EVIDEN

Identity and Access Management

DirX Identity

Installation Guide

Version 8.10.14, Edition March 2026

Table of Contents

Preface

This manual describes how to install and configure DirX Identity. It consists of the following chapters:

- Chapter 1 provides a summary of the installation procedures and their requirements.
- Chapter 2 describes how to install DirX Identity on a single machine.
- Chapter 3 describes the DirX Identity installation procedure.
- Chapter 4 describes the DirX Identity configuration procedure.
- Chapter 5 describes how to install single components.
- Chapter 6 describes other installation configurations.
- Chapter 7 describes how to install the DirX Identity Windows Password Listener.
- Chapter 8 describes how to deploy the JMS-Audit handler into a DirX Identity installation.
- Chapter 9 provides detailed information about the Java environment for DirX Identity.
- Chapter 10 explains additional topics
- Appendix A describes how to set up Windows single sign-on based on Kerberos.
- Appendix B describes how to integrate Web Center into NetWeaver.

DirX Identity Documentation Set

*Version 8.10.14 | Build 1858 | Date 2026-03-26 *

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 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.

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

DirX Identity provides the following installation procedures to build up a DirX Identity environment:

- An installation procedure simply copies the necessary files to the file system and updates registry entries (on Windows) and environment variables (which requires a restart on Windows). The installation procedure can handle either local or distributed DirX Identity systems.
- A subsequent configuration procedure extends the schema of the directory server for DirX Identity, loads the DirX Identity domains with initial data and configures all other components of DirX Identity. The configuration procedure is tailored to configure either local or distributed DirX Identity systems. (See section "Schema and Content Handling" in chapter "Additional Topics" for details.)

Installation and configuration is clearly separated. Select all components that are necessary on a specific machine. Afterwards you can configure these components with the DirX Identity Configurator.

The remainder of this chapter provides general information about the installation and configuration procedures. This chapter does not discuss installation in a distributed environment.

Please note that new versions of DirX Identity are distributed about every half year. To allow intermediate updates (new features or bug fixes), service packs are delivered.

For example, Service packs can be used to:

- Enhance the DirX Identity Manager with new functionality.
- Extend the Connectivity or Provisioning Configuration with new default applications.
- Deliver new or updated agents or connectors.
- Extend or correct the documentation / help.
- Correct known bugs with high importance.

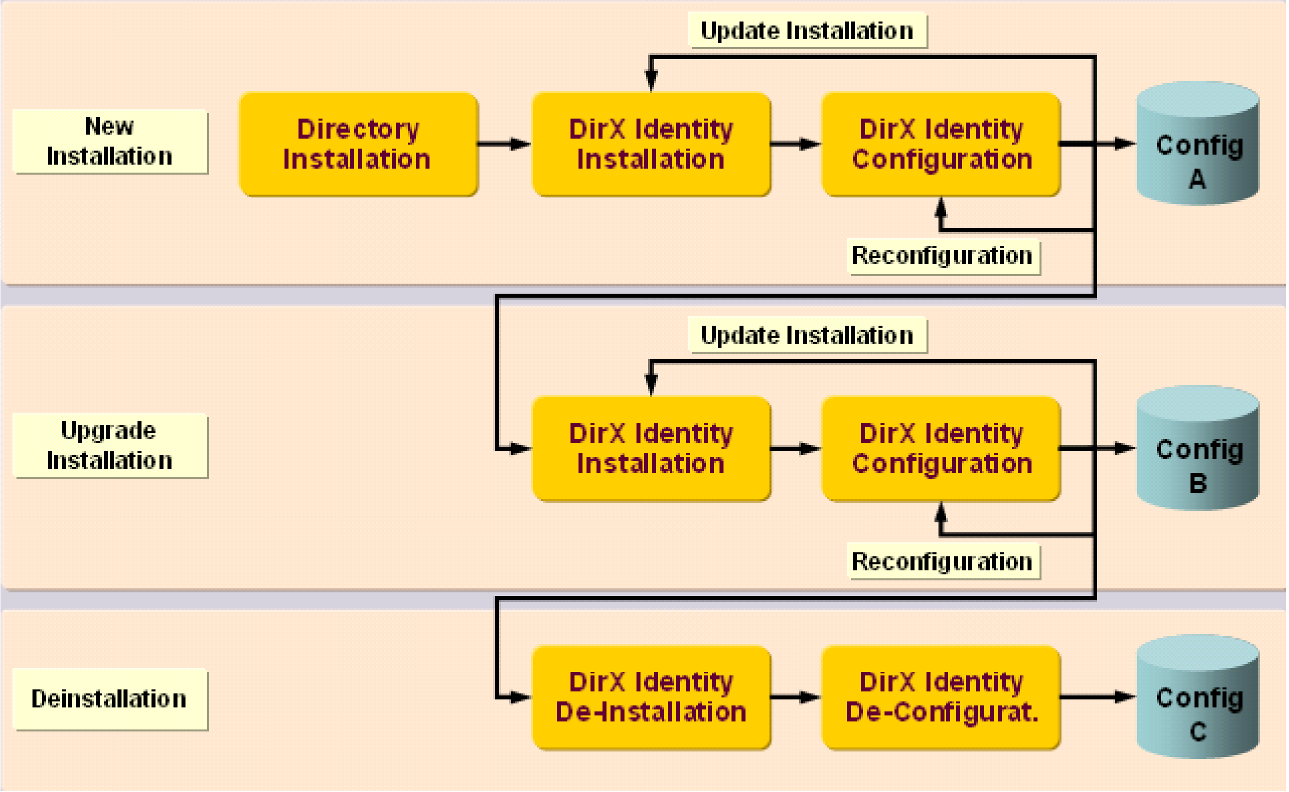
Contact your support organization for the latest information about service packs.

1.1. General Information

This section provides information that applies to all DirX Identity installation procedures.

1.1.1. Supported Use Cases

Only the following use cases are supported:



1.1.1.1. New Installation

Installing DirX Identity for the first time requires installation of one of the supported directory servers (**Directory Installation**). Afterwards, the **DirX Identity Installation** is to be performed. It installs all necessary software. Running the **DirX Identity Configuration** imports and configures all necessary data into the LDAP configuration stores (Config A).

You can extend or change the configuration at any time (**Reconfiguration**).

1.1.1.2. Update Installation

Running an **Update Installation** is also possible if you destroyed parts of the default objects in the configuration stores.

Before running an Update Installation, check the section "Preserving Files" in the chapter "Preparing the Migration" of the *DirX Identity Migration Guide* for files to be preserved and create backup copies of these files.

Running the **DirX Identity Configuration** imports and configures all necessary data into the LDAP configuration stores (Config A).

After running an Update Installation with Configuration, check the section "Restoring Preserved Files" in the chapter "Manual Migration" of the *DirX Identity Migration Guide* for files to be restored and restore these files according to said section.

You can extend or change the configuration at any time (**Reconfiguration**).

1.1.1.3. Upgrade Installation

Installing a new version of DirX Identity requires an Upgrade Installation. Run the **DirX Identity Installation** of the new version and then perform a DirX Identity Configuration. The **DirX Identity Configuration** performs automatic migration and configures all necessary new data. Check the *DirX Identity Migration Guide* for manual steps to be performed.

You can extend or change the configuration at any time (**Reconfiguration**).

1.1.1.4. De-Installation

If you intend to un-install DirX Identity, run the **DirX Identity De-Installation**. This includes the **DirX Identity De-Configuration** routine. After these two steps all installed software is removed from the machine.

Because you may want to use all or part of the LDAP configuration stores, this data is not touched and is therefore preserved.

Note that it is not possible to run a new installation on such a configuration store. Perform a new installation (see above) on an empty configuration store of the new DirX Identity version instead and then migrate the data from your old configuration store using the corresponding directory server tools.

1.1.2. Supported Meta Directories

You can run the DirX Identity installation on the following LDAP directory servers:

- DirX Directory Server

See the release notes for the supported version numbers of these directory products.

1.1.3. Supported Operating Systems

You can run the DirX Identity installation on the following operating systems:

- Microsoft Windows
- Linux

See the release notes for the supported version numbers, prerequisites, and limitations of these operating systems.

The next sections provide specific hints and procedures for the related operating system.

1.1.4. Compatibility with Previous Releases

You can upgrade from previous versions of DirX Identity. See the corresponding guidelines in the *DirX Identity Migration Guide*.

1.1.5. Disk Space Requirements

The installation requires temporarily 1400 MB of disk space. The complete DirX Identity installation requires 980 MB of disk space. For data and log files, additional space is required.

See the section "Disk Space Calculation" in the chapter "Additional Topics" for more information.

1.1.5.1. Hints for Firewall Configuration

The default ports you should open for firewalls are (only if you use the corresponding component):

Service	Non SSL	SSL
Apache ActiveMQ broker	61616	61617
Apache ActiveMQ admin Web console	8161	8161
Apache ActiveMQ (JMX)	10098+10099	10098+10099
C++-based Server (SPML Service)	9900	9901
C++-based Server (proprietary JMX)	5315	5315
Java-based Server (HTTP/HTTPS Web services)	40*n*00	40*n*00
Java-based Server (JMX)	40*n*05+40*n*06	40*n*05+40*n*06
Tomcat deployments (defaults)	8080	8443

These ports are the default ports that you can change during the DirX Identity configuration. If you change them, open these ports in your firewalls. For the IdS-J server, the *n* is set to **0** for S1, **1** for S2, and so on.

Check the ports of the LDAP server(s) you intend to use as the Connectivity Store and/or Provisioning Store, respectively. Open these ports on the server-side if your scenario requires remote access to these LDAP servers(s). For DirX Directory Servers, the defaults are **389** (Non SSL) or **636** (SSL), but the ports that are actually relevant depend on the LDAP configuration.

If you are running DirX Directory Server 9.0 or later on the same host as the tomcat for DirX Identity, make sure, that the secure port used for the DirX Directory REST service (default 8443) is different from the secure port (default 8443) used for the tomcat installed for DirX Identity. The port 8443 will be configured in the configuration file of the DirX Identity Business User Interface for accessing the DirX Identity REST service.

Note that two ports are now used for JMX Access. In the configuration, you set the first number in the configuration; the second is always the first port number +1 and is the JMX RMI port.

Check for additional ports for connectors and agents necessary to access target systems you intend to provision (see the service definition for the corresponding connected directories).

The C++-based Server uses the default port 1111 for the transfer of private keys from the server to an agent. This is local process intercommunication so do not open this port in your firewall.

If you defined other ports during DirX Identity configuration, adapt your firewall configuration accordingly.

Note: With a socket connection, an “ephemeral” (short-lived) port is used on the client side, which the client requests from the operating system. In Microsoft Windows, the range of these ports is usually between 49.152 and 65.536. If a port is in use, change the port number during configuration accordingly.

1.1.6. Installation Limitations

The installation and configuration procedures have the following general limitations:

1. You must run the installation procedure on the machine that is the installation target (remote installation is currently unavailable).
2. If DirX Identity is installed in a distributed environment, be sure to update all machines with the new software version. Otherwise, severe interworking problems could be the result. You can check the installed version on a machine in the **install_history.txt** file in the installation directory.
3. Before performing an update or an upgrade installation, you need to perform these steps:
   - Stop all running workflows (disable scheduling, shutdown event managers). You can use the maintenance scripts to perform this task.
   - Stop all DirX Identity services and user interface components, including the Tomcat Services into which you deployed DirX Identity components.

1.1.7. Deploying Web Services

DirX Identity provides several Web Services which can be deployed into an Apache Tomcat Web container. The Tomcat Web container can be a separate, stand-alone Web container or the container embedded into the IdS-J server (embedded Tomcat). The IdS-J server contains a built-in (embedded) Tomcat service with default port 40.000.

Note that when you deploy them into the IdS-J server container, they are started and stopped together with the server. The operation of an external Tomcat web server as a service is out of scope of this manual.

1.1.8. Determining the Account for Configuration on Linux Platforms

The appropriate permissions are required to perform the configuration of your DirX Identity installation on Linux platforms. Superuser permissions are always sufficient.

However, if you intend to run configuration tasks as the DirX Identity installation account, you must ensure that the following conditions are satisfied:

- **Conditions regarding the Tomcat installation.** If you are going to deploy DirX Identity

Web Applications, you must ensure that the DirX Identity installation account has read, write and execute access to the Tomcat installation directory and that these subdirectories of the Tomcat installation are present:

- conf/Catalina/localhost
- work/Catalina/localhost

You can satisfy these requirements by:

- Logging in as the DirX Identity installation account and then installing Tomcat into a subdirectory of the DirX Identity installation account; or:
- Installing Tomcat using some other account or as superuser and then changing the permissions for the directories listed above. The permissions must be **775** if there is a Linux group of which both the Tomcat account and the DirX Identity installation account are members. Otherwise, the permissions must be **777**.
- **Conditions regarding the LDAP directory installation:**
- Superuser permissions are always required for configuration tasks.
- The home directory of the DirX installation must be readable and executable for group members.
- A Linux group must be defined so that both the DirX installation account and the DirX Identity installation account are members of this group.

1.1.9. Accounts for Tomcat and DirX Identity Installations (Linux Platforms Only)

If you are going to deploy DirX Identity Web Applications, you must ensure that the Tomcat installation account has read and write access to the **password.properties** files of the related Web Applications (for example, Web Center). Options for completing this task are:

- Install Tomcat as superuser.
- Define a Linux group so that both the Tomcat installation account and the DirX Identity installation account are members of this group.
- Log in as the DirX Identity installation account and then install Tomcat into a subdirectory of the DirX Identity installation account.

2. Installation on a Single Machine

To install all DirX Identity components on a single machine:

1. Install a directory server on the local machine (use the native tools to perform this step).
2. Install Tomcat on the local machine. During installation, select the Windows Service on Windows platforms. Refer to the release notes regarding supported Tomcat versions and the suitable Java environment and satisfy these prerequisites for the Tomcat used for your DirX Identity installation.
3. Run the DirX Identity installation procedure (see chapter "Installing DirX Identity"):
    - In the **Choose Licensed Features Set** dialog select the set of features you have licensed, according to the description of that dialog in the chapter "Install DirX Identity".
4. Run the DirX Identity configuration procedure (see the chapter "Configuring DirX Identity"):
    - In the **Configuration Options** dialog, select Connectivity Schema and Data Configuration, Domain Configuration, Provisioning Schema and Data Configuration, ActiveMQ Message Broker Configuration, C++-based Server Configuration, Java-based Server Configuration, Server Admin (including Java-based Supervisor) Configuration, Manager Configuration, Supervisor Configuration, Web Center Configuration, **Web Center for Password Management Configuration** (if you have installed this component)
    - Please note: Selecting the step **Server Admin (including Java-based Supervisor) Configuration** deploys this functionality into a Java-based Server being configured on the same machine and is possible only when you have installed the related High Availability component **Server Admin** and have selected Java-based Server Configuration. See the *Use Case Description High Availability* for details.
    - Fill out the entire subsequent configuration dialogs.
5. Extend the directory schema as required.

Now your system is ready to run.

3. Installing DirX Identity

This chapter describes how to install and un-install DirX Identity.

3.1. Installation

This section describes how to run the DirX Identity installation procedure to install the DirX Identity software on a machine.

3.1.1. General Remarks

For each successful installation / un-installation, a record is written to the file
*install_path***/install_history.txt**
providing information about

- Date of installation / un-installation
- DirX Identity version
- Name of user performing the installation / un-installation
- Installed components

For each successful installation, there is a related installation log file *install_path***/_DirX_Identity_***version***_Install_***timestamp***.log**.

For each successful uninstallation, there is a related uninstallation log file *install_path***/_DirX_Identity_***version***_Uninstall_***timestamp***.log**.

3.1.1.1. Windows Instructions:

To install, configure and run DirX Identity or any of its patches, consider the following issues resulting from the User Access Control (UAC) functionality introduced with these operating system versions. With UAC, Microsoft introduced a technique to "elevate" a user "on flow" from a standard to an administrative user by letting a standard user "explicitly confirm" when trying to perform an administrative task, like writing to the registry, creating, editing or deleting files and so on. UAC is active by default to prevent the system from unauthorized user manipulation.

Because this explicit confirmation cannot be done at any time during Installation and Configuration, you must:

- Put the logged in user account to the Local Administrators (Windows Client) - or the Administrators (Windows Server) group
- Disable UAC during Installation and Configuration and turn it on again afterwards if you want to.

Another issue besides UAC to be considered is the access rights required on the installation folder and subfolders. You no longer automatically need to have the read, write and create files rights on each installation subfolder even if you are a member of the Administrators group. To get these rights, you can:

- Install DirX Identity under a different path (for example, C:\My_Program Files…) from the default path (C:\Program Files…), or
- Take the default path and explicitly set those rights on the subfolders (Properties → Security → Permissions) for the logged-in user where configuration files need to be edited or temporary files or log files need to be created, or
- Always open a DOS command prompt with administrative rights if you want to edit or delete a file in a specific subfolder.

3.1.1.2. Linux Instructions:

The login name of a Linux user determines the destination folder for installation. The folder is *userID_home_directory***/DirX/Identity**, where *userID_home_directory* is the home directory of the specified account. For the DirX Identity package you can use any account which is different from the account that is used for DirX Directory Server. The user ID must exist before you perform the installation procedure.

A graphical and a command-line based (console mode is default) installation procedure is available.

The following description shows the **graphical installation procedure**. The screenshots are taken on Windows. The look on Linux is slightly different.

During the graphical installation mode, you can click **Cancel** at any time to leave the installation program. You can click **Previous** at any time to return to a previous dialog.

Console mode mimics the default GUI steps provided by InstallAnywhere and uses standard input and output. X-Windows (X11) is not necessary to run the DirX Identity installation in console mode. Console mode outputs text to the console line-by-line. It does not allow for any formatting, clearing of the screen, or positioning of the cursor. The console mode information is almost identical to the graphical display. Thus, it is not listed in this manual.

During this mode, you must respond to each prompt to proceed to the next step in the installation. If you want to go back to a previous step, type 'back'. You may cancel the console installation at any time by typing 'quit'.

3.1.2. Starting the Installation

Before performing an update / upgrade installation, you need to perform these steps:

- Stop all running workflows (disable scheduling, shutdown event managers). You can use the maintenance scripts to perform this task.
- Stop all DirX Identity services and user interface components, including the Tomcat Services into which you deployed DirX Identity components.

3.1.2.1. Windows Instructions:

To install DirX Identity on Windows Server:

- Log on as administrator.

- With Windows Explorer, navigate to **\Installation\DirXIdentity\Windows\Server** on the DVD.
- Double-click **dirxidty.exe**.

3.1.2.2. Linux Instructions:

To install DirX Identity:

1. Log in as a Linux user.
2. Insert the DVD for your Linux system. The system mounts it automatically.
3. Open a shell.
4. Perform the command
   cd /*mount_point***/Installation/DirXIdentity/Linux/Server**.
5. Start the installation:

   To perform the graphical installation routine, type

   - **sh ./dirxidty.bin –i gui**

   To trigger a console installer from the command line, type the following command:

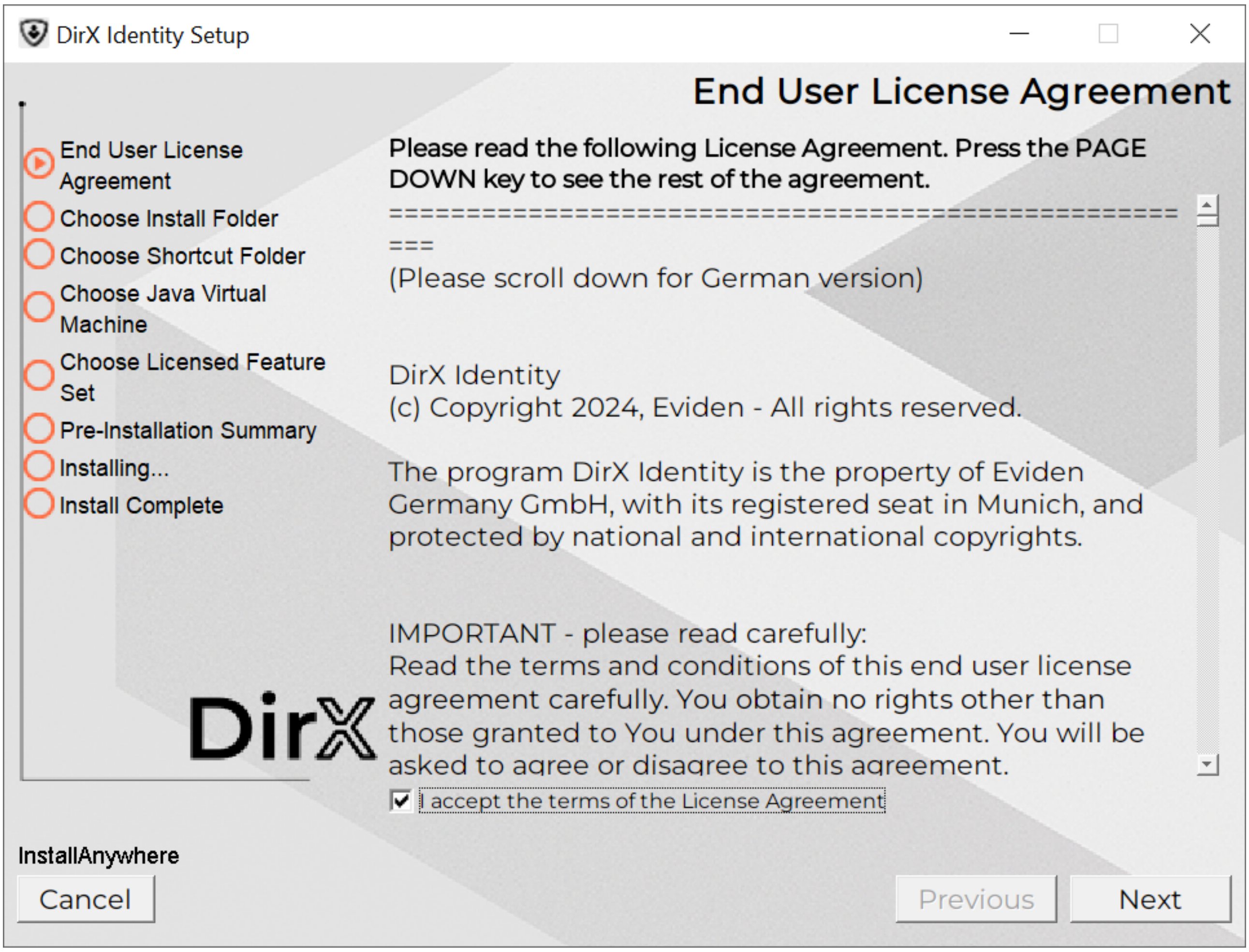
   - **sh ./dirxidty.bin**
     or
   - **sh ./dirxidty.bin –i console**

This is the default Linux installer UI mode.

3.1.3. Graphical Installation Procedure

3.1.3.1. License Information Dialog

Setup displays a License Information dialog:



DirX Identity Setup

End User License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

==
===

(Please scroll down for German version)

DirX Identity
(c) Copyright 2024, Eviden - All rights reserved.

The program DirX Identity is the property of Eviden Germany GmbH, with its registered seat in Munich, and protected by national and international copyrights.

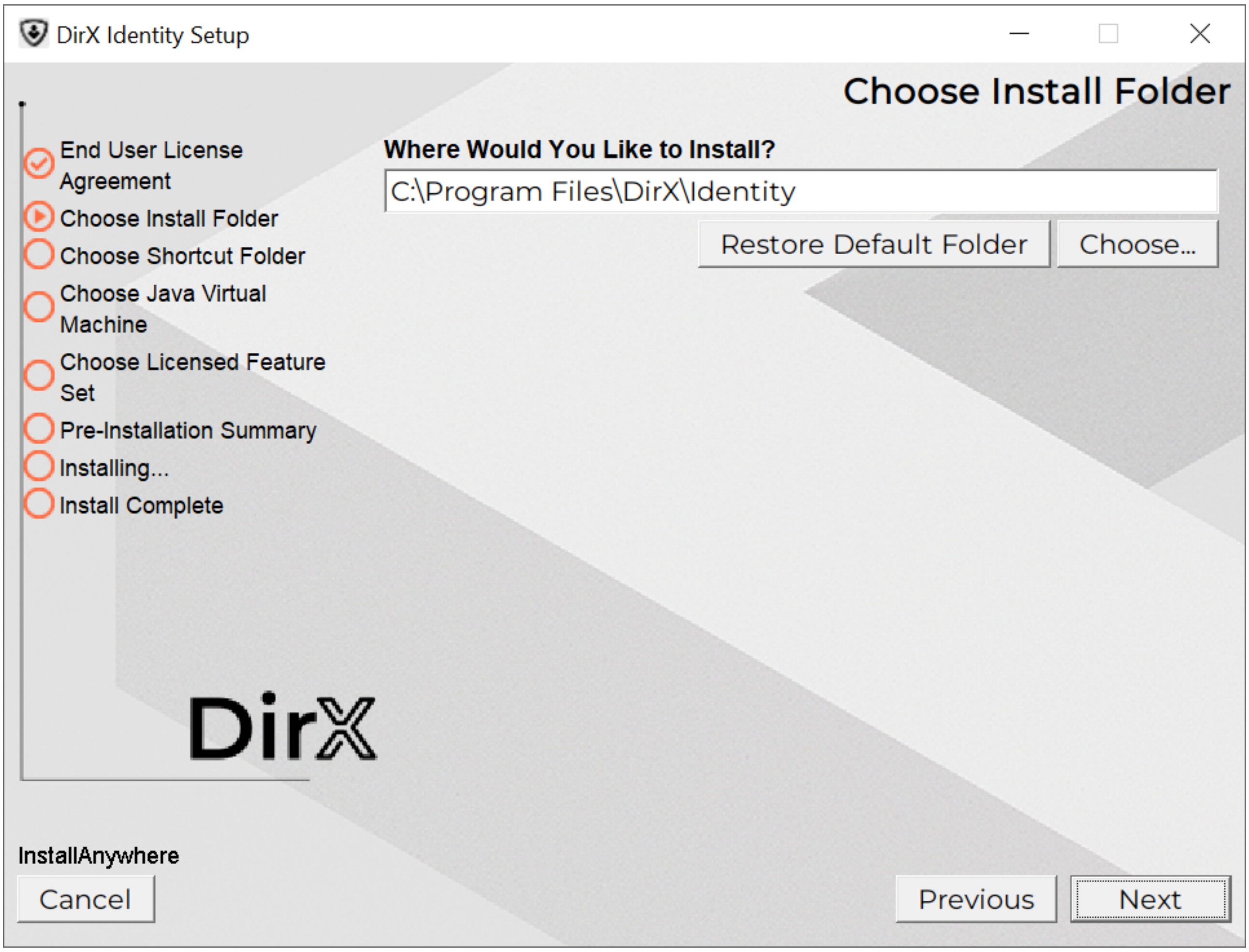
IMPORTANT - please read carefully:
Read the terms and conditions of this end user license agreement carefully. You obtain no rights other than those granted to You under this agreement. You will be asked to agree or disagree to this agreement.

☑ I accept the terms of the License Agreement

- Read the licensing information, select **Yes** if you agree and then click **Next**.

3.1.3.2. Choose Installation Folder Dialog (Windows only)

Setup presents this dialog when you are installing DirX Identity for the first time or if you have previously uninstalled it. Otherwise, Setup takes the installation path from the Windows registry, and you cannot change it.



DirX Identity Setup

Choose Install Folder

- End User License Agreement
- Choose Install Folder
- Choose Shortcut Folder
- Choose Java Virtual Machine
- Choose Licensed Feature Set
- Pre-Installation Summary
- Installing...
- Install Complete

Where Would You Like to Install?

C:\Program Files\DirX\Identity

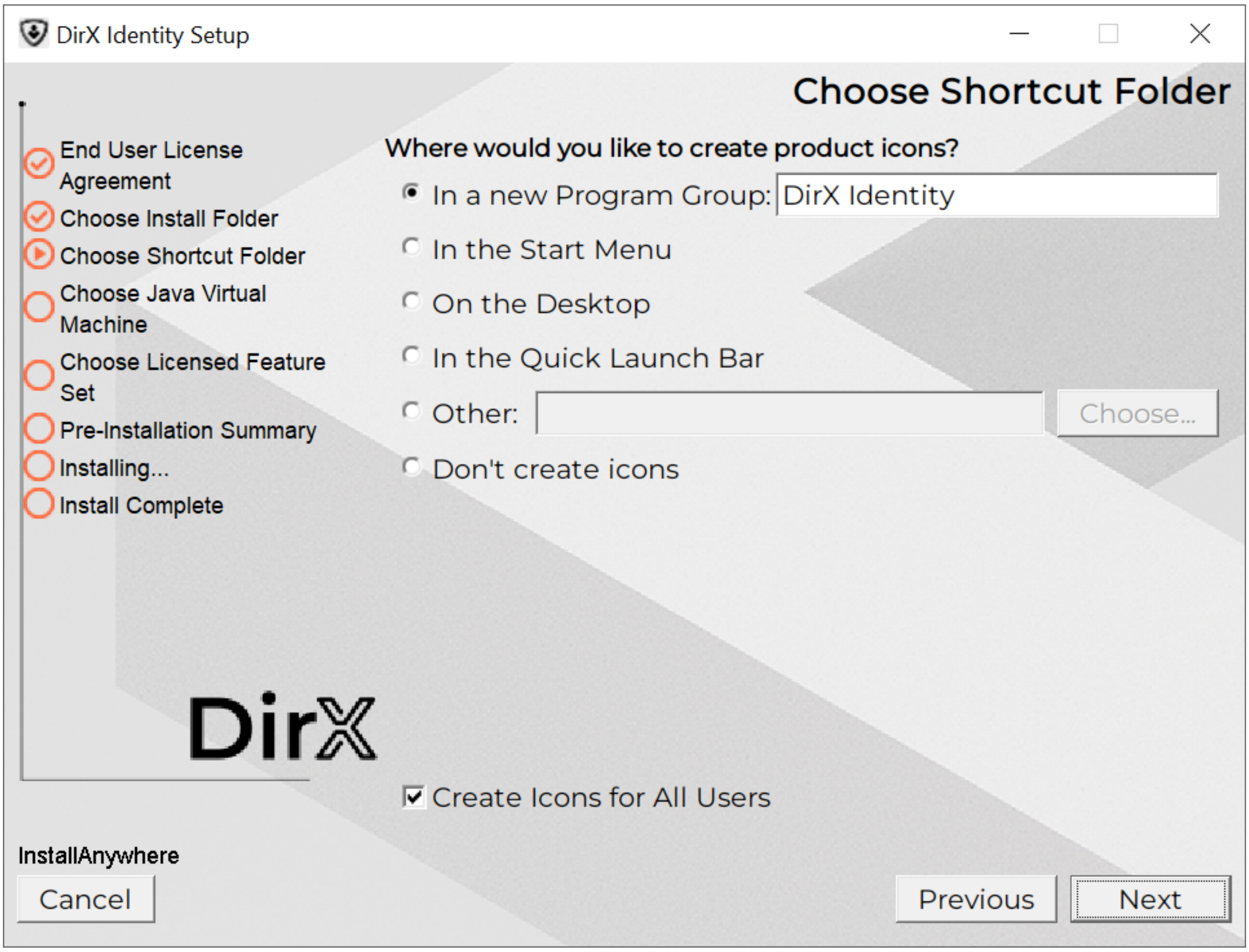
The default installation folder is *ProgramFiles***DirX\Identity**. The Windows system variable **ProgramFiles** contains the fully qualified name of the folder defined by Windows to store applications.

