EVIDEN

Identity and Access Management

DirX Identity

Migration Guide

Version 9.0.0, Edition July 2026

Table of Contents

Preface

The *DirX Identity Migration Guide* is designed to help you to perform the migration from previous versions. It consists of the following sections:

- Introduction discusses the migration process and describes the concepts.
- Migration Procedure describes the general migration procedure.
- Preparing the Migration describes what must be done before you start migration.
- Automatic Migration during Installation and Configuration describes the automatic part of the migration process.
- Manual Migration describes how to perform additional manual migration tasks that are required to complete the migration.
- Known Issues describes how to solve known post-migration issues.

Perfect migration is difficult to achieve because the variety of configuration databases at the customer site is infinite. Thus, you should carefully follow the sequence of steps described in this guide to achieve successful migration. Test all of your workflows and applications after migration to ensure that everything works properly.

DirX Identity Documentation Set

Version: 9.0.0 | Build: 29615 | Date: 2026-07-14

The DirX Identity document set consists of the following manuals:

- *DirX Identity Introduction*. Use this book to obtain a description of DirX Identity architecture and components.
- *DirX Identity Release Notes*. Use this book to understand the features and limitations of the current release. This document is shipped with the DirX Identity installation as the file **release-notes.pdf**.
- *DirX Identity History of Changes*. Use this book to understand the features of previous releases. This document is shipped with the DirX Identity installation as the file **history-of-changes.pdf**.
- *DirX Identity Tutorial*. Use this book to get familiar quickly with your DirX Identity installation.
- *DirX Identity Provisioning Administration Guide*. Use this book to obtain a description of DirX Identity provisioning architecture and components and to understand the basic tasks of DirX Identity provisioning administration using DirX Identity Manager.
- *DirX Identity Connectivity Administration Guide*. Use this book to obtain a description of DirX Identity connectivity architecture and components and to understand the basic tasks of DirX Identity connectivity administration using DirX Identity Manager.
- *DirX Identity User Interfaces Guide*. Use this book to obtain a description of the user interfaces provided with DirX Identity.
- *DirX Identity Application Development Guide*. Use this book to obtain information how to extend DirX Identity and to use the default applications.
- *DirX Identity Customization Guide*. Use this book to customize your DirX Identity environment.
- *DirX Identity Integration Framework*. Use this book to understand the DirX Identity framework and to obtain a description how to extend DirX Identity.
- *DirX Identity Web Center Reference*. Use this book to obtain reference information about the DirX Identity Web Center.
- *DirX Identity Web Center Customization Guide*. Use this book to obtain information how to customize the DirX Identity Web Center.
- *DirX Identity Resolution Service Setup Guide*. Use this book to set up the DirX Identity Resolution Service as a standalone service.
- *DirX Identity Meta Controller Reference*. Use this book to obtain reference information about the DirX Identity meta controller and its associated command-line programs and files.
- *DirX Identity Connectivity Reference*. Use this book to obtain reference information about the DirX Identity agent programs, scripts, and files.
- *DirX Identity Troubleshooting Guide*. Use this book to track down and solve problems in your DirX Identity installation.

- *DirX Identity Installation Guide*. Use this book to install DirX Identity.
- *DirX Identity Migration Guide*. Use this book to migrate from previous versions.
- *DirX Identity REST Service Guide*. Use this book to migrate from previous versions.

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.

userID_home_directory
The exact name of the home directory. The default home directory is the home directory of the specified UNIX user, who is logged in on UNIX systems. In this manual, the home pathname is represented by the notation *userID_home_directory*.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Identity** on UNIX systems and **C:\Program Files\DirX\Identity** 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*.

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

dxi_java_home
The exact name of the root directory of the Java environment for DirX Identity. This location is specified while installing the product. For details see the sections "Installation" and "The Java for DirX Identity".

tmp_path

The exact name of the tmp directory. The default tmp directory is /tmp on UNIX systems. In this manual, the tmp pathname is represented by the notation *tmp_path*.

tomcat_install_path
The exact name of the root of the directory where Apache Tomcat programs and files are installed. This location is defined during product installation.

mount_point
The mount point for DVD device (for example, **/cdrom/cdrom0**).

1. Introduction

New customers install DirX Identity and work with the product. Existing customers must migrate their environment.

1.1. Migration from Versions older than V8.3

With DirX Identity V8.3, the Messaging functionality was changed. If you want to preserve and process your unprocessed messages (like password changes, Provisioning events, and so on), you must migrate them to the new Messaging functionality. DirX Identity V8.3 offers a migration tool for this task. In this case, you must migrate to V8.3. After successful migration to V8.3, you can migrate to the current version in a second step. See the V8.3 migration guide for information on how to migrate to V8.3. If you are not interested in message migration, you can migrate directly to V8.6.

1.2. Migration from Versions older than V8.7

This section is only of interest if you use the RACF schema extensions.

In all versions older than V8.7, the following RACF attributes were incorrectly defined with conflicting equality matching rules (Case Ignore equality matching) and substring matching rules (Case Exact substring matching).

- racfLNotesShortName
- racfNdsUserName
- krbPrincipalName
- racfLdapBindDN
- racfLdapBindPw

To solve this problem, we provide an automatic migration procedure that runs as part of the DirX Identity Configuration tool. The procedure copies the attribute values from the erroneous attributes to the new attributes that are correctly defined. We have renamed the erroneous attributes to LDAP attribute names with the suffix **OLD**; for example, **racfLNotesShortNameOLD**. After the data has been migrated in LDAP, you'll need to update the LDAP schema to remove these renamed erroneous attributes from several object classes. For details, see the section "Extending the DirX Identity Schema for Customer Domains" in the chapter "Manual Migration".

