a system service. This parameter is set (checked) and read-only on initial configuration.
- **Run as a system service** – Whether (checked) or not (unchecked) to run the message broker as a system service.

  Windows Instructions

  - **Service startup type** – The service start type. Use the drop-down list to make your selection (**AUTO** / **AUTO_DELAYED** / **DISABLED** / **MANUAL**).
  - **Log on as** – The account under which the DirX Audit Message Broker should run. You can select **System Account** or **Other Account**. If you select **Other Account**, you must specify **Domain**, **User** and **Password** for this account.

  UNIX Instructions

  - **Run system service as user:** – The user under which the DirX Audit Message Broker should run.
  - **Run system service under group:** – The group under which the DirX Audit Message Broker should run.
- **Start system service now** – Whether (checked) or not (unchecked) to start the message broker service after finishing the configuration.
- **System service name** – The service name.
- **System service display name** – The service display name.

Related Topics: “Starting the Configuration Wizard”

4.2.9. Message Broker Administration

In the Message Broker Administration dialog, you set the administration credentials for the ActiveMQ system user and you can enable or disable the monitoring with Java Management Extensions technology and the Web console:

- **System (system)** – The password for the internal ActiveMQ system account for administration.
- **Enable JMX** – Whether (checked) or not (unchecked) DirX Audit Message Broker monitoring with Java Management Extensions technology is enabled. It is enabled by default and has read-only access.
  - **Username** – The user name to use for connecting to the JMX agent.
  - **Password** – The password to use for connecting to the JMX agent.
- **Enable Web Console** – Whether (checked) or not (unchecked) Message Broker Web Console is enabled. It is enabled by default. JMX have to be enabled to enable Web Console.
  - **Admin (admin)** – The password for the administration account for WebConsole (the administrator can delete queues, for example).
  - **User (user)** – The password for the normal user account for WebConsole.

Click the button at the end of the password field to view the passwords. Passwords are saved in the configuration files and are encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host.

Related Topics: “Starting the Configuration Wizard”

4.2.10. Common Managers Container Configuration

In the Common Managers Container Configuration dialog, specify the full pathname of the installed container (Apache Tomcat) or click the **Open file browser** button to browse to the installed container. The specified directory must exist and contain a supported version of Apache Tomcat.

Related Topics: “Starting the Configuration Wizard”

4.2.11. Audit Manager Classic Application

The Audit Manager Classic Application dialog displays the application configuration. You can specify the following parameters:

- **(Re-)deploy Audit Manager Classic application** – Whether (checked) or not (unchecked) to re-deploy the Manager Classic application with your changes.
- **Choose default tab** – The default tab which is displayed in DirX Audit Manager Classic

after user login.

Related Topics: “Starting the Configuration Wizard”

4.2.12. Audit Manager Classic Authentication

In the Audit Manager Classic Authentication dialog, you can specify parameters needed for your preferred authentication method common for all tenants for the DirX Audit Manager Classic. Later in the Tenant configuration you can specify tenant specific authentication options.

Header SSO
If you have set up single sign-on (SSO), you can use the HTTP header injection to integrate DirX Audit Manager Classic with an external authentication system such as DirX Access. The external system can pass the user name and the tenant name of an authenticated user to the DirX Audit Manager Classic application in the DXT_USER and DXT_TENANT HTTP request header variables. If the DirX Audit Manager Classic with the enabled SSO setting detects a valid user name in the HTTP request (by comparing it with an LDAP source), it bypasses the LDAP user name and password authentication.

For this authentication method, specify the following parameters:

- **Enable SSO** – Whether (checked) or not (unchecked) to use SSO with header injection authentication.
- **User header** – The name of the HTTP request header that conveys the user name.
- **Tenant header** – The name of the HTTP request header that conveys the tenant name.

If you enable SSO with the header injection authentication, this method has the highest priority and is used even if you set up other authentication options in the tenant configuration.

Windows user name and password
If you have set up an Active Directory domain controller, you can use the Windows authentication method for the DirX Audit Manager Classic login.

For this authentication method, specify the following parameters:

- **Kerberos file** – The path to the Kerberos configuration file which contains the settings for Kerberos. For more details, see the chapter “Windows Authentication Using Kerberos Login Module” in the *DirX Audit Administration Guide*.

Related Topics: “Starting the Configuration Wizard”

4.2.13. Server Scheduled Jobs

In the Server Scheduled Jobs dialog, specify the scheduled jobs time range for the server application. Later in the Tenant configuration you can specify tenant specific server options.

Note: The dialog window may be different for Windows and for UNIX.

- **Time range for running scheduled jobs** – The time range when you want to run scheduled jobs. The default values are at night 9 p.m. – 5 a.m.
- **Exclude range** – When checked, the time range when scheduled jobs should not be run; for example, between 2 a.m. and 3 a.m. because time is shifting or your system backup is in progress.

Related Topics: "Starting the Configuration Wizard"

4.2.14. Pre-Configuration Summary

The Configuration Wizard displays the Core configuration selections you have made and asks you to review them.

- Click **Previous** to change any settings you have made.
- Click **Next** to start the Core configuration process.

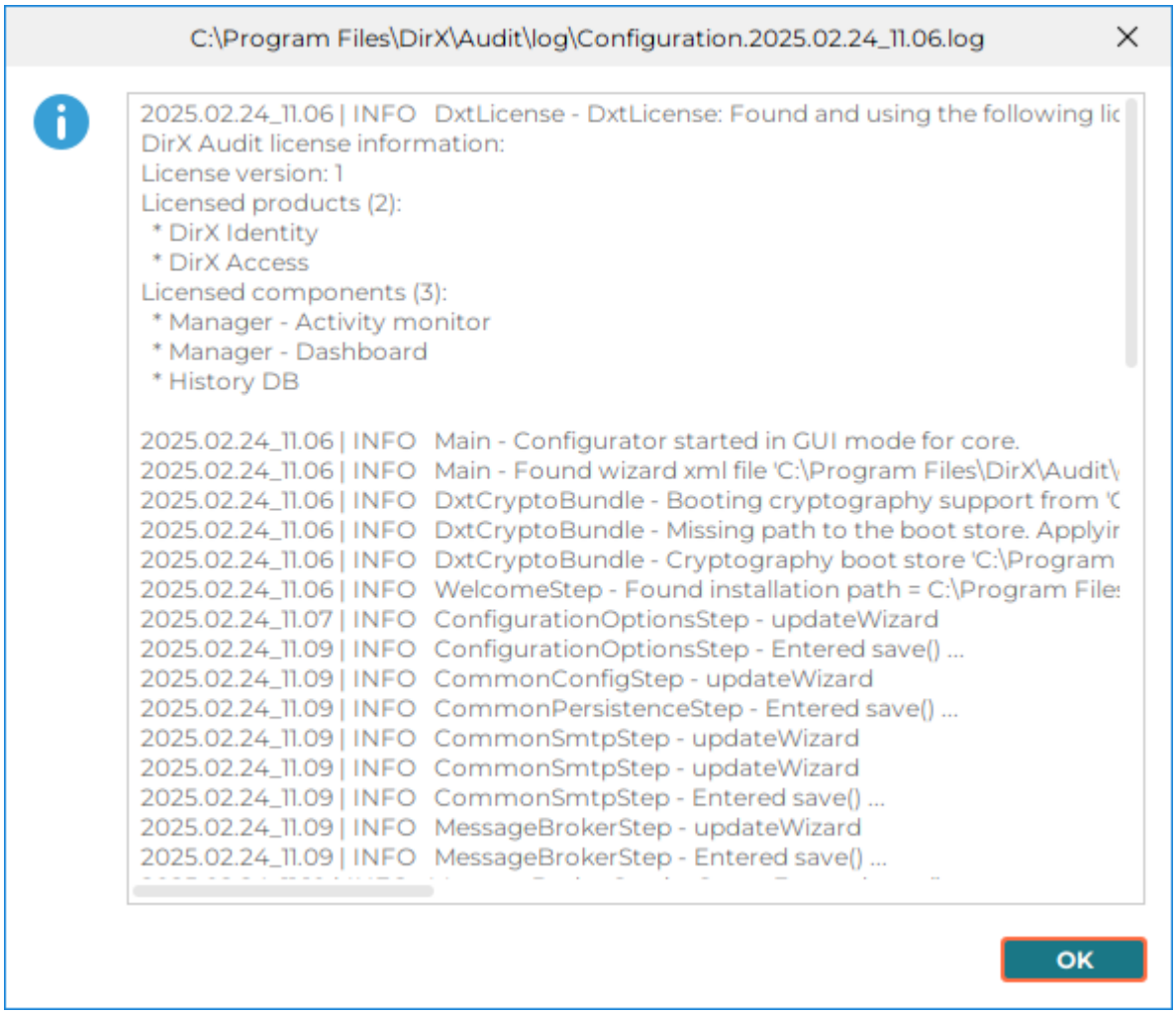
Related Topics: "Starting the Configuration Wizard"

4.2.15. Configuration in Progress

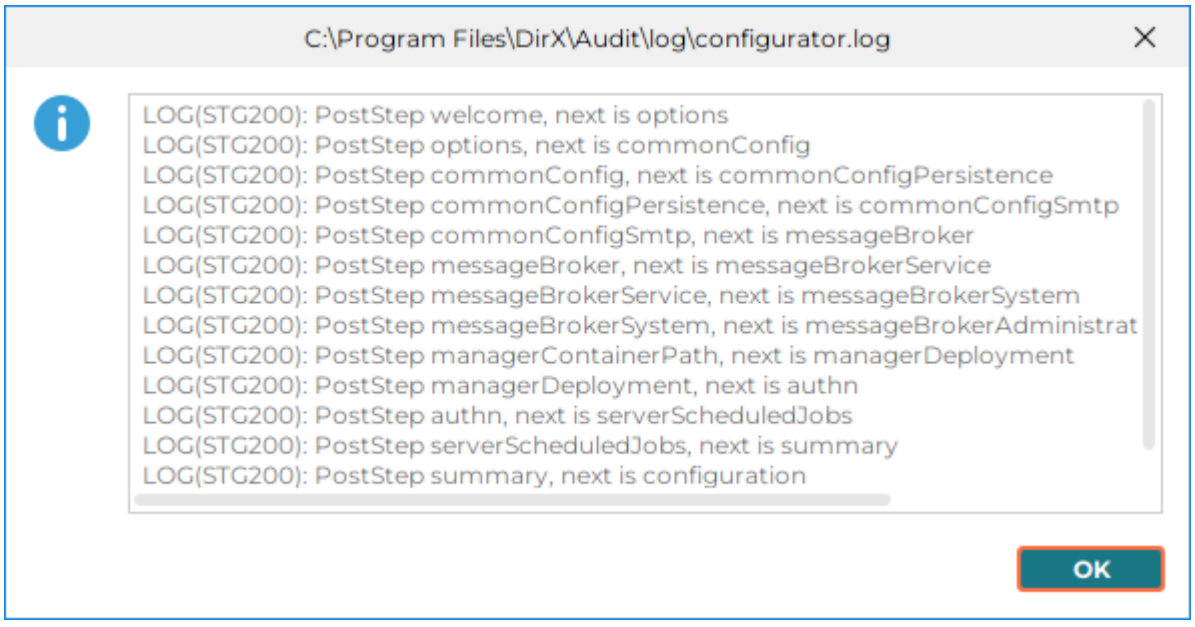
While configuring the DirX Audit core is in progress, the Configuration Wizard displays the current task in orange, successfully performed tasks in green and failed tasks in red. It displays the detailed action of the current task in the **Action detail** field.

When the Core configuration process completes, click:

- **Display current configuration log** – To display information on the DirX Audit configuration you just performed, including thrown exceptions.



- **Display configurator log** – To display information on the application status of the Configuration Wizard.



- **Next** – To start the Tenant configuration.

Related Topics: “Starting the Configuration Wizard”

4.2.16. Next Actions Options

In the Next Actions Options dialog allows you to start the Tenant configuration and specify how many tenants you want to configure. In the dialog, you can specify:

- **Run Tenant Configuration** – Whether (checked) or not (unchecked) to start the Tenant Configuration. At least one tenant must be configured if you configure a new installation.
- **Expected number of tenants** – The number of tenants you want to configure. At least one tenant must be configured.

If you select to configure multiple tenants, the Tenant configuration dialogs are started as many times as the number of tenants you enter.

- Click **Finish** to finish the Core configuration process and to start the Tenant configuration process.

Related Topics: "Starting the Configuration Wizard"

4.3. Using the Configuration Wizard for the Tenant Configuration

This section provides information about the Tenant configuration. It is started automatically when you click **Finish** in the **Next Actions Options** dialog in the Core configuration.

You can start the Configuration Wizard for the Tenant configuration at any time to modify your existing tenant configuration or add a new tenant. For more details on how to start the Tenant configuration, see the section "Re-configuration" in this guide.

4.3.1. Tenant Options

In the Tenant Options dialog, select what you want to configure:

- **Create New Tenant** – To create a new tenant.
- **Modify Existing Tenant** – To configure settings of an existing tenant.
- **Remove Existing Tenant** – To remove a tenant.

When you select what you want to configure, the Configuration Wizard displays the configuration tasks to be performed on the left-hand side of the dialog and you can click **Next** to continue.

4.3.1.1. Create New Tenant

The Create New Tenant dialog is displayed when you select **Create New Tenant** in the Tenant Options dialog.

In the Create New Tenant dialog, specify the tenant name. The tenant name must be unique and it is used as default for the server service display name and description and also on the login page for DirX Audit Manager Classic if multi-tenancy is configured. The Tenant ID is generated automatically and it is used for internal server folders, server service name, and tenant identification; for example, in the Message Broker configuration and in the DirX Audit Managers URL.

