

Geschäftsprozesse erfolgreich digitalisieren

Die digitale Transformation durch die Low-Code-Plattform X4 BPMS beschleunigen

X4 Administration Guide

Die in dieser Dokumentation enthaltenen Informationen und die zugehörigen Programme können ohne besondere Ankündigung geändert werden. Für etwaige Fehler übernimmt SoftProject keine Haftung.

Diese Dokumentation und die zugehörigen Programme dürfen ohne schriftliche Zustimmung der SoftProject GmbH weder ganz noch teilweise kopiert, reproduziert, verändert oder in irgendeine elektronische oder maschinenlesbare Form umgewandelt werden.

Alle genannten Warenzeichen sind Warenzeichen der jeweiligen Eigentümer.

Kontakt

SoftProject GmbH

Am Erlengraben 3

D-76275 Ettlingen

Website: www.softproject.de

Vertrieb

Telefon: +49 7243 56175-0

vertrieb@softproject.de

SoftProject-Support

Telefon: +49 7243 56175-333

support@softproject.de

© SoftProject GmbH. Alle Rechte vorbehalten.

Inhaltsverzeichnis

1	Systemvoraussetzungen	8
2	Installation	10
2.1	Installation des X4 Servers	10
2.1.1	Installation auf Windows Systemen	10
2.1.2	Installation auf Ubuntu/Debian Linux Systemen	20
2.1.3	Installation auf Red Hat Enterprise Linux Systemen.....	22
2.1.4	Installation auf SuSe Linux Systemen	25
2.1.5	X4 Server in Docker installieren	27
2.1.6	X4 Server auf anderen Betriebssystemen installieren	29
2.2	Lizenz initial installieren	29
2.3	Lizenz erneuern.....	29
2.4	Lizenz-Informationen anzeigen	30
2.5	X4 Designer installieren und deinstallieren	30
2.5.1	X4 Designer installieren.....	30
2.5.2	X4 Designer deinstallieren.....	32
2.5.3	Parameter der unbeaufsichtigten Installation.....	33
2.6	Installation und Migration der System-Datenbank und der X4DB	33
2.7	Installation des Authentifizierungsproviders	33
3	Konfiguration	35
3.1	X4 Server konfigurieren.....	35
3.1.1	Datenbank einrichten	35
3.1.2	Konfiguration über X4config.xml	41
3.1.3	Logging/Protokollierung konfigurieren.....	44
3.1.4	Production Mode konfigurieren	46
3.1.5	SSL und HTTPS für den X4 Server einrichten	46
3.2	X4 Designer konfigurieren	49
3.2.1	Verbindungskonfiguration bearbeiten	49
3.2.2	Process Editor konfigurieren.....	50

3.2.3	Run-/Debug-Modus konfigurieren	51
3.2.4	Mapping Editor konfigurieren	53
3.2.5	Vorlagen für Repository-Elemente verwalten	54
3.2.6	Dateitypen zu internen und externen Editoren zuordnen.....	54
3.2.7	Web Browser konfigurieren	56
3.2.8	JSON-Editor konfigurieren.....	57
3.2.9	Sprache der Hilfe umschalten.....	58
4	Administration des X4 Servers	59
4.1	X4 Repository im Production Mode aktualisieren	59
4.2	X4 Server kontrolliert herunterfahren (via JMX)	59
4.3	Prozess-Bibliotheken bereitstellen.....	61
5	Hochverfügbarkeit	62
5.1	Lastverteilung (Load Balancing)	62
5.1.1	Szenario – Wenige hauptsächlich lesende Datenbankzugriffe	62
5.1.2	Szenario – Gemeinsamer Zugriff über Message Queue	65
5.2	Ausfallsicherheit (Fail Over).....	65
5.2.1	Szenario – Eine exklusive Datenbank	66
5.2.2	Szenario – Systemdatenbank pro X4 Server	67
5.3	Load Balancing mit Scheduler	67
5.3.1	Szenario – Dedizierter X4 Server für Scheduling	68
5.3.2	Szenario – Ein Server zuständig für Scheduling.....	69
5.3.3	Szenario – Externer Scheduler	70
6	Keycloak	71
6.1	Hinweise zur verwendeten Datenbank	72
6.2	Einrichten	73
6.2.1	Docker-Image laden und Container starten.....	73
6.2.2	Eigene Keycloak-Installation anbinden	73
6.3	Konfigurieren	74
6.3.1	Authorization Code Flow anwenden.....	74
6.3.2	Zugriff auf X4 Repository einschränken	75
6.3.3	Standardkonfiguration	75

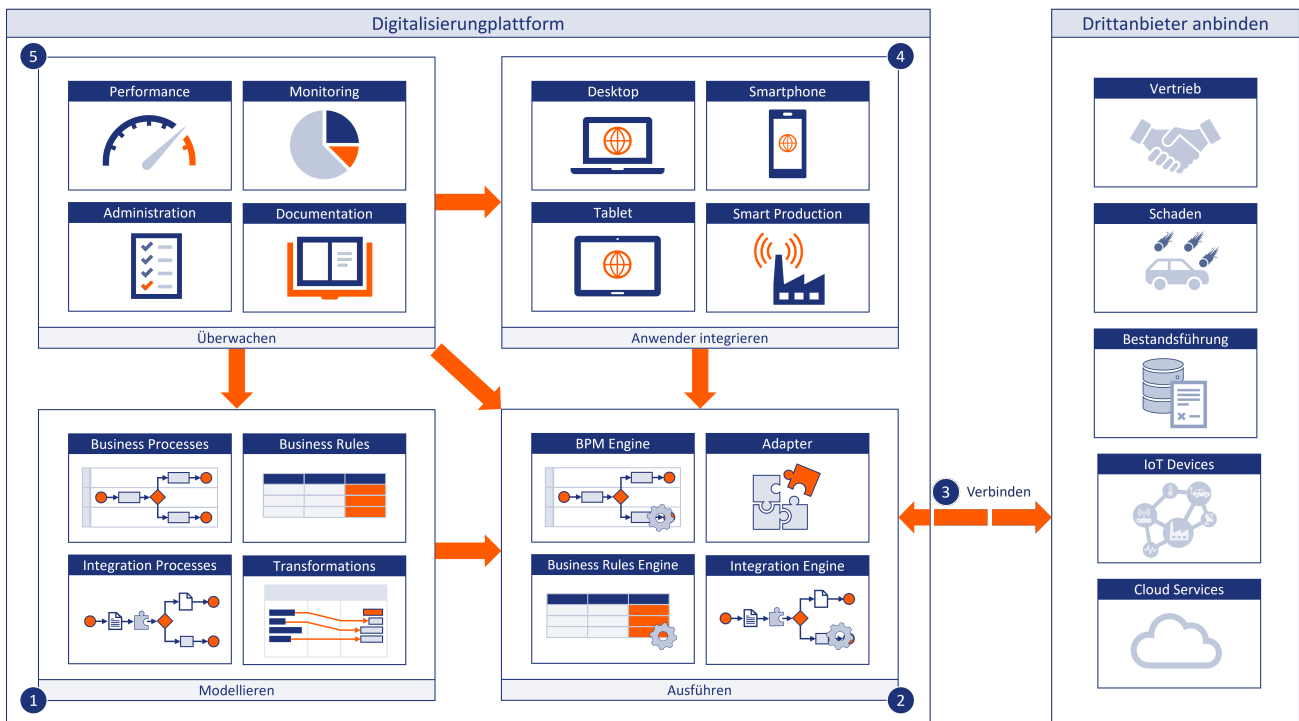
6.3.4	LDAP anbinden.....	78
6.3.5	SAML v2.0 anbinden	80
6.3.6	Kerberos anbinden	82
6.3.7	Social Identity-Anbieter anbinden	84
6.3.8	OpenID Connect anbinden	85
6.3.9	Anmeldeseite	87
6.3.10	Passwörter.....	96
6.3.11	Themes	99
6.4	Benutzer	100
6.4.1	Benutzer erstellen	100
6.4.2	Benutzer eine Rolle zuweisen	101
6.4.3	Benutzer eine Gruppe zuweisen.....	107
6.4.4	Benutzer aus einer Gruppe entfernen	113
6.5	Rollen.....	119
6.5.1	Rolle erstellen	119
6.6	Gruppen	121
6.6.1	Gruppe erstellen.....	121

Über die X4 BPMS

Digitalisierung braucht eine ganzheitliche Betrachtung, die sich in der einzusetzenden Lösung widerspiegeln muss. Als zentrale Plattform unterstützt Sie die X4 BPMS dabei, diese Herausforderungen zu lösen. Im Fokus stehen dabei die Modellierung, Implementierung und Überwachung Ihrer Geschäftsprozesse. Daher enthält die X4 BPMS alle benötigten Werkzeuge und ist mit einer Vielzahl an Schnittstellen und Formaten kompatibel. Mit der X4 BPMS vermeiden Sie isolierte Informationssilos, produktivitätshemmende Medienbrüche und beschleunigen die Digitalisierung.

Geschäftsprozesse ohne Programmieraufwand zu realisieren, ermöglicht einem großen Anwenderkreis den Einstieg in das Management von Geschäftsprozessen. Das lohnt sich, denn Mitarbeiter der Fachabteilung wissen in der Regel am besten, worauf es bei den jeweiligen Geschäftsabläufen im Kern ankommt. Setzen Sie daher auf die X4 BPMS als Plattform, deren Werkzeuge die Komplexität soweit reduzieren, dass sich auch ohne Programmierkenntnisse Geschäftsprozesse analysieren, optimieren, modellieren als auch kontrollieren und dokumentieren lassen. Alle Werkzeuge unterstützen eine integrierte, grafische Prozessmodellierung und -implementierung und erzeugen Prozesse, die von der X4 BPMS performant ausgeführt werden.

- **X4 Designer:** Prozesse und Regeln grafisch modellieren
- **X4 Server:** Simulation und Ausführung der Prozesse und Regeln
- **X4 Adapter:** Drittsysteme in Prozesse integrieren
- **X4 Web Apps:** Web Apps für Mitarbeiter und Kunden bereitstellen



An wen richtet sich dieses Dokument?

Dieses Dokument richtet sich an Administratoren, die den X4 Server installieren, konfigurieren und administrieren möchten. Dazu werden neben detailliertem fachlichem Wissen der bestehenden IT-Infrastruktur auch grundsätzliches Wissen über Java EE, XML-Technologien und den Applikations-Server benötigt.

1 Systemvoraussetzungen

X4 Server

Betriebssystem	• 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 • Zum Einsatz des X4 Servers in einer anderen Umgebung beraten wir Sie gerne. • Es werden nur 64-Bit-Betriebssysteme unterstützt (x86_64). • Für den Einsatz des X4 Proxy Servers ist aus Sicherheitsgründen eine gehärtete Konfiguration des X4 Servers dringend notwendig. Gerne beraten wir Sie hierzu.
Plattform	• Laufzeitumgebung: Der X4 Designer basiert auf der Java 11 Plattform. Mit Version 11 ist Azul Zulu 11.54.23 (Java 11.0.14) bereits als Laufzeitumgebung integriert. • Applikationsserver: Der X4 Server verwendet einen integrierten WildFly-Applikationsserver in Version 25.0.1. • Authentifizierungsprovider: Der X4 Server verwendet den Authentifizierungsprovider Keycloak in der Version 16.1.0. • System-Datenbank: Der X4 Server benötigt zur Verwaltung von Laufzeit- und Authentifizierungsinformationen eine System-Datenbank. Folgende Datenbanken werden unterstützt: • 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 • Bei speziellen Anforderungen bezüglich Java-Laufzeitumgebung oder hinsichtlich der Verwendung alternativer Applikationsserver im Rahmen von kundenspezifischen Anpassungen beraten wir Sie gerne. • Zur Verwendung des X4 Servers mit einer anderen Version der oben genannten Datenbank Management Systeme beraten wir Sie gerne.
Hardware-Anforderungen	• Mindestens 2 Prozessorkerne • Mindestens 5 GB freier Festplatten-Speicherplatz • Mindestens 8 GB Arbeitsspeicher i Ab einer Anzahl von 500 auszuführenden Prozessen empfehlen wir ein System mit mindestens 8 Prozessorkernen und 16 GB Arbeitsspeicher, die ausschließlich für den X4 Server verfügbar sind.