1.3. Manual Migration Overview

The following table lists the relevant manual steps described in the sections of chapter "Manual Migration" you should consider depending on your base version:

Base \ Target version \ version	**9.0**
V8.10	

Base \ Target version \ version	9.0
V8.9	“General Aspects” and “Aspects Relevant for DirX Identity V8.9”
V8.7	Additional to the sections above “Aspects Relevant for Upgrade from V8.7” in this chapter
V8.6	Additional to the sections above “Aspects Relevant for Upgrade from V8.6” in this chapter
V8.5	Additional to the sections above “Aspects Relevant for Upgrade from V8.5” in this chapter
V8.4	Additional to the sections above “Aspects Relevant for Upgrade from V8.4” in this chapter
V8.3 , V8.3 R2	Additional to the sections above “Aspects Relevant for Upgrade from V8.3” in this chapter
V8.2C	Additional to the sections above “Aspects Relevant for Upgrade from V8.2C” in this chapter
V8.2B	Additional to the sections above “Aspects Relevant for Upgrade from V8.2B” in this chapter
V8.2A	All sections.

1.3.1. Web Center Migration Overview

For Web Center migration, you need to consider all the change files on the version path. For example, if you want to migrate from V8.2A SP2 to V8.5, you need to read the following files:

- WebCenterChanges-82A-SP2-to-82C.txt
- WebCenterChanges-82C-to-83.txt
- WebCenterChanges-83-to-84.txt
- WebCenterChanges-83-to-85.txt

1.4. Features to be Migrated

This section gives an overview of the features to be migrated and explains the underlying concepts.

Many items in the next sections are performed automatically, but in some cases, manual steps are necessary.Consider all these next sections accordingly depending on the base version from which you want to upgrade.

1.4.1. General Issues

This section discusses issues that are relevant to all versions.

1.4.1.1. Deletion of Old Objects

Renaming of objects in the Provisioning configuration database requires deletion of the old objects after adding the new ones. This comes from the fact that the cn, which is part of the DN, is used as a display attribute. Procedures exist that handle the deletion task automatically.

1.4.2. Issues Relevant for Upgrade from V8.2A

This chapter describes all issues that are relevant for V8.2A only.

1.4.2.1. Typo ClearOnMasterRemoval

In the **UserCommon.xml**, this flag was not correctly written.

1.4.2.2. Identity API

The Identity API has changed. For details, see the DirX Identity API documentation delivered with Web Center.

1.4.2.3. Adaption of Policies

The object description names for password policies and provisioning rules had to be changed.

1.4.3. Issues Relevant for Upgrade from V8.2B

This section comprises all issues relevant for V8.2B only.

1.4.3.1. Migration of JMS Subscriptions

Subscription IDs of the C++-based Server were unified. The structure of the subscription IDs is now identical for Windows and UNIX systems. Statustracker subscription IDs no longer include the hostname of the system where it runs, because it may move to another host.

The new format for subscription ID is:

host.**jms.***module.topic*

For statustracker:

jms.*module.topic*

The old format is:

- Windows:

host.**jms.***module.host.topic*

For statustracker:

jms.*module.host.topic*

- UNIX:

host.**libmqjms_dxm.***host.topic*

For statustracker:

libmqjms_dxm.*module.host.topic*

An automatic migration routine performs this task during the upgrade configuration when you start the C++-based Server hosting ATS the first time.

1.4.3.2. Migration of Activation Date in Request Workflow Instances

Request workflows started with older versions may include an activation date (the workflow creation date) in the order. This causes a ticket creation during processing of the order. Migration eliminates these activation dates.

1.4.3.3. Migration of XML Content to LDAP Attributes in Request Workflow/Activity instances

In older versions, a lot of attributes were managed by an XML structure in the dxmContent LDAP attribute. For performance reasons, these attributes are now represented by LDAP attributes. Without a migration Request Workflow/Activity instances cannot be displayed correctly in the Identity Manager (especially the graphic). Therefore Request Workflow/Activity instances created by older versions are migrated.

1.4.4. Issues Relevant for Upgrade from V8.2C

This section describes all issues relevant for version V8.2C only.

1.4.4.1. Migration of Realtime Channels to Support Delta Handling

DirX Identity V8.3 supports delta handling in realtime workflows. This new feature requires an extension in the XML definition of the realtime channels. (LDAP attribute “dxmContent”).

An automatic migration routine performs this task during the upgrade configuration.

You can run this routine by hand at any time.

1.4.4.2. Migration of Event Port in Realtime Workflows

The realtime workflows can send JMS events for the event-based workflows. Internally the workflows have an event port integrated that starts a JMS connector. The XML definition for this JMS connector (LDAP attribute “dxmContent”) had some connection parameters defined that were not used by the workflow at runtime. With the integration of ActiveMQ as the JMS messaging system, these parameters were even invalid due to broken links to LDAP objects that no longer existed. Therefore, the XML definition of the JMS connector will now be updated by the migration routine.

An automatic migration routine performs this task during the upgrade configuration.

You can run this routine by hand at any time.

1.4.4.3. Deletion of the Certificate Handler adaptor in the IdS-J

The Certificate Handler is automatically deleted during the upgrade configuration.

It was used in the pre V8.2C versions for the Windows Password Listener. In V8.2C, the feature to distribute certificates and the message server list was assumed by the Configuration Handler adaptor. Therefore, in V8.3, this adaptor is no longer necessary.

1.4.4.4. Issues Relevant for Upgrade from V8.3 or V8.3 R2

This section comprises all issues relevant for V8.3 or V8.3 R2 only.