If you already have another tenant configured, the following check box is displayed:

- **Copy configuration from** – Check to copy the tenant configuration from an existing tenant to your current tenant configuration. Use the drop-down list to make your tenant selection.

Click **Next** to continue with the Tenant configuration. The next step is the Configuration Options dialog.

4.3.1.2. Modify Existing Tenant

The Modify Existing Tenant dialog is displayed when you select **Modify Existing Tenant** in the Tenant Options dialog.

In the Modify Existing Tenant dialog, specify the tenant you want to configure:

- **Tenant to modify** – Select the tenant you want to modify from the drop-down list.
- **Tenant name** – You can modify the tenant name. The modified name will be used, for example, for the server service description. If you want to modify an existing server service display name, you must go through the Application Container Configuration in the Tenant configuration.
- **Tenant ID** – The Tenant ID is generated automatically and cannot be edited.
- **Copy configuration from** – Check to copy the tenant configuration from an existing tenant to your current tenant configuration. Use the drop-down list to make your tenant selection.

Click **Next** to continue with the Tenant configuration. The next step is the Configuration Options dialog.

4.3.1.3. Remove Existing Tenant

The Remove Existing Tenant dialog is displayed when you select **Remove Existing Tenant** in the Tenant Options dialog.

In the Remove Existing Tenant dialog, specify the tenant you want to remove:

- **Tenant to remove** – Select the tenant you want to remove from the drop-down list.

Click **Next** to continue with the Tenant configuration. The next step is the Pre-configuration Summary dialog.

Related Topics: "Using the Configuration Wizard for the Tenant Configuration"

4.3.2. Configuration Options

In the Configuration Options dialog, specify the components you want to configure:

- **Database Configuration**
  - **Data DB Configuration** – Configure the required database connectivity parameters for storing audit data.
  - **Configuration DB Configuration** – Configure the required database connectivity parameters for storing configuration data.
  - **History DB Configuration** – Configure the required database connectivity parameters for storing history data.
- **Authentication Configuration** – Configure the required authentication parameters.
- **Audit Manager Application Configuration** – Configure deployment of Audit Manager Application .
- **Authorization Configuration** – Configure fine-grained access control method to be applied when accessing audit data.
- **Audit Server Application Configuration**
  - **Application Container Configuration** – Configure the application container for running the DirX Audit Server application.
  - **REST Service Configuration** – Configure REST Service to access resources audit data in databases.
  - **REST Service Authentication Configuration** – Configure authentication for REST Service to access audit data in databases.
  - **Collectors Configuration** – Configure the DirX Audit Server collectors.
  - **Scheduled Jobs Configuration** – Configure the options for scheduling the DirX Audit Server jobs.
  - **Scheduled Purge Jobs Configuration** – Configure the DirX Audit data for which the DirX Audit Server purge job(s) should be configured.
  - **Scheduled History Synchronization Jobs Configuration** – Configure the options for history entries synchronization.

When you set up a new tenant, the Configuration Wizard requires that you configure all components.

Related Topics:
"Starting the Configuration Wizard"
"Using the Configuration Wizard for the Tenant Configuration"

4.3.3. Data DB Configuration

In the Data DB Configuration dialog, specify the required database connectivity parameters.
This database is used to store audit messages.

- **DB Server type** – The supported relational database management systems (RDBMS).
- **Authentication method** – The supported authentication methods for the selected database server type. The available options are:
  - **Database Authentication with username and password** – this is the only possible method for the Oracle **DB Server type** values.
  - **Kerberos Authentication with username and password** – this option is available only for the Microsoft SQL Server **DB Server type** values.
  - **Windows Authentication** – this option is available only for the Microsoft SQL Server **DB Server type** values.
- **Driver class name** – The full Java class name of the JDBC driver for the selected database. You can use the pre-defined value or replace it with the correct one.
- **Connection URL** – The URL used for connecting to the Data DB. You can use the default pre-defined URL syntax and replace the *hostname* (the host name of the database server), *port* (the port number for the JDBC connection) and *servicename* or *dbname* with the current values in your environment.

  Default syntax for SQL Server:
  jdbc:sqlserver://*hostname***:***port***;databaseName=***dbname***;encrypt=false**

  Default syntaxes for Oracle Database:
  jdbc:oracle:thin:@//*hostname***:***port***:***servicename* or
  jdbc:oracle:thin:@//*hostname***:***port***:***OracleSID*

  If you have problem with the validation of the server certificate, you can configure the driver to ignore the certificate validity and trust any provided server certificate by using the following URL. You should not use this option for productive environments (as it's unsafe).

  For SQL Server:
  jdbc:sqlserver://*hostname***:***port***;databaseName=***dbname***;encrypt=true;trustServerCertificate=true**

  If you wish to connect with encryption, you must have the DBMS certificate available in a truststore and use the following URL.

  For SQL Server:
  jdbc:sqlserver://*hostname***:***port***;databaseName=***dbname***;**
  encrypt=true;trustServerCertificate=false

  or
  jdbc:sqlserver://*hostname***:***port***;databaseName=***dbname***;**

encrypt=true;trustServerCertificate=false;
trustStore=*storename***;trustStorePassword=***storepassword***;**
hostNameInCertificate=*certificatehostname*

Note that the Connection URL is stored unencrypted in the **configuration.cfg** file. You can expose the truststore password when specifying it.

For Oracle Database:
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(PORT=*port***)**
(HOST=*hostname***))(CONNECT_DATA=(SERVICE_NAME=***servicename***))(SECURITY=(ssl_s**
erver_cert_dn="*servercertificatedn***")))**

Note that Oracle Database uses a different port for unsecured (default **1521**) and secured (default **2484**) connections.

Make sure that you enter different Data DBs for different tenants.

- **Username** – The RDBMS technical account name for connection when **Database Authentication with username and password** is selected in **Authentication method**. The Kerberos principal is in the form *username***@REALM**; for example, **admin@MY-COMPANY.COM**, when **Kerberos Authentication with username and password** is selected in **Authentication method**. The Kerberos realm name is always case-sensitive and by convention (best practice) uppercase. This parameter is not available when the **Windows Authentication** is selected in **Authentication method**.
- **Password** – The password that belongs to **Username**. The password is saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password. This parameter is not available when the **Windows Authentication** is selected in **Authentication method**.
- **Save original audit messages** – Whether (checked) or not (unchecked) the original audit message should be saved in the database. Possible values are true and false. If set to true, the original message is saved.
- **Use full-text search** – Whether (checked) or not (unchecked) to use full-text for searching in selected fields (for example, Audit Event – Detail). Using full-text search is usually faster on bigger data. Important note: The full-text catalogs / indexes must be created in the selected database.
- **Test connection** – Click to test the database connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on. When **Windows Authentication** is selected in **Authentication method**, be sure that you use the same account to run the Configuration Wizard as is used to run DirX Audit Server and Apache Tomcat system services or the connection test can be misleading.
- **Validate DB** – Click to validate the database schema. This action validates the existing schema, or if the database schema does not exist, the validation action creates it. A prerequisite is that the technical account used for the database connectivity has sufficient privileges for creating database objects like tables, views, materialized / indexed views, indexes and triggers. If your database schema is not valid, contact your

support organization.

Once you click **Next**, the Configuration Wizard checks the Data DB connection. If invalid values are provided – for example, for the JDBC driver – an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on. The Configuration Wizard checks to make sure your Data DB is not in use by another tenant. If it is, you cannot continue with the configuration process until you supply valid values.

Related Topics:
"Starting the Configuration Wizard"
"Using the Configuration Wizard for the Tenant Configuration"

4.3.4. Config DB Configuration

In the Config DB Configuration dialog, specify the required database connectivity parameters. This database is used to store configuration data.

- **The same as data DB** – Whether (checked) or not (unchecked) to use the same settings here as you used for the database containing audit messages.
- **DB Server type** – The supported relational database management systems.
- **Authentication method** – The supported authentication methods for the selected database server type. The available options are:
  - **Database Authentication with username and password** – this is the only possible method for the Oracle **DB Server type** values.
  - **Kerberos Authentication with username and password** – this option is available only for the Microsoft SQL Server **DB Server type** values.
  - **Windows Authentication** – this option is available only for the Microsoft SQL Server **DB Server type** values.
- **Driver class name** – The full Java class name of the JDBC driver for the selected database. You can use the pre-defined value or replace it with the correct one.
- **Connection URL** – The URL used for connecting to the Config DB. You can use the default pre-defined URL syntax and replace the *hostname* (the host name of the database server), *port* (the port number for the JDBC connection) and *servicename* or *dbname* with the current values in your environment.

  Default syntax for SQL Server:
  `jdbc:sqlserver://`*`hostname`*`:`*`port`*`;databaseName=`*`dbname`*`;encrypt=false`**

  Default syntaxes for Oracle Database:
  `jdbc:oracle:thin:@//`*`hostname`*`:`*`port`*`:`*`servicename`* or
  `jdbc:oracle:thin:@//`*`hostname`*`:`*`port`*`:`*`OracleSID`*

  If you have problem with the validation of the server certificate, you can configure the driver to ignore the certificate validity and trust any provided server certificate by using the following URL. You should not use this option for productive environments (as it's unsafe).

For SQL Server:
jdbc:sqlserver://*hostname*:*port*;**databaseName=***dbname*;**encrypt=true;trustServerCertificate=true**

If you wish to connect with encryption, you must have the DBMS certificate available in a truststore and use the following URL.

For SQL Server:
jdbc:sqlserver://*hostname*:*port*;**databaseName=***dbname*;
encrypt=true;trustServerCertificate=false;
trustStore=*storename*;**trustStorePassword=***storepassword*;
hostNameInCertificate=*certificatehostname*

For Oracle Database:
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(PORT=*port*)(**HOST=***hostname*))(**CONNECT_DATA=(SERVICE_NAME=***servicename*))(**SECURITY=(ssl_server_cert_dn="***servercertificatedn*"))**

Note that Oracle Database uses a different port for unsecured (default **1521**) and secured (default **2484**) connections.

Make sure that you enter different Config DBs for different tenants.

- **Username** – The RDBMS technical account name for connection when **Database Authentication with username and password** is selected in **Authentication method**. The Kerberos principal is in the form *username***@REALM**; for example, **admin@MY-COMPANY.COM**, when **Kerberos Authentication with username and password** is selected in **Authentication method**. The Kerberos realm name is always case-sensitive and by convention (best practice) uppercase. This parameter is not available when the **Windows Authentication** is selected in **Authentication method**.
- **Password** – The password that belongs to **Username**. The password is saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password. This parameter is not available when the **Windows Authentication** is selected in **Authentication method**.
- **Test connection** – Click to test the database connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on. When **Windows Authentication** is selected in **Authentication method**, be sure that you use the same account to run the Configuration Wizard as is used to run DirX Audit Server and Apache Tomcat system services or the connection test can be misleading.
- **Validate DB** – Click to validate the database schema. This action validates the existing schema, or if the database schema does not exist, the validation action creates it. A prerequisite is that the technical account used for the database connectivity has sufficient privileges for creating database objects like tables, views, materialized / indexed views, indexes and triggers. If your database schema is not valid, contact your support organization.

Once you click **Next**, the Configuration Wizard checks the Config DB connection. If invalid values are provided – for example, for the JDBC driver – an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later. The Configuration Wizard checks to make sure that your Config DB is not in use by another tenant. If it is, you cannot continue with the configuration process until you supply valid values.

Related Topics:
"Starting the Configuration Wizard"
"Using the Configuration Wizard for the Tenant Configuration"

4.3.5. History DB Configuration

In the History DB Configuration dialog, specify the required database connectivity parameters.
This database is used to store history entries.

- **The same as data DB** – Whether (checked) or not (unchecked) to use the same settings here as you used for the database containing audit messages.
- **The same as config DB** – Whether (checked) or not (unchecked) to use the same settings here as you used for the database containing configuration data.
- **DB Server type** – The supported relational database management systems (RDBMS).
- **Authentication method** – The supported authentication methods for the selected database server type. The available options are:
  - **Database Authentication with username and password** – this is the only possible method for the Oracle **DB Server type** values.
  - **Kerberos Authentication with username and password** – this option is available only for the Microsoft SQL Server **DB Server type** values.
  - **Windows Authentication** – this option is available only for the Microsoft SQL Server **DB Server type** values.
- **Driver class name** – The full Java class name of the JDBC driver for the selected database. You can use the pre-defined value or replace it with the correct one.
- **Connection URL** – The URL used for connecting to the History DB. You can use the default pre-defined URL syntax and replace the *hostname* (the host name of the database server), *port* (the port number for the JDBC connection) and *servicename* or *dbname* with the current values in your environment.

  Default syntax for SQL Server:
  jdbc:sqlserver://*hostname*:*port*,databaseName=*dbname*;encrypt=false*

  Default syntaxes for Oracle Database:
  jdbc:oracle:thin:@//*hostname*:*port*:*servicename* or
  jdbc:oracle:thin:@//*hostname*:*port*:*OracleSID*

  If you have problem with the validation of the server certificate, you can configure the

driver to ignore the certificate validity and trust any provided server certificate by using the following URL. You should not use this option for productive environments (as it's unsafe).

For SQL Server:

jdbc:sqlserver://*hostname*:*port*;**databaseName=***dbname*;**encrypt=true;trustServerCertificate=true**

If you wish to connect with encryption, you must have the DBMS certificate available in a truststore and use the following URL.

For SQL Server:
jdbc:sqlserver://*hostname*:*port*;**databaseName=***dbname*;
encrypt=true;trustServerCertificate=false;
trustStore=*storename*;**trustStorePassword=***storepassword*;
hostNameInCertificate=*certificatehostname*

For Oracle Database:
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(PORT=*port*)(**HOST=***hostname*))(**CONNECT_DATA=(SERVICE_NAME=***servicename*))(**SECURITY=(ssl_server_cert_dn="***servercertificatedn*"))**

Note that Oracle Database uses a different port for unsecured (default **1521**) and secured (default **2484**) connections.