In this dialog, you can:

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

3.1.3.3. Choose Shortcut Folder Dialog (Windows only)

The Choose Shortcut Folder dialog allows you to select a program group for DirX Identity.


DirX Identity Setup

Choose Shortcut Folder

- End User License Agreement
- Choose Install Folder
- Choose Shortcut Folder
- Choose Java Virtual Machine
- Choose Licensed Feature Set
- Pre-Installation Summary
- Installing...
- Install Complete

Where would you like to create product icons?

● In a new Program Group: DirX Identity

○ In the Start Menu

○ On the Desktop

○ In the Quick Launch Bar

○ Other: Choose...

○ Don't create icons

☑ Create Icons for All Users

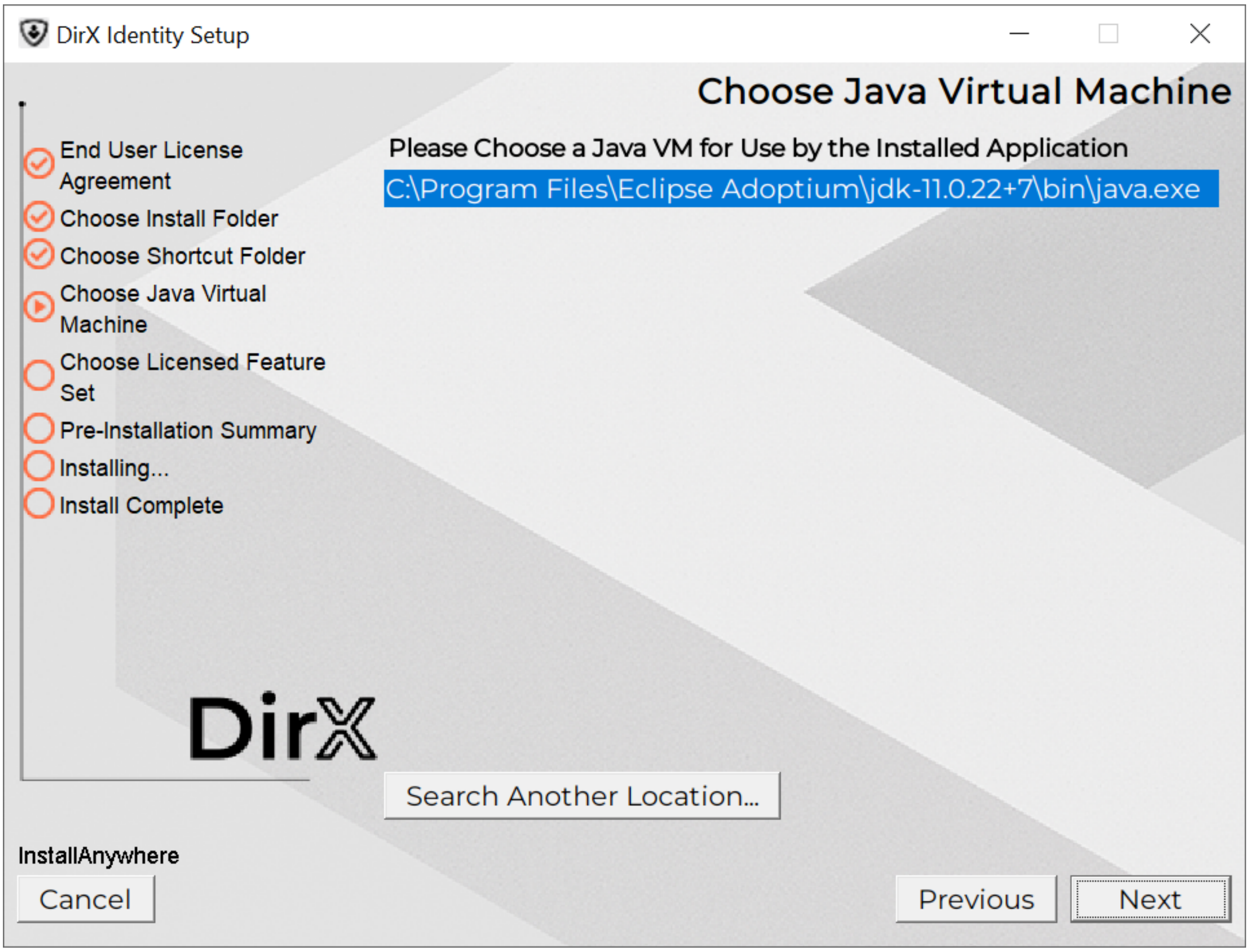
In this dialog, you can:

- Click **Next** to select the default program group.
- Click **In a new Program Group** and select a program group, and then click **Next**.
- Click **In the Start Menu**, and then click **Next**.
- Click **On the Desktop**, and then click **Next**.
- Click **In the Quick Launch Bar**, and then click **Next**.
- Click **Other** and then **Choose…** to select another program group, and then click **Next**.
- Click **Don’t create icons**, and then click **Next**.

Additionally, you can deselect the option **Create Icons for All Users.**

3.1.3.4. Choose Java VM Dialog

Setup presents this dialog.



DirX Identity Setup

Choose Java Virtual Machine

Please Choose a Java VM for Use by the Installed Application

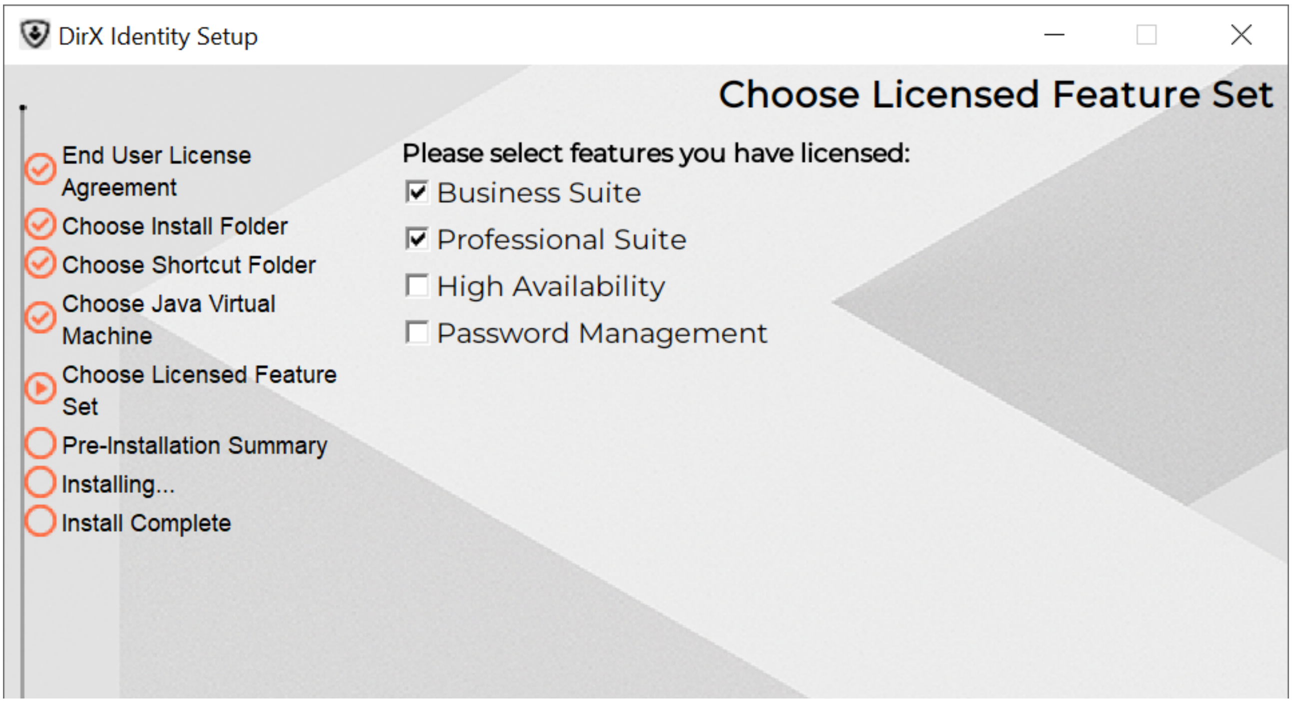
C:\Program Files\Eclipse Adoptium\jdk-11.0.22+7\bin\java.exe

In this dialog, you can select the Java environment to be used for all the DirX Identity processes not hosted by a Apache Tomcat Web Server. To make the appropriate selection, you should read the chapter “The Java for DirX Identity”. You can:

- Select one of the presented Java 11 VMs.or by clicking **Search another location** you can choose a path of a Java 11 VM. You must choose the home directory.
- Click **Next** to confirm your selection.

3.1.3.5. Choose Licensed Features Set Dialog

In the Choose Licensed Features Set dialog you have to check the features you have licensed:



DirX Identity Setup

Choose Licensed Feature Set

Please select features you have licensed:

☑ Business Suite

☑ Professional Suite

□ High Availability

□ Password Management

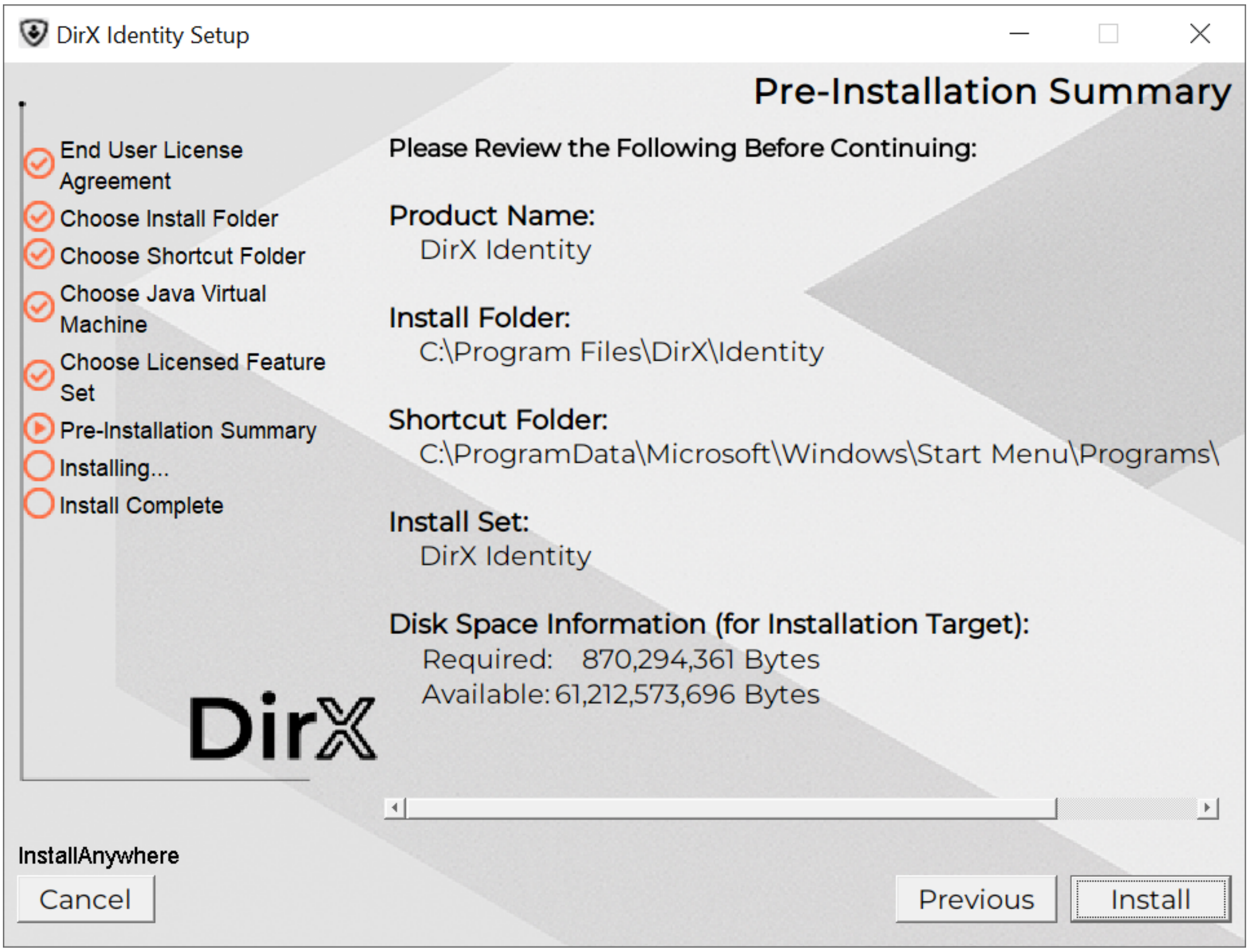
Select only the features you have licensed. The selection affects the selectable components in the subsequent **Choose Install Set Dialog.** The following list shortly explains the relevant feature list:

- **Business Suite** – This license entitles you to install the core functionality of the product and the basic connectivity packages. Note that for other connectivity packages you need additional licenses.
- **Provisioning Suite** - This license entitles you to install the **Pro Suite Upgrade** to the Business Suite.
- **High Availability** - This license is an add-on to the Business Suite and entitles you to install the High Availability components.
- **Password Management –** Select this box, if you have Password Management either as an add-on to the Business Suite or as a standalone license. It includes the necessary components from the Business Suite and additional components only available with Password Management.

Revise your selection carefully. Once you proceed to the next step, this selection is read-only and you have to restart the Installation procedure in order to correct this selection. Click **Next** to confirm your selection.

3.1.3.6. Pre-Installation Summary Dialog

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



Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name:
DirX Identity

Install Folder:
C:\Program Files\DirX\Identity

Shortcut Folder:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\

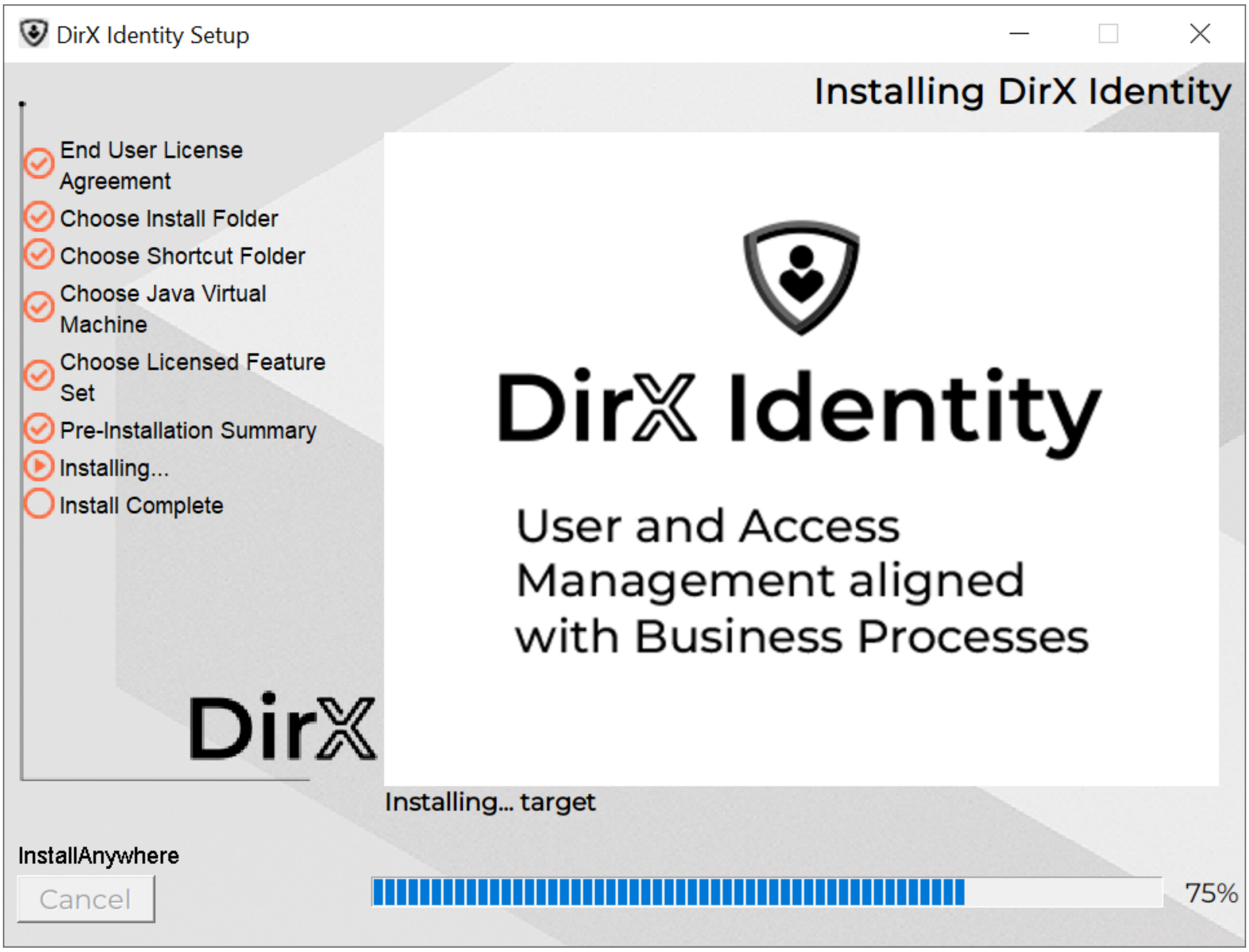
Install Set:
DirX Identity

Disk Space Information (for Installation Target):
Required: 870,294,361 Bytes
Available: 61,212,573,696 Bytes

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

3.1.3.7. Installing…

Setup displays the Installing… dialog, for example:



DirX Identity Setup

Installing DirX Identity

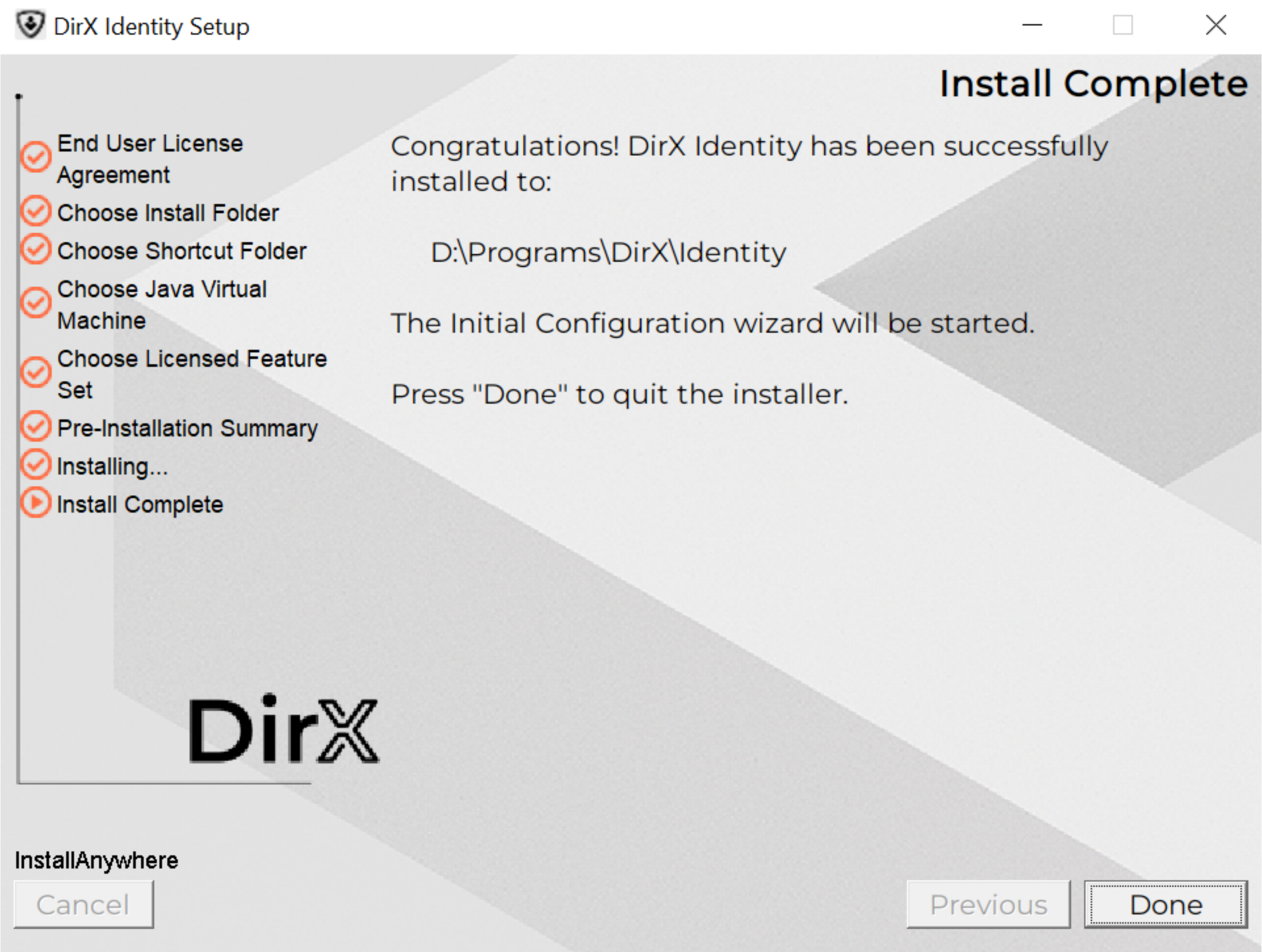
End User License Agreement
Choose Install Folder
Choose Shortcut Folder
Choose Java Virtual Machine
Choose Licensed Feature Set
Pre-Installation Summary
Installing...
Install Complete
DirX
DirX Identity
User and Access Management aligned with Business Processes
InstallAnywhere
Cancel

Installing... target

75%

3.1.3.8. Setup Complete

Setup displays this dialog if you are installing DirX Identity and no errors occur:



DirX Identity Setup

Install Complete

- End User License Agreement
- Choose Install Folder
- Choose Shortcut Folder
- Choose Java Virtual Machine
- Choose Licensed Feature Set
- Pre-Installation Summary
- Installing...
- Install Complete

Congratulations! DirX Identity has been successfully installed to:

D:\Programs\DirX\Identity

The Initial Configuration wizard will be started.

Press "Done" to quit the installer.

- If the dialog indicates successful installation without errors as above, then click **Done** to quit the installer.
- Otherwise, check the *DirX Identity Troubleshooting Guide* for a solution to the problem if the installation result is different from the **Setup Complete** dialog above; for example, because it contains a text like **The installation of Atos DirX Identity is complete, but some errors occurred during the install. Please see the installation log for details**.

3.1.3.9. Completing the installation

After installing DirX Identity, the Initial Configuration wizard must be started to prepare the product for the first use. The Initial Configuration wizard is started automatically after a successful installation. Alternatively, it can be manually started using its Start Menu shortcut or launcher.

3.1.4. Environment Variable Settings

The environment variable PATH will be expanded with *install_path*/**bin**.

The environment variables DIRXMETAHUB_INST_PATH, and DIRXIDENTITY_INST_PATH will be set to *install_path*. For Windows platforms, this will be done defining or extending the related system environment variables.

For Linux platforms, this will be done by changing the profile of the user.

Before changing the profile of the user a backup will be created,
for example *userID_home_directory***/.profile***number*.

Remove these files by hand, if necessary.

For Linux platforms, DXI_JAVA_HOME will be set to *dxi_java_home*.

For Windows platforms, a script *install_path*/**setdxienv.bat** will be created which contains the settings for DXI_JAVA_HOME as *dxi_java_home* (Windows notation).

3.2. Uninstallation

The uninstallation process performs the following tasks:

- Removes the DirX Identity part from the path variable.
- Deletes the variable s DIRXMETAHUB_INST_PATH, DIRXIDENTITY_INST_PATH.
- Removes all installed files.

To uninstall DirX Identity, perform these steps:

Windows Instructions:

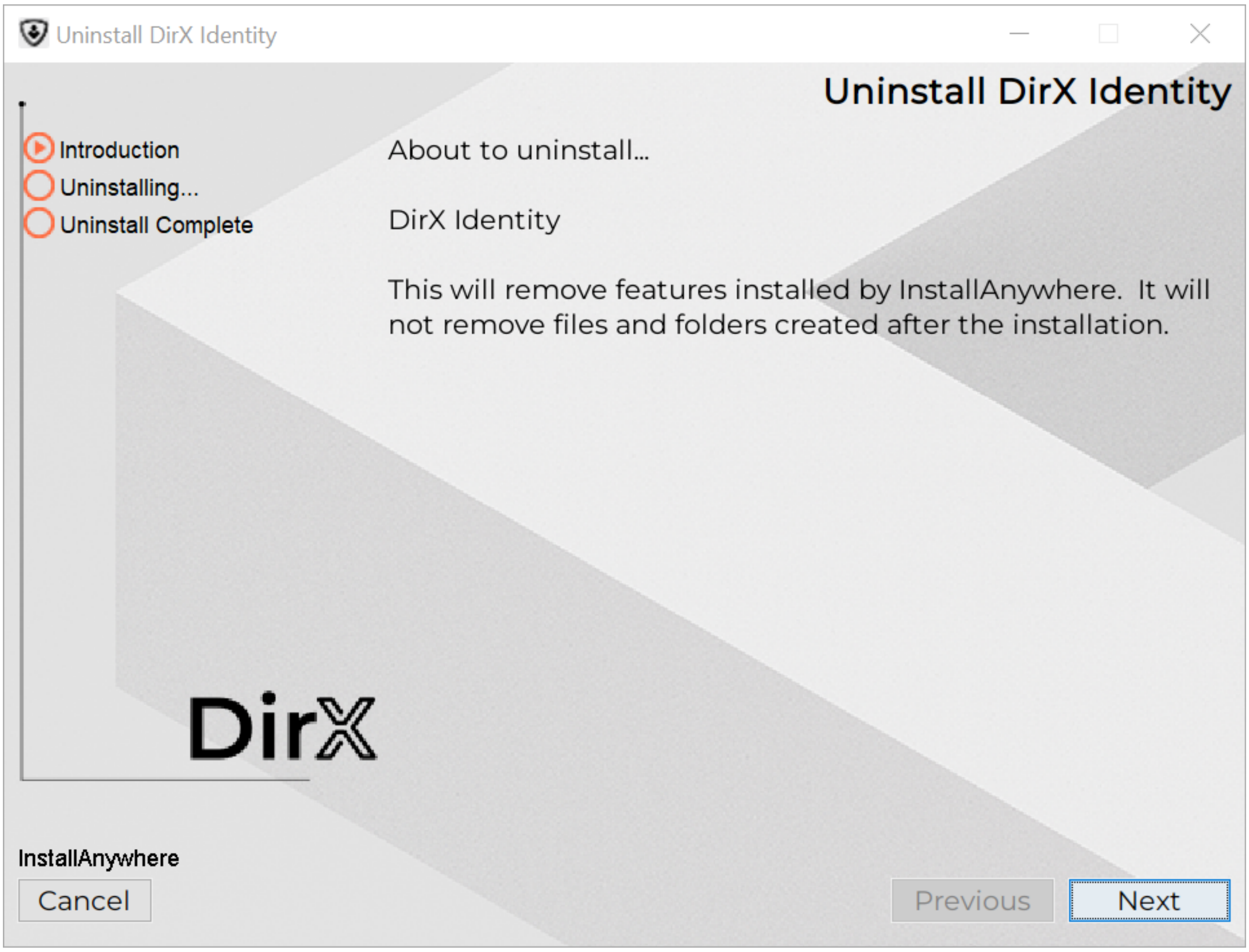
- Open the Windows option for uninstalling software on your computer. Depending on the operating system on your computer, it is **Add or Remove Programs** or **Programs and Features**.
- Look for the entry **Atos DirX Identity** *version* and select it.
- Click **Change / Remove**

Linux Instructions:

- Log in as Linux user.
- Perform **cd** *install_path**/UninstallerData*
for example *userID_home_directory***/DirX Identity/UninstallerData**
- For graphical installation mode, type:
sh ./Uninstall_DirX_Identity -i gui
- For console mode, type:
sh ./Uninstall_DirX_Identity

If un-configuration has not yet been performed, the un-installation process starts the Configurator in un-configuration mode for un-configuring DirX Identity. Then the introduction dialog is displayed.

Introduction Dialog



Uninstall DirX Identity

About to uninstall...

