EVIDEN

Identity and Access Management

DirX Identity

Release Notes

Version 8.10.10, Edition June 2025

Table of Contents

Release Notes

1. General

This Readme file contains information about changes and enhancements of DirX Identity 8.10.10 (build 1514) in addition to the standard documentation set.

This release of DirX Identity is a cumulative patch based on DirX Identity 8.10 SP2. It provides installation packages for Windows and Linux that contain a license as txt file, the ReleaseNotes, the HistoryOfChanges, in addition to the whole user manuals and use case documents of this release in PDF format.

For any other documentation or files, please have a look at the released DirX Identity 8.10 SP2 iso-image, which can be downloaded from the DirX support portal (https://support.dirx.solutions/).

The zip-archive (DirX_Identity_8.10.10-Windows.zip) contains the Windows installation package available in the sub folder 'Windows-Installer'.

The zip-archive (DirX_Identity_8.10.10-Linux.zip) contains the Linux installation package available in the sub folder 'linux-installer'.

The cumulative patch can be installed without having any DirX Identity installed beforehand but can also be installed as patch for any previous installed DirX Identity V8.9 or V8.10 instances including the SP variants.

For a simple installation (initial or patch) on Windows, just start the dirxidty.exe in a graphical environment.

For a simple installation (initial or patch) on Linux, start "chmod 700 dirxidty.bin; .\dirxidty.bin -i GUI" in a graphical environment.

For a more detailed information about installation, please refer to the DirX Identity Installation Guide.

The installation of DirX Identity 8.10.10 requires a Java Runtime Environment 11.

1.1. Licenses

The End User License Agreement must be accepted to use the DirX Identity software products. Please refer to the file license.txt on Windows systems or read the file license agreement with page resp. more on Linux systems.

1.2. DirX Identity Highlights

1.2.1. General Features

DirX Identity provides a comprehensive, process-driven, customizable, cloud-ready, scalable, and highly available identity management solution for enterprises and organizations. It delivers risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Features include life-cycle management for users

and roles, cross-platform and rule-based provisioning in real-time, Web-based user self-service and delegated administration, request workflows, access certification, password management, metadirectory and auditing and reporting.

DirX Identity is available with two options for the base license: Business Suite and Pro Suite. The Pro Upgrade option allows a customer to extend the Business Suite license to a Pro Suite license. The base licenses can be extended by the following add-on license options: Connectivity Packages, Password Management Option and High Availability Option.

The Business Suite comprises these features:

- Powerful applications to create identities from various sources
- DirX Identity Business User Access – various user interfaces
- Self-service capability for group assignments
- Access policies for delegated administration
- Maintenance applications for consistency checking and/or automatic repair of detected problems
- Policy-based automatic provisioning for groups
- Automatic inheritance of groups from business objects
- Real-time and scheduled target system synchronization and validation/reconciliation for accounts and groups
- Event-based change notification to trigger real-time provisioning
- Identity Manager administrator interface
- DirX Identity Servers for Java-based and C/C++-based connectivity to target systems
- Support for monitoring DirX Identity Servers with Nagios
- DirX Identity Framework for Java and C/C++ to build customer specific connectivity to target systems
- DirX Identity Web and REST services to handle most of DirX Identity's functionality
- Status reports for basic auditing (also available through the Web Center)
- A basic connectivity package that comprises file-based, LDAP-based, SPML, and DirX Access connectivity

The Pro Suite includes the Business Suite and the following features:

- Risk management
- Additional privilege structures (roles and permissions) including parameters and hierarchies
- Policy-based provisioning for roles and permissions
- Automatic inheritance of roles and permissions from business objects
- Support for personas, user facets and functional users
- Hierarchical segregation of duty (SoD)

- Additional functionality within the Web Center
- Graphically configurable request workflows for creation, modification and approval of objects and assignments
- Access certification campaigns to verify periodically that roles are assigned to users in compliance
- Re-approval workflows to renew approvals for critical assignments before they expire
- Enhanced access policy functionality
- Comprehensive password management functionality
- Management of passwords for privileged (often called shared) accounts
- Configurable audit trail with optional system and client signature

The DirX Identity Business Access provides different user interfaces for administering the business features of DirX Identity:

- DirX Identity Business User Interface
- DirX Identity Web Center interface available as stand-alone and SAP NetWeaver version
- DirX Identity Web Admin / Server Admin to monitor and control DirX Identity Servers

Connectivity packages are available for:

- Microsoft applications
- Databases
- Cloud systems
- Proxies
- SAP applications
- IBM applications
- HCL applications
- Unify Office or HiPath applications
- Health care applications
- Physical security systems
- Enterprise single sign-on systems

The High Availability Option includes the following features:

- Server Admin as administrative user interface
- Administrative or automatic fail-over of Java-based and C++-based components including:
  - All Java JMS adaptors and thus the associated workflows to another Java-based Identity server
  - The scheduler to another Java-based Identity server

    The classic (Tcl-based) workflows to another C++-based Identity server

    - Automatic failover of ActiveMQ message brokers

The Password Management Option includes the following features:

- Password policies
- Password change by end user via Web Center
- Password change by end user for a subset of their accounts
- Display the password change status
- Challenge/response to reset forgotten passwords (self service)
- Challenge/response to reset forgotten passwords (via admin)
- Administrative password reset
- DirX Password Reset client