X4 Web Apps

Betriebssystem	X4 Web Apps sind plattformübergreifend via Browser nutzbar.
Plattform	Aktueller Browser (auch mobil) mit aktiviertem JavaScript: • Google Chrome (neuste Version) • Mozilla Firefox (neuste Version und Extended Support Release (ESR)) • Microsoft Edge (die 2 letzten Hauptversionen) • Apple Safari (die 2 letzten Hauptversionen) i Microsoft Internet Explorer und Microsoft Edge ("Projekt Spartan") werden von Microsoft nicht mehr weiterentwickelt. Bitte verwenden Sie stattdessen Microsoft Edge (Chromium-basiert) oder einen anderen kompatiblen Browser.

X4 Designer

Betriebssystem	• Microsoft Windows 8.1, 10 (ab Version 1803) • Microsoft Windows Server 2012, 2012 R2, 2016, 2019 i • Es werden nur 64-Bit-Betriebssysteme unterstützt (x86_64). • Es werden lediglich Windows-Betriebssysteme unterstützt, die die Ausführung von Desktop-Anwendungen erlauben. Core-Versionen des Microsoft Windows Servers werden damit nicht unterstützt. • Desktop-Virtualisierungslösungen (z. B. Citrix XenDesktop oder Citrix XenApp) werden nicht offiziell unterstützt. Einige Kunden setzen jedoch den X4 Designer in solchen Umgebungen ein. Gerne beraten wir Sie hierzu.
Plattform	Laufzeitumgebung Der X4 Designer basiert auf der Java 11 Plattform. Mit Version 11 ist Azul Zulu 11.54.23 (Java 11.0.14) bereits als Laufzeitumgebung integriert.
Hardware-Anforderungen	• Mindestens 2 Prozessorkerne • Mindestens 2 GB freier Festplatten-Speicherplatz • Mindestens 8 GB Arbeitsspeicher

2 Installation

2.1 Installation des X4 Servers

Hier erfahren Sie, wie der X4 Server installiert wird.

 Für die Installation sind Administratorrechte erforderlich.

2.1.1 Installation auf Windows Systemen

Hier erfahren Sie, wie sich der X4 Server – bei Bedarf auch als NT-Dienst – unter Windows installieren.

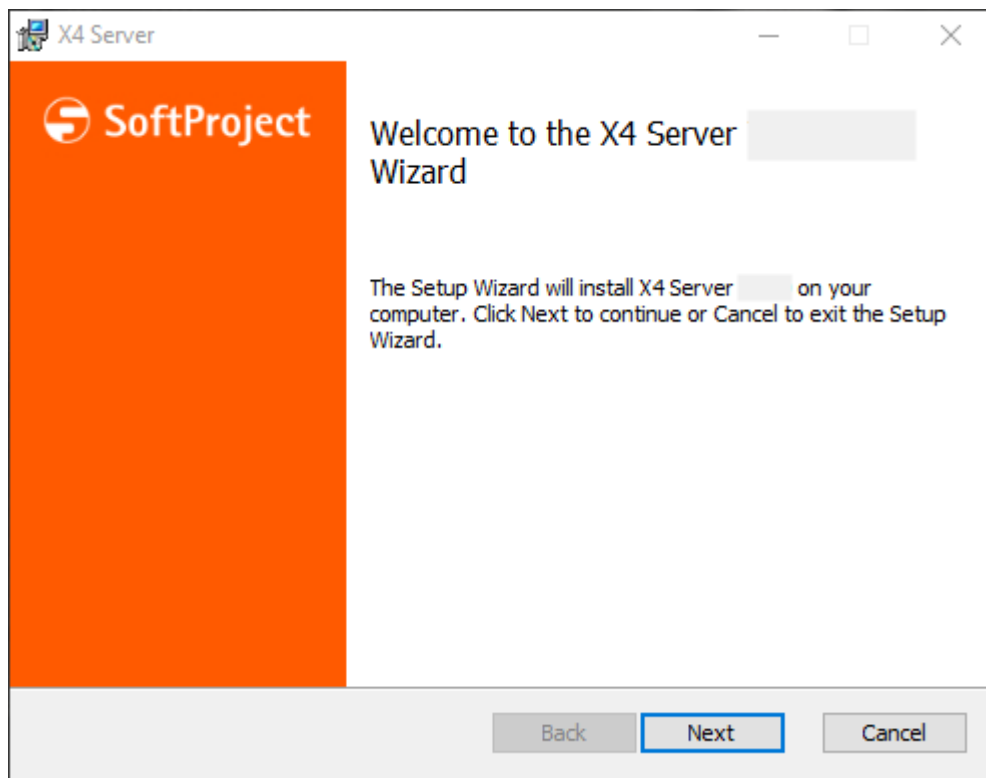
2.1.1.1 X4 Server installieren

Der X4 Server wird für **Produktionszwecke** als separates MS Windows-Installationspaket in Form einer MSI-Datei bereitgestellt.

- 
- Sie können auf einem Windows-System nur einen X4 Server installieren. Das MS Windows-Installationspaket überschreibt existierende Installationen. Wenn Sie eine existierende Installation überschreiben, kann dies zu Problemen und Datenverlust führen.
 - Um mehrere X4 Server zu Testzwecken zu verwenden, stellen wir Ihnen das **MS Windows All-in-one** Installationspaket im [Downloadbereich](#) unserer Webseite zur Verfügung.

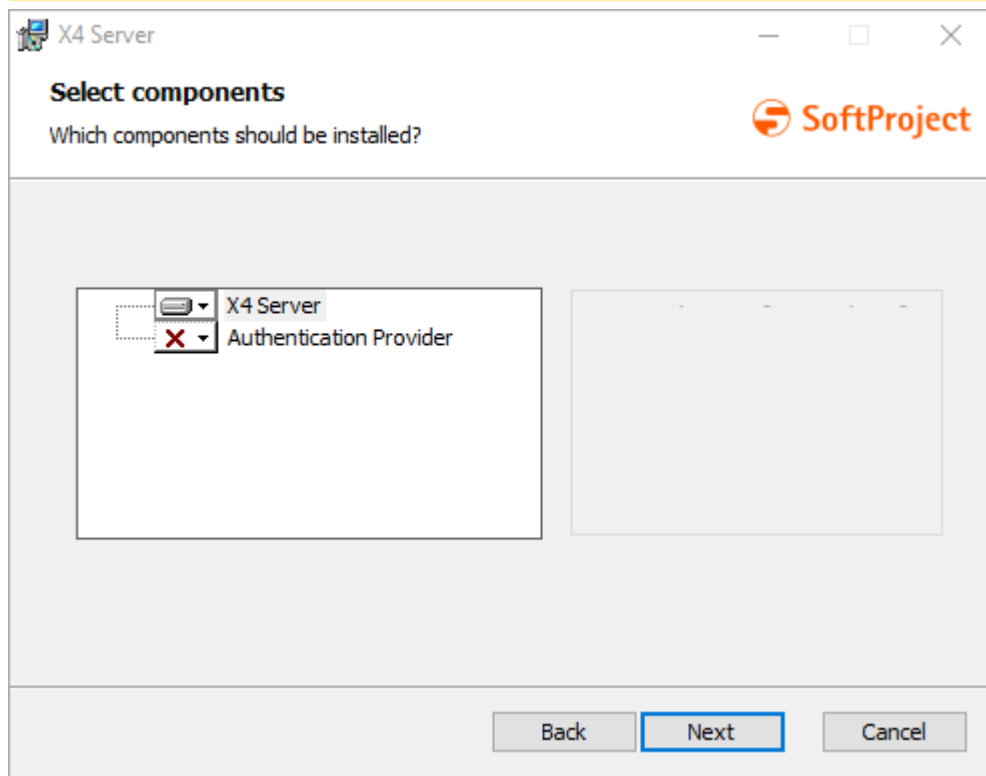
1. Das von SoftProject bereitgestellte Installationspaket `X4ServerSetup_7.v.v_64bit.msi` mit Administratorrechten oder entsprechenden Schreibrechten ausführen.

 Beim Installationsstart wird eine Warnung durch Windows Defender SmartScreen ausgegeben. **Weitere Informationen** klicken und mit **Trotzdem ausführen** die Installationsroutine wie gewohnt starten.

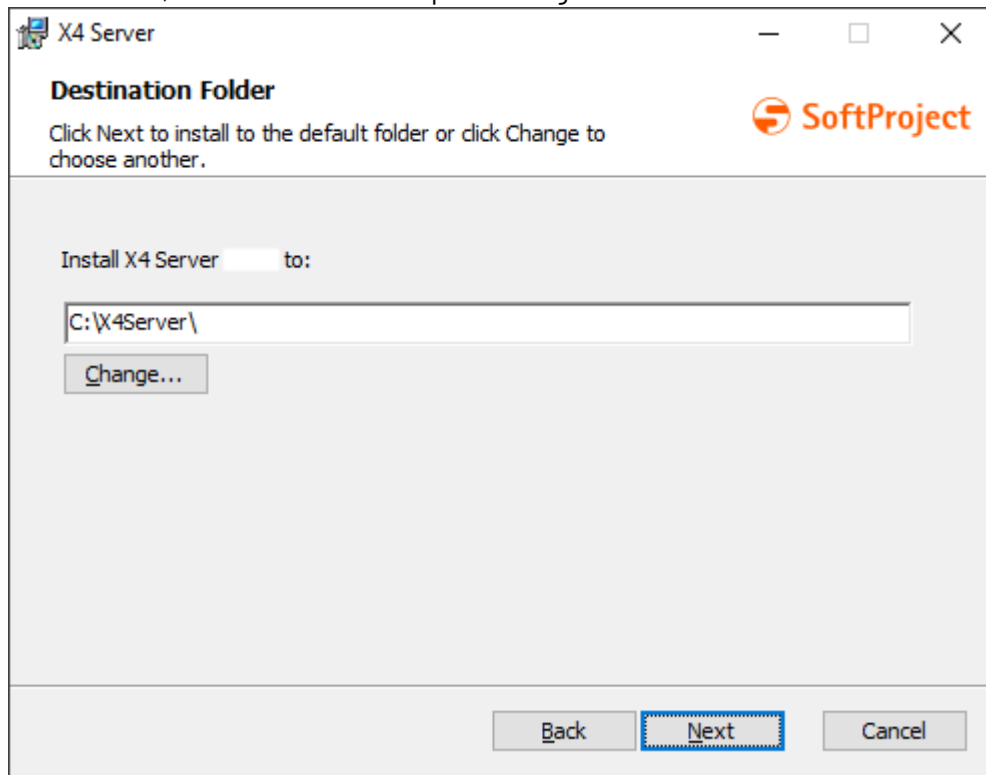


2. **Next** klicken, um die zu installierenden Komponenten auszuwählen.

⚠ Wenn Sie keinen Authentication Provider im Einsatz haben, müssen Sie die mitgelieferte Komponente **Authentication Provider** installieren.