DirX Identity

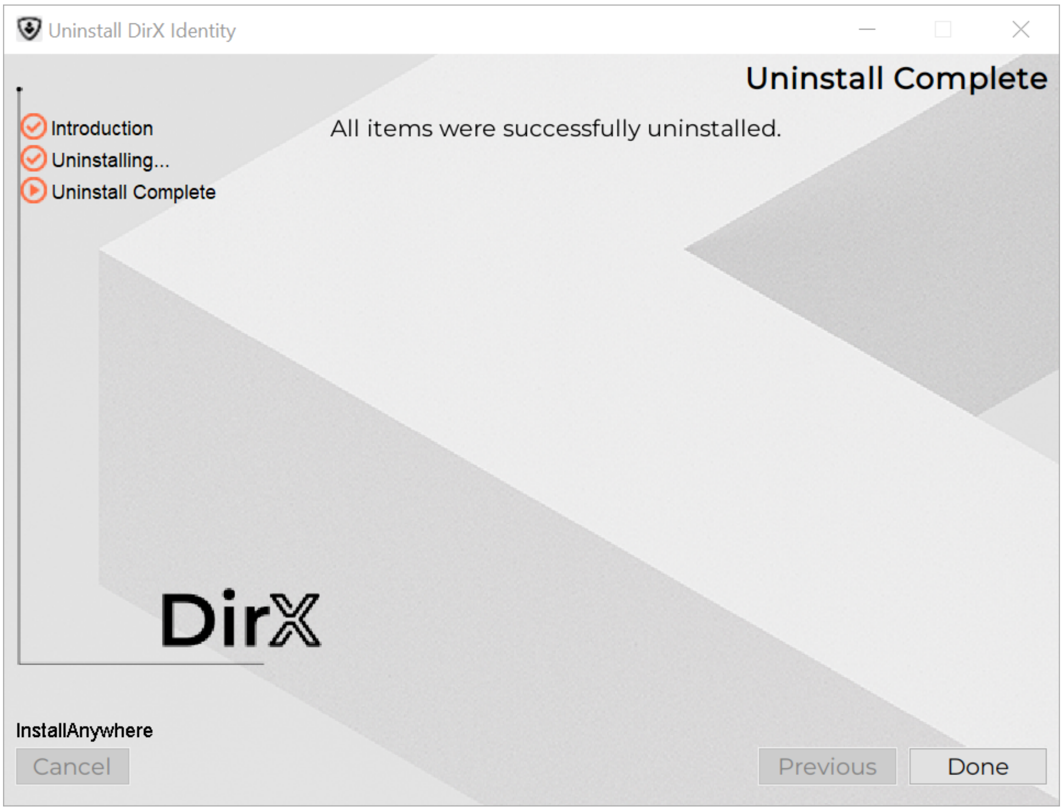
This will remove features installed by InstallAnywhere. It will not remove files and folders created after the installation.

- Click **Uninstall** to start the un-installation program. Only the software shall be removed from your computer
- Click **Cancel** to leave the un-installation program.

After un-installation, un-configuration including removal of the database is no longer possible.

Please run the configuration tool before uninstalling.

Uninstall Complete Dialog



Uninstall Complete

All items were successfully uninstalled.

The un-installation procedure has successfully removed DirX Identity from your computer.

- Click **Done** to exit the installer.

3.3. Additional instructions for Linux

The following instructions must be carried out after installation of the product:

- Relevant for Linux platforms only: If the DirX Identity installation account has been created so that the login shell is **bash**, then you need to ensure that the file **.profile** in the related home directory will be executed with each login and each startup of a graphical session. The technical background is that at login time, the files **.bash_profile, .bash_login, .profile** are accessed exactly in this order and that only the first readable file in this list is evaluated. One option for accomplishing this task is to perform these steps:
- Append the statement **. ~/.profile** to your **.bashrc** file.
- Add the statement **. ~/.bashrc** to your **.bash_profile** file if not yet done.
- Any login as the DirX Identity installation account must be redone in order to work with the correct environment settings.

3.4. Update Installation

There are two ways to update a DirX Identity Installation:

- Method 1: Un-configure and uninstall DirX Identity completely, and then perform a new installation and Initial Configuration.

- Method 2: Perform an installation on your existing DirX Identity installation. Select all components you installed during the previous installation. The files are set up as new and all configuration files are saved. Then perform an Initial Configuration.

3.5. Silent Installation

You can install DirX Identity on a machine without interaction. Follow these steps to create a silent setup:

- Copy the content of the folder **DirXIdentity/Server** from the DVD to a folder on your machine.
- Customize the file **dirxidty.properties**.
- Start the installation program in the folder on your machine.
- Check for errors

The file **dirxidty.properties** looks like this:

```
…

# UI mode for the installer
# INSTALLER_UI=[SILENT | CONSOLE | GUI]

# Default for Windows: GUI
# Default for Unix: CONSOLE

######################################################################
#########
#
# DirX Identity specific installation properties
#
######################################################################
#########

# Installation path for DirX Identity
# PROP_USER_INSTALL_DIR=<path>

# Default for Windows:
# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$DirX$/$Identity

# Default for Linux:
# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$DirX_Identity

# Note for Windows:
```

```
# If an existing installation path for DirX Identity is found in the
registry
# then this path will be used for the installation, and it cannot be
overridden
# with the PROP_USER_INSTALL_DIR property

# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$Atos$/$DirX Identity

#
---------------------------------------------------------------------
-------

# Shortcut group for DirX Identity
# PROP_USER_SHORTCUTS=<shortcut group>

# Default:
# PROP_USER_SHORTCUTS=$WIN_COMMON_PROGRAMS_MENU$$/$DirX Identity

# Note for Windows:
# If an existing shortcut group for DirX Identity is found in the
registry
# then this shortcut group will be used for the installation, and it
cannot be
# overridden with the PROP_USER_SHORTCUTS property

#
---------------------------------------------------------------------
-------

# Selected licenses for DirX Identity

# Apply selected licenses: the selected license values will be
applied if
# PROP_SET_LICENSES is set to 1
PROP_SET_LICENSES=1

# Selected licenses
# <license>=[1 | 0]
# 1: License will be selected
# 0: License will be not selected

PROP_LIC_Business_Suite=1
```

```
PROP_LIC_Professional_Suite=1
PROP_LIC_HighAvailability=0
PROP_LIC_PwdMgmt=0

#
---------------------------------------------------------------------
-------

# Selected Java environment
# PROP_SELECTED_JRE=<path to existing JDK or JRE>

# Example for Windows:
# PROP_SELECTED_JRE=C\:\\Program Files\\Java\\java-17
# Example for Linux:
# PROP_SELECTED_JRE=/opt/java-17

#
---------------------------------------------------------------------
-------

# Restart Windows - applicable for (un-)installation in silent mode
# Note:
# The following property can be used to force restarting the computer
after the
# installation has been completed

# PROP_RESTART_NEEDED=YES

#
---------------------------------------------------------------------
-------

# Skip configuration after restart
# Note:
# The following property can be used to skip starting the Initial
Configuration
# Wizard after the next restart of the computer

# PROP_SKIP_CONFIG_AFTER_RESTART=YES

#
---------------------------------------------------------------------
```

```
-------
```

Change the line INSTALLER_UI=swing to INSTALLER_UI=SILENT.

Customize the PROP_LIC_… values according to the features you have licensed, specifying value **1** for features you have licensed and value **0** for features you have not licensed.

Change (and uncomment) the PROP_ … values in the section starting **# Install features for DirX Identity** if you will not use the default settings.

For selection of an already JRE for DirX Identity, customize and activate the setting for the property **PROP_SELECTED_JRE** according to the inline comments above.

The next de-installation after a silent installation runs in silent mode.

4. Configuring DirX Identity

This chapter describes how to configure DirX Identity on all available platforms. The Configurator serves different purposes:

- It can perform a complete initial configuration. (This part is automatically presented after an installation on Windows).
- The customer can perform a reconfiguration at any time; for example, to create a new domain.
- During un-installation or when executed by user request, it can perform an un-configuration.

4.1. Starting the Configuration

The configuration is based on the content in the file:

install_path/**configuration.ini**

This file determines the components and agents to configure and contains the passwords for a silent configuration.For details about the **configuration.ini** file see "Silent Configuration / Un-configuration".

> *Windows*
>
> - With the operating systems Windows 2008 and Windows 7 (Vista), Microsoft introduced a new technique called User Access Control (UAC) to "elevate" a user "on the flow" from a standard to an administrative user by letting a standard user "explicitly confirm" when trying to perform an administrative task, for example writing to the registry. Because this explicit confirmation cannot be performed at several situations while the Configurator is running, either put the user who is running the Configurator to the local administrator group, start the **InitialConfiguration.bat** / **Configuration.bat** with "run as Administrator" or disable UAC during configuration.

> *UNIX*
>
> - Normally, superuser permissions are required for starting the configuration. However, if the conditions described in "Determining the Account for Configuration on UNIX platforms" are satisfied, then a login as the DirX Identity installation account is sufficient for starting the configuration. However, if you have once started the configuration as superuser, then subsequent runs of the configuration / un-configuration must be performed as superuser, too.
> - **For Linux platforms only**: Setting and exporting the environment variable LD_ASSUME_KERNEL (value 2.4.19) is no longer required and is incorrect. Undo this setting if it is still active in your environment.

4.1.1. Initial Configuration

After finishing the installation, you must configure DirX Identity with the DirX Identity Initial Configuration Wizard.

4.1.1.1. Windows Platforms

You can start the initial configuration wizard on Windows platforms at any time:

Run **Start** → **Programs** → **DirX Identity** → **Initial Configuration**

ℹ This tool is located on Windows platforms in *install_path**bin*. The syntax of the tool is as follows:

InitialConfiguration.bat

At the end of an update installation, the Initial Configuration Wizard starts automatically.

4.1.1.2. Linux Platforms

You must start the initial configuration wizard on Linux platforms by hand.

Note: This tool is located in *install_path***/bin**:

InitialConfiguration.sh

4.1.2. Configuration

You can re-configure DirX Identity at any time; for example, to create a new domain.

4.1.2.1. Windows Platforms

You can start the reconfiguration wizard via:

Run **Start** → **Programs** → **DirX Identity** → **Initial Configuration**

Or if you only want to re-configure the Java-based Server and / or Web Center:

Run **Start** → **Programs** → **DirX Identity** → **Configuration**

ℹ The configuration tool is located in *install_path***\bin**. The syntax of the tool is as follows:

Configuration.bat *type mode* [*Java-based_server_configuration_file*]

where

type is one of the following values

- **InitialConfiguration** - Performs all initial configuration steps.
- **Configuration** - (default value) Performs configuration steps for the Java-based Server

and / or the Web Center.

- **UnConfiguration** - Performs an un-configuration.

mode is one of the following values:

- **normal** - (default value) The configuration runs in interactive mode.
- **silent** - The configuration runs in silent mode. (See "Silent Configuration / Un-configuration" for details.)

Java-based_server_configuration_file is the name of the configuration file containing the properties of the Java-based Server to be configured. (See "Java-based Server" for details about this file.) You can specify only one *Java-based_server_configuration_file*. It must be located in *install_path*/bin**. If you want to specify this parameter, you must specify all parameters in the correct order. You must perform the configuration tool for each Java-based Server you want to configure.

If *Java-based_server_configuration_file* is specified, the Configurator reads the Java-based Server properties from there. If no such file is specified, the values are read from **configuration.ini** as usual. The configured values - in **normal** mode, the user can change the pre-configured values - are written back to the **configuration.ini** file. The optional Java-based Server configuration file is only used for reading but never for writing.

If you want to run the configuration with parameters, run it as administrator in a command prompt window or from a shell script.

4.1.2.2. Linux Platforms

You can start the re-configuration wizard on Linux platforms by hand.

> ℹ This tool is located in *install_path*/**bin**:

Configuration.sh

4.1.3. Un-Configuration

Un-configuration can be performed before un-installation.

The un-configuration process performs the following tasks:

- Work Path and Status Path Deletion

Removes all files in the work and status folders.

- DirX Identity C++-based Server for Un-configuration

Unregisters the DirX Identity agents from the connectivity configuration directory and removes the C++-based Service on Windows platforms.

- DirX Identity Java-based Server for Un-configuration

Removes the Java-based Service on Windows platforms.

- Web Center Un-configuration for Tomcat

Uninstalls the Web Center component from the Tomcat installation folder.

- Web Center for Password Management Un-configuration for Tomcat

Uninstalls the Web Center for Password Management component from the Tomcat installation folder.

4.1.3.1. Windows Platforms

Un-configuration is requested during un-installation.

Manual un-configuration should not be necessary but can be performed.

This tool is located in *install_path***bin**:

UnConfiguration.bat

4.1.3.2. Linux Platforms

You must start the de-configuration wizard on Linux platforms by hand.

Note: This tool is located in *install_path*/**bin**:

UnConfiguration.sh

> If you have integrated the DirX Identity start/stop scripts into the Linux operating system (see the section "Integrating Start/Stop Scripts into the Linux Operating System"), you must undo these integration actions (see the subsection "Undoing the Integration") before un-installing the product.

4.2. Using the Configurator

This section provides information about all possible steps of the Configurator.Some steps contain exceptions for the different modes (initial configuration, configuration, un-configuration).

After startup, the Configurator shows the welcome screen.

4.2.1. Welcome Dialog

The first comment line provides information about the configuration type (initial configuration or configuration mode).

- Click **Next** to go to the next step.

The configuration wizard is built similar to the DirX Identity wizards, with all steps shown on the left side and title and help information shown on the right side.

Buttons at the bottom allow you to navigate in the wizard. You can use **Next** to step forward and **Previous** to step backwards. **Cancel** allows you to end the wizard operation at any time and **Finish** is enabled at the point where parameter settings are complete (all buttons in the navigation pane are green).

4.2.2. Configuration Options

The set of options for the **Configuration Options** dialog is:

- Connectivity Schema and Data Configuration

This component extends the LDAP directory server's schema with the DirX Identity connectivity data model and imports the connectivity configuration as follows:

- Creates the DirX Identity object classes
- Creates the DirX Identity attribute types
- Creates the DirX Identity name forms
- Creates access control and subschema subentries within the administrative areas

Within the administrative areas, subentries for access control and subschema are created. (See the section "Schema and Content Handling" for details.)

This configuration component has the following prerequisite:

- The directory server must be present on the local machine and running.

> The configuration procedure deletes and adds objects classes. If you have already used these object classes and have extended them, the content could be lost. In this case, you cannot use the delivered script. You must update the schema by hand.

- Provisioning Schema and Data Configuration

This component configures the provisioning schema and the system domain.

The Directory Schema extension extends the LDAP directory server's schema with the Provisioning data model, as follows:

- Creates the Provisioning object classes
- Creates the Provisioning attribute types
- Creates the Provisioning name forms
- Creates an administrative area for the Provisioning system domain
- Creates access control and subschema subentries within the administrative area

Within the administrative area, subentries for access control and subschema are created.

This configuration component has the following prerequisites:

- The directory server must be present on the local machine and running.
- The Connectivity Schema and Data Configuration must already exist or you must select the option.
- ActiveMQ Message Broker Configuration

This component configures the DirX Identity Message Broker (based on ActiveMQ) and starts it if the flag to start it after configuration is checked. This configuration component has the following prerequisites:

- The Connectivity Schema and Data Configuration must have been performed or you must select the option.
- C++-based Server Configuration

This component configures the DirX Identity C++-based Server and starts it if the flag to start it after configuration is checked. It adds configuration information about the installed agents to the database containing the connectivity schema.

This configuration component has the following prerequisites:

- The Connectivity Schema and Data Configuration must already exist, or you must select the option.
- Domain Configuration

This component performs the configuration of a customer domain and/or the sample domain. If you select this step, the step Provisioning Schema and Data Configuration is automatically selected.

This configuration component has the following prerequisite:

- The directory server must be present on the local machine and running.

Here is more detailed information about the sample domain and the customer domain:

Sample Domain:

The sample domain My-Company is created. The set of installed data objects is a useful starting point to play with users, privileges, target systems and policies. The roles are not yet resolved to group memberships and account objects are not provided.

Customer Domain:

The customer domain with the provided name is created. An administrative area is created automatically.

During a single run of the Configurator, only one customer domain can be configured. For each customer domain, the initial folder structure, the configuration objects and some policies are provided.

If the customer domain already exists, this task replaces the configuration and system default data of the domain: default object descriptions and property page descriptions, system rules and operations. It does not modify the customer extensions.

For easy access, DomainAdmin profiles to access the domain via the DirX Identity Manager are created automatically if a Manager is or will be configured on this machine.

This configuration component has the following prerequisites:

- The directory server must be present on the local machine and running.
- The Provisioning Schema and Data Configuration option is automatically selected then and is disabled for deselection.
- Java-based Server Configuration

This component configures a DirX Identity Java-based Server to a specific domain and starts it if the flag to start it after configuration is checked.

This configuration component has the following prerequisites:

- The Provisioning Schema and Data Configuration must already exist or you must select the option.
- A Domain Configuration must already exist or you must select the option.
- Server Admin (including Supervisor-J) Configuration

This component deploys the Server Admin files from *install_path*/**ha/serverAdmin.org** to the embedded Java server tomcat to *install_path*/**ids-j-**_domain_**-S**_n_**/tomcat/webapps/serverAdmin**.

This configuration component has the following prerequisite:

- The Java-based Server Configuration option is automatically selected and is disabled for de-selection.
- Manager Configuration

This component creates and customizes the manager profile files in the installation directory *install_path*/**GUI/profiles**.

This configuration component has the following prerequisites:

- The **Connectivity Schema and Data Configuration** must already exist or you must select the option.
- The **Provisioning Schema and Data Configuration** must already exist or you must select the option.
- Web Center Configuration

This component configures the DirX Identity Web Center for Tomcat.

This configuration component has the following prerequisites:

- The **Provisioning Schema and Data Configuration** must already exist or you must select the option.

- Web Center for SAP NetWeaver Configuration

This component configures the DirX Identity Web Center for SAP NetWeaver and can only be chosen as an alternative to the Web Center Configuration.

> You must perform additional configuration steps manually.

- Web Center for Password Management Configuration

This component configures the DirX Identity Web Center for Password Management for Tomcat.

This configuration component has the following prerequisites:

- The **Provisioning Schema and Data Configuration** must already exist or you must select the option.
- Provisioning Web Service Configuration

This component configures the DirX Identity Provisioning Web Service for Tomcat.

This configuration component has the following prerequisites:

- The **Provisioning Schema and Data Configuration** must already exist or you must select the option.
- Identity REST Service Configuration

This component configures the DirX Identity REST Service for Tomcat.

This configuration component has the following prerequisites:

- The **Provisioning Schema and Data Configuration** must already exist or you must select the option.
- Business User Interface Configuration

This component configures the DirX Identity HTML5 Business User Interface for Tomcat.

This configuration component has the following prerequisites:

- The **Provisioning Schema and Data Configuration** must already exist or you must select the option.

Select the components or options you want to configure and click **Next**.

Note: The number of steps on the left side will be different depending on the options you have selected.

4.2.2.1. Linux Platforms

If **C++-based Server Configuration** is selected during an update configuration or un-configuration, the Configurator now checks the C++-based DirX Identity server. When the server is running, the Configurator asks you if it should stop the server. If your answer is

"No", you must stop the server before you can continue with the configuration. Otherwise the Configurator will stop the server.

4.2.3. DirX Directory Server for Connectivity

For **Connectivity Schema and Data Configuration**, the dialog asks you for the necessary properties of the directory server.

- Enter the host name and the port number of the directory server.
- Select the path where the directory server is installed.
- Check **Use SSL** if you want to connect with SSL to the directory server where the Connectivity database resides. Make sure you entered the appropriate port then.

> If you are using SSL for the first time to bind to the directory server with the Configurator, you must import the test CA certificate of the LDAP server into the trust store *dxi_java_path*/**lib/security/cacerts** of the JRE for DirX Identity before you run the Configurator. (See the chapter "Setting up the Java-based Configuration Wizard" in the *DirX Identity Connectivity Administration Guide* for details.) If DirX Identity was not installed before and you cannot use the DirX Identity Manager to import certificates into trust stores, then you must use **keytool.exe** under *dxi_java_home*/**bin** to import the certificate.

For **Connectivity Schema and Data Configuration**, the dialog asks you for the name and password of the administrator who has the right to make changes to the directory server schema. You can:

- Click **Next** to use the default directory administrator.
- Enter the name and password of the directory administrator, and then click **Next**.

If **Connectivity Schema and Data Configuration** is selected, the Configurator now checks the directory path. A warning is displayed when the path is incorrect. You can enter the correct path and try again or cancel the configuration. The Configurator then tries to connect to the directory server with the administrator account that you specified. If this action fails, an error dialog is displayed. You can correct the address and/or the credentials and try again or cancel the configuration.

4.2.4. DirX Directory Server for Provisioning

For **Provisioning Schema and Data Configuration**, the dialog asks you for the necessary properties of the directory server.

- Enter the host name and port number of the directory server.
- Select the path where the directory server is installed.
- Check **Use SSL** if you want to connect with SSL to the directory server where the Provisioning database resides. Make sure you entered the appropriate port then.

> If you use SSL the first time for binding to the directory server with the

> Configurator, you must import the CA certificate of the LDAP server into the truststore *dxi_java_path***/lib/security/cacerts** of the JRE for DirX Identity before you run the Configurator. (See the chapter "Setting up the Java-based Configuration Wizard" in the *DirX Identity Connectivity Administration Guide* for details.) If DirX Identity was not installed before and you cannot use the DirX Identity Manager to import certificates into truststores, you must use **keytool.exe** under *dxi_java_home***/bin** to import the certificate.

For **Provisioning Schema and Data Configuration**, the dialog asks you for the name and password of the administrator who has the right to make changes to the directory server schema. You can:

- Click **Next** to use the default directory administrator.
- Enter the name and password of the directory administrator, and then click **Next**.

For **Provisioning Schema and Data Configuration**, the Configurator now checks the directory path. A warning is displayed when the path is incorrect. You can enter the correct path and try again or cancel the configuration. The Configurator then tries to connect to the directory server with the administrator account that you specified. If this fails, an error dialogs is displayed. You can correct the address and/or the credentials and try again or cancel the configuration.

4.2.5. DirX Identity Administrators

This dialog asks you for the passwords of the DirX Identity administrators.

The **admin** account is used to access the DirX Identity configuration database during configuration runs. If the DirX Identity configuration database does not yet exist in the directory, the Configurator will store the given password in the directory for future logins.

- Enter the password of the administrator admin.

The DirX Identity C++-based Server and the supervisor use the **server_admin** account to access the directory. If the account does not yet exist in the directory, the Configurator will store the given password in the directory for future logins.

- Enter the password of the administrator account **server_admin**.

The **SystemDomain** account is used to access the DirX Identity provisioning database. If the DirX Identity provisioning database does not yet exist in the directory, the Configurator will store the given password in the directory for future logins.

The Configurator now tries to connect to the LDAP directories with the given credentials. If this fails, a warning is displayed. Possible reasons are:

- The directory address is invalid or the directory server is not running. Correct the given address or start the directory server and try it again.
- The DirX Identity database does not yet exist in the directory (this is the case during a new installation). You can ignore the warning.

- The DirX Identity database already exists in the directory. The password for the displayed user is not valid. You must go back, correct the password and try it again.

4.2.6. System-wide Configuration

This dialog is only displayed when either **ActiveMQ Message Broker** or **Java-based Server** or **C++-based Server** is selected.

If you want to activate the High Availability functionality system wide, which is selectable only if the HA license is installed:

- Check **Activate High Availability**.

If you want to use secure connections to the ActiveMQ Messaging Server(s) and to the Java Servers running in the system:

- Check **Use SSL**.

SSL cannot be set on new installations because some certificate and keystore- and truststore-generating scripts as described in the chapter "Securing Identity Server Connections with SSL" in the *DirX Identity Connectivity Administration Guide* must be run first. Also the Connectivity schema and data step must be selected to be able to select or deselect SSL.

> When preparing the above mentioned scripts for generating certificates and key and trust store, be sure that you specify the local machine name (hostname) the same way - either in the short form or in the fully-qualified name form, which is recommended in a wide area network - as you intend to do in the configuration steps for the ActiveMQ Message Broker, Java-based Server and C++-based Server. They all write the specified hostname into the same Connectivity system object, which must match the name contained in the server certificate for that machine.

If SSL is selected, the Configurator asks you to set:

- **Keystore Password**.

The passwords are written to the *install_path*/**ssl/password.properties** file. Be sure that you specify the same passwords as you did when generating the store. In silent configuration, the keystore password is read from the property **systemwide.keystore_pwd** in the **configuration.ini** file.

If encryption mode is configured at the Connectivity **Configuration** object or the **cn=server_admin,dxmC=DirXmetahub** object contains a certificate, the Configurator asks you to set:

- **Pin** for reading the private key from the **server_admin** object.
- **Previous Pin** for reading the previous private key from the **server_admin** object.

The PINs are written to the *install_path**/ssl/password.properties* file. Be sure that you specify the same PINs as you did when generating the certificate and private key for the Connectivity **server_admin** object with the **dirxgenpse** tool. In silent configuration, the Pin and the Previous Pin are read from the properties **systemwide.pin** and **systemwide.previous_pin** in the **configuration.ini** file.

If client signature is configured at the Provisioning **Domain** object, the Configurator asks you to set:

- **Signature Pin** for reading the private key from the **DomainAdmin** user object.

The domain-specific signature PIN is written to the *install_path*/**idsj-***domain***-S** *n*/**private/password.properties** file (if a Java-based Server is also configured in this configuration run). Be sure that you specify the same PIN as you did when generating the certificate and private key for the Provisioning **cn=DomainAdmin,cn=***domain_name* object with the **dirxgenpse** tool. In silent configuration, the Signature Pin is read from the property **systemwide.signature_pin** in the **configuration.ini** file.

The **password.properties** file is always written in this step, no matter whether ssl, encryption or client signature is set. If one of them is not set and so the Configurator does not ask for the related password or PIN, the default value is written to the **password.properties** file, which is **changeme** for the key store password, **1234** for the Pin and the Previous Pin and **5678** for the Signature Pin.

4.2.7. ActiveMQ Message Broker Configuration

This dialog is only displayed when ActiveMQ Message Broker Configuration is selected.

In this dialog, you can:

- Click **Next** to use the proposed values or
- Change the proposed values for the editable fields and then click **Next**.

You can change:

- The **Host Name** of the system this server runs on.

If SSL is used or planned to be used for the system, specify the host name in the same form - short or fully-qualified - as for generating the server certificate for this host. In a wide area network a fully-qualified host name could be required for SSL to work properly.

- The **Display Name** field cannot be changed. It is either the display name of an existing Message Broker or a new Broker name. A new Broker name consists of the prefix **Message Broker** and the number of the Broker configured for your (possibly distributed) installation.
- The **Port** for message transfer (default **61616**).
- The **Secure Port** for message transfer (default **61617**).

- The **Admin (Web Console) Port** (default **8161**).
- The **JMX Port** (default **10098**).
  Note that the port (*n*+1) is also configured and used.
- The **Message repository** path to be specified either as absolute path or as UNC path on a Windows system referring to a shared folder. The Configurator displays the default location *install_path***/messagebroker/data/kahadb** or the location specified in the last configuration run.
- The checkbox **Set service start type to automatic**, which is only shown on Windows Systems (default **checked**).
- The checkbox **Start service after configuration** (default **checked**).

4.2.8. ActiveMQ Message Broker Service Account

This dialog is only displayed on Windows platforms when **ActiveMQ Message Broker Configuration** is selected.

The Configurator asks under which account the ActiveMQ Message-Broker service should run.

- Enter your preferred account or use the system account.
- Set the checkbox **Set service start type to automatic** (default **checked**).
- Set the checkbox **Start service after configuration** (default **checked**).
- Click **Next**.

Setup now checks whether the specified account is valid and has the right to create files in the directory *install_path*.

Note: To perform these checks, the account under which this configuration procedure runs (the account you are logged in) must have the advanced user rights "Act as part of the operating system" and "Replace a process level token". If this is not the case, the Configurator displays a message box with the text "A required privilege is not held by the account …". We recommend aborting the configuration at that point and performing this procedure:

- Cancel the configuration.
- Grant the required rights to the user.
- Reboot your computer.
- Run the DirX Identity Configurator again.

4.2.9. C++-based Server Configuration

This dialog is only displayed when **C++-based Server** is selected.

In this dialog, you can:

- Click **Next**, to use the proposed values or

- Change the proposed values for the editable fields and then click **Next**.

You can change:

- The **Host Name** of the system the server runs on.

Note: If SSL is used or planned to be used for the system, specify the host name in the same form - short or fully-qualified - as for generating the server certificate for this host.

- The **Port for key transfer** (default **1111**) for secure connections between the DirX Identity C++-based server and the DirX Identity Java-based agents if encryption mode is to be used.
- The **Work path**.
- The **Status path**.

The Configurator asks you to select a work path directory and a status path directory. It displays the default locations in the fields provided.

> i We recommend locating the work and status path on separate disks in production environments. DirX Identity is designed to ignore a full status area disk but cannot ignore a full disk where the work area is located.

- The **Primary DirX Identity C Server** checkbox (the default is checked).

This checkbox is only visible if you are configuring a C Server on a machine other than the one on which the Connectivity Database resides. If you want to configure your primary C Server to this host name, check the box. When the box is not checked, a secondary C Server is configured to this host name. When reconfiguring a primary or secondary C Server (where the server already exists in the database), be sure to set the host name to the same name as before (the suggestion is taken from the **configuration.ini** file) and don't change from short to long form or vice versa, because then the C Server object is not found in the database and a new object is created, which is wrong.

4.2.10. C++-based Service Account

This dialog is only displayed on Windows platforms when **C++-based Server** is selected.

The Configurator asks under which account the DirX Identity C++-based service should run.

- Enter your preferred account or use the system account. We recommend that you do not use the system account:
- If you intend to set up a distributed DirX Identity environment to run distributed workflows,
- If you define a work or status path on another machine (the system account cannot access any resources on other machines).
- Set the checkbox **Set service start type to automatic** (default **checked**).
- Set the checkbox **Start service after configuration** (default **checked**).
- Click **Next**.

Setup now checks whether the specified account is valid and has the right to create files in the directory *install_path*.

> To perform these checks, the account under which this configuration procedure runs (the account you are logged in) must have the advanced user rights "Act as part of the operating system" and "Replace a process level token". If this is not the case, the Configurator displays a message box with the text "A required privilege is not held by the account …". We recommend aborting the configuration at that point and performing this procedure:

- Cancel the configuration.
- Grant the required rights to the user.
- Reboot your computer.
- Run the DirX Identity Configurator again.

4.2.11. Domain Configuration

This dialog is only displayed in this form when **Domain Configuration** is selected. If it is not selected but **Java-based Server** - or **Web Center Configuration** is selected, only the part to configure a customer domain is shown.

- Select the domain you want to use.

The sample domain is a complete and fully working example. For more information, see the *DirX Identity Tutorial Guide*.

The English and German health care domains are sample hospital domains with a typical medical person and role hierarchy.

For a customer domain configuration:

- Enter the domain name.
- The configuration process suggests a technical domain name. This name is used for creating the folder *install_path***/idsj-***technical_domain***-S***n* on your machine relating to the *n*th Java-based Server for that domain and for service names relating to the Java-based Servers for that domain. For technical reasons, these names must consist of only alphanumerical characters (**A-Z**, **a-z**, **0-9**) and/or the minus sign (**-**) or the underscore (**). The name is also appended to the URL of the Web Center. (See chapter "Using the Web Center" in the _DirX Identity User Interfaces Guide** for details.