Make sure that you enter different History DBs for different tenants.

- **Username** – The RDBMS technical account name for connection when **Database Authentication with username and password** is selected in **Authentication method**. The Kerberos principal is in the form *username***@REALM**; for example, **admin@MY-COMPANY.COM**, when **Kerberos Authentication with username and password** is selected in **Authentication method**. The Kerberos realm name is always case-sensitive and by convention (best practice) uppercase. This parameter is not available when the **Windows Authentication** is selected in **Authentication method**.
- **Password** – The password that belongs to **Username**. The password is saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password. This parameter is not available when the **Windows Authentication** is selected in **Authentication method**.
- **Test connection** – Click to test the database connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on. When **Windows Authentication** is selected in **Authentication method**, be sure that you use the same account to run the Configuration Wizard as is used to run DirX Audit Server and Apache Tomcat system services or the connection test can be misleading
- **Validate DB** – Click to validate the database schema. This action validates the existing schema, or if the database schema does not exist, the validation action creates it. A

prerequisite is that the technical account used for the database connectivity has sufficient privileges for creating database objects like tables, views, materialized / indexed views, indexes and triggers. If your database schema is not valid, contact your support organization.

Once you click **Next**, the Configuration Wizard checks the History DB connection. If invalid values are provided – for example, for the JDBC driver – an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later. The Configuration Wizard checks to make sure that your History DB is not in use by another tenant. If it is, you cannot continue with the configuration process until you supply valid values.

Related Topics:
"Starting the Configuration Wizard"
"Using the Configuration Wizard for the Tenant Configuration"

4.3.6. Authentication Configuration

In the Authentication Configuration dialog, specify the required authentication connectivity parameters. The settings are used both for authenticating users when accessing DirX Audit Manager Classic and when DirX Audit Server is creating scheduled reports on users' behalf.

In the Enabled authentication methods, you can specify which authentication methods you want to use:

- **Header SSO** – Whether (checked) or not (unchecked) to use SSO with header injection authentication. The tenant configuration reads the checkbox status from the values saved by the Core Configurator Authentication dialog.
- **Windows SSO** – Whether (checked) or not (unchecked) to use SSO authentication with SPNEGO mechanism using Kerberos authentication protocol.
- **Windows username and password** – Whether (checked) or not (unchecked) to use Windows authentication with Kerberos realm\username credentials controlled with an Active Directory domain controller for logging in to DirX Audit Manager Classic.
- **LDAP username and password** – mandatory/required LDAP authentication method used for the authentication when other methods are not configured.

The authentication methods are sorted by priority. That is that if you enable the SSO with header injection authentication, this method has the highest priority and is used even if you set up other authentication options.

In the event, that SSO authentication (header injection or Windows SSO) was not successful; the user is redirected to login page. After entering a user name and password, the application first tries the Windows authentication. If it was not successful, the LDAP authentication is used. The Windows user name and password authentication is used, only if it is enabled in the configuration.

Sample scenarios:

- **Header SSO**
  Prerequisites:
  In the **Enabled authentication methods**, **Header SSO** is checked.
  The user accessed the DirX Audit Manager Classic with the following link:
  `https://`*`hostname`***`:`***`port`***`/AuditManager/`** with HTTP request headers DXT_TENANT and DXT_USER. **Header SSO** is checked; the application is aware that the user is pre-authenticated and no additional authentication method is executed.

  If the authentication is not successful, the application continues with the Windows SSO (if checked) and the username and password authentication methods.
  If the user is authorized, the application is redirected to the protected area of the DirX Audit Manager Classic.
  If the user is not authorized, the application is redirected to the logout page.

- **Windows SSO**
  Prerequisites:
  The user is not authenticated with Header SSO and **Windows SSO** is checked in the **Enabled authentication methods**.
  The user accessed the DirX Audit Manager Classic with the following link:
  https://*hostname*:*port*/**AuditManager/?tenant=***tenantID*

  If **Header SSO** is checked in the **Enabled authentication methods** it is performed first. If the authentication is not successful, then the Windows SSO method is executed.
  The application verifies if the user is logged in the Active Directory domain.
  If the authentication is not successful, the application is redirected to the login page for user name and password authentication.
  If the user is authorized, the application is redirected to the protected area of the DirX Audit Manager Classic.
  If the user is not authorized, the application is redirected to the logout page.
- **Windows username and password**
  Prerequisites:
  The user is not authenticated with Header SSO or Windows SSO and **Windows username and password** is checked in the **Enabled authentication methods**.
  The user accessed the DirX Audit Manager Classic with the following link:
  https://*hostname*:*port*/**AuditManager/?tenant=***tenantID*

  Specify the user name in the following format: [*REALM*\]username
  Examples:
  `username` – no realm predefined
  `MY-COMPANY.COM\username` – with a realm

  The [*REALM*] part is optional. It should be used only if the DNS name is not configured correctly or if the user is registered in a realm different from the DNS name.
  The Windows username and password authentication is performed before the LDAP username and password authentication is performed. If the Windows username and password authentication is successful, the LDAP username and password authentication is skipped.
  If the user is authorized, the application is redirected to the protected area of the DirX Audit Manager Classic.
  If the user is not authorized, the application is redirected to the logout page.
- **LDAP username and password**
  Prerequisites:
  The user is not authenticated with one of the previous methods.
  The user accessed the DirX Audit Manager Classic with the following link:
  https://*hostname*:*port*/**AuditManager/?tenant=***tenantID*

  The user with the specified user name and password is searched in the configured LDAP directory service. If it is found and if a valid password is provided, the user is authenticated.
  If the user is authorized, the application is redirected to the protected area of the DirX Audit Manager Classic.
  If the user is not authorized, the application is redirected to the logout page.

For more information about authentication methods, see the section "Managing DirX Audit Manager Classic" in the *DirX Audit Administration Guide*.

In the **Windows SSO** section, specify the required parameters:

- **Keytab location** – Specifies the keytab file location for the application service generated by an Active Directory administrator. For more details, see the "Configuring SSO (Single Sign-on) Web Authentication Using SPNEGO / Kerberos" chapter in the *DirX Audit Administration Guide*.
- **Service principal name** – Specifies the service principal name, the unique application service name, configured in the Active Directory domain.

In the **LDAP username and password** section, specify the required LDAP authentication parameters.

- **LDAP server host** – The host name of the LDAP server.
- **Use SSL** – Whether (checked) or not (unchecked) the LDAP connection is an SSL connection. Using an SSL connection is the default setting because we recommend communicating over secure channels between components and services.
- **LDAP server port** – The port number for the LDAP connection.
- **Authentication type** – The authentication type. Please keep the predefined value **SIMPLE**.
- **Domain** – The DirX Identity domain. This value is used in the next LDAP authentication parameters and replaces the *${domain}* placeholder.
- **Search account user DN** – The Distinguished Name of the technical LDAP account for searching users and groups on authentication.
- **Search account password** – The password of the technical account. The password is saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password.
- **Search base for users** – The base for the LDAP search. Use this setting to limit the subtree where you search for the authenticating user.
- **Search filter for users** – The LDAP filter to use to limit the result where the authenticating user is searched. Use **%s** to represent a string containing the user target naming attribute, the equal sign and the user name provided by the authentication form or an HTTP request header variable for a single sign on; for example, **cn=Tinker Boris**.
- **User target** – The naming attribute of users. It is usually the **cn** attribute.
- **Search base for groups** – The base for the LDAP search. Use this setting to limit the subtree where you search for the groups of which the authenticating user can be a member.
- **Search filter for groups** – The LDAP filter to use to limit the result where the groups of which the authenticating user can be a member are searched. Use **%d** to represent a distinguished name (DN) of the authenticating user.

- **List of auditor groups** – The list of LDAP groups (DNs) to be mapped to the Auditor role. Separate each group DN with a semicolon (;).
- **List of restricted auditor groups** – The list of LDAP groups (DNs) to be mapped to the Restricted Auditor role. Separate each group DN with a semicolon (;).
- **List of audit administrators groups** – The list of LDAP groups (DNs) to be mapped to the Audit Administrator role. Separate each group DN with a semicolon (;).
- **User identification attribute** – The unique identifying attribute of users. Ensure that all entries in the authentication service have a non-empty value in this attribute and that these values are unique.
- **User email attribute** – The LDAP attribute holding the user's email address. The attribute value is used when the user configures scheduled reporting jobs.
- **Truststore location** – The path to the truststore used for establishing secure SSL/TLS connections to the LDAP directory server. For more information about the default locations and how to prepare your own truststore, see the section "Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration". If you used the described example, the expected truststore file is named *install_path***/conf/crypto/stores/ldap-ts.jks**. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location field can be left empty. If it is missing, the standard Java KeyStore (JKS) is assumed.
- **Truststore password** – The password to access the truststore. Click the button at the end of the password field to view the password. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location and the password fields can be left empty.
- **Test connection** – Click to test the LDAP connection.

Once you click **Next**, the Configuration Wizard checks the LDAP connection. If invalid values are provided – for example, server host or truststore – an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later. The Configuration Wizard also checks if your LDAP connection is in use by another tenant. If it is, a warning message is displayed, but you can continue with the configuration process if desired.

Related Topics:
"Starting the Configuration Wizard"
"Using the Configuration Wizard for the Tenant Configuration"
"Preparing Truststores and Keystores for SSL Configuration"

4.3.7. Audit Manager Application

The Audit Manager Application dialog displays the application configuration. You can specify the following parameters:

- **(Re-)deploy Audit Manager application** – Whether (checked) or not (unchecked) to re-deploy the Audit Manager application with your changes.

Related Topics:
“Starting the Configuration Wizard”
“Using the Configuration Wizard for the Tenant Configuration”

4.3.8. Authorization Configuration

In the Authorization Configuration dialog, specify the authorization method you want to configure:

In **Authorization method**, select:

Empty PEP – No data access authorization is defined and no additional configuration is required.
The response is always **'permit'**. Response caching is disabled.

DirX Access PEP – The data access authorization based on policies defined and stored at DirX Access. Provide information to connect to DirX Access Server. To set up the secure connection to DirX Access Server, you need to use the relevant DirX Access Server certificate and the relevant DirX Access Server CA certificate (Certificate Authority that signed the server certificate). For more information, see the section “Preparing the DirX Access Server Secure Connection” in the chapter “Installation Configurations” of this guide.

- **Use response cache** – Whether (checked) or not (unchecked) to use the response cache. If checked, a valid cached response is used instead of accessing the DirX Access PDP repeatedly.
  To disable caching, uncheck the option.
  - **Response cache timeout** – The value in minutes to keep authorization PEP responses valid. Used only when the response cache is enabled.
- **PEP Id** – The identification of the PEP when communicating with the DirX Access Server.

- **Authorization service URL** – The URL used for connecting to the DirX Access Server. You can use the default URL syntax and replace the hostname (the host name of the DirX Access Server) and port (the port number for connecting to DirX Access Server).
  For DirX Access 8.9:
  `https://`*`host`***`:`***`port`***`/clientservice/sessioning/AuthorizationDecisionXacmlAction`**
  For DirX Access 8.10:
  `https://`*`host`***`:`***`port`***`/odata4/sessioning/1_0_0/AuthorizationDecisionXacml`**
  For DirX Access 9.0 and newer:
  `https://`*`host`***`:`***`port`***`/odata4/legacy/sessioning/1_0_0/AuthorizationDecisionXacml`**
- **Username** – The user name for the authorization service.
- **Password** – The password for the authorization service user. The password is saved in the configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password.
- **Truststore location** – The path to the truststore used for establishing a secure SSL/TLS connection to the DirX Access Server. For more information, see the section "Preparing Truststores and Keystores for SSL Configuration" → "Preparing the DirX Access Server Secure Connection". If you follow the instruction described there, the expected truststore file is *install_path***/conf/crypto/stores/ws-sec-comm.client.jks**. If it is missing, the standard Java KeyStore (JKS) is assumed.
- **Truststore password** – The password to access the truststore. Click the button at the end of the password field to view the password.

Related Topics:
"Starting the Configuration Wizard"
"Using the Configuration Wizard for the Tenant Configuration"
"Preparing Truststores and Keystores for SSL Configuration"

4.3.9. Application Container Configuration

In the Application Container Configuration dialog, configure the tenant-specific server container. You can specify the following parameters.

Note: The dialog window may be different for Windows and for UNIX.

- **(Re-)Install system service support** – Whether (checked) or not (unchecked) to install or re-install support for running as a system service. This parameter is set (checked) and read-only on initial configuration.
- **Run as a system service** – Whether (checked) or not (unchecked) to run the server container as a system service.

  Windows Instructions

- **Service startup type** – The service start type. Use the drop-down list to make your selection (**AUTO** / **AUTO_DELAYED** / **DISABLED** / **MANUAL**).
- **Log on as** – The account under which the DirX Audit Server should run. You can select **System Account** or **Other Account**. If you select **Other Account**, you must specify **Domain**, **User** and **Password** for this account.

UNIX Instructions

- **Run system service as user:** – The user under which the DirX Audit Server should run.
- **Run system service under group:** – The group under which the DirX Audit Server should run.

- **Start system service now** – Whether (checked) or not (unchecked) to start the server container service after finishing the configuration.
- **System service name** – The service name that contains the tenant's unique identification.
- **System service display name** – The service display name that contains the tenant's unique name.
- **Enable JMX** – Whether (checked) or not (unchecked) DirX Audit Server monitoring with Java Management Extensions technology is enabled. It is enabled by default and has read-only access.
  - **Username** – The user name to use for connecting to the JMX agent.
  - **Password** – The password to use for connecting to the JMX agent.
  - **RMI registry port** – The Remote Method Invocation (RMI) registry port specific for each tenant for the JMX interface. The value is selected by default from the range **30091** – **30xxx**.
  - **RMI server port** – The Remote Method Invocation (RMI) server port specific for each tenant for the JMX interface. The value is selected by default from the range **30451** – **304xx**.