1.4.4.5. JMS Audit Handler

The JMS-Audit handler is neither configured nor updated automatically as part of the normal installation and configuration. See the chapter in the Installation Guide to upgrade the JMS audit handler.

1.4.5. Issues Relevant for Upgrade from V8.4

This section comprises all issues relevant for V8.4 only.

1.4.5.1. Java-based Server

There are two new special adaptors responsible for the consumption of scheduler and Identity Manager messages:

- The **Entry Change Start Workflow Listener** and
- The **Provisioning Request Start Workflow Listener**.

The Entry Change Start Workflow Listener (or Provisioning Request Start Workflow Listener) is always co-located with the Entry Change Listener adaptor (or Provisioning Request Listener adaptor) and starts event-based processing (or provisioning) workflows.

These new adaptors replace the legacy adaptor **Start Realtime Workflow Listener**. There are no manual steps necessary.

1.4.6. Issues Relevant for Upgrade from V8.5

This section describes all issues relevant for V8.5 only.

1.4.6.1. Use of SSL

In V8.6, SSL handling has been extended. For ActiveMQ, only client-side SSL is now supported. As a result, you need to perform the manual steps described in the chapter “Manual Migration” to migrate Windows Password Listeners that connect with SSL to ActiveMQ to connect with client-side SSL.

1.4.7. Issues Relevant for Upgrade from V8.6

This section describes all issues relevant for V8.6 only.

1.4.7.1. Clear Text Passwords

In V8.7, the use of clear text passwords has been minimized. In older versions, the following features stored clear text passwords in LDAP:

- Passwords for JMS-based auditing
- Passwords for sending e-mail notifications in request workflows
- Passwords for sending notification e-mail in Tcl-based workflows

Now these passwords are stored encrypted. See the relevant sections in the chapter “Manual Migration” for details on how to migrate the passwords formerly stored as clear text passwords.

1.4.8. Issues Relevant for Upgrade from V8.7

This section describes all issues relevant for V8.7 only.

1.4.8.1. Topic Prefixes

In V8.9, target system-specific adaptors were introduced. In this context, the topic prefix name of the following listeners was changed:

Listener	Old Topic Prefix	New Topic Prefix
SetAccountPasswordListener	dxm.setPasswordRequest	dxm.setPasswordRequest._default
ProvisioningRequestListener	dxm.request.provisionToTS	dxm.request.provisionToTS._default
ProvisioningRequest StartWorkflowListener	dxm.request.workflow.provisionToTS	dxm.request.workflow.provisionToTS._default

If you upgrade from an older version, for example, V8.5, these changes were not made in all cases automatically. So, you must make the canges manually with Web Admin.

1.4.9. Issues Relevant for Upgrade from V8.9

This section describes all issues relevant for V8.9 only.

1.4.9.1. Client-side SSL Support in Realtime Workflows

In V8.10, client-side SSL for realtime workflows using either an ADS Connector or LDAP Connector or RACF Connector is supported. Additional connection parameters for this feature need to be put into the XML workflow definition. There are no manual steps necessary.

1.4.9.2. New LDAP Controls LDAP_CTRL_NO_MODTIME_UPD (1.3.12.2.1107.1.3.2.12.9) and LDAP Conditioned Operation Control (1.3.12.2.1107.1.3.2.12.10)

In V8.10, the LDAP lock mechanism has been revised and improved. For better performance, two new LDAP controls are implemented by the DirX Directory server V8.9 (9.4.454 or higher). These controls are set at the LDAP root in the LDAP attribute **supportedControl** (DAP attribute name: **SCON**) if you installed DirX Directory from scratch. If you just do a DirX Directory upgrade installation, these LDAP controls are not set at the LDAP root.

DirX Identity checks at configuration time whether the current DirX Directory version supports these controls. If the LDAP controls are supported, then it updates the LDAP-root automatically if missing. But keep in mind that manual migration is necessary if you decide to upgrade the DirX installation later.

1.4.9.3. Topic Prefixes

In V8.9, target system-specific adaptors were introduced. In this context, the topic prefix name of the following listener is automatically changed in V8.10:

Listener	Old Topic Prefix	New Topic Prefix
ImportToIdentity	dxm.request.importToIdentity	dxm.request.importToIdentity._default

2. Migration Procedure

The general migration procedure is:

1. Prepare the Migration.
2. Perform the Installation and Configuration with Automatic Migration.
3. Perform the Manual Migration Steps.
4. Test all of your applications and workflows thoroughly to be sure that everything works well.
5. If you encounter any problems, read the ch6_problems.pdf.

3. Preparing the Migration

These steps are necessary to prepare the migration. Depending on the features you used, you need to perform the steps described in the next chapters.

3.1. Preserving Files

If you changed default parameters in files, back up these files. Examples of these changes are:

- idmsvc.ini - you increased, for example, memory requirements (IdS-J server)
- dxi.cfg - you made customizations according to the user documentation
- runserver.bat or runserver.sh - you increased, for example, memory requirements
- dxmmsssvr.ini - you used different port parameters, passwords or a **certdb** file path
- domain.xml - you set a different search timeout limit than the default
- bindcredentials.xml - you set your own timeout limits
- password.properties - you provided PIN values for encryption or signature (IdS-J server) or SSL keystore password.The file is written anew by the Configuration Wizard, which asks you to set your PIN values.
- gen*Keystores.bat/sh - scripts to generate keys; check for changed parameters
- set_Environment.bat/sh - scripts to generate certificates and keys; check for changed parameters
- web.xml - you changed parameters like SSL or debug
- cacerts - you set up certificates for SSL in this file in the Java JRE folder *dxi_java_home***/lib/security**. When creating the cacerts backup, ensure that your backup is outside *dxi_java_home*.