  You may change the suggested name.
- Enter the password of the customer domain administrator.
- Click **Next**.

If the domain does not yet exist in the directory, the Configurator will store the given password in the directory for future logins.

The Configurator creates the account **cn=DomainAdmin,cn=My-Company** with a default password for the sample domain.

4.2.12. Java-based Server

This dialog is only displayed when **Java-based Server** is selected.

In this dialog, you can:

- Click **Next** to use the proposed values, or
- Change the proposed values for the editable fields and then click **Next**.

You can make the following changes:

- You can select whether you want to update or create a new Java-based server from the drop-down list provided for the **Server to configure** field. You are not allowed to update a Java-based Server for the domain specified in **Domain Configuration** if that Java-based Server is already configured for another domain. For DirX Identity version 8.2A and newer, you are allowed to configure multiple Java servers per domain.
- You can change the **Host Name** of the system on which the Java-based Server runs.

If SSL is used or planned to be used for the system, specify the host name in the same form - short or fully-qualified - as for generating the server certificate for this host.

- You can change the **Heap Size** of the Java-based Server (default 2 GByte).
- You can change the **IdS-J Http(s) Port** (default **40000**).
- You can change the **IdS-J JMX Port** (default **40005**).
  Note that the port (*n*+1) is also configured and used.
- You can change the path where the Java-based Server writes its warning and server logging files. By default, the path is **../logs**. This path is also used for classloading logging and other items.
- You can check or uncheck the **Set service start type to automatic** checkbox (only displayed on Windows platforms (default **checked**)).
- You can check or uncheck the **Start service after configuration** checkbox (default **checked**).

Note that you cannot change the **Display Name** field. It is either the display name of an existing Java-based Server or, for a new Java-based Server, a proposed name consisting of the technical domain name, the number of the server configured for this domain and the host name the Java-based Server runs on (domain_name*-S*n*-*host_name).

The Configurator checks whether the configured or interactively changed values are consistent regarding value ranges, for example, for the heap size, or regarding the naming conventions for the Java-based Server name. If the values are not consistent, an error message is displayed and in case of silent configuration the Configurator is aborted.

You can turn off name checking for the host name. You may need to take this action when your host can be accessed via different names (and also if you want to use localhost). In these cases, you can deactivate the checks by setting the following line in the configuration.ini file:

```
IdS-J.relaxed_name_check=1
```

If you do so, please be careful.

4.2.13. Java-based Service

This dialog is only displayed on Windows platforms when **Java-based Server** is selected.

The Configurator asks under which account the Java-based Server service should run.

- Enter your preferred account or use the system account.
- The checkbox **Set service start type to automatic** (default **checked**).
- The checkbox **Start service after configuration** (default **checked**).
- Click **Next**.

Setup now checks whether the specified account is valid and has the right to create files in the directory *install_path*.

> To perform these checks, the account under which this configuration procedure runs (the account you are logged in) must have the advanced user rights "Act as part of the operating system" and "Replace a process level token". If this is not the case, the Configurator displays a message box with the text "A required privilege is not held by the account …". We recommend aborting the configuration at that point and performing this procedure:

- Cancel the configuration.
- Grant the required rights to the user.
- Reboot your computer.
- Run the DirX Identity Configurator again.

At the end of the Java-based Service configuration step, the Configurator always saves a template file containing the Java-based Server properties. The name of this template file is *Java-based_Server_Display_Name***-configuration.tpl**. It is saved in *install_path*. Here is an example of a template file:

```
IdS-J.heap_size=2 GByte
IdS-J.host=MC0XCNXX
IdS-J.port=40000
IdS-J.jmx_port=40005
IdS-J.protocol=http
```

```
IdS-J.log_path=../logs
IdS-J.server_name=My-Company-S1-MC0XCNXX
IdS-J.start_after_configuration=1
IdS-J.start_type_automatic=1
domain= My-Company
IdS-J-service.domain=mydomain
IdS-J-service. account=myaccount
tech_customer_domain=My-Company
```

For silent installation, you can specify the password of the service account with:

IdS-J-service.password=*password*

The name of the template file is **My-Company-S1-MC0XCNXX-configuration.tpl**.

You can use the Configurator tool **Configuration.bat** to configure several Java-based Servers automatically. For this purpose, create one configuration file for each Java-based Server in *install_path***/bin**. You can use a template file as input for a Java-based Server configuration file. Then run the wizard for each Java-based Server and specify the name of the Java-based Server configuration file as the third parameter. (See "Configuration" for details.)

If in silent mode a customer domain is to be created or updated, the password for the domain admin user (*cn=DomainAdmin,cn=*domain*) can also be specified in the Java-based Server configuration file. If it is not specified there, the Configurator tries to read it from **configuration.ini**.

4.2.14. Web Center Configuration

This dialog is only displayed when **Web Center Configuration** is selected.

The Web Center is configured to the domain specified in **Domain Configuration**. You can configure a Web Center for each domain. The technical domain name is used to deploy the Web Center into Tomcat. Thus, the URL part for the Web Center is:

webCenter-*technical_domain_name*, for example **webCenter-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the **...** button.
- Enter the name of the Service (on Windows platforms).
- The checkbox **Start Tomcat service after configuration** (default **checked**).
- Click **Next** to go to the next dialog.

> The DirX Identity Web Center can be set up with other Web servers, too. Contact your support group to get more information about configuration with your specific Web server.

4.2.15. Web Center for Password Management

This dialog is only displayed when **Web Center for Password Management Configuration** is selected.

The Web Center for Password Management is configured to the domain specified in **Domain Configuration**. You can configure a Web Center for Password Management for each domain. The technical domain name is used to deploy the Web Center for Password Management into Tomcat to:

pwdManagement-*technical_domain_name*; for example, **pwdManagement-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the **…** button.
- Enter the name of the Tomcat service (on Windows platforms).
- Check the checkbox **Start Tomcat service after configuration** (default is **checked**).

The fields for specifying the Tomcat parameters described above are only enabled for editing if Tomcat has not already been configured in the previous step. Otherwise, the previously configured parameters are displayed in the disabled fields.

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

4.2.16. Provisioning Web Service

This dialog is only displayed when **Provisioning Web Service Configuration** is selected.

The Provisioning Web Service is configured to the domain specified in **Domain Configuration**. You can configure a Provisioning Web Service for each domain. The technical domain name is used to deploy the Provisioning Web Service into Tomcat to:

ProvisioningService-*technical_domain_name*; for example, **ProvisioningService-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the **…** button.
- Enter the name of the Tomcat service (on Windows platforms).
- Check the **Start Tomcat service after configuration** checkbox (the default is checked).

The fields for specifying the Tomcat parameters described above are only enabled for editing if Tomcat has not already been configured in one of the previous steps. Otherwise, the previously configured parameters are displayed in the disabled fields.

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

4.2.17. Server Admin REST Service

This dialog is only displayed when **Server Admin REST Service Configuration** is selected.

The Server Admin REST Service is configured to the domain specified in **Domain Configuration**. You can configure a Server Admin REST Service for each domain. The technical domain name is used to deploy the Server Admin REST Service into Tomcat to:

ServerAdminRestService-*technical_domain_name*; for example, **ServerAdminRestService-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the … button.
- Enter the name of the Tomcat service (on Windows platforms).
- Check the **Start Tomcat service after configuration** checkbox (the default is **checked**).

Note that the fields for specifying the Tomcat parameters described above are only enabled for editing if Tomcat has not already been configured in one of the previous steps. Otherwise, the previously configured parameters are displayed in the disabled fields.

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

4.2.18. Server Admin User Interface

This dialog is only displayed when **Server Admin User Interface Configuration** is selected.

The Server Admin User Interface Web Application (HTML5) is configured to the domain specified in **Domain Configuration**. You can configure a Server Admin User Interface for each domain. The technical domain name is used to deploy the Server Admin User Interface into Tomcat to:

DirXIdentityServerAdmin-*technical_domain_name*; for example, **DirXIdentityServerAdmin-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the … button.
- Enter the name of the Tomcat service (on Windows platforms).
- Check the **Start Tomcat service after configuration** checkbox (the default is **checked**).

Note that the fields for specifying the Tomcat parameters described above are only enabled for editing if Tomcat has not already been configured in one of the previous steps. Otherwise, the previously configured parameters are displayed in the disabled fields.

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

4.2.19. Identity REST Service

This dialog is only displayed when **Identity REST Service Configuration** is selected.

The Identity REST Service is configured to the domain specified in **Domain Configuration**. You can configure an Identity REST Service for each domain. The technical domain name is used to deploy the Identity REST Service into Tomcat to:

DirXIdentityRestService-*technical_domain_name*; for example, **DirXIdentityRestService-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the **…** button.
- Enter the name of the Tomcat service (on Windows platforms).
- Check the **Start Tomcat service after configuration** checkbox (the default is checked).

Note that the fields for specifying the Tomcat parameters described above are only enabled for editing if Tomcat has not already been configured in one of the previous steps. Otherwise, the previously configured parameters are displayed in the disabled fields.

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

4.2.20. Business User Interface

This dialog is only displayed when **Business User Interface Configuration** is selected.

The Approval Web Application (HTML5) is configured to the domain specified in **Domain Configuration**. You can configure a Business User Interface for each domain. The technical domain name is used to deploy the Business User Interface into Tomcat to:

BusinessUserInterface-*technical_domain_name*; for example, **BusinessUserInterface-CustomerDomain**.

Specify the following parameters:

- Enter the path to the Tomcat installation directory or choose it via the **…** button.
- Enter the name of the Tomcat service (on Windows platforms).
- Check the **Start Tomcat service after configuration** checkbox (the default is checked).

Note that the fields for specifying the Tomcat parameters described above are only enabled for editing if Tomcat has not already been configured in one of the previous steps. Otherwise, the previously configured parameters are displayed in the disabled fields.

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

4.2.21. HCL Notes Client

This dialog is only displayed on Windows platforms when **C++-based Server Configuration** is selected and the Connectivity Package HCL Notes has been installed.

- Enter the path where your Notes Client is or will be installed.
- Click **Next**.

Before you can use connectivity to the IBM Notes system, you must reboot the machine.

4.2.22. ODBC Library Path

This dialog is only displayed on Linux platforms when **C++-based Server Configuration** is selected and the Connectivity Package ODBC is installed. The Configurator asks you for the path where your ODBC libraries are installed.

In this dialog, you can:

- Click **Next** to select the default location.
- Select a different location and then click **Next**.

The Configurator tries to load the ODBC Agent. If this action fails, a warning is displayed. You can step back and enter a correct path, cancel the configuration or continue without configuring the agent.

4.2.23. SAP ECC UM Library Path

This dialog is only displayed on Linux platforms when **C++-based Server Configuration** is selected and the Connectivity Package SAP ECC UM is installed. The Configurator asks you for the path where your SAP JCo files are installed.

In this dialog, you can:

- Click **Next** to select the default locations.
- Select a different location and then click **Next**.

4.2.24. Pre-Configuration Summary

Before the specified configuration tasks are performed, you can review them here. The text window displays a complete list of tasks that will be performed after you click the **Next** button.

- Click **Next** to start the configuration procedure.
- Click **Previous** to correct data that is incorrect.

4.2.25. Configuration in Progress

The configuration is running now. It performs all steps displayed:

- A running step is displayed in gray.
- If a step is performed successfully, its color turns to green and the configuration procedure proceeds with the next step.
- If a step fails, its color turns to red.The configuration procedure is aborted and a message is displayed that asks whether you want to view the log file.

Correct the problem and then re-start the configuration process.You can select only those configuration options for which the configuration procedure previously failed.

If all steps are performed successfully, you have completely configured DirX Identity.

Click **Finish** to close the Configurator.

> Don't forget to set the correct passwords for all of the pre-configured accounts in the DirX Identity database.(See the section "Managing Administrative Accounts" in the chapter "Managing the Connectivity System" in the *DirX Identity Connectivity Administration Guide* for details.)

4.3. Integrating Start/Stop Scripts into the Linux Operating System

For Linux platforms, the following DirX Identity service components are not necessarily stopped during system shutdown and not necessarily started during system start:

- Message Broker
- C++-based Server
- Java-based Servers

This section describes how to use the DirX Identity integration utility to integrate start and stop scripts for these DirX Identity components into Linux and how to undo the integration if necessary.

4.3.1. Using the Integration Utility

Use the **updrcs-linux.sh** utility located in *install_path***/etc** to integrate or unintegrate the start/stop scripts created for the listed DirX Identity components in **/etc/init.d**. The default names for these scripts are:

- **dmsvr** for the C++-based Server
- **dmmbrk-***number* for a DirX Identity Message Broker
- **dmsvrj-***technical_domain_name***-S***number* for a Java-based Server

It is unlikely but possible that a script with a default name already exists in this folder which does not belong to DirX Identity. The utility automatically detects this kind of naming conflict. In this case, the utility can be customized by modifying the value of the shell variable **UNIQUESUFFIX** (default: empty string) in order to append a suffix to the default names. To integrate these scripts, perform the Linux command **chkconfig -add** with the related script names.

The scripts are similar to the scripts **dmmbrk-*** and **S99*** in *install_path***/etc**. For instance, the script **dmsvr** on SuSE platforms is a concatenation of the suitable INIT-V information in *install_path***/etc/suse/S99dmsvr.txt** *install_path***/etc/S99dmsvr**. Here the related placeholders (like **@dirx@**) are substituted so that they reflect the dependencies correctly. For RedHat platforms, the related file in *install_path**/etc/redhat* is used.

The script **updrcs-linux.sh** uses the technical domain name rather than the original domain name when handling domain-specific components.

For the Message Broker and the Java-based Servers, the script prompts the user to specify whether the related component needs configuration or un-configuration because this cannot be determined from **configuration.ini**.

4.3.2. Performing the Integration

If the DirX Identity components whose start/stop scripts are to be integrated use a co-located DirX Directory Server installation as the configuration and/or Provisioning store, the following prerequisites must be satisfied:

- DirX Directory has been configured so that it is started when entering runlevels 3 or 5 and stopped during shutdown. See the DirX Directory documentation for Linux platforms for further details.

For SuSE, this prerequisite means:

- A start/stop script *dirx_script_name* for DirX (for example, **dirx**) must exist in **/etc/init.d**.
- The Linux command **chkconfig --list** *dirx_script_name* is successful.

You must be superuser in order to verify these prerequisites.

If these prerequisites are satisfied, perform these steps:

- Login as superuser.
- Using a shell, navigate to *install_path**/etc*.
- Execute the command **./updrcs-linux.sh**. For SuSE Linux platforms, *dirx_script_name* must be supplied as an input argument if the DirX Identity installation uses a co-located DirX installation.
- The script displays the exit code on screen. An exit code indicates successful execution of the script. A log file **updrcs-linux.sh.log** is also written.

The integration is now complete. The relevant DirX Identity components are started during system startup (in the order listed in "Integrating Start/Stop Scripts into the Linux Operating System") listed and stopped during system shutdown (in reverse order).

> Running this script is required whenever the configuration has been changed with respect to these DirX Identity components.

4.3.3. Undoing the Integration

Before uninstalling DirX Identity, the integration must be undone:

- Log in as superuser.
- Using a shell, navigate to *install_path***/etc**.
- Execute the command **./updrcs-linux.sh -cleanup** and then check the exit code and the

log file.

4.3.4. Silent Configuration and Un-configuration

You can configure DirX Identity on a machine without interaction.Follow these steps to create a silent configuration:

- Run the Initial Configuration in normal mode and then cancel it when the dialog **Pre-Configuration Summary** is displayed.This action customizes the response file **configuration.ini** and creates the Java-based Server configuration template in the installation folder.
- Set the required passwords in **configuration.ini** and then save a copy of the file.
- If necessary, create the Java-based Server configuration files in *install_path**/bin*.(See "Java-based Server" for details.)
- Run **Configuration.bat** (**Configuration.sh**) in *install_path***/bin** with the following parameters:
- **InitialConfiguration silent** [*Java-based_server_config_file*]
- Check for errors and search for the string **The configuration finished successfully!** in the file *install_path***/logs/silent.log**

You must perform the first two steps only after the first installation or when you want to change configuration settings. Otherwise, copy the saved **configuration.ini** file into the installation folder when the silent installation has finished and run the silent configuration.

By changing the configuration settings, you can:

- Determine what components are configured by specifying the **option** properties. In a silent configuration, the components associated with the selected options are configured. In a non-silent configuration, the options determine whether the associated configuration step is preselected, which the user can change interactively. Here is the list of options that can be set:
- **option.dxm_schema=1** specifies that the Connectivity Schema and Data is configured.
- **option.dxr_schema=1** specifies that the Provisioning Schema and Data is configured.
- **option.MessageBroker=1** specifies that the Message Broker is configured.
- **option.idsc=1** specifies that the C++-based Server is configured.
- **option.idsj_server=1** specifies that the Java-based Server is configured.
- **option.sample_domain=1** specifies that the sample domain is configured.
- **option.cust_domain=1** specifies that the customer domain with the name specified in **domain=** is configured
- **HighAvailability.Serveradmin=1** specifies that the Server Admin application including the Java-based supervisor are configured.
- **option.configureManager=1** specifies that the Identity Manager is configured.
- **option.WebCenter=1** specifies that the Web Center is configured.

- **option.WebCenterPwdMgmt=1** specifies that the Web Center for Password Management is configured.
- **option.WebCenterSAP=1** specifies that Web Center for SAP is configured.
- **option.ProvisioningWebService=1** specifies that Provisioning Web Service is configured.
- **option.RestService=1** specifies that Identity REST Service is configured.
- **option.BusinessUserInterface=1** specifies that Business User Interface (HTML5) is configured.
- Determine default values for certain properties. The properties are evaluated if the related component has been selected for configuration by the related **option** property described above. Here is a list of some properties with sample values:
- MessageBroker.admin_port=8161
- MessageBroker.displayname=Message Broker 1
- MessageBroker.host=dxiptest01-vm
- MessageBroker.jmx_port=10098
- MessageBroker.port=61616
- MessageBroker.secure_port=61617
- MessageBroker.start_after_configuration=1
- MessageBroker.start_type_automatic=1
- MessageBroker-service.domain=*domain*
- MessageBroker-service.account=*account*
- MessageBroker-service.password=*password*
- path.notes=C\:\\Program Files\\lotus\\notes
- path.status=C\:\\Program Files\\Atos\\DirX Identity\\status
- path.work=C\:\\Program Files\\Atos\\DirX Identity\\work
- connectivityStore.directory_inst_path=C\:/Program Files/Atos/DirX
- connectivityStore.host=dxiptest01-vm
- connectivityStore.port=389
- connectivityStore.ssl=0
- connectivityStore.type=DirX Directory V8.x
- connectivityStore.user=cn\=admin,o\=My-Company
- provisioningStore.directory_inst_path=C\:/Program Files/Atos/DirX
- provisioningStore.host=dxiptest01-vm
- provisioningStore.port=389
- provisioningStore.ssl=0
- provisioningStore.type=DirX Directory V8.x
- provisioningStore.user=cn\=admin,o\=My-Company

- roleadmin.user=cn\=SystemAdmin,cn\=DirXmetaRole-SystemDomain
- svcadmin.user=cn\=server_admin,dxmC\=DirXmetahub
- systemwide.ha=0
- systemwide.ssl=0
- tomcat.path=C\:/Program Files/Apache Software Foundation/Tomcat 9.0
- tomcat.service_name=Tomcat9
- tomcat.start_after_configuration=1
- The names of all properties can be seen in the **configuration.ini** file after the Configurator has run. Their values can be changed and will be taken for preselection (in silent mode for final selection) in the next run.

If the Configurator runs in silent mode, the selected components are configured with the specified property values. In non-silent mode, the Configurator displays the steps and dialog boxes corresponding to the selected components and the specified properties. These preselections can then be changed by the user.

Password settings in the **configuration.ini** file for silent configuration include:

```
# Password of the directory administrator for connectivity (that is,
cn=admin,o=My-Company)
connectivityStore.password=password
# Password of the directory administrator for provisioning (that is,
cn=admin,o=My-Company)
provisioningStore.password=password
# password of cn=SystemAdmin,cn=DirXmetaRole-SystemDomain
roleadmin.password=password
# password of the customer domain admin (cn=DomainAdmin,cn=Customer
Domain)
domainadmin.password=password
# password of cn=admin,dxmC=DirXmetahub
hubadmin.password=password
# password of cn=server_admin,dxmC=DirXmetahub
svcadmin.password=password
# password of the C++-based server account
IdS-C-service.password=password
# password of the Java-based service account
IdS-J-service.password=password
# password of the ActiveMQ MessageBroker service account
MessageBroker-service.password=password
# password of the system-wide keystore
systemwide.keystore_pwd=password
```

```
# system-wide pin
systemwide.pin=pin
# system-wide previous pin
systemwide.previous_pin=pin
# system-wide signature pin
systemwide.signature_pin=pin
```

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

For a silent un-configuration:

- Run **Configuration.bat** (**Configuration.sh**) in *install_path*/**bin** with the following parameters:
- UnConfiguration silent

5. Configuring Single Components

This chapter provides information on how to configure components separately, including:

- Installing the directory server
- Configuring the Tomcat server
- Configuring Connectivity
- Configuring Provisioning
- Configuring a separate C++-based Identity Server
- Configuring a separate Java-based Identity Server
- Configuring a separate Identity Manager
- Configuring a separate Web Center
- Configuring a separate Business User Interface
- Configuring a separate supervisor
- Configuring agents
- Configuring connectors

5.1. Hints for Installing the DirX Directory Server

- Install the directory with the default settings.If you are working with an empty database, you must create an LDAP configuration and an administrator object in the directory before running the DirX Identity installations (see the DirX Directory administration documentation for details).
- If you have loaded the example database (see the DirX administration documentation for details), enter the name **cn=admin,o=my-company** with a default password, when the DirX Identity installation prompts you for the directory administrator.

> If you have installed DirX directory after a de-installation of the software and without a new setup of DirX Identity, you must restore the database and copy the dirxabbr-ext.DirXmetahub… and dirxabbr-ext.DirXmetaRole… files from *install_path*/**client/conf** to *dirx_install_path*/**client/conf**.

> *DirX Identity with shadow agreements*
>
> - Check the indexing requirements of your installation environment (see the section "Indexed Attributes" in the chapter "Additional Topics" for more information).If you do not define enough indexes, the configuration will fail!
> - If you install DirX Identity on a DirX Directory server where shadow agreements are set up, be sure to exclude the DirX Identity configuration part from these agreements.
> - If you use a shadow agreement that shadows the data beginning at the root context prefix, then DirX Identity configuration data will be

shadowed, too.In this case the DirX Identity configuration part of the schema must be present on all shadows.

- Another alternative is to separate the Connectivity Configuration from the Provisioning database into another DirX Directory server.

5.2. Hints for Configuring the Tomcat Server

Running an application in the Tomcat server requires an appropriate setup of enough maximum memory.

On Windows, select **Configure Tomcat** from Tomcat’s program folder, open the **Java** tab and set the required value of **Maximum memory pool** appropriately.

On Linux, add the following line at the beginning of Tomcat’s startup script **startup.sh**:

JAVA_OPTS=-Xmx512m; export JAVA_OPTS

In this example, a value of 512 Megabytes is set.

Restart the Tomcat server for the change to become effective.

5.3. Configuring Connectivity Schema and Data

A separate installation of the Connectivity LDAP configuration schema and data part of DirX Identity requires performing these steps:

1. Prerequisite: Existence of a directory server on this machine (use the native tools to perform this step).
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity"):
   - Select Connectivity Schema and Data Configuration in the Configuration Options dialog.
4. Extend the directory schema as required.

(See also "Schema and Content Handling" in chapter "Additional Topics" for details.)

5.4. Configuring Provisioning Schema and Data

A separate installation of the Provisioning LDAP configuration schema and data part of DirX Identity requires performing these steps:

1. Prerequisite: Existence of a directory server on this machine (use the native tools to

perform this step).

2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity"):
   - Select Provisioning Schema and Data Configuration in the Configuration Options dialog.
4. Extend the directory schema as required.

5.5. Message Broker

A separate installation of a Message Broker requires performing these steps:

1. Prerequisites: Existence of a setup Connectivity Configuration.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select ActiveMQ Message Broker Configuration in the Configuration Options dialog.

5.6. C++-based Identity Server

A separate installation of a C++-based Server requires performing these steps:

1. Prerequisites: Existence of a setup Connectivity Configuration and Message Broker.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed, according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select C++-based Server Configuration in the Configuration Options dialog.

The server type field of the first server that is installed is set to **primary** (it runs the Status Tracker); all other servers are set to **secondary**.

The DirX Identity Meta Controller (metacp) will be installed without explicit selection.

Please note that it is not possible to install more than one C++-based Identity Server on the same computer.

5.7. Java-based Identity Server

A separate installation of a Java-based Server requires performing these steps:

1. Prerequisite: Existence of a setup Connectivity Configuration and Message Broker.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog select the set of features you have licensed, according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select Java-based Server Configuration in the Configuration Options dialog.

Note that the server type field of all installed servers is set to **primary** (it contains the repository).Secondary servers are not supported in this release.

5.8. DirX Identity Manager

A separate installation of a DirX Identity Manager requires performing these steps:

1. Prerequisite: Existence of a setup Connectivity Configuration.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed, according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select Manager Configuration in the Configuration Options dialog.

5.9. DirX Identity Web Center

A separate installation of a DirX Identity Web Center requires performing these steps:

1. Prerequisite: Existence of a setup Connectivity Configuration, a setup Provisioning Configuration (including a configuration of a sample or customer domain) and a supported Tomcat installation (see the release notes) on this machine.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed according to the description of that dialog in the chapter "Installing DirX

Identity".

3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select Web Center Configuration in the Configuration Options dialog.

5.10. Business User Interface

A separate installation of a Business User Interface requires performing these steps:

1. Prerequisite: A Connectivity Configuration setup, a Provisioning Configuration (including a configuration of a sample or customer domain) setup and a supported Tomcat installation (see the release notes) must all exist on this machine.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed according to the description of this dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select Business User Interface Configuration in the Configuration Options dialog.

5.11. DirX Identity Connectivity Packages - Agents

A separate installation of a DirX Identity agent requires performing these steps:

1. Prerequisite: A Connectivity Configuration setup must exist.
2. Run the installation procedure on this machine (see the chapter "Installing DirX Identity"):
   - In the Choose Licensed Features Set dialog, select the set of features you have licensed according to the description of that dialog in the chapter "Installing DirX Identity".
3. Run the configuration procedure on this machine (see the chapter "Configuring DirX Identity")
   - Select C++-based Server Configuration in the Configuration Options dialog.

Note that the server type field of the installed C++-based Server is set to **secondary**.

5.12. DirX Identity Connectivity Packages - Connectors

A separate installation of a DirX Identity connector requires performing these steps:

1. Prerequisite: A Connectivity Configuration setup must exist.
2. Run the installation procedure on this machine (see the chapter "Installing DirX

Identity"):

   - In the Choose Licensed Features Set dialog select the set of features you have licensed, according to the description of that dialog in the chapter "Installing DirX Identity".

3. Run the configuration procedure on this machine (see chapter "Configuring DirX Identity")

   - Select Java-based Server Configuration in the Configuration Options dialog.

6. Other Installation Configurations

This chapter provides information about other installation configurations:

- A sample distributed installation on several machines
- Password Management (including Web Center for Password Management)
- Configurations using DirX Identity High Availability Features

6.1. Distributed Installation

You can also distribute the DirX Identity components on different machines.

If DirX Identity is installed in a distributed environment, be sure to update all machines with the new software version.Otherwise, severe interworking problems could be the result.You can check the installed version on a machine in the install_history.txt file in the installation directory.

An example for a distributed installation is:

- DirX Directory with the Connectivity configuration and the Identity Store (with the users) resides on machine A.
- Machine B hosts these components:
- A Message Broker for all DirX Identity components in the distributed environment.
- A C++-based Identity Server 1. This server hosts a Notes connector. A Notes agent is also deployed on this system that is controlled by the C++-based Server.
- A Java-based Identity Server 1. This server also is responsible for processing the request workflows.
- Machine C hosts 2 servers:
- C++-based Identity Server 2. It controls the Active Directory agent.
- Java-based Identity Server 2: it run the Java-based real-time workflows, especially that for provisioning and password synchronization.
- The Web Center shall run on machine D.

The following figure illustrates this distributed installation:

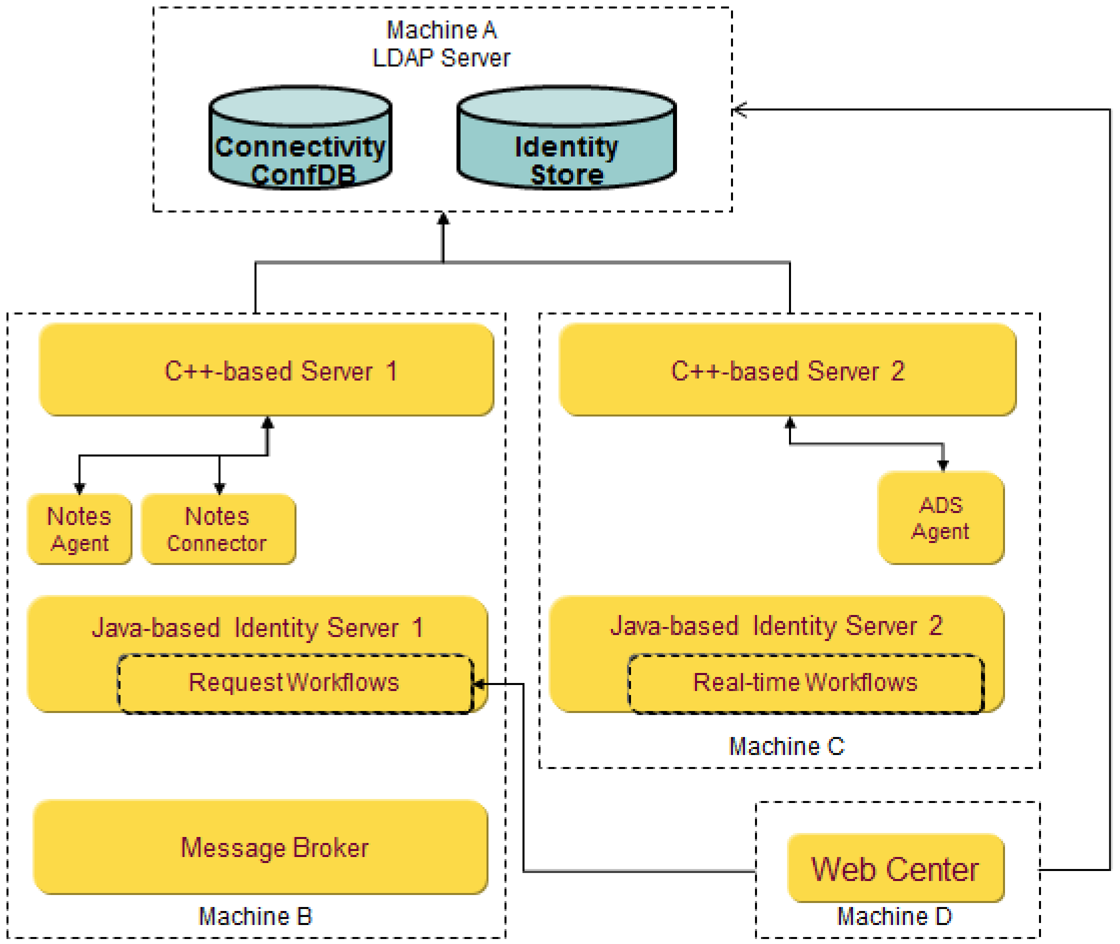


Figure 1. Distributed Installation

As a pre-requisite for this deployment, you need the appropriate licenses: **Business Suite**, **Professional Suite** (because of the request workflows) and the connectivity packages for Active Directory and Lotus Notes.