Related Topics:
"Starting the Configuration Wizard"

4.3.10. REST Service Configuration

In the REST Service Configuration dialog, specify the REST service parameters:

- **REST service port** – The REST service port specific for each tenant for the REST interface. The value is selected by default from the range **30501 – 305xx**.
- **Allow origins** – Origins which will access REST Service. Origins should contain protocol, host and port of clients accessing resources via REST service. For example, if Audit Manager runs on domain *https://localhost:8443*, field **Allow origins** should contain this. Added origins can be set each on new line or separated by comma.
- **Session cookie domain** – Session cookie domain field is optional. This value should be set if domain setting the cookie is different from domain reading the cookie. Domain should contain the host. For example, if Audit Manager runs on *https://localhost:8443* and REST Service runs on *https://localhost:30501* there is no need to set this attribute. If the REST Service runs on *https://different-host:30501*, the session cookie domain should be set to value *different-host*.
- **Enable caching** – Whether (checked) or not (unchecked) to use the REST Service caches. To disable caching, uncheck the option.
- **Enable SSL** – Whether (checked) or not (unchecked) the Audit Server should use SSL connection. Using an SSL connection is the default setting because we recommend communicating over secure channels between components and services.
  - **Keystore location** – The path to the keystore which will be used for secure connection. Click the Open file browser button at the end of the line to find your location. The keystore location should be: *install_path***/conf/crypto/stores/server-ks.jks**. For more information, see the section "Preparing Truststores and Keystores for SSL Configuration" in this guide. This field is mandatory if **Enable SSL** is checked.
  - **Keystore password** – The valid password for your keystore. Click the button at the end of the password field to view the password. This field is mandatory if **Enable SSL** is checked.
  - **Truststore location** – The path to the truststore which will be used for secure connection. Click the Open file browser button at the end of the line to find your location. The location should be: *install_path***/conf/crypto/stores/server-ts.jks**. For more information, see the section "Preparing Truststores and Keystores for SSL Configuration" in this guide. If it is missing, the standard Java KeyStore (JKS) is assumed. This field is not mandatory if Enable SSL is checked.
  - **Truststore password** – The valid password for your truststore. Click the button at the end of the password field to view the password. This field is not mandatory if Enable SSL is checked.
- **Local client URI** – The local connection URI for client connecting to this REST service locally, in the format **http(s)://***localhost***:***port***/Tenants/***tenantID***/api/audit**, where *localhost* specifies your local server name, *port* specifies the server port number and *tenantID* specifies your configured tenant ID. The default port value depends on previous selection **(30501 – 305xx)**.
- **Remote client URI** – The remote connection URI for client connecting to this REST service remotely, in the format **http(s)://***host***:***port***/Tenants/***tenantID***/api/audit**, where *host* specifies your server name, *port* specifies the server port number and *tenantID*

specifies your configured tenant ID. The default port value depends on previous selection **(30501 – 305xx)**. You should open these ports on firewalls on the machine where DirX Audit is installed.

Related Topics:
“Starting the Configuration Wizard”
“Preparing Truststores and Keystores for SSL Configuration”

4.3.11. REST Service Authentication Configuration

In the REST Service Authentication Configuration dialog, specify the required REST service authentication connectivity parameters.

In the **Authentication method**, you can specify which authentication methods you want to use:

- LDAP authentication
- OpenId Connect authentication

Sample scenarios:

- LDAP authentication
  Prerequisites:
  The user accessed the DirX Audit Manager with the following link:
  https://*hostname***:***port***/audit-manager-***tenantID*
  The user with the specified username and password is searched in the configured LDAP directory service. If it is found and if a valid password is provided, the user is authenticated.
  If the user is authorized, the application is redirected to the protected area of the DirX Audit Manager.
  If the user is not authorized, the application shows message that the user is unauthorized.

In the **LDAP authentication** section, specify the required LDAP authentication parameters.

- **Use common authentication** – Whether (checked) or not (unchecked) to use common authentication connectivity parameters saved in a previous Authentication Configuration dialog. If you choose common authentication, the parameters below are read-only.

If you want to set other authentication connectivity parameters, you must specify the required parameters:

- **LDAP server host** – The host name of the LDAP server.
- **Use SSL** – Whether (checked) or not (unchecked) the LDAP connection is an SSL connection. Using an SSL connection is the default setting because we recommend communicating over secure channels between components and services.
- **LDAP server port** – The port number for the LDAP connection.

- **Authentication type** – The authentication type. Please keep the predefined value **SIMPLE**.
- **Domain** – The DirX Identity domain. This value is used in the next LDAP authentication parameters and replaces the *${domain}* placeholder.
- **Search account user DN** – The Distinguished Name of the technical LDAP account for searching users and groups on authentication.
- **Search account password** – The password of the technical account. The password is saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password.
- **Search base for users** – The base for the LDAP search. Use this setting to limit the subtree where you search for the authenticating user.
- **Search filter for users** – The LDAP filter to use to limit the result where the authenticating user is searched. Use **%s** to represent a string containing the user target naming attribute, the equal sign and the user name provided by the authentication form or an HTTP request header variable for a single sign on; for example, **cn=Tinker Boris**.
- **User target** – The naming attribute of users. It is usually the **cn** attribute.
- **Search base for groups** – The base for the LDAP search. Use this setting to limit the subtree where you search for the groups of which the authenticating user can be a member.
- **Search filter for groups** – The LDAP filter to use to limit the result where the groups of which the authenticating user can be a member are searched. Use **%d** to represent a distinguished name (DN) of the authenticating user.
- **List of auditor groups** – The list of LDAP groups (DNs) to be mapped to the Auditor role. Separate each group DN with a semicolon (;).
- **List of restricted auditor groups** – The list of LDAP groups (DNs) to be mapped to the Restricted Auditor role. Separate each group DN with a semicolon (;).
- **List of audit administrators groups** – The list of LDAP groups (DNs) to be mapped to the Audit Administrator role. Separate each group DN with a semicolon (;).
- Mapping of LDAP attributes that should be accessible for user authenticated in Audit Manager.
  - **ID**, **Name** and **Email** are mandatory and pre-defined with default values.
  - **Other attributes** – Provide additional option to add attributes that can be found in the user's LDAP. Specify each attribute as a key-value pair in the format `attributeName_label:LDAP_attributeName`. You can add multiple attributes each pair on separate line, for example
    `phone:telephonenumber`
    `work_id:employeenumber`
- **Truststore location** – The path to the truststore used for establishing secure SSL/TLS connections to the LDAP directory server. For more information about the default locations and how to prepare your own truststore, see the section "Preparing the LDAP

Truststore for Authentication and LDAP Collector Configuration". If you used the described example, the expected truststore file is named *install_path*/**conf/crypto/stores/ldap-ts.jks**. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location field can be left empty. If it is missing, the standard Java KeyStore (JKS) is assumed.

- **Truststore password** – The password to access the truststore. Click the button at the end of the password field to view the password. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location and the password fields can be left empty.
- **Inactive session lifetime (m)** – The time in minutes representing the lifetime of an inactive session after which the inactive session is timed out.
- **Maximum session lifetime (m)** – The time in minutes representing the maximum lifetime of a session cookie after which the session cookie is invalidated and new session cookie must be created.
- **Test connection** – Click to test the LDAP connection.

In the **OpenId Connect authentication** section, specify the required authentication parameters.

- **Use custom truststore** – Whether (checked) or not (unchecked) use the custom truststore.
  - **Truststore location** – The path to the truststore used for establishing secure SSL/TLS connections to the authorization server.
  - **Truststore password** – The password to access the truststore. Click the button at the end of the password field to view the password.
- **OpenID Configuration** – OpenID Connect configuration on OAuth authentication server,
  for example *`https://oauth-provider-hostname:port/oauth-provider/.well-known/openid-configuration`*
- Specific configuration values – you can use **Load values from service** button to load values from OpenID Connect configuration service.
  - **Issuer** – The Issuer Identifier of the OpenID Connect Provider. This value is the same as the iss claim value in the ID tokens issued by this provider.
    For example *`https://oauth-provider-hostname:port/oauth-provider`* .
  - **JWT Set URI** – The URL of the OpenID Connect Provider's JSON Web Key Set document. This document contains signing keys that clients use to validate the signatures from the provider.
    For example *`https://oauth-provider-hostname:port/oauth-provider/.well-known/jwks.json`* .
  - **Authorization endpoint** – The URL of the OpenID Connect Provider's OAuth Authorization Endpoint used to configure authorization in security scheme of OpenAPI (Swagger).
    For example *`https://oauth-provider-hostname:port/oauth-provider/authz`* .
  - **Token endpoint** – The URL of the OpenID Connect Provider's OAuth Token Endpoint

used to configure authorization in security scheme of OpenAPI (Swagger).
For example *`https://oauth-provider-hostname:port/oauth-provider/token`*.

- **Client ID** – Unique identifier of client application.
- **Redirect URI** – URI to be redirected to after authorizing on authorization server.
For example, *https://localhost:8443/audit-manager-tenantID/dirx-dxt-app-manager*
- The list of roles to be mapped to the specific role:
  - **List of auditor roles** – The list of roles to be mapped to the Auditor role. Separate each role with a comma (,).
  - **List of restricted auditor roles** – The list of roles to be mapped to the Restricted Auditor role. Separate each role with a comma (,).
  - **List of audit administrators roles** – The list of roles to be mapped to the Audit Administrator role. Separate each role with a comma (,).
- Claims mapping – Names of claims contained in JSON web token that should be accessible for user authenticated in Audit Manager.
  - **Roles**, **ID**, **Name** and **Email** are mandatory and pre-defined with default values.
  - **Other claims** – Provide additional option to add extra claims that can be found in claims of JSON web token. Specify each claim as a key-value pair in the format `claimName_label:JSON_claimValue`. You can add multiple claims each pair on separate line, for example
    `audience:aud`
    `expiration:exp`
- **Test connection** – Click to test the OpenID connection.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"
"Configuring LDAP Authentication"
"Configuring OIDC Authentication"

4.3.12. Audited Systems Selection

In the Audited Systems Selection dialog, choose the set of collectors for the systems that will be audited:

- **DirX Audit (base)** – Selects the generic collectors for collecting audit messages in the DirX Audit format.
- **DirX Identity** – Selects the collectors for collecting audit messages in the DirX Identity format.
- **DirX Access** – Selects the collectors for collecting audit messages from DirX Access.

The Configuration Wizard calculates the next steps depending on the number of products selected.

Related Topics: “Starting the Configuration Wizard”

4.3.13. Collectors Configuration

In the Collectors Configuration dialog, choose the collectors and components that should be enabled (E) and configured (C):

- **Error handling** – Check to enable and configure the components that handle errors during audit messages processing.
- **File collectors** – Check to enable and configure the collectors that load audit messages from files.
- **JMS collectors** – Check to enable and configure the collectors that load audit messages from a queue of the Message Broker.
- **LDAP collectors** – Check to enable and configure the collectors that load audit messages from an LDAP server.

In the dialog, you can select:

- **Do not cleanup the server container even if stopped** – Check to prevent immediate server container cleanup when changes are configured.

Related Topics: “Starting the Configuration Wizard”

4.3.14. Server Error Handling

In the Server Error Handling dialog, specify the error-handling parameters:

- **Errors folder** – The folder path at which to store audit messages with errors. Note that the folder name is configurable. When you enter only a folder name instead of the full path, the Configurator creates the folder in the following default path: *install_path*/**server_container/tenants/***tenantID*/**.**
  The folder path must be unique and must not conflict with other folder paths of the same or other tenants to prevent mixing data originating from different sources. If the folder does not exist at DirX Audit Server service start-up, it is created automatically

Related Topics: “Starting the Configuration Wizard”

4.3.15. Server LDAP Collector for DirX Identity Format

In the Server LDAP Collector for DirX Identity Format dialog, specify the required parameters.

- **Server host** – The host name or IP address of the LDAP server.
- **Use SSL** – Whether (checked) or not (unchecked) the connection is an SSL connection. Using an SSL connection is the default setting because we recommend communicating over secure channels between components and services.
- **Port** – The port number for the LDAP/LDAPs connection.
- **Domain** – The DirX Identity domain. This value is used in the next LDAP Collector authentication parameters and replaces the *${domain}* placeholder.
- **User name** – The LDAP technical account name for connection.
- **Password** – The password of the technical account. Click the button at the end of the password field to view the password.
- **Search base** – The base for the LDAP search. Use this parameter to specify the subtree from which you want to get the audit messages.
- **Repeat interval** – The time in milliseconds between runs. If there is a collector running when the timer is triggered, it is ignored.
- **Send record count** –The number of messages to be sent together in one enterprise service bus (ESB) message. Use this parameter to reduce ESB traffic and improve performance.
- **Truststore location** – The path to the truststore used for establishing secure SSL/TLS connections to the LDAP collector. For more information about default locations and how to prepare your own truststore, see the section “Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration” in the chapter “Installation Configurations”. If you used the same LDAP server as you are using for authentication, you can use the truststore you created. If you followed our example, the expected truststore file is named *install_path*/**conf/crypto/stores/ldap-ts.jks**. In the event that the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location field can be left empty. If it is missing, the standard

Java KeyStore (JKS) is assumed.

- **Truststore password** – The truststore password. Click the button at the end of the password field to view the password. In the event that the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location and the password fields can be left empty.
- **Test connection** – Click to test the LDAP connection. If invalid values are provided an error message is displayed. In this case, you can continue with the configuration but it is your responsibility to correct your settings later on.

