

Digitize business processes successfully

Accelerate digital transformation with the X4 BPMS low code platform

X4 Administration Guide

Digitize business processes successfully

Accelerate digital transformation with the X4 BPMS low code platform

The information in this document is subject to change without notice. SoftProject GmbH assumes no responsibility for any errors that may appear in this document.

This document may not be copied, photocopied, reproduced, translated or converted to any electronic or machine-readable form in whole or in part without prior written approval of SoftProject GmbH.

Mentioned products are trademarks or registered trademarks of their respective owners.

Contact

SoftProject GmbH

Am Erlengraben 3

D-76275 Ettlingen – Germany

Website: www.softproject.de

Sales

Phone: +49 7243 56175-0

vertrieb@softproject.de

SoftProject Support

Phone: +49 7243 56175-333

support@softproject.de

© SoftProject GmbH. All rights reserved.

Table of Contents

1	System requirements	10
2	Installation	12
2.1	Installing the X4 Server.....	12
2.1.1	Installation on Windows systems.....	12
2.1.1.1	Install X4 Server	12
2.1.1.2	Update existing installation since version 5.5.4	19
2.1.1.3	Parameters of the unattended installation.....	20
2.1.2	Installation on Ubuntu/Debian Linux systems	22
2.1.2.1	Install X4 Server	22
2.1.2.2	Control options for the X4 Server service	23
2.1.2.3	Control options for Keycloak	24
2.1.2.4	Uninstall X4-Server service	24
2.1.3	Installation on Red Hat Enterprise Linux systems	24
2.1.3.1	Installing the X4 Server.....	24
2.1.3.2	Control options for the X4 Server service	25
2.1.3.3	Control options for Keycloak	26
2.1.3.4	Uninstalling the service X4-Server.....	26
2.1.4	Installation on SuSe Linux systems.....	26
2.1.4.1	Install X4 Server	26
2.1.4.2	Control options for the X4 Server service	28
2.1.4.3	Uninstalling the service X4-Server.....	28
2.1.5	Installing the X4 Server in Docker	28
2.1.6	Installing the X4 Server on other operating systems	30
2.2	Initially installing a licence	30
2.3	Renewing license	30
2.4	Displaying license information.....	31
2.5	Install and uninstall X4 Designer	31
2.5.1	Install X4 Designer.....	31
2.5.2	Uninstall X4 Designer	33

2.5.3	Parameters of the unattended installation.....	34
2.6	Installation and migration of the system database and X4DB	34
2.7	Installation of the authentication provider	34
3	Configuration	36
3.1	Configuring the X4 Server.....	36
3.1.1	Setting up the Database	36
3.1.1.1	Setting up the Oracle Database	36
3.1.1.2	Configuration for MSSQL and PostgreSQL.....	39
3.1.2	Configuring via the X4config.xml	42
3.1.2.1	iXServ configuration.....	42
3.1.2.2	SNMP configuration	42
3.1.2.3	Configuring the Placeholder Storage for X4 Server	43
3.1.2.4	LDAPS configuration	44
3.1.3	Configuring the Logging	45
3.1.3.1	Save Point Configuration for the X4 Server	45
3.1.3.2	SNMP trap appender.....	45
3.1.3.3	Ad hoc logging at runtime	46
3.1.4	Configuring the production mode	47
3.1.5	Enabling SSL and HTTPS for X4 Server	47
3.1.5.1	Customize key-stores.....	48
3.1.5.2	Customize key-managers	48
3.1.5.3	Customize server-ssl-contexts	49
3.1.5.4	Customize https-listener.....	49
3.1.5.5	Customize socket-binding.....	49
3.2	Configuring the X4 Designer	50
3.2.1	Editing the connection configuration	50
3.2.2	Configuring the Process Editor.....	51
3.2.3	Configuring the Run/Debug Mode	52
3.2.4	Configuring the Mapping Editor	54
3.2.5	Managing templates for repository elements.....	55
3.2.6	Assigning file types to external or internal editors	55

3.2.7	Configuring the Web Browser	57
3.2.8	Configuring the JSON Editor	57
3.2.9	Changing the Help Language	58
4	Administering the X4 Server	60
4.1	Updating the X4 Repository in production mode	60
4.2	Controlled shutdown of the X4 Server (via JMX)	60
4.3	Providing Process Libraries	61
5	High Availability	63
5.1	Load Balancing	63
5.1.1	Scenario – Few Mainly Reading Database Accesses	63
5.1.1.1	Simple – Direct database access	64
5.1.1.2	Complex – Shared access via an X4 instance	65
5.1.2	Scenario – Shares Access via Message Queue	66
5.2	Fail Over	66
5.2.1	Scenario – A Single Exclusive Database	67
5.2.2	Scenario – System Database per X4 Server	68
5.3	Load Balancing via Scheduler	68
5.3.1	Scenario – Dedicated X4 Server for Scheduling	69
5.3.2	Scenario – One Server Responsible for Scheduling	70
5.3.3	Scenario – External Scheduler	71
6	Keycloak	72
6.1	About the used database	73
6.2	Set up	74
6.2.1	Loading Docker image and launching container	74
6.2.2	Connecting your own Keycloak installation	74
6.3	Configure	75
6.3.1	Applying Authorization Code Flow	75
6.3.2	Restricting access to X4 repository	76
6.3.2.1	Sample	76
6.3.3	Default configuration	76
6.3.3.1	Realm Settings	76

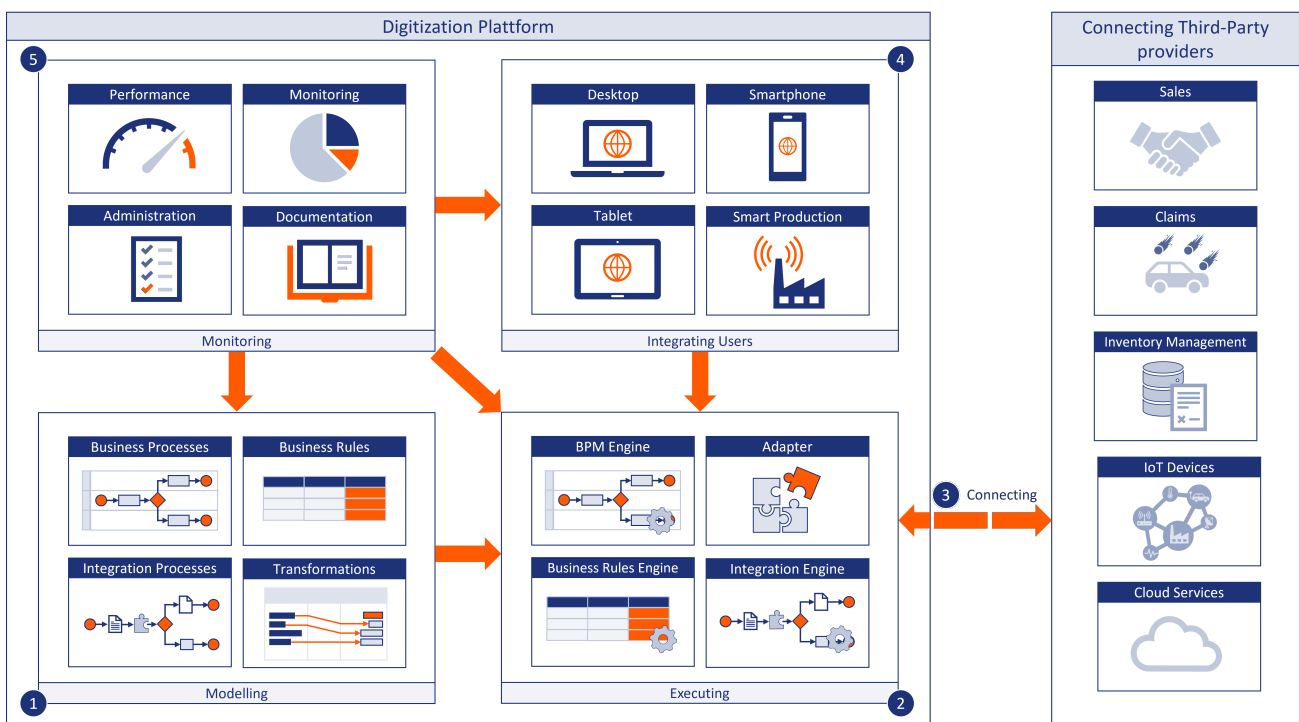
6.3.3.2	Clients.....	77
6.3.4	Connect LDAP	79
6.3.5	Connect SAML v2.0	81
6.3.6	Connect Kerberos	83
6.3.7	Connect social identity providers	85
6.3.8	Connect OpenID Connect.....	86
6.3.9	Login page	88
6.3.9.1	Remember Me button	88
6.3.9.2	Create Forgot Password button.....	91
6.3.9.3	Activate user registration.....	94
6.3.10	Passwords.....	97
6.3.10.1	Set password policies	97
6.3.11	Themes	100
6.4	Users	101
6.4.1	Create user	101
6.4.2	Assign a role to a user.....	102
6.4.3	Assign user to a group	108
6.4.4	Remove user from a group.....	114
6.5	Roles	120
6.5.1	Create role	120
6.6	Groups	122
6.6.1	Create group	122

About the X4 BPMS

Digitalization requires a holistic approach, which presupposes that also the used solution has to reflect that. X4 BPMS supports you as a central platform in solving these challenges. The focus is on modeling, implementing and monitoring your business processes. Therefore, the X4 BPMS contains all necessary tools and is compatible with a variety of interfaces and formats. That helps to avoid isolated information silos and media breaks that inhibit productivity, and accelerate digitization at the same time.

Implementing business processes without programming effort enables a large number of users to enter into the management of business processes. That's important, since employees of the specialist department usually know best what is important in the respective business processes. Therefore, you should rely on the X4 BPMS as a platform whose tools reduce complexity to such an extent that business processes can be analyzed, optimized, modeled, as well as controlled and documented even without programming knowledge. All tools support integrated, graphical process modeling and implementation and generate processes that are executed by the X4 BPMS with high performance.

- **X4 Designer:** Modelling processes and rules graphically
- **X4 Server:** Simulating and executing processes and rules
- **X4 Adapter:** Integrating third-party systems into processes
- **X4 Activities:** Providing web apps for employees and customers



Who is the target group of this document?

This document targets administrators who want to install, configure and administer the X4 Server. In addition to detailed technical knowledge of the existing IT infrastructure, basic knowledge of Java EE, XML technologies and the application server is required.

1 System requirements

X4 Server

Operating system	• Microsoft Windows Server 2012, 2012 R2, 2016, 2019 • SUSE Linux Enterprise Server 15, Red Hat Enterprise Linux 8, Ubuntu Linux 18.04 LTS, Debian GNU/Linux 10.1 i • If you want to use the X4 server in another environment, we will be glad to consult you. • Only 64-bit operating systems are supported (x86_64). • For security reasons, a hardened configuration of the X4 Server is required to use the X4 Proxy Server. Do not hesitate to contact us for advice.
Platform	• Runtime environment: X4 Server is based on the Java 11 platform. With Version 11 Azul Zulu 11.54.23 (Java 11.0.14) is already included as runtime environment. • Application server: The X4 Server uses an integrated WildFly application server in version 25.0.1. • Authentication provider: The X4 server uses the authentication provider Keycloak in version 16.1.0. • System database: X4 Server requires a system database to manage runtime and authentication information. The following databases are supported: • Oracle (11g, 12c, 18c, 19c) • Microsoft SQL Server (2012 Service Pack 4, 2014 Service Pack 3, 2016 Service Pack 2, 2017) • PostgreSQL (11.5, 12.0) i • If you have special requirements regarding the Java runtime environment or if you want to use an alternative application server for customer-specific adaptations, do not hesitate to contact us for advice. • If you want to use the X4 Server with a different version of the above database management systems, do not hesitate to contact us for advice.
Hardware requirements	• At least 2 processor cores • At least 5 GB of free hard disk space • At least 8 GB RAM i Starting with a number of 500 processes to be executed, we recommend a system with at least 8 processor cores and 16 GB main memory, which must be available exclusively for X4 Server.

X4 Web Apps

Operating system	X4 Web Apps are cross-platform usable via browser.
Platform	Current browser (also mobile) with enabled JavaScript: • Google Chrome (latest version) • Mozilla Firefox (latest version and extended support release (ESR)) • Microsoft Edge (last 2 major versions) • Apple Safari (last 2 major versions) i Microsoft Internet Explorer and Microsoft Edge ("Project Spartan") are discontinued by Microsoft. Please switch to Microsoft Edge (Chromium-Based) or any other compatible browser.

X4 Designer

Operating system	• Microsoft Windows 8.1, 10 (since version 1803) • Microsoft Windows Server 2012, 2012 R2, 2016, 2019 i • Only 64-bit operating systems are supported (x86_64). • Only Windows operating systems allowing the execution of desktop applications are supported. Core versions of Microsoft Windows Server are not supported. • Desktop virtualization solutions (e.g. Citrix XenDesktop or Citrix XenApp) are not officially supported. However, some customers are using X4 Designer in environments like these. Do not hesitate to contact us for advice.
Platform	Runtime environment The X4 Designer is based on the Java 11 platform. Azul Zulu 11.54.23 (Java 11.0.14) is already integrated as runtime environment.
Hardware requirements	• At least 2 processor cores • At least 2 GB free hard disk space • At least 8 GB RAM

2 Installation

2.1 Installing the X4 Server

Here you will find information on how to install the X4 server.

 Administrator permissions are required for the installation.

2.1.1 Installation on Windows systems

Here you will learn how to install the X4 Server - if required also as NT service - on Windows.

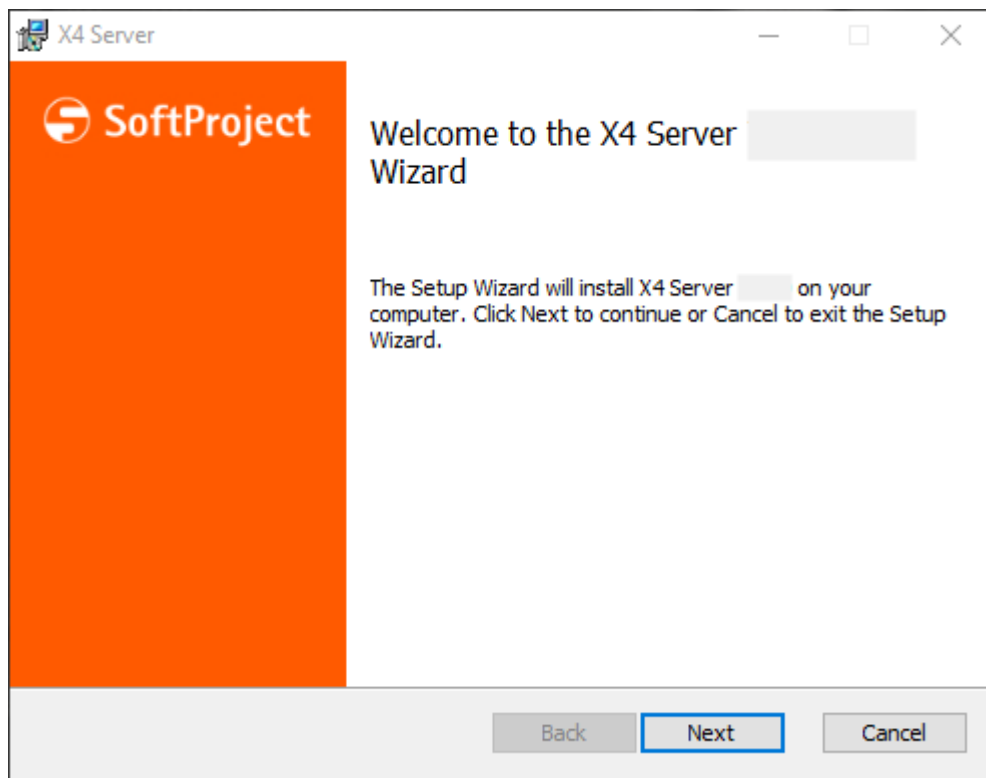
2.1.1.1 Install X4 Server

For **production purposes**, the X4 Server is provided as a separate MS Windows installation package in the form of an MSI file.

- 
- You can install only one X4 Server on a Windows system. The MS Windows installation package overwrites existing installations. If you overwrite an existing installation, this can lead to problems and data loss.
 - To use multiple X4 Servers for testing purposes, we provide the **MS Windows All-in-one** installation package in the [download section](#) of our website.

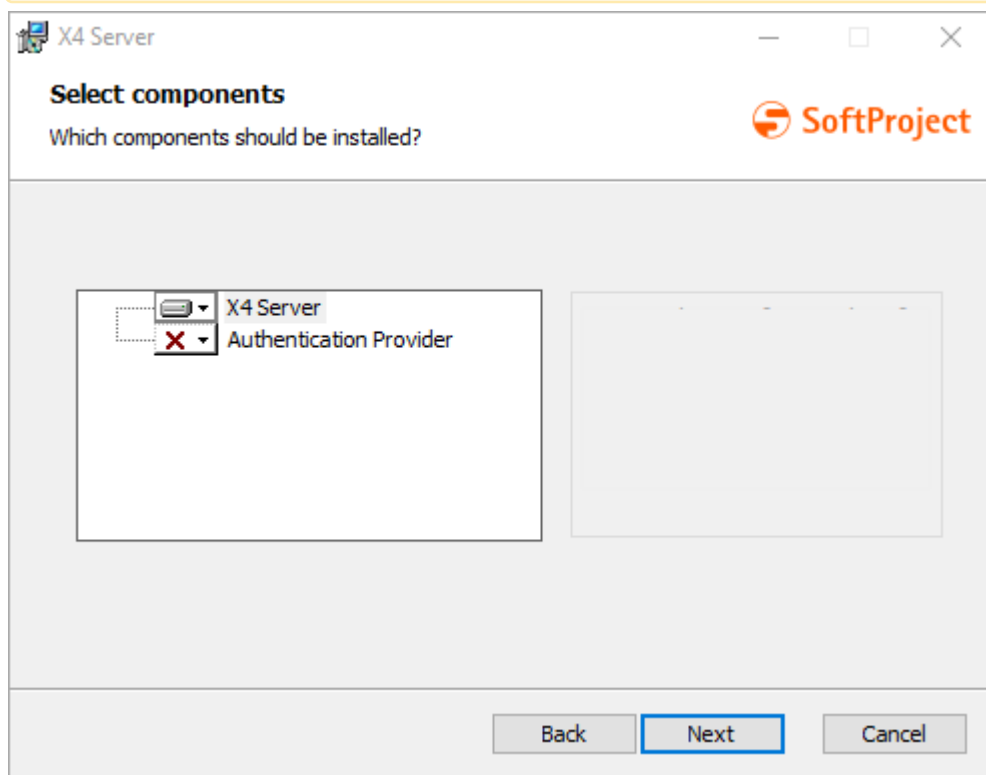
1. Run the installation package `X4ServerSetup_7.v.v_64bit.msi` provided by SoftProject with administrator rights or appropriate write rights.

 Windows Defender SmartScreen issues a warning at the start of the installation. Click **More information** and start the installation routine as usual with **Run anyway**.

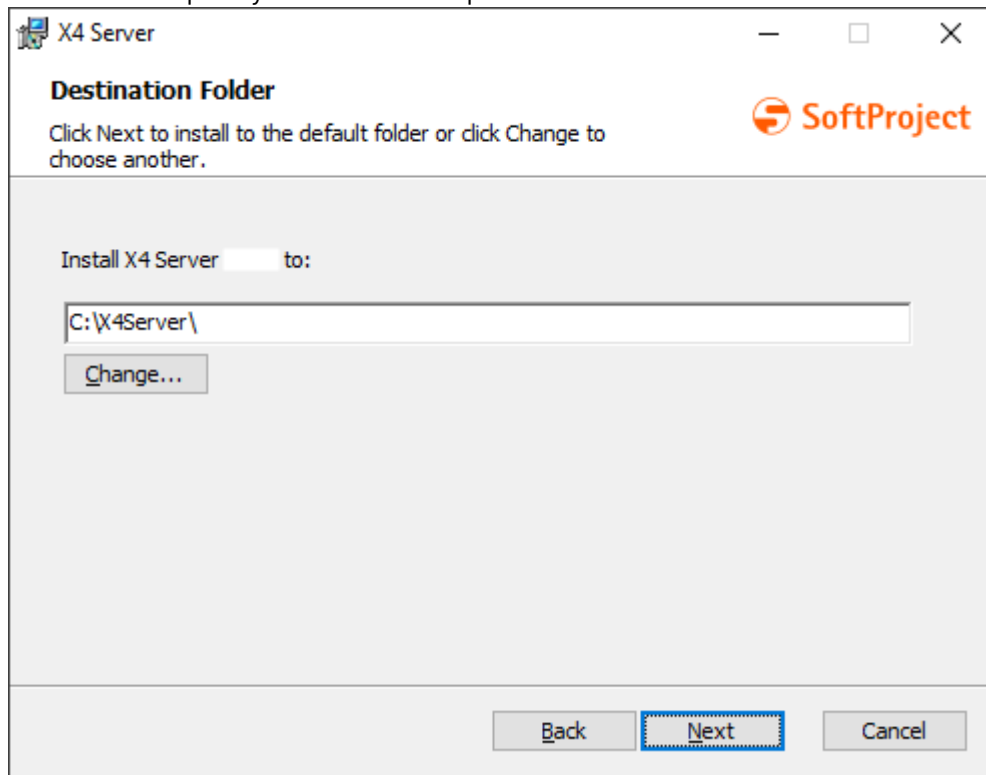


2. Click **Next** to select the components to be installed.

⚠ If you do not have an Authentication Provider in use, you have to install the provided **Authentication Provider** component.



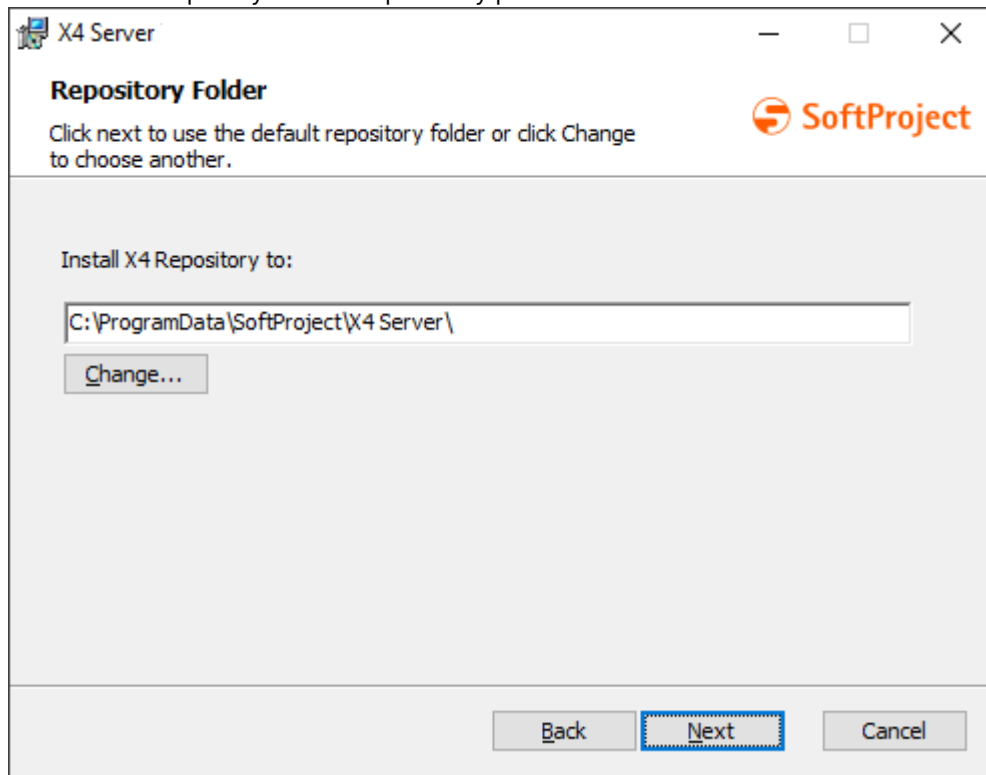
- Click **Next** to specify the installation path.



 By default, the X4 Server is installed in `C:\X4Server_7.v.v.\`, but the installation path can be changed via **Change**.

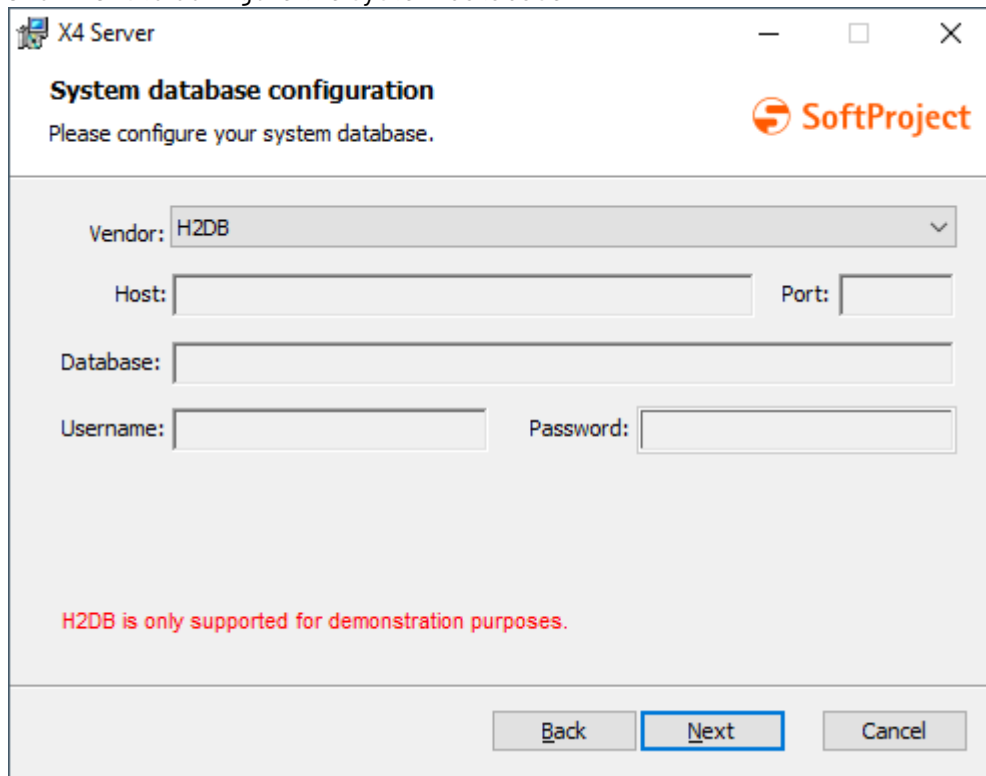
 Do not use spaces in the installation path. This may cause errors when installing the X4 Server as a service.

4. Click **Next** to specify the X4 repository path.



 By default, the X4 repository is installed in C:\ProgramData\SoftProject\X4Server\, but you can change the path via **Change**.

5. Click **Next** to configure the system database.



6. Configure system database:

- **Vendor:** Specify database to use
 - H2DB

 Note that H2DB is not suitable for productive use!

- Microsoft SQL Server
- Oracle Database 11g

 Note that the database driver for Oracle Database 11g is not included in the installation package. The corresponding driver must be installed separately, see also [Setting up the Oracle Database](#).

- Oracle Database 12c/18c/19c

 Note that the database driver for Oracle Database 12c/18c/19c is not included in the installation package. The corresponding driver must be installed separately, see also [Setting up the Oracle Database](#).

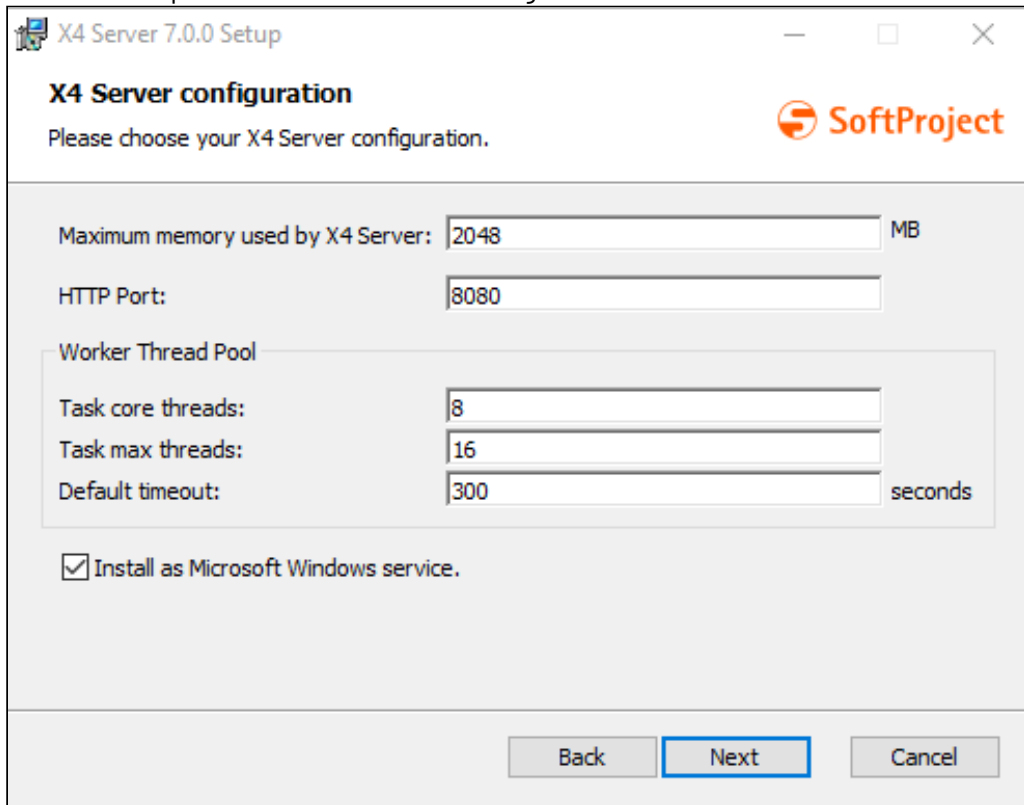
- PostgreSQL

- **Host:** specify database host
- **Port:** Specify database port
- **Database:** Specify database
- **Authentication:** specify authentication with SQL Server Authentication or Windows Authentication

 This parameter is available only for Microsoft SQL Server. If Windows Authentication is specified as authentication, the **Username** and **Password** credentials do not need to be specified because they correspond to the Windows credentials.

- **Username:** specify user name for database connection
- **Password:** specify password for database connection

7. Click **Next** to perform the X4 Server configuration.



The screenshot shows the 'X4 Server configuration' window of the 'X4 Server 7.0.0 Setup' application. The window title bar includes the application name and standard Windows window controls. The main heading is 'X4 Server configuration' with the instruction 'Please choose your X4 Server configuration.' and the SoftProject logo. The configuration fields are as follows:

- Maximum memory used by X4 Server:** A text box containing '2048' followed by 'MB'.
- HTTP Port:** A text box containing '8080'.
- Worker Thread Pool:** A group box containing three text boxes:
 - Task core threads:** Contains '8'.
 - Task max threads:** Contains '16'.
 - Default timeout:** Contains '300' followed by 'seconds'.
- Install as Microsoft Windows service:** A checkbox that is checked.

At the bottom, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

8. Configure X4 Server:

- **Maximum memory used by X4 Server:** Specify maximum memory used
- **HTTP Port:** specify HTTP port for X4 Web Apps
- Configure **Worker Thread Pool:**
 - **Task core threads:** Initial number of threads in the thread pool

 This number is the minimum number of threads that the server uses.
The number of core threads should be able to handle the normal request load.

- **Aufgabe max Threads:** Maximum number of threads in the thread pool

- ⓘ If no value is specified, the default value is used. The default value is calculated by the formula $\text{CPU-count} * 16$ if the JMX property `MaxFileDescriptorCount` allows this number, otherwise max is considered in the calculation to adjust the number accordingly.
- This property depends on the server hardware because the hardware can provide a maximum number of threads. It is used to control the maximum allocation of system resources under heavy load.
- The number of threads is between the initial number and the maximum number of threads in the thread pool.

- **Default timeout:** Default transaction time in seconds

- ⓘ For long-running transactions, WildFly may time out during the EJB processing method. In this case, you can change the default transaction runtime of 300 seconds using the `standalone.xml` file.

- **Install as Microsoft Windows service:** Activate if the X4 Server is to be installed as a service
- **Create a shortcut for X4 Server on the desktop:** Enable if you want to create a desktop shortcut for the X4 Server.

- ⓘ This option is available when `Install as Microsoft service` is disabled.

9. Click **Next** to perform the network configuration for the X4 Server.

- Address binding: Specify address binding
 - Any address: Any address

 Note that specifying Any Address makes the X4 Server publicly accessible.

- IP Address/Domain: Specific IP address and domain
 - **IP Address / Domain:** Specify IP address and domain
10. Click **Next** to confirm the information.
11. Click **Install** to perform the installation.
The X4 Server will now be installed.
12. If required, enable the **Launch X4 Server when setup exists** option to start the server after installation.
13. Click **Finish** to terminate the installation.
The installation is now complete.
14. Check whether error messages occurred in the server log.
A correctly installed and started X4 server does not issue any error messages (ERROR or FATAL) in the server log.

2.1.1.2 Update existing installation since version 5.5.4

 If you have an older version installed, you must first update to version 5.5.4.

You can find the current update tool in the download area on our website. For more information, please read the README.txt in the update tool.

2.1.1.3 Parameters of the unattended installation

To perform an unattended installation using the command line, the following parameters have to be set:

 If a parameter is not specified, the default value is used during installation.

Parameter	Description
INSTALLFOLDER	Installation path Possible values • Path specification (default: C:\X4Server_<version>\)
PRODUCTNAMEDIRECTORY	X4 Repository folder • Path specification (default: C:\ProgramData\SoftProject\X4Server\)  Do not use spaces in the installation path. This may cause errors when installing the X4 server as a service.
INSTALLSERVICE	Install X4 Server as Windows Service Possible values • True (default): X4 server is installed as a Windows service • False: X4 server is not installed as a Windows service
INSTALLDESKTOPSHORTCUT	Create X4 server desktop shortcut (only possible if X4 server is not installed as Windows service) Possible values • True (default): Desktop shortcut is created • False: Desktop shortcut is not created
DATABASETYPE	Database type Possible values • h2 (default): H2 • postgresql: PostgreSQL • sqlserver: Microsoft SQL Server • oracle11: Oracle Database 11g • oracle12: Oracle Database 12c/18c/19c

Parameter	Description
HOSTDB	Database host IP address (example: 127.0.0.1)
PORTDB	Database port Integers (example: 3307)
DATABASENAME	Database name
USERNAMEDB	Username for authentication to the database
PASSWORDDB	Password for authentication to the database
MEMORY	Maximum used memory in MB Integers (default: 2048)
HTTPPORT	HTTP port Integers (default: 8080)
AUTHENTICATION_SQLSERVER	Database authentication type Possible values - sqlserver (default) - windows
TASKCORETHREADS	Minimum number of threads Possible values Integers (default: 8)
TASKMAXTHREADS	Maximum number of threads Possible values Integers (default: 16)
DEFAULTTIMEOUT	Timeout in seconds Possible values Integers (default: 300)
ADDRESSTYPE	Address type Possible values - anyAddress (default): any address  Note that with this configuration the X4 server is accessible to everyone. - ipDomain: IP address/domain

Parameter	Description
EXTERNALLIP	IP address/domain (only relevant if ADDRESSTYPE=ipDomain) Possible values IP address (example: 127.0.0.1)

2.1.2 Installation on Ubuntu/Debian Linux systems

The following describes how the X4 Server and Keycloak based on a Debian package (.deb) can be automatically installed on an Ubuntu or Debian Linux system, registered as a service, started and administered.