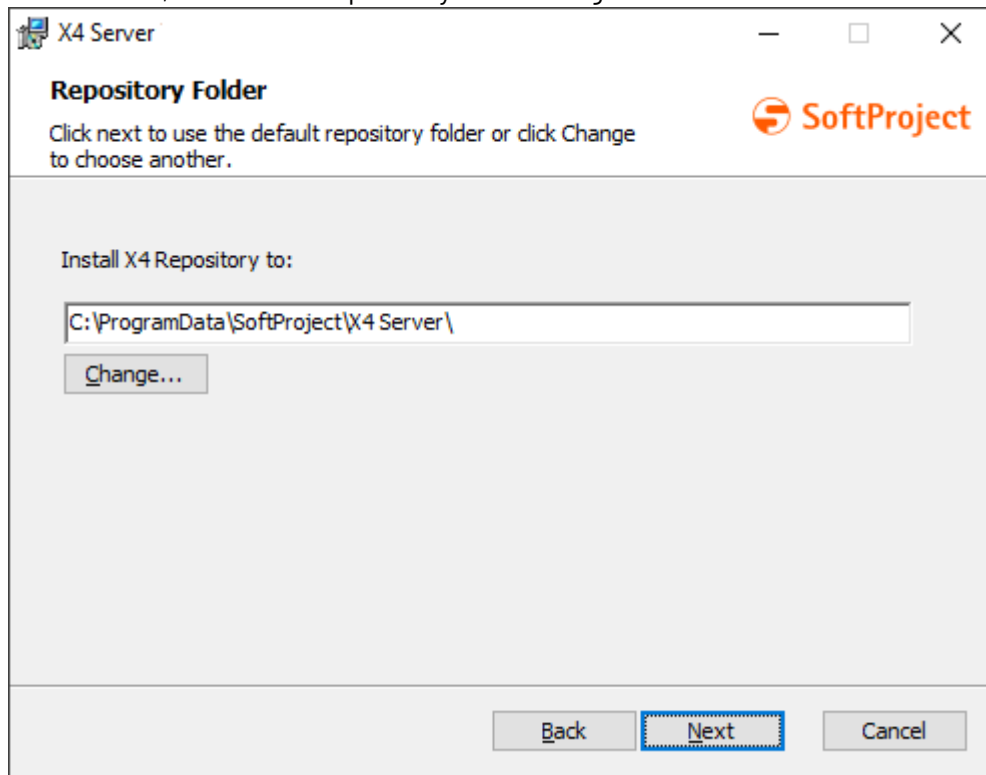
3. **Next** klicken, um den Installationspfad anzugeben.



 Standardmäßig wird der X4 Server unter C:\X4Server_7.v.v.\ installiert, über **Change** lässt sich der Installationspfad jedoch ändern.

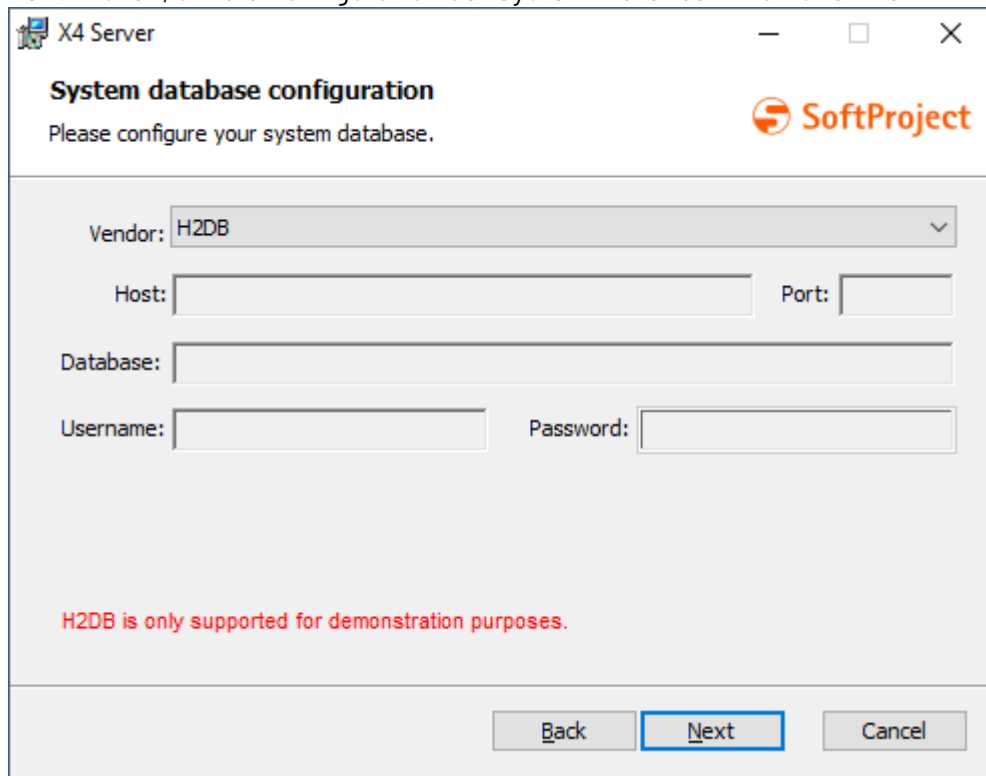
 Verwenden Sie keine Leerzeichen im Installationspfad. Bei der Installation des X4 Servers als Dienst kann dies zu Fehlern führen.

4. **Next** klicken, um den X4 Repository-Pfad anzugeben.



- ① Standardmäßig wird das X4 Repository unter C:\ProgramData\SoftProject\X4Server\ installiert, über **Change** lässt sich der Pfad jedoch ändern.

5. **Next** klicken, um die Konfiguration der System-Datenbank vorzunehmen.



6. System-Datenbank konfigurieren:

- **Vendor:** Zu verwendende Datenbank angeben

- H2DB

 Beachten Sie, dass H2DB nicht für den Produktiveinsatz geeignet ist!

- Microsoft SQL Server
- Oracle Database 11g

 Beachten Sie, dass der Datenbank-Treiber für Oracle Database 11g nicht im Installationspaket enthalten ist. Der entsprechenden Treiber muss gesondert installiert werden, siehe auch [Oracle-Datenbank einrichten](#).

- Oracle Database 12c/18c/19c

⚠ Beachten Sie, dass der Datenbank-Treiber für Oracle Database 12c/18c/19c nicht im Installationspaket enthalten ist. Der entsprechenden Treiber muss gesondert installiert werden, siehe auch [Oracle-Datenbank einrichten](#).

- PostgreSQL
- **Host:** Datenbank-Host angeben
- **Port:** Datenbank-Port angeben
- **Database:** Datenbank angeben
- **Authentication:** Authentifizierung mit SQL Server Authentication oder Windows Authentication angeben

i Dieser Parameter ist nur für Microsoft SQL Server verfügbar.
Wird Windows Authentication als Authentifizierung angegeben, müssen die Zugangsdaten **Username** und **Password** nicht angegeben werden, da diese den Windows-Zugangsdaten entsprechen.

- **Username:** Benutzernamen für die Datenbankverbindung angeben
- **Password:** Passwort für die Datenbankverbindung angeben

7. **Next** klicken, um die X4 Server-Konfiguration vorzunehmen.

8. X4 Server konfigurieren:

- **Maximum memory used by X4 Server:** Maximal genutzten Speicher angeben
- **HTTP Port:** HTTP-Port für X4 Web Apps angeben
- **Worker Thread Pool** konfigurieren:

- **Task core threads:** Anfängliche Anzahl von Threads im Threadpool



- Diese Zahl ist die minimale Anzahl der Threads, die der Server verwendet.
- Die Anzahl der Kern-Threads sollte in der Lage sein, die normale Anforderungslast zu bewältigen.

- **Task max threads:** Maximale Anzahl von Threads im Threadpool



- Ist kein Wert angegeben, wird der Standardwert verwendet. Der Standardwert wird durch die Formel $\text{CPU-Anzahl} * 16$ berechnet wird, sofern die JMX-Eigenschaft `MaxFileDescriptorCount` diese Zahl zulässt, andernfalls wird bei der Berechnung `max` berücksichtigt, um die Zahl entsprechend anzupassen.
- Diese Eigenschaft hängt von der Server-Hardware ab, da die Hardware eine maximale Anzahl von Threads zur Verfügung stellen kann. Sie wird verwendet, um die maximale Zuweisung von Systemressourcen bei hoher Last zu steuern.
- Die Anzahl der Threads liegt zwischen der anfänglichen Anzahl und der maximalen Anzahl von Threads im Threadpool.

- **Default timeout:** Standard-Transaktionslaufzeit in Sekunden



Bei langlaufende Transaktionen kann es in WildFly während der EJB-Verarbeitungsmethode zu einer Zeitüberschreitung kommen. In diesem Fall können Sie die Standard-Transaktionslaufzeit von 300 Sekunden über die Datei `standalone.xml` ändern.

- **Install as Microsoft Windows service :** Aktivieren, wenn der X4 Server als Service installiert werden soll
- **Create a shortcut for X4 Server on the desktop:** Aktivieren, wenn eine Desktop-Verknüpfungen für den X4 Server erstellt werden soll



Diese Option ist verfügbar, wenn `Install as Microsoft service` deaktiviert ist.

9. **Next** klicken, um die Netzwerk-Konfiguration für den X4 Server vorzunehmen.

- Address binding: Adressen-Binding angeben
- Any address: Beliebige Adresse

 Beachten Sie, dass mit der Angabe Any Address der X4 Server öffentlich zugänglich ist.

- IP Address/Domain: Spezielle IP-Adresse und Domain
 - **IP Address / Domain:** IP-Adresse und Domain angeben
10. **Next** klicken, um die Angaben zu bestätigen.
 11. **Install** klicken, um die Installation durchzuführen.
Der X4 Server wird nun installiert.
 12. Bei Bedarf die Option **Launch X4 Server when setup exists** aktivieren, um den Server nach der Installation zu starten.
 13. **Finish** klicken, um die Installation zu beenden.
Die Installation ist nun vollständig.
 14. Prüfen, ob im Server-Protokoll Fehlermeldungen auftraten.
Ein korrekt installierter und gestarteter X4 Server gibt im Server-Protokoll keine Fehlermeldungen (ERROR oder FATAL) aus.

2.1.1.2 Bestehende Installation ab Version 5.5.4 aktualisieren

 Sollten Sie eine ältere Version installiert haben, müssen Sie zuerst auf die Version 5.5.4 aktualisieren.

Das aktuelle Update Tool finden Sie im Download-Bereich auf unserer Website. Weitere Informationen entnehmen Sie der README.txt im Update Tool.

2.1.1.3 Parameter der unbeaufsichtigten Installation

Um eine unbeaufsichtigte Installation mit der Kommandozeile durchzuführen, müssen folgende Parameter gesetzt werden:

 Bei fehlender Angabe eines Parameters wird bei der Installation der Standard-Wert verwendet.

Parameter	Beschreibung
INSTALLFOLDER	Installationspfad Mögliche Werte • Pfadangabe (Standard: C:\X4Server_<version>\)
PRODUCTNAMEDIRECTORY	X4 Repository-Ordner • Pfadangabe (Standard: C:\ProgramData\SoftProject\X4Server\)  Verwenden Sie keine Leerzeichen im Installationspfad. Bei der Installation des X4 Servers als Dienst kann dies zu Fehlern führen.
INSTALLSERVICE	X4 Server als Windows-Dienst installieren Mögliche Werte • True (Standard): X4 Server wird als Windows-Dienst installiert • False: X4 Server wird nicht als Windows-Dienst installiert
INSTALLDESKTOPSHORTCUT	X4 Server-Desktopverknüpfung erstellen (nur möglich, wenn X4 Server nicht als Windows-Dienst installiert wird) Mögliche Werte • True (Standard): Desktopverknüpfung wird erstellt • False: Desktopverknüpfung wird nicht erstellt
DATABASETYPE	Datenbank-Typ Mögliche Werte • h2 (Standard): H2 • postgresql: PostgreSQL • sqlserver: Microsoft SQL Server • oracle11: Oracle Database 11g • oracle12: Oracle Database 12c/18c/19c

Parameter	Beschreibung
HOSTDB	Datenbankhost IP-Adresse (Beispiel: 127.0.0.1)
PORTDB	Datenbankport Ganze Zahlen (Beispiel: 3307)
DATABASENAME	Datenbankname
USERNAMEDB	Benutzername zur Authentifizierung an der Datenbank
PASSWORDDB	Passwort zur Authentifizierung an der Datenbank
MEMORY	Maximal verwendeter Arbeitsspeicher in MB Ganze Zahlen (Standard: 2048)
HTTPPORT	HTTP-Port Ganze Zahlen (Standard: 8080)
AUTHENTICATION_SQLSERVER	Authentifizierungstyp der Datenbank Mögliche Werte - sqlserver (Standard) - windows
TASKCORETHREADS	Minimale Anzahl von Threads Mögliche Werte Ganze Zahlen (Standard: 8)
TASKMAXTHREADS	Maximale Anzahl von Threads Mögliche Werte Ganze Zahlen (Standard: 16)
DEFAULTTIMEOUT	Zeitüberschreitung in Sekunden Mögliche Werte Ganze Zahlen (Standard: 300)
ADDRESSTYPE	Adresstyp Mögliche Werte - anyAddress (Standard): beliebige Adresse  Beachten Sie, dass der X4 Server mit dieser Konfiguration für jeden zugänglich ist. - ipDomain: IP-Adresse/Domain

Parameter	Beschreibung
EXTERNALLIP	IP-Adresse/Domain (nur relevant, wenn ADDRESSTYPE=ipDomain) Mögliche Werte IP-Adresse (Beispiel: 127.0.0.1)

2.1.2 Installation auf Ubuntu/Debian Linux Systemen

Wie sich der komplette X4 Server und Keycloak auf Basis eines Debian-Pakets (.deb) automatisch auf einem Ubuntu- bzw. Debian-Linux-System installieren, als Dienst registrieren, starten und verwalten lässt, wird im Folgenden beschrieben.