Once you click **Next**, the Configuration Wizard checks the LDAP connection. If invalid values are provided – for example, server host or truststore – an error message is displayed. In this case, you can continue with the configuration but it is your responsibility to correct your settings later. The Configuration Wizard checks to make sure that your LDAP connection is not in use by another tenant. If it is, you cannot continue with the configuration process until you supply valid values.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"

4.3.16. Server JMS Collector for DirX Identity Format

In the Server JMS Collector for DirX Identity Format dialog, specify the required parameters.

- **Custom Message Broker** – Whether (checked) or not (unchecked) to use a custom Message Broker. Using a custom Message Broker means specifying a separate installation already configured outside of DirX Audit. If you want to use a custom Message Broker, you will enter only already configured settings for Reader:
  - **Broker URL** – The JMS message broker URL. The default JMS broker syntax is:
    `tcp://`*`host`*`:`*`port`*`?wireFormat.maxFrameSize=104857600&wireFormat.maxInactivityDuration=0`

    where you replace *host* (specify the server name) and *port* (the server port number) with the current values in your environment.
  - **Queue name** – The JMS queue name. Note that this name must be the same as the name configured at the custom Message Broker installation and must be unique. The name must be the same as the one you need to set for the corresponding JMS collector on the DirX Audit Server side.
  - **User** – The user name to authenticate when accessing the message queue.
  - **Password** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
  - **Truststore location** – The path to the truststore to be used for a secure connection. If you followed our example for truststore preparation and you saved your created truststore to the default location, the location should be: *install_path***/conf/crypto/stores/broker-ts.jks**. For more information, see the section

"Preparing Truststores and Keystores for SSL Configuration" in the chapter "Installation Configurations". If it is missing, the standard Java KeyStore (JKS) is assumed.

- **Truststore password** – The valid password for your truststore. Click the button at the end of the password field to view the password.
- **Test connection** – Click to test the Message Broker connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on.

- If you use DirX Audit Message Broker, you can see or configure:
  - **Broker URL** – The JMS message broker URL. The Configuration Wizard takes it from the Local client (connector) URI in the Message Broker Service dialog and it is read-only here. The default JMS broker syntax is:
    `tcp://host:port?wireFormat.maxFrameSize=104857600&wireFormat.maxInactivityDuration=0`
  - **Queue name** – The JMS queue name. Note that this name must be the same as the name configured at the publisher. For example, the DirX Identity JMS Audit Handler publishes the audit messages to a queue. The name must be the same name – for example, **dxt.tenantID.dxi** – as the one you need to set for the corresponding JMS collector on the DirX Audit Server side. Note that this queue name is pre-defined (it contains the tenant ID); only the queue name suffix is configurable. The queue name must be unique and must not conflict with the queue names of other JMS collectors.
  - **Use common accounts** – Whether (checked) or not (unchecked) to use the same (shared) common accounts for all collectors. If you want to use common accounts, they will be configured later in the Common JMS Collector Credentials dialog. If you want to use specific accounts for each collector, you must configure:
    - **User for Reader** – The user name to authenticate when accessing the message queue.
    - **Password for Reader** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
    - **User for Writer** – The user name to authenticate when accessing the message queue.
    - **Password for Writer** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"

4.3.17. Server JMS Collector for DirX Access Format

In the Server JMS Collector for DirX Access Format dialog, specify the required parameters.

- **Custom Message Broker** – Whether (checked) or not (unchecked) to use a custom Message Broker. Using a custom Message Broker means specifying a separate installation already configured outside of DirX Audit. If you want to use a custom Message Broker, you will enter only already configured settings for Reader:
  - **Broker URL** – The JMS message broker URL. The default JMS broker syntax is:
    `tcp://`*`host`*`:`***`port?wireFormat.maxFrameSize=104857600&wireFormat.maxInactivityDuration=0`**

    where you replace *host* (specify the server name) and *port* (the server port number) with the current values in your environment.
  - **Queue name** – The JMS queue name. Note that this name must be the same as the name configured at the custom Message Broker installation and must be unique. The name must be the same as the one you need to set for the corresponding JMS collector on the DirX Audit Server side.
  - **User** – The user name to authenticate when accessing the message queue.
  - **Password** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
  - **Truststore location** – The path to the truststore to be used for a secure connection. If you followed our example for truststore preparation and you saved your created truststore to the default location, the location should be: *install_path***/conf/crypto/stores/broker-ts.jks**. For more information, see the section “Preparing Truststores and Keystores for SSL Configuration” in the chapter “Installation Configurations”. If it is missing, the standard Java KeyStore (JKS) is assumed.
  - **Truststore password** – The valid password for your truststore. Click the button at the end of the password field to view the password.
  - **Test connection** – Click to test the Message Broker connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on.
- If you use DirX Audit Message Broker, you can see or configure:
  - **Broker URL** – The JMS message broker URL. The Configuration Wizard takes it from the Local client (connector) URI in the Message Broker Service dialog and it is read-only here. The default JMS broker syntax is:
    `tcp://`*`host`*`:`***`port?`**
    `wireFormat.maxFrameSize=104857600&wireFormat.maxInactivityDuration=0``
  - **Queue name** – The JMS queue name. Note that this name must be the same as the name configured at the publisher. For example, the DirX Identity JMS Audit Handler publishes the audit messages to a queue. The name must be the same name – for example, **dxt.tenantID.dxa** – as the one you need to set for the corresponding JMS collector on the DirX Audit Server side. Note that this queue name is pre-defined (it contains the tenant ID); only the queue name suffix is configurable. The queue name

must be unique and must not conflict with the queue names of other JMS collectors.

- **Use common accounts** – Whether (checked) or not (unchecked) to use the same (shared) common accounts for all collectors. If you want to use common accounts, they will be configured later in the Common JMS Collector Credentials dialog. If you want to use specific accounts for each collector, you must configure:
  - **User for Reader** – The user name to authenticate when accessing the message queue.
  - **Password for Reader** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
  - **User for Writer** – The user name to authenticate when accessing the message queue.
  - **Password for Writer** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"

4.3.18. Server JMS Collector for DirX Audit Format

In the Server JMS Collector for DirX Audit Format dialog, specify the required parameters:

- **Custom Message Broker** – Whether (checked) or not (unchecked) to use a custom Message Broker. Using a custom Message Broker means specifying a separate installation already configured outside of DirX Audit. If you want to use a custom Message Broker, you will enter only already configured settings for Reader:
  - **Broker URL** – The JMS message broker URL. The default JMS broker syntax is:
    `tcp://`*`host`*`:`*`port`*`?wireFormat.maxFrameSize=104857600&wireFormat.maxInactivityDuration=0`

    where you replace *host* (specify the server name) and *port* (the server port number) with the current values in your environment.
  - **Queue name** – The JMS queue name. Note that this name must be the same as the name configured at the custom Message Broker installation and must be unique. The name must be the same as the one you need to set for the corresponding JMS collector on the DirX Audit Server side.
  - **User** – The user name to authenticate when accessing the message queue.
  - **Password** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
  - **Truststore location** – The path to the truststore to be used for a secure connection. If you followed our example for truststore preparation and you saved your created

truststore to the default location, the location should be: *install_path*/**conf/crypto/stores/broker-ts.jks**. For more information, see the section "Preparing Truststores and Keystores for SSL Configuration" in the chapter "Installation Configurations". If it is missing, the standard Java KeyStore (JKS) is assumed.

- **Truststore password** – The valid password for your truststore. Click the button at the end of the password field to view the password.
- **Test connection** – Click to test the Message Broker connection. If the connection fails, an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later on.

- If you use DirX Audit Message Broker, you can see or configure:
  - **Broker URL** – The JMS message broker URL. The Configuration Wizard takes it from the Local client (connector) URI in the Message Broker Service dialog and it is read-only here. The default JMS broker syntax is:
    `tcp://`*`host`*`:`***`port`**`?`**
    `wireFormat.maxFrameSize=104857600&wireFormat.maxInactivityDuration=0`
  - **Queue name** – The JMS queue name. Note that this name must be the same as the name configured at the publisher. For example, the DirX Identity JMS Audit Handler publishes the audit messages to a queue. The name must be the same name – for example, **dxt.tenantID.dxt** – as the one you need to set for the corresponding JMS collector on the DirX Audit Server side. Note that this queue name is pre-defined (it contains the tenant ID); only the queue name suffix is configurable. The queue name must be unique and must not conflict with the queue names of other JMS collectors.
  - **Use common accounts** – Whether (checked) or not (unchecked) to use the same (shared) common accounts for all collectors. If you want to use common accounts, they will be configured later in the Common JMS Collector Credentials dialog. If you want to use specific accounts for each collector, you must configure:
    - **User for Reader** – The user name to authenticate when accessing the message queue.
    - **Password for Reader** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
    - **User for Writer** – The user name to authenticate when accessing the message queue.
    - **Password for Writer** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"

4.3.19. Common JMS Collector Credentials

In the Common JMS Collector Credentials dialog, specify common credentials that will be used for all JMS collectors where you have specified that you want to use common accounts.

- **Reader**:
  - **User** – The user name to authenticate when accessing the message queue. The name is pre-defined.
  - **Password** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.
- **Writer**:
  - **User** – The user name to authenticate when accessing the message queue.
  - **Password** – The password to authenticate when accessing the message queue. Click the button at the end of the password field to view the password.

Related Topics: "Starting the Configuration Wizard"

4.3.20. Server File Collector for DirX Identity Format

In the Server File Collector for DirX Identity Formats dialog, specify the required parameters:

- **Input folder** – The path to the folder to be monitored for audit messages. All files stored in this folder are processed except the ones that do not match the file mask; see the parameter **File mask**. Note that this folder name is configurable and is not hard coded. When you enter only a folder name instead of the full path, the Configurator creates the folder in the following default path: *install_path*/**server_container/tenants/***tenantID*. The folder path must be unique and must not conflict with other folder paths of the same or other tenants to prevent the mixing of data originating from different sources.
- **Automatically create the folder** – Whether (checked) or not (unchecked) to create the input directory automatically. When checked, the input directory is created automatically on DirX Audit Server service start-up. When unchecked, it must already exist.
- **File mask** – The filter that defines the files to be processed. Only files that match this filter will be processed. You can use the asterisk (*****) and the question mark (**?**) as wildcards.
- **Recursive** – Whether (checked) or not (unchecked) to monitor all of the subfolders within the folder specified in **Input folder**.
- **Period** – The time delay between runs in milliseconds.
- **Delay** – The initial delay (before the first run) in milliseconds.

Related Topics: "Starting the Configuration Wizard"

4.3.21. Server File Collector for DirX Access Format

In the Server File Collector for DirX Access Format dialog, specify the required parameters:

- **Input folder** – the path to the folder to be monitored for audit messages. All files stored in this folder are processed except the ones that do not match the file mask (see the parameter **File mask**). Note that this folder name is configurable and is not hard coded. When you enter only a folder name instead of the full path, the Configurator creates the folder in the following default path: *install_path***/server_container/tenants/***tenantID*. The folder path must be unique and must not conflict with other folder paths of the same or other tenants to prevent the mixing of data originating from different sources.
- **Automatically create the folder** – Whether (checked) or not (unchecked) to create the input directory automatically. When checked, the input directory is created automatically on DirX Audit Server service start-up. When unchecked, it must already exist.
- **File mask** – The filter that defines the files to be processed. Only files that match this filter will be processed. You can use the asterisk (*****) and the question mark (**?**) as wildcards.
- **Recursive** – Whether (checked) or not (unchecked) to monitor all subfolders within the folder specified in **Input folder**.
- **Period** – The time delay between runs in milliseconds.
- **Delay** – The initial delay (before the first run) in milliseconds.

Related Topics: “Starting the Configuration Wizard”

4.3.22. Server File Collector for DirX Audit Format

In the Server File Collector for DirX Audit Format dialog, specify the required parameters:

- **Input folder** – The path to the folder to be monitored for audit messages. All files stored in this folder are processed except for the ones that do not match the file mask; see the parameter **File mask**. Note that this folder name is configurable and is not hard coded. When you enter only a folder name instead of the full path, the Configurator creates the folder in the following default path: *install_path*/**server_container/tenants/***tenantID*. The folder path must be unique and must not conflict with other folder paths of the same or other tenants to prevent the mixing of data originating from different sources.
- **Automatically create the folder** – Whether (checked) or not (unchecked) to create the input directory automatically. When checked, the input directory is created automatically on DirX Audit Server service start-up. When unchecked, it must already exist.
- **File mask** – The filter that defines the files to be processed. Only files that match this filter will be processed. You can use the asterisk (*****) and the question mark (**?**) as wildcards.
- **Recursive** – Whether (checked) or not (unchecked) to monitor all subfolders within the folder specified in **Input folder**.
- **Period** – The time delay between runs in milliseconds.
- **Delay** – The initial delay (before the first run) in milliseconds.

Related Topics: "Starting the Configuration Wizard"

4.3.23. Scheduled Jobs Configuration

In the Scheduled Jobs Configuration dialog, specify the schedules for DirX Audit Server jobs which typically run regularly (daily) to process the data collected over a period of a few days. You can specify different times for all configured tenants to avoid overloading the DirX Audit Server.

You can set up an advanced CRON expression to schedule the jobs more precisely. For example, the expression `0+0/10+*+?+*+*` starts the job every ten minutes. For more information on how to set up a CRON expression, see http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html.

Alternatively, you can click the **Simple time configuration** button to display the setting options. Select **daily at** to specify hour and minutes; or select **every** to specify minutes.