Install the Connectivity Configuration on machine A

1. Perform the steps described in section "Hints for Installing the Directory Server" to create a directory server on this machine.
2. Perform the steps described in section "Configuring Connectivity Schema and Data".
3. Perform the steps described in section "Configuring Provisioning Schema and Data".

Install the Message Broker, Servers, the Manager and the Notes connectivity on machine B

4. Run the installation procedure (see chapter "Installing DirX Identity"):
   - Select Message Broker, C++-based Server, Java-based Server, Manager and the IBM Connectivity Package in the Choose Install Set dialog.

Install more Servers, the Manager and the Microsoft connectivity on machine C

5. Run the installation procedure (see chapter "Installing DirX Identity"):

    - Select C++-based Server, Java-based Server, Manager and the Microsoft Connectivity Package in the Choose Install Set dialog.

Install the Web Center on machine D

6. Perform the steps described in section "DirX Identity Web Center".

The configuration procedure writes information about the installed servers and connectivity packages into the DirX Identity Connectivity configuration.

6.2. Password Management including specialized Web Center

This section provides an overview about installing the password management feature described in *Use Case Description Password Management*.Please note that you need the **Password Management** license for installing **Web Center for Password Management**.

Perform these steps to install password management with its prerequisites on a single machine:

1. Install a directory server on the local machine (use the native tools to perform this step).
2. Install Tomcat on the local machine.During installation select the NT Service on Windows platforms.Refer to the release notes regarding supported Tomcat versions and the suitable Java environment and satisfy these prerequisites for the Tomcat used for your DirX Identity installation.
3. Run the DirX Identity installation procedure (see chapter "Installing DirX Identity"):
    - In the **Choose Licensed Features Set** dialog select the appropriate licenses, at least **Password Management**.
    - In the **Choose Install Set** dialog make your choice according to the section “Installation” in *Use Case Description Password Management*.The appropriate Web Center for this use case is the **Password Management** component **Web Center for Password Management Configuration.**
4. Run the DirX Identity configuration procedure (see chapter "Configuring DirX Identity"):
    - In the **Configuration Options** dialog select the appropriate steps according to the section “Initial Configuration” in *Use Case Description Password Management**.* Fill out the entire subsequent configuration dialogs.

For details, see the *Use Case Description Password Management* and related user documentation listed in section “Documentation” of that use case description.

6.3. Configurations using DirX Identity High Availability Features

Setting up configurations using DirX Identity High Availability Features requires understanding *Use Case Description High Availability*.As a pre-requisite you need the licenses for **Business Suite**, **High Availability** and the connectivity packages you are going to deploy in your installations.

Planning High Availability configurations requires consideration of

- Multiple C++-based Servers
- Multiple Java-based Servers per provisioning domain.A good High Availability concept will include deployment of such servers on multiple hosts
- Identical set of connectivity packages for each host you deploy your C++-based and/or Java-based Servers
- Two Message Brokers on different machines with a shared message repository
- Server Admin to be installed for each Java-based Server host
- Shared folders for message repository and repository of each Java-based Server
- Other components you are going to use for productive use

Having identified the necessary installations and components to be configured, perform these steps:

1. For each relevant host, run the DirX Identity installation procedure (see chapter "Installing DirX Identity"):
   - In the **Choose Licensed Features Set** dialog select the set of features you have licensed, according to the description of that dialog in the chapter "Install DirX Identity". This selection must be identical for each host because that information is stored in several locations in the individual installations and must be consistent in your necessarily distributed configuration.
   - In the **Choose Install Set** dialog choose the relevant components in accordance with the section “Initial Configuration” in *Use Case Description High Availability*.
2. For each relevant host, run the DirX Identity configuration procedure (Initial Configuration, see chapter "Configuring DirX Identity"):
   - In the **Configuration Options** dialog select the relevant components in accordance with the section “Initial Configuration” in *Use Case Description High Availability*.
3. For each relevant host, perform additional steps according to “Configuration” in *Use Case Description High Availability*) in order to implement your High Availability scenario.

7. Installing the Windows Password Listener

This chapter describes how to run the DirX Identity Windows Password Listener installation procedure on Windows Server 2016 (Long-Term Servicing Channel) / Windows Server 2019 (with Desktop Experience) platforms to install the DirX Identity Windows Password Listener on a machine.

This procedure is only necessary if you intend to capture user passwords for password synchronization. Then you must install the Windows Password Listener on all machines that contain an Active Directory installation.

ℹ The Windows Password Listener does not require an installation of any other DirX Identity component on the same machine.

ℹ The Windows Password Listener needs a Java Environment only during the installation and un-installation process. For un-installation, a Java at any place of your system accessible through the system “path” variable is sufficient.

The installation creates the Windows Password Listener configuration files **libdxmEventListenerAds.ini** and **options.ini** with the default values. During an update or upgrade installation, the values are taken from the existing files or from input during the installation.

Upgrade installations are supported from Windows Password Listener versions 8.7 and 8.9.

For installing the Windows Password Listener on several domain controllers, you can install the software once on one domain controller and then create the response file. You can then copy and use this response file on the other domain controllers and run the installation without user interaction (see section "Unattended (silent) installation") based on this response file.

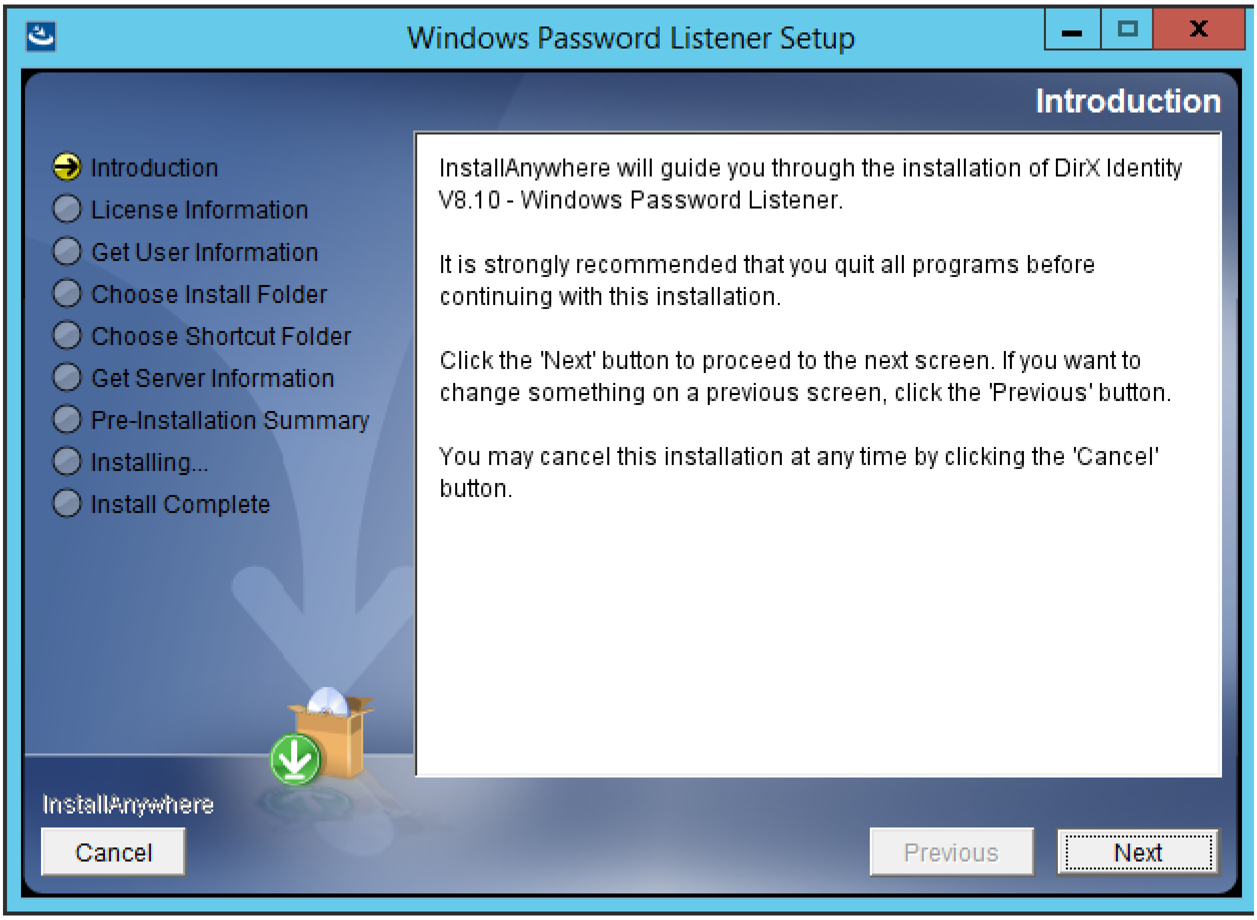
The Windows Password Listener uses ActiveMQ messaging of a DirX Identity installation as its messaging service. The Windows Password Listener installation procedure asks for the host name and port number of the already installed messaging service and whether you want to use SSL for the messaging connections. If you check SSL, you can proceed with the installation and afterwards copy the files **ca-crt.pem**, **client-key.pem** and **password.properties** from the DirX Identity installation **ssl** subfolder where they have been created to the **ssl** subfolder of the Password Listener installation before you start the Password Listener service.

ℹ The Password Listener cannot encrypt passwords in the password.properties file. You must copy a file with encrypted values that is working in the Identity installation. If you change the password value in the installation environment, you must copy the file with newly encrypted values again.

If SSL is set, the Password Listener always performs client-side SSL to the ActiveMQ Message Server. For a description of how to create these SSL related files on the DirX Identity side, see the chapter “Securing Identity Server Connections with SSL” in the *Connectivity Administration Guide*.

7.1. Installing the Windows Password Listener

- Run **setup.exe** from the DirX Identity DVD. Setup displays a dialog box:
- Click DirX Identity.
- Click Install DirX Identity Windows Password Listener.



InstallAnywhere will guide you through the installation of DirX Identity V8.10 - Windows Password Listener.

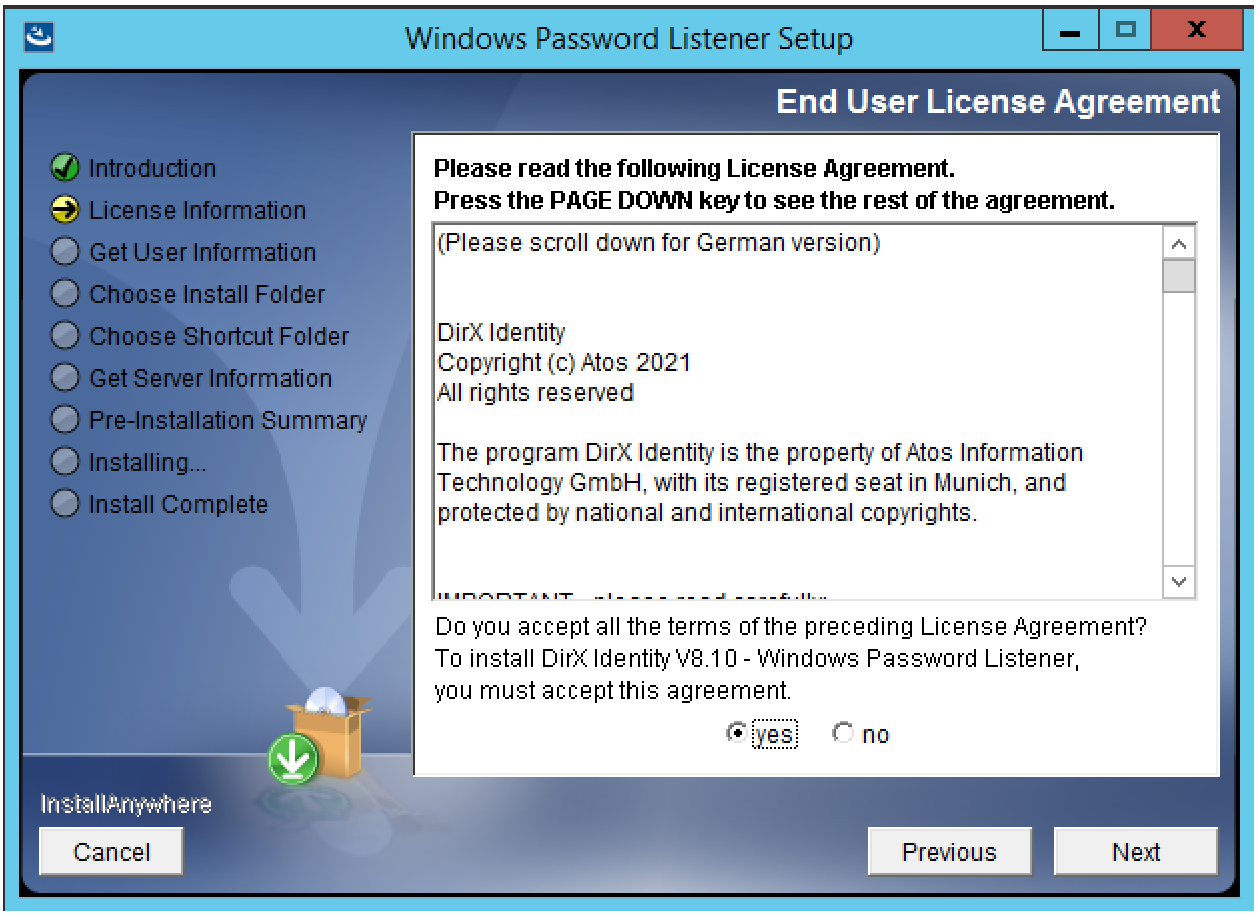
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

- Click **Next**.

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



Please read the following License Agreement.
Press the PAGE DOWN key to see the rest of the agreement.

(Please scroll down for German version)

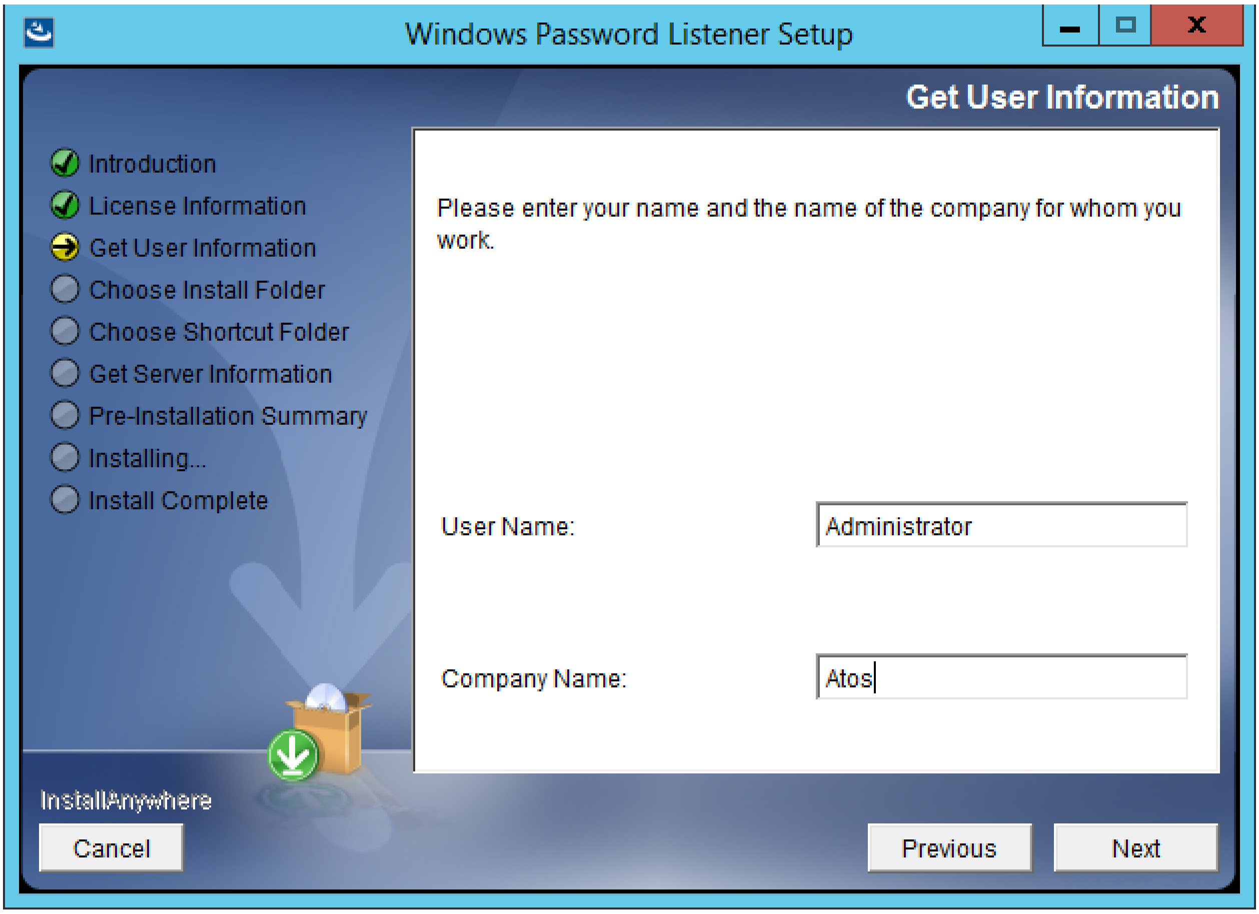
DirX Identity
Copyright (c) Atos 2021
All rights reserved

The program DirX Identity is the property of Atos Information Technology GmbH, with its registered seat in Munich, and protected by national and international copyrights.

Do you accept all the terms of the preceding License Agreement?
To install DirX Identity V8.10 - Windows Password Listener,
you must accept this agreement.

● yes ○ no

- Setup displays a License Information dialog.
- Read the licensing information, and then click **Yes** and then click **Next**. Clicking **No** cancels the installation.



Windows Password Listener Setup

Get User Information

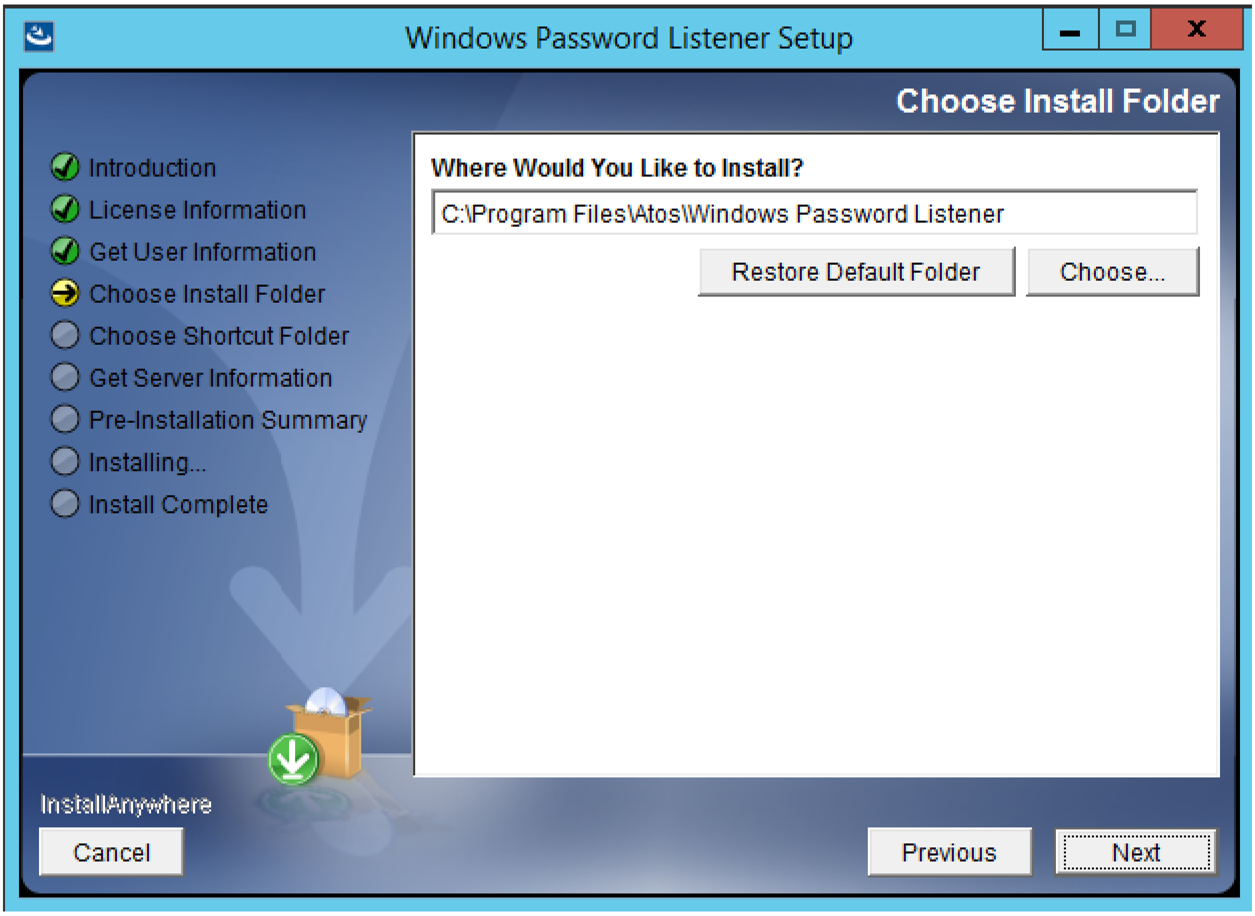
- ✓ Introduction
- ✓ License Information
- ➔ Get User Information
- ○ Choose Install Folder
- ○ Choose Shortcut Folder
- ○ Get Server Information
- ○ Pre-Installation Summary
- ○ Installing...
- ○ Install Complete

Please enter your name and the name of the company for whom you work.

User Name: Administrator

Company Name: Atos

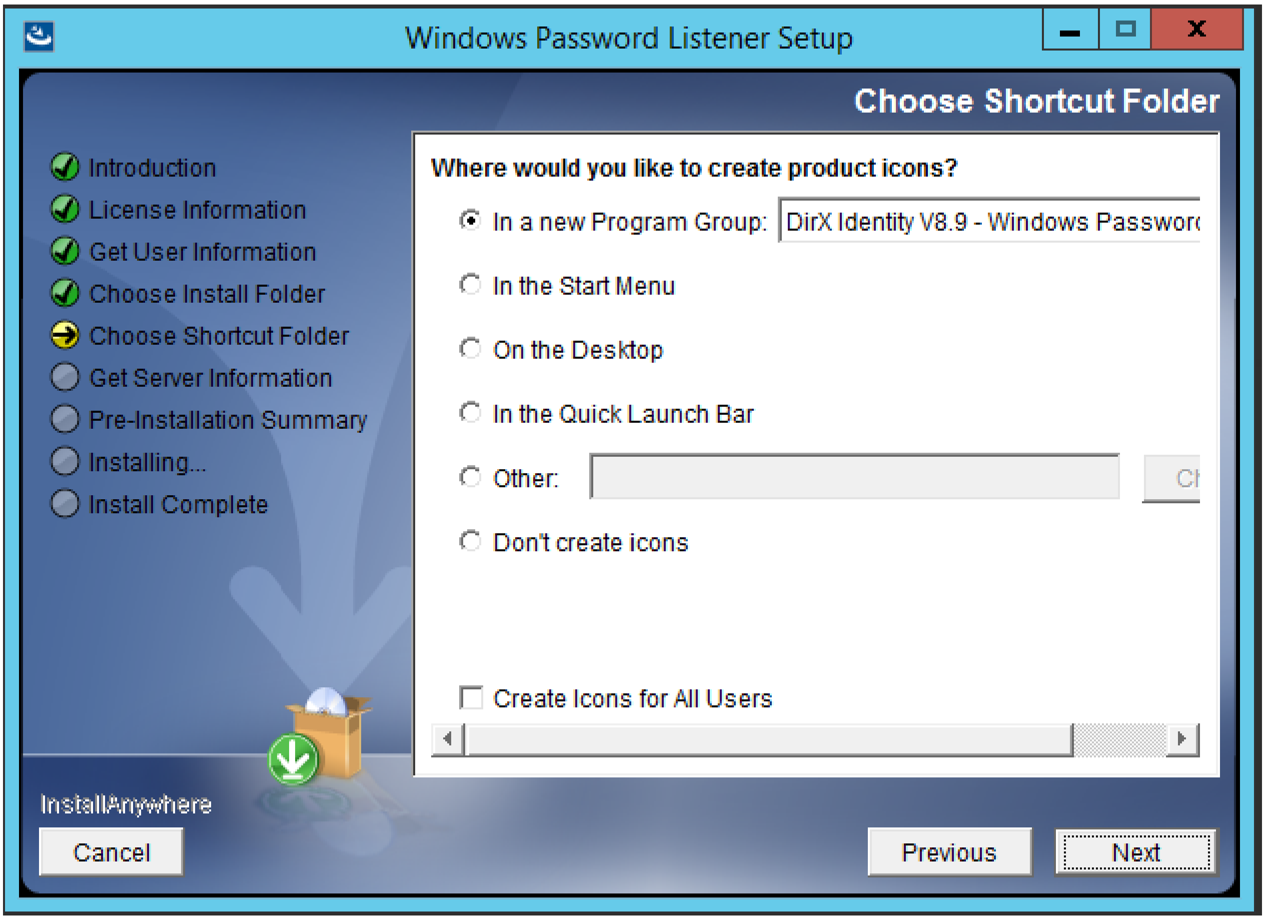
- Setup displays a Customer Information dialog.
- Enter your name and your company name in the fields provided, and then click **Next**.



Where Would You Like to Install?

C:\Program Files\Atos\Windows Password Listener

- Setup asks you to select an installation directory. It displays the default location in the field provided.
- In this dialog, you can:
- Click **Next** to select the default location.
- Click **Choose** to select a different directory, and then click **Next**.



Where would you like to create product icons?

● In a new Program Group: DirX Identity V8.9 - Windows Passwor

○ In the Start Menu

○ On the Desktop

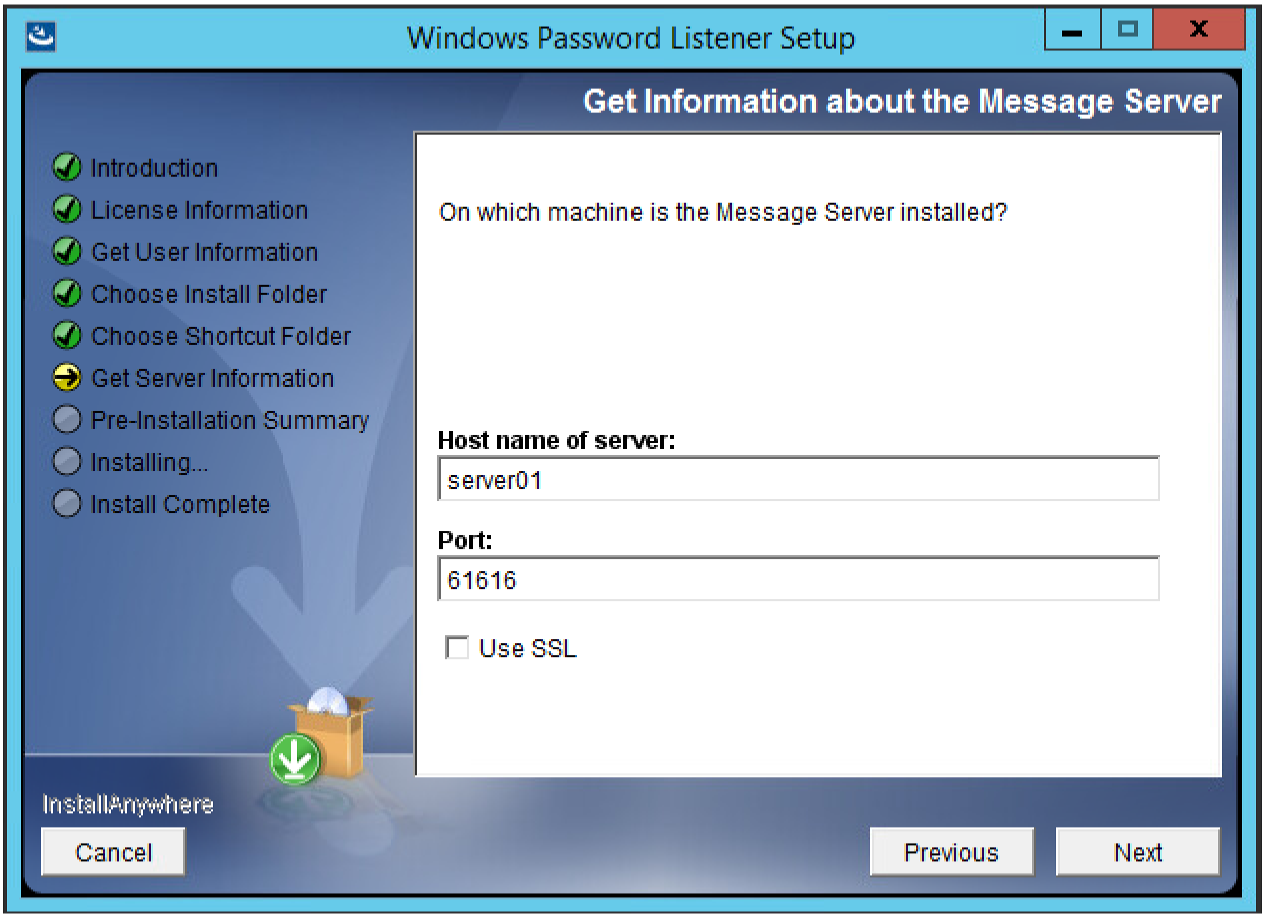
○ In the Quick Launch Bar

○ Other: Ch

○ Don't create icons

□ Create Icons for All Users

- Setup asks you where you would like to create product icons. It displays the default location in the field provided.
  Note: If you upgrade from an older version, the currently used Program Group name is shown **In a new Program Group:** (in the picture above, from version V8.9). Otherwise, a default name is shown.
- In this dialog, you can:
- Click **Next** to select the default location.
- Select a radio button of another predefined location and then click **Next**.