1.2.2. New Changes of DirX Identity 8.10.10

1.2.2.1. Bug Fixes

- Fixed issue with ParamAD Connector Bug: Validation Source null: delete groups and accounts. (SDX-1196)
- Fixed issue with Critical Vulnerability - Apache Tomcat - remote code execution vulnerability (CVE-2025-24813). (SDX-1146)
- Fixed issue with security issue with the embedded tomcat of DXI. (SDX-1192)
- Fixed issue with Privileges (Roles/Permissions/Groups) correct deletion behavior via regular Process (Consistency Rule / State DELETED). (SDX-1138)
- Fixed issue Default language setting not saved in BUI. (SDX-1109)
- Fixed issue with duplicated user in TS groups. (SDX-489)
- Fixed issue with REST API Get /Worflows returns wrong objects. (SDX-950)
- Fixed issuw with DirX Identity – RQWF and CANCEL Process. (SDX-933)
- Fixed issuw with scriptContext.getObject().getStorage().getRootID() return rootDN upper and lower Case. (SDX-1134)
- Fixed issuw with DXI – REST API call GET /Workflows/{workflowId}/task returns wrong object/results. (SDX-945)
- Fixed issuw with Re-Approval Workflow not found for Persona. (SDX-899)
- Fixed issuw with RestService behavior for invalid roles. (SDX-513)

1.2.3. Information about Discontinued Features

DirX Identity V8.10 (SP1/SP2) or newer does no longer support these features:

- Deploy ProvisioningServlet in the Embedded Tomcat of a Java server
- Internet Explorer 11 browser support

- DirX Approvals App for Apple® iOS

DirX Identity V8.10 (SP1/SP2) or a cumulative patch to V8.10 SP2 is the last version that supports the following features:

- Support of Microsoft Lync 2013
- Connectivity package for Imprivata OneSign
- Connectivity package for HiPath 4000
- Connectivity package for SiPass
- Connectivity package for ODBC Agent
- Reapproval Workflows (use Certification campaigns)
- Boston Workstation Connectivity (connector)
- XSLT-based Reports

DirX Identity 8.10.6 is the last version that supports the following features:

- Linux Kernel v3 as used in Red Hat 7
- Linux Red Hat Enterprise Linux 7 (x86-64 Intel architecture)

1.2.4. Previous Releases

Previous DirX Identity releases:

DirX Identity 8.10.9.a	(build 1483)	May. 09, 2025	*)
DirX Identity 8.10.9	(build 1474)	Apr. 13, 2025	*)
DirX Identity 8.10.8	(build 1432)	Mar. 25, 2025	*)
DirX Identity 8.10.7	(build 1360)	Feb. 12, 2025	*)
DirX Identity 8.10.6	(build 344932)	Jan. 8, 2025	*)
DirX Identity 8.10.5	(build 344643)	Dec. 2, 2024	*)
DirX Identity 8.10.4	(build 344084)	Nov. 8, 2024	*)
DirX Identity 8.10.3	(build 343905)	Sep. 25, 2024	*)
DirX Identity V8.10 SP2	(build 112)	Jun. 28, 2024	*)
DirX Identity V8.10 SP1	(build 34)	Dec. 16, 2022	*)
DirX Identity V8.10	(build 33)	Feb. 7, 2022	*)
DirX Identity V8.9 SP3		Apr. 13, 2022	*)
DirX Identity V8.9 SP2		Feb. 25, 2021	*)
DirX Identity V8.9 SP1		Jul. 13, 2020	*)

DirX Identity V8.9	(build 22)	Jul. 31, 2019	*)
DirX Identity V8.7 SP4		Nov. 30, 2019	*)
DirX Identity V8.7 SP3		Nov. 30, 2018	*)
DirX Identity V8.7 SP2		Jun. 29, 2018	*)
DirX Identity V8.7 SP1		Apr. 30, 2018	*)
DirX Identity V8.7	(build 15)	Dec. 21, 2017	*)

*) See the history-of-changes.pdf file for a history of changes of these DirX Identity releases.

1.3. Supported Platforms

DirX Identity V8.10 (SP2) or newer is available on the following platforms:

Windows	Microsoft Windows Server 2016 (Long-Term Service Channel - LTSC, x86-64 Intel architecture) Microsoft Windows Server 2019 (x86-64 Intel architecture; with Desktop Experience) Microsoft Windows Server 2022 (x86-64 Intel architecture; with Desktop Experience)

The DirX Identity Manager client runs also on Microsoft Windows 10 / Windows 11.

You can install DirX Identity completely on Microsoft Windows 10 or 11 for non-productive use (demos or POCs). Do not use this configuration for productive use.

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

Additional remarks for using Linux platforms:

32-bit libraries are not installed by default on Red Hat Enterprise Linux.

To run DirX Identity successfully for Red Hat Enterprise Linux, you need to install at least the following 32- and 64-bit library packages:

- yum install ksh
- yum install xinetd
- yum install glibc.i686
- yum install libXext.i686

- yum install libXtst.i686
- yum install libuuid.i686
- yum install libgcc.i686
- yum install libnsl.i686
- yum install cyrus-sasl-lib.i686
- yum install libstdc++.i686
- yum install zlib.i686
- yum install libXrender.i686
- yum install chkconfig (only for Red Hat 9)
- yum install initscripts (only for Red Hat 9)

Don’t forget to add the 32-bit library path /lib to your LD_LIBRARY_PATH environment variable.

Soft links

Additionally, for Red Hat you need libsasl2.so.2 which is missing. To overcome this issue for DirX Identity, just create a soft link

- /lib/libsasl2.so.2 which points to /lib/libsasl2.so.3 and a soft link
- /usr/lib64/libsasl2.so.2 which points to /usr/lib64/libsasl2.so.3

if not already done.

Additionally, for Red Hat 9, a link to libcrypt.so.1 from libcrypt.so.2:

cd /lib

ln -s libcrypt.so.2 libcrypt.so.1

For SUSE Linux, above mentioned library packages might need installing - especially if your operating system installation is not a default installation. The list of required 32- and 64-bit library is like Red Hat for SUSE Linux, except for package names which might be slightly different and for the installation utility to be used (yast instead of yum). This is the related search pattern list for verifying their presence when using the related graphical interface (yast -> Software Manager):

- ksh
- xinetd
- glibc
- libXext
- libuuid
- libgcc
- libnsl

- cyrus-sasl
- libstdc++
- zlib.i686
- libXrender
- libcrypt1-32bit
- insserv-compat

Additionally, for SUSE Linux you need libsasl2.so.2 which is missing. To overcome this issue for DirX Identity, just create a soft link

- /lib/libsasl2.so.2 which points to /lib/libsasl2.so.3 and a soft link
- /usr/lib64/libsasl2.so.2 which points to /usr/lib64/libsasl2.so.3

if not already done.