2.1.2.1 X4 Server installieren

Beachten Sie!

- Das Installationspaket wird mit sudo-Berechtigungen gestartet.
- Während der Installation des X4 Servers werden ein neuer Benutzer X4 und eine neue Gruppe X4 angelegt.
- Nach der Installation gehört das X4 Server-Dateisystem dem Benutzer X4 und der Gruppe X4.
- Der installierte Dienst X4-Server wird zwar mit sudo-Berechtigungen gestartet, jedoch ist der Benutzer X4 Eigentümer dieser Dienstaufführung.
- Stellen Sie sicher, dass Sie über die entsprechenden Rechte für den angegebenen Installationspfad verfügt.

1. Das von SoftProject bereitgestellte Debian-Paket X4-Server_Ubuntu-7.v.v-r.x86_64 auf das Ubuntu- bzw. Debian-System laden.
2. Die Installation mit dem Befehl `sudo dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb` ausführen.

 Wenn Sie den Authentifizierungsprovider Keycloak nicht installieren möchten, verwenden Sie den Befehl `sudo X4_INSTALL_AUTH_PROVIDER=no dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb`.

Beispiel: `sudo dpkg -i X4-Server_Ubuntu-7.0.0-1.x86_64.deb` für Release 1 der X4 Server-Version 7.0.0.

 Der X4 Server wird standardmäßig unter /opt/X4 installiert. Mit der Variablen `INSTALL_PATH` kann der Installationspfad geändert werden, z.B. `sudo INSTALL_PATH=/myNewPath/Tools dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb`

Der X4 Server wird nun im angegebenen Ordner installiert, als Dienst X4-Server registriert und direkt gestartet. Dieser Vorgang kann einige Sekunden dauern.



- Falls bereits eine Installation des X4 Servers vorhanden ist, werden die zentralen Bestandteile des X4 Servers bei erneutem Ausführung des Installationsbefehls `sudo dpkg -i X4-Server_Ubuntu-7.v.v-r.x86_64.deb` automatisch aktualisiert. Im Unterordner `/opt/X4_backups` werden dabei Sicherungskopien der Konfigurationsdateien erstellt.
- Um Dateien zu migrieren, die nicht Teil des automatischen Update-Prozesses sind, muss im Installations- und Migrationswerkzeug der Installationspfad der X4 BPMS angegeben werden. Mit der Angabe `/opt/X4/jdk/bin/java -jar de.softproject.x4.database-6.3.0.jar --installX4path /opt/X4/Server` werden beispielsweise alle `.war`-Dateien, die nicht bereits automatisch migriert wurden, in die neue Installation migriert.

- Prüfen, ob im Server-Protokoll `/opt/X4/wildfly/standalone/log/server.log` Fehlermeldungen auftraten.
Ein korrekt installierter und gestarteter X4 Server gibt im Server-Protokoll keine Fehlermeldungen (ERROR oder FATAL) aus. Dies sollte spätestens beim zweiten Start des X4 Servers der Fall sein.
- Prüfen, ob im Server-Protokoll `/opt/X4/keycloak/standalone/log/server.log` Fehlermeldungen auftraten.
Ein korrekt installierter und gestarteter Keycloak gibt im Server-Protokoll keine Fehlermeldungen (ERROR oder FATAL) aus. Dies sollte spätestens beim zweiten Start des Keycloaks der Fall sein.
- Den X4 Server mit dem Befehl `sudo service X4-Server restart` neu starten.
Der X4 Server wurde erfolgreich installiert und wird als Dienst X4-Server ausgeführt.
- Den Keycloak mit dem Befehl `sudo service X4-Authentication-Provider restart` neu starten.
Der Keycloak wurde erfolgreich installiert.

Nach erfolgreicher Installation bzw. Aktualisierung des X4 Servers über ein Debian-Paket enthält der Installationsordner folgende Elemente:

Ordner	Erläuterung
jdk	Enthält die aktuelle Java Runtime Version als Laufzeitumgebung für den WildFly Applikations Server
SQL	Enthält in Unterordner H2DB die mitgelieferte In-Memory-Datenbank für Testzwecke
wildfly	Enthält den vorkonfigurierten WildFly Applikations Server
keycloak	Enthält Keycloak
X4DB	Enthält das zentrale X4 Repository
x4.license	Lizenzdatei für den X4 Server, siehe Lizenzen über den Designer installieren

Ordner	Erläuterung
X4config.xml	Zentrale Konfigurationsdatei des X4 Servers, siehe Konfiguration über X4config.xml

2.1.2.2 Steuerungsmöglichkeiten für den Dienst X4-Server

Über die Kommandozeile stehen folgende Optionen zur Verfügung, um den X4 Server bzw. dessen Dienst X4-Server zu steuern:

Dienst X4-Server starten:	Befehl <code>service X4-Server start</code> ausführen.
Dienst X4-Server stoppen:	Befehl <code>service X4-Server stop</code> ausführen.
Dienst X4-Server neu starten:	Befehl <code>service X4-Server restart</code> ausführen.

2.1.2.3 Steuerungsmöglichkeiten für den Keycloak

Über die Kommandozeile stehen folgende Optionen zur Verfügung, um den Keycloak X4-Authentication-Provider zu steuern:

Dienst X4-Authentication-Provider starten:	Befehl <code>service X4-Authentication-Provider</code> ausführen.
Dienst X4-Authentication-Provider stoppen:	Befehl <code>service X4-Authentication-Provider</code> ausführen.
Dienst X4-Authentication-Provider neu starten:	Befehl <code>service X4-Authentication-Provider</code> ausführen.

2.1.2.4 Dienst X4-Server deinstallieren

Um einen via Debian-Paket installierten X4 Server und dessen entsprechenden Dienst X4-Server zu deinstallieren, den Befehl `sudo dpkg -r X4-Server` eingeben.

Das rückstandslose Entfernen aller Installationsartefakte inklusive Konfigurationsdateien etc. zum Dienst X4-Server ist über den Befehl `sudo dpkg -P X4-Server` möglich.

 Beim Deinstallieren ist das Setzen der Variablen `INSTALL_PATH` nicht notwendig.

2.1.3 Installation auf Red Hat Enterprise Linux Systemen

Wie sich der komplette X4 Server auf Basis eines RPM-Pakets (.rpm) automatisch auf einem Red Hat Enterprise Linux System installieren, als Dienst registrieren, starten und verwalten lässt, wird im Folgenden beschrieben.

2.1.3.1 X4 Server installieren

- ① Stellen Sie vor der Installation sicher, dass unter `/etc/hosts` die IP-Adresse des Servers und der Host-Name eingetragen sind.

Beispiel: 192.168.147.153 vmettopensuse01

① **Beachten Sie!**

- Das Installationspaket wird mit `sudo`-Berechtigungen gestartet.
- Während der Installation des X4 Servers werden ein neuer Benutzer X4 und eine neue Gruppe X4 angelegt.
- Nach der Installation gehört das X4 Server-Dateisystem dem Benutzer X4 und der Gruppe X4.
- Der installierte Dienst X4-Server wird zwar mit `sudo`-Berechtigungen gestartet, jedoch ist der Benutzer X4 Eigentümer dieser Dienstaufführung.
- Stellen Sie sicher, dass Sie über die entsprechenden Rechte für den angegebenen Installationspfad verfügt.

1. Das von SoftProject bereitgestellte RPM-Paket `X4-Server_RHEL-7.v.v-r.x86_64.rpm` auf das Red-Hat-System laden.
2. Die Installation mit dem Befehl `sudo rpm -i X4-Server_RHEL-7.v.v-r.x86_64.rpm` ausführen.

Beispiel: `sudo rpm -i X4-Server_RHEL-7.0.0-1.x86_64.rpm` für Release 1 der X4 Server-Version 7.0.0.

- ① Der X4 Server wird standardmäßig unter `/opt/X4` installiert. Mit dem Parameter `--prefix` kann der Installationspfad geändert werden, z.B. `sudo rpm -i X4-Server_RHEL-7.v.v-r.x86_64.rpm --prefix=/new_path`

Der X4 Server wird nun im angegebenen Ordner installiert, als Dienst X4-Server registriert und direkt gestartet. Dieser Vorgang kann einige Sekunden dauern.

3. Ggf. Ihre Lizenzdatei `x4.license` in den Installationsordner des X4 Servers kopieren.
Beispiel: `sudo cp x4.license /opt/X4`
4. Ggf. prüfen, ob im Server-Protokoll `/opt/X4/wildfly/standalone/log/server.log` Fehlermeldungen auftraten.
Ein korrekt installierter und gestarteter X4 Server gibt im Server-Protokoll keine Fehlermeldungen (ERROR oder FATAL) aus. Dies sollte spätestens beim zweiten Start des X4 Servers der Fall sein.
5. Ggf. prüfen, ob im Keycloak-Protokoll `/opt/X4/keycloak/standalone/log/server.log` Fehlermeldungen auftraten.
Ein korrekt installierter und gestarteter Keycloak gibt im Server-Protokoll keine Fehlermeldungen (ERROR oder FATAL) aus.

Nach erfolgreicher Installation bzw. Aktualisierung des X4 Servers über ein RPM-Paket enthält der Installationsordner folgende Elemente:

Ordner	Erläuterung
jdk	Enthält die aktuelle Java Runtime Version als Laufzeitumgebung für den WildFly Applikations Server
SQL	Enthält in Unterordner H2DB die mitgelieferte In-Memory-Datenbank für Testzwecke
wildfly	Enthält den vorkonfigurierten WildFly Applikations Server
keycloak	Enthält Keycloak
X4DB	Enthält das zentrale X4 Repository
x4.license	Lizenzdatei für den X4 Server, siehe Lizenzen über den Designer installieren
X4config.xml	Zentrale Konfigurationsdatei des X4 Servers, siehe Konfiguration über X4config.xml

2.1.3.2 Steuerungsmöglichkeiten für den Dienst X4-Server

Über die Kommandozeile stehen folgende Optionen zur Verfügung, um den X4 Server bzw. dessen Dienst X4-Server zu steuern:

Dienst X4-Server starten:	Befehl <code>systemctl start X4-Server</code> ausführen.
Dienst X4-Server stoppen:	Befehl <code>systemctl stop X4-Server</code> ausführen.
Dienst X4-Server neustarten:	Befehl <code>systemctl restart X4-Server</code> ausführen.
Status des Dienstes X4-Server einsehen:	Befehl <code>systemctl status X4-Server</code> ausführen.
Dienst X4-Server neu laden:	Befehl <code>systemctl reload X4-Server</code> ausführen.