For each job, you can select whether you want to schedule the job and specify the following parameters:

- **Recommended time range** – The time range when the server runs scheduled jobs. The Tenant configuration reads the values saved by the Core Configurator Server Container dialog. You can use the **Fill in recommended values** button to fill all schedules in recommended time range.
- **Scheduled reports** – Whether (checked) or not (unchecked) to schedule the job. The default value is `0/30+*+*+?+*+*` which starts the Synchronization scheduled reports job every 30 seconds.
- **Context records calculation** – Whether (checked) or not (unchecked) to schedule the job. The default value is `0+0/5+*+?+*+*` which starts the job every 5 minutes. The **message limit per run** field for this job controls the number of messages processed in a run of the context records calculation job. Specify the value as a positive nonzero integer; the recommended range for the value is between **100** and **1000**. The higher the value, the less frequent the execution should be. The default value for **message limit per run** is set to **100** and the default frequency at which the job is run corresponds to this value.
- **History DB update** – Whether (checked) or not (unchecked) to schedule the job. The default value is `0+0+21+?+*+*` which starts the History post–processing job at 21:00.
- **Fact population** – Whether (checked) or not (unchecked) to schedule the job. The default value is `0+40+23+?+*+*` which starts the Fact population job at 23:40.

Related Topics: “Starting the Configuration Wizard”

4.3.24. Scheduled Purge Jobs Configuration

DirX Audit Server provides several different purge jobs. Each job processes a specific kind of DirX Audit data. In the Scheduled Purge Jobs Configuration dialog, select the type of DirX Audit data to be processed:

- **History entries data purge job configuration** – Checkout to enable schedule configuration for delete expired history entries data.
- **Audit messages data purge job configuration** – Checkout to enable schedule configuration for delete complete audit messages, including message additions and original messages.
- **Original audit messages data purge job configuration** – Checkout to enable schedule configuration for delete only original messages. You cannot select this type unless **Save original audit messages** is selected in the Data DB Configuration dialog.

Use the “Schedule Configuration for Purging...” dialogs to activate and schedule the job(s) for the DirX Audit data type(s) you select in this dialog and to specify how old the data should be in order for it to be deleted.

Related Topics: “Starting the Configuration Wizard”

4.3.25. Schedule Configuration for Purging Ended History Entries Data

Use the Schedule Configuration for Purging Ended History Entries Data dialog to specify:

- **Enable history entries data purge** – Whether (checked) or not (unchecked) to activate the DirX Audit Server job that deletes this type of DirX Audit data. If you enable history entries data purge, you can set:
  - The age of the data to be deleted, in years or months.
- **Enable export for data to be purged** – Whether (checked) or not (unchecked) to export and save the data to be purged.
  If you enable export you must select **Purged data export folder** and the DirX Audit Server job exports data before it is deleted.
  You can use it only if history entries data purge is enabled.

If you enable history entries data purge, you can set:

- Whether the job should run daily or monthly, and if monthly, the day of the month on which it should run, and the time of day at which it should be run.
  Alternatively, you can check **Set with CRON expression** and specify the schedule as a CRON expression.
  For example, the expression `0+0+10+?+*+1#1` starts the job at 10am on the first Sunday of each month.
  For more information on how to set up a CRON expression, see http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html.

Related Topics: “Starting the Configuration Wizard”

4.3.26. Schedule Configuration for Purging Audit Messages Data

Use the Schedule Configuration for Purging Audit Messages Data dialog to specify:

- **Enable audit messages data purge** – Whether (checked) or not (unchecked) to activate the DirX Audit Server job that deletes this type of DirX Audit data. If you enable audit messages data purge, you can set:
  - The age of the data to be deleted, in years or months.
- **Enable export for data to be purged** – Whether (checked) or not (unchecked) to export and save the data to be purged.
  If you enable export you must select **Purged data export folder** and the DirX Audit Server job exports data before it is deleted.
  You can use it only if audit message data purge is enabled.

If you enable history entries data purge, you can set:

- Whether the job should run daily or monthly, and if monthly, the day of the month on which it should run, and the time of day at which it should be run.
  Alternatively, you can check **Set with CRON expression** and specify the schedule as a

CRON expression.
For example, the expression `0+0+10+?+*+1#1` starts the job at 10am on the first Sunday of each month. For more information on how to set up a CRON expression, see http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html.

Related Topics: “Starting the Configuration Wizard”

4.3.27. Schedule Configuration for Purging Original Audit Messages Data

Use the Schedule Configuration for Purging Original Audit Messages Data dialog to specify:

- **Enable original audit messages data purge** – Whether (checked) or not (unchecked) to activate the DirX Audit server job that deletes this type of DirX Audit data. If you enable original audit messages data purge, you can set:
  - The age of the data to be deleted, in years or months.
  - Whether the job should run daily or monthly, and if monthly, the day of the month on which it should run, and the time of day at which it should be run. Alternatively, you can check **Set with CRON expression** and specify the schedule as a CRON expression.
    For example, the expression `0+0+10+?+*+1#1` starts the job at 10am on the first Sunday of each month. For more information on how to set up a CRON expression, see http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html.

Related Topics: "Starting the Configuration Wizard"

4.3.28. History Synchronization LDAP Configuration

In the History Synchronization LDAP Configuration dialog, specify the LDAP connection parameters used for audit entries synchronization.

- **Use common authentication** – Whether (checked) or not (unchecked) to use common authentication connectivity parameters saved in a previous Authentication Configuration dialog. If you choose common authentication, the parameters below are read-only. Only the **Page size** can be modified.

If you want to set other authentication connectivity parameters, you must specify the required parameters:

- **LDAP server host** – The host name of the LDAP server.
- **Use SSL** – Whether (checked) or not (unchecked) the LDAP connection is an SSL connection. Using an SSL connection is the default setting because we recommend communicating over secure channels between components and services.
- **LDAP server port** – The port number for the LDAP connection.
- **Authentication type** – The authentication type. Please keep the predefined value **SIMPLE**.
- **Domain** – The DirX Identity domain. This value is used in the next LDAP authentication parameters and replaces the *${domain}* placeholder.
- **Search account user DN** – The Distinguished Name of the technical LDAP account for searching users and groups on authentication.
- **Search account password** – The password of the technical account. The password is

saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password.

- **Page size** – The maximum number of entries per page when LDAP paging is used for iterating through results. The default is **100** and should be modified only when needed.
- **Truststore location** – The path to the truststore used for establishing secure SSL/TLS connections to the LDAP directory server. For more information about the default locations and how to prepare your own truststore, see the section "Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration". If you used the described example, the expected truststore file is named *install_path*/**conf/crypto/stores/ldap-ts.jks**. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location field can be left empty. If it is missing, the standard Java KeyStore (JKS) is assumed.
- **Truststore password** – The password to access the truststore. Click the button at the end of the password field to view the password. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location and the password fields can be left empty.
- **Test connection** – Click to test the LDAP connection.

Once you click **Next**, the Configuration Wizard checks the LDAP connection. If invalid values are provided – for example, server host or truststore – an error message is displayed. In this case, you can continue with the configuration, but it is your responsibility to correct your settings later. The Configuration Wizard also checks if your LDAP connection is in use by another tenant. If it is, a warning message is displayed, but you can continue with the configuration process if desired.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"
DirX Audit History Synchronization Guide

4.3.29. Discontinued DirX Identity Synchronization Workflows Migration Connectivity Configuration

As of DirX Audit 7.2, the new DirX Audit History Synchronization jobs replace the DirX Identity synchronization workflows for the DirX Audit History Database. During the migration process, the Configuration Wizard checks if there are any discontinued workflows configured on DirX Identity. If there are, it displays them in the following steps and offers actions that can be taken.

The Discontinued DirX Identity Synchronization Workflows Migration Connectivity Configuration dialog is displayed only during the migration process. Specify the LDAP connection parameters used for migration:

- **LDAP server host** – The host name of the LDAP server where discontinued DirX Identity synchronization workflows for the DirX Audit History Database may be used and

configured.

- **Use SSL** – Whether (checked) or not (unchecked) the LDAP connection is an SSL connection. Using an SSL connection is the default setting because we recommend communicating over secure channels between components and services.
- **LDAP server port** – The port number for the LDAP connection.
- **Authentication type** – The authentication type. Please keep the predefined value **SIMPLE**.
- **Domain** – The DirX Identity domain where discontinued DirX Identity synchronization workflows for the DirX Audit History Database may be used and configured.
- **Admin account user DN** – The Distinguished Name of the technical LDAP account for searching workflows, attributes, and their subsequent deactivation.
- **Admin account password** – The password of the technical account. The password is saved in the Tenant configuration file and is encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Click the button at the end of the password field to view the password.
- **Workflows folder** – Name of folder containing the Discontinued DirX Identity Synchronization Workflows. If the field is left empty all Discontinued DirX Identity Synchronization Workflows will be taken into consideration.
- **Truststore location** – The path to the truststore used for establishing secure SSL/TLS connections to the LDAP directory server. For more information about the default locations and how to prepare your own truststore, see the section “Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration”. If you used the described example, the expected truststore file is named *install_path*/**conf/crypto/stores/ldap-ts.jks**. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location field can be left empty. If it is missing, the standard Java KeyStore (JKS) is assumed.
- **Truststore password** – The password to access the truststore. Click the button at the end of the password field to view the password. If the requested certificates are part of certificates imported in the Java Runtime Environment, the truststore location and the password fields can be left empty.
- **Test connection** – Click to test the LDAP connection.

Once you click **Next**, the Configuration Wizard checks the LDAP connection. If invalid values are provided – for example, server host or truststore – an error is displayed and you must correct it for the migration process to continue.

Related Topics:
“Starting the Configuration Wizard”
“Preparing Truststores and Keystores for SSL Configuration”
DirX Audit History Synchronization Guide

4.3.30. Discontinued DirX Identity Synchronization Workflows Channels Configuration

As of DirX Audit 7.2, the new DirX Audit History Synchronization jobs replace the DirX Identity synchronization workflows for the DirX Audit History Database. During the migration process, the Configuration Wizard checks if any discontinued workflows are configured. If yes, it will display them and offer actions that can be taken.

The Discontinued DirX Identity Synchronization Workflows Channels dialog is displayed only during the migration process. It displays discovered configured discontinued workflows with their configuration (entry type and attribute mapping). You should check these workflows and decide if you want to migrate their attribute mapping configuration to the new DirX Audit History Synchronization. You can select:

- **Migrate workflows** – Whether (checked) or not (unchecked) to migrate the discontinued workflows configuration (entry type and its attribute mapping) to the new DirX Audit History Synchronization.
- **Exclude all large attributes** – Whether (checked) or not (unchecked) to exclude all large attributes configured in discontinued DirX Identity synchronization workflows for the DirX Audit History Database from the new DirX Audit History Synchronization. See the *DirX Audit History Synchronization Guide* for more details about excluded attributes.

Once you click **Next**, the Configuration Wizard checks your choices. If migration is selected, it prepares to migrate the discontinued DirX Identity synchronization workflows attribute mapping configuration.

Migrated attribute mappings that are different from the default DirX Audit History Synchronization configuration (*install_path***/conf/defaults/tenant/configuration.cfg**) are written in the tenant-specific configuration file (*install_path***/conf/tenants/***tenantID***/configuration.cfg**). A complete list of migrated attribute mapping configuration is also written to a text file for your review (*install_path***/conf/tenants/***tenantID***/history_migration_result.txt**).

Related Topics:
“Starting the Configuration Wizard”
“Preparing Truststores and Keystores for SSL Configuration”
DirX Audit History Synchronization Guide

4.3.31. Discontinued DirX Identity Synchronization Workflows Deactivation

As of DirX Audit 7.2, the new DirX Audit History Synchronization jobs replace the DirX Identity synchronization workflows for the DirX Audit History Database. These discontinued workflows must be disabled on DirX Identity. During the migration process, the Configuration Wizard checks if any discontinued workflows are configured and active. If there are, it displays them and offers actions that can be taken.

The Discontinued DirX Identity Synchronization Workflows Deactivation dialog is displayed only during the migration process. It displays discovered configured and active discontinued workflows. You should check these workflows and decide if you want to deactivate them on DirX Identity. You can select:

- **Deactivate workflows** – Whether (checked) or not (unchecked) the discontinued workflows should be automatically deactivated on DirX Identity.

If you don't want to deactivate discontinued workflows automatically during the migration process, you must do it manually as these workflows are no longer supported.

Once you click **Next**, the Configuration Wizard checks your choices. If you have selected workflow deactivation, it prepares for deactivation and then deactivates them when you finish the configuration.

The Configuration Wizard also checks combined DirX Identity workflows. If these workflows contain only discontinued DirX Identity synchronization workflows for the DirX Audit History Database, they are also automatically deactivated if you choose this option. However, combined DirX Identity workflows that contain other workflows not used for synchronization to the DirX Audit History Database cannot be deactivated automatically. In this case, the information message is displayed and you must either manually deactivate them or remove the references to the discontinued DirX Identity synchronization workflows for the DirX Audit History Database from the combined workflow configuration.

The complete list of disabled DirX Identity synchronization workflows for the DirX Audit History Database workflows is saved in the following text file:
install_path/**conf/tenants/***tenantID*/**history_workflows_disable_result.txt**.

The list of combined DirX Identity workflows which contain other workflows that are not relevant to DirX Audit History Database synchronization is saved in the following text file:
install_path/**conf/tenants/***tenantID*/**history_combined_nonhdb_workflows_result.txt**.

Related Topics:
"Starting the Configuration Wizard"
"Preparing Truststores and Keystores for SSL Configuration"
DirX Audit History Synchronization Guide

4.3.32. Scheduled History Synchronization Jobs Configuration

In the Scheduled History Synchronization Jobs Configuration dialog, you can create,

modify, or remove the History synchronization jobs used for history entries synchronization.