Support of virtual machines:

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

Support of hardware cluster configurations is available on request.

1.4. Java Requirements for DirX Identity

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

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

- The product must be an implementation of the Java Platform, Standard Edition (Java SE).
- The related version number must be 11.0.xx.
- It must be a 64-bit distribution.
- The distribution must be TCK tested (Technology Compatibility Kit for Java)

Tested and considered working Java distributions are:

- Oracle Java SE 11 (LTS)
- Adoptium Eclipse Temurin JDK-11

For details regarding said installation options, see the chapter "Installation" and "The Java for DirX Identity" in the DirX Identity Installation Guide.

1.5. Supported Apache Tomcat Installations

DirX Identity Web Center / Web Center for Password Management / Business User Interface / REST service / Provisioning web service support these Apache Tomcat versions (running with a Java SE 11):

- Tomcat 9

Use an installed Java SE 11 version with the latest security patches installed. It is customer's responsibility to download and install any Java SE security patches in time.

Please consider also additional steps to secure Tomcat beyond the default installation. As the Tomcat installation comes with a default username / password for the Tomcat administrator we strongly recommend to consider additional measures to secure the Web container Tomcat by following the guidelines in https://tomcat.apache.org/tomcat-9.0-doc/security-howto.html.

1.6. Supported Directories

Product	Version
DirX Directory	V8.9 or higher

Patch level 9.4.454 or higher is preferred because of support of new LDAP controls that increase the performance of the LDAP lock feature.

Please note that all components of DirX Identity must work with the master directory server of DirX Directory or with a synchronous DirX Directory shadow server. It cannot work with asynchronous shadow servers due to the delay that occurs after a write operation on the shadow until the information is provided via chaining from the master again. Using asynchronous shadow servers is only allowed for pure read applications. For best performance, the master directory server should be used.

1.7. Supported JMS Messaging Servers

DirX Identity supports the following JMS messaging server:

- Apache ActiveMQ message broker (included in the installation)

1.8. Delivery Packages

This section provides information about DirX Identity V8.10 (SP2) or newer delivery packages on the supported platforms.

1.8.1. Windows Platforms

For Windows platforms a single installation package is provided that allows to install the following DirX Identity components:

- Connectivity - LDAP Schema and Configuration Data
- Provisioning - LDAP Schema and Configuration Data
- ActiveMQ Message Broker
- Identity Server (C++-based)
- Identity Server (Java-based)
- Server Admin (including Supervisor-J)
- Manager
- Web Center
- Web Center for SAP NetWeaver
- Web Center for Password Management
- Business User Interface
- Provisioning Web service
- REST service

It also includes these connectivity packages:

- Default: LDAP, Files, SPML
- Microsoft: ADS (including Exchange), SharePoint, Lync
- Database: JDBC, ODBC
- SAP: SAP ERP HR UniCode (former SAP R/3), SAP ECC UM (former SAP R/3), SAP NetWeaver (former EP) UM
- IBM: RACF
- HCL: Notes
- HiPath: HiPath 4000 Manager
- HealthCare: Medico//s
- Physical Security Systems: SiPass
- ESSO: Evidian ESSO, Imprivata OneSign
- Cloud Systems: Google Apps, Citrix ShareFile, Microsoft Office 365, Salesforce
- Proxy: Remote Upload Connector, OpenICF Proxy Connector

The Business package can be upgraded with a special license (Pro Suite Upgrade) to obtain additional powerful functionality.

For a detailed description of the installation prerequisite and procedure see the DirX Identity Installation Guide.

1.8.2. Linux Platforms

For Linux platforms a single installation package is provided that allows to install all DirX Identity components as for Windows but without the connectivity packages for:

- Microsoft: ADS (agent only, connector is running)
- HCL: Notes
- Physical Security Systems: SiPass

1.8.3. Distribution Media

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

The cumulative patch 8.10.10 is delivered in two zip-archives:

- The zip-archive (DirX_Identity_8.10.10-Windows.zip) contains the Windows installation package available in the sub folder 'Windows-Installer'.
- The zip-archive (DirX_Identity_8.10.10-Linux.zip) contains the Linux installation package available in the sub folder 'linux-installer'.

They can be downloaded from the DirX support portal (https://support.dirx.solutions/).

In addition to the distribution medium, you must purchase separate product licenses to use the software packages.

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

1.8.4. Resources

Each DVD or zip-archive ships with modified sources of the:

- Mozilla LDAP Java SDK 4.18 (see also: https://www.mozilla.org). You can find them - along with a brief documentation of the modifications - in the folder Resources of the DVD.
- Genivia gSOAP C++ SOAP Server (see also: https://www.genivia.com/dev.html). You can find them - along with a brief documentation of the modifications - in the folder Resources of the DVD.