3.1.1. Custom Libraries

If you used custom libraries (JAR files) in your previous installation, back up these files. Since **9.0.0**, you can use the Custom Libraries feature to preserve these files.

The installation and configuration process removes old JAR files from previous installations, and even though it tries to do that only to the non-custom files, it is safer to back up your custom JAR files.

4. Automatic Migration during Installation and Configuration

Now you can start the Installation followed by Configuration. see Update Installation.
During Configuration, some migration steps are performed automatically.

5. Manual Migration

Perform all the steps described in this chapter that are relevant to adapting your environment to DirX Identity.

5.1. General Aspects

The following manual migration steps are relevant for all DirX Identity versions.

5.1.1. Restoring Preserved Files

Restore the specific information from the files you backed up as described in the section “Preserving Files” in the chapter “Preparing the Migration” by merging the information in the backup files into the files in the relevant locations.

You only need to update the file *dxi_java_home***/lib/security/cacerts** with the information from the relevant backup.

5.1.2. Migrating Passwords for JMS-based Auditing

Performing this task is only necessary if you use JMS-based auditing; that is, if the **JMS-based Auditing** flag is checked in the Status and Auditing tab of your IdS-J Server (Java-based Server) configuration object in the Connectivity database. (Connectivity view → DirX Identity Servers → *your-ids-j-server* → Status and Auditing tab → Auditing – General section).

In older DirX Identity versions, the password and user were taken from an attribute at the ids-j object where the password was stored in clear text. Beginning with V8.7, the user and password are now taken from a specified bind profile. If you use JMS-based auditing, you need to migrate the configured user and password as follows:

1. Create a bind profile that holds the user and password. We recommend adding the bind profile to your Identity Store connected directory. Only the **User** and **Password** bind parameters are required. Enter the text **JMS** in **Anchor**.
2. In the IdS-J Server’s Status and Auditing tab, enter the newly created bind profile into **Bind Profile**.
3. Restart the Ids-J Server.
4. Repeat steps 2 and 3 for every IdS-J Server configuration object that uses JMS-based auditing using the bind profile you created in step 1.

5.1.3. Migrating Passwords for Mail and SMS Gateway Configuration

In the Provisioning view, the **SMTP** configuration object for sending e-mail notifications and the **SMS Gateway** configuration object for sending SMS notifications are located in **Workflows** → **Configuration** → **Services**.

If the **Authenticate** flag is checked for these configuration objects, the password

information for these objects needs to be migrated.

For each configuration object, enter the password in the relevant field and then save the object. Now the passwords are stored encrypted according to the type of encryption mode specified in the Connectivity database's central configuration object (in **Encryption Mode** in the Server tab).

5.1.4. Migrating Passwords for Sending Notifications in Tcl-based Workflows

You can define notifications in the Connectivity view at the **metacp** job in the Operation tab. If you have used these notifications with a user and password, you need to migrate the referenced service object, which is usually the Mail Service (**Configuration** → **Services** → **System** → **Mail Service**).

Open the notification object (it's usually located below the **metacp** job object (Connectivity view → **Jobs** → *your_metacp_job* → *your_notification_object*)) and then click the **Service** link in the Service Definition area to open the service object. Enter the password and save the object. Now the password is stored encrypted according to the encryption mode defined in the Connectivity central configuration object (**Encryption Mode** in the Servers tab).

5.1.5. Using SAP JCo version 3.1.4 or Higher for SAP ECC UM Connector/Agent

We recommend upgrading to the latest version.

5.1.6. Migrating SPML Provisioning Web Services

After installing and configuring DirX Identity, configure the services according to the section "Runtime Operation" in the chapter "SPML Provisioning Web Services" in the *DirX Identity Integration Framework Guide*.

After customizing the Provisioning Web Services, merge the relevant configuration information from your backup into the relevant files of the folder *install_path* /**web/instances/provisioningService/provisioningService-***technical_domain_name*.

For selected migration paths, the files **ProvisioningWebServicesChanges**.txt* in the subfolder **Documentation/DirXIdentity/ProvisioningWebServices** of the installation media list all files and folders to be merged.

When upgrading from a version lower than V8.5, the folder *install_path/***provisioningServlet** is obsolete. Keep a related backup outside the DirX Identity installation and then remove this folder. When you are sure that the backup is no longer needed, remove the backup, too.

5.1.7. Migrating SPML Provisioning Web Services Clients

Migrating the SPML Provisioning Web Services clients consists of the following steps:

- Stop using the obsolete, unsupported sample client and remove the following related

files: **agentconf.xml**, **conf.xml**, **cpappend.bat**, **fireSOAP-Request.bat**, **fireSOAP-Request.sh**, **log4j.properties**, **request.xml** in the folder *install_path/***provisioningServices/lib**. These files represent an obsolete sample client that uses a proprietary format in sent requests and received responses. Using this client is no longer supported. Stop using this client or related customizations and then remove these files.

- Update the runtime environment of your Web Services clients with the jar files shipped with DirX Identity. The set of jar files to be used is located in the folder *install_path/***provisioningServices/lib**.
- Ensure that the classpath in your runtime environment of your Web Services clients is computed so that the appropriate set of jar files is on the classpath. You'll find samples of the correct classpath computation in the file *install_path/***provisioningServices/spmlv2/fireSpmlv2-Request.bat** (Windows platforms) or **fireSpmlv2-Request.sh** (UNIX platforms).
- The file *install_path***/provisioningServices/spmlv2/conf.xml** is overwritten at installation time. Therefore, you must adapt this file according to the section "Getting Started with the Test Client" in the chapter "SPML Provisioning Web Services" in the *DirX Identity Integration Framework Guide*. You can do this either from scratch or by merging the relevant information from a related backup.