Important: Before you configure History Synchronization jobs to run regularly you must:

- Check if the discontinued DirX Identity synchronization workflows used for audit entries synchronization to the DirX Audit History Database are disabled on DirX Identity.
- Check if DirX Identity Store is configured as required by History Synchronization, see the "Preparing the DirX Identity Store" in the *DirX Audit History Synchronization Guide* for details.
- Check the default History Synchronization attribute configuration. You need to decide whether it is sufficient to synchronize only the attributes defined in the default tenant configuration (*install_path*/**conf/defaults/tenant/configuration.cfg**) or if you need to change or extend the list of synchronized attributes. If you want to modify the list of synchronized attributes, you must modify them in the tenant-specific configuration file created after the first tenant configuration (*install_path*/**conf/tenants/***tenantID*/**configuration.cfg**). See the *DirX Audit History Synchronization Guide* for details on how to configure attributes for synchronized entry types.

You can schedule two types of History Synchronization jobs – **Modify** job and **Delete** job. The **Modify** job synchronizes recently added or modified entries and all their attributes together with validity periods from DirX Identity domain to the DirX Audit History Database. The **Delete** job detects entries deleted from the DirX Identity domain and closes the validity of entries and their attributes in the DirX Audit History Database.

Make sure not to schedule two or more DirX Audit History Synchronization jobs at the same time. If the second job is scheduled to start while another History Synchronization job is still running, the second job will not start.

If you are migrating from an older DirX Audit version that used DirX Identity synchronization workflows for the DirX Audit History Database and you choose automatic migration, two History Synchronization jobs are predefined for you. Their configuration is set according to the information obtained during the migration process. They are disabled and you must verify their settings before you enable them and run regularly.

- Modify job for migration
- Delete job for migration

In the "Scheduled History Synchronization Jobs Configuration" dialog, specify the configuration for each configured job:

- **Enable / disable (E)** – Whether the configured job is enabled (checked) or disabled (unchecked).
- **Synchronization job modification** – Click on the drop-down list to change the job name and its configuration. Specify the parameters:
  - **Description** – A detailed description of the job.
  - **Schedule** – When the job should run. You must use CRON expression to schedule the job. For example, `0+0+21+?+*+*` for a **delete** job, which starts the job at 21:00,

and `0+0+0/3+?+*+*` for a **modify** job, which starts the job every 3 hours. For more information on how to set up a CRON expression, see http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html.

- **Entry types** – The entry types will be synchronized. You must use the entry type's id defined in the Tenant configuration file separated by a comma. For example, for synchronization information about users and their roles and permissions, you can use the following entry type ids:
  - permission,role,user

    The complete list of all entry type ids:
  - account,businessobject,certificationassignmentchange,certificationcampaign, certificationentry,certificationnotification,configurationobject,domainobject, tsconfigurationobject,accessright,delegation,group,permission,auditpolicy,policy, role,roleparam,targetsystem,ticket,user,assignment,activitydefinition, workflowdefinition, activityinstance,workflowinstance
- **Only modified since** – How old modifications should be synchronized. This option is available only for the **modify** job. You can use relative date-time range defined in the following syntax: <*CurrentTimePeriodType*>[(**+**|**-**)<*Offset*>] where <*CurrentTimePeriodType*> is one of: **TH**, **TD**, **TW**, **TM**, **TY** expressing hour, day, week, month or year, and <*Offset*> is an integer representing the offset by which to shift the given time period; for example, **TD-5**. You can also leave it empty to synchronize all selected entry types without a time restriction (it is recommended if you don't have synchronized objects created in the past).

- **Remove (R)** – Click the minus button to remove the job from configuration.

You can add a new job on the last line: fill in the name, select the type of synchronization job (**modify**/**delete**) and then click the plus button to add it to the list. The job is added to the list with an automatically generated unique id and you can modify its configuration.

Once you click **Next**, the Configuration Wizard checks the jobs configuration. If some value is missing or invalid values are provided, an error message is displayed and you must correct it.

Related Topics:
"Starting the Configuration Wizard"
DirX Audit History Synchronization Guide

4.3.33. Pre-Configuration Summary

The Configuration Wizard displays the Tenant configuration selections you have made and asks you to review them.

- Click **Previous** to change any settings you have made.
- Click **Next** to start the Tenant configuration process.

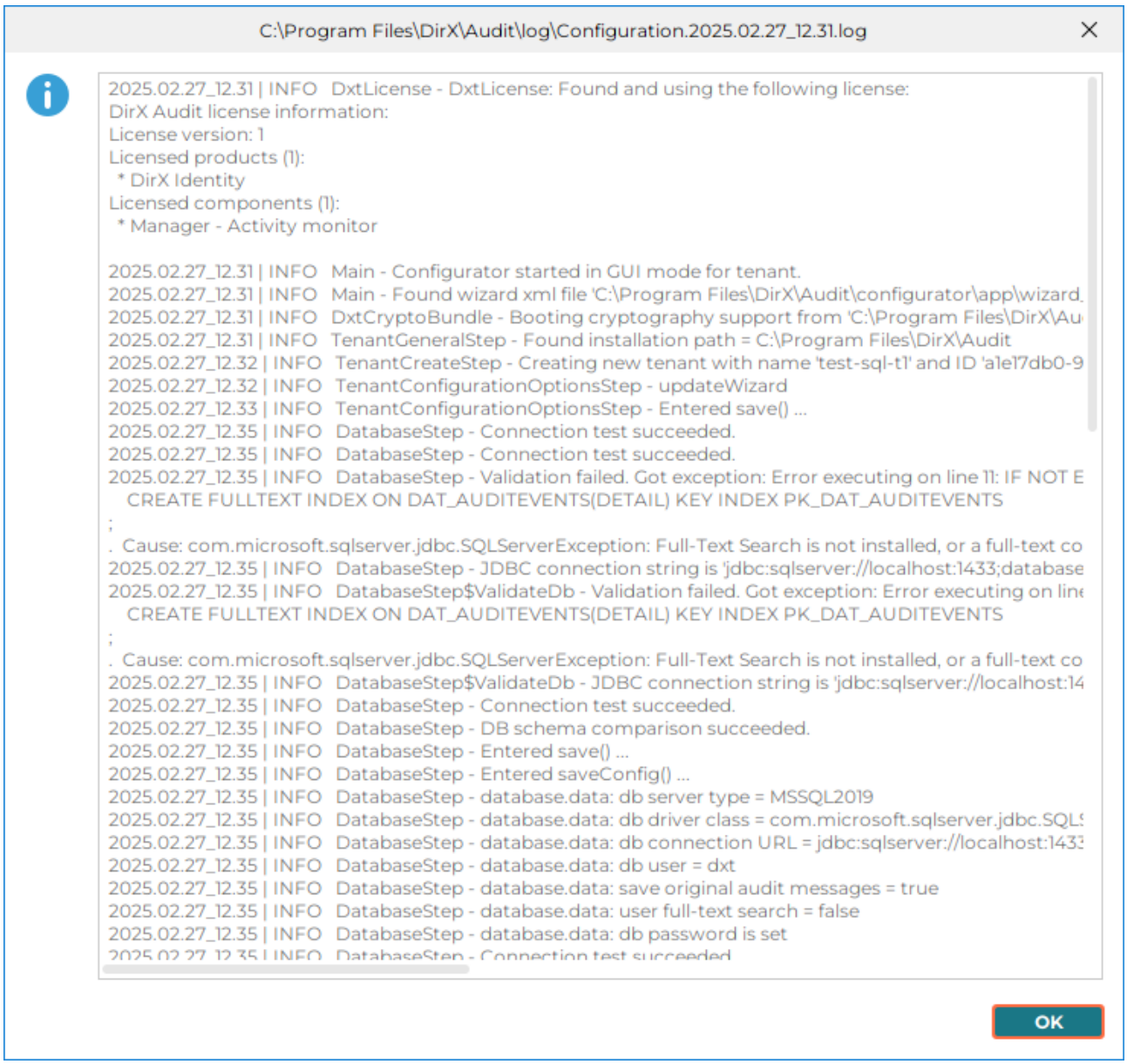
Related Topics:
“Starting the Configuration Wizard”

4.3.34. Configuration in Progress

While configuring the tenant is in progress, the Configuration Wizard displays the current task in gray, successfully performed tasks in green and failed tasks in red. It displays the detailed action of the current task in the **Action detail** field.

When the Tenant configuration process completes, click:

- **Display current configuration log** – To display information on the DirX Audit Tenant configuration you just performed, including thrown exceptions.



- **Next** – To continue with the Tenant configuration.

Related Topics:
"Starting the Configuration Wizard"

4.3.35. Next Actions Options

In the Next Actions Options dialog, specify whether or not you want to continue with Tenant configuration:

- **Run Tenant Configuration** - Whether (checked) or not (unchecked) you want to start the Tenant configuration procedure again to keep creating or modifying new or existing tenants.
- Click **Finish** to complete the Tenant configuration process.

Related Topics:
"Starting the Configuration Wizard"

4.4. Post-Configuration Tasks

Before using some of the features, you may want to adapt some settings or you may need to perform additional actions. The following sections discuss these tasks.

4.4.1. Dashboard and Fact Population

The DirX Audit Manager Classic's Dashboard feature evaluates OLAP tables that are created and filled by the fact population component of DirX Audit Server.

Fact population runs scheduled according to the default schedule you specified in the Scheduled Jobs Configuration dialog, which usually starts the job once per night. Before you can view charts on audit events in DirX Audit Manager Classic, you must make sure that the corresponding tables exist. You can adapt the schedule or run the fact population CLI tool manually. For details, see the chapter "Managing Fact and Dimension Tables" in the *DirX Audit Administration Guide*.

DirX Audit comes with a set of default Dashboard components that you can load into the DirX Audit Manager Classic and use right away. See the section "Loading the Default Dashboard Components" in the "Getting Started" chapter of the *DirX Audit Tutorial*.

4.4.2. History Entry Setup

Before you can view history entries using DirX Audit Managers, you must:

- Import history entries from DirX Identity at least once. See the "History Synchronization LDAP Configuration" and "Scheduled History Synchronization Jobs Configuration" dialogs description in this chapter for details how to run DirX Audit History Synchronization job. See the *DirX Audit History Synchronization Guide* for details on how to configure the History Synchronization jobs.
- Run the history post-processing server job at least once. For details on how to adapt the schedule for updating the foreign keys in the DirX Audit History Database, see the chapter "Managing History Database Tables" in the *DirX Audit Administration Guide*. The default schedule you specified in the Scheduled Jobs Configuration dialog usually starts the job once per night.

4.4.3. Database Indexing

To achieve satisfactory database performance, you should strongly consider creating indexes. For more information on this task, see the chapter "Tuning Database Performance" in the *DirX Audit Administration Guide*.

4.5. Using Silent Configuration

DirX Audit can also be configured in silent mode, which requires no user interaction. To initiate a silent configuration:

- Run the Core configuration in the standard/GUI mode and then cancel it and choose to keep the changes when the Pre-Configuration Summary dialog is displayed. This action customizes the core **configuration.cfg** properties file in the *install_path***/conf** folder so that you can use it as a preset for the silent Core configuration operation.
- Run the Tenant configuration in the standard/GUI mode and then cancel it and choose to keep the changes when the Pre-Configuration Summary dialog is displayed. This action customizes the tenant-specific **configuration.cfg** properties file in the *install_path***/conf/tenants/***tenantID* folder so that you can use it as a preset for the silent Tenant configuration operation.
- We recommend stopping DirX Audit services, including the Apache Tomcat service if it is used to start the DirX Audit Managers.
- Start the Core configuration: Run **configuration.bat** (**configuration.sh**) in *install_path***/configurator/bin** with the following parameters:
  `configuration.bat -i SILENT -`*`option(s)`*

  For example: `configuration.bat -i SILENT -ca`
- Start the Tenant configuration: Run **configuration.bat** (**configuration.sh**) in *install_path***/configurator/bin** with the following parameters:
  `configuration.bat tenant -i SILENT -id` *`tenantID1 tenantID2 -option(s)`*

  In the following example, the silent complete tenant configuration will be started for all tenants:
  `configuration.bat tenant -i SILENT -ca`

  In the following example, the silent tenant message broker configuration will be started for a tenant with the ID **4f753e1d-d0de-4aef-bb22-caace7342e99**:
  `configuration.bat tenant -i SILENT -id 4f753e1d-d0de-4aef-bb22-caace7342e99 -mb`

  In the following example, the silent complete tenant configuration will be started for two tenants with IDs **4f753e1d-d0de-4aef-bb22-caace7342e99** and **1eb03110-0e7d-42f8-be24-7f2acd5e757d**:
  `configuration.bat tenant -i SILENT -id 4f753e1d-d0de-4aef-bb22-caace7342e99 1eb03110-0e7d-42f8-be24-7f2acd5e757d -ca`
- Check for errors and search for the string **The configuration finished successfully!** in the file *install_path***/log/Configuration.***configurationDate***_Time.log**.

To run in silent mode, you must specify the option for all components (**-ca**) or a list of the component options you want to configure. To use the optional test/verify database options in silent mode, you must also specify at least one component option.

4.5.1. Using Core Configuration Options

You can run **configuration.bat core -h** or **configuration.bat core --help** to get an overview of the available options.

Common Core configuration options

-h or **--help** – Lists common options and their description.
-i *arg* – Configuration mode.

Component options are

-ca or **--configure_all** – Configure all components.
-cs or **--common_settings** – Configure Common settings.
-ep or --encrypt_passwords – Encrypt passwords.
-mc or **--manager_container** – Configure Common Managers Container.
-md or **--manager_deployment** – Configure Manager Classic Deployment.
-mb or **--message_broker** – Configure Message Broker.

4.5.2. Using Tenant Configuration Options

You can run **configuration.bat tenant -h** or **configuration.bat tenant --help** to get an overview of the available options.