2.1.2.1 Install X4 Server

Note!

- The installation package is started with sudo permissions.
- During the installation of the X4 Server, a new user X4 and a new group X4 are created.
- After installation, the X4 Server file system belongs to the user X4 and the group X4.
- The installed service X4 Server is started with sudo permissions, but the user X4 is the owner of this service execution.
- Make sure that you have the appropriate rights for the specified installation path.

1. Load the Debian package X4-Server_Ubuntu-7.v.v-r.x86_64 provided by SoftProject onto the Ubuntu or Debian system.
2. Run the installation with the command `sudo dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb`.

 If you do not want the authentication provider Keycloak installed, use the command `sudo X4_INSTALL_AUTH_PROVIDER=no dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb`.

Example: `sudo dpkg -i X4-Server_Ubuntu-7.0.0-1.x86_64.deb` for release 1 of X4 Server version 7.0.0.

 The X4 Server is installed under /opt/X4 by default. The `INSTALL_PATH` variable can be used to change the installation path, e.g. `sudo INSTALL_PATH=/myNewPath/Tools dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb`

The X4 Server is now installed in the specified folder, registered as the X4-Server service and started directly. This process may take a few seconds.



- If an installation of the X4 Server already exists, the central components of the X4 Server are automatically updated when the installation command `sudo dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb` is executed again. Backup copies of the configuration files are created in the subfolder `/opt/X4_backups`.
- To migrate files that are not part of the automatic update process, the installation path of the X4 BPMS must be specified in the installation and migration tool. For example, specifying `/opt/X4/jdk/bin/java -jar en.softproject.x4.database-6.3.0.jar --installX4path /opt/X4/Server` will migrate all `.war` files that have not already been migrated automatically to the new installation.

3. Check whether error messages occurred in the server log `/opt/X4/wildfly/standalone/log/server.log`.

A correctly installed and started X4 Server does not give any error messages (ERROR or FATAL) in the server log. This should be the case at the second start of the X4 Server at the latest.

4. Check whether error messages occurred in Keycloak log `/opt/X4/keycloak/standalone/log/server.log`.

A correctly installed and started Keycloak does not output any error messages (ERROR or FATAL) in Keycloak log.

5. Restart the X4 Server with the command `sudo service X4-Server restart`.

The X4 Server has been successfully installed and is running as service X4-Server.

6. Restart the Keycloak with the command `sudo service X4-Authentication-Provider restart`.

The Keycloak has been installed successfully.

After successfully installing or updating the X4 Server via a Debian package, the installation folder contains the following items:

Folder	Explanation
jdk	Contains the current Java runtime version as runtime environment for the WildFly application server
SQL	Contains the supplied in-memory database for test purposes in subfolder H2DB
wildfly	Contains the pre-configured WildFly application server
keycloak	Contains Keycloak
X4DB	Contains the central X4 repository
x4.license	Licence file for the X4 Server, see Installing licences via the Designer
X4config.xml	Central configuration file of the X4 Server, see Configuration via X4config.xml

2.1.2.2 Control options for the X4 Server service

The following options are available via the command line to control the X4 Server or its service X4-Server:

Start X4-Server service:	Execute the command <code>service X4-Server start</code> .
---------------------------------	--

Stop X4-Server service:	Execute the command <code>service X4-Server stop</code> .
Restart the X4-Server service:	Execute the command <code>service X4-Server restart</code> .

2.1.2.3 Control options for Keycloak

The following options are available via the command line to control Keycloak X4-Authentication-Provider:

Start X4-Authentication-Provider service:	Execute the command <code>service X4-Authentication-Provider</code> .
Stop X4-Authentication-Provider service:	Execute the command <code>service X4-Authentication-Provider</code> .
Restart the X4-Authentication-Provider service:	Execute the command <code>service X4-Authentication-Provider</code> .

2.1.2.4 Uninstall X4-Server service

To uninstall an X4 Server installed via Debian package and its corresponding service X4-Server, enter the command `sudo dpkg -r X4-Server`.

For a clean removal of all installation artefacts including configuration files etc. from the X4-Server service run the command `sudo dpkg -P X4-Server`.

i When uninstalling, it is not necessary to set the `INSTALL_PATH` variable.

2.1.3 Installation on Red Hat Enterprise Linux systems

How to automatically install, register as a service, start, and manage the complete X4 Server on a Red Hat Enterprise Linux system based on an RPM (.rpm) package is described below.

2.1.3.1 Installing the X4 Server

i Before installation, make sure that the IP address of the server and the host name are entered under `/etc/hosts`.

Example: 192.168.147.153 vmettopensuse01

i Please note!

- The installation package is started with `sudo` permissions.
- During the installation of the X4 Server, a new user X4 and a new group X4 are created.
- After installation, the X4 Server file system belongs to the user X4 and the group X4.
- The installed service X4 Server is started with `sudo` permissions, but the user X4 is the owner of this service execution.
- Make sure that you have the appropriate rights for the specified installation path.

1. Load the RPM package `X4-Server_RHEL-7.v.v-r.x86_64.rpm` provided by SoftProject onto the Red Hat system.
2. Execute the installation with the command `sudo rpm -i X4-Server_RHEL-7.v.v-r.x86_64.rpm`.

Example: `sudo rpm -i X4-Server_RHEL-7.0.0-1.x86_64.rpm` for release 1 of X4 Server version 7.0.0.

i The X4 server is installed under `/opt/X4` by default. The `--prefix` parameter can be used to change the installation path, e.g. `sudo rpm -i X4-Server_RHEL-7.v.v-r.x86_64.rpm --prefix=/new_path`

The X4 Server is now installed in the specified folder, registered as the X4-Server service and started directly. This process may take a few seconds.

3. If necessary, copy your license file `x4.license` into the installation folder of the X4 server.
Example: `sudo cp x4.license /opt/X4`
4. If necessary, check whether error messages occurred in the server log `/opt/X4/wildfly/standalone/log/server.log`.
A correctly installed and started X4 server does not output any error messages (ERROR or FATAL) in the server log. This should be the case at the second start of the X4 Server at the latest.
5. If necessary, check whether error messages occurred in Keycloak log `/opt/X4/keycloak/standalone/log/server.log`.
A correctly installed and started Keycloak instance does not output any error messages (ERROR or FATAL) in the log.

After successfully installing or updating the X4 Server via RPM package, the installation folder contains the following elements:

Folder	Explanation
<code>jdk</code>	Contains the current Java runtime version as runtime environment for the WildFly application server
<code>SQL</code>	Contains the supplied in-memory database for test purposes in subfolder <code>H2DB</code>
<code>wildfly</code>	Contains the pre-configured WildFly application server
<code>keycloak</code>	Contains Keycloak
<code>X4DB</code>	Contains the central X4 repository
<code>x4.license</code>	Licence file for the X4 Server, see Installing licences via the Designer
<code>X4config.xml</code>	Central configuration file of the X4 Server, see Configuration via X4config.xml

2.1.3.2 Control options for the X4 Server service

The following options are available from the command line to control the X4 server or its service X4-Server:

Starting service X4-Server:	Execute command <code>systemctl start X4-Server</code> .
Stopping service X4-Server:	Execute command <code>systemctl stop X4-Server</code> .

Restarting service X4-Server:	Execute command <code>systemctl restart X4-Server.</code>
See status of service X4-Server:	Execute command <code>systemctl status X4-Server.</code>
Reload service X4-Server:	Execute command <code>systemctl reload X4-Server.</code>

2.1.3.3 Control options for Keycloak

The following options are available from the command line to control Keycloak X4-Authentication-Provider:

Starting service X4-Authentication-Provider:	Execute command <code>systemctl start X4-Authentication-Provider.</code>
Stopping service X4-Authentication-Provider:	Execute command <code>systemctl stop X4-Authentication-Provider.</code>
Restarting service X4-Authentication-Provider:	Execute command <code>systemctl restart X4-Authentication-Provider.</code>
See status of service X4-Authentication-Provider:	Execute command <code>systemctl status X4-Authentication-Provider.</code>
Reload service X4-Authentication-Provider:	Execute command <code>systemctl reload X4-Authentication-Provider.</code>

2.1.3.4 Uninstalling the service X4-Server

To uninstall an X4 server installed via RPM package and its corresponding service `X4_server`, enter the command `sudo rpm -e X4-Server_RHEL-7.v.v-r.x86_64.`

During uninstallation, backup copies of the configuration files, system database and X4DB are automatically created under `opt/x4_backups`.

2.1.4 Installation on SuSe Linux systems

How the complete X4 server based on an RPM package (`.rpm`) can be automatically installed on an Open-Suse Linux system, registered as a service, started and managed is described below.

2.1.4.1 Install X4 Server

Prerequisite

- The **insserv-compat** package is installed.
The package can be installed in the command line with the following command: `zypper install insserv-compat`

i Before installation, make sure that the IP address of the server and the host name are entered under `/etc/hosts`.
Example: 192.168.147.153 vmettopensuse01

❗ Please note!

- The installation package is started with sudo permissions.
- During the installation of the X4 Server, a new user X4 and a new group X4 are created.
- After installation, the X4 Server file system belongs to the user X4 and the group X4.
- The installed service X4 Server is started with sudo permissions, but the user X4 is the owner of this service execution.
- Make sure that you have the appropriate rights for the specified installation path.

1. Load the RPM package `X4-Server_SLES-7.v.v-r.x86_64.rpm` provided by SoftProject onto the Suse Linux system.
2. Execute the installation with the command `sudo rpm -i X4-Server_SLES-7.v.v-r.x86_64.rpm`.

Example: `sudo rpm -i X4-Server_SLES-7.0.0-1.x86_64.rpm` for release 1 of X4 Server version 7.0.0.

- ❗ The X4 server is installed under `/opt/X4` by default. The `--prefix` parameter can be used to change the installation path, e.g. `sudo rpm -i X4-Server_SLES-7.v.v-r.x86_64.rpm --prefix=/new_path`

The X4 Server is now installed in the specified folder, registered as the X4-Server service and started directly. This process may take a few seconds.

- ❗ To migrate files that are not part of the automatic update process, the installation path of the X4 BPMS must be specified in the installation and migration tool. For example, specifying `/opt/X4/jdk/bin/java -jar de.softproject.x4.database-7.0.0.jar --installX4path /opt/X4/Server` will migrate all `.war` files that have not already been migrated automatically to the new installation.

3. If necessary, copy your license file `x4.license` into the installation folder of the X4 server.
Example: `sudo cp x4.license /opt/X4`

4. Check whether error messages occurred in the server log `/opt/X4/wildfly/standalone/log/server.log`.

A correctly installed and started X4 Server does not give any error messages (ERROR or FATAL) in the server log. This should be the case at the second start of the X4 Server at the latest.

After successfully installing or updating the X4 Server via RPM package, the installation folder contains the following elements:

Folder	Explanation
jdk	Contains the current Java runtime version as runtime environment for the WildFly application server
SQL	Contains the supplied in-memory database for test purposes in subfolder H2DB

Folder	Explanation
wildfly	Contains the pre-configured WildFly application server
X4DB	Contains the central X4 repository
x4.license	Licence file for the X4 Server, see Installing licences via the Designer
X4config.xml	Central configuration file of the X4 Server, see Configuration via X4config.xml

2.1.4.2 Control options for the X4 Server service

The following options are available from the command line to control the X4 server or its service X4-Server:

Starting service X4-Server:	Execute <code>systemctl start X4 server</code> or <code>service X4 server start</code> command.
Stopping service X4-Server:	Execute <code>systemctl stop X4 server</code> or <code>service X4 server stop</code> command.
Restarting service X4-Server:	Execute <code>systemctl restart X4 server</code> or <code>service X4 server restart</code> command.
See status of service X4-Server:	Execute <code>systemctl status X4 server</code> or <code>service X4 server status</code> command.
Reload service X4-Server:	Execute <code>systemctl reload X4 server</code> or <code>service X4 server reload</code> command.

2.1.4.3 Uninstalling the service X4-Server

To uninstall an X4 server installed via RPM package and its corresponding service X4 Server, enter the command `sudo rpm -e X4-Server_SLES-7.v.v-r.x86_64`.

During uninstallation, backup copies of the configuration files, the system database and the X4DB are automatically created under `opt/x4_backups`.

2.1.5 Installing the X4 Server in Docker

In this section, you will learn how to install the X4 Server in a docker and run it as a docker container.

Prerequisites

- Docker has to be installed and set up on your system. You can find information within the Docker documentation under <https://docs.docker.com/>.
- Knowledge of the docker mode of operation is assumed.
- `x4_server:6.x.x` refers to the current X4 BPMS version.

1. Run the docker using the command `docker run -d -p 8080:8080 --name x4-servercontainer softproject/x4_server`.

Further helpful commands:

Application example	Command
Run a container and display the logs after creating the container:	<code>docker run -d -p 8080:8080 --name x4-server-container softproject/x4_server && docker logs x4-server-container</code>
Run X4 Server with a PostgreSQL database X4 - Host: 10.0.75.1 - Default PostgreSQL port: 5432	<code>docker run -d -p 8080:8080 -e DATABASE_MODE='postgresql' -e DATABASE_HOST='10.0.75.1' softproject/x4_server</code>
Run X4 Server with port 8081 and a PostgreSQL database X4 - Host: 10.0.75.1 - Port: 5435	<code>docker run -d -p 8081:8080 -e DATABASE_MODE='postgresql' -e DATABASE_HOST='10.0.75.1' -e DATABASE_PORT='5435' softproject/x4_server</code>
Run X4 Server with port 8081 and a PostgreSQL database X4 - Access data: postgres/postgres - Host: 10.0.75.1 - Port: 5435	<code>docker run -d -p 8081:8080 -e DATABASE_MODE='postgresql' -e DATABASE_USER='postgres' -e DATABASE_PASSWORD='postgres' -e DATABASE_HOST='10.0.75.1' -e DATABASE_PORT='5435' softproject/x4_server</code>
Run X4 Server with an MS SQL database X4 - Access data: X4/X4 - Host: 10.0.75.1 - Port: 1434	<code>docker run -d -p 8080:8080 -e DATABASE_MODE=sqlserver -e DATABASE_HOST=10.0.75.1 -e DATABASE_NAME=X4 -e DATABASE_PORT=1434 -e DATABASE_USER=X4 -e DATABASE_PASSWORD=X4 softproject/x4_server</code>
Run X4 Server and map the X4DB folder from an external path to the X4DB folder within the container (only for Linux)	<code>docker run -d -p 8080:8080 -v /home/anyUser/X4/X4DB/1:/opt/X4/X4DB/1 softproject/x4_server</code>

Environment variables

Variable	Erläuterung
X4_UID	The unix user ID the technical process is run as
X4_GID	The unix group ID the technical process is run as
JAVA_XMS	Initial heap space for the JVM Default value: 512M
JAVA_XMX	Maximum heap space for the JVM Default value: 2048M
DATABASE_MODE	Determines the database connection driver and strategy Possible values are h2 (default), postgresql and sqlserver

Variable	Erläuterung
DATABASE_HOST	Host name of the database server (if not h2) The default value is database, obliging you to change it.
DATABASE_PORT	Port number of the database server (if not h2). The default port for PostgreSQL server (postgres) is 5432. The default port is not set automatically.
DATABASE_NAME	Name of the database hosted within the database server to use for the X4 Server (if not h2)
DATABASE_USER	Name of the database user
DATABASE_PASSWORD	Password to access the database

2.1.6 Installing the X4 Server on other operating systems

If required, the X4 Server can also be installed on other operating systems. Please contact SoftProject for further information.

2.2 Initially installing a licence

1. Click the  icon in the toolbar.
2. Click **Install license**.
3. Select X4 license
4. Click **Open**.

Your new license is now installed. In the status bar at the bottom of X4 Designer you can see how long your license is still valid.

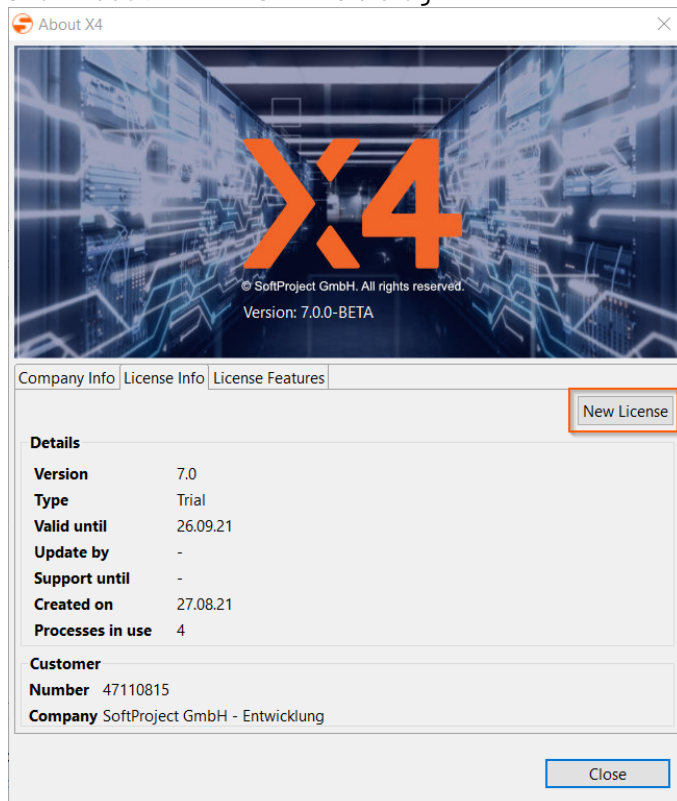
✔ Via **Help > About X4 BPMS > License Information** and **License Features** you have the possibility to retrieve information about your license at any time.

2.3 Renewing license

⚠ To renew a license, you must have previously installed a license.

1. Click **Help** in the menu bar.

2. Click **About X4 BPMS** in the dialog.



3. Under **License Info** click **New license**.
4. Navigate to the new license and click **Open**.

If the installation is successful, the license information will update automatically after a short time.

2.4 Displaying license information

 To display license information, a license must be installed.

1. In the X4 Designer menu bar, click **Help > About X4 BPMS**.
2. To view the license information, click the **License Info** tab or the **License Features** tab.

2.5 Install and uninstall X4 Designer

2.5.1 Install X4 Designer

For **production purposes**, the X4 Designer is provided as a separate MS Windows installation package in the form of an MSI file.



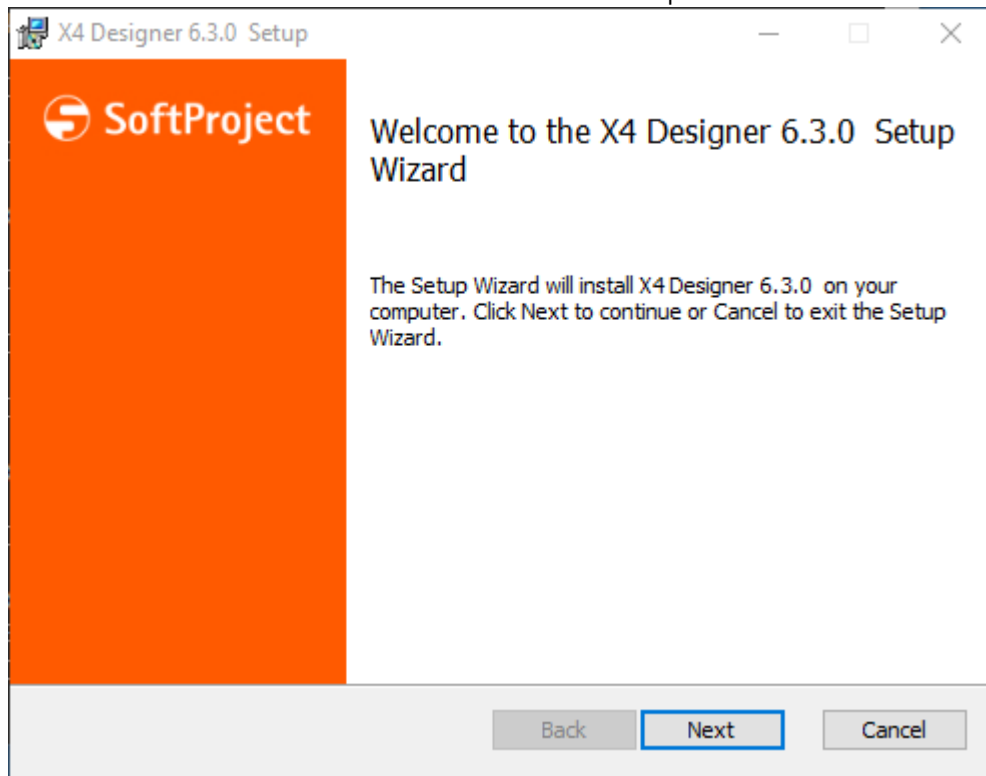
- You can install only one X4 Designer on a Windows system. The MS Windows installation package overwrites existing installations. If you overwrite an existing installation, this can lead to problems and data loss.
- To use multiple X4 Designer for testing purposes, we provide the **MS Windows All-in-one** installation package in the [download section](#) of our website.

1. Double-click the X4Designer_Setup.msi executable file to begin the installation.



Windows Defender SmartScreen issues a warning at the start of the installation. Click **More information** and start the installation routine as usual with **Run anyway**.

The start screen of the installation routine will now open.



2. Click **Next**.
3. Specify the installation path for X4 Designer.
4. If necessary, create a shortcut to the desktop by activating the option **Create a shortcut for X4 Designer on the desktop**.
5. Click **Next** to confirm the path.
6. Click **Install** to execute the installation.
The progress of the installation is now displayed.
7. **Finish** button to terminate the installation.

- ✓ By activating the **Launch X4 Designer when setup exists** option, X4 Designer is started immediately after installation.

The X4 Designer has now been installed under the specified path.

8. If not already done automatically, start X4 Designer to check the installation.

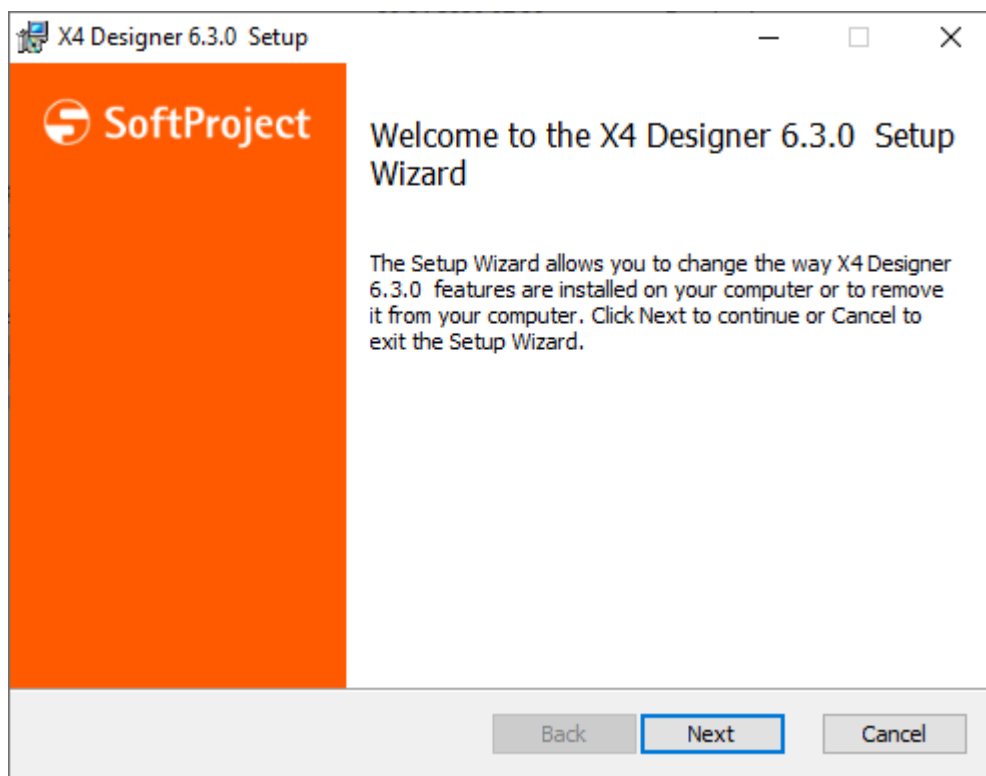
✓ Unattended installation

The installation of the X4 Designer can also be performed via an unattended installation. To do this, enter the following command in the command line, for example: `*C:\Installation location of the MSI /q/n /L*V "C:\temp\test.log*`

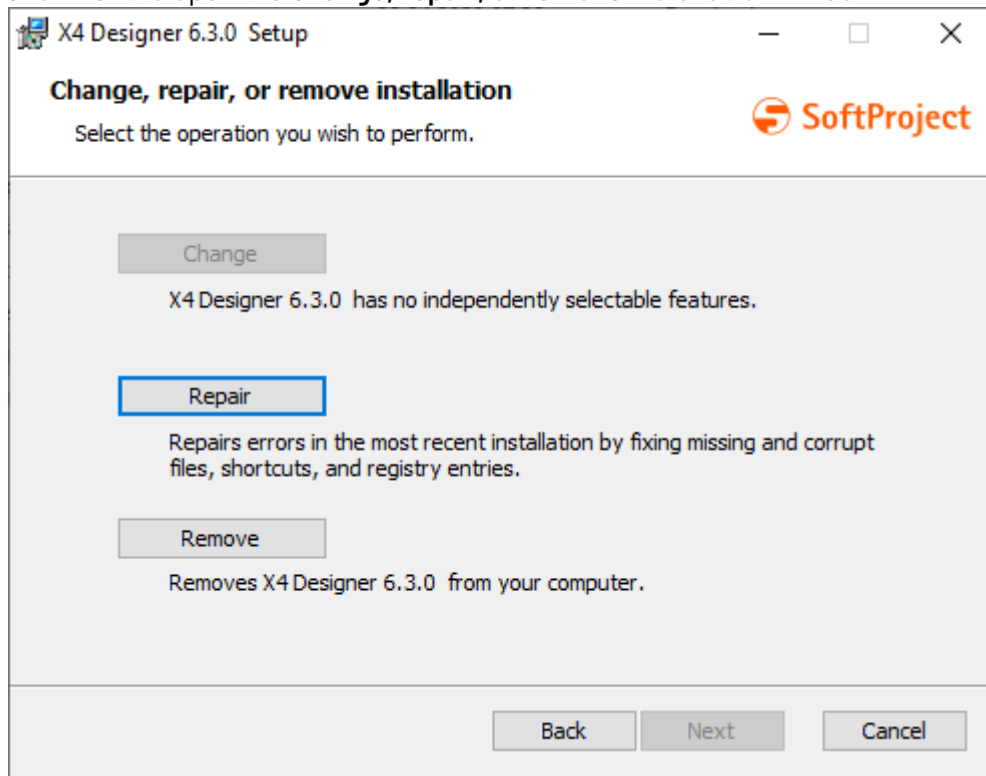
2.5.2 Uninstall X4 Designer

X4 Designer can be uninstalled either via the Windows Start menu, the Windows Control Panel or by executing the installation file again.

1. Die Ausführbare Datei X4Designer_Setup.msi doppelklicken.
Der Startbildschirm der Installationsroutine wird nun geöffnet.



- Click **Next** to open the **Change, repair, or remove installation** window.



- Click **Remove**.
- In the next window click **Remove** again to start the uninstallation. The progress of the uninstallation is now displayed.
- Click **Finish** to terminate the uninstallation. X4 Designer has now been uninstalled.

2.5.3 Parameters of the unattended installation

To perform an unattended installation using the command line, the following parameters must be set:

Parameters	Description
INSTALLFOLDER	Installation path

2.6 Installation and migration of the system database and X4DB

You can download the update tool from the download section of our website.

2.7 Installation of the authentication provider

The authentication provider Keycloak is included in the X4 Server installation package.

If you want to launch the Keycloak authentication provider as a Docker container, you need to load the Docker image.

✔ For more information, see section [Loading Docker image and launching container](#).

3 Configuration

3.1 Configuring the X4 Server

How to customize the configuration of the *X4 Server* to your environment

3.1.1 Setting up the Database

- Setting up the Oracle Database
- Configuration for MSSQL and PostgreSQL

3.1.1.1 Setting up the Oracle Database

If you are using an Oracle database, the following additional settings must be made:

Using the migration/installation tool with Oracle

Note:

- The migration/installation tool must be run even if no migration of an existing X4 BPMS installation is intended.
- Before running the migration/installation tool, you must first create an empty database named X4.
- To use the migration tool (see [Updating the X4 Server](#)) with Oracle, the Oracle driver must be added to the classpath when starting the tool.
- You can find drivers for the corresponding Oracle database under <https://www.oracle.com/database/technologies/appdev/jdbc.html>.

Providing the driver as WildFly module

1. Download the corresponding driver under <https://www.oracle.com/database/technologies/appdev/jdbc.html>.
2. Create a WildFly module for the JDBC driver. Therefore, create the folder structure `oracle\jdbc\main` under `X4\Server\wildfly\modules\`.
3. Unpack the JDBC driver (e. g.: `ojdbc.jar`) within the folder structure created above.
4. Create the file `module.xml` with the following content:

module.xml

```
<module xmlns="urn:jboss:module:1.5" name="oracle.jdbc"><!-- The namespace
urn:jboss:module:1.5 may differ depending on the WildFly version. -->
  <resources>
    <resource-root path="ojdbc.jar"/><!-- Enter the file name of the JDBC
driver to be used and which is situated within the specified folder here. -->
  </resources>
  <dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

The module `oracle.jdbc` is now available.

Registering the driver within the standalone.xml

To use the driver within the datasources, register the driver within the `standalone.xml` under `X4\Server\wildfly\standalone\configuration\`:

```
...
<subsystem xmlns="urn:jboss:domain:datasources:5.0">
  <datasources>
    ...
    <drivers>
      ...
      <driver name="oracle" module="oracle.jdbc"><!-- Enter the module name here -->
        <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
      </driver>
    </drivers>
  </datasources>
</subsystem>
...
```

Configuring the datasources

Configure the Oracle datasources within the `standalone.xml` under `X4\Server\wildfly\standalone\configuration\`:

```

...
<subsystem xmlns="urn:jboss:domain:datasources:5.0">
  <datasources>
    ...
    <datasource jta="false" jndi-name="java:/X4BAM_DS" pool-name="X4BAM_DS" enabled="
true" use-java-context="true">
      <connection-url>jdbc:oracle:thin:@localhost:1521/pluggable-database</connection-
url><!-- Enter the corresponding Host, Port, SID or Service name here -->
      <driver>oracle</driver><!-- Enter the driver name here -->
      <security>
        <user-name>X4SERVER</user-name>
        <password>X4</password>
      </security>
      <statement>
        <prepared-statement-cache-size>32</prepared-statement-cache-size>
      </statement>
      <!-- In <validation> and <timeout> define settings for automatic reconnection
-->
      <validation>
        <check-valid-connection-sql>select 1 from dual</check-valid-connection-sql>
        <validate-on-match>false</validate-on-match>
        <background-validation>true</background-validation>
        <background-validation-millis>1000</background-validation-millis>
      </validation>
      <timeout>
        <allocation-retry>60</allocation-retry>
        <allocation-retry-wait-millis>1000</allocation-retry-wait-millis>
      </timeout>
    </datasource>
    <datasource jta="true" jndi-name="java:/PermissionDS" pool-name="PermissionDS"
enabled="true" use-java-context="true">
      <connection-url>jdbc:oracle:thin:@localhost:1521/pluggable-database</connection-
url><!-- Enter the corresponding Host, Port, SID or Service name here -->
      <driver>oracle</driver><!-- Enter the driver name here -->
      <security>
        <user-name>X4SERVER</user-name>
        <password>X4</password>
      </security>
      <statement>
        <prepared-statement-cache-size>32</prepared-statement-cache-size>
      </statement>
      <!-- In <validation> and <timeout> define settings for automatic reconnection
-->
      <validation>
        <check-valid-connection-sql>select 1 from dual</check-valid-connection-sql>
        <validate-on-match>false</validate-on-match>
        <background-validation>true</background-validation>
        <background-validation-millis>1000</background-validation-millis>
      </validation>
      <timeout>
        <allocation-retry>60</allocation-retry>
        <allocation-retry-wait-millis>1000</allocation-retry-wait-millis>
      </timeout>
    </datasource>
  
```

```
<drivers>
...
  <driver name="oracle" module="oracle.jdbc"><!-- Enter the module name here -->
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
  </driver>
</drivers>
</datasources>
</subsystem>
...
```

3.1.1.2 Configuration for MSSQL and PostgreSQL

If you are using a PostgreSQL or MS SQL database, the following additional settings must be made:

Using the migration/installation tool with Oracle

-  The migration/installation tool must be run even if no migration of an existing X4 BPMS installation is intended, see [Updating the X4 Server](#). Before running the migration/installation tool, you must first create an empty database named X4.

Configuring the datasources

Configure the datasources within the `standalone.xml` under `X4\Server\wildfly\standalone\configuration\` as follows:

```

...
<!-- PostgreSQL -->
<datasource jta="false" jndi-name="java:/X4BAM_DS" pool-name="X4BAM_DS" enabled="true"
" use-java-context="true">
  <connection-url>jdbc:postgresql://localhost:5432/X4</connection-url>
  <driver>postgresql</driver>
  <new-connection-sql>SET search_path TO X4SERVER;</new-connection-sql>
  <pool>
    <max-pool-size>20</max-pool-size>
  </pool>
  <security>
    <user-name>x4</user-name>
    <password>x4</password>
  </security>
  <statement>
    <prepared-statement-cache-size>20</prepared-statement-cache-size>
    <share-prepared-statements>true</share-prepared-statements>
  </statement>
  <!-- In <validation> and <timeout> define settings for automatic reconnection -->
  <validation>
    <check-valid-connection-sql>select 1</check-valid-connection-sql>
    <validate-on-match>false</validate-on-match>
    <background-validation>true</background-validation>
    <background-validation-millis>1000</background-validation-millis>
  </validation>
  <timeout>
    <allocation-retry>60</allocation-retry>
    <allocation-retry-wait-millis>1000</allocation-retry-wait-millis>
  </timeout>
</datasource>
<datasource jndi-name="java:/PermissionDS" pool-name="PermissionDS" enabled="true"
use-java-context="true">
  <connection-url>jdbc:postgresql://localhost:5432/X4</connection-url>
  <driver>postgresql</driver>
  <new-connection-sql>SET search_path TO X4SERVER;</new-connection-sql>
  <pool>
    <max-pool-size>20</max-pool-size>
  </pool>
  <security>
    <user-name>x4</user-name>
    <password>x4</password>
  </security>
  <statement>
    <prepared-statement-cache-size>20</prepared-statement-cache-size>
    <share-prepared-statements>true</share-prepared-statements>
  </statement>
  <!-- In <validation> and <timeout> define settings for automatic reconnection -->
  <validation>
    <check-valid-connection-sql>select 1</check-valid-connection-sql>
    <validate-on-match>false</validate-on-match>
    <background-validation>true</background-validation>
    <background-validation-millis>1000</background-validation-millis>
  </validation>
  <timeout>

```

```

        <allocation-retry>60</allocation-retry>
        <allocation-retry-wait-millis>1000</allocation-retry-wait-millis>
    </timeout>
</datasource>
<!-- MSSQL -->
<datasource jndi-name="java:/PermissionDS" pool-name="PermissionDS" enabled="true"
use-ccm="true">
    <connection-url>jdbc:sqlserver://localhost:1433;databaseName=X4</connection-url>
    <driver>sqlserver</driver>
    <transaction-isolation>TRANSACTION_READ_COMMITTED</transaction-isolation>
    <pool>
        <min-pool-size>5</min-pool-size>
        <max-pool-size>20</max-pool-size>
    </pool>
    <security>
        <user-name>x4s</user-name>
        <password>x4</password>
    </security>
    <!-- In <validation> and <timeout> define settings for automatic reconnection -->
    <validation>
        <check-valid-connection-sql>select 1</check-valid-connection-sql>
        <validate-on-match>false</validate-on-match>
        <background-validation>true</background-validation>
        <background-validation-millis>1000</background-validation-millis>
    </validation>
    <timeout>
        <allocation-retry>60</allocation-retry>
        <allocation-retry-wait-millis>1000</allocation-retry-wait-millis>
    </timeout>
</datasource>
<datasource jta="false" jndi-name="java:/X4BAM_DS" pool-name="X4BAM_DS" enabled="true
" use-ccm="true">
    <connection-url>jdbc:sqlserver://localhost:1433;databaseName=X4</connection-url>
    <driver>sqlserver</driver>
    <transaction-isolation>TRANSACTION_READ_COMMITTED</transaction-isolation>
    <pool>
        <min-pool-size>5</min-pool-size>
        <max-pool-size>20</max-pool-size>
    </pool>
    <security>
        <user-name>x4s</user-name>
        <password>x4</password>
    </security>
    <!-- In <validation> and <timeout> define settings for automatic reconnection -->
    <validation>
        <check-valid-connection-sql>select 1</check-valid-connection-sql>
        <validate-on-match>false</validate-on-match>
        <background-validation>true</background-validation>
        <background-validation-millis>1000</background-validation-millis>
    </validation>
    <timeout>
        <allocation-retry>60</allocation-retry>
        <allocation-retry-wait-millis>1000</allocation-retry-wait-millis>
    </timeout>
</datasource>

```

```

...
<drivers>
  ...
  <driver name="postgresql" module="org.postgresql">
    <driver-class>org.postgresql.Driver</driver-class>
  </driver>
  <driver name="sqlserver" module="com.microsoft.sqlserver">
    <driver-class>com.microsoft.sqlserver.jdbc.SQLServerDriver</driver-class>
  </driver>
  ...
</drivers>

```

3.1.2 Configuring via the X4config.xml

The global configuration file `X4config.xml` allows you to change various setting of the X4 Server.

3.1.2.1 iXServ configuration

In the `server > services` element within the `X4config.xml`, various X4 Server services can be enabled and disabled.

<snmpagent>	Activate SNMP (Simple Network Management Protocol). For this, an SNMP Trap Appender must be configured, see SNMP trap appender. Possible values: • <i>on</i>: Enable SNMP service • <i>off</i>: Disable SNMP service (default)
<jcoserver>	Enable SAP Java Connector service Possible values: • <i>on</i>: Activate JCo service • <i>off</i>: Disable JCo service (default)

3.1.2.2 SNMP configuration

Within the element `<snmp>` of the `X4config.xml` you can configure various settings for the *Simple Network Management Protocol* (SNMP). MIB files that are required therefore can be requested at the SoftProject support team.

<readCommunity>	Configure the SNMP <i>Read-only Community String</i> Possible values: <i>public</i>: Public (default)
-----------------	--

<code><writeCommunity></code>	Configure the SNMP <i>Write Community String</i> Possible values: <i>private</i> : Private (default)
<code><agentPort></code>	Port at which the SNMP agent listens Possible values: - Any integer number <i>10161</i>: Port 10161 (default)
<code><version></code>	Used SNMP version Possible values: <i>1</i>: Use SNMP version 1 <i>2</i>: Use SNMP version 2 (default)

3.1.2.3 Configuring the Placeholder Storage for X4 Server

A placeholder storage is configured within the file `X4config.xml`. The root element `x4` can be added a placeholder element where the configuration is made.