2.1.3.3 Steuerungsmöglichkeiten für den KeyCloak

Über die Kommandozeile stehen folgende Optionen zur Verfügung, um den Keycloak zu steuern: X4-Authentication-Provider:

Dienst X4-Authentication-Provider starten:	Execute command <code>systemctl start X4-Authentication-Provider</code> .
Dienst X4-Authentication-Provider stoppen:	Execute command <code>systemctl stop X4-Authentication-Provider</code> .
Dienst X4-Authentication-Provider neustarten:	Execute command <code>systemctl restart X4-Authentication-Provider</code> .
Status des Dienstes X4-Authentication-Provider einsehen:	Execute command <code>systemctl status X4-Authentication-Provider</code> .

**Dienst X4-
Authentication-
Provider neu laden:**

Execute command `systemctl reload X4-Authentication-Provider`.

2.1.3.4 Dienst X4-Server deinstallieren

Um einen via RPM-Paket installierten X4 Server und dessen entsprechenden Dienst X4-Server zu deinstallieren, den Befehl `sudo rpm -e X4-Server_RHEL-7.v.v-r.x86_64` eingeben.

Bei der Deinstallation werden automatisch Sicherungskopien der Konfigurationsdateien, der Systemdatenbank und der X4DB unter `opt/x4_backups` erstellt.

2.1.4 Installation auf SuSe Linux Systemen

Wie sich der komplette X4 Server auf Basis eines RPM-Pakets (.rpm) automatisch auf einem Open-Suse-Linux-System installieren, als Dienst registrieren, starten und verwalten lässt, wird im Folgenden beschrieben.

2.1.4.1 X4 Server installieren

Voraussetzung

- Das Paket **insserv-compat** wurde installiert.
Das Paket kann in der Kommandozeile mit folgendem Kommando installiert werden: `zypper install insserv-compat`

i Stellen Sie vor der Installation sicher, dass unter `/etc/hosts` die IP-Adresse des Servers und der Host-Name eingetragen sind.

Beispiel: 192.168.147.153 vmnettopensuse01

i **Beachten Sie!**

- Das Installationspaket wird mit `sudo`-Berechtigungen gestartet.
- Während der Installation des X4 Servers werden ein neuer Benutzer X4 und eine neue Gruppe X4 angelegt.
- Nach der Installation gehört das X4 Server-Dateisystem dem Benutzer X4 und der Gruppe X4.
- Der installierte Dienst X4-Server wird zwar mit `sudo`-Berechtigungen gestartet, jedoch ist der Benutzer X4 Eigentümer dieser Dienstaufführung.
- Stellen Sie sicher, dass Sie über die entsprechenden Rechte für den angegebenen Installationspfad verfügt.

1. Das von SoftProject bereitgestellte RPM-Paket `X4-Server_SLES-7.v.v-r.x86_64.rpm` auf das Suse-Linux-System laden.

- Die Installation mit dem Befehl `sudo rpm -i X4-Server_SLES-7.v.v-r.x86_64.rpm` ausführen.

Beispiel: `sudo rpm -i X4-Server_SLES-7.0.0-1.x86_64.rpm` für Release 1 der X4 Server-Version 7.0.0.

i Der X4 Server wird standardmäßig unter `/opt/X4` installiert. Mit dem Parameter `--prefix` kann der Installationspfad geändert werden, z.B. `sudo rpm -i X4-Server_SLES-7.v.v-r.x86_64.rpm --prefix=/new_path`

Der X4 Server wird nun im angegebenen Ordner installiert, als Dienst `X4-Server` registriert und direkt gestartet. Dieser Vorgang kann einige Sekunden dauern.

i Um Dateien zu migrieren, die nicht Teil des automatischen Update-Prozesses sind, muss im Installations- und Migrationswerkzeug der Installationspfad der X4 BPMS angegeben werden. Mit der Angabe `/opt/X4/jdk/bin/java -jar de.softproject.x4.database-7.0.0.jar --installX4path /opt/X4/Server` werden beispielsweise alle `.war`-Dateien, die nicht bereits automatisch migriert wurden, in die neue Installation migriert.

- Ggf. Ihre Lizenzdatei `x4.license` in den Installationsordner des X4 Servers kopieren.

Beispiel: `sudo cp x4.license /opt/X4`

- Prüfen, ob im Server-Protokoll `/opt/X4/wildfly/standalone/log/server.log` Fehlermeldungen auftraten.

Ein korrekt installierter und gestarteter X4 Server gibt im Server-Protokoll keine Fehlermeldungen (ERROR oder FATAL) aus. Dies sollte spätestens beim zweiten Start des X4 Servers der Fall sein.

Nach erfolgreicher Installation bzw. Aktualisierung des X4 Servers über ein RPM-Paket enthält der Installationsordner folgende Elemente:

Ordner	Erläuterung
jdk	Enthält die aktuelle Java Runtime Version als Laufzeitumgebung für den WildFly Applikations Server
SQL	Enthält in Unterordner H2DB die mitgelieferte In-Memory-Datenbank für Testzwecke
wildfly	Enthält den vorkonfigurierten WildFly Applikations Server
X4DB	Enthält das zentrale X4 Repository
x4.license	Lizenzdatei für den X4 Server, siehe Lizenzen über den Designer installieren
X4config.xml	Zentrale Konfigurationsdatei des X4 Servers, siehe Konfiguration über X4config.xml

2.1.4.2 Steuerungsmöglichkeiten für den Dienst X4-Server

Über die Kommandozeile stehen folgende Optionen zur Verfügung, um den X4 Server bzw. dessen Dienst X4-Server zu steuern:

Dienst X4-Server starten:	Befehl <code>systemctl start X4-Server</code> oder <code>service X4-Server start</code> ausführen.
Dienst X4-Server stoppen:	Befehl <code>systemctl stop X4-Server</code> oder <code>service X4-Server stop</code> ausführen.
Dienst X4-Server neustarten:	Befehl <code>systemctl restart X4-Server</code> oder <code>service X4-Server restart</code> ausführen.
Status des Dienstes X4-Server einsehen:	Befehl <code>systemctl status X4-Server</code> oder <code>service X4-Server status</code> ausführen.
Dienst X4-Server neu laden:	Befehl <code>systemctl reload X4-Server</code> oder <code>service X4-Server reload</code> ausführen.

2.1.4.3 Dienst X4-Server deinstallieren

Um einen via RPM-Paket installierten X4 Server und dessen entsprechenden Dienst X4-Server zu deinstallieren, den Befehl `sudo rpm -e X4-Server_SLES-7.v.v-r.x86_64.` eingeben.

Bei der Deinstallation werden automatisch Sicherungskopien der Konfigurationsdateien, der Systemdatenbank und der X4DB unter `opt/x4_backups` erstellt.

2.1.5 X4 Server in Docker installieren

In diesem Abschnitt erfahren Sie wie sich der X4 Server in Docker installieren und als Docker-Container starten lässt.

Voraussetzungen

- Docker muss auf dem System installiert und eingerichtet sein. Informationen hierzu finden Sie in der Docker-Dokumentation unter <https://docs.docker.com/>.
- Kenntnisse der Docker-Funktionsweise werden vorausgesetzt.
- `x4_server:7.v.v` bezieht sich auf die aktuelle X4 BPMS Version.

1. Docker mit dem Kommando `docker run -d -p 8080:8080 --name x4-servercontainer softproject/x4_server` ausführen.

Weitere hilfreiche Befehle:

Anwendungsbeispiele	Kommando
Container ausführen und Logs nach dem Anlegen des Containers anzeigen	<code>docker run -d -p 8080:8080 --name x4-server-container softproject/x4_server && docker logs x4-server-container</code>
X4 Server mit einer PostgreSQL-Datenbank namens X4 ausführen - Host: 10.0.75.1 - postgreSQL-Standardport: 5432	<code>docker run -d -p 8080:8080 -e DATABASE_MODE='postgresql' -e DATABASE_HOST='10.0.75.1' softproject/x4_server</code>
X4 Server mit Port 8081 und einer PostgreSQL-Datenbank namens X4 ausführen - 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>
X4 Server mit Port 8081 und einer PostgreSQL-Datenbank namens X4 ausführen - Zugangsdaten: 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>
X4 Server mit einer MS-SQL-Datenbank namens X4 ausführen - Zugangsdaten: 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>
X4 Server ausführen und dabei das X4DB-Verzeichnis von einem externen Pfad auf das X4DB-Verzeichnis innerhalb des Containers mappen (nur unter Linux)	<code>docker run -d -p 8080:8080 -v /home/anyUser/X4/X4DB/1:/opt/X4/X4DB/1 softproject/x4_server</code>

Umgebungsvariablen:

Variable	Erläuterung
X4_UID	Unix Benutzer-ID unter der der technische Prozess ausgeführt wird
X4_GID	Unix Gruppen-ID unter der der technische Prozess ausgeführt wird
JAVA_XMS	Anfänglicher heap space für die JVM; Standardwert: 512M
JAVA_XMX	Maximaler heap space für die JVM; Standardwert: 2048M
DATABASE_MODE	Definiert die Datenbank und die Strategie für die Datenbankverbindung. Mögliche Werte sind h2 (Standard), postgresql und sqlserver.

Variable	Erläuterung
DATABASE_HOST	Host-Name des Datenbank-Servers (wenn nicht h2). Der Standardwert ist database, sodass eine Änderung erzwungen wird.
DATABASE_PORT	Port-Nummer des Datenbank-Servers (wenn nicht h2). Der Standard-Port für den PostgreSQL-Server (postgres) ist 5432. Der Standard-Port wird nicht automatisch gesetzt.
DATABASE_NAME	Name der Datenbank, die auf dem Datenbank-Server gehostet wird und für den X4 Server verwendet werden soll (wenn nicht h2).
DATABASE_USER	Name des Datenbank-Benutzers
DATABASE_PASSWORD	Passwort für den Datenbank-Zugriff

2.1.6 X4 Server auf anderen Betriebssystemen installieren

Bei Bedarf lässt sich der X4 Server auch auf weiteren Betriebssystemen installieren. Für weitere Informationen hierzu nehmen Sie Kontakt mit SoftProject auf.

2.2 Lizenz initial installieren

1. In der Symbolleiste auf das -Symbol klicken.
2. **Install license** klicken.
3. X4-Lizenz wählen.
4. **Öffnen** klicken.

Ihre neue Lizenz ist nun installiert. In der Statusleiste am unteren Rand des X4 Designers sehen Sie, wie lange Ihre Lizenz noch gültig ist.

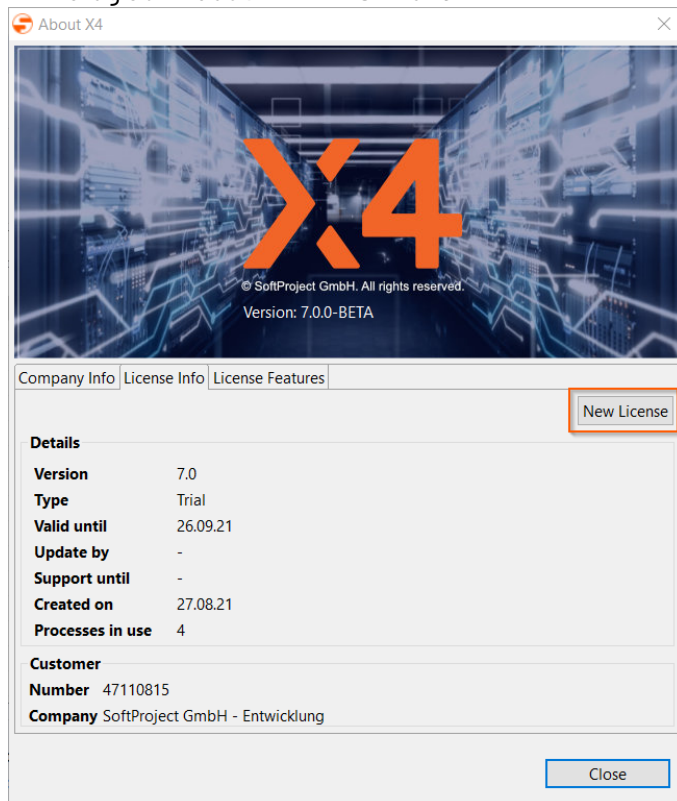
✓ Über **Help > About X4 BPMS > License Information** und **Licence Features** haben Sie jederzeit die Möglichkeit, Informationen zu Ihrer Lizenz abzurufen.