On which machine is the Message Server installed?

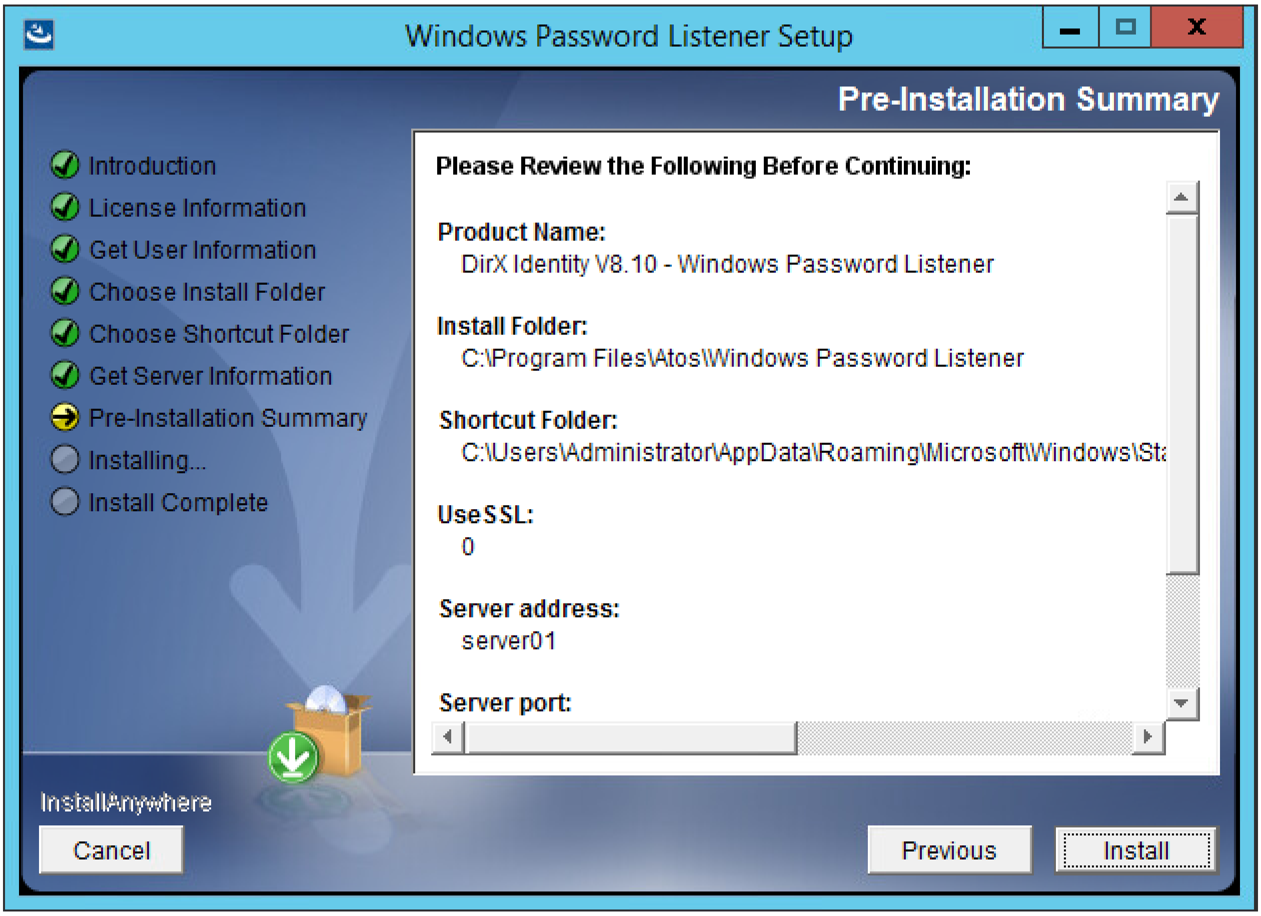
Host name of server: server01

Port: 61616

□ Use SSL

- Setup asks you for information about the message server.
- Enter the host name of the machine on which the message server is installed and the port number of the message server in the fields provided.
- Check **Use SSL** if you want to use an SSL connection to the server.
- Click **Next**.

Be sure that your DNS (domain name service) works correctly if you use symbolic names for the host name. If you are not sure, use a TCP/IP address instead. If you use SSL, you must give the exact same server name of the messaging server that is used in its server certificate.



Please Review the Following Before Continuing:

Product Name:
DirX Identity V8.10 - Windows Password Listener

Install Folder:
C:\Program Files\Atos\Windows Password Listener

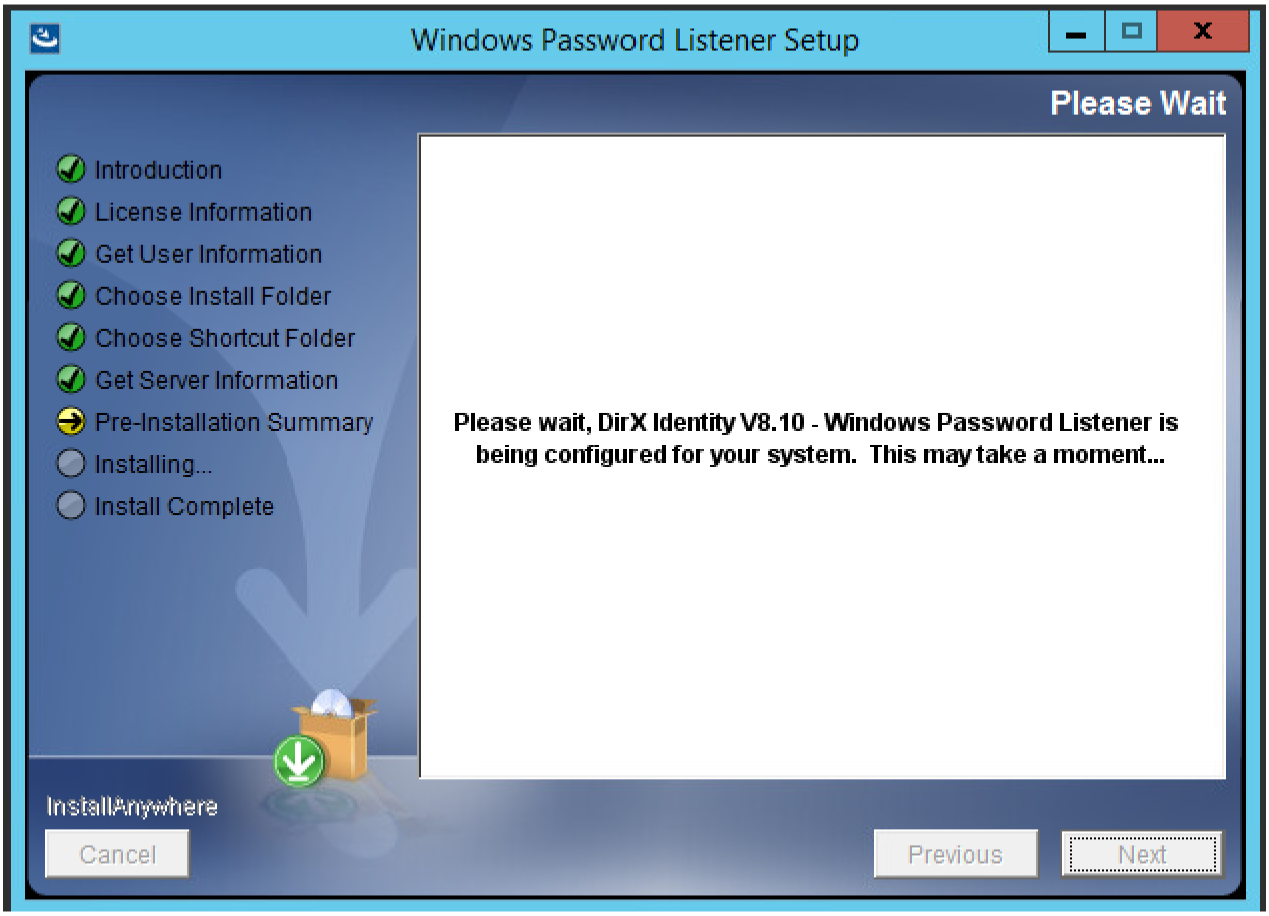
Shortcut Folder:
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Sta

UseSSL:
0

Server address:
server01

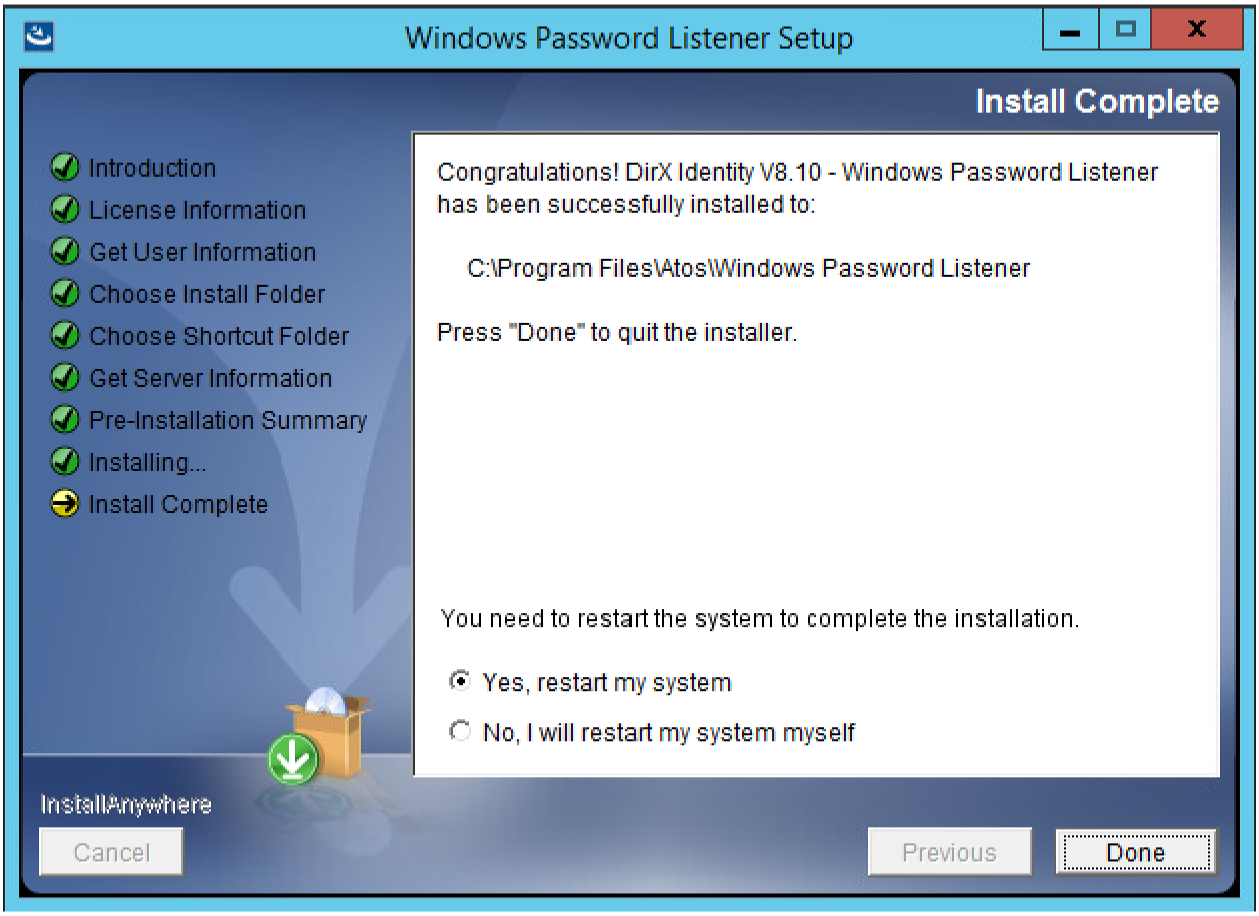
Server port:

- Setup displays the installation selections you have made and asks you to review them.
- Click **Previous** to change any settings you have made. Otherwise, click **Install**.



Please wait, DirX Identity V8.10 - Windows Password Listener is being configured for your system. This may take a moment...

- Setup displays the installation status.
- When Setup completes the installation, it displays the following dialog.



Congratulations! DirX Identity V8.10 - Windows Password Listener has been successfully installed to:

C:\Program Files\Atos\Windows Password Listener

Press "Done" to quit the installer.

You need to restart the system to complete the installation.

● Yes, restart my system

○ No, I will restart my system myself

- Click **Done** to exit Setup.DirX Identity Windows Password Listener installation is now complete.
- Wait for restart of the computer.The restart is necessary to register the Windows Password Listener Plugin DLL correctly into the LSASS service of the Windows domain controller.

7.2. Unattended (Silent) Installation/Uninstallation

You can install the Windows Password Listener on a machine without interaction.Follow these steps to create a silent setup:

- Copy the content of the folder **DirXIdentity/WinPWListener** from the DVD to a folder on your machine.
- Customize the file **dirxidty_wpl.properties.**
- Start the installation program in the folder on your machine.
- Check for errors

Here is the content of the file **dirxidty_pwl.properties**:

```
######################################################################
#########
# DirX Identity - Windows Password Listener install properties for
# InstallAnywhere
#####################################################################
#########
# Release Information
# Release=8.10
# Version=8.10
# Build=nn
# CreationDate=YYYYMMDD
#####################################################################
#########
# installer created with InstallAnywhere by Flexera
# InstallAnywhere 2021 Build 6526
#####################################################################
#########
# InstallAnywhere install properties
#####################################################################
#########
# UI mode for the installer
# INSTALLER_UI=[SILENT | CONSOLE | GUI | SWING | AWT]

# default for Windows: swing
# default for Unix: console

###############################################
# Note for Windows:
# if INSTALLER_UI is set to swing, than installer does not prompt
with a
# dialog "Not enough space...", if necessary
###############################################

#INSTALLER_UI=swing
#####################################################################
#########
# own DirX Identity - Windows Password Listener install properties
#####################################################################
#########
#--------------------------------------------------------------------
---------
#Get User Information
#--------------------
#PROP_DX_USER_INFORMATION_1=<userName>
```

```
# default:
#PROP_DX_USER_INFORMATION_1=<login user>

#PROP_DX_USER_INFORMATION_2=<companyName>
# default:
#PROP_DX_USER_INFORMATION_2=<>

#--------------------------------------------------------------------
---------
#Choose Install Folder
#---------------------
# PROP_USER_INSTALL_DIR=<path>

# default for Windows:
# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$Atos$/$Windows Password
Listener

# Note for Windows:
# If an install path for Windows Password Listener is found in the
registry,
# then this path will be taken!

# PROP_USER_INSTALL_DIR=$PROGRAMS_DIR$$/$Atos$/$Windows Password
Listener
#--------------------------------------------------------------------
---------
#Choose Shortcut Folder
#----------------------
# PROP_USER_SHORTCUTS=<program group>

# default:
# PROP_USER_SHORTCUTS=$WIN_COMMON_PROGRAMS_MENU$$/$Atos DirX
Identity$/$Windows Password Listener

# Note for Windows:
# If a program group for DirX Identity is found in the registry,
# than this program group is taken!

#--------------------------------------------------------------------
---------
#Get Information about the Message Server
#----------------------------------------
```

```
#PROP_DX_LOCAL_HOST=<hostName>

#PROP_DX_PORT=<port>
# default:
#PROP_DX_PORT=61616

#PROP_DX_Q_MGR=<Q-Name>

# use SSL
#PROP_DX_USE_SSL=[0|1]
# default:
#PROP_DX_USE_SSL=0
#--------------------------------------------------------------------
---------

#Get Service Account Information
#-------------------------------
#PROP_DX_ACCOUNT=<accountName>
#PROP_DX_USER_PASSWORD=<password>
#
---------------------------------------------------------------------
---------
# sleep time
# installation / uninstallation is waiting, when the service will be
removed
#PROP_DX_SLEEP_TIME=<msec>

# default:
#PROP_DX_SLEEP_TIME=10000
#
---------------------------------------------------------------------
---------

# Restart Windows - (De)-Installation in silent modus
# Note:
# When you want to force a reboot, if necessary,
# you can set the following variable

# PROP_RESTART_NEEDED=YES
#
---------------------------------------------------------------------
```

```
---------
```

8. Installing the JMS-Audit Handler

The JMS-Audit handler is neither configured nor updated automatically as part of the normal installation and configuration. This chapter describes the manual steps for its deployment. It requires an existing DirX Audit installation.

8.1. Deploying the JMS-Audit Handler

The JMS-Audit Handler is delivered with the DirX Identity product.You find it in the folder

product_media_DirX Identity/**Additions/jmsAuditHandler**.

The handler depends on the DirX Identity version and might be different from version to version.Therefore, always take the plug-in from the corresponding DirX Identity installation media and perform the following steps.

The folder **jmsAuditHandler** contains a zip file **com.siemens.idm.audit.jms.zip** with the **server.xml** configuration file and especially the **jar** file(s) in the **lib** subfolder.The file **com.siemens.idm.audit.jms.JmsAuditLogHandler.jar** contains the plug-in itself.As of DirX Identity 8.3 no further jar files are needed.If you already deployed the handler in a previous version, please make sure that no other jar is in the lib folder.

You have to deploy the handler to each DirX Identity Java-based Server.In the folder

dxi_install_path/**ids-j-***domain***-S***n***/extensions**

create a sub-folder **com.siemens.idm.audit.jms** and unzip to it the file **com.siemens.idm.audit.jms.zip**.

8.2. Configuring the JMS-Audit Handler

You configure the handler with DirX Identity Manager.In the **Connectivity** view's **Expert** view, navigate to the LDAP entry representing the DirX Identity Java-based server (IdS-J) and open the tab **Status and Auditing**.

- By checking the flag **JMS-based Auditing**, you enable auditing via JMS and disable auditing into files.
- Make sure the value for the **message broker URL** matches what you have configured in the DirX Audit Configuration Wizard for the DirX Identity JMS collector.The typical URL for non-SSL is: **tcp://host:30666**; the corresponding URL for SSL is: **ssl://host:30667**.
- The **JMS queue** must match what you have configured in the DirX Audit Configuration Wizard for the DirX Identity JMS collector.Note that beginning with DirX Audit V7, the queue names are tenant specific and so the queue name contains the tenant ID; for example, **dxt.***tenantID***.dxi**.
- Make sure that **user** and **password** match a user of the Message Broker with enough access rights for writing into the queue.The default DirX Audit Configuration Wizard creates a writer user for DirX Identity.As of DirX Audit V7 this user is tenant specific; the default writer is: **dxt-***tenantID***-writer**.

- If the JMS Audit handler is not able to send the audit records to the message server, it stores them temporarily into the **Audit Trail Folder**: one message per file.Per default the folder is local to the server.This is indicated by the placeholder ${IDM_HOME}: it represents the home folder of the Java server.If you specify a relative path, keep in mind that it is generated relative to the working folder of IdS-J, which is *dxi_install_path* /**ids-j-***domain***-S***n***/bin**.As soon as the handler can connect to the message broker again, it sends the audit records from the files and then deletes the files.So normally you don’t have to manage these files yourself, unless the connection problems last too long and the files fill the disk space.

If you use **SSL** for connecting to the DirX Audit Message Broker, make sure to import the CA certificate of the broker into the truststore of the Java VM running the IdS-J server.By default, this is the file *JRE_folder***/lib/security/cacerts**.You could use the following Java keytool command for the import assuming you have the CA certificate in file **ca.crt** (notation for Windows):

%JAVA_HOME%bin\keytool -importcert -trustcacerts -keystore cacerts -storepass *cacerts-pwd* **-alias** *ca-alias* **-file ca.crt**

If the handler doesn’t find its configuration in the IdS-J server configuration, it uses the configuration stored in the file **server.xml** from its extension folder.

Note that in this case the default LDAP configuration activates the audit file writer, which writes audit records into files (multiple records per file). This might be what you want or not. In any case, you have to care about moving or deleting these files to avoid filling up your disk.

You might use the same ActiveMQ message broker for DirX Identity and DirX Audit. This might help to simplify the overall installation by reducing the number of installed components and services.

9. The Java for DirX Identity

Many essential DirX Identity components are implemented in Java. Therefore, at least one Java installation is required for using the product.

The Java for DirX Identity is Java 11, which is used by the core components of DirX Identity, such as Java-based servers, DirX Identity Manager and the Configuration utility.

Some DirX Identity components require deployment into an external Tomcat which runs with Java 11. The Java instance used by that Tomcat depends on the related Tomcat configuration.

In contrast to previous releases, this version needs an external Java installation and does not provide any embedded Java environment.

The advantages of a customer-supplied Java installation include:

- The external Tomcat for DirX Identity applications can be configured so that they use this Java installation, too.
- The installation can also be used for internet browser or browser applications.
- Updating the Java installation is straightforward, with an official update package for the appropriate version. See the section “Security Updates for a Customer-supplied Java Runtime Environment“ for details.

9.1. Requirements Regarding the Java for DirX Identity

A customer-supplied Java must satisfy the following requirements to be selectable as the Java for DirX Identity:

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

Supported Java products are for example:

- Oracle Java SE 11 (LTS)

9.2. Security Updates for the Java for DirX Identity

Adoptium Eclipse Temurin JDK-11 This section describes how to perform security updates for the Java for DirX Identity.

9.2.1. Security Updates for a Customer-supplied Java Runtime Environment

This Java environment can only be updated with an official, downloadable update for the appropriate version (for example 11.0.xx), using the related standard method.

You must download the appropriate 64-bit patch.

General procedure:

- Stop all DirX Identity services and close all DirX Identity programs.
- If the file *dxi_java_home*/**lib/security/cacerts** contains own certificates, create a backup copy of that file so that it is outside *dxi_java_home*.
- Download and install the Java update. Regarding the Java installation path, your options are:
  - Specifying the installation path so that it matches the current path of *dxi_java_home*. This ensures consistency with your product installation. This option is not recommended if your *dxi_java_home* already contains a path name of the form **java-11.***number*.
  - Using the default installation path (for example, **C:\Program Files\Java\java-11.***number*). This results into a new value for *dxi_java_home* to be propagated to the DirX Identity installation.
- Put your own certificates from the backup copy into the updated and potentially relocated file *dxi_java_home*/**lib/security/cacerts**.
- If the Java update from previous steps results in a different installation path, you must perform additional actions according to the section “Managing a Relocated Customer-Supplied Java”.
- To verify your update regarding the Java version, run the suitable command in *dxi_java_home*/**bin**:
  - **.\java -version** (Windows platforms)
  - **./java -version** (UNIX platforms)
- Restart the services.

9.2.2. Managing a Relocated Customer-Supplied Java

These are the actions to be performed when the customer-supplied Java has been relocated due to a Java update.

1. Revise these files regarding the new location of this Java :
   - Windows only: *install_path*/**setdxienv.bat** (setting of DXI_JAVA_HOME). Ensure that you specify the related path in Windows notation when updating this file. Here is a sample line:

     SET DXI_JAVA_HOME=C:\Program Files\Java\java-11

- UNIX only: *install_path***/.dirxmetarc** (setting of DXI_JAVA_HOME). Ensure that you specify the related path in UNIX notation when updating this file. Here is a sample line:

  DXI_JAVA_HOME=/opt/java-11

- All platforms: *install_path*/configuration.ini (setting of dxi.java.home).

Ensure that you specify the related path in Windows notation with escaped characters ":" following the drive letter and "\" character when updating this file for a Windows platform. Here is a sample line for Windows:

```
dxi.java.home=C\:\\Program Files\\Java\\java-11
```

Ensure that you specify the related path in UNIX notation with escaped "\" character when updating this file for a UNIX platform. Here is a sample line for UNIX:

```
dxi.java.home=/opt/java-11
```

2. Perform Initial Configuration for the Message Broker and the Java-based Servers.
3. If you have configured Tomcat so that it uses the Java for DirX Identity, then configure Tomcat so that it uses the relocated Java.

10. Additional Topics

This chapter provides additional information that is useful for understanding and administering the DirX Identity system.

This information is especially useful when some steps fail during the configuration. Check the log file to find out which part(s) did not run. Correct the error and start the configurator again. You may only select those steps that did not finish successful.

10.1. Disk Space Calculation

To calculate the required disk space you will need for a DirX Identity installation, you should take several issues into account:

1. The space for DirX Identity.(See the section "Disk Space Requirements" in the chapter "Introduction".)
2. Running auditing requires additional disk space.
3. The space needed for the work and status areas where DirX Identity stores its temporary and permanent files.

The next sections discuss disk space requirements for auditing and DirX Identity working and status files and areas.

10.1.1. Space for Auditing

The required space for auditing depends on these issues:

- Remove regularly auditing information from this area. Either import it into a database or store it on backup devices.
- Audit only the absolutely necessary objects in your Identity Store.
- Configure only the absolutely necessary attributes for these objects.
- Check whether you really need signed audit records. If you keep the audit area secure, this is not always necessary. Signed records require about double the space for auditing and slow down performance of real-time workflows considerably.

We recommend reserving enough space for auditing. Additionally, we recommend writing audit information to a separate disk to prevent influence on the server operation.

10.1.2. Space for Work and Status Areas

This issue can only be estimated and depends highly on several issues:

- The files you have configured to be stored in the status area (by default, all files are stored).
- The amount of data (number and size of entries) to be synchronized.
- The frequency of your scheduled workflows, the configured status expiration time and

the status compression mode.

Because it is easy to fill your disk with status information, DirX Identity is designed to ignore a full disk in that area, but DirX Identity is not able to handle this problem for the work area.

Therefore, we strongly recommend following these guidelines:

- Keep the work area and the status area on different disks.
- Mark only important files to be stored automatically in the status area (for example trace and report files but not data files with a huge amount of data).You can of course activate more files during a test phase, but do not forget to deactivate it at the end.
- Set individual status expiration times for each workflow.This helps to not overcrowd the directory with status entries.We recommend setting one month when the workflow runs every week, one week when it runs daily and one day when it runs every 10 minutes.
- Set individual status expiration times for all Java-based Identity Servers.

This all should help to make your system more reliable and to restrict the use of resources.

10.2. Schema and Content Handling

During configuration, DirX Identity prepares the LDAP directory according to the requirements of DirX Identity.It extends the LDAP directory schema for the Connectivity Configuration tree and imports the basic content into that tree that contains the DirX Identity Default Applications.

To run workflows, specific object classes and attributes for each agent type are needed to work correctly.You must extend the schema for the joined data in the Identity Store with the agent specific schema parts.

The next sections describe these procedures in more detail.

10.2.1. Setup of the Schema for the Connectivity Configuration

DirX Identity extends the schema of the defined LDAP directory with the object and attribute definitions needed for the DirX Identity Connectivity Configuration to permit correct DirX Identity operation.

10.2.2. Basic Content Extension

In this step, DirX Identity writes all pre-configured objects (workflow, activity, job, connected directory definitions and much more) from LDIF files to the LDAP directory. Based on this information, the DirX Identity administrator can configure his own objects and synchronizations with the powerful features of DirX Identity.

10.2.3. Target System Specific Schema Extensions

To set up the Identity Store schema depending on the type of target systems you'd like to provision is a task that should be thoroughly planned. You should only set up the required object classes and attributes to guarantee high performance and easy handling.

DirX Identity automatically extends the schema if you have selected the Sample Domain. A minimal set of attributes and object classes is defined for all target systems that require LDAP schema extensions. Note that not all target systems require schema changes. Using additional attributes in the Sample Domain requires a manual additional schema extension. Use the methods for customer domain schema extensions that are described in the next sections.

For customer domain schema extension, DirX Identity comes with several complete sets of attribute and object class extensions for each supported target system type. To perform the schema extension, perform these steps:

- We strongly recommend backing up your directory before you run any scripts! You cannot reverse schema extensions in a directory.

   1. Open the directory *install_path/***schema/tools**
   2. Open the sub directory for your directory type: **dirx-ee** for DirX installation
   3. Copy the entire **Customer Domain** subdirectory and name it **Customer Domain.orig**.
   4. Update the schema definitions in the **Customer Domain** subdirectory according to your requirements.

      The following steps need to be performed:

      - Directory type **dirx-ee** (used for DirX V8.3 or higher):

        Select the LDIF file of your DirX Identity Connectivity package in the subdirectory **ldif**; for example, **dirx.nt.ldif**.

        Drop all the attributes in which you are not interested by removing the appropriate "MODIFY" records that refer to "attributeTypes" creations.

        Remove the attributes from the object class definitions by dropping the appropriate LDAP attribute names from the "MODIFY" records that refer to "objectClasses" creations.

        If indexes were defined for the attributes, drop the attribute types from the "dbconfig_opt" statements in the **dirxadm** script of your DirX Identity Connectivity package; for example, **DirXmetahub-schema.Nt.adm** (for NT)

   5. Run the script **agent-schema.**bat (on Windows) or **agent-schema.sh** (on Linux) under schema/tools

- Type the password of the DirX Identity administrator **admin**
- Select the DirX Identity Connectivity package to install this part of the schema extension. (Each package has to be selected separately.)
- Select whether to create the attribute indexes

The schema extensions are installed now. Check the **trace.txt** file at the end for errors (the exit codes at the end should be 0).