```
<placeholder>
  <storage>
    <class>example.PlaceholderStorage</class><!-- Fully qualified class name of
the implementation to be used. -->
    <config /><!-- Optional and depending on the placeholder storage
implementation. -->
  </storage>
</placeholder>
```

Available Placeholder Storages

The following three placeholder storages are available by default:

Name	Class name	Description
<i>Properties Placeholder Storage</i>	<code>de.softproject.integration.engine.placeholder.PropertiesPlaceholderStorage</code>	Placeholders are stored in <code>Properties</code> files in the file system. The directory containing the files is configurable.
<i>SQL Placeholder Storage</i>	<code>de.softproject.integration.engine.placeholder.SQLPlaceholderStorage</code>	Placeholders are stored in an SQL database. The target database is configurable.

Name	Class name	Description
<i>In-Memory Placeholder Storage</i>	de.softproject.integration.engine.placeholder.InMemoryPlaceholderStorage	Placeholders are stored in main memory and are therefore NOT persistent. If no or no valid placeholder storage is defined, it will be used as fallback.

Properties Placeholder Storage Configuration

The directory where the Properties files are located can be defined within the `config` element as follows:

```
<placeholder>
  <storage>
    <class>de.softproject.integration.engine.placeholder.PropertiesPlaceholderStorage</class>
    <config>
      <path>C:/X4/PlaceholderStorage</path>
    </config>
  </storage>
</placeholder>
```

SQL Placeholder Storage Configuration

The database to be used can be defined within the `config` element as follows:

 The corresponding tables must exist in the *X4Server schema*!

```
<placeholder>
  <storage>
    <class>de.softproject.integration.engine.placeholder.SQLPlaceholderStorage</class>
    <config>
      <jndi>java:/X4BAM_DS</jndi>
    </config>
  </storage>
</placeholder>
```

3.1.2.4 LDAPS configuration

To allow self-signed certificates for LDAPS, the path to the truststore and the corresponding password must be specified in the `X4config.xml` configuration file via the `<trustStore>` and `<trustStorePassword>` elements.

⚠ You can specify only one truststore. The specified truststore affects the HTTPS configuration and the use of certificates.

```
<x4>
...
<webContainerURL/>
<trustStore>TrustStore path</trustStore>
<trustStorePassword>TrustStore password</trustStorePassword>
<logging/>
...
</x4>
```

3.1.3 Configuring the Logging

How to configure the X4 Server's logging behavior.

3.1.3.1 Save Point Configuration for the X4 Server

The Save Point configuration for the X4 server can be configured via the `x4config.xml`. The following parameters can be defined:

Sample logging configuration

```
<savepoint storage="database"></savepoint>
```

Explanation of the parameters of the `savepoint` element:

Attribute	Description
storage	Defines the location for processing save points in the X4 server <i>Possible values:</i> <i>filesystem</i>: Save Points are written to the filesystem, to the server directory savepoints <i>database</i>: Save Points are written to the X4 system database

i If the `savepoint` element in the `x4config.xml` is removed, then no save points are saved.

3.1.3.2 SNMP trap appender

As an extension for Log4j you can use an appender for Simple Network Management Protocol (SNMP) traps. It allows to output log events as formatted string to a specific Management Host as an SNMP trap.

To generate SNMP traps it is required to configure an SNMP trap appender for Log4j, and to assign a corresponding category to the appender.

3.1.3.3 Ad hoc logging at runtime

For extended error analysis, it is possible to log the output of individual process steps at runtime. This requires neither changing the `.wrf` file of the related technical process nor restarting the server. In addition, conditional logging in sub-processes is also made possible, e.g. if a sub-process was called by a certain main process.

Configuration

The logging behaviour can be controlled via the `tracelog.properties` file under `X4\Server\X4DB\0`. The expected format is also described here, among other things, if a process or process step is to be addressed and logging is to be switched on:

- **Log individual process steps:** Individual process steps that are to be logged can be specified according to the following scheme: `<user>/<process path>/<ActionID> = 1`
- **Conditional logging of subprocess steps:** If single process steps are to be logged in a subprocess that was called by a specific parent process, this can be specified using the following scheme: `executor_user>/<process_path_parent>/<user>/<process_path_subprocess>/<ActionID> = 1`

The content of the log output corresponds to the content of the logging via `Log4J` on a transition, i.e. the status or the data of the last process step is logged via `Log4J`. The `Log4J` logger used is `de.softproject.integration.logging.integrated.TraceLog` and the `Log4J` log level is `INFO`.

If changes have been made in the `tracelog.properties` file, the configuration must be read in again. The reading of the configuration can be triggered via the MBean. To do this, execute the MBean operation **reloadTraceLogSettings**.

Sample configurations

Log single process steps

Sample configuration for logging a specific process step

```
1/Test/Log/logtest.wrf/2 = 1
```

Explanation

Logging is enabled for:

- user `1`
- Process `Test/Log/logtest.wrf`
- Process component with `Action ID 2`

Conditional logging of subprocess steps

Sample configuration for conditional logging of a subprocess

```
1/Test/Log/logtestParent.wrf/1/Test/Log/logtestSub.wrf/2 = 1
```

Explanation

Logging is enabled for:

- User *1*
- Process *Test/Log/logtestSub.wrf*
- Process component with *Action ID 2*

Condition:

- Process *Test/Log/logtestParent.wrf* was executed by
- user *1*

3.1.4 Configuring the production mode

As the most common way to improve the performance, the *X4 Server* provides a production mode. Thereby, the caching for the repository is activated.

1. In the central configuration file `X4config.xml` set the value of `<productionMode>` to *on*.
2. Restart the *X4 Server*, see [Controlled shutdown of the X4 Server \(via JMX\)](#).

The production mode respectively the caching is enabled after the restart.

Please note:

- To disable the production mode, set the value of `<productionMode>` back to *off* and restart the server.
- To edit the repository during the production mode, e.g if you want to modify processes and schedules, it is not required to restart the *X4 Server*.

3.1.5 Enabling SSL and HTTPS for X4 Server

SSL and HTTPS can be configured for the *X4 Server* that is based on WildFly.

Requirements

- You have already created a keystore
- You have a valid certificate

3.1.5.1 Customize key-stores

1. Open the **standalone.xml** in the server directory under **\wildfly\standalone\configuration**.
2. Modify the following lines.

```
<subsystem xmlns="urn:wildfly:elytron:14.0" final-providers="combined-  
providers" disallowed-providers="OracleUcrypto">  
...  
  <tls>  
    <key-stores>  
      <key-store name="KeystoreName">  
        <credential-reference clear-text="password"/>  
        <file path="server.keystore" relative-to="jboss.server.config.dir"/>  
      </key-store>  
    </key-stores>  
    ...  
  </tls>  
  ...  
</subsystem>
```

- name: Name of the key-store. Used to reference the key-store in the key-manager element.
- file: Path to the key-store. In the above example, a relative path is specified. If you specify an absolute path to the key-store, the `relative-to` attribute is obsolete.

3.1.5.2 Customize key-managers

1. Open the **standalone.xml** in the server directory under **\wildfly\standalone\configuration**.
2. Modify the following lines.

```
<subsystem xmlns="urn:wildfly:elytron:14.0" final-providers="combined-  
providers" disallowed-providers="OracleUcrypto">  
...  
  <tls>  
    ...  
    <key-managers>  
      <key-manager name="KeymanagerName" key-store="KeystoreName">  
        <credential-reference clear-text="password"/>  
      </key-manager>  
    </key-managers>  
    ...  
  </tls>  
  ...  
</subsystem>
```

- name: Name of the key-manager.
- key-store: Name of the key-store that will be used.

- `clear-text`: Password of the key-store.

3.1.5.3 Customize server-ssl-contexts

1. Open the **standalone.xml** in the server directory under `\wildfly\standalone\configuration`.
2. Modify the following lines.

```
<subsystem xmlns="urn:wildfly:elytron:14.0" final-providers="combined-  
providers" disallowed-providers="OracleUCrypto">  
...  
  <tls>  
    ...  
    <server-ssl-contexts>  
      <server-ssl-context name="httpsSSC" key-manager="KeymanagerName"  
protocols="TLSv1.2"/>  
    </server-ssl-contexts>  
    ...  
  </tls>  
  ...  
</subsystem>
```

- `name`: Name of the SSL-context.
- `key-manager`: Name of the key-manager that will be used.
- `protocols`: SSL/TLS protocol to be used. The above example uses TLSv1.2.

3.1.5.4 Customize https-listener

1. Open the **standalone.xml** in the server directory under `\wildfly\standalone\configuration`.
2. Modify the following lines.
3. To disable HTTP, remove the `<http-listener>` line.

```
<subsystem xmlns="urn:jboss:domain:undertow:12.0" default-server="default-  
server" default-virtual-host="default-host" default-servlet-container="default"  
default-security-domain="other" statistics-enabled="$  
{wildfly.undertow.statistics-enabled:${wildfly.statistics-enabled:false}}">  
...  
  <https-listener name="https" socket-binding="https" ssl-context="httpsSSC"  
enable-http2="true"/>  
  ...  
</subsystem>
```

- `ssl-context`: Name of the SSL context that will be used.

3.1.5.5 Customize socket-binding

1. Open the **standalone.xml** in the server directory under `\wildfly\standalone\configuration`.
2. Modify the following lines.

```
<socket-binding-group name="standard-sockets" default-interface="public" port-  
offset="${jboss.socket.binding.port-offset:0}">  
  ...  
  <socket-binding name="https" port="${jboss.https.port:8443}"/>  
  ...  
</socket-binding-group>
```

 By default, the https port is set to 8443, but you can customize the port as you wish.

 For more information, see the official WildFly documentation at https://docs.wildfly.org/25/WildFly_Elytron_Security.html#configure-sslts.

3.2 Configuring the X4 Designer

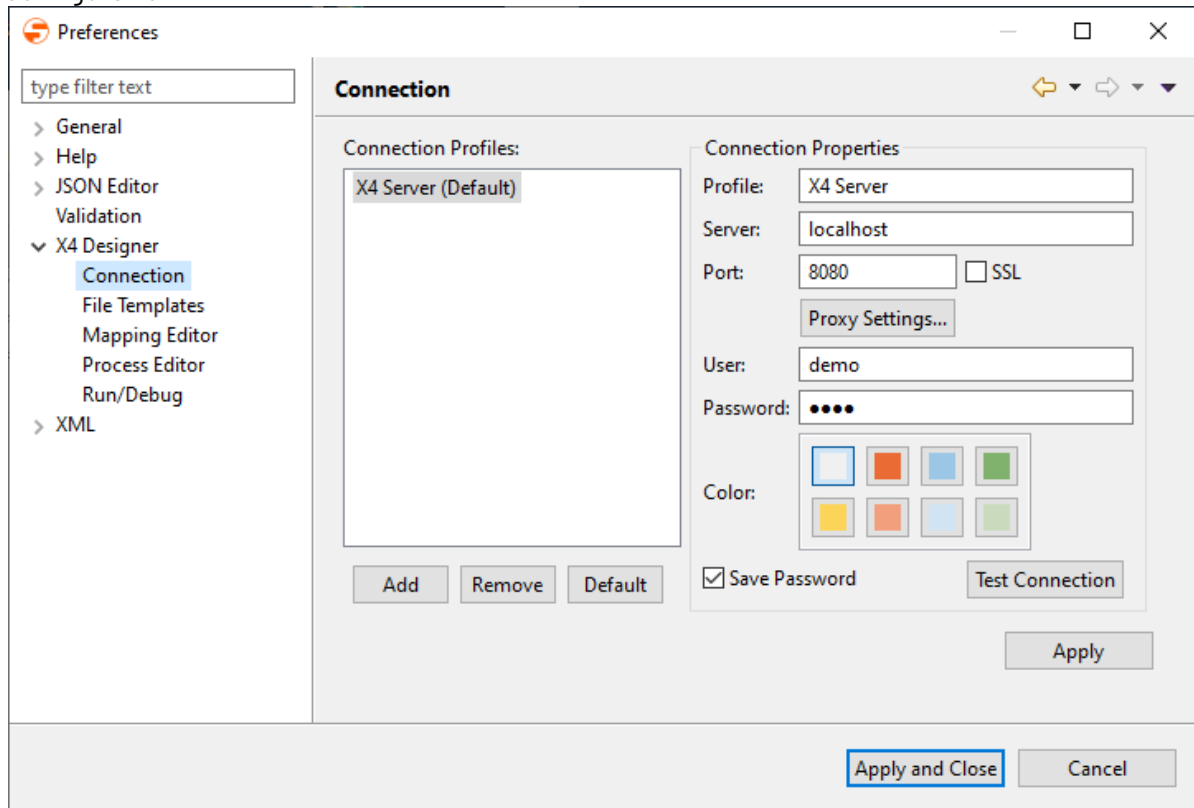
How to customize the appearance and behavior of the *X4 Designer*

3.2.1 Editing the connection configuration

Connection profiles with the respective profile data can be stored under **Connection**.

1. Select menu **Tools> Options**.

- On the left side, double-click **X4 Designer**, and select **Connection** to open the connections configuration.



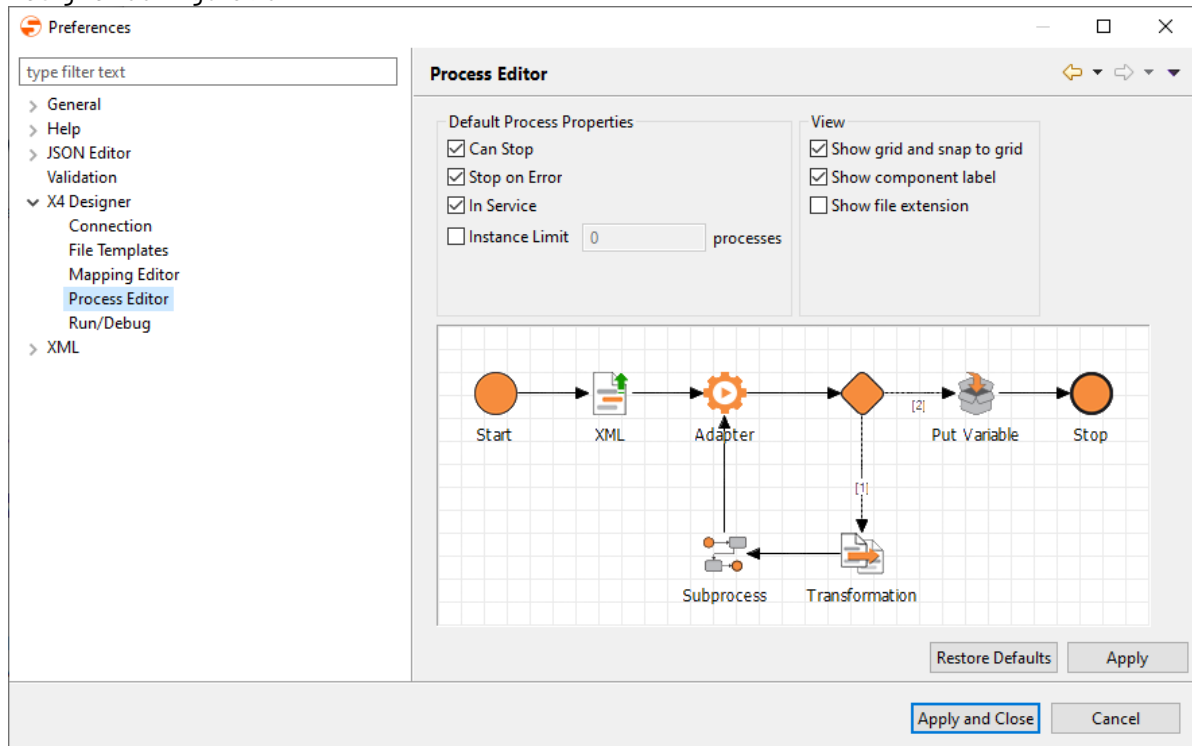
- Make the required connection settings:
 - Profile:** Name of the connection profile (arbitrary)
 - Server:** IP address or host name of the *X4 Server* (Example: localhost)
 - Port:** Port number
 - Proxy Settings:** Default settings for proxy servers and your internet connection
 - User:** Name of the repository user
 - Password:** Corresponding password
 - Color:** Color for the connection setting (optional)
 -  The color will be displayed in the *X4 Designer's* status bar on the next connect and helps you to differentiate between different *X4 Servers*.
- Click **Test Connection** to check if the connection functions properly.
- Click **Apply and Close** to save the configuration and close the window.

3.2.2 Configuring the Process Editor

Under **Process Editor**, settings for the representation of processes can be stored.

- Select menu **Tools> Options**.

- On the left side, double-click **X4 Designer**, and select **Process Editor** to open the Process Designer configuration.



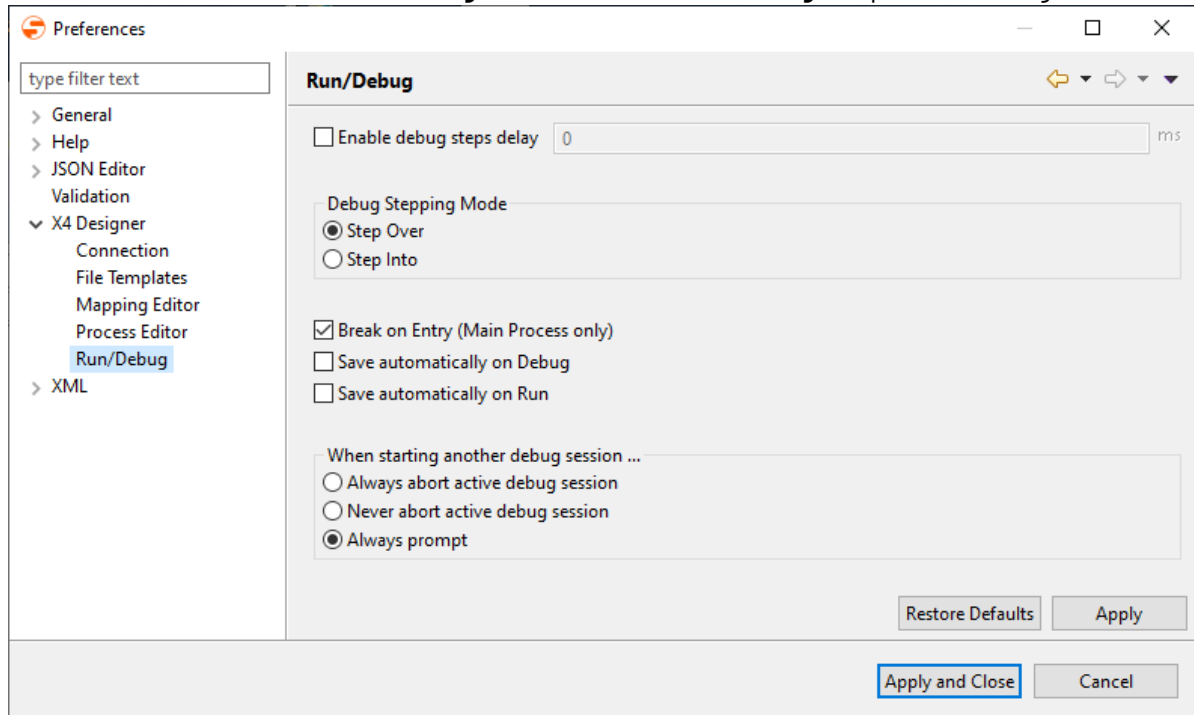
- Edit default behavior and properties of new processes in **Default Process Properties**:
 - **Can Stop**: Allows the process to be terminated
 - **Stop on Error**: Cancels process execution automatically when an error occurs
 - **Public/Private**: Process is executable
 - **Instance Limit**: Limit the number of process instances
 - **Show grid and snap to grid**: Display a grid and align all symbols to the grid lines
 - **Show component label**: Display a text label below process component symbols
 - **Show file extension**: Show process components with their file extensions (deactivated by default)
- Click **Apply and Close** to save the configuration and close the window.

3.2.3 Configuring the Run/Debug Mode

You can define the behavior of processes when they are run or debugged in the *X4 Designer*.

- Select menu **Tools > Options**.

2. On the left side double-click **X4 Designer**, and select **Run/Debug** to open the configuration.



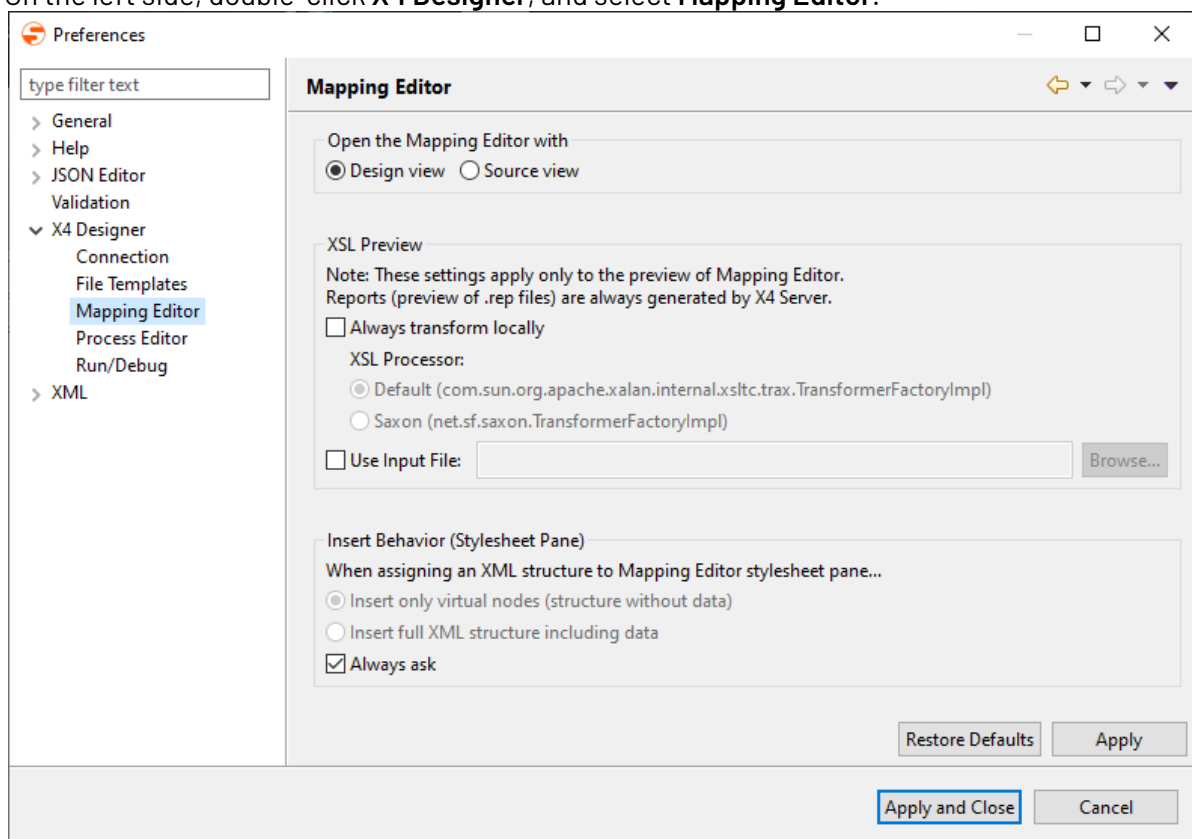
3. Make the required settings:
- **Enable debug steps delay:** Define the delay (in milliseconds) between each run process step in debug mode
 - i** The delay is only applied, if the process execution is continued via **Resume**.
 - **Debug Stepping Mode:** Default appearance of debugged process steps:
 - **Step Over:** Execute steps and debug each sub-process as one step
 - **Step Into:** Execute steps, jump into sub-processes, and display each sub-process action in debug mode
 - **Break on Entry (Main Process only):** Stop debugging after executing the first process action
 - **Save automatically on debug:** Save the process automatically before debugging
 - **Save automatically on run:** Save the process automatically before running
 - **When starting another debug session:** The debugger's behaviour when another debugging session is already active:
 - **Always abort active debug session:** The active debugging session will be aborted, and a new debugging session will start immediately.
 - **Never abort active debug session:** The active debugging session will never be aborted when trying to start another session (the active session must be aborted manually by the user).
 - **Always prompt:** When starting debug mode you will be prompted to abort.
 - i** The debugging can always be restarted via the F4 key.
4. Click **Apply and Close** to save the configuration and close the window.

3.2.4 Configuring the Mapping Editor

For the Mapping Editor's transformation preview, you can define whether the transformation is executed by the X4 Server or locally by the X4 Designer. In addition, you can configure if XML structures shall be inserted with or without content.

 This configuration applies only to the Mapping Editor when clicking  or when pressing the **F9** key! XSL mappings in executed processes are always transformed on the X4 Server!

1. Select menu **Tools > Options**.
2. On the left side, double-click **X4 Designer**, and select **Mapping Editor**.



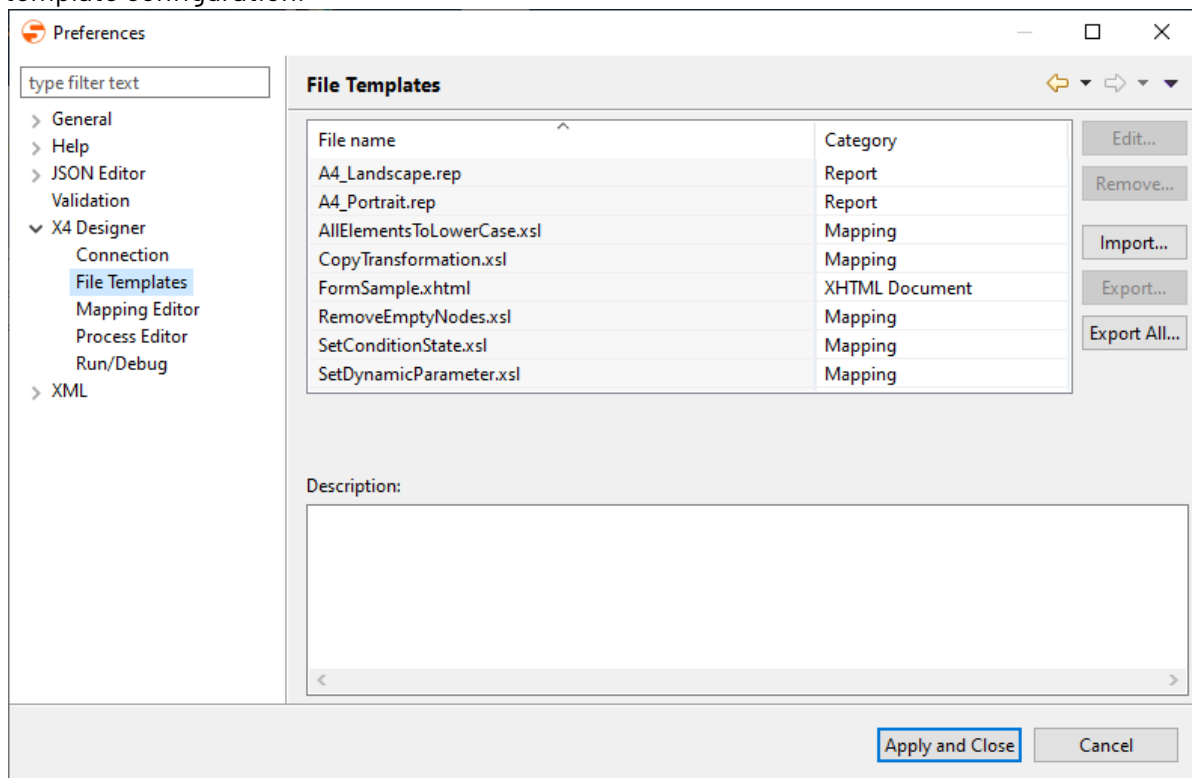
3. Configure the Mapping Editor's behavior:
 - In **Open the Mapping Editor with** define how XSL mappings shall be opened:
 - **Design view:** Open in the graphical mapping view (default)
 - **Source view:** Open in the source code view
 - In **XSL Preview** configure the behavior of XSL transformation previews
 - In **Insert Behavior (Stylesheet Pane)** define the default behavior when inserting XML:
 - **Insert only virtual nodes:** Display only the structure as virtual nodes in the Stylesheet pane
 - **Insert full XML structure including data:** Insert the full XML document structure including values
 - **Always ask:** Always ask when inserting XML via drag&drop, via the context menu or by **Strg+V** (checked by default)

4. Click **Apply and Close** to save the configuration and close the window.

3.2.5 Managing templates for repository elements

X4 Designer allows to define file templates for processes, process components or folders enabling to create repeating patterns quickly and easily.

1. Select menu **Tools > Options**.
2. On the left side, double-click **X4 Designer**, and select **File templates** to open the template configuration.



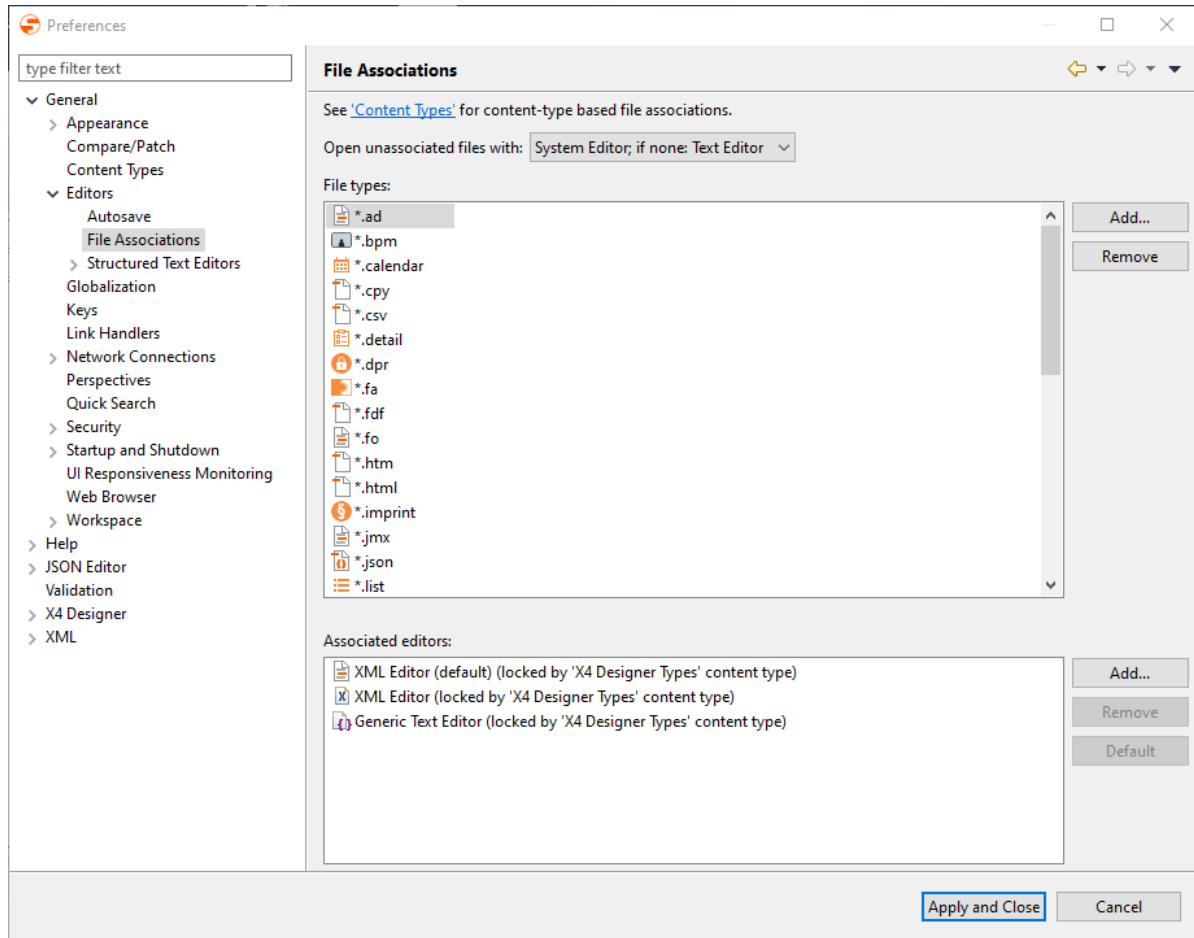
3. Manage the templates as desired:
 - **Edit:** Edit the template's name or description text
 - **Remove:** Delete a selected template
 - **Import:** Import an existing template folder
 - Only template directories with the same structure as the folder <X4>/X4DB/0/Templates can be imported.
 - **Export** respectively **Export All:** Export a selected template respectively all templates as template directories
4. Click **Apply and Close** to save the configuration and close the window.

3.2.6 Assigning file types to external or internal editors

X4 Designer allows to link any file types with editors and other programs.

1. Select the menu **Tools > Options**.

2. On the left side, select **General > Editors > File Associations**.



3. In **File types**, select an existing file type or add a new by clicking **Add**.

i You can either define a file extension using a * wildcard or a full file name. Example:
*.xyz or Filename.xyz

4. In **Associated editors**, select a suitable editor for the file type, or open the **Editor Selection** window by clicking **Add**. Then select the editor from a list of available editors.

i If you want to use an external editor, choose the option **External programs** within the **Editor Selection** window and click **Browse** to select the file of the external *application*.
Example: C:\Program Files\Notepad++\notepad++.exe.

✓ If the file type shall be opened by default with a selected editor, click **Default**.

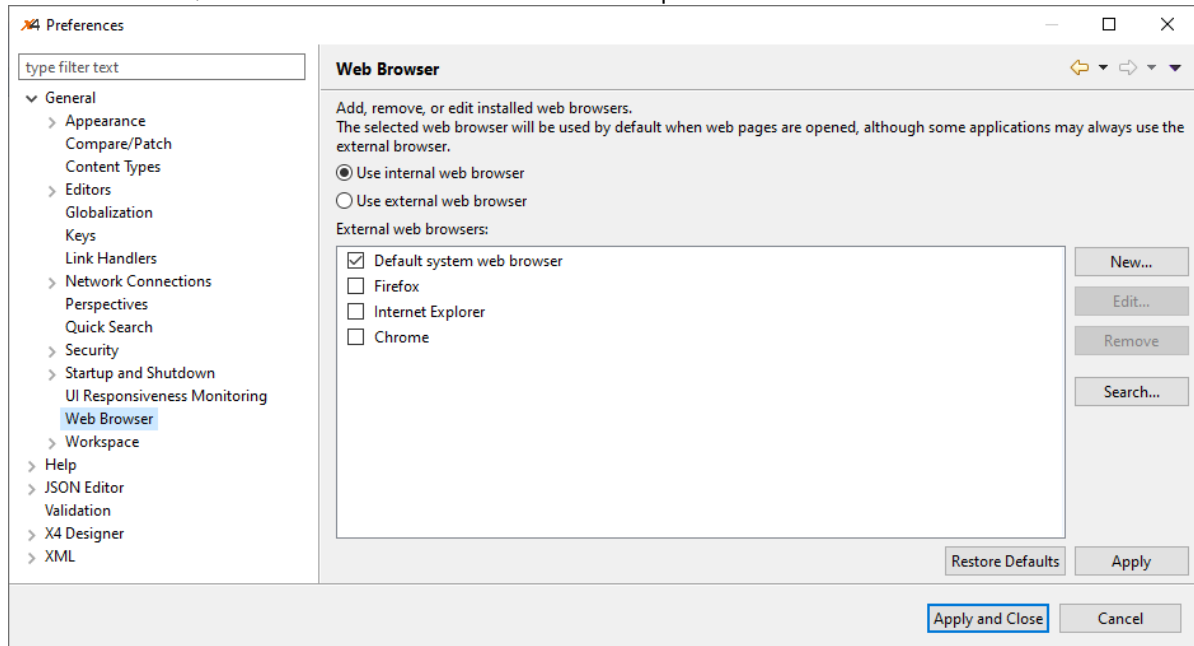
5. Click **Apply and Close** to save the settings and close the window.

The **Repository Navigator**'s context menu entry **Open with** now provides all internal or external editors assigned to this file type.

3.2.7 Configuring the Web Browser

Different browsers can be used to display browser-based components of the X4 BPMS (see [System requirements](#)). The browser used can be specified in the X4 BPMS.

1. Open **Tools> Options**.
2. On the left side, choose **General > Web Browser** to open the browser.



3. Choose one of the defined browsers or click **New**.
4. If **New** was clicked:
 - **Name:** Display name of the browser configuration
 - **Location:** File system path to the browser
 - **Parameters:** Parameters that are to be used when the browser is called.

To use Microsoft Edge the following must be entered:
Location: File system path to Microsoft prompt, e.g. `C:\Windows\System32\cmd.exe`
Parameters: `/c "start microsoft-edge: %URL%"`

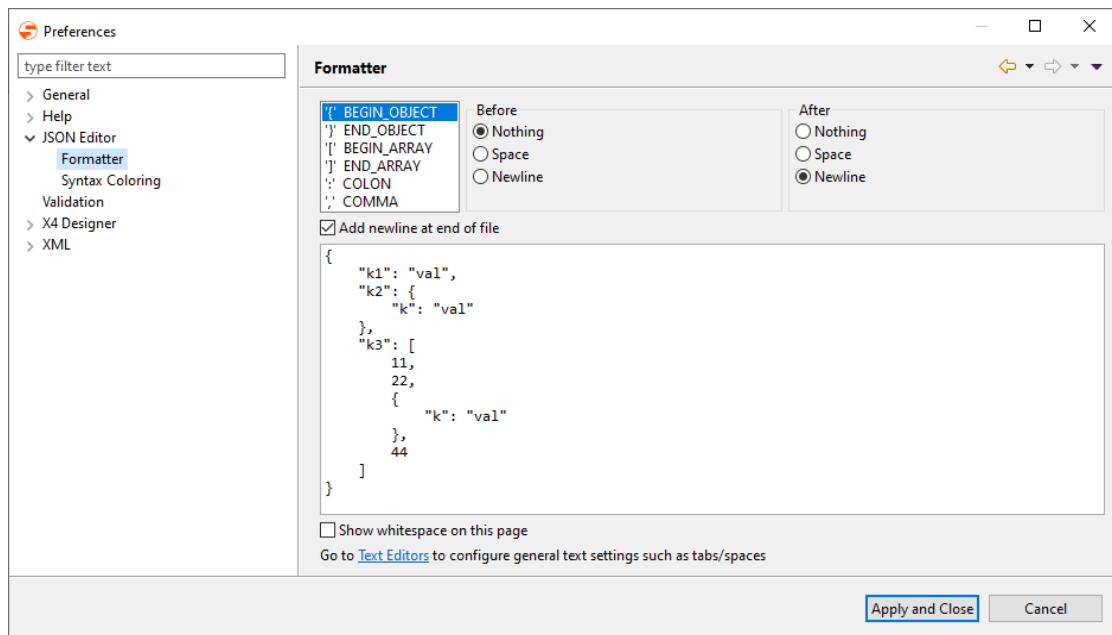
5. Confirm the settings with **OK**.
6. Click **Apply and Close** to save the configuration and close the window.

3.2.8 Configuring the JSON Editor

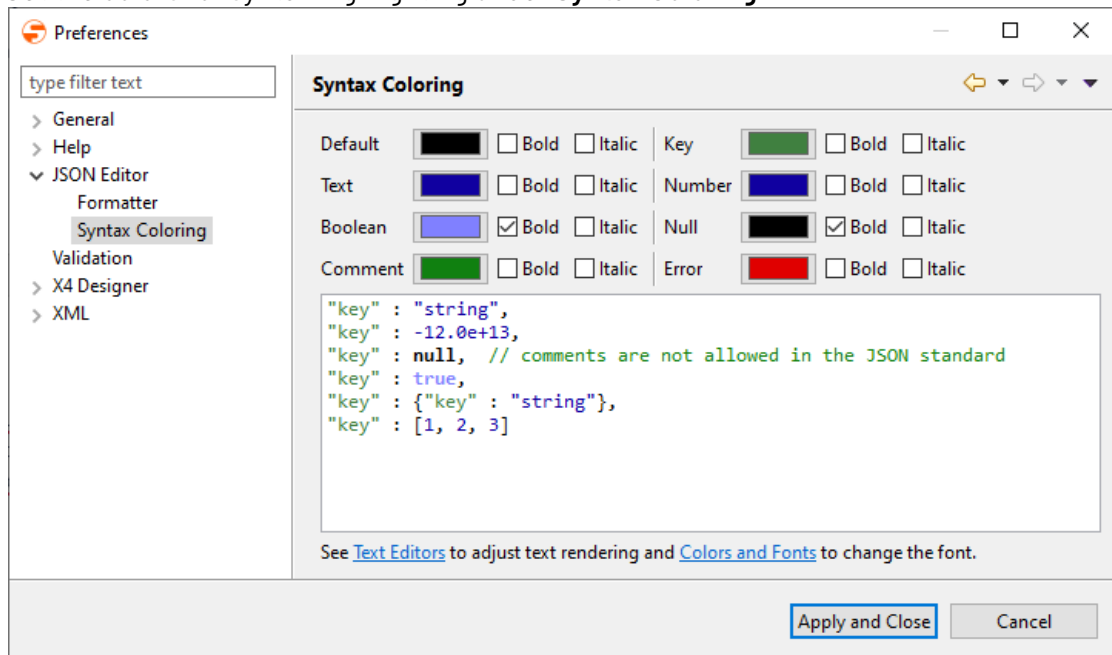
Under **JSON Editor**, settings for the JSON Editor can be stored.

1. Select menu **Tools> Options**.
2. On the left side, double-click **JSON Editor** to open the editor configuration.
3. Make the desired settings:

- Set the formatting of the JSON code under **Formatter**



- Set the colors for syntax highlighting under **Syntax Coloring**



4. Click **Apply and Close** to save the configuration and to close the window.

3.2.9 Changing the Help Language

The integrated help can be opened in a separate window via the menu **Help > Help Contents**. The help is divided into books, each one focusing on a different topic within the context of the X4 BPMS.

The language of the displayed help contents is based on the specified system language. However, it is possible to change the language at any time. If the system language is neither German nor English,

the help will be displayed in English by default.

The language can be adjusted within the file `X4Designer.ini` under `<X4>/Designer`. To switch the language, the language specification `en` for English or `de` for German must be adjusted.

Example: Adjustment for english help contents