5.1.8. Migrating a Customized Web Center

If you have a customized Web Center, you must merge the changes from your backed-up customized version into the new version of Web Center which now contains the domain name:

*install_path***/web/instances/webCenter-***technical_domainname*

The files **WebCenterChanges*.txt** in the subfolder **Documentation/DirXIdentity/WebCenter** of the installation media list all files and folders to be merged.

Note that the new URL is now

http://host**:8080/webCenter-***technical_domainname*

You can rename the URL by renaming the related file **webCenter-***technical_domainname***.xml** in the folder *tomcat_path***/conf/Catalina/localhost**. If you rename the URL, you must update the related URL in the Provisioning Store accordingly. (DirX Identity Manager → Provisioning → Workflows → Configuration → Services → Approval, Property **Location (URL, server)**).

5.1.9. Migrating a Customized Web Center for Password Management

If you have a customized Web Center for Password Management, you must merge the changes from your backed-up customized version into the new version of Web Center which now contains the domain name:

*install_path***/web/instances/pwdManagement-***technical_domainname*

The files **WebCenterChanges**.txt* in the subfolder **Documentation/DirXIdentity/WebCenter** of the installation media list all files and folders to be merged.

5.1.10. Migrating a Customized Business User Interface

See the *Business User Interface Configuration Guide* for more detail information about migrating.

5.1.11. Migrating the 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 V8.10 does not work.

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

5.1.12. Adapting Size Limits for LDAP Searches (using DirX Directory)

The size limit applied to an LDAP search operation limits the number of returned entries in single searches and paged searches.

The source is:

1. LDAP search operations option size limit (user defined)
2. LDAP server's configuration property "**Ldap-Search-Svc-Ctl**" (**LSES**) (defined by the administrator for each LDAP server)
3. DSA's User Policy (defined by the administrator, user specific)

The value in force is 3 or a smaller limit from 2 or 1 (if there is no specific limit for that user; for example, there is no DSA User Policy for that user).

Older directory versions (before release "DirX Directory V8.2B") had a problem interpreting the size limit in search operations: they applied the size limit to every single search operation in a series of paged searches. Therefore, the size limit could easily be circumvented by specifying a page size smaller than the size limit in force.

Starting with DirX Directory 8.2B, the size limit is applied to the entire search operation regardless of whether or not it uses simple paging control.

Caution: Applications may see a changed behavior:

- Retrieving the n^{th} page of a paged search operation may return with a "size limit reached" return code and an empty cookie.
- The size limit in force must be big enough for all entries in all pages returned in one search operation.
- For anonymous users, the size limit is defaulted to 2048.

- Use the UserPolicy (USP attribute of the root DSE) to set the required limits.

Please note that DirX Identity has defined user policies with a size limit of 32,768 for non-paged searches and a paged result size limit of 100,000 (for the Connectivity branch and for each domain in the Provisioning branch).

Example (including the sample domain):

```
dirxadm> show / -attr USP -p
1) /
     User-Policy
         User-Subtree-Name       :
/DXMC=DirXmetahub/DXMC=Groups/CN=Read
         Size-Limit              : 32768
         Paged-Search-Size-Limit : 100000
     User-Policy
         User-Subtree-Name       : /CN=DirXmetaRole-
SystemDomain/CN=SystemAdmin
         Size-Limit              : 32768
         Paged-Search-Size-Limit 100000
     User-Policy
         User-Subtree-Name       : /CN=My-
Company/CN=TargetSystems/CN=DirXmetaRole/CN=Groups/CN=DomainAdmins
         Size-Limit              : 32768
         Paged-Search-Size-Limit : 100000
```

Normally you should not have any size limit problems; if you do, you must increase either the size limit of 32,768 or the paged result size limit of 100,000 to some higher value.

When configuring a new customer domain, the default values for the two size limits are as described in this section.

5.1.13. Extending the DirX Identity Schema for Customer Domains

If you upgrade to a new DirX Identity version, be aware that the schema for certain target system objects may have been extended for the purpose of provisioning new connected system attributes. The schema for the My-Company domain is updated during Initial Configuration if the domain step with the My-Company domain is selected. If you configure your own customer domain, you must update the schema for that domain by running the appropriate agent schema scripts provided in the *install_path*/schema/tools* folder. For a detailed description of this procedure, see the section “Extending the Schema for the Target System Workflows” in the *DirX Identity Application Development Guide*.

The following sections provide an overview of the schema changes provided for all the supported connected systems. Except for RACF, no migration needs to be done manually.

5.1.13.1. Agent Schema Changes in V8.10

There are no agent schema changes in V8.10.

5.1.13.2. Agent Schema Changes in V8.9

The following systems are no longer supported:

- UNIX-PAM
- SoarianClinical

5.1.13.3. Agent Schema Changes in V8.7

There are no agent schema changes in V8.7.

5.1.13.4. Agent Schema Changes in V8.6

5.1.13.4.1. RACF

The following attributes had an erroneous substring matching rule (caseExactSubstringMatching instead of caseIgnoreSubstringMatching)

- krbPrincipalName
- racfLdapBindDN
- racfLdapBindPw
- racfNdsUserName
- racfLNotesShortName

An automatic migration of these attributes is available and is executed while running the DirX Identity Configuration tool. You can also start this migration step by hand at any time. It is located in:

install_path/**tools/migration/86/database**

As the Provisioning part is migrated, all arguments refer to the Provisioning configuration database.