1.9. User Documentation

1.9.1. DirX Identity User Manuals

The following manuals are available in PDF format of Adobe:

- DirX Identity V8.10 Introduction (introduction.pdf)
- DirX Identity V8.10 Tutorial (tutorial.pdf)
- DirX Identity V8.10 Provisioning Administration Guide (prov-admin-guide.pdf)
- DirX Identity V8.10 Connectivity Administration Guide (conn-admin-guide.pdf)
- DirX Identity V8.10 User Interface Guide (bui-user-guide.pdf)
- DirX Identity V8.10 Application Development Guide (appl-dev-guide.pdf)

- DirX Identity V8.10 Customization Guide (custom-guide.pdf)
- DirX Identity V8.10 Integration Framework Guide (integration-framework.pdf)
- DirX Identity V8.10 Connectivity Meta Controller Reference (metacp-ref.pdf)
- DirX Identity V8.10 Connectivity Reference (conn-ref.pdf)
- DirX Identity V8.10 Web Center Reference (web-center-ref.pdf)
- DirX Identity V8.10 Web Center Customization Guide (web-center-custom-guide.pdf)
- DirX Identity V8.10 Troubleshooting Guide (troubleshooting-guide.pdf)
- DirX Identity V8.10 Installation Guide (install-guide.pdf)
- DirX Identity V8.10 Migration Guide (migration-guide.pdf)

The DVD may optionally contain the migration guides of previous DirX Identity versions.

Additionally, a set of Use Case documents is available:

- Creating a Custom Target System Type (creating-custom-targetSystemType.pdf)
- Java Programming in DirX Identity (java-programming)
- Service Management (service-management.pdf)
- Using Domains (using-domains.pdf)
- Using Segregation of Duties (using-segregation-of-duties.pdf)
- Password Management (password-management.pdf)
- High Availability (high-availability.pdf)
- Realtime Synchronization within an Identity Domain (realtime-synchronization.pdf)
- Enabling Smart Card Login for Identity Manager (smart-card-login-manager.pdf)
- Monitoring DirX Identity Servers with Nagios (nagios-support.pdf)
- User specific Proposal Lists for Role Parameters (user-specific-proposals-for-roleParameters.pdf)
- Certification Campaigns (certification-campaign.pdf)
- Configuring the Maintenance Workflows for User Facets (userFacet-maintenance.pdf)
- Web Center File Upload (webCenter-file-upload.pdf)
- Atos Password Reset Client Installation Guide (password-reset-client-installation.pdf)
- Atos Password Reset Client User Interface Guide (password-reset-client-gui.pdf)
- Business User Interface User Guide (bui-user-guide.pdf)
- Business User Interface Configuration Guide (bui-config-guide.pdf)
- Jaspersoft Reports (jaspersoft-reports.pdf)

You need Adobe Acrobat Reader to view PDF files. For a free copy of Adobe Acrobat Reader please refer to

https://www.adobe.com/products/reader.html

or to

https://www.adobe.com

The documentation set also provides a full-text index. The subfolder with the suffix "_IDX" contains the full-text index data files for the manuals. The file with the suffix ".PDX" contains the index description.

If you open a manual the associated index is attached automatically. All word options (Case sensitive, Sounds Like, and Word Stemming) were enabled when the index was built. There are no numbers or stopwords excluded from the index.

Browsers may not provide Adobe Acrobat Search. To use this feature just open one of the manual files, e.g. Documentation\DirXIdentity\introduction.pdf with Adobe Acrobat Reader.

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

The setup also provides each document.

1.9.2. DirX Identity Online Help

All manuals except the guides for Installation, Migration and Web Center as well as the Use Case documents are also available in the DirX Identity Manager online help.

This cumulative patch does not provide any new or updated online help.

The latest help files are available from the DVD. The installer copies these files automatically to the relevant folders in the installation directory. It copies:

- all files from “DVD:\Documentation\DirXIdentity\Help“ to <*install_path*>\GUI\modules\help (only if such a folder exists on DVD)
- all files from “DVD:\Documentation\DirXIdentity\Help_configurator” to <*install_path*>\configurator\help (only if such a folder exists on DVD)

If you copy the installer from your DVD to another location, perform this copy procedure manually.

1.9.3. DirX Support Notes

Please refer to the DirX Identity Support Notes in the IAM Support Portal for more information about important warnings, known problems and their solutions.

1.9.4. Third Party Documentation

The subfolder tcl_V83_part contains the license agreement (license_terms.txt) and the reference pages of the Tcl V8.3 commands (in html format). Part of this information is also

contained in the DirX Identity Manager online help.

1.10. Hardware Requirements

This section provides information about hardware requirements.

1.10.1. RAM

On 64-bit platforms at least 8 GB RAM is recommended. RAM size should be increased to at least 16 GB for managing more than 10,000 users.

1.10.2. Disk Space

At least 14 GB of free disk space is recommended for DirX Identity. This value does not include Apache Tomcat and DirX Directory but includes Apache ActiveMQ. Note that Apache ActiveMQ message broker is pre-configured to use a persistent store of maximum 10 GB.

1.11. Software Requirements

DirX Identity V8.10 (SP2) or newer requires:

- An installation of one of the supported directory servers (see section above).
- One of the supported operating systems (see section above).
- A supported Apache Tomcat installation (see section above).

The DirX Identity Web Center supports these types of browsers:

- Mozilla Firefox 78 or newer
- Google Chrome 96 or newer (Request signing via Java applet is not supported)
- Microsoft Edge 96 or newer (Request signing via Java applet is not supported)

The DirX Identity Web Center for Password Management supports these types of browsers:

- Mozilla Firefox 78 or newer
- Google Chrome 96 or newer
- Microsoft Edge 96 or newer

The DirX Identity Server Admin / Web Admin support these types of browsers:

- Mozilla Firefox 78 or newer
- Google Chrome 96 or newer
- Microsoft Edge 96 or newer

The Business User Interface application supports these types of browsers:

- Mozilla Firefox 78 or newer

- Google Chrome 96 or newer
- Microsoft Edge 96 or newer

Make sure that the browsers allow the application to store information into its local session storage.