```
-startup
plugins/org.eclipse.equinox.launcher_1.2.0.v20110502.jar
--launcher.library
plugins/org.eclipse.equinox.launcher.win32.win32.x86_1.1.100.v20110502
-nl
en
-vm
jre\bin\
-vmargs
-Xms64m
-Xmx1024m
-XX:MaxPermSize=128m
```

After restarting the X4 Designer, the help contents are available in the respective language.

4 Administering the X4 Server

Learn how to administer a productive X4 BPMS installation via JMX.

4.1 Updating the X4 Repository in production mode

In the X4 Server's production mode the caching for the X4 Repository is enabled. You can update repository project without restarting the server.

To avoid that outdated cache files will be used, the cache must be reset after updating the X4 Repository. This can be done with a JMX Management Bean (MBean) provided by the X4 Server with the name `X4Management`.

i The JMX MBean `X4Management` allows to reset the cache using the method `resetCache()`. In addition, caching statistics can be accessed with the method `cacheStatistics()` and an SAP JCo server can be restarted using the method `restartSAPJCoServer()`.

1. Update your X4 Repository.
2. Open the JMX MBean `X4Management`
 - Start the `jconsole` tool.
 - Open the JMX MBean `X4Management` in a domain `de.softproject.X4`
3. Invoke the MBean method `resetCache()`.
The cache will be reset.

4.2 Controlled shutdown of the X4 Server (via JMX)

How to shut down the *X4 Server* in a controlled way during processes are running

i **Prerequisites for shutting down**

A controlled shutdown of the X4 Server ensures that all currently running processes are fully executed and no more processes are started. This requires that the property `Can Stop` is not set for processes that are not allowed to be stopped. Moreover, endless processes must be modeled in such a way that they interrupt processing at regular intervals so that they can be stopped.

Depending on the message queue adapter, this can be done as follows:

- *JMS and RequestReply Transfer*: Specify a timeout in parameter `timeout`. If the adapter returns the status `0`, the queue is empty and the process control goes back to the adapter, allowing the process to be halted.
- *MQ Series Transfer and WebSphere MQ*: Enable the parameter `MQGetMessageOptions.options.MQC.MQGM0_WAIT` to activate waiting for a message, and specify in parameter `MQGetMessageOptions.waitInterval` a timeout in milliseconds that will be waited until an appropriate message can be received.

1. Access the MBean `X4Management`

- Start the jconsole tool.
 - Open the MBean X4Management in a domain `de.softproject.X4`
2. Invoke the MBean method `setAllOutOfService()`.
The property `OutOfService` will be set for all processes. This causes that no more processes can be started.
 3. Invoke the MBean method `stopAllProcesses()`.
All processes that are currently executed and are allowed to be stopped, will be terminated.
 4. Wait until the MBean method `runningWorkflowCount()` displays `0`.
No process is executed any longer.

 Alternatively, you can also invoke the method `shutdownAllProcesses(longtimeoutInMS)`. This causes the MBean methods `setAllOutOfService()`, `stopAllProcesses()`, and `runningWorkflowCount()` to be executed consecutively.

- In **ParamValue** specify a timeout in milliseconds, to be handed over to the method as parameter `longtimeoutInMS`.
- Click **Invoke** to execute the method. This returns *True*, if `runningWorkflowCount()` displays `0` before the timeout exceeds.

5. Shut down the X4 Server.

4.3 Providing Process Libraries

Process libraries provide an easy way to use process models for multiple users. They allow know-how to be bundled, stored centrally and to be reused in a targeted manner.

To provide process libraries the following steps are required:

1. *Installing the process library:* Place the process library as ZIP or jar file under `Server\X4DB\X4modules`.
2. *Configuring and providing the process library:* Configure and provide the process library on the Server via the file `modules.xml` (`Server\X4DB\X4modules\`).

Sample configuration via the modules.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<modules>
  <global project="MyFirstLibrary" jar="MyFirstLibrary.zip"/>
  <local  userId="1" project="MySecondLibrary" jar="MyFirstLibrary.jar"/>
</modules>
```

Explanation:

Element	Description
global	The library is provided globally and thus available for all users
local	The library is provided locally and thus available only for a certain user
userId	User who can access the library
project	Project name; The project name must correspond to the project name of the process library.
jar	Reference to the ZIP or jar file of the process library

5 High Availability

In systems with high workloads or critical services, high availability is an important part of the system landscape. With X4 BPMS, there are several scenarios for implementing high availability.

Basically, three different use cases are described: load balancing, fail over and high availability with planned process executions.

With high availability, data integrity often plays a role and must therefore be guaranteed. Thus, it is important to consider the database in the system landscape.

The load balancer is an external system component that must be set up based on the environment. It receives the external requests and forwards them to the corresponding X4 Server instance. This makes external callers independent of the underlying system landscape and allows extensions to be made without having to perform changes on client side.

5.1 Load Balancing

In the case of load balancing, the problem is caused by many simultaneous requests and their processing. More requests are to be processed simultaneously by connecting several X4 Server instances behind a load balancing system, thus achieving higher computing power. This enables a high demand-driven scalability. However, it must be ensured that the shared data of the X4 systems is known to all systems. Therefore, there are different scenarios depending on the application.

5.1.1 Scenario – Few Mainly Reading Database Accesses

If the processes contain mainly calculations or additional services are addressed, a load distribution can be realized over several X4 Servers, each of them managing its system database, and another database containing the shared data. Here, two expansion stages can be distinguished.

5.1.1.1 Simple – Direct database access

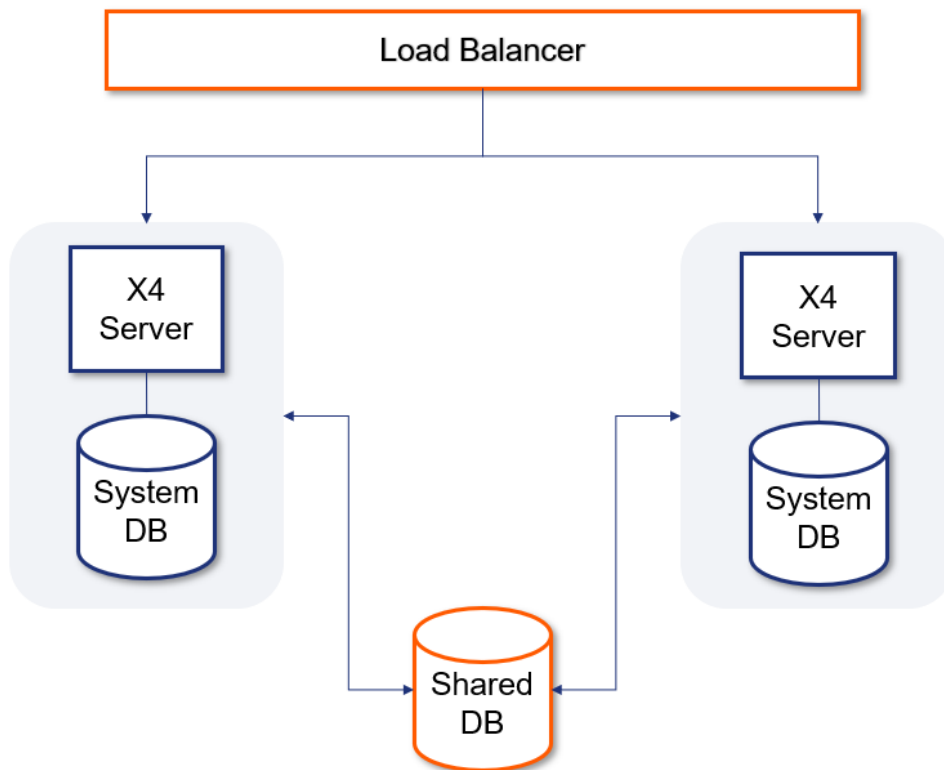


Figure: Direct database access

Access to the shared data can be managed directly via the database' access layer. This is the simplest solution to the problem and a good solution for small systems since the database itself cannot be easily decoupled.

5.1.1.2 Complex – Shared access via an X4 instance

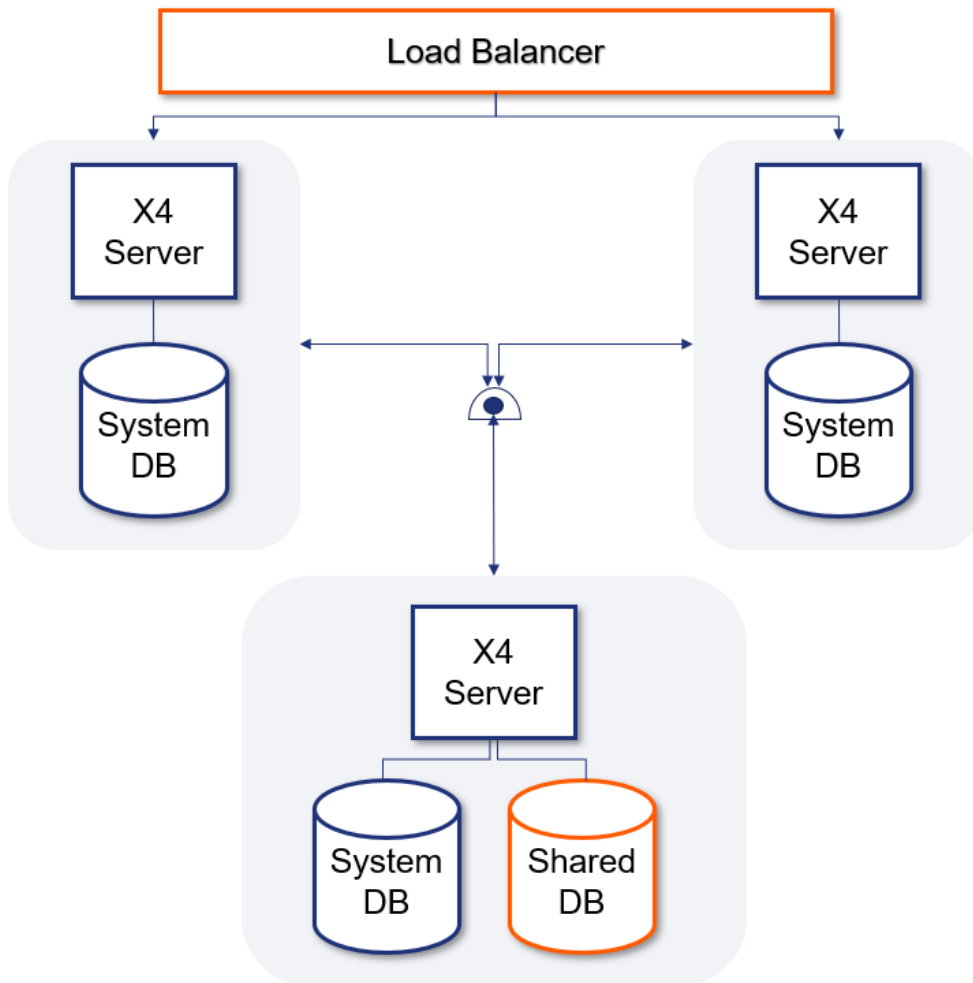


Figure: Shared database access via an X4 instance

If the database should be decoupled, it is a good idea to insert a service layer between the database and the X4 Servers. It encapsulates the common database and thus makes the data storage layer exchangeable. This is important for larger systems in order to better guarantee maintainability, testability and integrity.

5.1.2 Scenario – Shares Access via Message Queue

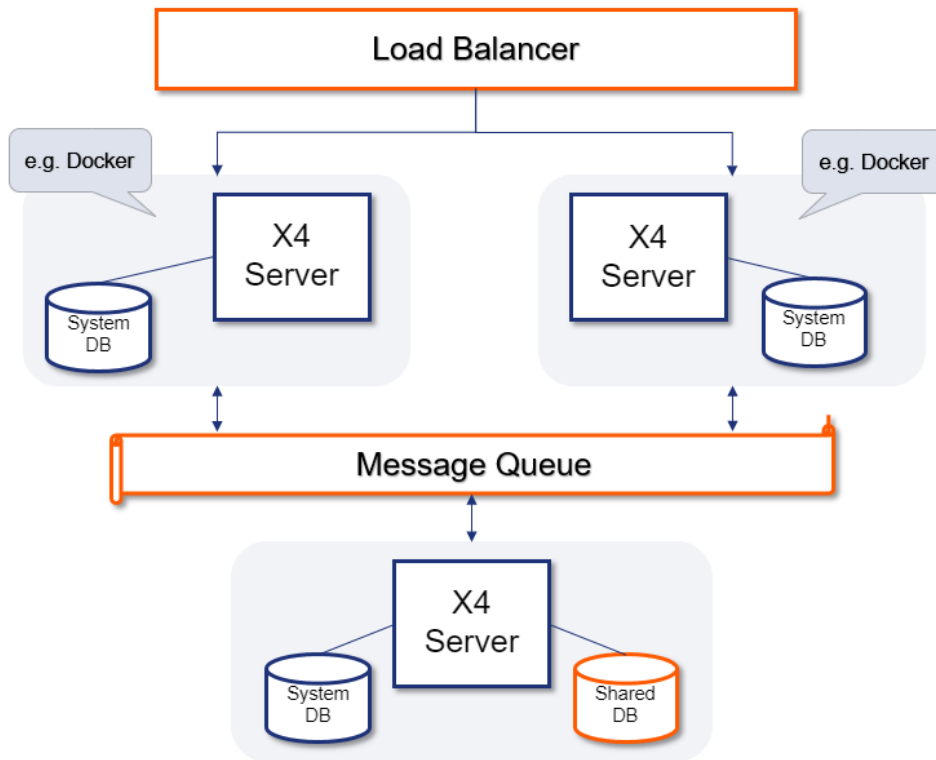


Figure: Shared database access via Message Queue

Another possibility to decouple the database is via a middleware. This is recommended for critical applications where no messages may be lost between the X4 Servers and the X4 Server of the shared database. The middleware ensures that messages are kept persistent until they have been processed by the recipient.

5.2 Fail Over

In contrast to load balancing, fail over operation requires that the system is accessible at all times. However, usually only one server is primarily used for requests. If this server fails, the second server is used and the end user does not notice the failure.

A keep-alive service ensures that the load distributor is notified if a system failure occurs. This allows to immediately switch over to the second server.

5.2.1 Scenario – A Single Exclusive Database

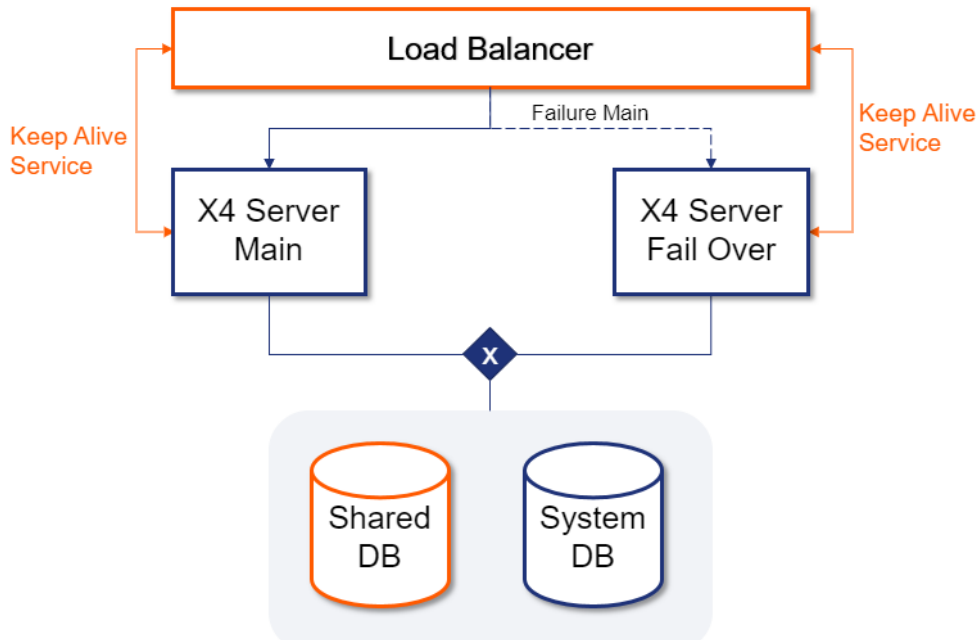


Figure: A single database with exclusive access

The simplest system contains two X4 Server instances that can receive both requests. A single database is used for both servers. Thus, for data integrity it is important that only one of the two servers has access to the database at a time.

Scheduled services can be implemented using an external scheduler or a logical lock on a table of the shared database *Shared DB*.

5.2.2 Scenario – System Database per X4 Server

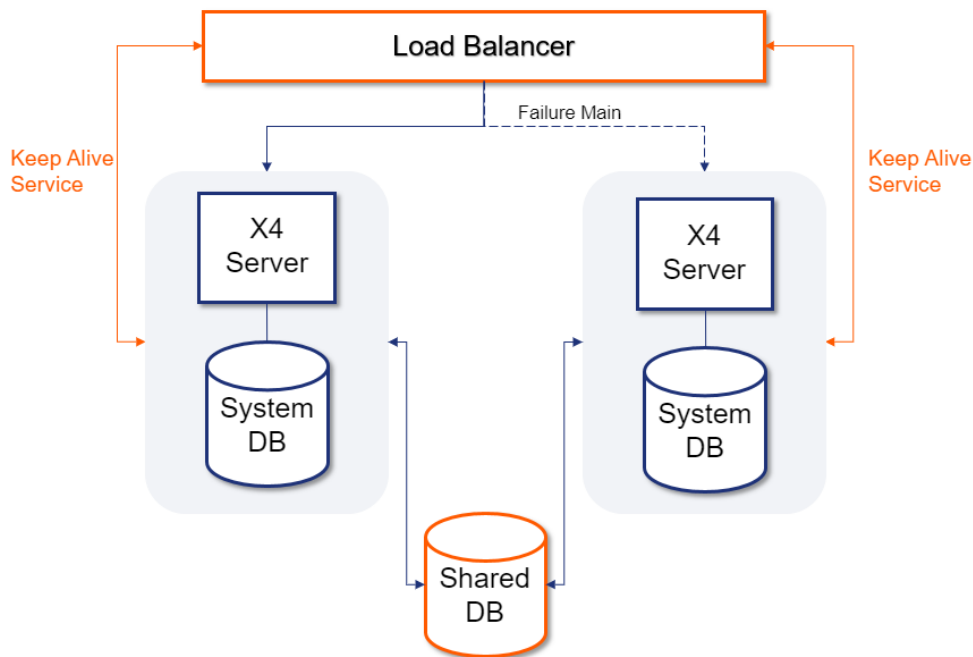


Figure: Separate system databases

If load balancing and fail over are to be provided through the system structure, each X4 Server requires its own system database. This allows each X4 Server to respond to requests. If only fail over is to be ensured, all requests are redirected to only one of the two X4 Servers.

Scheduled services can be implemented using an external scheduler or a logical lock on a table of the shared database *Shared DB*.

5.3 Load Balancing via Scheduler

If, in addition to load balancing, processes are to be started automatically via a scheduler, it must be ensured that execution is not triggered multiple times.

5.3.1 Scenario – Dedicated X4 Server for Scheduling

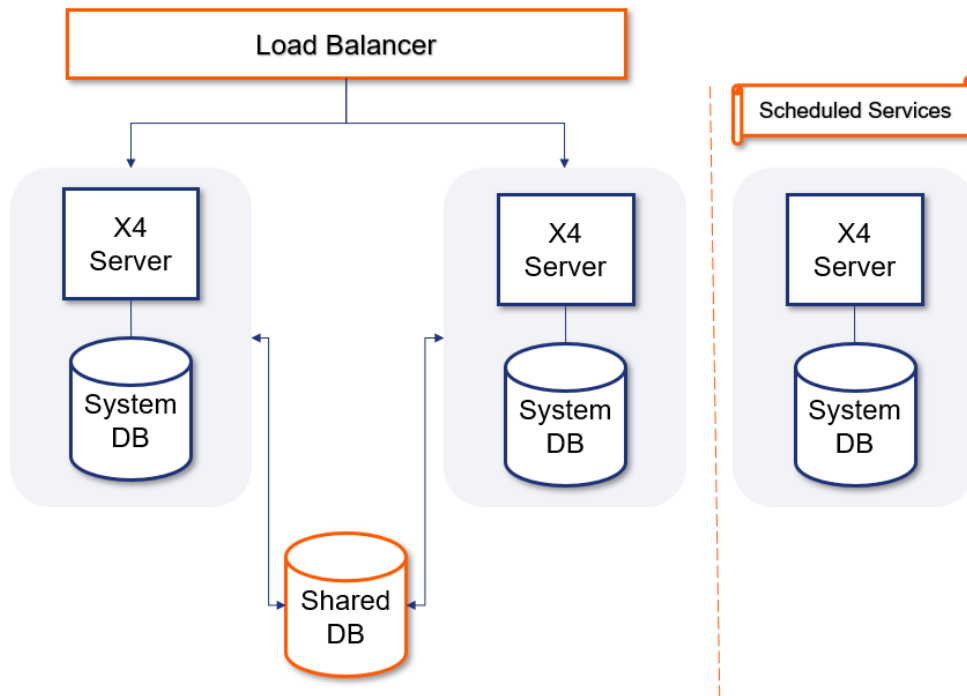


Figure: Dedicated Scheduler X4 Server

If scheduling should take place independently of the current load distribution, a dedicated X4 Server is set up containing only the automatically started processes. This X4 Server instance has the possibility to notifying the other X4 Systems via the shared database. As described in the section *Scenario – Shared Access via Message Queue*, it is also possible to exchange messages with the shared database via a message queue.