Usage:

MigrateRACFschema.bat *host port user password ssl domain-DN logfile*

Example:

```
MigrateRACFschema.bat localhost 389 "cn=DomainAdmin,cn=My-Company"
dirx 0 "cn=My-Company" log.txt
```

Manual schema update:

After the user data has been migrated, you must drop the erroneous attributes manually from the schema. The erroneous attributes have been renamed in the schema by appending the suffix **OLD**. Adapt the relevant object classes as listed in the following files:

install_path/**tools/migration/86/database/postSchemaUpdate/dirx.racf.ldif** (for DirX Directory)

For DirX Directory, the relevant changes are:

```
# "racfLNotesShortNameOLD" has been dropped
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.12.2.1107.1.3.102.6.16.16 NAME
'racfLNotesSegment'
    DESC 'This is a proprietary DirXmetahub objectclass.'
    AUXILIARY
    MAY ( racfLNotesShortName ) )
-
# "racfNdsUserNameOLD" has been dropped
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.12.2.1107.1.3.102.6.16.17 NAME 'racfNdsSegment'
    DESC 'This is a proprietary DirXmetahub objectclass.'
    AUXILIARY
    MAY ( racfNdsUserName ) )
-
# "racfLdapBindDNOLD" has been dropped
# "racfLdapBindPwOLD" has been dropped
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.12.2.1107.1.3.102.6.16.18 NAME
'racfProxySegment'
    DESC 'This is a proprietary DirXmetahub objectclass.'
    AUXILIARY
    MAY ( racfLdapBindDN $ racfLdapBindPw $ racfLdapHost ) )
-
# "krbPrincipalNameOLD" has been dropped
dn: cn=schema
changetype: modify
```

```
add: objectclasses
objectclasses: ( 1.3.12.2.1107.1.3.102.6.16.19 NAME
'racfKerberosInfo'
    DESC 'This is a proprietary DirXmetahub objectclass.'
    AUXILIARY
    MAY ( racfCurkeyVersion $ racfEncryptType $ krbPrincipalName $
    krbPrincipalNameOLD $ maxticketage ) )
-
```

5.1.13.4.2. Salesforce

The following new attributes are provided:

- dxmSLSFcontactId
- dxmSLSFcontactName
- dxmSLSFdefaultPermissionSet
- dxmSLSFdefaultPermissionSet-DN
- dxmSLSFpermissionSet
- dxmSLSFpermissionSet-DN
- dxmSLSFprofileId
- dxmSLSFprofileName
- dxmSLSFprofile-DN
- dxmSLSFuserLicenseName

The following new object class is provided:

dxmSLSFpermissionSet

Please note that currently only the schema for Salesforce has been extended. These attributes and object classes are currently not supported by the Salesforce Connector and the Salesforce realtime workflow.

5.1.13.5. Agent Schema Changes in V8.5

5.1.13.5.1. ADS

The following new attributes are provided:

- dxmLyncInternetAccessEnabled
- dxmLyncOptionFlags
- dxmLyncPrimaryHomeServer
- dxmLyncUserPolicies
- dxmLyncUserRoutingGroupId

- dxmLyncUserEnabled
- dxmLyncFederationEnabled
- dxmLyncDeploymentLocator
- dxmLyncPrimaryUserAddress

The following new object class is provided:

dxmLyncUser

5.1.13.6. Agent Schema Changes in V8.4

DSWin is no longer supported.

NDS is no longer supported.

Salesforce is new.

5.1.14. LDAP Lock Mechanism for User Objects

A lock mechanism (preventing parallel updates for a user) has been implemented in DirX Identity V8.6 and was revised in DirX Identity V8.6-SP1 and again in DirX Identity V8.10. More details are available in the use case document *DXI Java Programming*.

5.1.15. Migrating Realtime Workflows to Support Client-side SSL Authentication

Client-side SSL authentication is supported in realtime workflows when using one of the following connectors: ADSConnector, LDAPConnector, and RACFConnector.

The XML workflow definition needs to be adapted to support additional connection parameters.

Migration is done automatically during the first Configuration Wizard run. All workflows in the Connectivity database (using any of the connectors listed above) are processed.

You can start this migration step by hand at any time. It is located in:

install_path/**tools/migration/89/rtworkflows**

As the Connectivity part is migrated, all arguments refer to the Connectivity configuration database.

Usage:

MigratePortForClientSSL.bat *host port user password ssl logfile*

or

MigratePortForClientSSL.sh *host port user password ssl logfile*

Example:

MigratePortForClientSSL.bat localhost 389 "cn=admin,dxmC=DirXmetahub" dirx 0 trace.txt

5.2. Aspects Relevant to Using DirX Directory V8.6 or Higher

5.2.1. Rebuilding Attribute Indexes to Handle Improved Search Operations

DirX Directory V8.6 and higher versions provides improved search operation processing, especially for AND filter combinations that begin with filter items (for example, **uid=b***), “greater than or equal to” filter items (for example, **time>=20170716**) and/or “less than or equal to” filter items (for example, **time⇐20170716**) - apply.

For best performance, we recommend re-building the indexes for the attributes where these search filters apply on a regular basis; for example, on a bimonthly schedule.To perform this task, for example, use the following **dirxadm db attrconfig** command:

dirxadm> db attrconfig uid time -index BUILD

Note that the DSA runs in the POSTINDEXING operation mode while the db attrconfig command is in progress and update operations will be rejected.