10.2.4. Indexed Attributes

DirX Identity requires a set of indexes. The minimum number of indexes is 84, the maximum number of indexes is 137 (all target system schema extensions performed).

This information is especially important to set up DirX correctly.

10.2.4.1. DirX Identity Connectivity Configuration (17 attribute indexes)

dxmActive
dxmActivityStatusData-DN
dxmC
dxmDisplayName
dxmEndTime
dxmExitCode
dxmExpirationTime
dxmName
dxmOkStatus
dxmOrigWorkflow-DN
dxmResult
dxmScheduleName
dxmStartTime
dxmStatusExpirationTime
dxmType
dxmWarningStatus
dxmWorkflowInstID

10.2.4.2. DirX Identity Provisioning Configuration Extensions (67 attribute indexes)

dxmOprEventDivision
dxmOprMaster
dxmOprOriginator
dxmOprTriggerOrigin
dxmPwdLastChange
dxrAccessRightLink
dxrApproverLink
dxrApproverPotentialLink
dxrAssignedAccounts
dxrAssignedGroups
dxrAssignFrom
dxrAssignTo
dxrAssignmentLink
dxrCurrentParticipants
dxrDeleteDate
dxrDisableStartDate
dxrDisableEndDate
dxrEndDate
dxrErrorExpDate

dxrError
dxrExpirationDate
dxrGroupLink
dxrGroupMemberAdd
dxrGroupMemberDelete
dxrGroupMemberIgnore
dxrGroupMemberImported
dxrGroupMemberOK
dxrInheritedPrivilegeLink
dxrInheritedUserFacetPrivilegeLink
dxrIsActive
dxrIsExtensionGroup
dxrIsInconsistent
dxrName
dxrNeedsApproval
dxrNextApprovalDate
dxrObjectComplete
dxrObjectType
dxrOperationImp
dxrPeerTS
dxrPermissionLink
dxrPrimaryKey
dxrPrivilegeLink
dxrPrivilegesGrantedLink
dxrPwdChangedTime
dxrPwdChangeState
dxrReference
dxrResourceGroupLink
dxrResourceLink
dxrRoleID
dxrRoleLink
dxrRPvalues
dxrStartDate
dxrState
dxrSubjectLink
dxrSubjectGroupLink
dxrTBA
dxrToDo
dxrToPeer
dxrTSState
dxrTSStateExtended
dxrType
dxrUID
dxrUsedBy
dxrUserAssignementPossible
dxrUserLink
employeeNumber
uniqueMember

10.2.4.3. DirX Identity Connectivity Package Schema Extensions (18 attribute indexes)

If you install the sample domain, you need 18 additional indexes.

A) ADS: (7)

dxmADsComputerName
dxmADsDNSdomainName
dxmADsDomain
dxmADsForest
dxmADsGuid
dxmADsSamAccountName

B) Exchange 5.5: (2)

dxmEXcn
dxmEXrfc822Mailbox

C) Notes: (4)

dxmLNfullName
dxmLNlistName
dxmLNnoteID
dxmLNshortName

D) ODBC: (4)

dxmODBCdatabaseName
dxmODBCdatabaseType
dxmODBCfirstName
dxmODBClastName

E) SAP/R3-UM: (1)

sapUsername

10.2.4.4. DirX Identity Agent Schema Extensions for a Customer Domain (52 attribute indexes max)

For each Connectivity Package schema extension, you need the corresponding number of indexes. This list shows the maximum number delivered with each default set. If you extended the schema with fewer attributes, the number of indexes is lower.

A) ADS: (6)

dxmADsComputerName
dxmADsDNSdomainName
dxmADsDomain
dxmADsForest
dxmADsGuid
dxmADsSamAccountName

B) Exchange: (8)

dxmEXcn
dxmEXdescription
dxmEXemployeeNumber
dxmEXgivenName
dxmEXname
dxmEXrdn
dxmEXrfc822Mailbox
dxmEXsn

C) HDMS: (11)

dxmHDbuilding
dxmHDchristianName
dxmHDcompany
dxmHDcountry
dxmHDdmsid
dxmHDlocation
dxmHDname
dxmHDorg1
dxmHDorg2
dxmHDorg3
dxmHDsortName

D) Notes: (10)

dxmLNcomment
dxmLNemployeeID
dxmLNfirstName
dxmLNfullName
dxmLNinternetAddress
dxmLNlastName
dxmLNlistDescription
dxmLNlistName
dxmLNnoteID
dxmLNshortName

E) ODBC: (4)

dxmODBCdatabaseName
dxmODBCdatabaseType
dxmODBCfirstName
dxmODBClastName

F) SAPR3/HR: (4)

dxmSAPR3HRcommonName
dxmSAPR3HRgivenName
dxmSAPR3HrpersonnelNumber
dxmSAPR3HRsurName

G) SAP/R3-UM: (1)

sapUsername

Appendix A: DirX Identity Web Center - Kerberos Authentication

This document describes how to set up Kerberos authentication for Web Center via the SPNEGO mechanism.

A.1. Introduction

Some terms used in this document:

- **Host** - The simple name of the host with the Tomcat server Web Center is deployed into.For example, “alpha“.
- **Domain** - The fully qualified domain name of the host; for example, “beta.com“.
- **Service Principal Name** - The service principal name is http/host.domain@DOMAIN, for example “http/alpha.beta.com@BETA.COM“.
- ***tomcat_install_path*** - The installation folder of the Tomcat server, for example “C:/Program Files/Apache/Tomcat 9016”.Note that “*tomcat_install_path*“ is just a notation used in this document.Always replace it with the real path name of the Tomcat installation folder.

Restrictions:

- Kerberos authentication does not work if browser and Tomcat run on the same machine.

A.2. Windows Prerequisites

For Kerberos on Windows, you must create a Windows user account, register the service principal name for that account, and create a keytab for the service principal name.This section describes how to perform these steps on a Windows Server 2012 R2. The details might be different on other server versions like Windows Server 2016 and 2019.

A.2.1. Creating an Active Directory User Account

Create a user account for Kerberos in Active Directory via program “Active Directory Users and Computers”.Assign a “User logon name” and a password.Check the flag “Password never expires”.

Kerberos on Windows works with one of three different encryption modes:

- **RC4-HMAC-NT** – The default 128-bit encryption.
- **AES256-SHA1** – AES256-CTS-HMAC-SHA1-96 encryption. This is the recommended encryption mode.
- **AES128-SHA1** – AES128-CTS-HMAC-SHA1-96 encryption.

When using AES encryption for Kerberos (as recommended), open the created user account and select tab “Account”. In the options list, check the flag “This account supports Kerberos AES 128-bit encryption” or “This account supports Kerberos AES 256-bit encryption” as appropriate.

In the following examples, we assume the logon name is “beta\kerberosUser”.

A.2.2. Registering the Service Principal Name

Use the windows tool **setspn** to register the service principal name for the created Kerberos account:

```
setspn -u -s <servicePrincipalName> <accountName>
```

For example

```
setspn -u -s http/alpha.beta.com@BETA.COM beta\kerberosUser
```

Note that the service principal name must not be registered for more than one account. You can check this with

```
setspn -q <servicePrincipalName>
```

For example

```
setspn -q http/alpha.beta.com@BETA.COM
```

You can unregister a service principal name with

```
setspn -d <servicePrincipalName> <accountName>
```

After having registered the service principal name, open the Kerberos user account again and select the new tab “Delegation”. Select the option “Trust this user for delegation to any service (Kerberos only)”.

A.2.3. Creating the Keytab File

Use the Windows utility **ktpass** to create a keytab for the service principal name. The keytab is used on the Tomcat server to perform Kerberos authentications.

```
ktpass /princ <servicePrincipalName>
       /ptype KRB5_NT_PRINCIPAL
       /mapuser <accountName>
       /out <keytabFileName>
       /crypto <AES256-SHA1 or AES128-SHA1 or RC4-HMAC-NT>
       /pass *
       /kvno 0
```

For example:

```
ktpass /princ http/alpha.beta.com@BETA.COM
       /ptype KRB5_NT_PRINCIPAL
       /mapuser beta\kerberosUser
       /out alpha.keytab
       /crypto AES256-SHA1
       /pass *
       /kvno 0
```

You are prompted for the password of the Kerberos user twice.

Note that you must create a new keytab file each time you change the Kerberos account in Active Directory.

Now open the Kerberos user account again and select tab “Account”.The “User logon name” should have changed to the service principal name.

A.3. Tomcat Configuration

In this section, we create some configuration files on the Tomcat server.We suggest putting the files into the folder *tomcat_install_path***/conf** but you can choose any other folder as well.Make sure that all the created files are readable by the Tomcat service.

A.3.1. Keytab

Copy the keytab file to *tomcat_install_path***/conf**.In the subsequent examples, we assume the keytab file is copied to *tomcat_install_path***/conf/alpha.keytab**.

A.3.2. File krb5.conf

Create file *tomcat_install_path**/conf/krb5.conf* with the following content:

```
#
# Kerberos configuration file for running JGSS applications.
# Adapt the entries to your environment.
#

[libdefaults]
    default_realm = <DOMAIN>
    permitted_enctypes = aes256-cts aes128-cts
    allow_weak_crypto = false
    kdc_timesync = 0
    kdc_default_options = 0x40000010
    clockskew = 300
    check_delegate = 0
    ccache_type = 3
    kdc_timeout = 60000

[realms]
    <DOMAIN> = {
        kdc = <keyDistributionCenter>:<keyDistributionCenterPort>
    }

[domain_realm]
    .<domain> = <DOMAIN>
```

Note that some lines have been splitted for better readability.

Replace each occurrence of

- <DOMAIN> with the fully qualified domain name in uppercase letters.
- <domain> with the fully qualified domain name in lowercase letters.
- <keyDistributionCenter> with the IP address or fully qualified host name of the Kerberos key distribution center, which is part of the Windows domain controller.
- <keyDistributionCenterPort> with the port number of the Kerberos key distribution center, which is usually 88.

Adjust the encryption types if necessary. They must include the encryption type of the created Windows user account. For example, add “rc4-hmac” if necessary.

The **krb5.conf** file for our sample data is:

```
#
# Kerberos configuration file for running JGSS applications.
# Adapt the entries to your environment.
#

[libdefaults]
    default_realm = BETA.COM
    permitted_enctypes = aes256-cts aes128-cts
    allow_weak_crypto = false
    kdc_timesync = 0
    kdc_default_options = 0x40000010
    clockskew = 300
    check_delegate = 0
    ccache_type = 3
    kdc_timeout = 60000
```

```
[realms]
    BETA.COM = {
        kdc = dc.beta.com:88
    }

[domain_realm]
    .beta.com = BETA.COM
```

A.3.3. File krb5-jaas.conf

Create file *tomcat_install_path***/conf/krb5-jaas.conf** with the following content:

```
/**
 * JAAS configuration file for JGSS.
 * Modify the entries to suit your environment.
 */

/* Needed for SPNEGO/Kerberos */
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
        debug=true
        doNotPrompt=true
        useKeyTab=true
        keyTab="<keytabPathName>"
        storeKey=true
        principal="<servicePrincipalName>"
    ;
};
```

Replace

- <servicePrincipalName> with the service principal name.
- <keytabPathName> with the full path name of the keytab file.

The **krb5-jaas.conf** file for our sample data is:

```
/**
 * JAAS configuration file for JGSS.
 * Modify the entries to suit your environment.
 */
```

```
/* Needed for SPNEGO/Kerberos */
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
        debug=true
        doNotPrompt=true
        useKeyTab=true
        keyTab="tomcat_install_path/conf/alpha.keytab"
        storeKey=true
        principal="http/alpha.beta.com@BETA.COM"
    ;
};
```

A.3.4. Java System Properties

Assign the path names of the Kerberos configuration files to Java system properties of the Tomcat service:

```
-Djava.security.krb5.conf=<krb5PathName>
-Djava.security.auth.login.config=<krb5jaasPathName>
```

Replace

- <krb5PathName> with the full path name of file **krb5.conf**.
- <krb5jaasPathName> with the full path name of file **krb5-jaas.conf**.

The values for our sample data are

```
-Djava.security.krb5.conf=tomcat_install_path/conf/krb5.conf
-Djava.security.auth.login.config
                         =tomcat_install_path/conf/krb5-jaas.conf
```

You can also enable some output for debugging purposes which will be written to some Tomcat log files:

```
-Dsun.security.krb5.debug=true
-Dsun.security.jgss.debug=true
```

To set the Java system properties for a Tomcat running as a Windows service, open the service’s “Configure Tomcat” item in the Windows start menu; another way to start the configurator is to run the program **tomcat9w.exe** in Tomcat’s **bin** folder manually. In the configurator, select the Java tab and then add the properties to the list of Java Options.

If running Tomcat from a batch script, assign the system properties to the environment variable “CATALINA_OPTS” before starting Tomcat, for example:

```
set KRB5_FILE=-Djava.security.krb5.conf=
               tomcat_install_path/conf/krb5.conf
set KRB5_JAAS_FILE=-Djava.security.auth.login.config =
               tomcat_install_path/conf/krb5-jaas.conf
SET KRB5_DEBUG=-Dsun.security.krb5.debug=true
SET JGSS_DEBUG=-Dsun.security.jgss.debug=true
SET CATALINA_OPTS=%KRB5_FILE% %KRB5_JAAS_FILE% %KRB5_DEBUG%
%JGSS_DEBUG%
```

Note that some lines have been splitted for better readability.

A.3.5. Copying the SPNEGO Jar File

Copy the SPNEGO jar file **spnego-tomcat9.jar** delivered with DirX Identity to Tomcat’s lib folder *tomcat_install_path***/lib**.

A.3.6. Increasing the Maximum HTTP Header Size

Tomcat limits the maximum size of HTTP headers by default to 4kb and discards any request with larger headers. Kerberos tickets are transferred from the browser to the server in an HTTP header. For Windows users with many groups the Kerberos ticket may become quite large so that the header size easily exceeds the default maximum size.

Therefore, you should increase the maximum HTTP header size permitted by Tomcat to 32kb or 64kb by adding the property maxHttpHeaderSize to your HTTP and/or HTTPS connector configuration in the file *tomcat_install_path***/conf/server.xml**.

```
<Connector port="8080" ...
    maxHttpHeaderSize="65536" .../>
<Connector port="8443" ...
    maxHttpHeaderSize="65536" .../>
```

A.4. Web Center Configuration

A.4.1. Activating SPNEGO Authentication

A.4.1.1. File web.xml

Uncomment the security settings in the deployment descriptor **WEB-INF/web.xml**:

```
<!-- SPNEGO Windows single sign-on security settings -->
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Restricted Area</web-resource-name>
        <url-pattern>*.do</url-pattern>
        <url-pattern>*.jsp</url-pattern>
        <url-pattern>/saveFile</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>SpnegoAuthenticatedUser</role-name>
    </auth-constraint>
</security-constraint>

<security-role>
    <description>SPNEGO authenticated users</description>
    <role-name>SpnegoAuthenticatedUser</role-name>
</security-role>
```

A.4.1.2. File webCenter-*dxiDomain*.xml

Add the Kerberos authentication elements “Realm” and “Valve” to Web Center’s context descriptor file **webCenter-***dxiDomain***.xml**.

The file is located in the folder *tomcat_install_path**/conf/***engineName/hostName*, where *engineName* and *hostName* depend on your Tomcat installation. In most cases, the location is *tomcat_install_path***/conf/Catalina/localhost*.

```
<Context ...>
  ...
  <!-- Kerberos authentications -->
  <Realm
      className="com.siemens.symphonia.spnego.SPNEGOVoidRealm"/>

  <Valve
     className="com.siemens.symphonia.spnego.SPNEGOAuthenticator"
     servicePrincipalName="<servicePrincipalName>"
     changeSessionIdOnAuthentication="false"/>
</Context>
```

Replace

- <servicePrincipalName> with the service principal name.

The context descriptor file for our sample data is:

```
<Context ...>
  ...
  <!-- Kerberos authentications -->
  <Realm
      className="com.siemens.symphonia.spnego.SPNEGOVoidRealm"/>

  <Valve
     className="com.siemens.symphonia.spnego.SPNEGOAuthenticator"
     servicePrincipalName="http/alpha.beta.com@BETA.COM"
     changeSessionIdOnAuthentication="false"/>
</Context>
```

A.4.2. Configuring User Mapping

A Kerberos authentication provides the authenticated user’s Windows account name and the fully qualified Windows domain name. The task is to map these data to a user in the DirX Identity database. Usually this is done by searching for a target system matching the domain name, and then by looking for an account matching the Windows account name in that target system. If the Windows credentials are stored in a user attribute, an alternative way is to search the user directly in the user tree.

The user mapping configuration is done in the deployment descriptor **WEB-INF/web.xml**.

Note that since **web.xml** is an XML file, ampersands in configuration values must be replaced with the corresponding XML character entity reference “&”.

Some configuration parameters accept a regular expression as value. The syntax for regular expressions is described in the Java API documentation of Java class “java.util.regex.Pattern”. The part of a pattern marked in bold letters shows the captured substring.

A.4.2.1. Activating the SSO Header Filter

Enable the filter by uncommenting it:

```
<!-- SSO header filter definition -->
<filter>
  <filter-name>SSOHeaderFilter</filter-name>
  <display-name>SSO Header Filter</display-name>
  <description>
    Evaluates single sign-on information passed in HTTP headers
  </description>
```

```
    <filter-class>
      com.siemens.webMgr.filter.SSOHeaderFilter
    </filter-class>
    ...
  </filter>
```

Set the filter’s authentication type to “SPNEGO/Kerberos”:

```
<init-param>
    <param-name>authType</param-name>
    <param-value>SPNEGO/Kerberos</param-value>
</init-param>
```

Set the filter’s header name to “RemoteUser”:

```
<init-param>
    <param-name>headerName</param-name>
    <param-value>RemoteUser</param-value>
</init-param>
```

Once you have Kerberos authentication with Web Center running, you can switch the log level back to “error”.

Other initialization parameters are described in the following sections.

Activate the mappings for the SSO header filter by uncommenting them:

```
<!-- SSOHeaderFilter mappings -->
<filter-mapping>
    <filter-name>SSOHeaderFilter</filter-name>
    <url-pattern>*.do</url-pattern>
</filter-mapping>

<filter-mapping>
    <filter-name>SSOHeaderFilter</filter-name>
    <url-pattern>*.jsp</url-pattern>
</filter-mapping>

<filter-mapping>
    <filter-name>SSOHeaderFilter</filter-name>
    <url-pattern>/saveFile</url-pattern>
```

```
</filter-mapping>
```

While the filter definition sequence is arbitrary, the filter mapping sequence is not. Insert the mappings of the SSO header filter directly before the mappings of the Session filter.

A.4.2.2. User Mapping via Target System and Account

A.4.2.2.1. Extracting Account and Domain Name

The Windows credentials are passed in the format accountName*@*fullDomainName. The first task is to extract the Windows account name and domain name from the credentials string.

Set the type of the SSO header filter to “account”:

```
<init-param>
    <param-name>type</param-name>
    <param-value>account</param-value>
</init-param>
```

By default, the extracted account name is the substring of the Windows credentials preceding the first @ character

```
<init-param>
    <param-name>accountRegExpr</param-name>
    <param-value>([^@]*)@.*</param-value>
</init-param>
```

By default, the extracted domain name is the substring between the first @ character and the next dot, which gives the simple domain name:

```
<init-param>
    <param-name>domainRegExpr</param-name>
    <param-value>[^@]+@([^.]+)(?:[.].*)?</param-value>
</init-param>
```

To extract the fully qualified domain name, use

```
<init-param>
    <param-name>domainRegExpr</param-name>
    <param-value>[^@]+@(.*)</param-value>
```

```
</init-param>
```

For example, if the provided Windows credentials are “smith@beta.com”, the extracted account name is “smith”, while the domain name is “beta” for the first domain pattern, and “beta.com” for the second domain pattern.

A.4.2.2.2. Finding the DirX Identity Target System

The target system is by default the one whose attribute “dxrTSDomainName” matches the domain name extracted in the previous step.

You can configure base and filter for the search operation via context parameters:

```
<context-param>
  <param-name>
      com.siemens.webMgr.auth.targetSystemBase
  </param-name>
  <param-value>cn=TargetSystems,cn=<dxiDomain></param-value>
</context-param>

<context-param>
  <param-name>
    com.siemens.webMgr.auth.targetSystemFilter
  </param-name>
  <param-value>
    (&amp;(objectclass=dxrTargetSystem)(dxrTSDomainName=%DOMAIN))
  </param-value>
</context-param>
```

Replace

- <dxiDomain> with your DirX Identity domain.

The placeholder “%DOMAIN” is replaced at runtime with the extracted Windows domain.

The search filter for the the Windows credentials “smith@beta.com” is

```
(&(objectClass=dxrTargetSystem)(dxrTSDomainName=beta.com))
```

when using the first of the above domain patterns, and

```
(&(objectClass=dxrTargetSystem)(dxrTSDomainName=beta))
```

when using the second pattern.

A.4.2.2.3. Finding the DirX Identity Account

The account is by default the one whose attribute dxmADsSamAccountName matches the extracted account name. The search base is the target system found in the previous step. If no target system was found, the search extends over all target systems.

You can configure the filter for the search operation via a context parameter:

```
<context-param>
  <param-name>
      com.siemens.webMgr.auth.accountFilter
  </param-name>
  <param-value>
      (&amp;(objectclass=dxrTargetSystemAccount)
          (dxmADsSamAccountName=%ACCOUNT))
  </param-value>
</context-param>
```

The placeholder “%ACCOUNT” is replaced at runtime with the Windows account extracted from the provided Windows credentials, the placeholder “%DOMAIN” (which is not used by default) with the extracted Windows domain.

The search filter for our sample Windows credentials “smith@beta.com” is

```
(&(objectClass=dxrTargetSystemAccount)
  (dxmADsSamAccountName=smith))
```

A.4.2.2.4. Finding the DirX Identity User

The user is the one referenced by attribute “dxrUserLink” of the DirX Identity account found in the previous step.

You can configure a different attribute via a context parameter:

```
<context-param>
  <param-name>
      com.siemens.webMgr.auth.accountUserLink
  </param-name>
  <param-value>
      dxrUserLink
  </param-value>
```

```
</context-param>
```

A.4.2.3. User Mapping via User Attribute

A.4.2.3.1. Extracting the Windows Credentials

The Windows credentials are passed in the format *accountName**@**fullDomainName*. The first task is to extract the part of the credentials that is needed to find the corresponding DirX Identity user.

Set the type of the SSO header filter to “user”:

```
<init-param>
    <param-name>type</param-name>
    <param-value>user</param-value>
</init-param>
```

The value to be extracted for the user filter is either the complete Windows credentials with account and fully qualified domain name, or a substring thereof.

The first example extracts the complete credentials with account and fully qualified domain name:

```
<init-param>
    <param-name>userRegExpr</param-name>
    <param-value>(.*)</param-value>
</init-param>
```

To extract the credentials with simple domain name, use:

```
<init-param>
    <param-name>userRegExpr</param-name>
    <param-value>([^@]+@[^.]+)(?:[.].*)?</param-value>
</init-param>
```

To extract the Windows account only, use:

```
<init-param>
    <param-name>userRegExpr</param-name>
    <param-value>([^@]*)@.*</param-value>
</init-param>
```

For example, if the provided Windows credentials are “smith@beta.com”, the extracted substring is “smith@beta.com” for the first pattern, “smith@beta” for the second pattern, and just “smith” for the third one.

Finding the DirX Identity User

You can configure base and filter for the search operation via context parameters:

```
<context-param>
  <param-name>
      com.siemens.webMgr.auth.userBase
  </param-name>
  <param-value>cn=Users,cn=<dxiDomain></param-value>
</context-param>

<context-param>
  <param-name>
    com.siemens.webMgr.auth.userFilter
  </param-name>
  <param-value>
    (&amp;(objectclass=dxrUser)(<attrName>=%USER_ID))
  </param-value>
</context-param>
```

Replace

- <dxiDomain> with your DirX Identity domain.
- <attrName> with the name of the user attribute holding the Windows credentials.

The placeholder “%USER_ID” is replaced at runtime with the Windows credentials extracted in the previous step.

The search filter with attribute name “description” for the Windows credentials “smith@beta.com” is

```
(&(objectClass=dxrUser)(description=smith@beta.com))
```

when using the first of the above user patterns,

```
(&(objectClass=dxrUser)(description=smith@beta))
```

when using the second pattern, and

```
(&(objectClass=dxrUser)(description=smith))
```

when using the third pattern.

A.5. Browser Settings

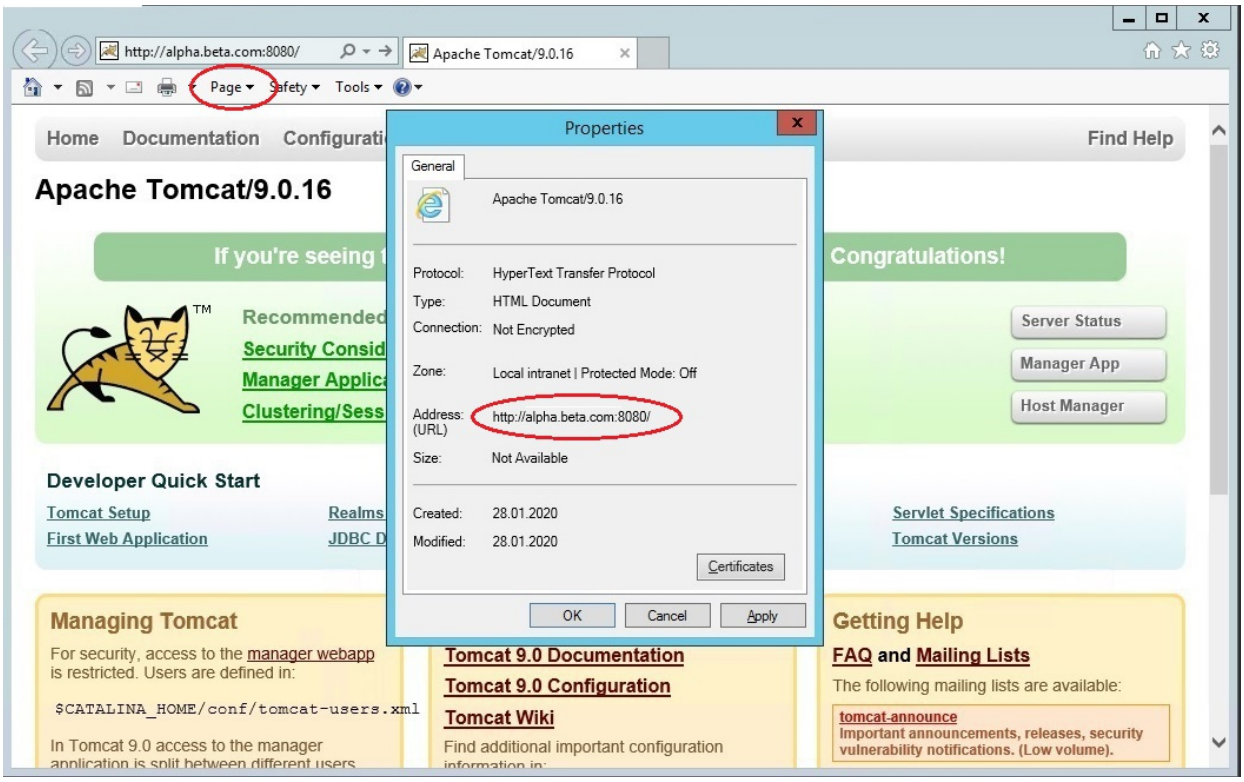
A.5.1. Internet Explorer

This section describes how to configure an Internet Explorer for Windows domain authentication based on Kerberos.This configuration requires Internet Explorer 11.

A.5.1.1. Configuring Local Intranet Sites

Internet Explorer requires servers to be configured in the category “Local intranet” to run Windows domain authentication based on Kerberos.

- Check if the Tomcat server belongs to the browser category “Local intranet” when accessing it.Go to the home page of your Tomcat, select item **Properties** from the **Page** menu, and check property **Zone**.



Apache Tomcat/9.0.16

Protocol: HyperText Transfer Protocol
Type: HTML Document
Connection: Not Encrypted

Zone: Local intranet | Protected Mode: Off

Address: (URL) http://alpha.beta.com:8080/

Size: Not Available

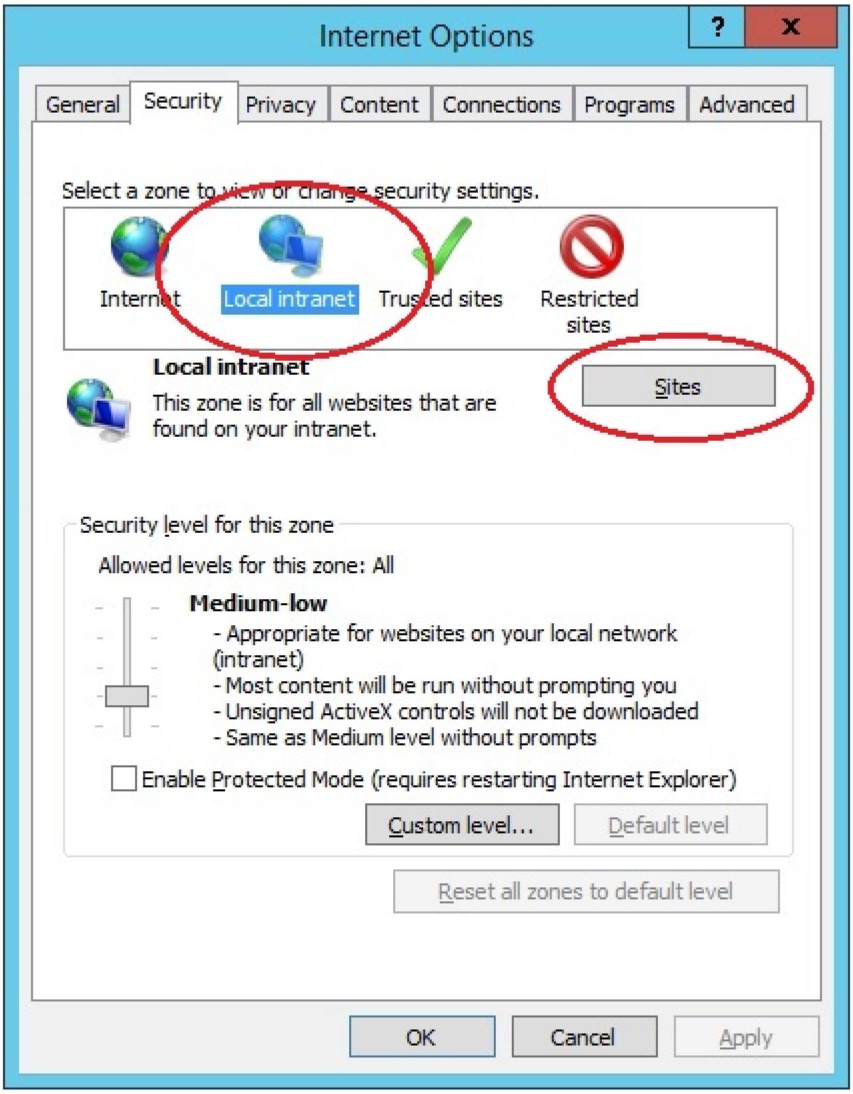
Created: 28.01.2020
Modified: 28.01.2020

If “Local intranet” is shown when accessing Tomcat, you can skip the configuration steps for local intranet sites.