Included 3rd party software:

- Apache ActiveMQ 5.18.4 message broker (included in the installation)
  If you consider upgrading the message broker, please contact the DirX support unit.
- Apache Embedded Tomcat 9.0.88 (included in the installation)
  If you consider upgrading the embedded Tomcat, please contact the DirX support unit.
- On Windows: Microsoft Visual C++ Redistributables for x86 and x64 (Visual Studio versions 2008 and 2017). If newer redistributables are installed, then the installer does not install an older version (included in the installation)
- Tanuki Java Service Wrapper Standard Edition 3.5.51 for starting Apache ActiveMQ as a service (included in the installation)

The HCL Notes Agent requires an installation of Notes Client 8.5 or higher. Ideally, the version number of the Notes Client should be equal to or greater than the version number of the Notes / Domino server.

The ODBC Agent requires an installation of an ODBC driver. Note: ODBC drivers are not part of the DirX Identity delivery.

The JDBC Agent/Connector requires an installation of a JDBC driver. Note: JDBC drivers are not part of the DirX Identity delivery – see the related Workflow description for more information.

The SAP ECC UM Agent/Connector supports ECC 6.0, SAP S/4HANA (1709 FPS1 or higher) on-premise and higher and runs with all NetWeaver (ABAP stack) platforms that are supported by the SAP Java Connector and by DirX Identity. For more details see the Connectivity Reference Guide, Chapter 3.10.

The SAP ECC UM Agent requires an installation of SAP JCo (Java Connector) Version 3.1.7 or higher. The 64 bit JCo is required.

For the DirX Identity backup functionality, gzip is required on all platforms.

For Linux, gzip is a part of the operating system and must have been installed. The minimum version required is gzip 1.3.5. The installed gzip version is displayed by the command gzip –V.

For Windows the gzip program must be downloaded. The minimum version required is gzip 1.3.12.

A suitable gzip program is available from https://www.gnu.org, for example. The gzip program “gzip.exe“ must be found via the PATH environment variable.

1.12. Changed Configuration Files

The following configuration files have changed. The base for this list is 8.10. Any changes that were done before an upgrade or update installation are overwritten:

- The configuration files idmsvc.ini/runServer.bat/sh for a Java-based server were changed.
- The configuration file dxmmsssvr.ini for a C++-based server was changed.
- Configuration files for Apache ActiveMQ were changed (activemq.xml, wrapper.conf).
- Configuration files for Apache Log4j were changed from version 1.x to 2.x.
- Changes for Web Center or Web Center for Password Management see the extra text files.
- Changes for SPML Provisioning Web Services see the extra text files.
- Changes for the Rest Services see the extra text files.

1.12.1. Changed Third-Party Files

The base for changed third-party files is 8.10. The following jar and libraries files have changed:

- log4j-1.2.8.jar to log4j-api-2.17.1.jar, log4j-core-2.17.1.jar, log4j-1.2-api-2.17.1.jar
- bcmail-jdk14-136.jar to bcmail-jdk15on-164.jar
- bcprov-jdk14-136.jar to bcprov-jdk15on-164.jar
- itext-2.1.7.js2.jar to itext-2.1.7.jar
- ecj-4.15.jar to ecj-4.20.jar
- jasperreports.jar – from version 6.6.0 to 6.17.0
- jasperreports-fonts.jar – from version 6.7.0 to 6.17.0
- commons-pool.jar – from version 1.5 to 1.6
- activemq-broker.jar, activemq-client.jar, activemq-openwire-legacy.jar, slf4j-api.jar (to 2.0.6), deleted log4j-slf4j-impl-2.17.1.jar – Apache Active MQ upgrade to version 5.18.4
- tomcat-embed-core.jar, tomcat-embed-el.jar, tomcat-embed-jasper.jar, tomcat-embed-websocket.jar, catalina-tribes.jar – Apache Embed Tomcat upgrade to 9.0.88
- New jar files: bcpkix-jdk15on-164.jar, tika-core-2.1.0.jar
- Jackson jar files upgraded to version 2.13.4:
  jackson-core.jar – in some places from version 2.13.3 to 2.13.5, jackson-annotations-2.9.4.jar to jackson-annotations-2.13.5.jar, jackson-core-2.9.4.jar to jackson-core-2.13.5.jar, jackson-databind-2.9.4.jar to jackson-databind-2.13.5.jar, jackson-jaxrs-base-2.9.4.jar to jackson-jaxrs-base-2.13.5.jar, jackson-jaxrs-json-provider-2.9.4.jar to jackson-jaxrs-json-provider-2.13.5.jar,
  deleted jackson-annotations.jar
- Spring jar files upgraded to version 5:
  spring-aop.jar version 4.0.6 to spring-aop-5.3.23.jar, spring-beans.jar version 4.0.6 to

spring-beans-5.3.23.jar, spring-context.jar version 4.0.6 to spring-context-5.3.23.jar, spring-core.jar version 4.0.6 to spring-core-5.3.23.jar, spring-expression.jar version 4.0.6 to spring-expression-5.3.23.jar, spring-tx.jar version 4.0.6 to spring-tx-5.3.23.jar, spring-web.jar version 4.0.6 to spring-web-5.3.23.jar, spring-ldap-core.jar version 1.3.2 to spring-ldap-core.2.3.8.jar, spring-security-config.jar version 3.2.0 to spring-security-config-5.7.4.jar, spring-security-core.jar version 3.2.0 to spring-security-core-5.7.4.jar, spring-security-ldap.jar version 3.2.0 to spring-security-ldap-5.7.4.jar, spring-security-web.jar version 3.2.0 to spring-security-web-5.7.4.jar, new spring-security-crypto-5.7.4.jar

- OpenSSL libraries updated to version 3.1.0: dirxssleay32.dll, dirxlibeay32.dll to libssl-dirx-3.dll, libcrypto-dirx-3.dll; libdirxssl.so, libdirxcrypto.so to libssl-dirx.so.3, libcrypto-dirx.so.3