5.3.2 Scenario – One Server Responsible for Scheduling

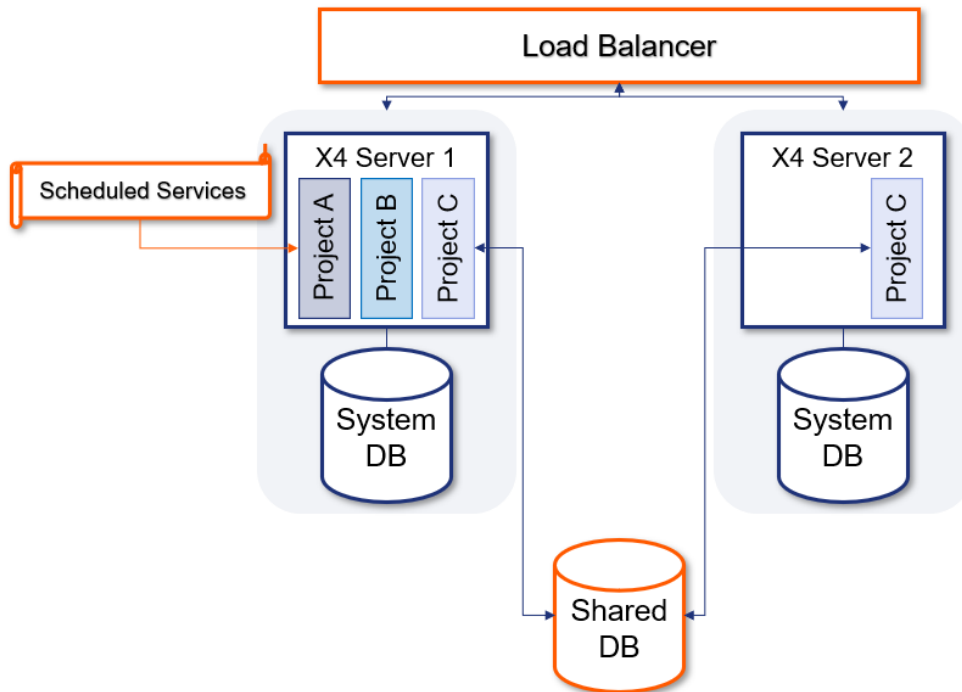


Figure: Planned processes in X4 project

If no additional X4 Server instance should be used for the automatic execution of processes, a separate project within the X4 projects can be used for these processes. This project is then installed exclusively on one of the two X4 Servers. This ensures that only this server instance executes the processes.

5.3.3 Scenario – External Scheduler

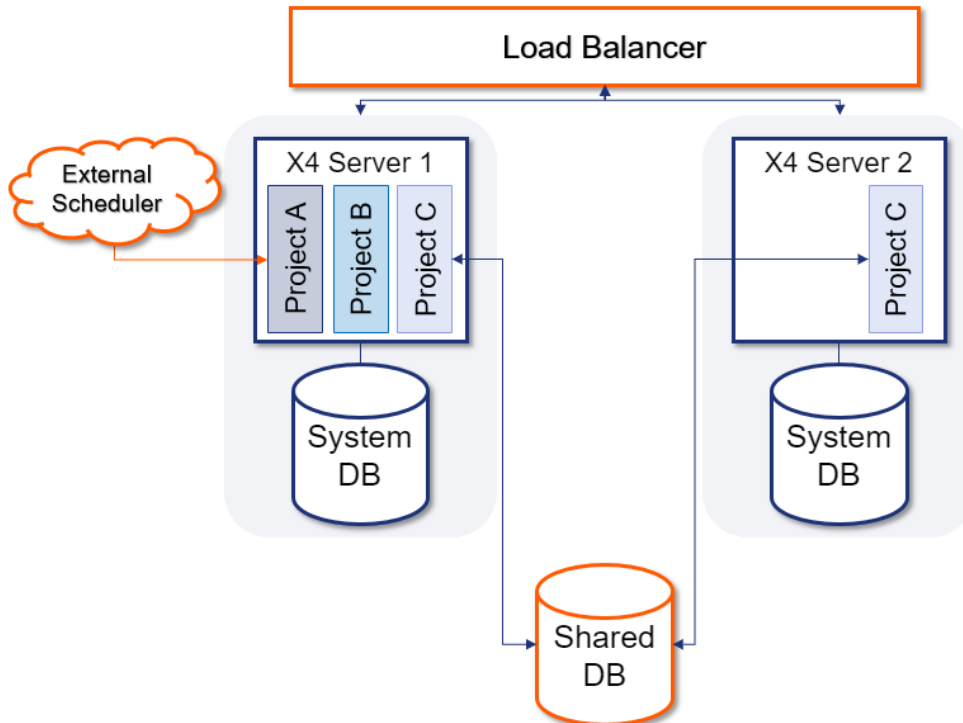


Figure: Planned processes via external scheduler service

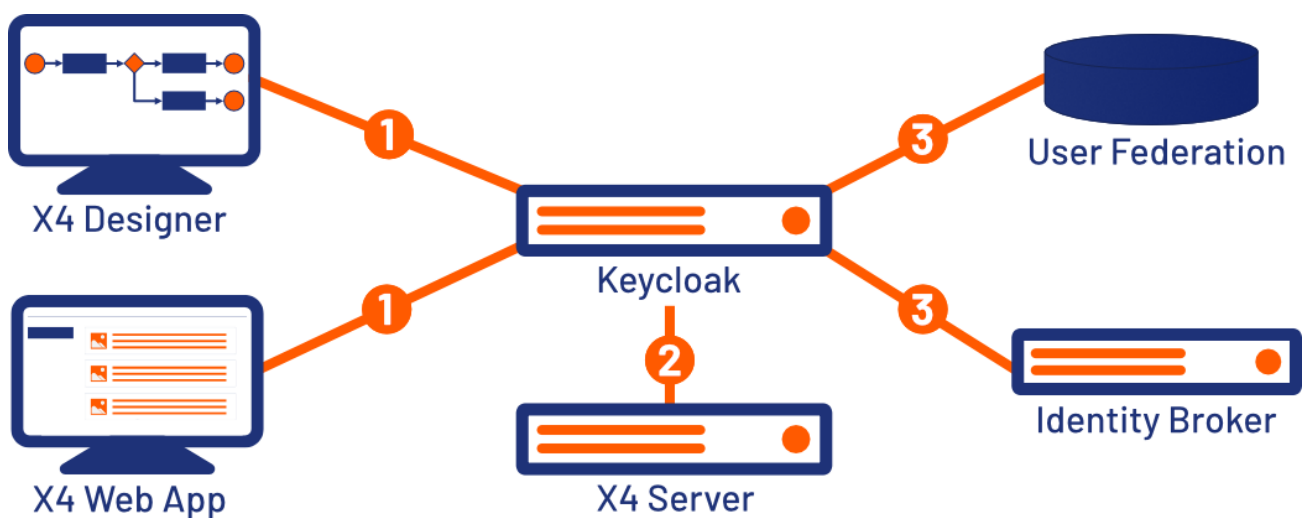
In addition to the scheduler included in the X4 Server, an external service can also start processes automatically. This service addresses the processes to be executed directly on the server on which *project A* is installed.

6 Keycloak

⚠ The authentication provider Keycloak has to be installed to use the X4 BPMS.

All components of X4 BPMS use the authentication provider Keycloak for authentication and authorization. The users, groups and roles are managed in Keycloak. The included Keycloak is already connected using a central configuration.

However, you also have the possibility of connecting existing identity providers such as LDAP or Active Directory using the included Keycloak. Keycloak also supports the integration of external providers such as Microsoft, Google or Facebook.



1	Authenticate
2	Token creation and validation
3	Connect

The Keycloak administration console can be opened via the URL <http://localhost:8085/auth/admin/>.

⚠ Potential security risk

In the test version of the X4 BPMS, a default user with administration permissions is pre-installed. The default user can be a potential security risk if the system goes live, so it is mandatory to secure the default user. Disable the default user or change the password in the Keycloak administration console.

 Keycloak**Default user**

- Username: admin
- Password: demo

Available roles

Role	Description
x4_admin_access	Gives access to the X4 ReST API.
x4_dev_access	Gives access to the X4 Designer.
x4_dev_access_*	Gives access to all X4Repositories.

 X4 Designer**Default user**

- Username: demo
- Password: demo

 X4 Web Apps**Default user**

- Username: demo
- Password: demo

The official Keycloak documentation can be accessed via the URL <https://www.keycloak.org/documentation.html>.

6.1 About the used database

Keycloak is shipped with an H2 database by default so that Keycloak can be used without further configuration. However, the H2 database is not suitable for productive operation due to security weaknesses and limited scalability. Therefore, we recommend the use of an alternative database. Before using the Keycloak productively, you should therefore connect an alternative database.

How to connect databases to Keycloak is described in the official Keycloak documentation.

- 
- For more information, visit
- https://www.keycloak.org/docs/latest/server_installation/index.html#_database
- .

6.2 Set up

6.2.1 Loading Docker image and launching container

In this section, you can find information on how to load the authentication provider Keycloak into Docker and start it as a container.

Requirements

- Docker must be installed and set up on the system. Information on this can be found in the Docker documentation at <https://docs.docker.com/>.
- Knowledge of how Docker works is assumed.

1. Load the installation package `keycloak-image.tar` provided by SoftProject onto your system using the command `docker load -i keycloak-image.tar`.
2. Run Docker with the command `docker run -d -p 8085:8085 --name keycloak softprojectgmbh/keycloak`.

6.2.2 Connecting your own Keycloak installation

If the included Keycloak installation is to be replaced by your own Keycloak installation, a Keycloak configuration file must be created in the server directory under **\configuration\keycloak_config.json**.

The configuration is done in the `connection` element.

Example

```
{
  "connection": {
    "realm": "X4Realm",
    "auth-server-url": "http://<host>:<port>/auth/",
    "resource": "X4",
    "credentials": {
      "secret": "XXXX"
    }
  },
  "rest-api-credentials": {
    "user": "username",
    "password": "password"
  }
}
```

The following roles must be created in Keycloak:

Role	Description
x4_admin_access	Gives access to the X4 ReST API.
x4_dev_access	Gives access to the X4 Designer.
x4_dev_access_*	Gives access to all X4Repositories.

To use the X4 ReST API, the following rights must be granted to the corresponding user:

Client Roles	• realm-management
Assigned Roles	• manage-users • view-users

System 

Details Attributes Credentials **Role Mappings** Groups Consents Sessions

Realm Roles

Available Roles ⓘ

x4_admin_access
x4_dev_access

Add selected >

Assigned Roles ⓘ

default-roles-x4realm

« Remove selected

Effective Roles ⓘ

default-roles-x4realm
offline_access
uma_authorization

Client Roles

realm-management

Available Roles ⓘ

create-client
impersonation
manage-authorization
manage-clients
manage-events

Add selected >

Assigned Roles ⓘ

manage-users
view-users

« Remove selected

Effective Roles ⓘ

manage-users
query-groups
query-users
view-users

✓ For more information on the configuration file, see https://www.keycloak.org/docs/latest/securing_apps/index.html#_java_adapter_config.

6.3 Configure

6.3.1 Applying Authorization Code Flow

The X4 BPMS supports different authorization code flows and the single sign-on authentication procedure. To apply the authorization code flows for X4 Web Apps, you must enter the path to the Web App in **Valid Redirect URIs** in the **Client** section of the Keycloak administration console.

Authorization Enabled  ☒ ON

Root URL 

* Valid Redirect URIs   

✓ For more information, see Configuration.

6.3.2 Restricting access to X4 repository

Access to individual workspaces can be restricted using roles. To do this, a new role with the name **x4_dev_access_<workspace name>** has to be created in the Keycloak Administrator console. The link to the workspace is established using the role name.

6.3.2.1 Sample

To restrict workspace **2** using a role, the **x4_dev_access_2** role is created in Keycloak. Only users assigned to the **x4_dev_access_2** role have access to the workspace.

6.3.3 Default configuration

This section describes the default configuration of the authentication provider in the delivery state.

6.3.3.1 Realm Settings

General

Label	Value
Name	X4Realm
Enabled	ON

Login

Label	Value
User registration	OFF
Edit username	OFF
Forgot password	OFF
Remember Me	OFF
Verify email	OFF
Login with email	ON
Require SSL	external requests

Tokens

Label	Value
Default Signature Algorithm	RS256
Revoke Refresh Token	OFF
SSO Session Idle	30 Minutes
SSO Session Max	10 Hours
SSO Session Idle Remember Me	0 Minutes
SSO Session Max Remember Me	0 Minutes
Offline Session Idle	30 Days
Offline Session Max Limited	OFF
Client Session Idle	0 Minutes
Client Session Max	0 Minutes
Access Token Lifespan	5 Minutes
Access Token Lifespan For Implicit Flow	15 Minutes
Client login timeout	1 Minutes
Login timeout	30 Minutes
Login action timeout	5 Minutes
User-Initiated Action Lifespan	5 Minutes
Default Admin-Initiated Action Lifespan	12 Hours
OAuth 2.0 Device Code Lifespan	10 Minutes
OAuth 2.0 Device Polling Interval	5

Security Defenses

Label	Value
X-Frame-Options	SAMEORIGIN
Content-Security-Policy	frame-src 'self'; frame-ancestors 'self'; object-src 'none';
X-Content-Type-Options	nosniff
X-Robots-Tag	none
X-XSS-Protection	1; mode=block
HTTP Strict Transport Security (HSTS)	max-age=31536000; includeSubDomains

6.3.3.2 Clients

Settings

Label	Value
Client ID	X4
Name	X4

Description	X4
Enabled	ON
Always Display in Console	OFF
Consent Required	OFF
Client Protocol	openid-connect
Access Type	confidential
Standard Flow Enabled	ON
Implicit Flow Enabled	OFF
Direct Access Grants Enabled	ON
Service Accounts Enabled	ON
OAuth 2.0 Device Authorization Grant Enabled	OFF
OIDC CIBA Grant Enabled	OFF
Authorization Enabled	ON
Root URL	http://localhost:8080/X4
Valid Redirect URIs	/*
Backchannel Logout Session Required	ON
Backchannel Logout Revoke Offline Sessions	OFF

Fine Grain OpenID Connect Configuration

Label	Value
User Info Signed Response Algorithm	unsigned
Request Object Signature Algorithm	any
Request Object Encryption Algorithm	any
Request Object Content Encryption Algorithm	any
Request Object Required	not required

OpenID Connect Compatibility Modes

Label	Value
Exclude Session State From Authentication Response	OFF
Use Refresh Tokens	ON
Use Refresh Tokens For Client Credentials Grant	OFF

Advanced Settings

Label	Value
OAuth 2.0 Mutual TLS Certificate Bound Access Tokens Enabled	OFF
Pushed Authorization Request Enabled	OFF

Credentials

Label	Value
Client Authenticator	Client Id and Secret

Client Scopes

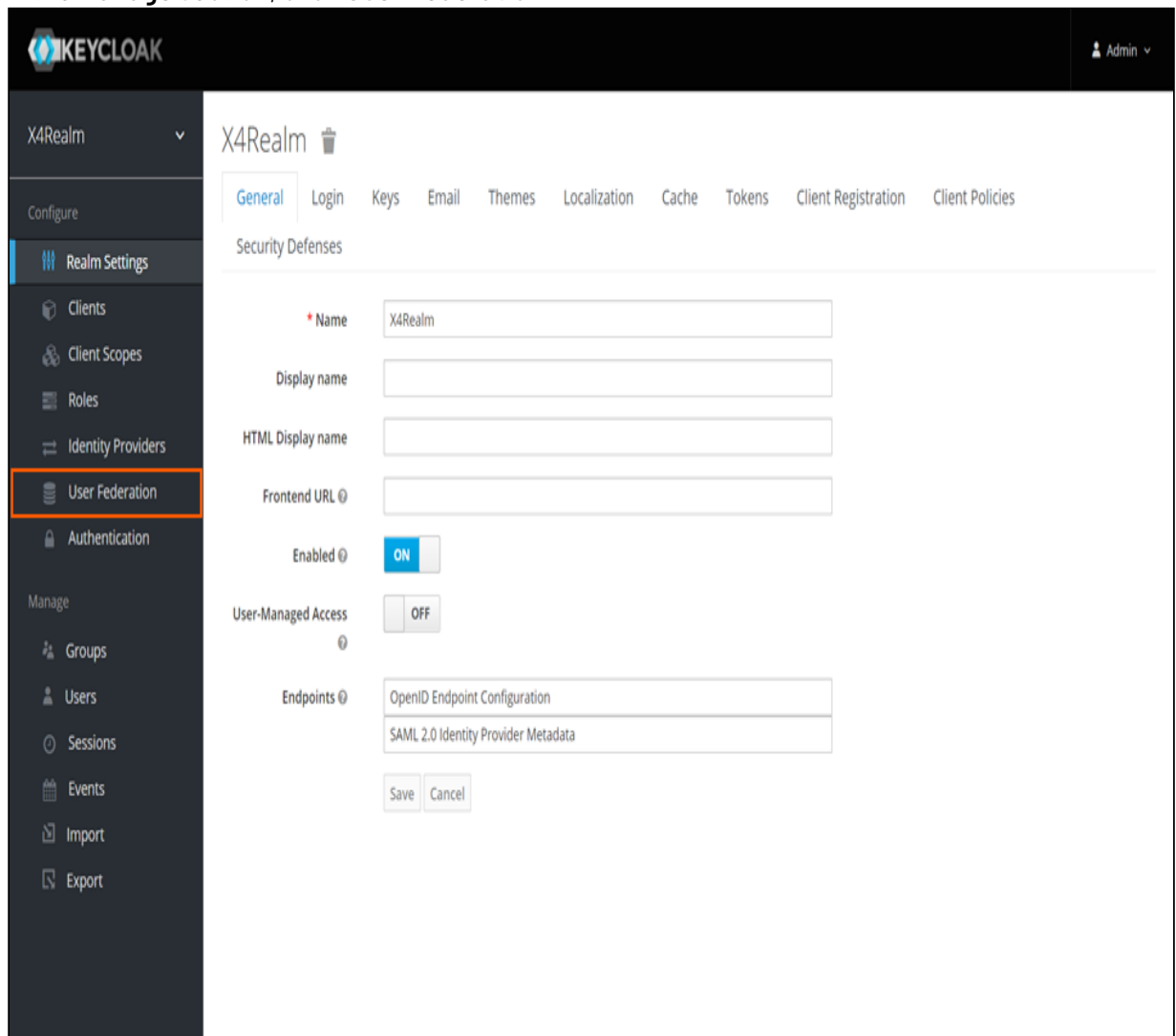
Label	Value
Assigned Default Client Scopes	• email • profile • roles • web-origins
Assigned Optional Client Scopes	• address • microprofile-jwt • offline_access • phone

6.3.4 Connect LDAP

In Keycloak you can connect an existing LDAP. Keycloak has a built-in LDAP/AD provider. It is possible to connect several different LDAP servers to the same Keycloak realm.

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **User Federation**.

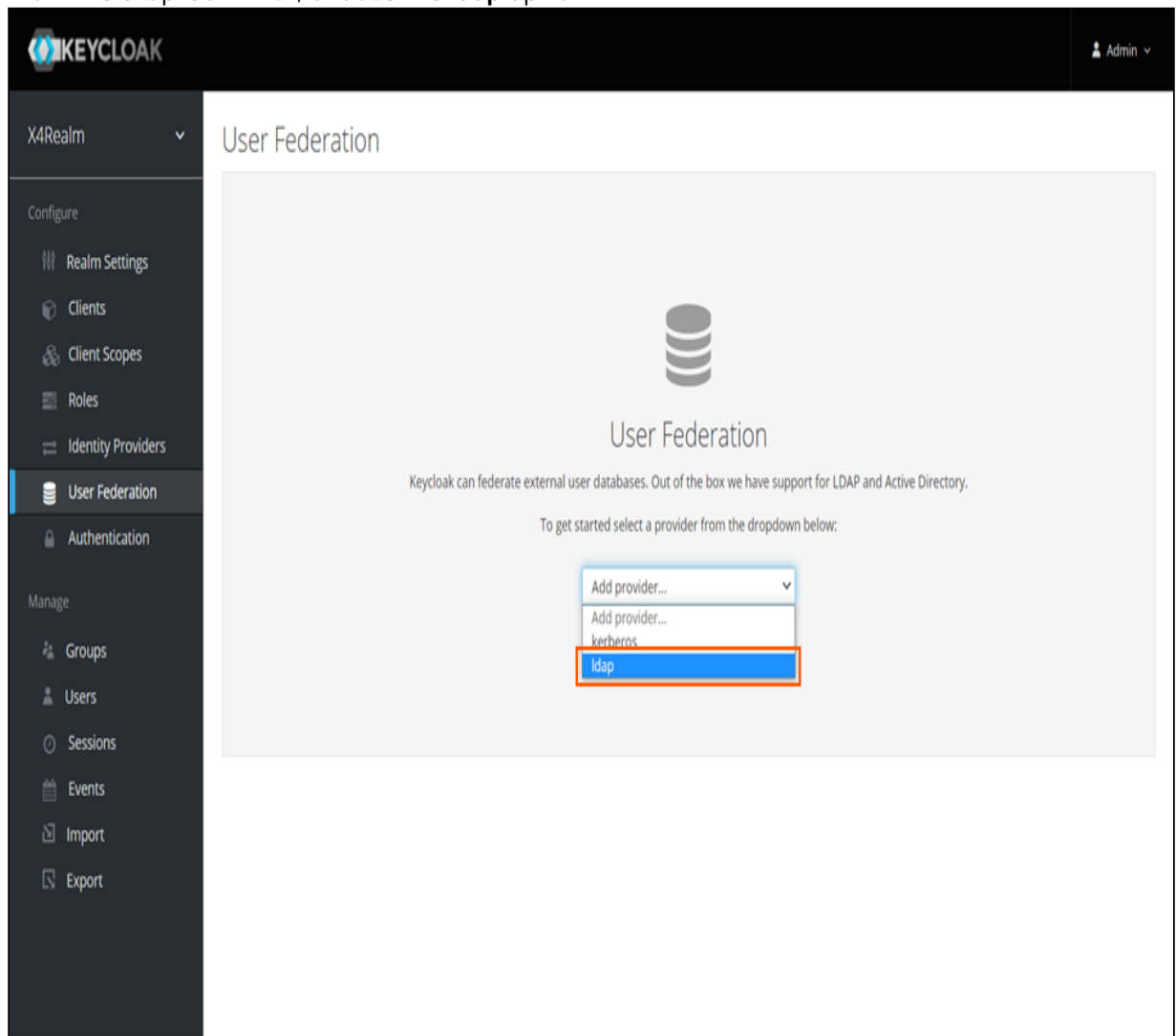


The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the Keycloak logo and the user 'Admin'. The left sidebar contains the 'Manage' section with various options, including 'User Federation', which is highlighted with an orange border. The main content area shows the 'X4Realm' configuration page, specifically the 'General' tab under 'Security Defenses'. The configuration fields include:

- Name:** X4Realm
- Display name:** (empty field)
- HTML Display name:** (empty field)
- Frontend URL:** (empty field)
- Enabled:** ON (toggle switch)
- User-Managed Access:** OFF (toggle switch)
- Endpoints:** OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

3. From the drop-down list, choose the **ldap** option.



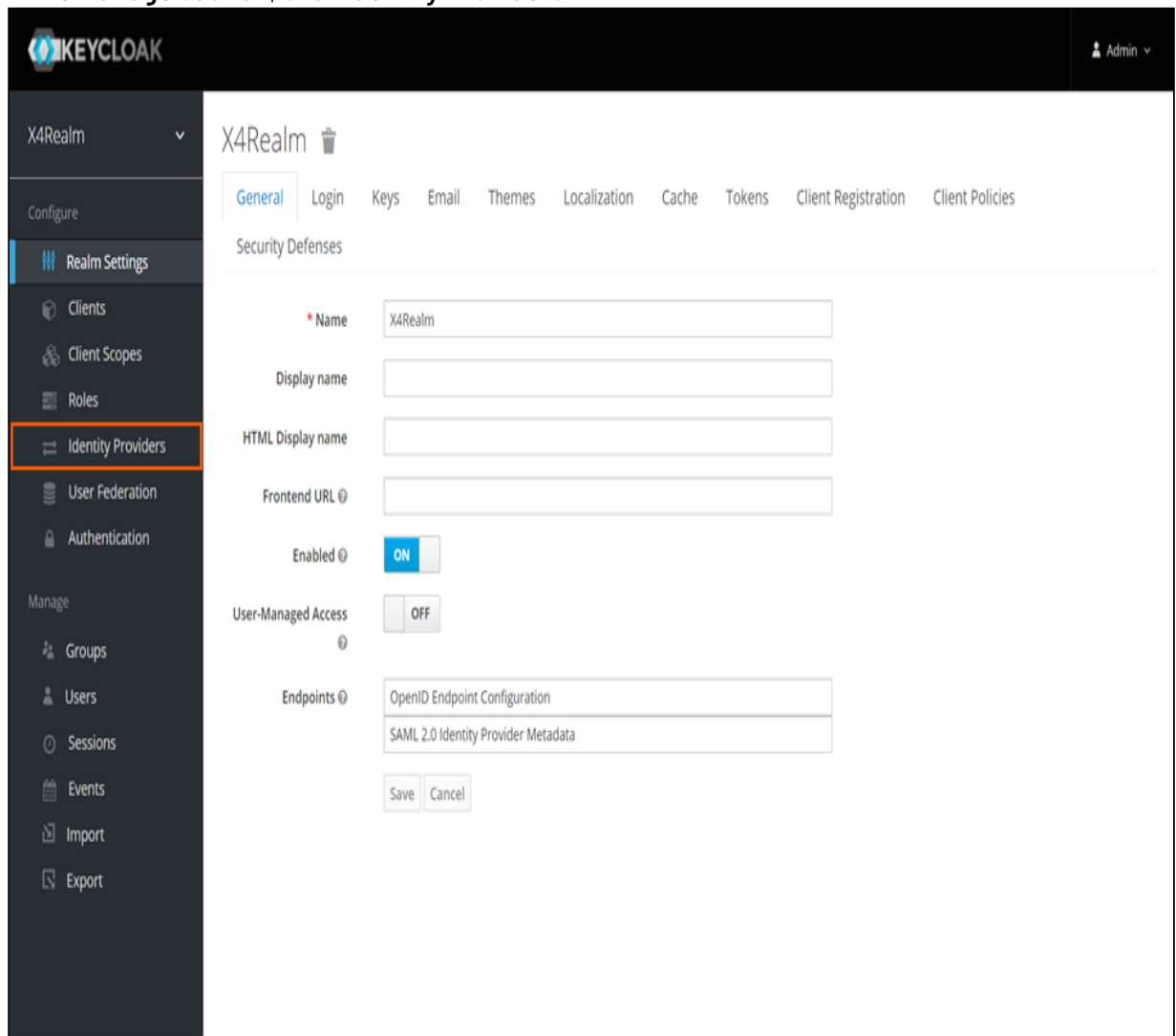
✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#_ldap.

6.3.5 Connect SAML v2.0

In Keycloak, you can connect an existing SAML v2.0. Keycloak can broker identity providers based on the SAML v2.0 protocol.

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **Identity Providers**.

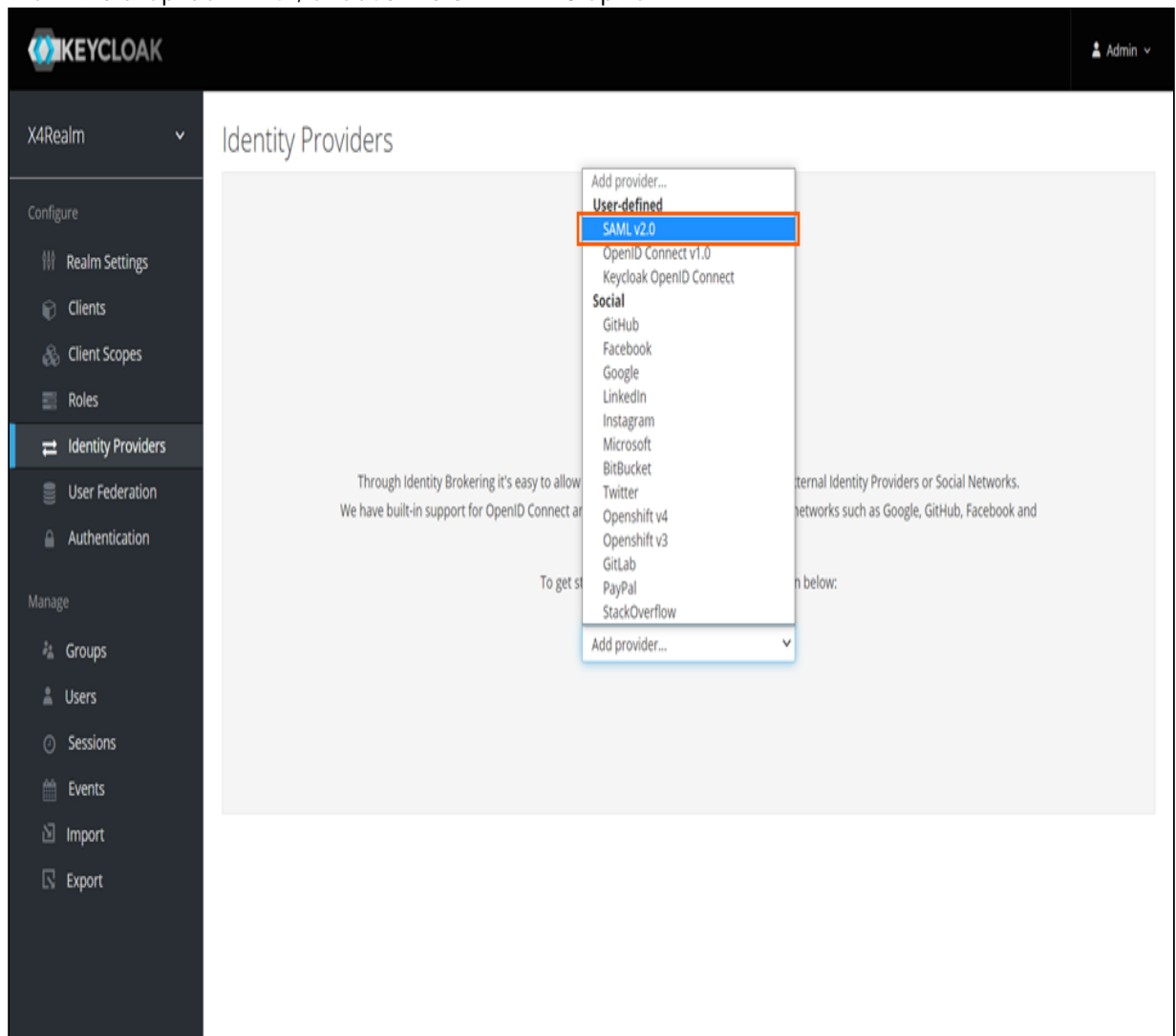


The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the Keycloak logo and the user 'Admin'. The left sidebar contains the 'Manage' section with 'Identity Providers' highlighted. The main content area shows the 'X4Realm' configuration page with tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, showing the 'Security Defenses' section. The configuration fields include:

- Name**: X4Realm
- Display name**: (empty)
- HTML Display name**: (empty)
- Frontend URL**: (empty)
- Enabled**: ON
- User-Managed Access**: OFF
- Endpoints**: OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

At the bottom of the configuration section are 'Save' and 'Cancel' buttons.

3. From the drop-down list, choose the **SAML v2.0** option.



✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#saml-v2-0-identity-providers.

6.3.6 Connect Kerberos

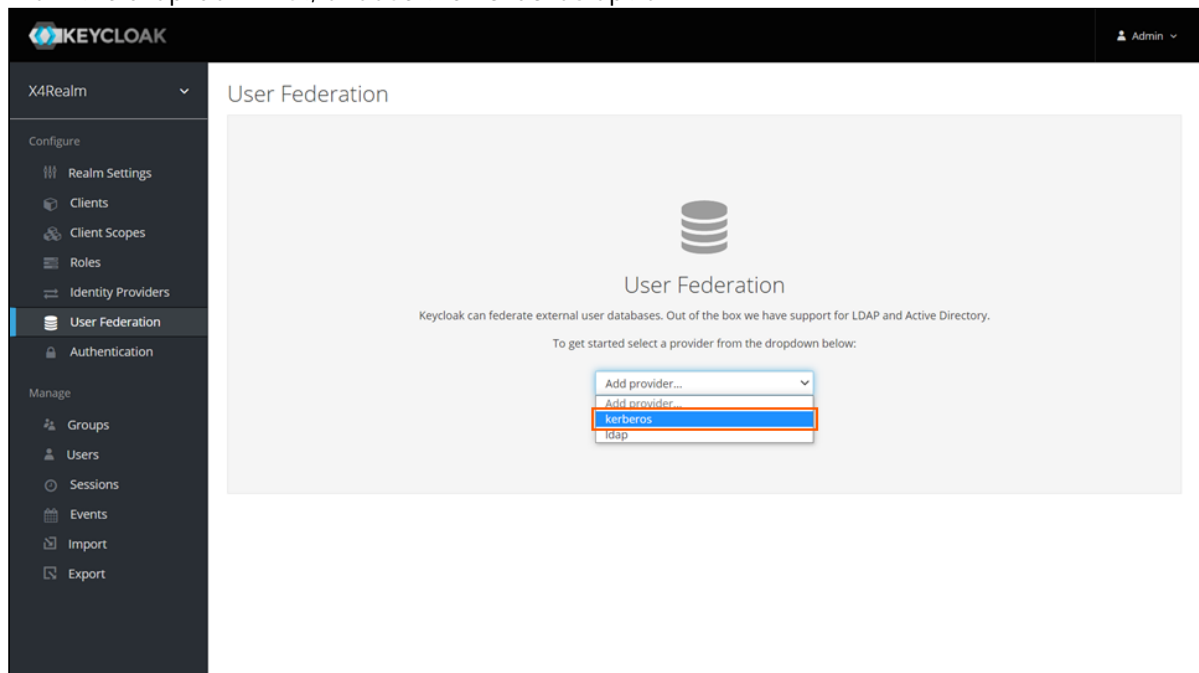
In Keycloak, you can connect an existing Kerberos. Keycloak supports logging in with a Kerberos ticket using the SPNEGO protocol.

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **User Federation**.

The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the Keycloak logo and the user 'Admin'. The left sidebar contains the 'Manage' section with various options, including 'User Federation', which is highlighted with an orange border. The main content area is titled 'X4Realm' and features a tabbed interface with 'General' selected. Below the tabs, the 'Security Defenses' section is visible, containing several configuration fields: 'Name' (set to 'X4Realm'), 'Display name', 'HTML Display name', 'Frontend URL', 'Enabled' (toggle set to 'ON'), 'User-Managed Access' (toggle set to 'OFF'), and 'Endpoints' (listing 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'). At the bottom of the form are 'Save' and 'Cancel' buttons.