DirX Identity attributes that need to be handled this way include:

dxmStatusExpirationTime

dxrCertificationDate

dxrDeleteDate

dxrDisableEndDate

dxrDisableStartDate

dxrEndDate

dxrExpirationDate

dxrPwdExpiryNotified

dxrStartDate

5.2.2. Migration of New LDAP Controls LDAP_CTRL_NO_MODTIME_UPD (1.3.12.2.1107.1.3.2.12.9) and LDAP Conditioned Operation Control (1.3.12.2.1107.1.3.2.12.10)

Starting with DirX Identity V8.10, the Entry Lock Manager has been improved and makes use of two new LDAP controls. These LDAP controls are available with DirX Directory Server

V8.9 (9.4.454 or higher) if you installed DirX from scratch. A DirX upgrade will not set the LDAP controls at the LDAP root.

The Configuration Wizard sets these LDAP controls.But please note that a manual migration is necessary if you decide to upgrade the DirX installation after you have already configured DirX Identity.

In this scenario, the migration procedure is as follows:

- Set the password of the DirX administrator (Tcl variable DIR_PW) in the file *install_path*/basic.input.tcl*.
- Open an MS-DOS command prompt or a UNIX shell in the directory *install_path*/schema/role-dirxee/SystemDomain*.
- Run the following command: **dirxadm init.v810.adm**.
- Check the content of the tracefile **setup-trace.txt** in the current directory.The tracefile should show that **dirxadm** terminated with exit code 0.
- Set the TCL variable DIR_PW in **basic.input.tcl** to "".

5.3. Aspects Relevant to DirX Identity 9.0

5.3.1. Support of Java 21 and Tomcat 11

This version runs with Java 21 (JRE or JDK) and Apache Tomcat 11 only. See Supported Java and Tomcat in the release notes for more details.

5.3.2. Recompilation of Java Source Mappings

5.3.2.1. Background

DirX Identity 9.0 introduces updated runtime components (including new versions of join.jar, map.jar, spml.jar and the switch to Java 21). Because of these changes, **existing Java Source Mappings** from DirX Identity 8.9 / 8.10 must be **recompiled** after upgrading to 9.0.

If Java Source Mappings are not recompiled, **Java Realtime Workflows** that use them may fail at runtime (for example with `MethodNotFoundException` or **similar errors** in the server logs).

Recompilation is **not performed automatically by the Deployment Tool**. After upgrading to 9.0, recompilation must be triggered manually in DirX Identity Manager using the context action **Recompile all**.

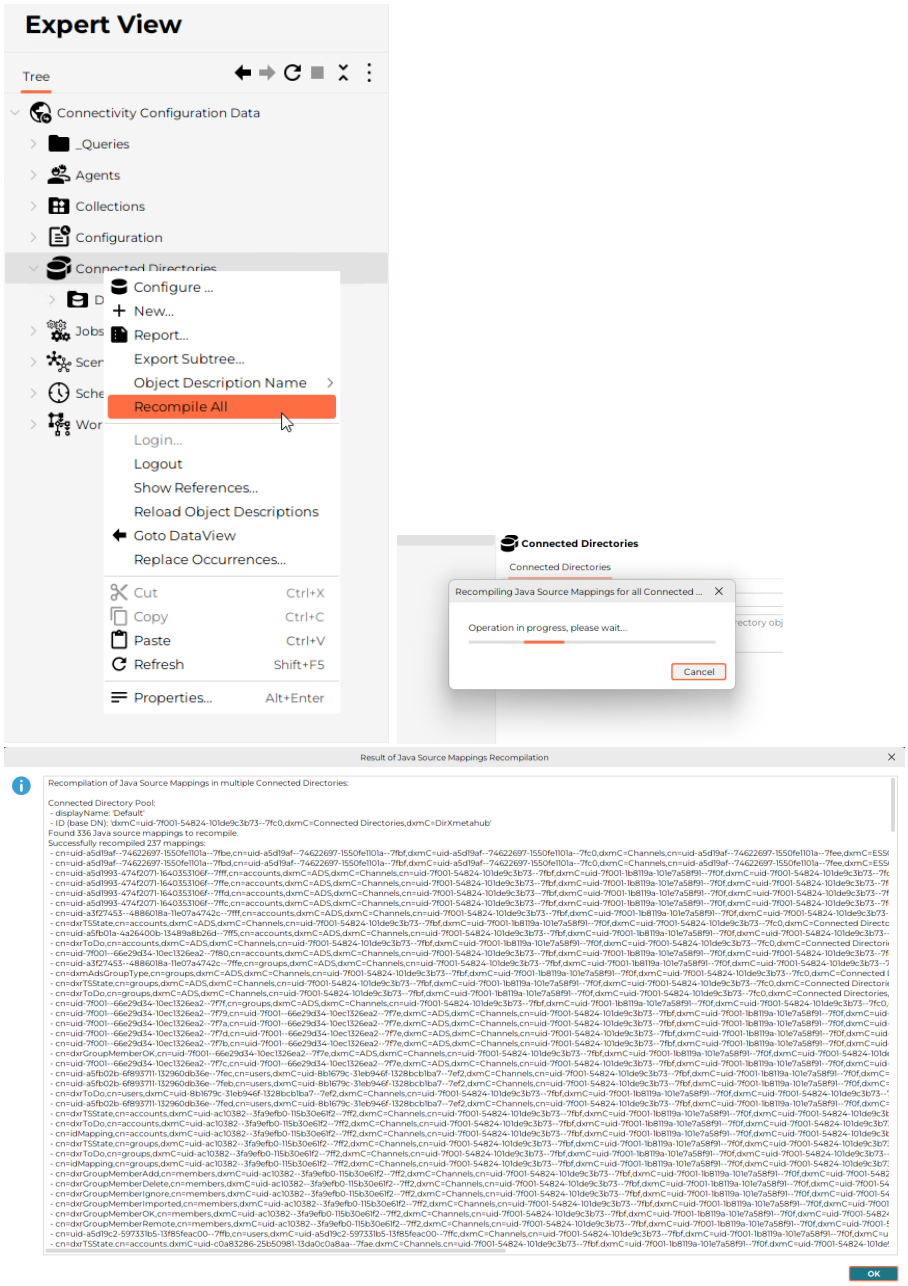
5.3.2.2. When is this required?