1.13. Restrictions

1.13.1. Ipv6 Address Support

There is full Ipv6 address support for all Java-based DirX Identity components.
The following components are not supporting Ipv6:

- C++-based Server
- Windows Password Listener
- APRC
- Meta Controller
- HCL Notes Agent / Connector
- ADS / Exchange Agent
- SiPass Agent

2. Compatibility

Compatibility of DirX Identity V8.10 with previous DirX Identity releases is detailed in the matrix below:

DirX Identity	metacp		Agents / Connectors						
Version	Scr	ACF	DF	NO	NT	ODBC	SAPhr	SAPum	ADS	HDMS
8.3	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
8.3 R2	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
8.4	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
8.5	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
8.6	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
8.7	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
8.9	no	yes	yes	yes	no	yes	yes	yes	yes	yes
8.10	no	yes	yes	yes	no	yes	yes	yes	yes	yes

DirX Identity	Agents / Connectors							
Version	SAPnw	JDBC	Dashb	SiPass	UNIX	Medico	ShareP.	Impriv.
8.3	yes	yes	yes	yes	yes	yes	yes	yes
8.3 R2	yes	yes	yes	yes	yes	yes	yes	yes
8.4	yes	yes	yes	yes	yes	yes	yes	yes
8.5	yes	yes	yes	yes	yes	yes	yes	yes
8.6	yes	yes	yes	yes	yes	yes	yes	yes
8.7	yes	yes	yes	yes	yes	yes	yes	yes
8.9	yes	yes	no	yes	yes	yes	yes	yes
8.10	yes	yes	no	yes	yes	yes	yes	yes

DirX Identity	Connectors (cont.)					
Version	GoogleApps	OpenICFUnix	OpenICFWin	Office365	Salesforce	UnifyOffice
8.3	yes	n/a	n/a	n/a	n/a	n/a
8.3 R2	yes	yes	yes	n/a	n/a	n/a
8.4	yes	yes	yes	yes	yes	n/a
8.5	yes	yes	yes	yes	yes	n/a
8.6	yes	yes	yes	yes	yes	n/a
8.7	yes	yes	yes	yes	yes	n/a

DirX Identity		Connectors (cont.)				
8.9	yes	yes	yes	yes	yes	n/a
8.10	yes	yes	yes	yes	yes	yes

Legend:

Scr	scripts
ACF	attribute configuration files
DF	data files
no	not compatible
yes	compatible
n/a	not applicable

3. Installation

The installable components, installation and migration configurations and procedures are described in the DirX Identity Installation Guide and in the DirX Identity Migration Guide.

Note that with an update or upgrade installation the folder <*install_path*>\security will be deleted because the files are of no use anymore. Do not forget to make an installation folder backup.

3.1. Installation Procedure on Windows Platforms

The base directory for installation is under administrator control on Windows platforms. The administrator can choose a pathname (the Windows system variable *ProgramFiles* contains the fully qualified name of the directory defined by Windows to store applications).

The default pathname on Windows platforms is:

%ProgramFiles%\DirX\Identity

Note that the default pathname has changed starting with 8.10 SP2.

3.1.1. Initial Installation

Read the Installation Guide and perform the necessary steps for your preferred configuration (see the "Installations Configurations" chapter for the supported installation configurations).

3.1.2. Prerequisites for Update or Upgrade Installation

These steps are necessary to prepare an update or upgrade installation:

- Backup all DirX Identity databases to be able to reset to the starting point if something goes wrong.
- Backup the installation folder.
- Check the section "Preserving Files" in the chapter "Preparing the Migration" of the *DirX Identity Migration Guide* for files to be preserved and create additional backup copies of these files.

3.1.3. Update Installation

You can perform an Update Installation at any time. Please note that the default applications are overwritten during an update installation. Be sure to not use modified default applications in productive environments.

Read the Installation Guide and perform the necessary steps for your preferred configuration (see the description of this use case in the section "General Information" of the chapter "Introduction").

3.1.4. Update Installation from 8.10, 8.10 SP1 or 8.10 SP2 to a Cumulative Patch

In contrast to former delivered service packages for older versions now for 8.10 full installer packages are delivered for service patches or cumulative patches.

Run the Identity Installation of a cumulative patch and then perform a DirX Identity Initial Configuration including **all steps** for components that you have installed. Note that you must select “Connectivity Schema and Data Configuration” and “Provisioning Schema and Data Configuration” on systems where the DirX Directory server is installed. Also note that you must update the tools Workflow Starter, Report Tool, or Eventing Tool if you used them before.

3.1.5. Upgrade Installation

Upgrade installation from previous versions of DirX Identity to a cumulative patch is supported for DirX Identity V8.7 and V8.9 including the latest service packages.

Run the Identity Installation of a cumulative patch and then perform a DirX Identity Initial Configuration including all steps for components that you have installed. Note that you must select “Connectivity Schema and Data Configuration” and “Provisioning Schema and Data Configuration” on systems where the DirX Directory server is installed. Also note that you must update the tools Workflow Starter, Report Tool, or Eventing Tool if you used them before.

A detailed description for this migration can be found in Documentation\DirXIdentity\identmigration.pdf. Read the instructions carefully and perform all steps in the recommended sequence.

Read the Installation Guide and perform the necessary steps for your preferred configuration (see the description of this use case in the section "General Information" of the chapter "Introduction").

3.2. Installation Procedure on Linux Platforms

The default pathname on Linux is:

<userID_home_directory>/DirX/Identity

3.2.1. Prerequisites

When installing your Linux operating system, you must consider that the default installation might not cover the system requirements for DirX Identity. Selection of all available Linux operating system packages will cover the system requirements for DirX Identity.

Due to general issues on how Linux GUIs using Wayland (for example, GNOME) display Java Swing applications, we recommend using a Xorg-based user interface (for example, GNOME Classic) to install and configure DirX Identity and to run DirX Identity Manager.