2.3 Lizenz erneuern

⚠ Um eine Lizenz zu erneuern, müssen Sie zuvor eine Lizenz installiert haben.

1. In der Menüleiste auf **Help** klicken.

- Im Dialog auf **About X4 BPMS** klicken.



- Unter **Licence Info** auf **New license** klicken.
- Zur neuen Lizenz navigieren und **Öffnen** klicken.
Bei erfolgreicher Installation aktualisieren sich die Informationen zur Lizenz nach kurzer Zeit automatisch.

2.4 Lizenz-Informationen anzeigen

 Um Lizenz-Informationen anzuzeigen, muss eine Lizenz installiert sein.

- In der Menüleiste des X4 Designers auf **Help > About X4 BPMS** klicken.
- Um die Lizenz-Informationen anzuzeigen, auf die Registerkarte **License Info** oder die Registerkarte **License Features** klicken.

2.5 X4 Designer installieren und deinstallieren

2.5.1 X4 Designer installieren

Der X4 Designer wird für **Produktionszwecke** als separates MS Windows-Installationspaket in Form einer MSI-Datei bereitgestellt.



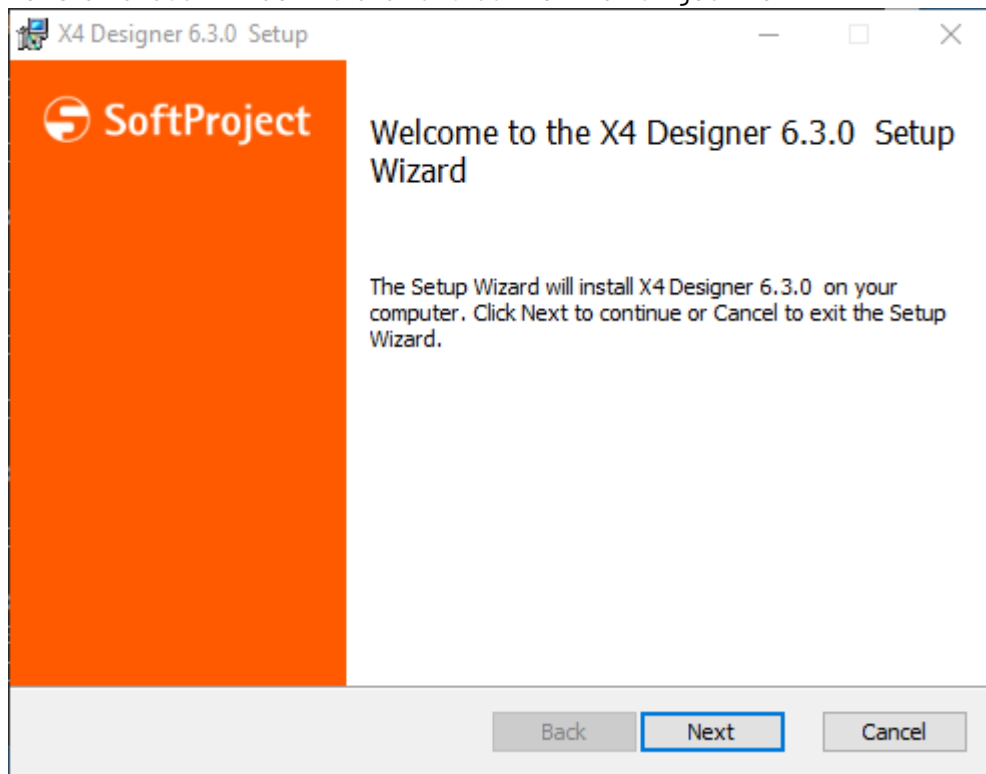
- Sie können auf einem Windows-System nur einen X4 Designer installieren. Das MS Windows-Installationspaket überschreibt existierende Installationen. Wenn Sie eine existierende Installation überschreiben, kann dies zu Problemen und Datenverlust führen.
- Um mehrere X4 Designer zu Testzwecken zu verwenden, stellen wir Ihnen das **MS Windows All-in-one** Installationspaket im [Downloadbereich](#) unserer Webseite zur Verfügung.

1. Die ausführbare Datei X4Designer_Setup.msi doppelklicken, um die Installation zu beginnen.



Beim Installationsstart wird eine Warnung durch Windows Defender SmartScreen ausgegeben. **Weitere Informationen** klicken und mit **Trotzdem ausführen** die Installationsroutine wie gewohnt starten.

Der Startbildschirm der Installationsroutine wird nun geöffnet.



2. **Next** klicken.
3. Den Installationspfad für den X4 Designer angeben.
4. Durch Aktivieren der Option **Create a shortcut for X4 Designer on the desktop** ggf. eine Verknüpfung auf den Desktop erstellen.
5. **Next** klicken, um den Pfad zu bestätigen.
6. **Install** klicken, um die Installation auszuführen.
Der Fortschritt der Installation wird nun angezeigt.

7. **Finish** klicken, um die Installation zu beenden.

✓ Durch Aktivieren der Option **Launch X4 Designer when setup exists**, wird der X4 Designer sofort nach der Installation gestartet.

Der X4 Designer wurde nun unter dem angegebenen Pfad installiert.

8. Falls nicht bereits automatisch passiert, X4 Designer starten, um die Installation zu prüfen.

✓ **Unbeaufsichtigte Installation**

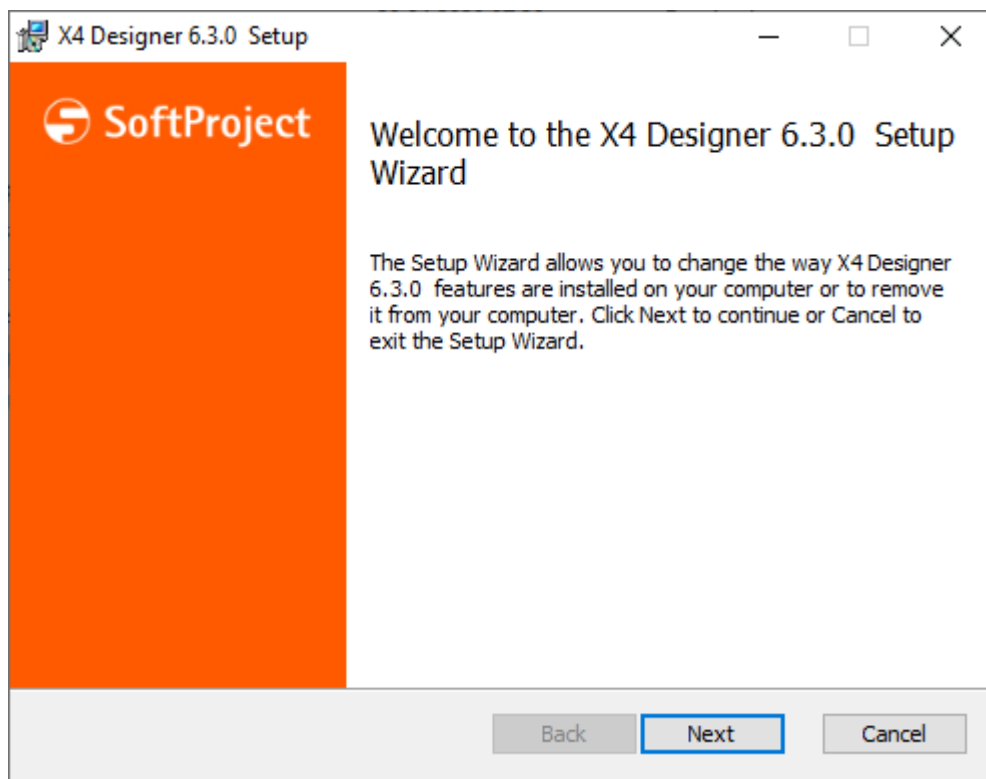
Die Installation des X4 Designers lässt sich auch über eine unbeaufsichtigte Installation durchführen. Geben Sie dazu z.B. folgenden Befehl in der Kommandozeile ein: **C:*

*\Installationsort der MSI /q/n /L*V "C:\temp\test.log**

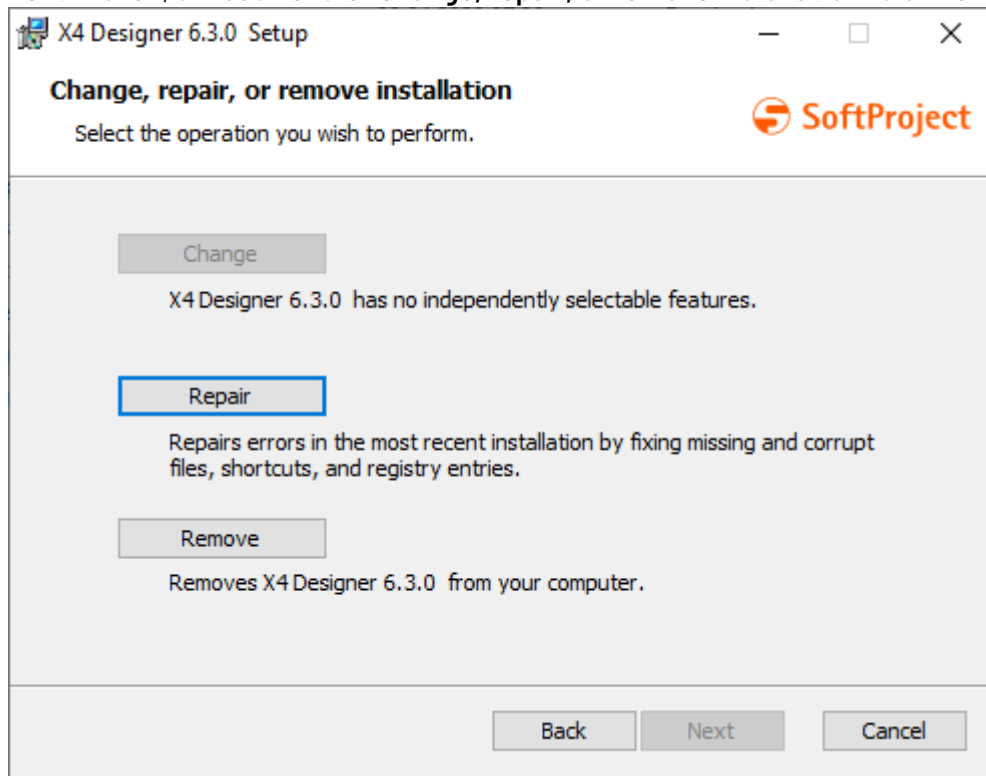
2.5.2 X4 Designer deinstallieren

Der X4 Designer lässt sich entweder über das Windows-Startmenü, die Windows-Systemsteuerung oder durch die erneute Ausführung der Installationsdatei deinstallieren.

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



3. **Next** klicken, um das Fenster **Change, repair, or remove installation** zu öffnen.



4. **Remove** klicken.
 5. Im nächsten Fenster erneut **Remove** klicken, um die Deinstallation zu beginnen. Der Fortschritt der Deinstallation wird nun angezeigt.
 6. **Finish** klicken, um die Deinstallation zu beenden. Der X4 Designer wurde nun deinstalliert.

2.5.3 Parameter der unbeaufsichtigten Installation

Um eine unbeaufsichtigte Installation mit der Kommandozeile durchzuführen, müssen folgende Parameter gesetzt werden:

Parameter	Beschreibung
INSTALLFOLDER	Installationspfad

2.6 Installation und Migration der System-Datenbank und der X4DB

Das Update Tool können Sie auf unserer Website im Download-Bereich herunterladen.

2.7 Installation des Authentifizierungsproviders

Der Authentifizierungsprovider Keycloak ist in dem X4 Server-Installationspaket enthalten.