- Configure local intranet sites:
  - In Internet Explorer, click **Tools**, and then click **Internet Options**.

    Click the **Security** tab.

- Click **Local intranet**.
- Click **Sites.**



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

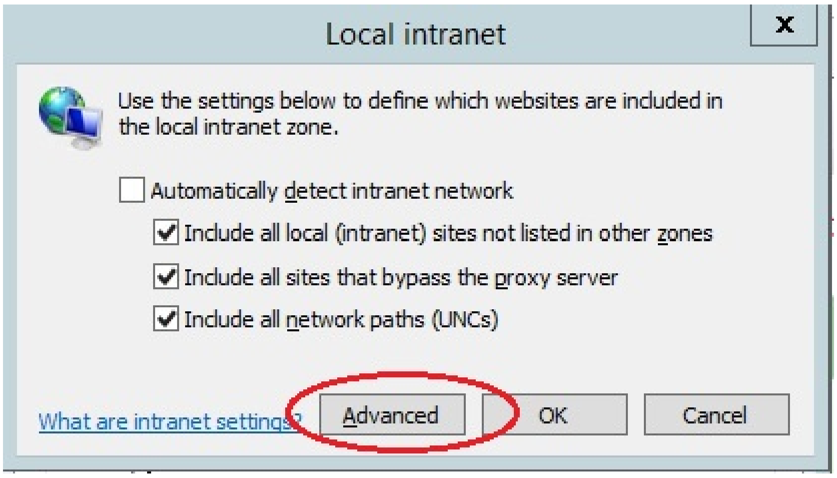
Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

□ Enable Protected Mode (requires restarting Internet Explorer)

- Ensure that **Include all sites that bypass the proxy server** is checked, then click **Advanced.**



Use the settings below to define which websites are included in the local intranet zone.

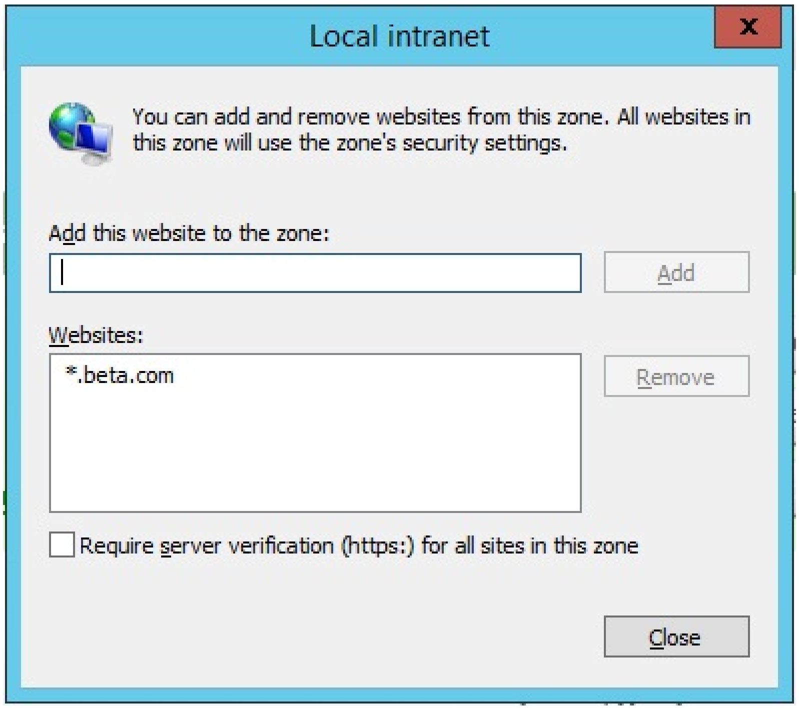
□ Automatically detect intranet network

☑ Include all local (intranet) sites not listed in other zones

☑ Include all sites that bypass the proxy server

☑ Include all network paths (UNCs)

- In the Local intranet (Advanced) dialog box, enter all relative domain names that will be used for Tomcat servers with enabled Windows domain authentication (for example, *.beta.com).



Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

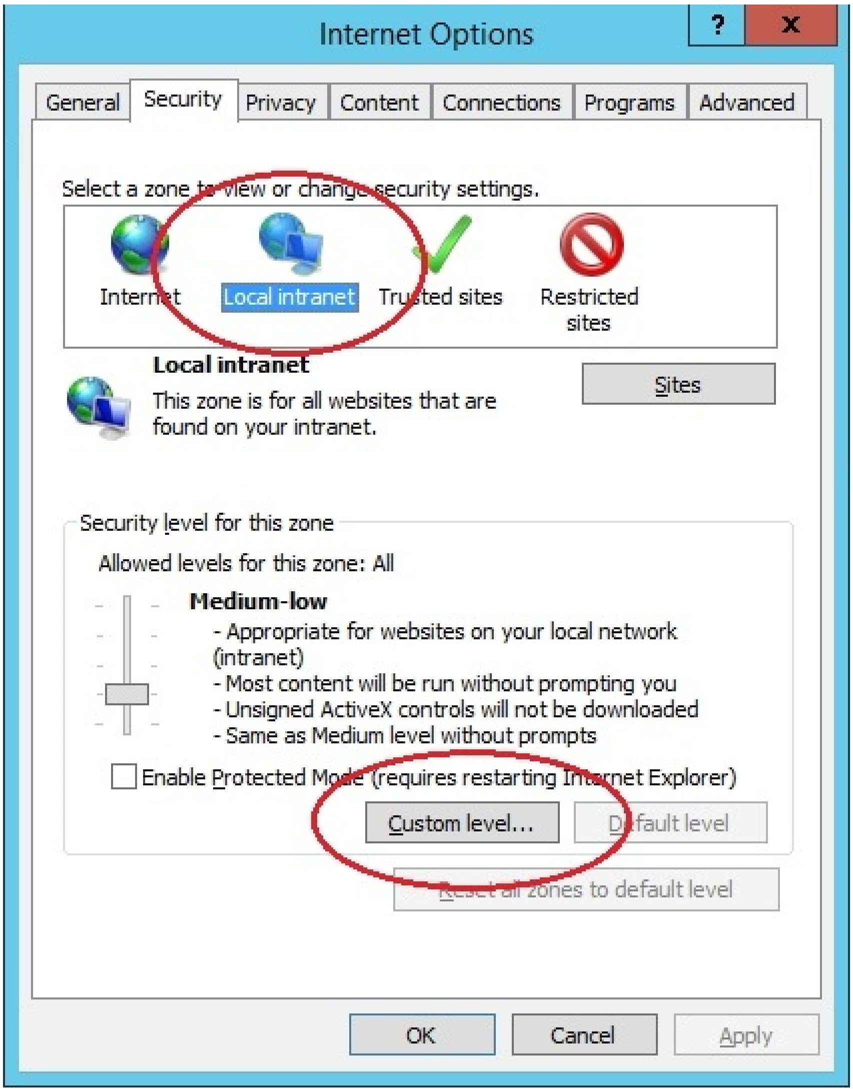
*.beta.com

□ Require server verification (https:) for all sites in this zone

- Click **Close** to close the dialog boxes.

A.5.1.2. Configuring Intranet Authentication

- Next, click the **Security** tab, click **Local intranet**, and then Click **Custom Level**.



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

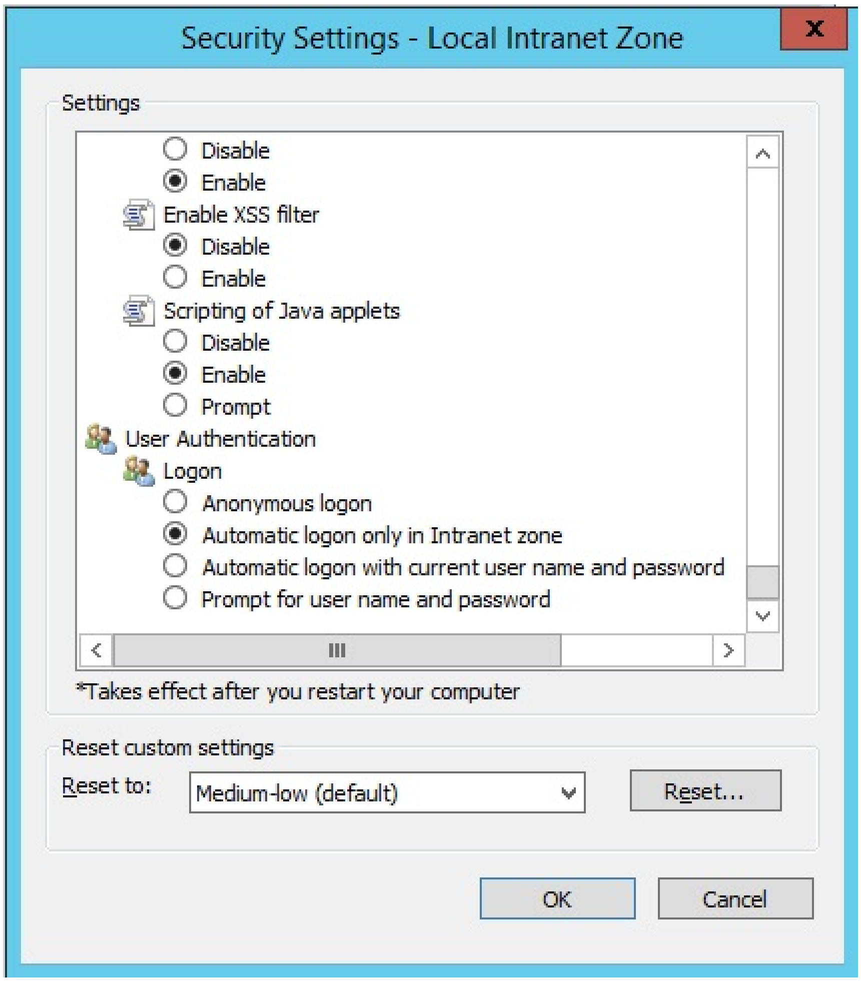
Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

☐ Enable Protected Mode (requires restarting Internet Explorer)

- In the **Security Settings** dialog box, scroll down to the **User Authentication** section of the list.



Security Settings - Local Intranet Zone

Settings

- ○ Disable
- ● Enable
- Enable XSS filter
  - ● Disable
  - ○ Enable
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt
- User Authentication
  - Logon
    - ○ Anonymous logon
    - ● Automatic logon only in Intranet zone
    - ○ Automatic logon with current user name and password
    - ○ Prompt for user name and password

*Takes effect after you restart your computer

Reset custom settings

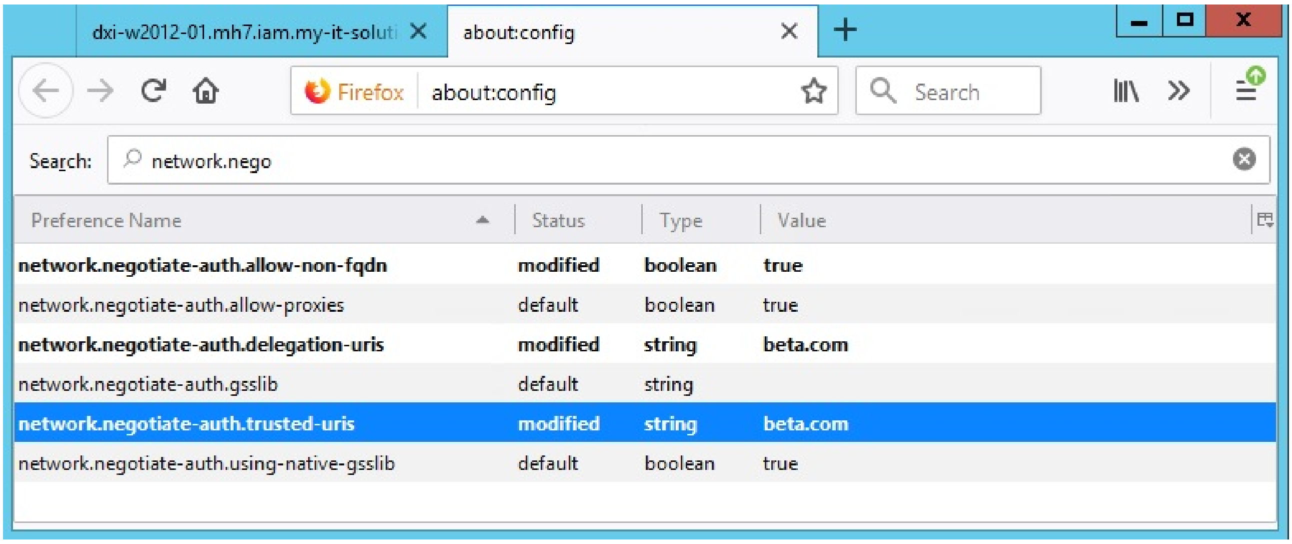
Reset to: Medium-low (default)

- Select **Automatic logon only in Intranet zone**. This setting enables integrated Windows domain authentication in the Internet Explorer.
- Click **OK** to close the Security Settings dialog box.

A.5.2. Firefox

This section describes how to configure Firefox for Windows domain authentication based on Kerberos.

- Open Firefox and enter “about:config” in the browser’s address bar.
- Enter “network.negotiate” in the search bar.search bar.
  - Add the fully qualified domain name to parameter “network.negotiate-auth.trusted-uris”.
  - Add the fully qualified domain name to parameter “network.negotiate-auth.delegation-uris”.
  - Set “network.negotiate-auth.allow-non-fqdn” to “true”.



Search: network.nego

Preference Name	Status	Type	Value
network.negotiate-auth.allow-non-fqdn	**modified**	**boolean**	**true**
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	**modified**	**string**	**beta.com**
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.trusted-uris	**modified**	**string**	**beta.com**
network.negotiate-auth.using-native-gsslib	default	boolean	true

A.5.3. Chrome

Kerberos authentication in Google Chrome should work out-of-the-box if you have configured it for Internet Explorer.

A.6. Testing

Restart Tomcat for the configuration changes to become effective.

Open a browser and enter the URL

```
http://<tomcatHost>:<tomcatPort>/webCenter-<dxiDomain>
```

Replace

- <tomcatHost> with the fully qualified host name of Tomcat.
- <tomcatPort> with the HTTP port of Tomcat.
- <dxiDomain> with your DirX Identity domain.

For example:

```
http://alpha.beta.com:8080/webCenter-My-Company
```

If everything works fine, you will be authenticated to Web Center and see Web Center's home page.

If it works, test again using the simple host name:

```
http://alpha:8080/webCenter-My-Company
```

Note that Kerberos usually doesn’t work if browser and Tomcat run on the same machine.

A.7. Logging and Debugging

A.7.1. Kerberos Ticket Evaluation

Logging for the standard Java classes evaluating and verifying Kerberos tickets and the keytab file is activated via

- Two Java system properties of the Tomcat service:

```
-Dsun.security.krb5.debug=true
-Dsun.security.jgss.debug=true
```

- A debug parameter in file **krb5-jaas.conf**:

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
        debug=true
        ...
```

For details see section “Tomcat Configuration”.

The logs are written to Tomcat’s standard output, which is usually redirected to a Tomcat log file (like *tomcat_install_path*/**logs/tomcat9-stdout.***date***.log**) or the Tomcat console window.

Logging for the ticket evaluation classes in jar file **spnego-tomcat9.jar** is activated by setting the general log level in file **WEB-INF/web.xml:**

```
<context-param>
    <param-name>com.siemens.webMgr.log.level</param-name>
    <param-value>2</param-value>
</context-param>
```

The logs are also written to Tomcat’s standard output.

A.7.2. User Mapping

Logging for the components involved in mapping the Windows credentials to a DirX Identity user is activated via the general log level in file **WEB-INF/web.xml:**

```
<context-param>
```

```
    <param-name>com.siemens.webMgr.log.level</param-name>
    <param-value>2</param-value>
</context-param>
```

The logs are written to Tomcat’s standard output.

A.7.3. Viewing Tickets

Use the Windows command “klist” to display the list of currently cached Kerberos tickets.

Listing the currently cached tickets:

```
klist
```

Deleting the tickets:

```
klist purge
```

A.8. Links

- An overview on Kerberos by MIT: https://web.mit.edu/kerberos
- Configuring Kerberos Authentication in Different Browsers: http://woshub.com/enable-kerberos-authentication-in-browser/#h2_2
- Configuring Kerberos Authentication in Firefox: https://developer.mozilla.org/en-US/docs/Mozilla/Integrated_authentication
- The Windows command **klist**: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/klist
- The Windows server command **ktpass**: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass

Appendix B: Integrating Web Center into NetWeaver

This appendix provides information how to integrate Web Center into NetWeaver 7.0.

B.1. Prerequisites

Single sign-on between NetWeaver and Web Center is based on SAP logon tickets and works only if both applications lie in the same domain.For example, if the NetWeaver URL is **http://abc.internal.my-company.com:**..., the Web Center URL should be like **http://xyz.internal.my-company.com:**.... This requirement can be relaxed to some extent; search for **ume.logon.security.relax_domain.level** on the SAP community network sites for details.

B.2. Web Center Components

This section provides information about components necessary to integrate Web Center into NetWeaver.They are delivered with DirX Identity.

B.2.1. NetWeaver Portal Packages

Web Center delivers the Business Package for DirX Identity to be imported into SAP NetWeaver Portal.

The package contains the portal objects required to access Web Center from within the portal:

- Two system objects to configure the connection to the Tomcat server hosting the Web Center web applications for administration and self service, respectively.
- Two roles to be assigned to NetWeaver users giving them access to the Web Center administration and self service, respectively.
- The worksets and iViews for the Web Center applications.

B.2.2. Web Applications

The web applications **sapWebCenter** and **sapSelfService** are customized versions of the standard Web Center applications.The pages they display include only menu, content and footer, but no header.

B.3. Integrating Web Center into NetWeaver 7.0

The following figure provides an overview about the steps that must be performed to integrate Web Center into NetWeaver 7.0.

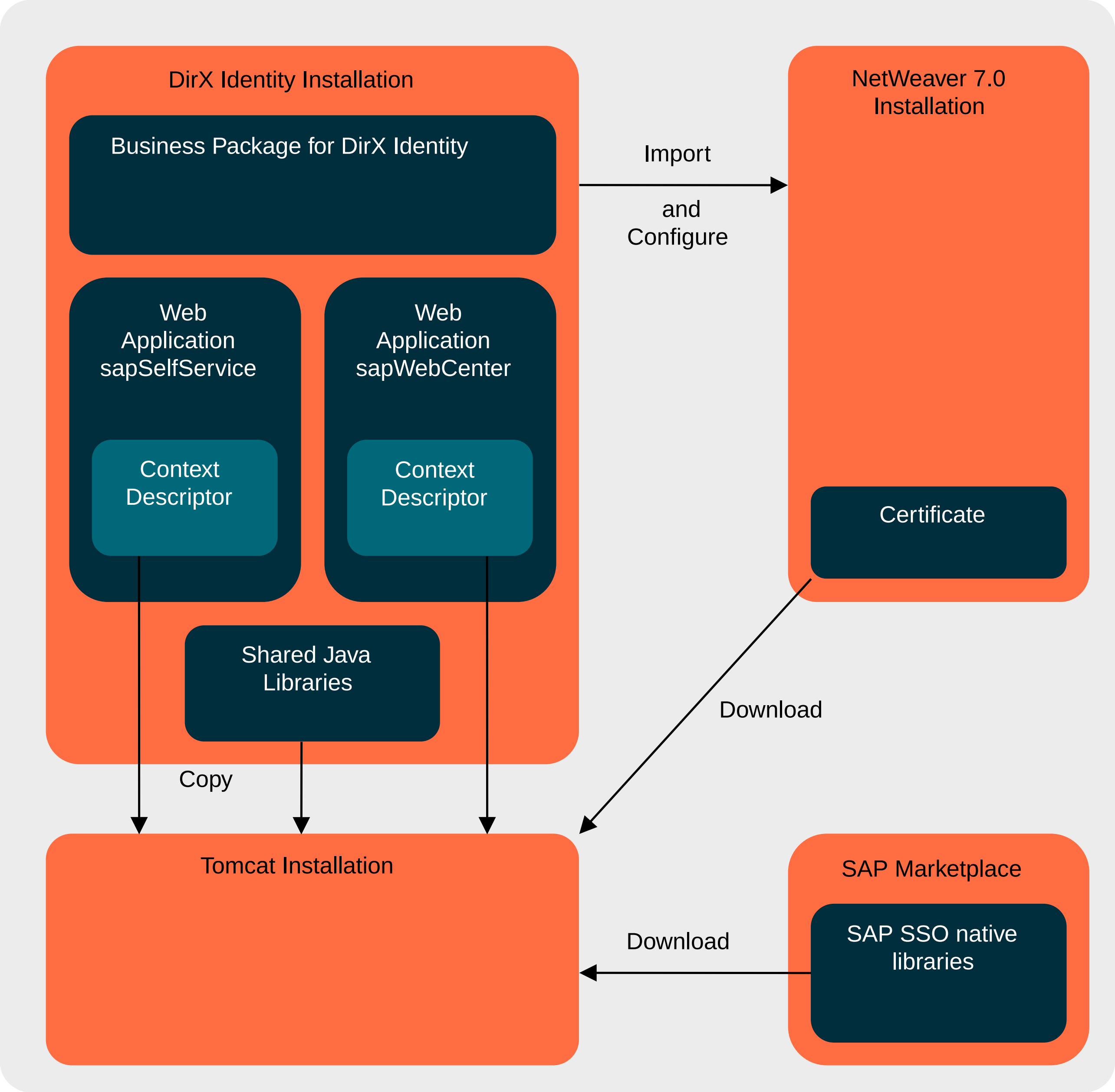


Figure 2. Integrating Web Center into NetWeaver

As shown in the figure above, integrating Web Center into NetWeaver includes the following steps:

- Importing the business package into NetWeaver.
- Configuring the imported objects.
- Downloading the SAP system certificate to Tomcat.
- Downloading the SAP SSO native libraries from the SAP Marketplace to the Tomcat server.
- Configuring Web Center for SAP NetWeaver in the DirX Identity configurator.
- Copying Web Center Java libraries to Tomcat.
- Copying web application context descriptor files to Tomcat.

Note that the three products may reside on different hosts, but that the following instructions (as well as the DirX Identity configurator) assume that DirX Identity and Tomcat run on the same host.

The following description of the integration steps is based on a SAP NetWeaver 7.0 (2004s) installation.

B.3.1. Importing the Web Center Package

Before you import the package, remove any previously imported release as described in the section "Removing the Web Center Package from NetWeaver".

Perform the following steps to import the Web Center package into NetWeaver:

- Log in to the NetWeaver Portal as administrator.
- Perform the following steps to import the Web Center business package **DirX Identity.epa**:
  - Go to System Administration -→ Transport -→ Transport Packages -→ Import.
  - Select **Client** as **Source for Package Files**.
  - Browse for the file *install_path*/**web/webManagerForSAP-***identity_domain*/**NetWeaver/DirX Identity.epa**
  - Click **Upload**.
  - Click **Import**.

B.3.2. Configuring Web Center Objects

Perform the following steps to configure the Web Center objects:

- Log in to NetWeaver Portal as administrator.
- Configure Tomcat systems:
  - Go to System Administration -→ System Configuration -→ System Landscape.
  - Browse to Portal Content -→ Content Provided by Other Vendors -→ End User Content -→ Siemens: DirX Identity -→ Systems.
  - Open the object **DirX Identity Administration**.
    - Select the property category **System Definition**.
    - As name of the server, enter the *fully qualified* host name of the Tomcat server.
    - Enter the port number of the Tomcat server.
    - Select the appropriate protocol.
    - Save the modifications.
    - Select the display **System Aliases**.
    - As the alias name, enter **Siemens_DirXIdentity_Administration**.
    - Click **Add**.

        - Save the modifications.
        - Select the display **Permissions**.
        - Search for **dirx_*** in **Roles**.
        - Select the role **dirx_identity_admin_showcase**.
        - Click **Add**.
        - Set the access rights for the role to **Read**.
        - Check the **End User** check box for the role.
        - Save the modifications.
        - Close the object.
    - Open the object **DirX Identity Self Service**.
        - Select the property category **System Definition**.
        - As the name of the server, enter the *fully-qualified* host name of the Tomcat server.
        - Enter the port number of the Tomcat server.
        - Select the appropriate protocol.
        - Save the modifications.
        - Select the display **System Aliases**.
        - As the alias name, enter **Siemens_DirXIdentity_SelfService**.
        - Click **Add**.
        - Save the modifications.
        - Select the display **Permissions**.
        - Search for **dirx_*** in **Roles**.
        - Select the role **dirx_identity_user_showcase**.
        - Click **Add**.
        - Set the access rights for the role to **Read**.
        - Check the **End User** check box for the role.
        - Save the modifications.
        - Close the object.
- Assign users to roles **dirx_identity_admin_showcase** and **dirx_identity_user_showcase**:
    - Go to User Administration -→ Identity Management.
    - Search for roles with filter **dirx_***.
    - Edit **dirx_identity_admin_showcase** and add users or groups (Web Center administrators)
    - Edit **dirx_identity_user_showcase** and add users or groups (Self Service users)

> Any reimport of the Web Center business package resets the Tomcat

systems configuration and the user-role assignments.

B.3.3. Download SAP System Certificate

The certificate is required to verify SAP logon tickets on the Tomcat server.

First, export the certificate from NetWeaver:

- Log in to the NetWeaver Portal as administrator.
- Export the certificate to file **verify.pse**
  - Go to System Administration -→ System Configuration -→ Keystore Administration.
  - Select the option **SAPLogonTicketKeypair-cert**.
  - Select **Download verify.pse File** and then save the file.

Then, copy the certificate to the Tomcat server:

- Create directory *tomcat_install_path*/**conf/sap**.
- Unzip the downloaded archive to *tomcat_install_path*/**conf/sap**. The archive contains just the file **verify.pse**.
- Make sure the file is accessible to the Tomcat process.

B.3.4. Download Native SAP SSO Libraries

- Login to SAP Marketplace.
- Download the package **SAP SSO EXT lib for SAP logon ticket verification** the operating system of the Tomcat host (do an extended search for SAP software with the filter **SAPSSOEXT** to find the download page.)
- Extract the native libraries `sapssoext` and `sapseculib` from the package to any folder on the Tomcat host that is included in Tomcat's PATH. On Windows, for example, you may put the libraries in C:\WINDOWS\system32.
- Make sure the libraries are accessible to the Tomcat process.

B.4. Copy Web Center Java Libraries to Tomcat

- Copy the following files to folder *tomcat_install_path*/**/lib**:
  - *install_path*/web/**webManagerForSAP-***identity_domain***/shared/dxmMySap.jar**
- Create folder *tomcat_install_path*/**dxilib** if not yet existing.
- Copy the following files to folder *tomcat_install_path*/**dxilb**:
  - *install_path***/web/webManagerForSAP-***identity_domain* /**endorsed/lib/dxmStorageURL.jar**
  - *install_path*/**lib/java/ext/bcprov-jdk14-136.jar**
- Append both jar files to Tomcat's Java classpath.

Make sure the libraries are accessible to the Tomcat process.

B.4.1. Deploy Web Applications into Tomcat

Copy the following files to the folder *tomcat_install_path***/conf/Catalina/localhost**:

- *install_path*/**web/webManagerForSAP-***identity_domain*/ **webCenter/WEB-INF/sapWebCenter.xml**
- *install_path*/**web/webManagerForSAP-***identity_domain*/ **selfService/WEB-INF/sapSelfService.xml**

> If Tomcat does not automatically load the new applications on detection of the new files, load the applications via Tomcat's Web Application Manager or restart the Tomcat server.

B.4.2. Additional Steps

In addition to the integration steps described here, you must

- Configure the Web Center SSO module for authentication with SAP logon tickets.
- Map NetWeaver logins to DirX Identity users, by either
  - Creating a corresponding SAP target system in the DirX Identity store and assigning NetWeaver logins to accounts in that target system, or
  - Assigning NetWeaver user logins directly to DirX Identity users.
- Set up single sign-on between Web Center and the DirX Identity Java-based server; this is required for access to the request workflow server only.

For details, see the documentation on WebCenter Single Sign-On.

B.5. Removing the Web Center Package from NetWeaver

Perform the following steps to remove the Web Center package from NetWeaver:

- Log in to the NetWeaver Portal as administrator.
- Browse to Portal Content → Content Provided by Other Vendors → End User Content.
- Delete the folder **Siemens: DirX Identity**.

B.6. Removing Web Center for SAP Applications from Tomcat

Perform the following steps to remove a Web Center for SAP application from Tomcat:

- Log in to the Tomcat Web Application Manager (//*tomcat_host* :_tomcat_port_**/manager/html**).

- Undeploy the application.

This will delete the application’s context descriptor file and the application’s working directory under *tomcat_install_path***/work**.

If you no longer need to access Web Center from within SAP, delete the following files manually:

- *tomcat_install_path***/lib/dxmMySap.jar**
- *tomcat_install_path***/conf/sap/verify.pse**
- **sapsecu.dll**
- **sapssoext.dll**

If you don’t run any other Web Center applications in Tomcat, delete also the following files:

- **bcprov-jdk14-136.jar**
- **dxmStorageURL.jar**

from the folder *tomcat_install_path***/dxilib.**

B.7. Upgrading from Earlier Releases

When upgrading from a release prior to 8.3, remove the files

- **jaxb-api.jar**
- **jaxws-api.jar**

from the folder *tomcat_install_path***/endorsed.**

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

EVIDEN

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.