Common tenant configuration options

-h or **--help** – Lists common options and their description.
-i *arg* – Configuration mode.
-id *tenantID(s)* – Specifies the tenant(s) for which the configuration is to start. This parameter is optional. If it is not used, the configuration starts for all tenants. Use the space character to separate multiple *tenantID*s.

Component options are

-ca or **--configure_all** – Configure all components.
-ep or --encrypt_passwords – Encrypt passwords.
-mb or **--message_broker** – Configure Message Broker.
-md or **--manager_deployment** – Configure Manager Deployment.
-sc or **--server_container** – Configure Server container.
-sd or **--server_deployment** – Configure Server deployment.

You can also use optional database operations options (which must be used in conjunction with at least one of the component options).

Optional database operations options

-tcc or **--test_config** – Test the Config DB connection.
-tdc or **--test_data** – Test the Data DB connection.
-thc or **--test_history** – Test the History DB connection.
-vcd or **--validate_config** – Validate the Config database.
-vdd or **--validate_data** – Validate the Data database.
-vhd or **--validate_history** – Validate the History database.

4.5.3. Running a Silent Configuration on a Different Machine

You can also use the configuration files from a different installation and machine (created by the same version of DirX Audit), but make sure that you take only the suitable Core or Tenant configuration files.

The following example describes how to start the Core and the Tenant configuration on the production machine; configuration files were prepared on the test machine with the Core and Tenant configuration:

1. Make your local copy of the *install_path***/conf/configuration.cfg** properties file from the test machine. Replace all encrypted passwords saved in the configuration file with plain text because all passwords are encrypted using an installation-specific master encryption key. This master key is randomly generated during the first installation on a given host and is different on each installed host. Save your changes.
2. Make your local copy of the *install_path***/conf/tenants** folder with the tenants you want to use and their properties files from the test machine. Replace all encrypted passwords saved in the configuration files with plain text. Save your changes.
3. Copy your modified **configuration.cfg** properties file to the *install_path***/conf** folder on the production machine where the Core silent configuration is to be run. In this example, DirX Audit is installed on the machine and *install_path* represents the DirX Audit installation location (you can use silent installation described in the section “Silent Installation” in the chapter “Installation Configurations”). You must check the file system paths in the copied **configuration.cfg** file and then update them to the new host (unless DirX Audit is installed in exactly the same path on both machines).
4. Copy your modified tenant properties file to the *install_path***/conf/tenants** folder on the production machine and check the file system paths in the copied files.
5. To run DirX Audit Managers, you must install Apache Tomcat, which serves as the DirX Audit Manager’s container. Make sure that the correct *install_path* is set in your configuration files.
6. To run Oracle Database as the DirX Audit database, you must copy the Oracle Database JDBC driver into the *install_path***/lib** folder on the production machine.
7. Copy all keystores and truststores prepared on the test machine to the *install_path***/conf/crypto/stores** folder on the production machine and check the paths in the configuration files.
8. We recommend stopping DirX Audit services, including the Apache Tomcat service if it is used to start the DirX Audit Managers.
9. Start the Core configuration: Run **configuration.bat** (**configuration.sh**) in *install_path* /**configurator/bin** with the following parameters:

   ```
   configuration.bat -i SILENT -option(s)
   ```

   For example:
   ```
   configuration.bat -i SILENT -ca
   ```
10. Check for errors and search for the string **The configuration finished successfully!** in the file *install_path***/log/Configuration.***configurationDate__Time_***.log**.

11. Start the Tenant configuration: Run **configuration.bat** (**configuration.sh**) in *install_path*/**configurator/bin** with the following parameters:

    configuration.bat tenant -i SILENT -id *tenantID1 tenantID2 -option(s)*

    In the following example, the silent complete tenant configuration will be started for all tenants:

    ```
    configuration.bat tenant -i SILENT -ca
    ```

12. Check for errors and search for the string **The configuration finished successfully!** in the file *install_path*/**log/Configuration.***configurationDate__Time_***.log**.

4.6. Configuring LDAPS

DirX Audit allows you to configure LDAP over SSL (LDAPS) for establishing secure SSL/TLS connections to the LDAP directory server. The secure communication is set as the default communication between components and services during configuration process and if you followed the default steps, no further settings are required.

If you have not set up secure SSL/TLS connections to the LDAP directory server, follow these steps to configure LDAPS in DirX Audit:

- Configure LDAPS authentication for DirX Audit Managers and DirX Audit Server.
- Configure LDAPS authentication for the DirX Audit Server LDAP Collector for DirX Identity.
- Start the DirX Audit services.

The next sections detail these tasks and explain how to set debugging.

4.6.1. Configure DirX Audit Manager and DirX Audit Server for LDAPS

To configure authentication over LDAPS for DirX Audit Manager and for DirX Audit Server when reporting jobs scheduled for DirX Audit Manager are run:

- Run the DirX Audit Configuration Wizard for Tenant configuration.
- Go to the **REST Service Authentication Configuration** step in the wizard.
- Check **Use SSL**.
- Enter the LDAP server SSL port. The default value is **636**.
- Enter the path and credentials for the truststore file that contains the relevant DirX Directory Server and trusted CA certificates. See the section "Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration" in the chapter "Installation Configurations" for details.
- Enter other settings as necessary.
- Finish the configuration.

4.6.2. Configure DirX Audit Manager Classic and DirX Audit Server for LDAPS

To configure authentication over LDAPS for DirX Audit Manager Classic and for DirX Audit Server when reporting jobs scheduled for DirX Audit Manager Classic are run:

- Run the DirX Audit Configuration Wizard for Tenant configuration.
- Go to the **Authentication Configuration** step in the wizard.
- Check **Use SSL**.
- Enter the LDAP server SSL port. The default value is **636**.
- Enter the path and credentials for the truststore file that contains the relevant DirX Directory Server and trusted CA certificates. See the section "Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration" in the chapter "Installation Configurations" for details.
- Enter other settings as necessary.
- Finish the configuration.

4.6.3. Configure the Server LDAP Collector for DirX Identity Format for LDAPS

To configure authentication over LDAPS for the DirX Audit Server LDAP Collector:

- Run the DirX Audit Configuration Wizard for Tenant configuration.
- Go to the **Server LDAP Collector for DirX Identity Format** step in the wizard.
- Check **Is SSL**.
- Enter the SSL port. The default value is **636**.
- Enter the path and credentials for the truststore file that contains the relevant DirX

Directory Server and trusted CA certificates. See the section "Preparing the LDAP Truststore for Authentication and LDAP Collector Configuration" in the chapter "Installation Configurations" for details.

- Enter other settings as necessary.
- Finish the configuration.

4.6.4. Start DirX Audit Services

Start the following DirX Audit services:

- DirX Audit Message Broker 9.0
- DirX Audit Server *tenant_display_name* 9.0 (a separate instance of DirX Audit Server is created for every tenant)
- The Apache Tomcat service where you deployed DirX Audit Managers

Next, check that the DirX Audit Server and DirX Audit Managers connectivity is set up correctly:

- Some minutes after start-up, DirX Audit Server tries to connect to the DirX Audit Message Broker and the LDAP server. Once the server has audit messages to import, it connects to the DirX Audit database. If something fails, you should see error messages in the log file *install_path***/server_container/tenants/***tenantID***/logs/dirxaudit-server.log**.
- Log in to the DirX Audit Manager to test whether you can authenticate. For error messages, check the console output in your browser (use the Developer Tools) or see the REST error messages in the server log file *install_path* **/server_container/tenants/***tenantID***/logs/dirxaudit-server.log**.
- Log in to the DirX Audit Manager Classic to test whether you can authenticate to LDAP and connect to the DirX Audit database. For error messages, check the log file *tomcat_install_path*/**logs/dirxaudit-manager.log**.

5. Installing DirX Audit System Services

The installed tools and containers (Message Broker and Server) are set up to be started as system services so that they start automatically on system start-up (on default settings). This option is available on both supported Windows and UNIX platforms. There is also the configuration option to disable the automatic startup service start and select the manual start, which means that the user will need to launch the service manually in order to be able to use it.

The services are installed by the configuration procedure. This chapter describes how to perform this step manually on the Linux platform if you cannot or do not want to do it with the configurator (e.g., you cannot run it as root). The service for Tomcat, which is used as a container for the DirX Audit Manager application, is configured using Tomcat native tools and configuration; for example, see http://tomcat.apache.org/tomcat-11.0-doc/setup.html.

Warning: You must configure DirX Audit before you start the services or restart the system. Starting the services or restarting the system without first configuring DirX Audit will create an inconsistent installation that you will need to reconfigure manually to restore to proper operation. See the chapter “Configuring DirX Audit” for instructions.

Linux

The operating system must use **systemd** to run system services.

To install the DirX Audit applications as system services:

1. Update the startup scripts to use the correct paths and other properties.
2. Register the service within the system.

The startup scripts are located at:

- Message broker:
  install_path`/message_broker/bin/service/linux_x86_64/dirx-audit-messagebroker`
- Server container (per tenant):
  install_path`/server_container/tenants/`*tenantID*`/bin/dirx-audit-server-container`

In each file, update values by checking and correcting the properties in this file. You need to fill in at least the correct values (user and group name) into the properties RUN_AS_USER and RUN_AS_GROUP or comment them out.

To install the service, run the following command in a shell as **root**:
pathToServiceScript `install`

where *pathToServiceScript* is the path to the updated startup script (see the location information in this section for the paths and names).

Example (replace 4f753e1d-d0de-4aef-bb22-caace7342e99 with the correct tenant ID):
install_path`/message_broker/bin/service/linux_x86_64/dirx-audit-messagebroker install`

install_path`/server_container/tenants/4f753e1d-d0de-4aef-bb22-caace7342e99/bin/dirx-audit-server-container install`

Once the service is successfully installed, you can start and stop the service or get its status via the
systemctl command (adjust the service name if you modified the default value in the script file, replace 4f753e1d-d0de-4aef-bb22-caace7342e99 with the correct tenant ID):

```
systemctl start dirx-audit-messagebroker.service

systemctl stop dirx-audit-messagebroker.service

systemctl status dirx-audit-messagebroker.service

systemctl start dirx-audit-server-4f753e1d-d0de-4aef-bb22-
caace7342e99.service

systemctl stop dirx-audit-server-4f753e1d-d0de-4aef-bb22-
caace7342e99.service

systemctl status dirx-audit-server-4f753e1d-d0de-4aef-bb22-
caace7342e99.service
```

To unregister the service from the system, run the **init** script with the **remove** command:
pathToServiceScript **remove**

Important: If you installed the services manually, you must manually stop and unregister the services before you start the uninstallation procedure.

6. Installing the DirX Identity JMS-Audit Handler Plug-in

The DirX Identity JMS-Audit Handler plug-in is delivered with the DirX Identity installation, but must be deployed separately. It enables DirX Identity to use the DirX Audit JMS collector to track DirX Identity audit events. See the *DirX Identity Installation Guide* (version 8.7 and higher) for instructions how to deploy and configure it.

Note that the DirX Identity JMS-Audit Handler plug-in depends on the DirX Identity version and may be different from version to version. Therefore, be sure to take the plug-in from the corresponding DirX Identity installation media.

Note that when you upgrade from an older version to DirX Audit V7, you need to adapt the queue name and user name for the JMS-Audit Handler plug-in. As of DirX Audit V7, these values are tenant-specific and contain the tenant ID. Take the corresponding values from the respective fields in the DirX Audit Configuration Wizard.

7. Installing the DirX Access JMS-Audit Handler Plug-in

The DirX Access JMS-Audit Handler plug-in allows DirX Access to use the DirX Audit JMS collector to track DirX Access audit events.

To set up this plug-in:

- Download the appropriate version of the plug-in from the IAM Support Portal https://iam-support.it-solutions.atos.net/ and unzip it.
- Install the DirX Access JMS-Audit Handler plug-in into DirX Access: Open the *readme.txt* contained in the .zip file and follow the installation instructions.
- Configure the DirX Access JMS-Audit Handler plug-in.

8. Configuring DirX Audit 9.0 installation & environment for the first time

This is a list of things to check for the newly delivered component DirX Audit Manager (REST / Angular) to be accessible

- Allow the REST API port (30501 by default) in the firewall settings. Each tenant has its separate port.
- Add the *hostname:port* where the Apache Tomcat service is running into the **allowOrigins** field in the REST configuration in DirX Audit Tenant Configuration Wizard, for example **https://***<hostname.domainname>:8443*. Make sure not to leave out the https:// URL protocol prefix!
- Add the DirX Audit Server hostname in the **hosts** file in case the hostname is not known to Windows, *C:\Windows\System32\drivers\etc\hosts*, for example 127.0.0.1 dxt-hostname.test.com.
- Both the Apache Tomcat service and the DirX Audit Server service for the respective tenant must be running to be able to access the DirX Audit Manager.
- Both the Apache Tomcat service and the DirX Audit Server REST service for the respective tenant must have **the same SSL settings** so that users can access the DirX Audit Manager. When the SSL is enabled for the REST service the user has to access the Apache Tomcat service hosting DirX Audit Manager via https, when the REST service does not use SSL the DirX Audit Manager can be only accessed via http.
- It might be necessary to access the REST service URI in your browser, for example **https://***<hostname.domainname>:<port>/Tenants/<tenantId>*/api/audit/common/Me and confirm a security exception or add the server certificate authority (CA) as trusted in your browser certificate list. The REST API port is by default 30501.
- Edit the *install_path***web\audit-manager-***<*tenantId*>**plugins\dirx-dxt-app-manager\assets\config\app-config.json** and check that the key **basePath** includes a hostname in the REST service URI and not an IP address.
- Disable (set to false) both cross-site request forgery (CSRF) settings in case of problems with getting the search results: *install_path* **\server_container\tenants***<*tenantId*>**\conf\application.properties**, for example **authn.csrf.enable=false** and **springdoc.swagger-ui.csrf.enabled=false**.

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.