3. From the drop-down list, choose the **kerberos** option.



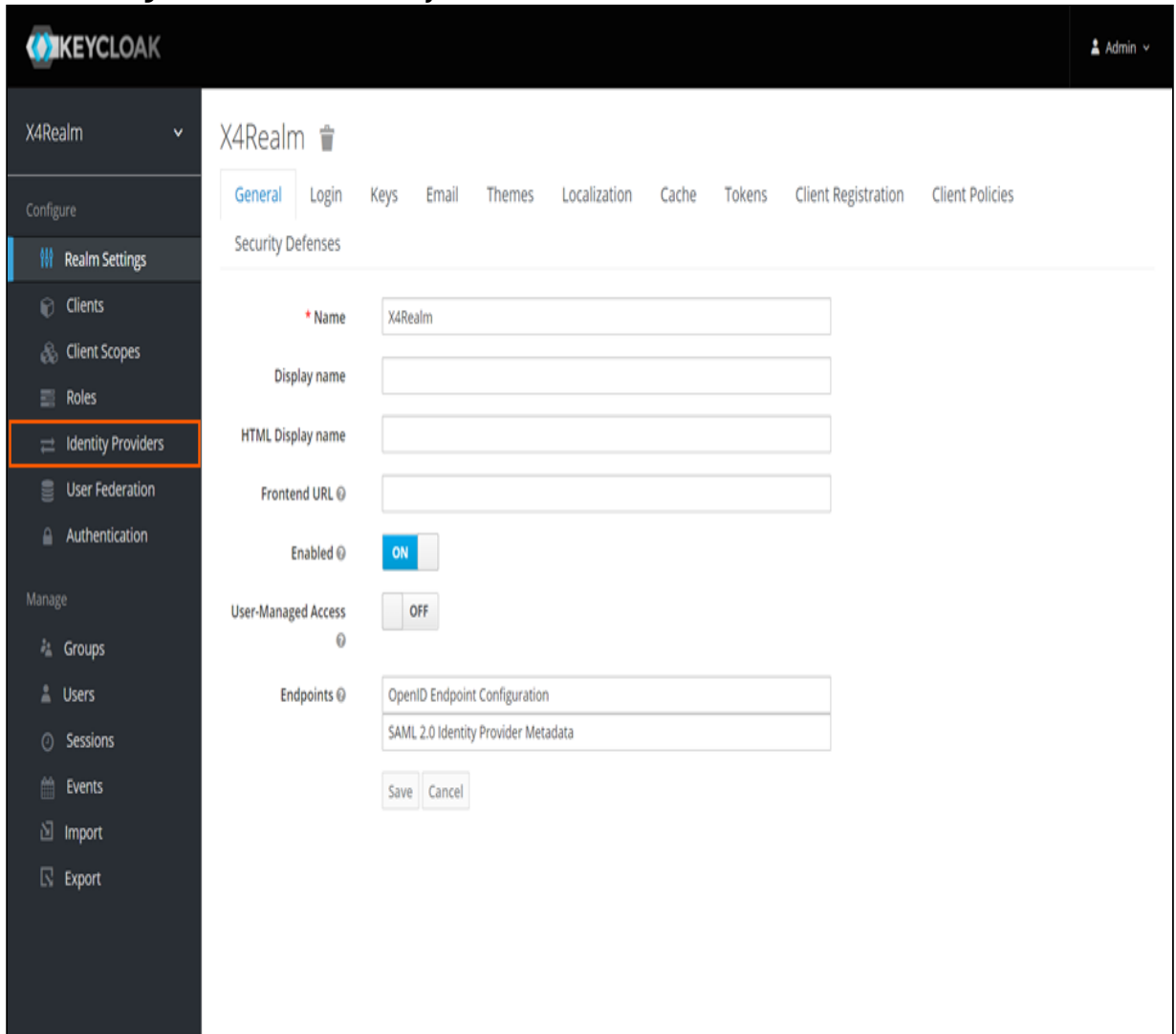
- ✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#_kerberos.

6.3.7 Connect social identity providers

In Keycloak, you can connect to various social identity providers. Keycloak provides built-in support for the most popular social networks, such as Google, Facebook, Twitter, GitHub, LinkedIn, Microsoft, and Stack Overflow.

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **Identity Providers**.



The screenshot shows the Keycloak Administration Console interface. The left sidebar contains a navigation menu with the following items: X4Realm (selected), Configure, Realm Settings (highlighted with a blue bar), Clients, Client Scopes, Roles, Identity Providers (highlighted with an orange box), User Federation, Authentication, Manage, Groups, Users, Sessions, Events, Import, and Export. The main content area is titled 'X4Realm' and features a 'Security Defenses' section. This section includes a 'General' tab (selected) and sub-tabs for Login, Keys, Email, Themes, Localization, Cache, Tokens, Client Registration, and Client Policies. The 'General' tab contains the following fields: Name (X4Realm), Display name, HTML Display name, Frontend URL, Enabled (ON), User-Managed Access (OFF), and Endpoints (OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata). At the bottom of the form are 'Save' and 'Cancel' buttons.

3. Select the desired social identity provider from the drop-down list.

✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#social-identity-providers.

6.3.8 Connect OpenID Connect

In Keycloak, you can connect to an existing OpenID Connect provider. The identity provider has to support the Authorization Code Flow to authenticate the user and authorize access.

1. Open the **Keycloak Administration Console**.

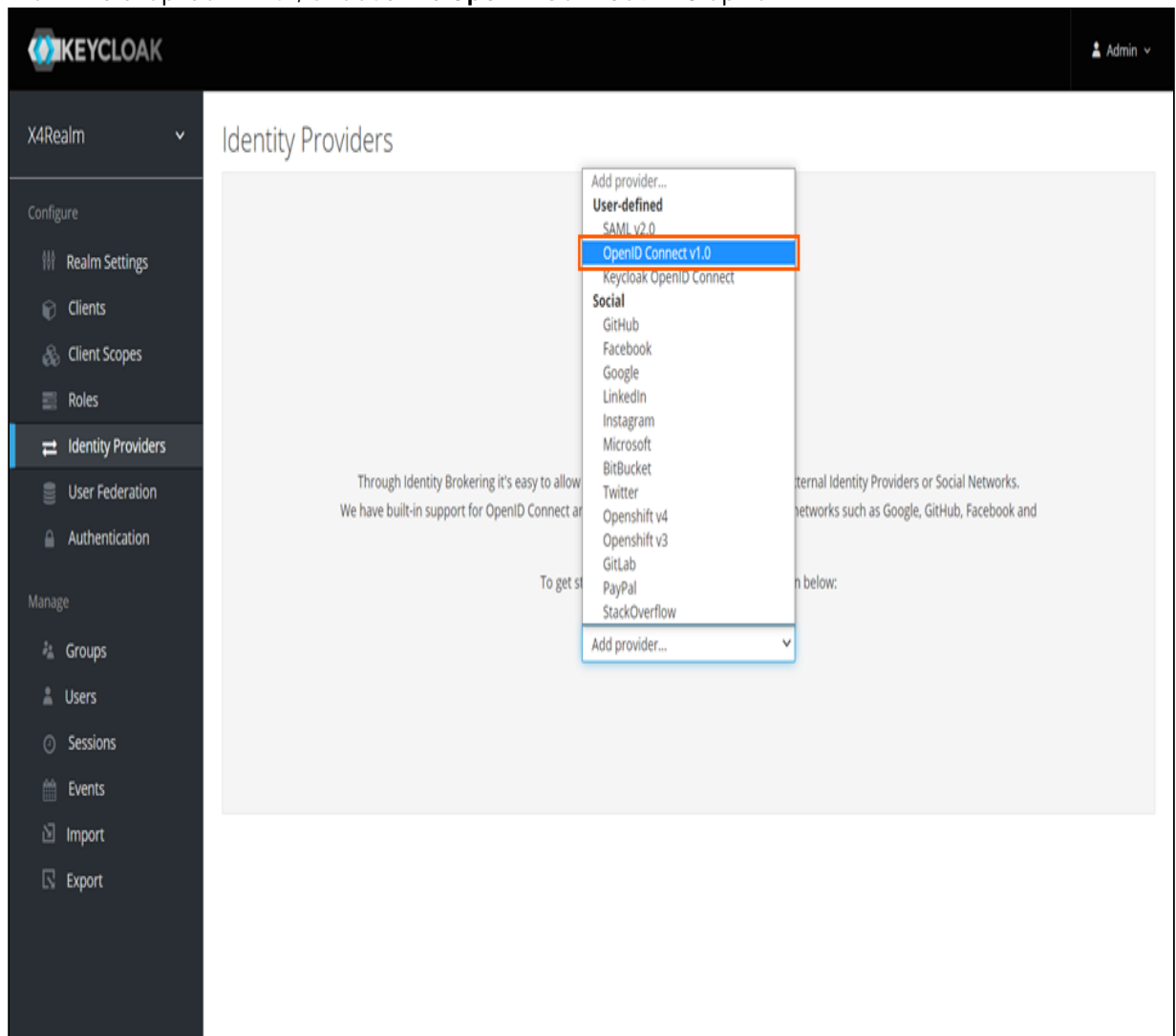
2. In the **Manage** section, click **Identity Providers**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar contains a 'Manage' section with 'Identity Providers' highlighted. The main content area is titled 'X4Realm' and shows the 'General' tab under 'Security Defenses'. The configuration fields are as follows:

Field	Value
Name	X4Realm
Display name	
HTML Display name	
Frontend URL	
Enabled	ON
User-Managed Access	OFF
Endpoints	OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

At the bottom of the form are 'Save' and 'Cancel' buttons.

3. From the drop-down list, choose the **OpenID Connect v1.0** option.



✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#_identity_broker_oidc.

6.3.9 Login page

6.3.9.1 Remember Me button

The Remember Me button can be enabled in the Keycloak Administration Console in the Realm Settings menu.

1. Open the **Keycloak Administration Console**.

2. In the **Configure** section, click **Realm Settings**.

The screenshot displays the Keycloak Admin Console interface. At the top, the Keycloak logo is on the left, and the user 'Admin' is on the right. The left sidebar contains a 'Configure' section with 'Realm Settings' highlighted. Below it are 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. The 'Manage' section includes 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The main content area is titled 'X4Realm' and features tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, showing 'Security Defenses' settings. These include: 'Name' (X4Realm), 'Display name' (empty), 'HTML Display name' (empty), 'Frontend URL' (empty), 'Enabled' (ON), 'User-Managed Access' (OFF), and 'Endpoints' (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK

Admin

X4Realm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

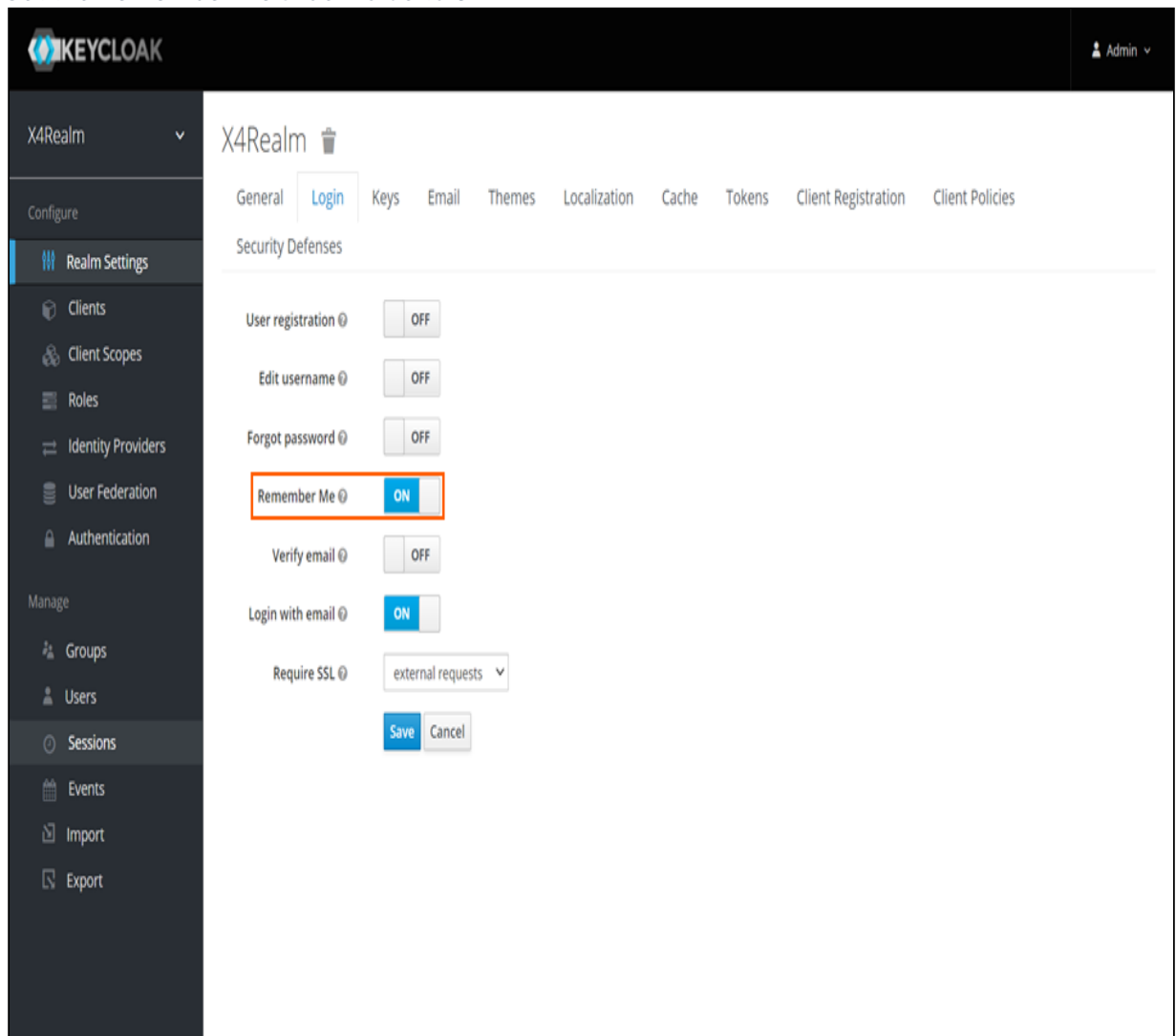
Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Save Cancel

3. Switch to the **Login** tab.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The 'Login' tab is selected and highlighted with a red box. The left sidebar contains a navigation menu with categories like 'Configure', 'Manage', and 'Authentication'. The main content area is titled 'X4Realm' and includes a trash icon. Below the title is a horizontal tab bar with 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'Login' tab is active. The 'Security Defenses' section contains several form fields: 'Name' (set to 'X4Realm'), 'Display name', 'HTML Display name', and 'Frontend URL'. There are also toggle switches for 'Enabled' (set to 'ON') and 'User-Managed Access' (set to 'OFF'). The 'Endpoints' section lists 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. At the bottom of the form are 'Save' and 'Cancel' buttons.

4. Set the **Remember Me** slider value to **ON**.



5. Click **Save**.

6.3.9.2 Create Forgot Password button

The Forgot Password button can be enabled in the Keycloak Administration Console in the Realm Settings menu.

1. Open the **Keycloak Administration Console**.

2. In the **Configure** section, click **Realm Settings**.

The screenshot displays the Keycloak Admin Console interface. At the top, the Keycloak logo is on the left, and the user 'Admin' is on the right. The left sidebar shows the 'Configure' section with 'Realm Settings' highlighted. The main content area is titled 'X4Realm' and contains tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, showing 'Security Defenses' settings. These settings include: 'Name' (X4Realm), 'Display name' (empty), 'HTML Display name' (empty), 'Frontend URL' (empty), 'Enabled' (ON), 'User-Managed Access' (OFF), and 'Endpoints' (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK

Admin

X4Realm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

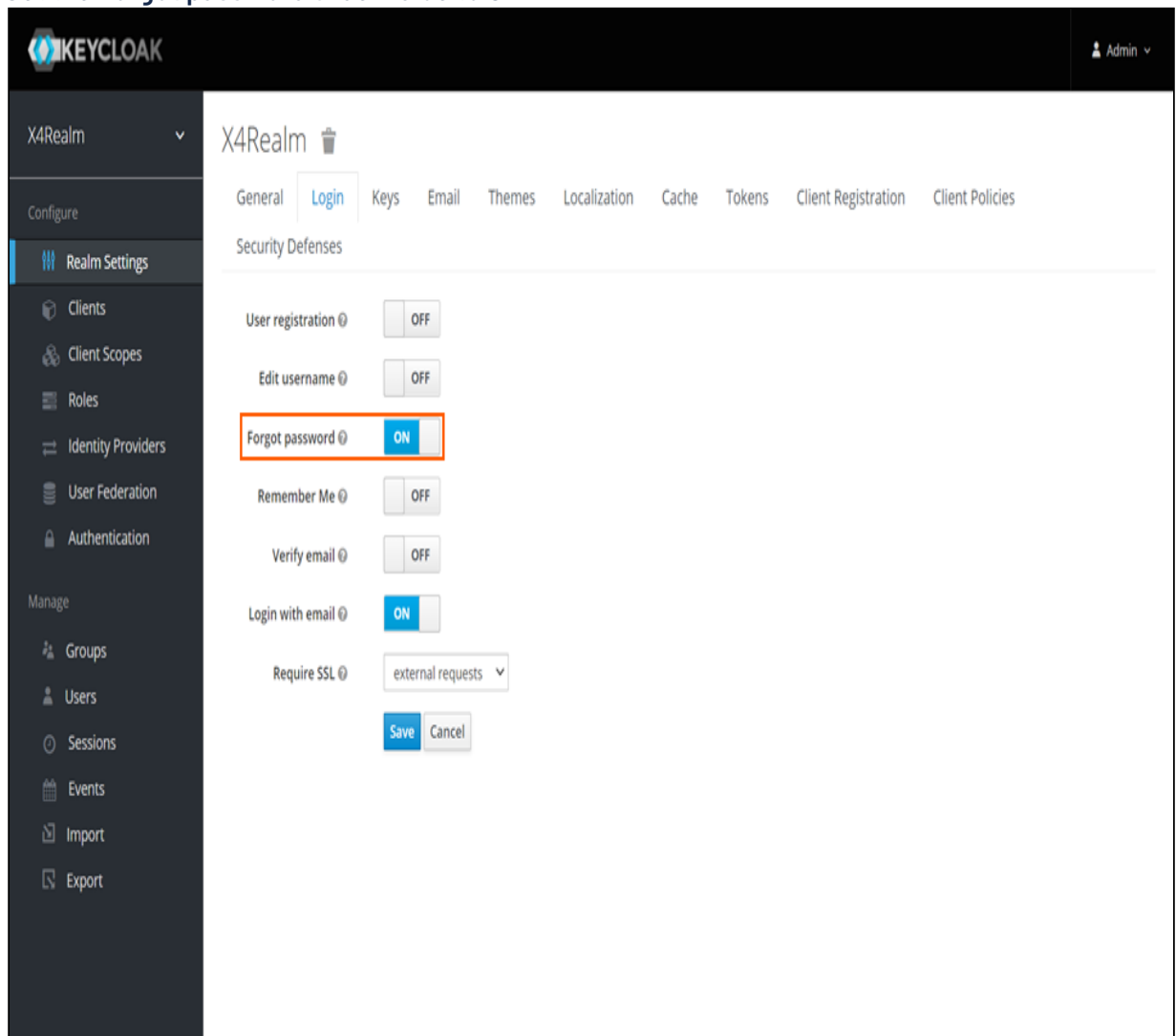
Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Save Cancel

3. Switch to the **Login** tab.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The 'Login' tab is selected and highlighted with a red box. The left sidebar contains a navigation menu with categories like 'Configure', 'Realm Settings', and 'Manage'. The main content area is titled 'X4Realm' and includes a trash icon. Below the title is a horizontal tab bar with 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'Login' tab is active. The 'Security Defenses' section contains several form fields: 'Name' (pre-filled with 'X4Realm'), 'Display name', 'HTML Display name', and 'Frontend URL'. There are also toggle switches for 'Enabled' (set to 'ON') and 'User-Managed Access' (set to 'OFF'). The 'Endpoints' section lists 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. At the bottom of the form are 'Save' and 'Cancel' buttons.

4. Set the **Forgot password** slider value to **ON**.



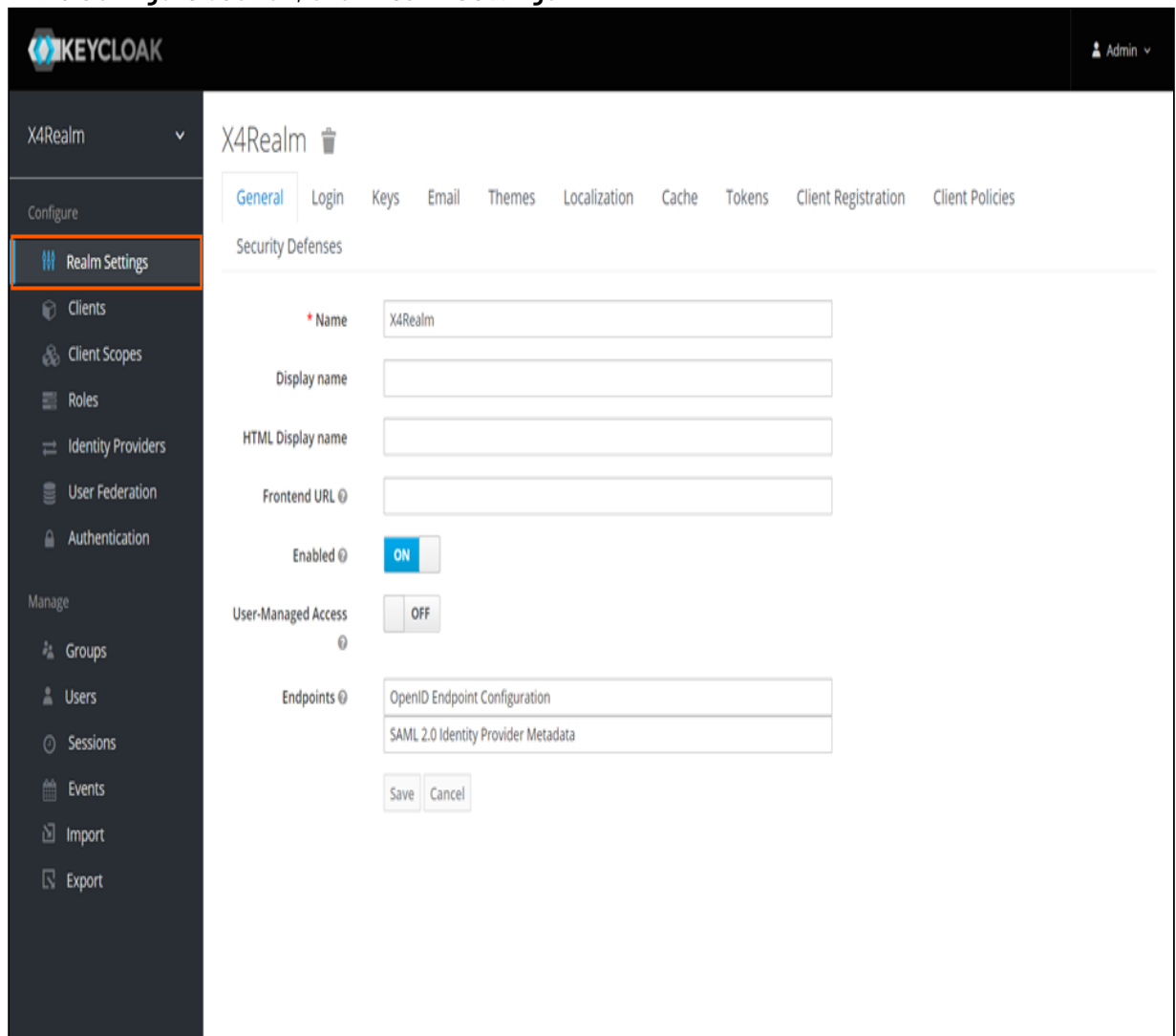
5. Click **Save**.

6.3.9.3 Activate user registration

The Register button can be enabled in the Keycloak Administration Console in the Realm Settings menu.

1. Open the **Keycloak Administration Console**.

2. In the **Configure** section, click **Realm Settings**.



The screenshot displays the Keycloak Admin Console interface. The top navigation bar includes the Keycloak logo and a user profile dropdown labeled 'Admin'. The left sidebar shows the 'Configure' section with 'Realm Settings' highlighted. The main content area is titled 'X4Realm' and contains tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, showing the 'Security Defenses' section. This section includes fields for 'Name' (X4Realm), 'Display name', 'HTML Display name', and 'Frontend URL'. There are also toggle switches for 'Enabled' (ON) and 'User-Managed Access' (OFF). At the bottom, there are 'Endpoints' for 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata', along with 'Save' and 'Cancel' buttons.

KEYCLOAK

Admin

X4Realm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

Endpoints

OpenID Endpoint Configuration

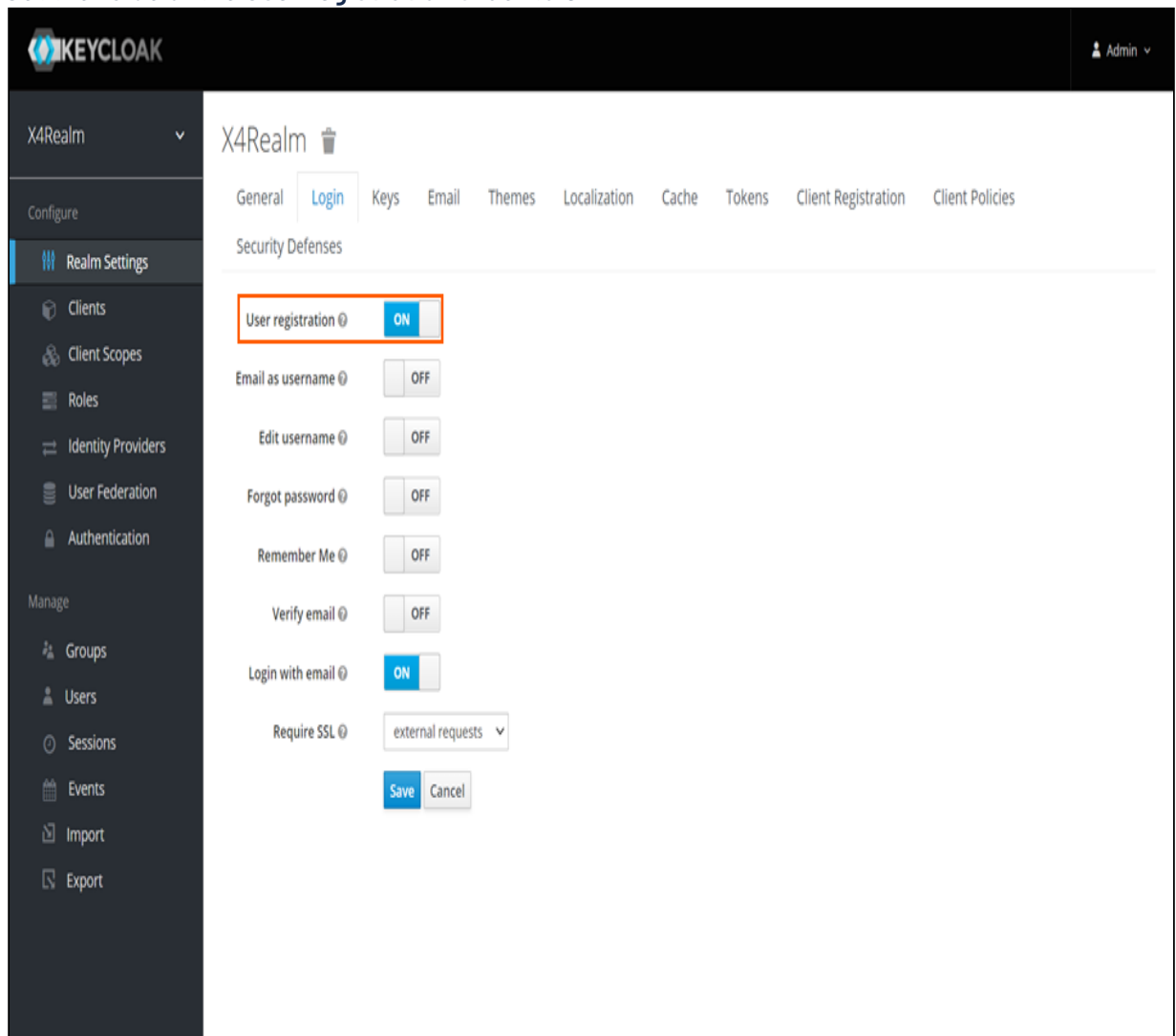
SAML 2.0 Identity Provider Metadata

Save Cancel

3. Switch to the **Login** tab.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The 'Login' tab is selected and highlighted with a red box. The left sidebar contains a navigation menu with categories like 'Configure', 'Manage', and 'Authentication'. The main content area is titled 'X4Realm' and includes a trash icon. Below the title is a horizontal tab bar with 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'Login' tab is active. The 'Security Defenses' section contains several form fields: 'Name' (set to 'X4Realm'), 'Display name', 'HTML Display name', and 'Frontend URL'. There are also toggle switches for 'Enabled' (set to 'ON') and 'User-Managed Access' (set to 'OFF'). The 'Endpoints' section lists 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. At the bottom of the form are 'Save' and 'Cancel' buttons.

4. Set the value of the **User registration** slider to **ON**.



The **Email as username** slider will appear.

5. If the email used for registration is to be used as the username, set the value of the **Email as username** slider to **ON**.
6. Click **Save**.

6.3.10 Passwords

In Keycloak you can define various settings for passwords, for instance, password policies.

6.3.10.1 Set password policies

In Keycloak you can set different password policies.

1. Open the **Keycloak Administration Console**.

2. In the **Configure** section, click **Authentication**.

The screenshot displays the Keycloak Administration Console interface. The top navigation bar shows the Keycloak logo and the user 'Admin'. The left sidebar contains the 'Configure' section with 'Authentication' highlighted. The main content area shows the 'X4Realm' configuration page with tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, showing the 'Security Defenses' section. The configuration fields include: 'Name' (X4Realm), 'Display name', 'HTML Display name', 'Frontend URL', 'Enabled' (ON), 'User-Managed Access' (OFF), and 'Endpoints' (OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK

Admin

X4Realm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

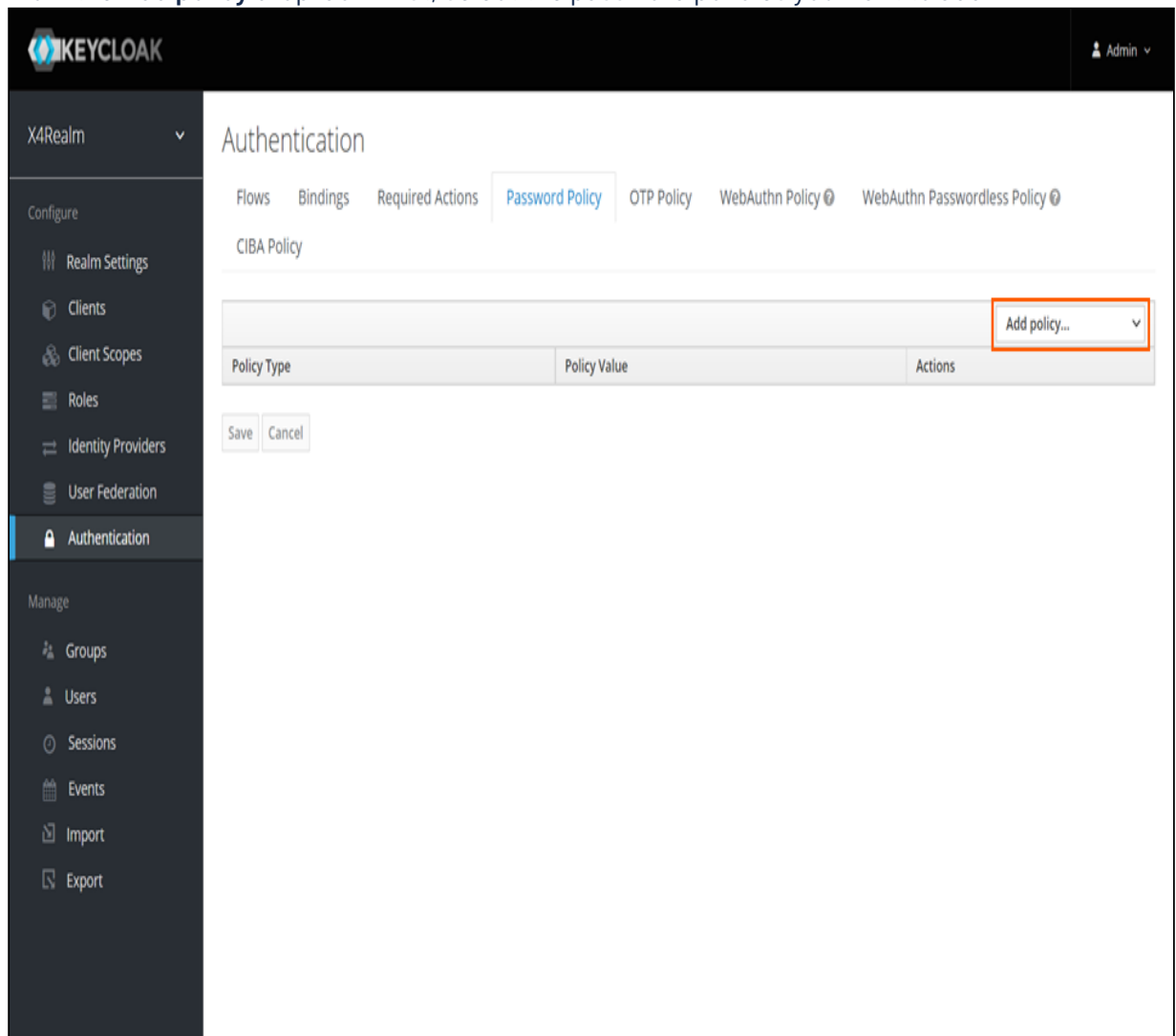
Save Cancel

3. Switch to the **Password Policy** tab.

The screenshot shows the Keycloak Administration Console interface. The top navigation bar includes the Keycloak logo, the realm name 'X4Realm', and the user 'Admin'. The left sidebar contains a 'Configure' section with links to Realm Settings, Clients, Client Scopes, Roles, Identity Providers, and User Federation, and a 'Manage' section with links to Groups, Users, Sessions, Events, Import, and Export. The 'Authentication' section is highlighted in the sidebar. The main content area is titled 'Authentication' and contains tabs for Flows, Bindings, Required Actions, Password Policy (which is selected and highlighted with an orange box), OTP Policy, WebAuthn Policy, and WebAuthn Passwordless Policy. Below the tabs is a 'CIBA Policy' section. The main area displays a table of authentication requirements. At the top of the table is a dropdown menu set to 'Browser' and buttons for 'New' and 'Copy'. The table has columns for 'Auth Type', 'Requirement', and 'Actions'. The requirements listed are: Cookie (REQUIRED, ALTERNATIVE, DISABLED), Kerberos (REQUIRED, ALTERNATIVE, DISABLED), Identity Provider Redirector (REQUIRED, ALTERNATIVE, DISABLED), Forms (REQUIRED, ALTERNATIVE, DISABLED, CONDITIONAL), Username Password Form (REQUIRED), Browser - Conditional OTP (REQUIRED, ALTERNATIVE, DISABLED, CONDITIONAL), Condition - User Configured (REQUIRED, DISABLED), and OTP Form (REQUIRED, ALTERNATIVE, DISABLED).