Wenn Sie den Authentifizierungsprovider Keycloak als Docker-Container starten möchten, müssen Sie das Docker-Image laden.



Weitere Informationen finden Sie im Abschnitt [Docker-Image laden und Container starten](#).

3 Konfiguration

3.1 X4 Server konfigurieren

Erfahren Sie, wie Sie die Konfiguration des *X4 Servers* an Ihre Gegebenheiten anpassen.

3.1.1 Datenbank einrichten

- Oracle-Datenbank einrichten
- Konfiguration für MSSQL und PostgreSQL

3.1.1.1 Oracle-Datenbank einrichten

Sollten Sie eine Oracle-Datenbank verwenden, müssen folgende zusätzlichen Einstellungen vorgenommen werden:

Migrations/Installations-Werkzeug ausführen

ⓘ Beachten Sie:

- Vor dem Ausführen des Migrations-/Installations-Tools, muss zunächst eine leere Datenbank mit dem Namen X4 angelegt werden.
- Um das Migrations-Werkzeug (siehe [Installation und Migration der System-Datenbank und der X4DB](#)) mit Oracle verwenden zu können, muss beim Aufruf des Tools der Oracle-Treiber dem Classpath hinzugefügt werden.
Treiber für die entsprechende Oracle Datenbank finden Sie unter <https://www.oracle.com/database/technologies/appdev/jdbc.html>.

Treiber als Wildfly-Modul bereitstellen

1. Entsprechenden Treiber unter <https://www.oracle.com/database/technologies/appdev/jdbc.html> herunterladen.
2. Wildfly-Modul für den JDBC-Treiber erstellen. Dazu im Verzeichnis `X4\Server\wildfly\modules\` zunächst die Verzeichnis-Struktur `oracle\jdbc\main` anlegen.
3. JDBC-Treiber (z. B.: `ojdbc.jar`) im oben angelegten Verzeichnis entpacken.
4. Die Datei `module.xml` mit folgendem Inhalt anlegen:

module.xml

```
<module xmlns="urn:jboss:module:1.5" name="oracle.jdbc"><!-- Der Namespace
urn:jboss:module:1.5 kann sich zwischen den Wildfly Versionen unterscheiden. --
>
  <resources>
    <resource-root path="ojdbc.jar"/><!-- Hier den Dateinamen des JDBC Treibers
angeben, der verwendet werden soll und sich im Verzeichnis befindet. -->
  </resources>
  <dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

Das Modul `oracle.jdbc` steht nun zur Verfügung.

Treiber in standalone.xml eintragen

Um den Treiber in den Datasources verwenden zu können, den Treiber in der `standalone.xml` unter `X4\Server\wildfly\standalone\configuration\` eintragen:

```
...
<subsystem xmlns="urn:jboss:domain:datasources:5.0">
  <datasources>
    ...
    <drivers>
      ...
      <driver name="oracle" module="oracle.jdbc"><!-- Hier den Modul-Namen eintragen
-->
        <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
      </driver>
    </drivers>
  </datasources>
</subsystem>
...
```

Datasources konfigurieren

Oracle-Datasources in der `standalone.xml` unter `X4\Server\wildfly\standalone\configuration\` konfigurieren:

```

...
<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><!-- Hier den entsprechenden Host, Port, SID oder Service-Namen eintragen -->
      <driver>oracle</driver><!-- Hier den Treiber-Namen eintragen -->
      <security>
        <user-name>X4SERVER</user-name>
        <password>X4</password>
      </security>
      <statement>
        <prepared-statement-cache-size>32</prepared-statement-cache-size>
      </statement>
      <!-- In <validation> und <timeout> Einstellungen zur automatischen
Verbindungsherstellung der Verbindung vornehmen -->
      <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><!-- Hier den entsprechenden Host, Port, SID oder Service-Namen eintragen -->
      <driver>oracle</driver><!-- Hier den Treiber-Namen eintragen -->
      <security>
        <user-name>X4SERVER</user-name>
        <password>X4</password>
      </security>
      <statement>
        <prepared-statement-cache-size>32</prepared-statement-cache-size>
      </statement>
      <!-- In <validation> und <timeout> Einstellungen zur automatischen
Verbindungsherstellung der Verbindung vornehmen -->
      <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>
  </datasources>

```

```
<drivers>
...
<driver name="oracle" module="oracle.jdbc"><!-- Hier den Modul-Namen eintragen
-->
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
</driver>
</drivers>
</datasources>
</subsystem>
...
```

3.1.1.2 Konfiguration für MSSQL und PostgreSQL

Sollten Sie eine PostgreSQL oder MS SQL Datenbank verwenden, müssen folgende zusätzlichen Einstellungen vorgenommen werden:

Migrations/Installations-Werkzeug ausführen

 Das Migrations/Installations-Werkzeug muss ausgeführt werden, auch wenn keine Migration einer vorhandenen Installation der X4 BPMS beabsichtigt ist, siehe [Installation und Migration der System-Datenbank und der X4DB](#).

Vor dem Ausführen des Migrations-/Installationswerkzeugs muss zunächst eine leere Datenbank mit dem Namen X4 angelegt werden.

Datasources konfigurieren

Datasources in der `standalone.xml` unter `X4\Server\wildfly\standalone\configuration\` konfigurieren:

```

...
<!-- 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> und <timeout> Einstellungen zur automatischen
Verbindungsherstellung der Verbindung vornehmen -->
  <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> und <timeout> Einstellungen zur automatischen
Verbindungsherstellung der Verbindung vornehmen -->
  <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> und <timeout> Einstellungen zur automatischen
Verbindungsherstellung der Verbindung vornehmen -->
    <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> und <timeout> Einstellungen zur automatischen
Verbindungsherstellung der Verbindung vornehmen -->
    <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 Konfiguration über X4config.xml

Über die zentrale Konfigurationsdatei `X4config.xml` lassen sich zahlreiche Einstellungen des *X4 Servers* beeinflussen.

3.1.2.1 iXServ-Konfiguration

Im Element `server > services` innerhalb der `X4config.xml` lassen sich verschiedene X4 Server-Dienste aktivieren und deaktivieren.

<snmpagent>	SNMP (Simple Network Management Protocol) aktivieren. Hierzu muss ein SNMP Trap Appender konfiguriert sein, siehe SNMP-Trap-Appender. Mögliche Werte: • <i>on</i>: SNMP-Dienst aktivieren • <i>off</i>: SNMP-Dienst deaktivieren (Standard)
<jcoserver>	SAP Java Connector-Dienst aktivieren Mögliche Werte: • <i>on</i>: JCo-Dienst aktivieren • <i>off</i>: JCo-Dienst deaktivieren (Standard)

3.1.2.2 SNMP-Konfiguration

Im Element `<snmp>` können Sie in der `X4config.xml` verschiedene Einstellungen zum Simple Network Management Protocol (SNMP) konfigurieren. Die hierfür erforderlichen MIB-Dateien können Sie beim SoftProject-Support anfragen.

<code><readCommunity></code>	SNMP Read-only Community String konfigurieren Mögliche Werte: <i>public</i> : Public (Standard)
<code><writeCommunity></code>	SNMP Write Community String konfigurieren Mögliche Werte: <i>private</i> : Private (Standard)
<code><agentPort></code>	Port, an dem der SNMP-Agent horcht Mögliche Werte: • Beliebige ganze Zahl • <i>10161</i>: Port 10161 (Standard)
<code><version></code>	Verwendete SNMP-Version Mögliche Werte: • <i>1</i>: SNMP-Version 1 verwenden • <i>2</i>: SNMP-Version 2 verwenden (Standard)

3.1.2.3 Platzhalter-Speicher-Konfiguration

Die Konfiguration eines Platzhalter-Speichers erfolgt in der `X4config.xml`. Innerhalb des Wurzelements `x4` kann ein `placeholder`-Element hinzugefügt werden, in welchem die Konfiguration vorgenommen wird.

```
<placeholder>
  <storage>
    <class>example.PlaceholderStorage</class><!-- vollqualifizierter Klassenname
der Implementierung, die verwendet werden soll. -->
    <config /><!-- Optional und abhängig vom der Platzhalter-Speicher-
Implementierung. -->
  </storage>
</placeholder>
```

3.1.2.3.1 Vorhandene Platzhalter-Speicher

Standardmäßig sind die folgenden drei Platzhalter-Speicher enthalten:

Name	Klassenname	Beschreibung
<i>Properties Placeholder Storage</i>	<code>de.softproject.integration.engine.placeholder.PropertiesPlaceholderStorage</code>	Platzhalter werden auf dem Dateisystem in <code>Properties</code> -Dateien abgelegt. Das Verzeichnis, das die Dateien enthält, ist konfigurierbar.

Name	Klassenname	Beschreibung
<i>SQL Placeholder Storage</i>	de.softproject.integration.engine.placeholder.SQLPlaceholderStorage	Platzhalter werden in einer SQL-Datenbank abgelegt. Die Ziel-Datenbank ist konfigurierbar.
<i>In-Memory Placeholder Storage</i>	de.softproject.integration.engine.placeholder.InMemoryPlaceholderStorage	Platzhalter werden im Hauptspeicher abgelegt und sind somit NICHT persistent. Ist kein oder kein gültiger Platzhalter-Speicher definiert, wird dieser als Fallback verwendet.

3.1.2.3.2 Konfiguration: Properties Placeholder Storage

Das Verzeichnis, in welchem sich die Properties-Dateien befinden, kann innerhalb des `config`-Elements wie folgt definiert werden:

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

3.1.2.3.3 Konfiguration: SQL Placeholder Storage

Die zu verwendende Datenbank kann innerhalb des `config`-Elements wie folgt definiert werden:

 Die entsprechenden Tabellen müssen im *X4Server-Schema* vorhanden sein!

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

3.1.2.4 LDAPS-Konfiguration

Um selbstsignierte Zertifikate für LDAPS zu erlauben, müssen in der Konfigurationsdatei `X4config.xml` über die Elemente `<trustStore>` und `<trustStorePassword>` der Pfad zum Truststore und das entsprechende Passwort angegeben werden.

⚠ Sie können nur einen Truststore angeben. Der angegebene Truststore hat Auswirkungen auf die HTTPS-Konfiguration und die Verwendung von Zertifikaten.

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

3.1.3 Logging/Protokollierung konfigurieren

Wie sich das Protokollierungsverhalten des *X4 Servers* beeinflussen lässt.

3.1.3.1 Save Point Konfiguration für den X4 Server

Das Save Point Konfiguration für den X4 Server lässt sich über die `X4config.xml` konfigurieren. Folgende Parameter lassen sich dabei definieren:

Beispielhafte Logging-Konfiguration

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

Erläuterung der Parameter des savepoint-Elements:

Attribut	Beschreibung
storage	Definiert den Speicherort für die Verarbeitung von Save Points im X4 Server <i>Mögliche Werte:</i> <i>filesystem</i>: Save Points werden ins Dateisystem, in das Server-Verzeichnis savepoints geschrieben <i>database</i>: Save Points werden in die X4-Systemdatenbank geschrieben

i Wenn das savepoint-Element in der `X4config.xml` weggelassen wird, dann werden keine Save Points gespeichert.

3.1.3.2 SNMP-Trap-Appender

Als Erweiterung von Log4j besteht die Möglichkeit, einen Appender für Simple Network Management Protocol (SNMP)-Traps einzusetzen, um Protokoll-Ereignisse als formatierte Zeichenkette an einen bestimmten Management Host in Form einer SNMP-Trap auszugeben. Um SNMP-Traps zu generieren, ist es erforderlich, einen SNMP-Trap-Appender für Log4j zu konfigurieren und eine entsprechende Kategorie für den Appender zuzuweisen.

3.1.3.3 Ad-Hoc Logging im Betrieb

Zur erweiterten Fehleranalyse besteht die Möglichkeit, die Ausgabe von einzelnen Prozessschritten im laufenden Betrieb zu loggen. Dabei muss weder die .wrf-Datei des jeweiligen technischen Prozesses geändert, noch der Server neu gestartet werden. Zudem wird auch das bedingte Logging in Subprozessen ermöglicht, z.B. falls ein Subprozess von einem bestimmten Hauptprozess aufgerufen wurde.