3.2.2. Initial Installation

a. Extract the tar.gz-archive. The installation package is available in the sub-folder **linux-installer**.

b. Read the Installation Guide and perform the described steps carefully.

c. Customize the file “dxi.cfg” as described in the help / documentation.

3.2.3. Prerequisites for Update or Upgrade Installation

These steps are necessary to prepare an update or upgrade installation:

- Backup all DirX Identity databases to be able to reset to the starting point if something goes wrong.
- Backup the installation folder.
- Check the section "Preserving Files" in the chapter "Preparing the Migration" of the *DirX Identity Migration Guide* for files to be preserved and create additional backup copies of these files.

3.2.4. Update Installation

You can perform an Update Installation at any time. See the description of this use case in the section "General Information" of the chapter "Introduction" in the installation Guide.

a. Extract the tar.gz-archive. The installation package is available in the sub-folder **linux-installer**.

b. Read the Installation Guide and perform the described steps carefully.

c. Customize the file “dxi.cfg” for the Identity Manager as described in the help / documentation.

3.2.5. Update Installation from 8.10, 8.10 SP1 or 8.10 SP2 to a Cumulative Patch

In contrast to former delivered service packages for older versions now for 8.10 full installer packages are delivered.

Run the Identity Installation of a cumulative patch and then perform a DirX Identity Initial Configuration including **all steps** for components that you have installed. Note that you must select “Connectivity Schema and Data Configuration” and “Provisioning Schema and Data Configuration” on systems where the DirX Directory server is installed. Also note that you must update the tools Workflow Starter, Report Tool, or Eventing Tool if you used them before.

3.2.6. Upgrade Installation

Upgrade installation from previous versions of DirX Identity a cumulative patch is supported for DirX Identity V8.7 and V8.9 including the latest service packages.

Run the Identity Installation of a cumulative patch and then perform a DirX Identity Initial

Configuration including all steps for components that you have installed. Note that you must select “Connectivity Schema and Data Configuration” and “Provisioning Schema and Data Configuration” on systems where the DirX Directory server is installed. Also note that you must update the tools Workflow Starter, Report Tool, or Eventing Tool if you used them before.

See the description of this use case in the section "General Information" of the chapter "Introduction" in the Installation Guide.

A detailed description for this migration can be found in Documentation\DirXIdentity\identmigration.pdf on your DVD. Read the instructions carefully and perform all steps in the recommended sequence.

a. Extract the tar.gz-archive. The installation package is available in the sub-folder **linux-installer**.
b. Read the Migration and Installation Guides and perform the described steps carefully.
c. Customize the file “dxi.cfg” for the Identity Manager as described in the help / documentation.

4. Documentation Extensions

The default pathname on Windows platforms has changed starting with 8.10 SP2. The notation convention *install_path* on Windows systems is **C:\Program Files\DirX\Identity**.

a. Meta Controller Reference, chapter 6.3 Certification Administration – correct link:

   For a complete documentation on the certutil command line tool see on project's page: https://firefox-source-docs.mozilla.org/security/nss/

   Use the option -d dbm:<directory> for the legacy database cert8.db.

b. Use Case document Monitoring DirX Identity Servers with Nagios, chapter 2.3.8:

   To obtain the JMX port for a Java-based Server, examine the following parameter in the INI file dxi_install_path/ids-j-domain-Sn/**bin/idmsvc.ini**:

   16=-Dcom.sun.management.jmxremote.port=40005

   

   The leading number might differ. Do not confuse that with the second parameter
   (-Dcom.sun.management.jmxremote.rmi.port=40006)

c. Use Case document *Enabling Smart Card Login for DirX Identity Manager*, chapter 2.1.4 – the ordering of the tasks must be changed: "Setting up the request workflow service for SASL authentication" is the first task not the last.
   The corrected paragraphs:

2.1.4 Configuring DirX Identity

Configuring DirX Identity for smart card login in the recommended scenario consists of the following tasks:

- Setting up the request workflow service for SASL authentication.
- Creating the personalized DomainAdmin in the Provisioning view.
- Storing the smart card certificate in the personalized DomainAdmin.
- Adding the personalized DomainAdmin to DirXmetahub read and write groups in the Connectivity view.

Set up Request Workflow Service SASL Authentication

To set up request workflow service authentication:

- Navigate to the **utils/ssl** subdirectory in the directory of the Java-based Server that runs the request workflows; for example, *dxi_install_path**/ids-j-My-Company-S1/utils/ssl*.
- Edit the following **genManager.bat** (or **.sh**) script parameters to your requirements:

  set dname - specifies the host name; for example, **dxi-w-2012-03**.

set alias - specifies the keystore alias; for example, **dxi-w-2012-03**.

set keystorePassword - specifies the keystore password. The default is **alpha123**.

set truststorePassword - specifies the truststore password. The default is **changeme**.

- Run the **genManager.bat** (or **.sh**) script.
- Copy the generated keystore file to *dxi_install_path***/GUI/bin** on the machine that hosts DirX Identity Manager.
- In *dxi_install_path***/GUI/bin**, edit the **dxi.cfg** property file: uncomment the following lines and then set the keystoreName and keystoreAlias values:

```
#keystoreName=manager-keystore-<alias>
#keystoreAlias=<alias>
```

For example:

```
keystoreName=manager-keystore-dxi-w2012-03
keystoreAlias=dxi-w2012-03
```

d. Migration Guide – the chapter *Aspects Relevant for Upgrade from 8.7* is missing:

Aspects Relevant for Upgrade from V8.7

This section describes all aspects relevant to upgrading to the current version from DirX Identity V8.7.