Auth Type	Requirement	Actions
Cookie	☐ REQUIRED ☒ ALTERNATIVE ☐ DISABLED	
Kerberos	☐ REQUIRED ☐ ALTERNATIVE ☒ DISABLED	
Identity Provider Redirector	☐ REQUIRED ☒ ALTERNATIVE ☐ DISABLED	Actions
Forms	☐ REQUIRED ☒ ALTERNATIVE ☐ DISABLED ☐ CONDITIONAL	
Username Password Form	☒ REQUIRED	
Browser - Conditional OTP	☐ REQUIRED ☐ ALTERNATIVE ☐ DISABLED ☒ CONDITIONAL	
Condition - User Configured	☒ REQUIRED ☐ DISABLED	
OTP Form	☒ REQUIRED ☐ ALTERNATIVE ☐ DISABLED	

4. From the **Add policy** drop-down list, select the password policies you want to add.



5. Click **Save**.

✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#password-policy-types.

6.3.11 Themes

You can use a predefined theme for the login page in Keycloak or design a custom login page.

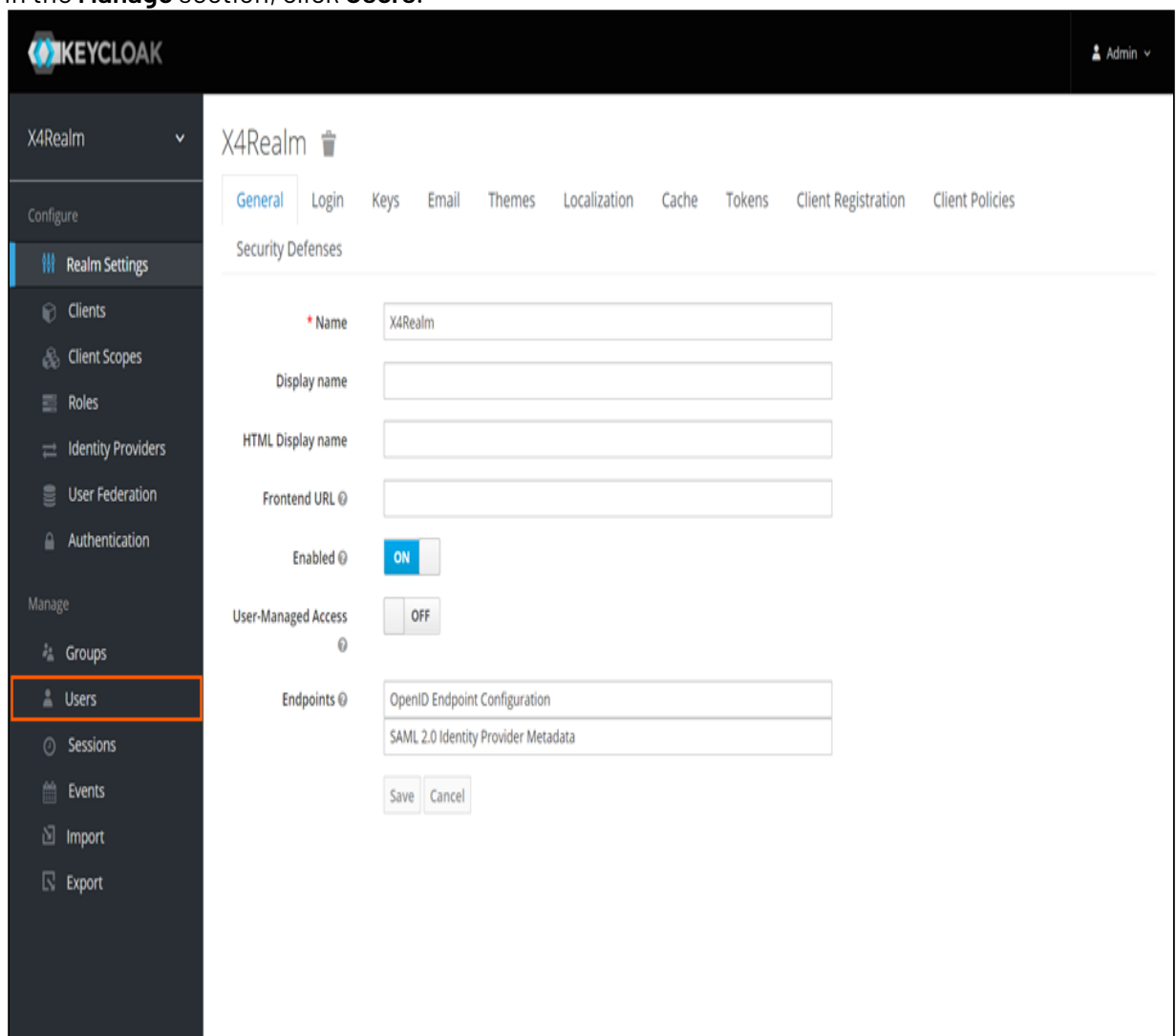
✓ For more information, visit https://www.keycloak.org/docs/latest/server_admin/#_themes.

6.4 Users

6.4.1 Create user

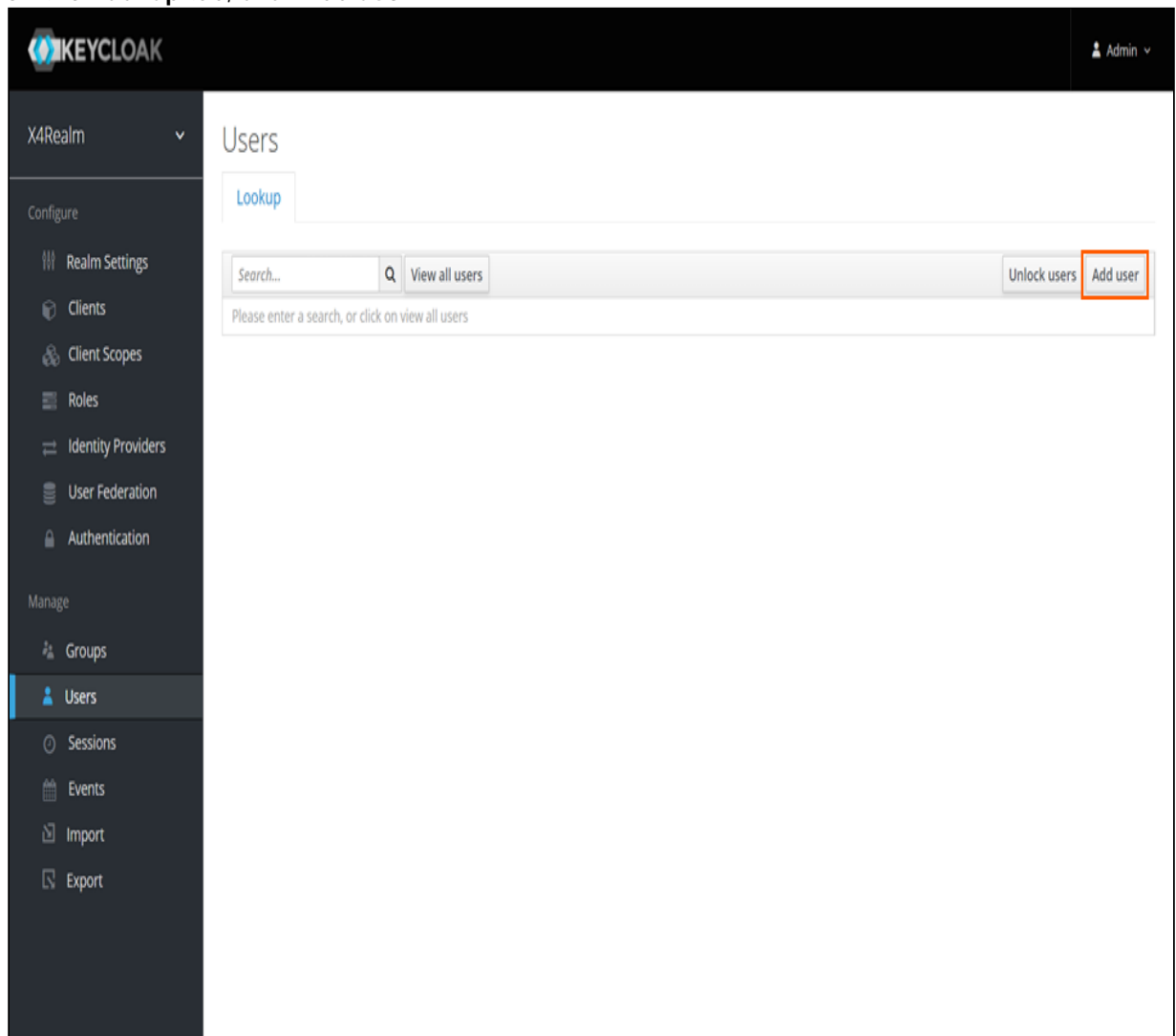
⚠ If a Web App uses the Resource Owner Password Flow authorization flow, a user with a temporary password cannot log in to that Web App.
If you want to use temporary passwords, use the Authorization Code Flow.

1. Open the **Keycloak Administration Console**.
2. In the **Manage** section, click **Users**.



The screenshot displays the Keycloak Administration Console interface. The top navigation bar shows the 'KEYCLOAK' logo and the user 'Admin'. The left sidebar contains a menu with 'Configure' and 'Manage' sections. Under 'Manage', the 'Users' option is highlighted with an orange border. The main content area shows the 'X4Realm' configuration page. The 'General' tab is selected, displaying fields for 'Name' (X4Realm), 'Display name', 'HTML Display name', 'Frontend URL', 'Enabled' (ON), 'User-Managed Access' (OFF), and 'Endpoints' (OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

3. On the **Lookup** tab, click **Add user**.



4. Enter the relevant data.
5. Click **Save**.

6.4.2 Assign a role to a user

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **Users**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar is divided into 'Configure' and 'Manage' sections. Under 'Manage', the 'Users' option is highlighted with an orange border. The main content area shows the 'X4Realm' configuration page with tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, displaying 'Security Defenses' settings. The 'Name' field is set to 'X4Realm'. The 'Display name' and 'HTML Display name' fields are empty. The 'Frontend URL' field is empty. The 'Enabled' toggle is set to 'ON'. The 'User-Managed Access' toggle is set to 'OFF'. The 'Endpoints' section shows 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. At the bottom, there are 'Save' and 'Cancel' buttons.

KEYCLOAK

Admin

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

* Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

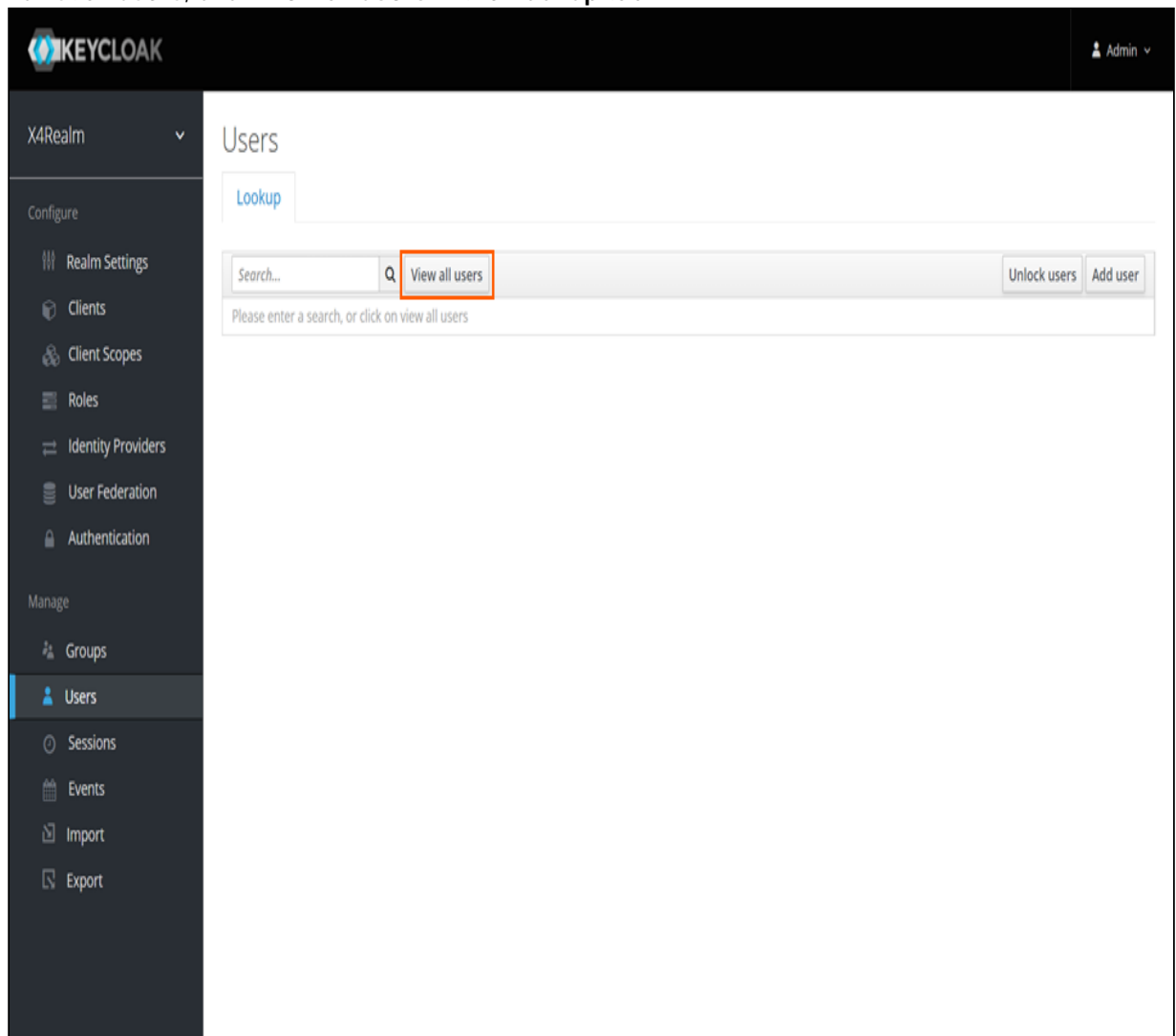
Endpoints

OpenID Endpoint Configuration

SAML 2.0 Identity Provider Metadata

Save Cancel

3. To list all users, click **View all users** in the **Lookup** tab.



4. In the row of the desired user, click **Edit** in the **Actions** column.

The screenshot shows the Keycloak administration interface. The left sidebar contains a menu with the following items: X4Realm, Configure (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication), Manage (Groups, Users, Sessions, Events, Import, Export). The 'Users' item is currently selected. The main content area is titled 'Users' and includes a 'Lookup' input field. Below this is a table of users with the following columns: ID, Username, Email, Last Name, First Name, and Actions. The table contains two rows of data. The 'Actions' column for each row contains three buttons: 'Edit', 'Impersonate', and 'Delete'. A red box highlights the 'Edit' button for the user with ID '1093de12-c495-48d8-...'.

ID	Username	Email	Last Name	First Name	Actions
1b367493-2a5a-4edc-...	demo				Edit Impersonate Delete
1093de12-c495-48d8-...	system				Edit Impersonate Delete

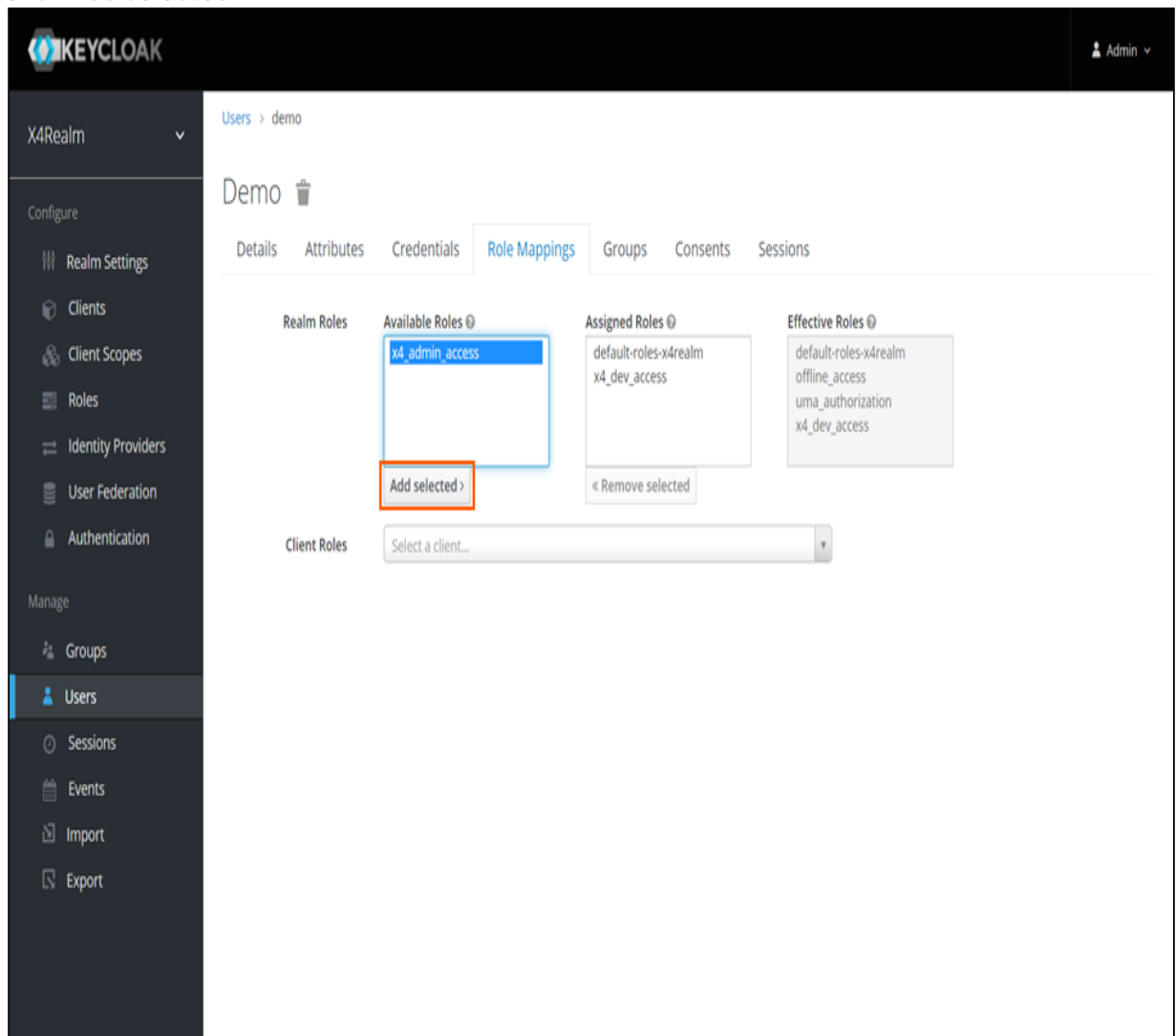
5. Switch to the **Role Mappings** tab.

The screenshot displays the Keycloak Admin Console interface. On the left is a dark sidebar with a menu. The top of the sidebar shows 'X4Realm' with a dropdown arrow. Below this, the menu is divided into 'Configure' (containing Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, and Authentication) and 'Manage' (containing Groups, Users, Sessions, Events, Import, and Export). The 'Users' option is currently selected and highlighted. The main content area on the right has a top bar with the Keycloak logo and 'Admin' with a dropdown. Below this, a breadcrumb trail shows 'Users > demo'. The main heading is 'Demo' with a trash icon. A horizontal tab bar contains 'Details', 'Attributes', 'Credentials', 'Role Mappings' (which is highlighted with an orange border), 'Groups', 'Consents', and 'Sessions'. The 'Role Mappings' tab displays the following fields and controls:

- ID:** 1b367493-2a5a-4edc-b858-f2ce71e1b625
- Created At:** 8/13/21 7:43:52 AM
- Username:** demo
- Email:** (empty text input)
- First Name:** (empty text input)
- Last Name:** (empty text input)
- User Enabled:** ON (toggle switch)
- Email Verified:** OFF (toggle switch)
- Required User Actions:** Select an action... (dropdown menu)
- Impersonate user:** Impersonate (button)
- Buttons:** Save, Cancel

6. In the **Available Roles** area, select the role to be assigned to the user.

The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the 'KEYCLOAK' logo and the user 'Admin'. The left sidebar contains the 'Configure' section with options like 'Realm Settings', 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication', as well as the 'Manage' section with 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The 'Users' option is currently selected. The main content area shows the 'demo' realm and the 'Demo' user. The 'Role Mappings' tab is active, displaying three columns: 'Realm Roles', 'Available Roles', and 'Assigned Roles'. The 'Available Roles' column is highlighted with an orange box and contains the role 'x4_admin_access'. Below this column is an 'Add selected >' button. The 'Assigned Roles' column contains 'default-roles-x4realm' and 'x4_dev_access', with a '< Remove selected' button below it. The 'Effective Roles' column lists 'default-roles-x4realm', 'offline_access', 'uma_authorization', and 'x4_dev_access'. At the bottom, there is a 'Client Roles' section with a dropdown menu labeled 'Select a client...'.

7. Click **Add selected**.

6.4.3 Assign user to a group

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **Users**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar is divided into 'Configure' and 'Manage' sections. Under 'Manage', the 'Users' option is highlighted with an orange border. The main content area shows the 'General' tab for 'Security Defenses'. The form includes fields for 'Name' (X4Realm), 'Display name', 'HTML Display name', and 'Frontend URL'. There are toggle switches for 'Enabled' (ON) and 'User-Managed Access' (OFF). Below these are text areas for 'Endpoints' containing 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK Admin

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

* Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

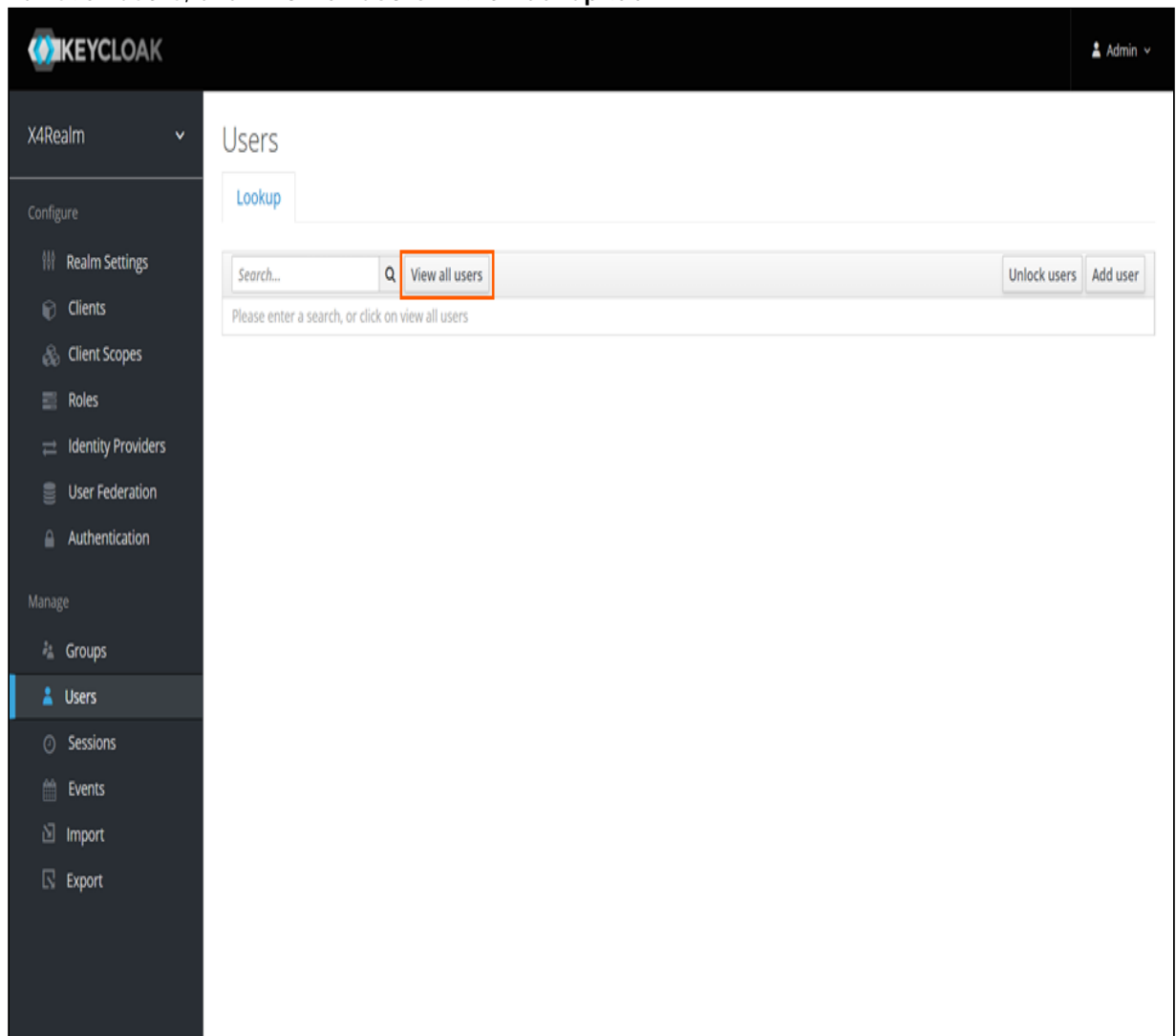
Endpoints

OpenID Endpoint Configuration

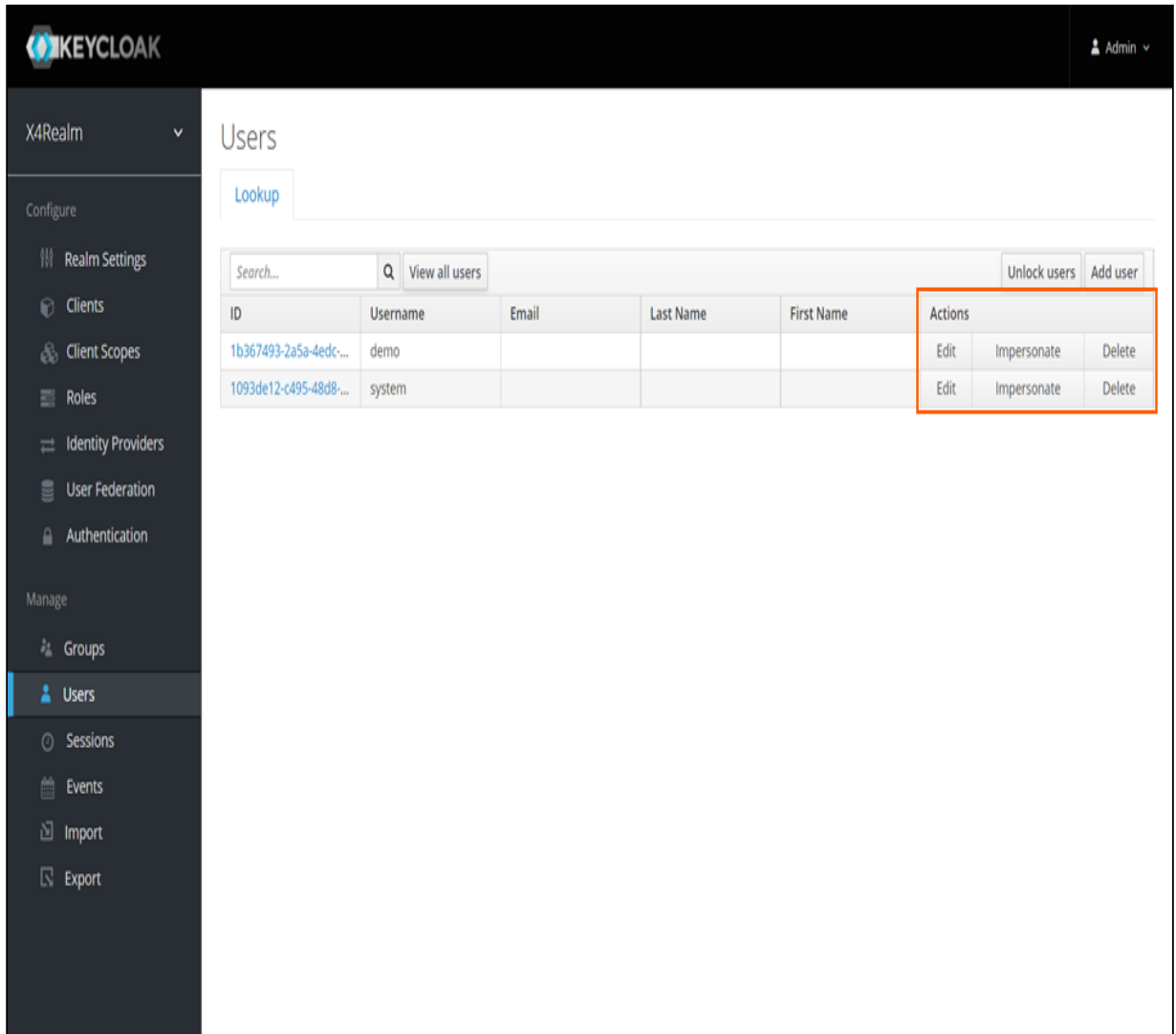
SAML 2.0 Identity Provider Metadata

Save Cancel

3. To list all users, click **View all users** in the **Lookup** tab.



4. In the row of the desired user, click **Edit** in the **Actions** column.



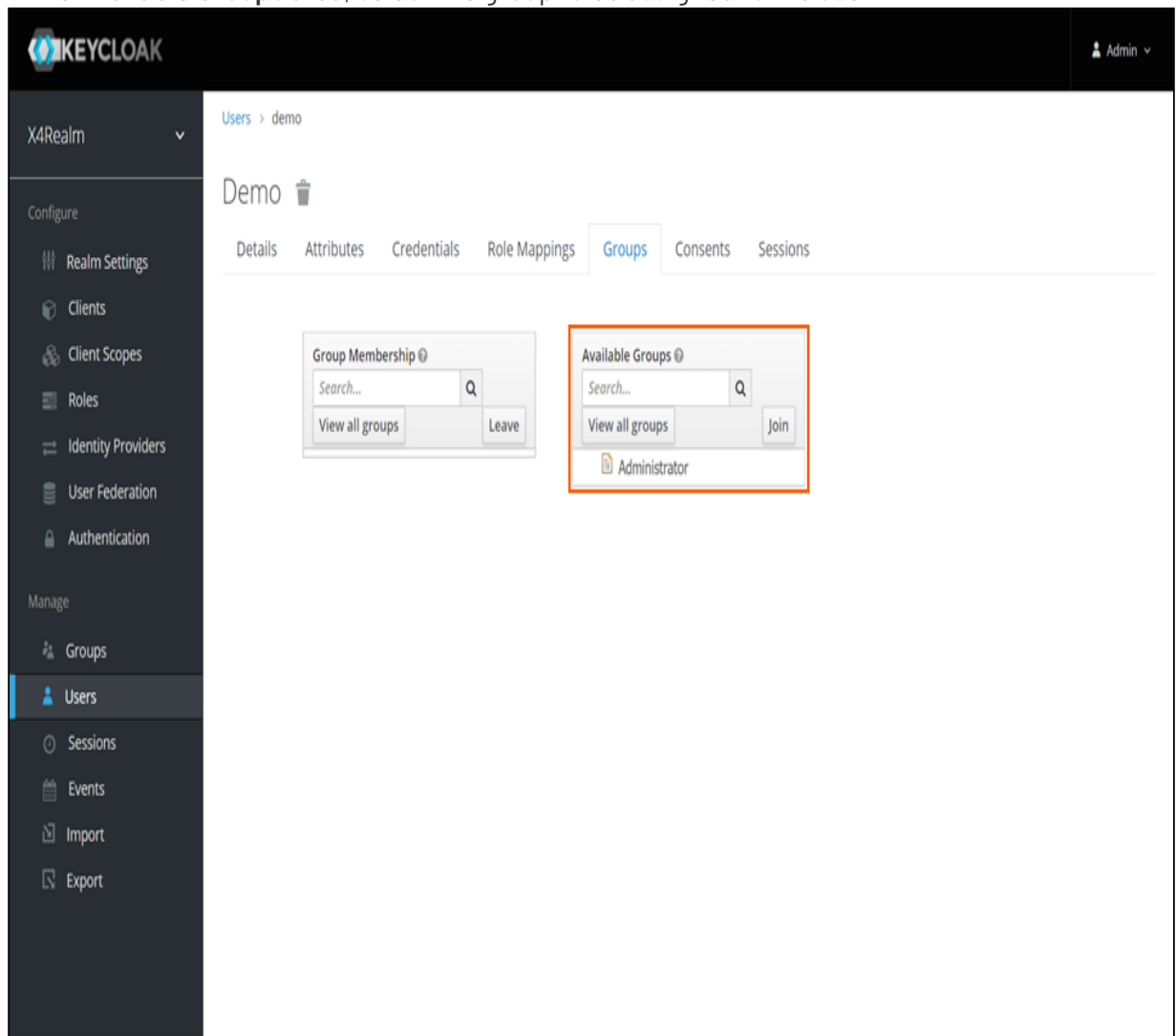
The screenshot shows the Keycloak administration interface. The left sidebar contains a menu with the following items: X4Realm, Configure (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication), Manage (Groups, Users, Sessions, Events, Import, Export). The 'Users' item is highlighted. The main content area is titled 'Users' and includes a 'Lookup' input field. Below this is a table of users with the following columns: ID, Username, Email, Last Name, First Name, and Actions. The table contains two rows of data. The 'Actions' column for each row contains three buttons: 'Edit', 'Impersonate', and 'Delete'. The 'Edit' button for the first user is highlighted with a red box.