You must perform this step if **both** of the following apply:

- You upgraded from **DirX Identity 8.9 or 8.10.x to 9.0**, and
- The environment contains **Java Realtime Workflows** that use **Java Source Mappings**

5.3.2.3. How to recompile (post-upgrade step)

1. Complete the software upgrade to **DirX Identity 9.0**.
2. Open **DirX Identity Manager**.
3. Navigate to the area where Java Source Mappings are managed (typically under the **Connected Directories** / channel configuration tree).
4. Use the context menu action Recompile all to recompile all Java Source Mappings.



Only then are all existing Java Source Mappings recompiled against the new libraries and Java runtime.

For new 9.0 installations without existing Java Source Mappings, this step has no adverse effect. Any delivered factory mappings present in the directory will simply be compiled.

5.3.2.4. Expected results

- The recompilation completes successfully.
- The compile result (byte code) is stored back on the mapping entries (see verification below).
- Workflows using those mappings run without the previous runtime errors.

5.3.2.5. How to verify successful recompilation

1. **Directory-level verification**
   Each Java Source Mapping is stored as an entry with object class dxmAttributeMapping that contains:
   a. **dxmContent** – the Java source code
   b. **dxmCompiled** – the compiled byte code

      After successful recompilation:

      - The attribute **dxmCompiled** is present for the Java Source Mapping entries.
      - In most cases the byte code stored in **dxmCompiled** differs from the value before the upgrade, because it has been recompiled against the new runtime.
2. **Functional verification (recommended)**
   - Trigger Java Realtime Workflows that use Java Source Mappings.
   - Check the DirX Identity server logs.

Before recompilation, you typically see errors like:

- **MethodNotFoundException** (or similar class/method resolution errors)

After running `Recompile all`, these errors should no longer occur and workflows should execute normally.

5.3.2.6. Troubleshooting

- If recompilation fails for specific mappings, fix the Java source code of the affected mapping(s) and run `Recompile all` again.
- If workflows still fail after recompilation, confirm that the workflow actually uses Java Source Mappings and re-check server logs for the concrete failing class/method.

5.3.2.7. Aspects Relevant for Upgrade from 8.9 to 9.0

5.3.2.8. Aspects Relevant for Upgrade from 8.10, 8.10 SP1, 8.10 SP2, 8.10.x to 9.0

6. Known Issues

6.1. Overwritten cert8.db file during Update installation

During an update or upgrade installation the cert8.db file is written again.If you used this default file for your certificates they are lost.

To prevent such type of errors, use another filename for your certificates and set the corresponding environment variable.

6.2. Overwritten agent batch files during Update installation

During the DirX Identity installation the agent batch files in the bin directory of the installation path are overwritten.If you changed something in these files (for example more memory for the Java processes) this information is lost.

To avoid this problem, you should copy the agent batch file before you perform the changes.To use the copied and changed files, set the link from the Agent objects in the DirX Identity configuration database (Connectivity Configuration Data → Agents) to the new files.

In a distributed environment be sure that all DirX Identity servers where this agent shall run have a copy of the changed file.

6.3. Deletion of Old Objects

If you have to delete objects after the InitialConfiguration run, which can only happen in the context of a collection import or other ldif file import after the InitialConfiguration, you can run the scripts again.

To run the scripts for deletion of objects listed in ***.ldif** files:

- Open a dos prompt,
- change to the directory *install_path***\confdb\data**,
- call **..\..\bin\metacp ..\tcl\load.ldif.change.tcl** *OutdatedObjects_filename trace_filename*

To run the scripts for deletion of objects listed in *.txt files:

- Open a dos prompt,
- change to the directory *install_path**\confdb\data*,
- call **..\..\bin\metacp ..\tcl\removeSubtree.tcl** *user password server port ssl subtree_dn tracefile* for every subtree dn listed in the ***.txt** file.

Because the **removeSubtree.tcl** script must be called for every subtree it is easier to delete the subtrees with the Identity Manager.

6.4. UID Generation Fails

Running migration.bat from the folder

`install-path\gui\migration\CreateDxrUids`

can result in the

`Set uid value for object dn failed.`

Cause could be that you extended your object description for example with save scripts. To solve this problem be sure that the DirX Identity Manager and the migration script use the same ClassPath.

6.5. Sample Domain: Doubled Memberships (ADD/OK)

Updating an existing and used sample domain can result in doubled memberships at accounts and groups. That means the dxrMemberADD and dxrMemberOK are both filled with the same members.

This problem comes from the fact that initially the members are all in ADD state. If you played with the sample domain, some or all of the members go to OK state. Updating the sample domain during an upgrade adds all ADD states again.

You can easily correct this problem if you resolve all users of the My-Company domain.

Run the Privilege resolution with the filter (objectClass=dxrUser). This resolves all users and corrects these doubled memberships.

6.6. Inconsistent Object Descriptions (single / multi value)

If an attribute is filled in the LDAP directory with multiple values and the object description for this attribute is defined as single value, errors could occur that were hard to find.

Starting with DirX Identity V8.2B such inconsistencies are reported via a warning message:

WAR(STG617): Multiple values exist for single value property '<attributename>' of dn=...

If you encounter such a warning, check the corresponding object description of that object and correct it.

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.