Not Deleted Jar Files in the Installation

The upgrade installation does not automatically delete the following jar files in specific folders:

- *install_path*/ids-j-*domain*-Sn/confdb/jobs/framework/lib/dxmSvcLayerConnector.jar
- *install_path*/ids-j-*domain*-Sn/confdb/jobs/framework/lib/ruleprocessing.jar

These files in the given folder must be deleted manually for all Java Server installations.

e. Description of the custom field validation for Business User Interface:

To add support for field validation in form (e.g., in “My profile” page), a script must be modified to enable field form validation. This script file is called *validator.js* file available in *extern* folder. This file provides a function *validate*. This function is called for when a field (control) is modified in the form.

To validate a field, following actions must be executed:

- Extract Formly **key** of the control (Formly does not provide direct access to this field and must be extracted from **_fields** attribute).
- Check if acquired **key** is the current target to be validated (e.g., key has value 'mobile'). Available **key** values are set in *json* files from *forms* folder (e.g., my-profile.json)
- Extract and check if field value passes the validation criteria.
- Return **null** is the value is valid, otherwise return an object with the **key** for invalid value. (e.g., { mobile: true }). See file *extern/validator.js* for more implementation details.

Formly is a dynamic form library for Angular and is used by the Business User Interface (see https://formly.dev/).

f. Installation Guide - Changed Configuration Wizard Parameter Name **deletePasswordsAfterSilentConfiguration**

   You can specify that the passwords and PINs in the section shown above should be deleted in the **configuration.ini** file and the *Java-based_server_config_file* (**.tpl**), if used, at the end of the configuration by setting:

   deletePasswordsAfterConfiguration=1

5. Known Restrictions

5.1. Client Signature with Java Applets

The solution is not supported anymore.

Java deployment technologies were deprecated in Java 9 and removed in Java SE 11. Java applet and Web Start functionality, including the Java plug-in, the Java Applet Viewer, Java Control Panel, and Java Web Start, along with javaws tool, have been removed in Java SE 11.

6. Known Issues

6.1. Zipping More Than 100 C++-based Server LOG Files With Dirx Diag Tool

If you have more than 100 LOG* files in the server\log folder and call dirxdiag_cserver.bat/sh to collect diagnosis files into a zip file the tool will hang.

In this case, delete or archive older files and rerun the command.

6.2. Missing MS Access Bridge Support with Oracle JRE

Starting with Oracle JRE 8, there is no JDBC ODBC Bridge for MS Access support any longer.

Use another driver instead. An example is the UCanAccess driver. Find a sample configuration in the Connectivity View: Connected Directories – Default - Source Scheduled - HR-JDBC CD.

6.3. Migrating of ActiveMQ messaging server

In some cases, the migration of the repository (file-based database kahadb) from a former ActiveMQ version to the version that comes with DirX Identity 8.9/8.10 does not work.

For that reason, we recommend strongly that you should verify that all message queues in ActiveMQ are empty before upgrading (enqueued and dequeued counters are equal in ActiveMQ Web Console). In rare cases, ActiveMQ doesn't start correctly after migration because of kahadb issues (the repository). In that case the only possibility is to delete the kahadb completely.

6.4. Message RPC741 and Rule AssocAccount2User

Message RPC741 is now logged as an informal message from the Policy Execution. If you have a rule that associates accounts to user and the association fails, then this is now not logged as a warning anymore. It is recommended checking out the unassigned accounts with a QueryFolder (in the TS View of the Identity Manager) instead of checking in the monitor area.

6.5. Warning about SOAP MetaFactory

With the introduction of modules, Java 11 for example logs the following warning:

```
“WARNING: Using deprecated META-INF/services mechanism with non-
```

```
standard property: javax.xml.soap.MetaFactory….”.
```

In order to suppress it, you have to set the full classname of a SOAP MetaFactory implementation in a system property when starting the JVM:

```
-Djavax.xml.soap.SAAJMetaFactory=com.sun.xml.messaging.saaj.soap.SAAJ
MetaFactoryImpl
```

For the Java VM used by the Tomcat container hosting Web Center or any other Identity service, you must do that manually. See the Tomcat documentation for configuring the setup under https://tomcat.apache.org/tomcat-9.0-doc/setup.html.

6.6. Warnings in the Java-based Server Log Files at Startup

During startup of the Java server several warnings are written like

```
24.11.2021 16:45:00.468 [Main-S1] [  ] *** WARNING ***
Called from
org.apache.catalina.util.SessionIdGeneratorBase.createSecureRandom()
 Creation of SecureRandom instance for session ID generation using
[SHA1PRNG] took [141] milliseconds.


24.11.2021 16:45:04.455 [Main-S1] [  ] *** WARNING ***
Called from
org.jboss.weld.bootstrap.events.BeforeBeanDiscoveryImpl.addAnnotatedT
ype()
 WELD-000146: BeforeBeanDiscovery.addAnnotatedType(AnnotatedType<?>)
used for {0} is deprecated from CDI 1.1!
----------------------------------------------------------------------
----------
```

The first warning is from Apache Tomcat and is related to a session Id create process. It is a more diagnostic message that can be ignored unless the given millisecond time is very high (more than several seconds).

The other warning comes because the used Rich Faces implementation for the Server Admin does not comply fully with Java 11. These warnings can be ignored.

6.7. Permission Parameters and Attribute Indexes

Starting with DirX Identity V8.9 the algorithm for calculating the matching groups of a permission has changed. Depending on the definition of the role match rules (namely the match expression refers to a “Group” definition with operator “=”) the matching groups are searched via an LDAP search. For better performance the permission parameters should be indexed.

The DirX Identity provides an attribute index for **dxrRPvalues**, but not for all the other attributes defined in the Permission Parameter Tab. The default permission parameters **departmentnumber**, **dxrProject, employeetype**, **l** and **manager** are not indexed whereas the permission parameters **c** and **ou** are indexed.

If you think of using these standard attributes in a productive environment, you should consider creating an attribute index for them. The same also applies if you defined your own attributes as permission parameters.

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.