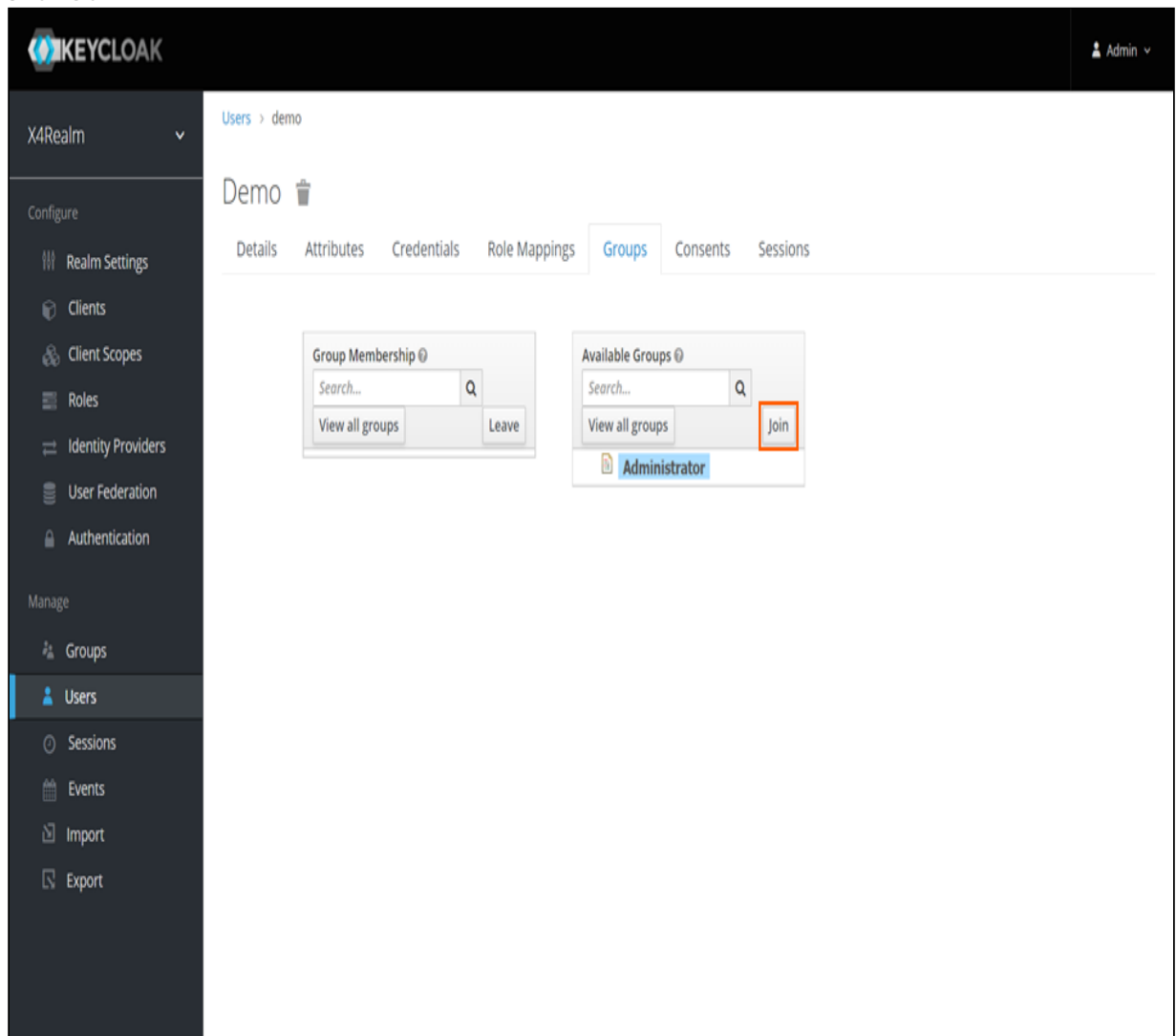
ID	Username	Email	Last Name	First Name	Actions
1b367493-2a5a-4edc...	demo				Edit Impersonate Delete
1093de12-c495-48d8...	system				Edit Impersonate Delete

5. Switch to the **Groups** tab.

The screenshot displays the Keycloak Admin Console interface. On the left is a dark sidebar with navigation options under 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The 'Users' option is currently selected. The main content area shows the 'demo' user profile. At the top, there's a breadcrumb 'Users > demo' and a 'Demo' header with a trash icon. Below this is a tabbed interface with 'Details', 'Attributes', 'Credentials', 'Role Mappings', 'Groups' (highlighted with an orange border), 'Consents', and 'Sessions'. The 'Groups' tab contains several fields: 'ID' (1b367493-2a5a-4edc-b858-f2ce71e1b625), 'Created At' (8/13/21 7:43:52 AM), 'Username' (demo), 'Email' (empty), 'First Name' (empty), 'Last Name' (empty), 'User Enabled' (toggle set to ON), 'Email Verified' (toggle set to OFF), 'Required User Actions' (dropdown showing 'Select an action...'), and an 'Impersonate user' button. At the bottom are 'Save' and 'Cancel' buttons. The top right of the console shows the 'KEYCLOAK' logo and an 'Admin' user dropdown.

6. In the **Available Groups** area, select the group to be assigned to the user.



7. Click **Join**.

6.4.4 Remove user from a group

1. Open the **Keycloak Administration Console**.

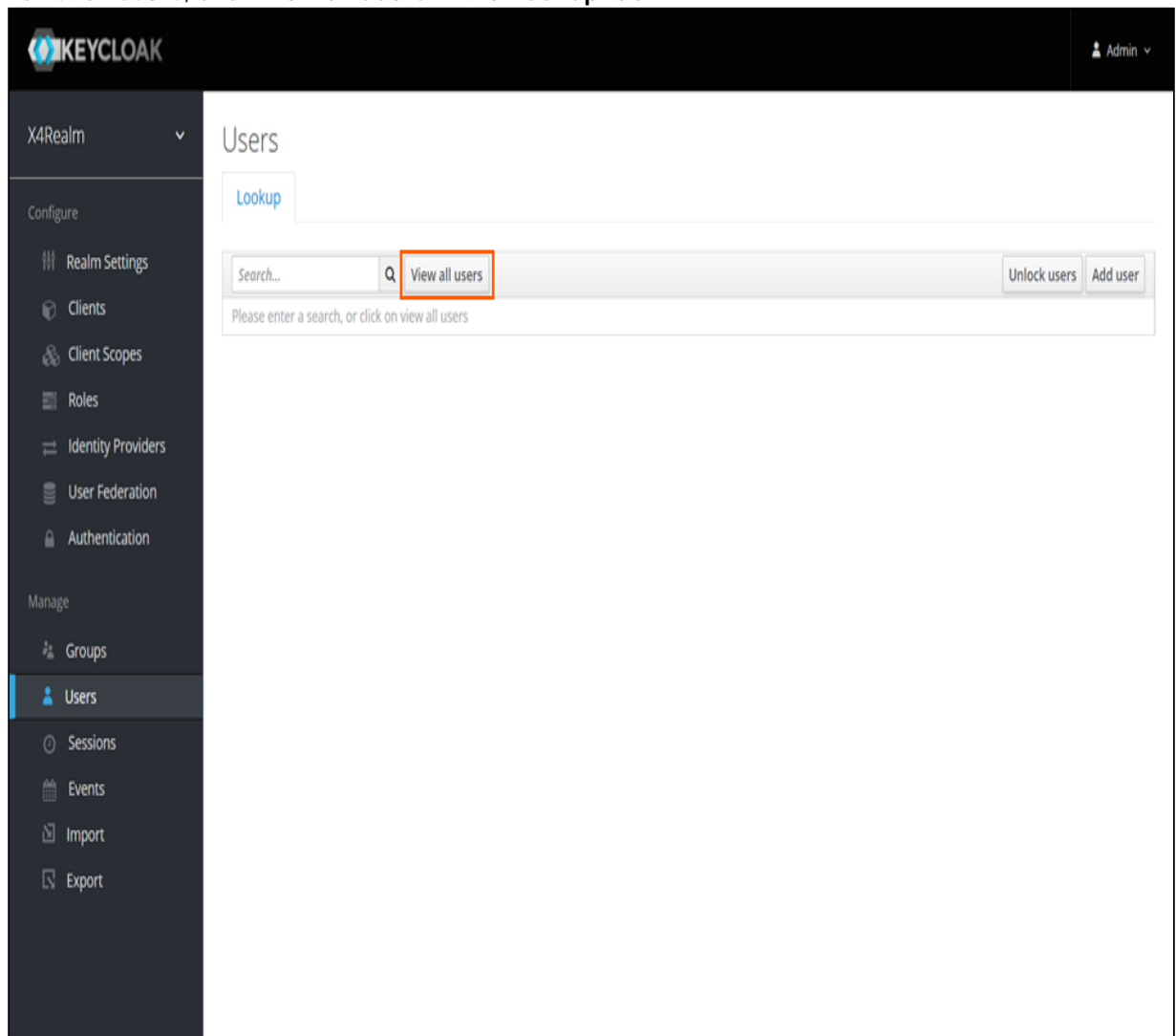
2. In the **Manage** section, click **Users**.

The screenshot displays the Keycloak administration interface for the 'X4Realm'. The left sidebar is divided into 'Configure' and 'Manage' sections. Under 'Manage', the 'Users' option is highlighted with an orange border. The main content area shows the 'General' tab for 'X4Realm' under 'Security Defenses'. The configuration fields include:

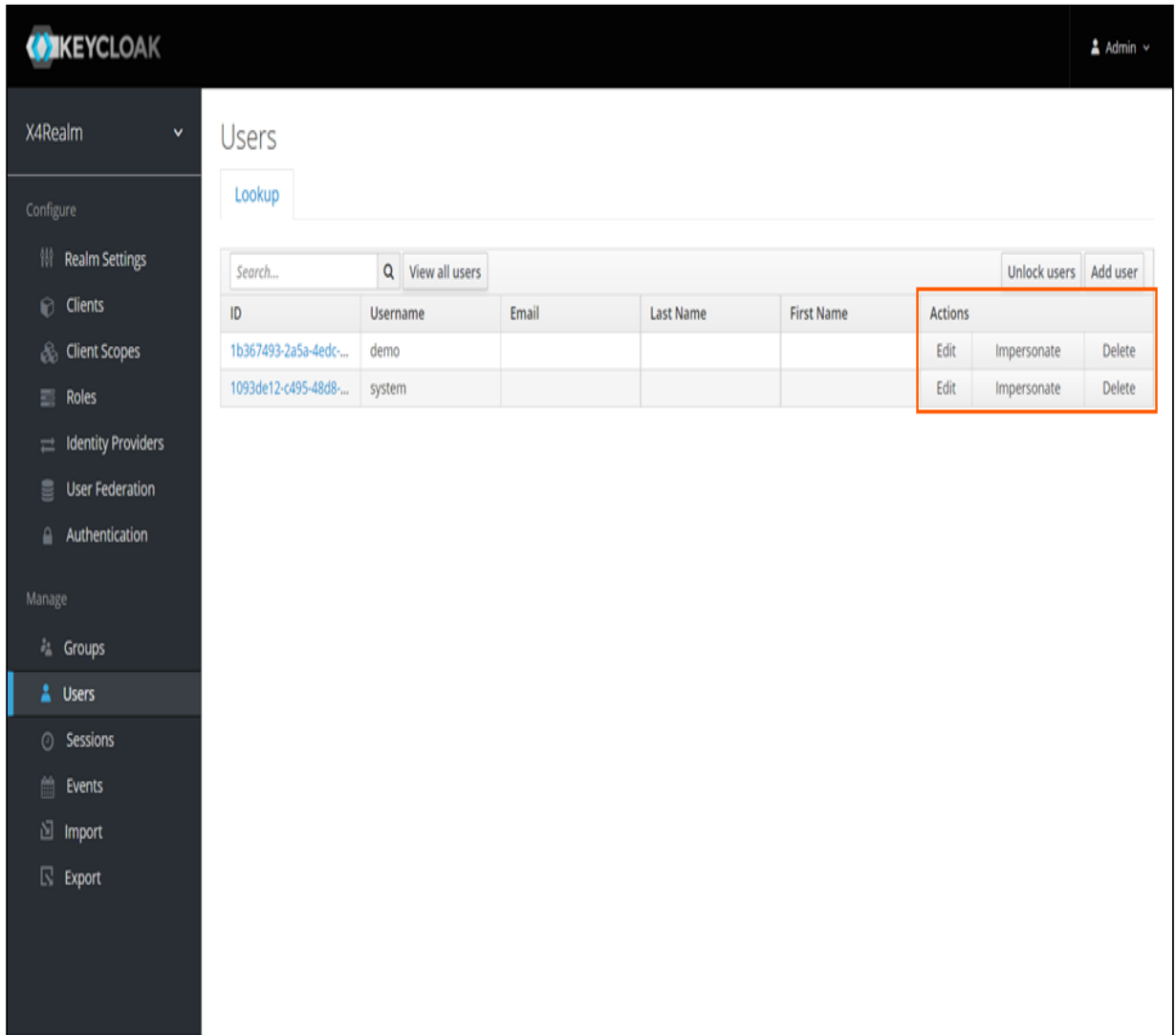
- Name:** X4Realm
- Display name:** (empty)
- HTML Display name:** (empty)
- Frontend URL:** (empty)
- Enabled:** ON (toggle)
- User-Managed Access:** OFF (toggle)
- Endpoints:** OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

At the bottom, there are 'Save' and 'Cancel' buttons.

3. To list all users, click **View all users** in the **Lookup** tab.



4. In the row of the desired user, click **Edit** in the **Actions** column.



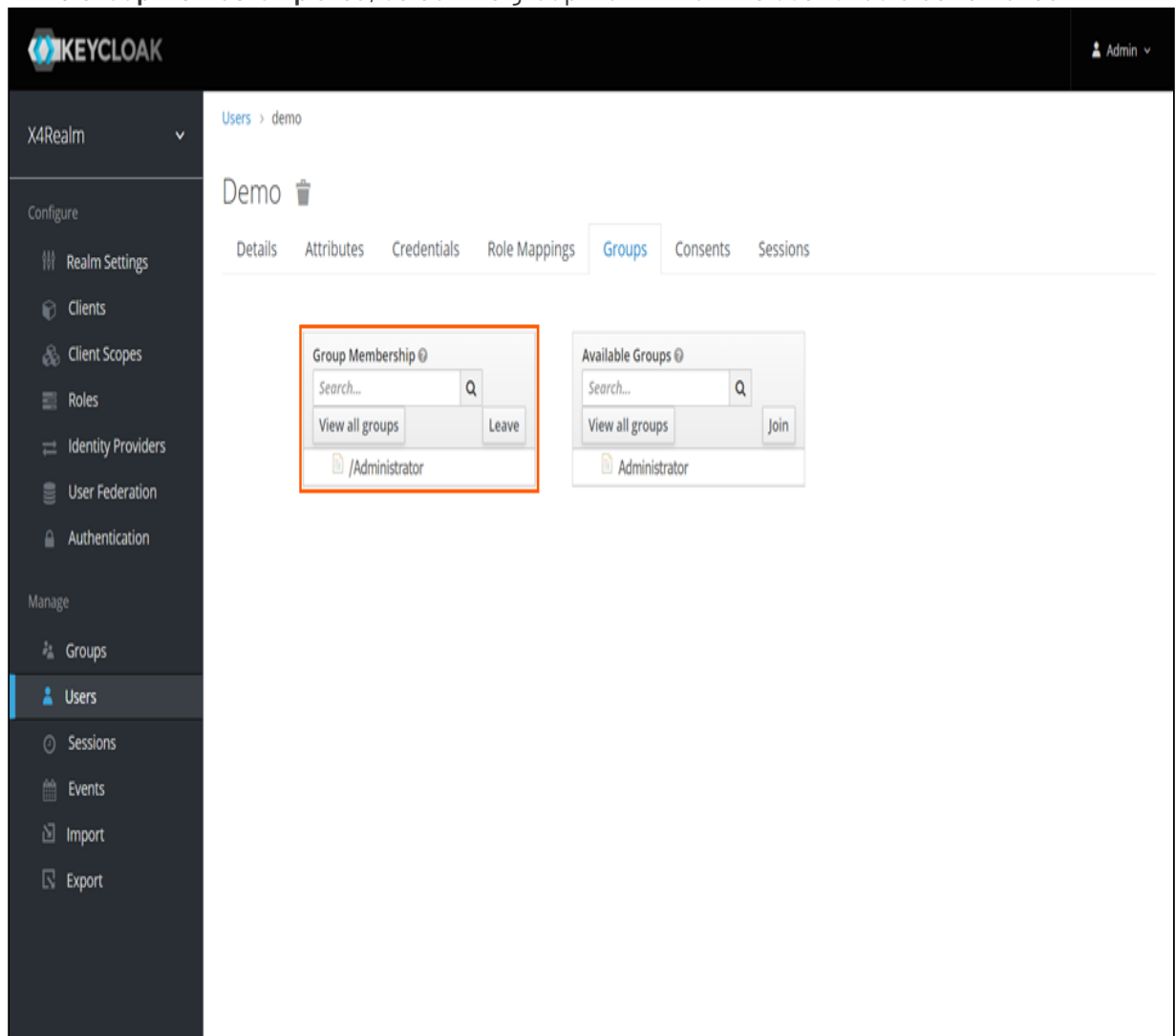
The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar contains a 'Configure' section with options like 'Realm Settings', 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. Below this is a 'Manage' section with 'Groups', 'Users' (highlighted), 'Sessions', 'Events', 'Import', and 'Export'. The main content area is titled 'Users' and includes a 'Lookup' input field. Below the input field is a table of users. The table has columns for ID, Username, Email, Last Name, First Name, and Actions. The 'Actions' column contains 'Edit', 'Impersonate', and 'Delete' buttons. A red box highlights the 'Edit' button for the user with ID '1b367493-2a5a-4edc-...' and Username 'demo'.

ID	Username	Email	Last Name	First Name	Actions
1b367493-2a5a-4edc-...	demo				Edit Impersonate Delete
1093de12-c495-48d8-...	system				Edit Impersonate Delete

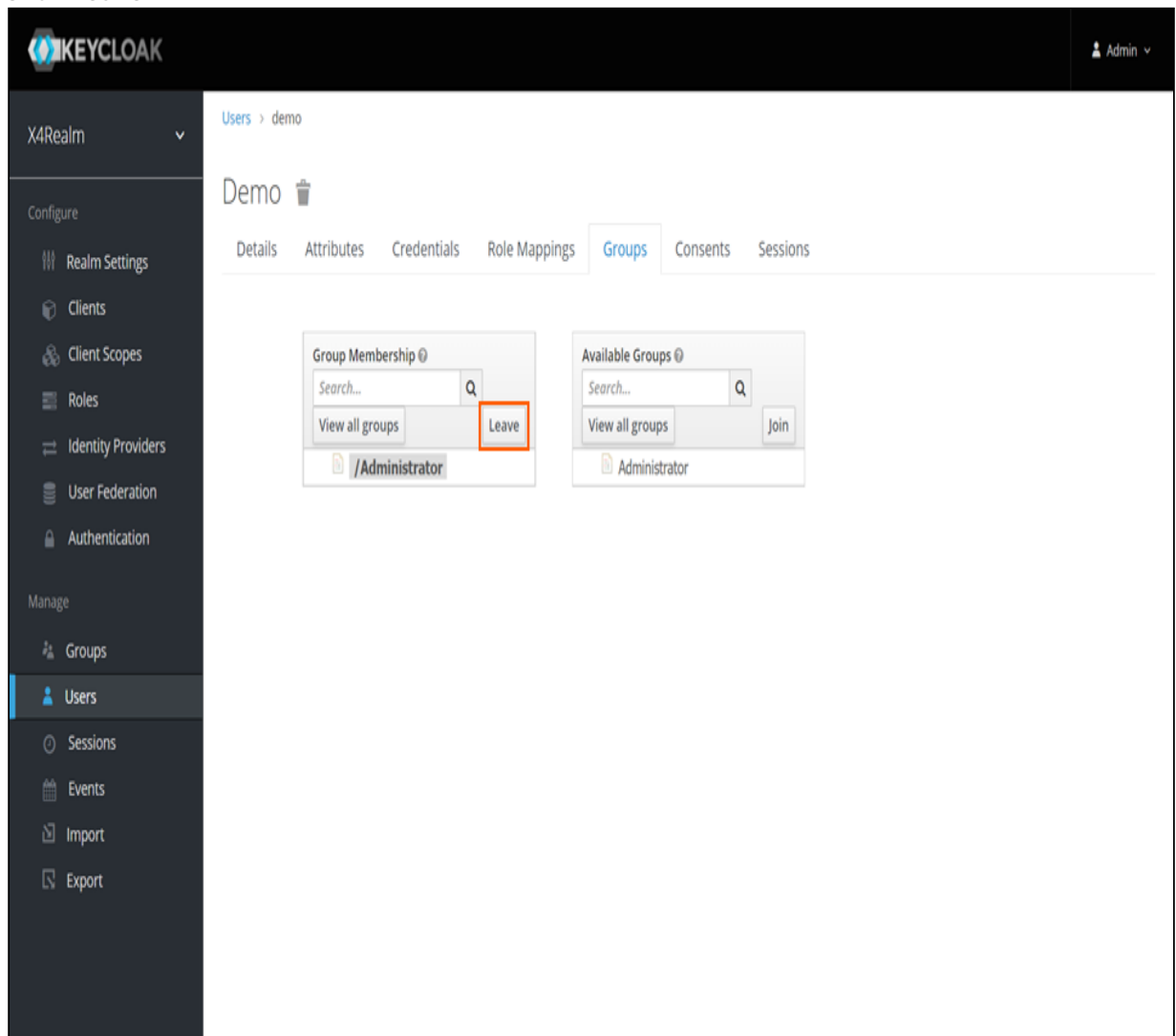
5. Switch to the **Groups** tab.

The screenshot displays the Keycloak Admin Console interface. On the left, a dark sidebar contains navigation links under 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The 'Users' link is highlighted. The main content area shows the 'demo' user profile. At the top, a breadcrumb trail reads 'Users > demo'. Below this, the 'Demo' user name is shown with a trash icon. A horizontal tab bar includes 'Details', 'Attributes', 'Credentials', 'Role Mappings', 'Groups' (highlighted with an orange border), 'Consents', and 'Sessions'. The 'Groups' tab is active, displaying the following fields: ID (1b367493-2a5a-4edc-b858-f2ce71e1b625), Created At (8/13/21 7:43:52 AM), Username (demo), Email (empty), First Name (empty), Last Name (empty), User Enabled (ON), Email Verified (OFF), Required User Actions (Select an action...), and an Impersonate user button. At the bottom are 'Save' and 'Cancel' buttons. The top right of the console shows the 'Admin' user profile.

6. In the **Group Membership** area, select the group from which the user should be removed.



7. Click **Leave**.



6.5 Roles

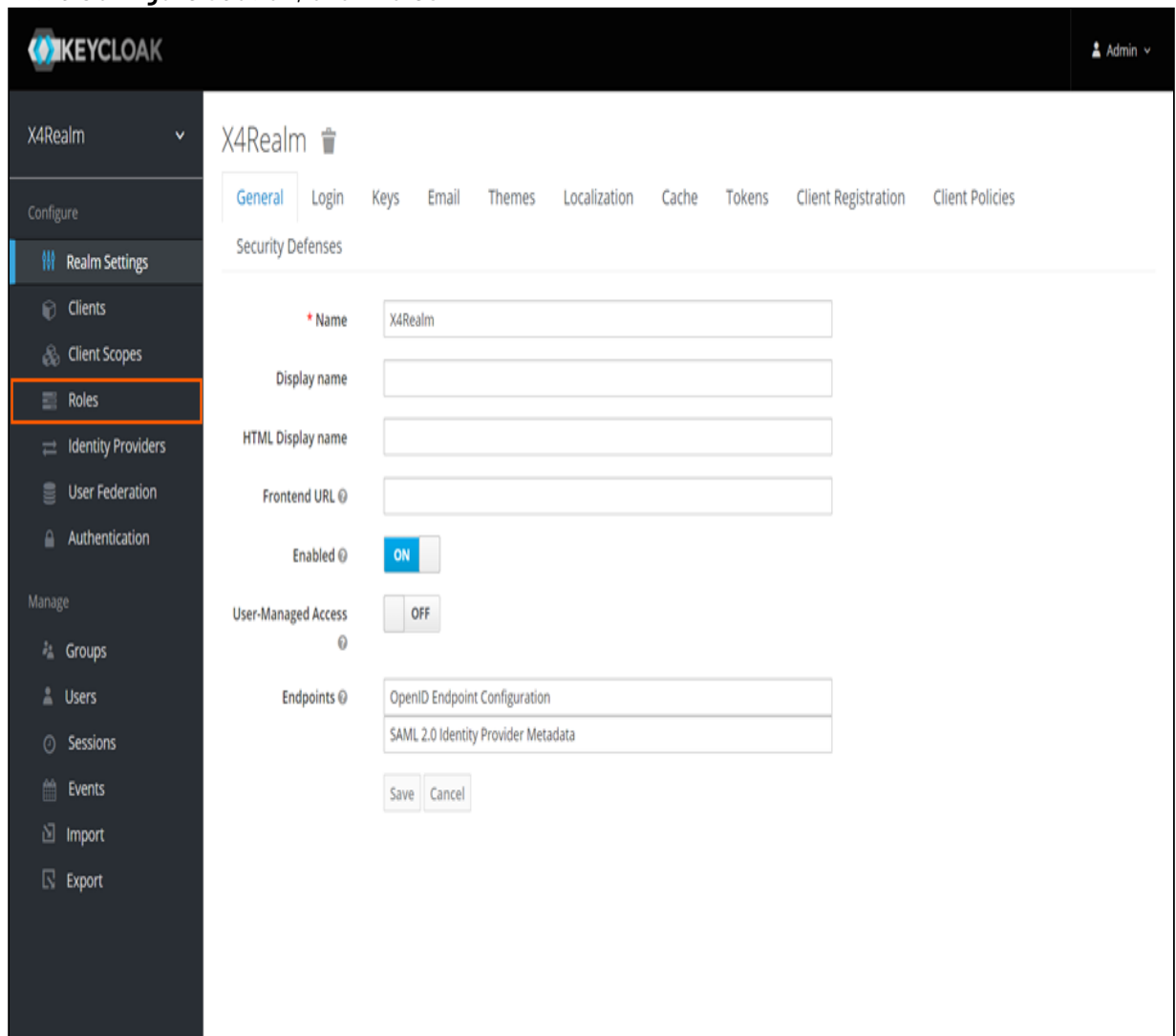
Client roles are basically a namespace dedicated to a client. Each client gets its own namespace.

Source: https://www.keycloak.org/docs/latest/server_admin/#client-roles

6.5.1 Create role

1. Open the **Keycloak Administration Console**.

2. In the **Configure** section, click **Roles**.

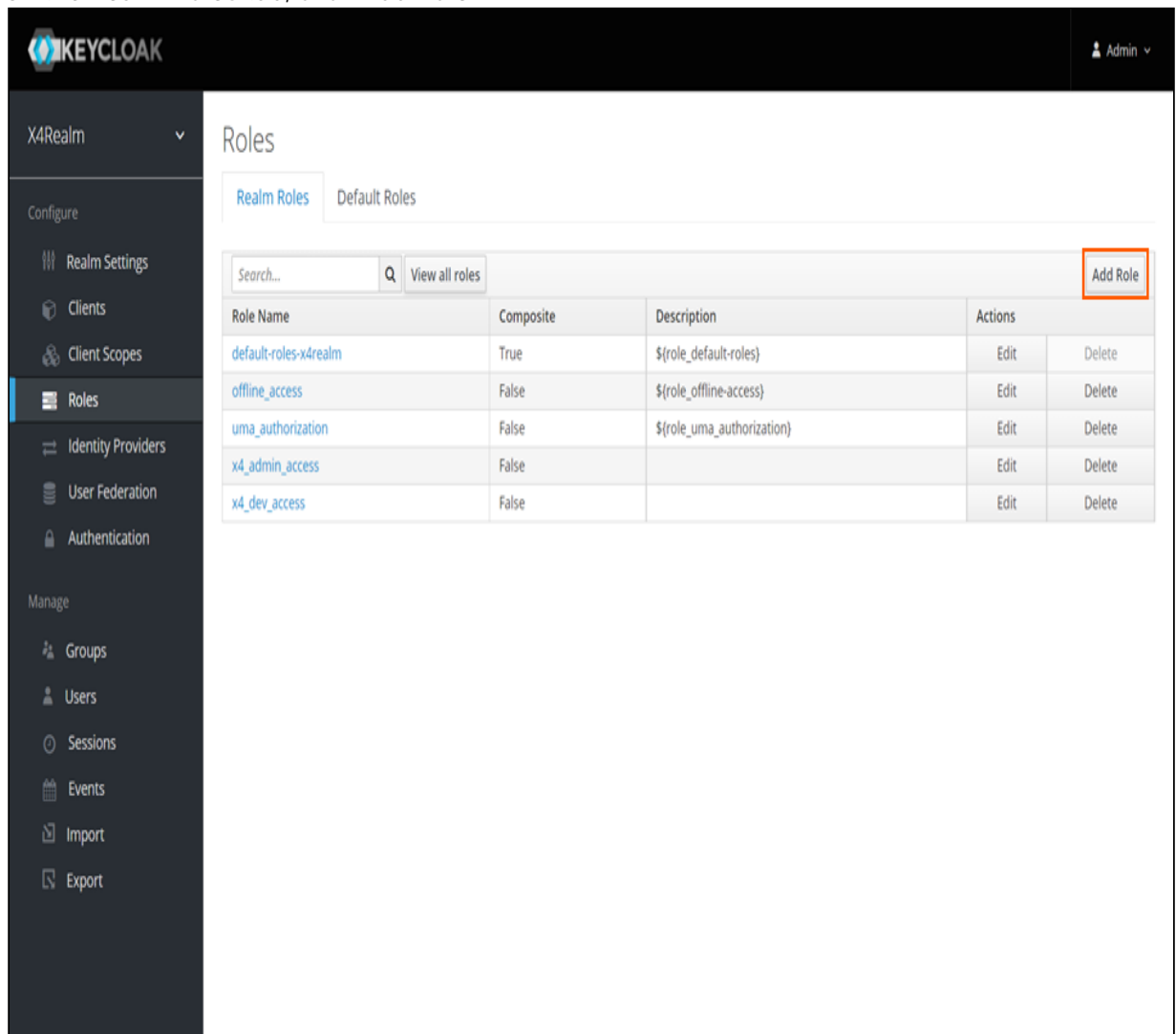


The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar is dark grey with a list of configuration options. The 'Roles' option is highlighted with an orange border. The main content area is white and shows the 'X4Realm' configuration page. The 'General' tab is selected, and the 'Security Defenses' section is visible. The configuration fields include:

- Name:** X4Realm
- Display name:** (empty field)
- HTML Display name:** (empty field)
- Frontend URL:** (empty field)
- Enabled:** ON (toggle switch)
- User-Managed Access:** OFF (toggle switch)
- Endpoints:** OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

At the bottom of the configuration section, there are 'Save' and 'Cancel' buttons.

3. On the **Realm Roles** tab, click **Add Role**.



4. Enter a name in the **Role Name** text box.
5. Click **Save**.

6.6 Groups

Groups in Keycloak allow you to manage a common set of attributes and role mappings for a set of users. Users can be members of zero or more groups. Users inherit the attributes and role mappings assigned to each group.

Source: https://www.keycloak.org/docs/latest/server_admin/#groups

6.6.1 Create group

1. Open the **Keycloak Administration Console**.

2. In the **Manage** section, click **Groups**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar is divided into 'Configure' and 'Manage' sections. Under 'Manage', the 'Groups' option is highlighted with an orange border. The main content area shows the 'X4Realm' configuration page with tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. The 'General' tab is active, displaying 'Security Defenses' settings. The 'Name' field is set to 'X4Realm'. The 'Display name' and 'HTML Display name' fields are empty. The 'Frontend URL' field is empty. The 'Enabled' toggle is set to 'ON'. The 'User-Managed Access' toggle is set to 'OFF'. The 'Endpoints' section shows 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. At the bottom, there are 'Save' and 'Cancel' buttons.

KEYCLOAK

Admin

X4Realm

General Login Keys Email Themes Localization Cache Tokens Client Registration Client Policies

Security Defenses

Name X4Realm

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

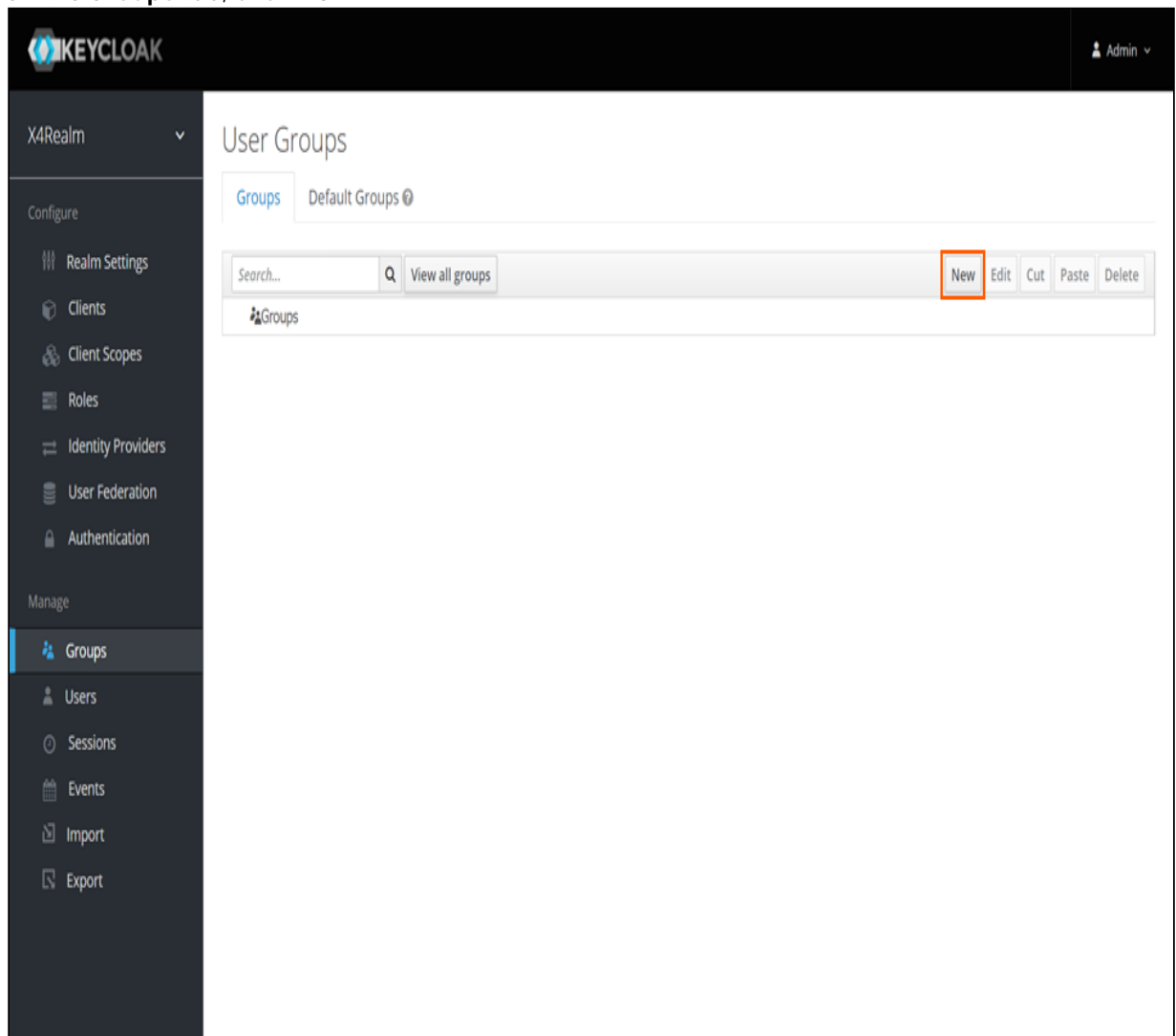
Endpoints

OpenID Endpoint Configuration

SAML 2.0 Identity Provider Metadata

Save Cancel

3. On the **Groups** tab, click **New**.



4. Enter a name in the **Name** text box.
5. Click **Save**.