3.1.3.3.1 Konfiguration

Das Protkollierverhalten kann über die `tracelog.properties`-Datei unter `X4\Server\X4DB\0` gesteuert werden. Hier wird u.a. auch das erwartete Format beschrieben, wenn man einen Prozess bzw. Prozessschritt adressieren und das Logging anschalten möchte:

- **Einzelne Prozessschritte loggen:** Einzelne Prozessschritte, die geloggt werden sollen, können nach folgendem Schema angegeben werden: `<Benutzer>/<Prozesspfad>/<ActionID> = 1`
- **Bedingtes Loggen von Subprozess-Schritten:** Wenn einzelne Prozessschritte in einem Subprozess geloggt werden sollen, der von einem bestimmten Elternprozess aufgerufen wurden, kann dies nach folgendem Schema angegeben werden: `<Ausführender_Benutzer>/<Prozesspfad_Elternprozess>/<Benutzer>/<Prozesspfad_Subprozess>/<ActionID> = 1`

Der Inhalt der Log-Ausgabe entspricht dem Inhalt des Loggings via *Log4J* auf einer Transition, d.h. der Status bzw. die Daten des letzten Prozessschrittes werden über *Log4J* geloggt. Als Log4J-Logger wird dabei `de.softproject.integration.logging.integrated.TraceLog` und als Log4J Log-Level `INFO` verwendet.

Wurden Änderungen an der `tracelog.properties`-Datei vorgenommen, so muss die Konfiguration neu eingelesen werden. Das Einlesen der Konfiguration kann über die MBean angestoßen werden. Dazu die MBean-Operation **reloadTraceLogSettings** ausführen.

3.1.3.3.2 Beispielkonfigurationen

3.1.3.3.2.1 Einzelne Prozessschritte loggen

Beispielkonfiguration für das Loggen eines bestimmten Prozessschrittes

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

Erläuterung

Logging ist aktiviert für:

- Benutzer `1`
- Prozess `Test/Log/logtest.wrf`

- Prozesskomponente mit *Action ID 2*

3.1.3.3.2 Bedingtes Loggen von Subprozess-Schritten

Beispielkonfiguration für bedingtes Loggen eines Subprozesses

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

Erläuterung

Logging ist aktiviert für:

- Benutzer *1*
- Prozess *Test/Log/logtestSub.wrf*
- Prozesskomponente mit *Action ID 2*

Bedingung:

- Prozess *Test/Log/logtestParent.wrf* wurde ausgeführt von
- Benutzer *1*

3.1.4 Production Mode konfigurieren

Als Mittel zur Performance-Steigerung bietet der X4 Server den Production Mode. Hierbei wird das Caching für das Repository aktiviert.

1. In der zentralen Konfigurationsdatei `X4config.xml` den Wert von `<productionMode>` auf *on* setzen.
2. X4 Server neu starten, siehe [X4 Server kontrolliert herunterfahren \(via JMX\)](#). Der Production Mode bzw. das Caching ist nach dem Neustart aktiviert.

Beachten Sie:

- Um den Production Mode wieder zu deaktivieren, setzen den Wert von `<productionMode>` zurück auf *off* und starten Sie den Server neu.
- Zum Bearbeiten des Repositorys während des Production Modes, z. B. zum Anpassen von Prozessen und Scheduling-Einstellungen, muss der X4 Server nicht neu gestartet werden.

3.1.5 SSL und HTTPS für den X4 Server einrichten

Für den X4 Server, der auf WildFly basiert, kann SSL und HTTPS konfiguriert werden.

Voraussetzungen

- Sie haben bereits ein Keystore erstellt
- Sie haben ein gültiges Zertifikat

3.1.5.1 key-stores anpassen

1. Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
2. Bearbeiten Sie folgende Zeilen ein.

```
<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 des Key-Stores. Wird verwendet, um den Key-Store im key-manager-Element zu referenzieren.
- **file**: Pfad zum Key-Store. Im obigen Beispiel wird ein relativer Pfad angegeben. Wenn Sie einen absoluten Pfad zum Key-Store angeben, ist das Attribut **relative-to** obsolete.

3.1.5.2 key-managers anpassen

1. Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
2. Bearbeiten Sie folgende Zeilen ein.

```
<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 des Key-Managers.
- key-store: Name des Key-Stores, der verwendet wird.
- clear-text: Passwort des Key-Stores.

3.1.5.3 server-ssl-contexts anpassen

1. Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
2. Bearbeiten Sie folgende Zeilen ein.

```
<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 des SSL-Context.
- key-manager: Name des Key-Managers, der verwendet wird.
- protocols: SSL/TLS-Protokoll, das verwendet werden soll. Das obigen Beispiel verwendet TLSv1.2.

3.1.5.4 https-listener anpassen

1. Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
2. Bearbeiten Sie folgende Zeilen ein.

- Um HTTP zu deaktivieren, entfernen Sie die Zeile `<http-listener>`.

```
<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 des SSL-Context, der verwendet wird.

3.1.5.5 socket-binding anpassen

- Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
- Bearbeiten Sie folgende Zeilen ein.

```
<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>
```

 Standardmäßig ist der https-Port auf 8443 gesetzt, aber Sie können den Port beliebig anpassen.

 Weitere Informationen finden Sie in der offiziellen WildFly-Dokumentation unter https://docs.wildfly.org/25/WildFly_Elytron_Security.html#configure-sslts.

3.2 X4 Designer konfigurieren

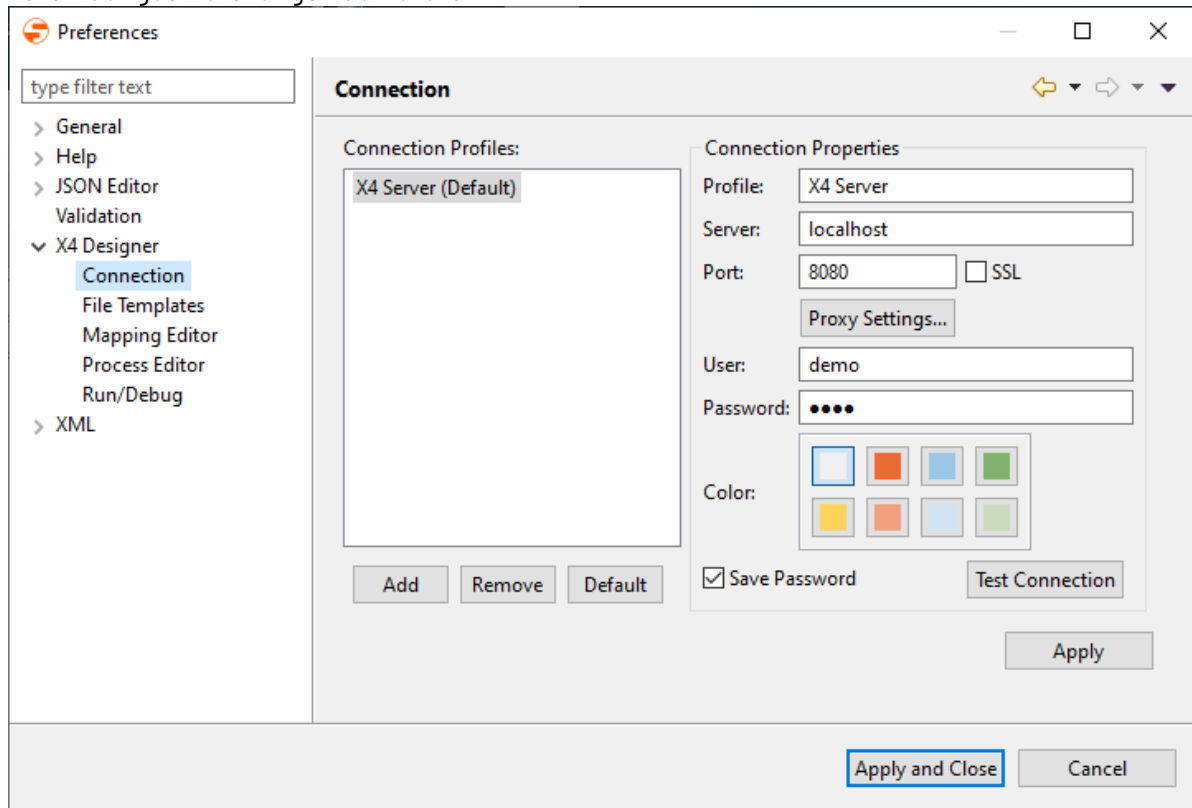
Wie sich Darstellung und das Verhalten einiger Komponenten des *X4 Designers* anpassen lassen

3.2.1 Verbindungskonfiguration bearbeiten

Unter **Connection** lassen sich Verbindungsprofile mit den jeweiligen Profildaten hinterlegen.

- Menü **Tools> Options** aufrufen.

2. Auf der linken Seite **X4 Designer** doppelklicken und **Connection** wählen, um die Verbindungseinstellungen aufzurufen.

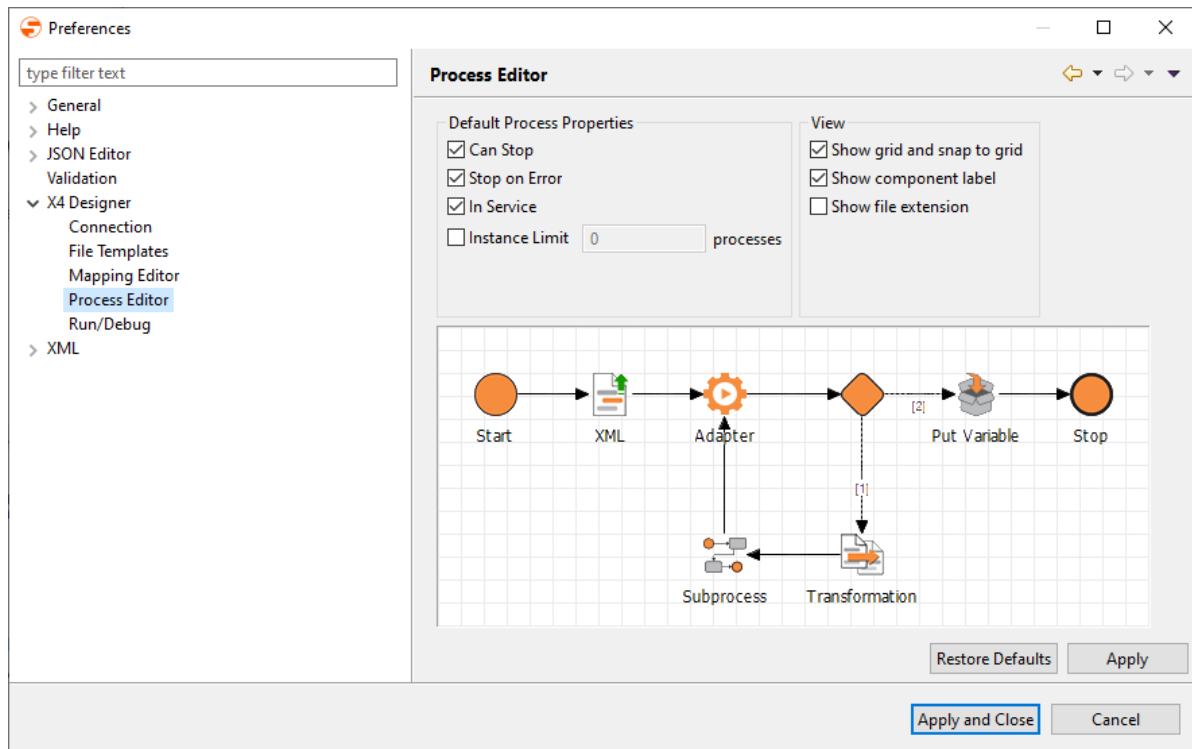


3. Gewünschte Verbindungseinstellungen vornehmen:
 - **Profile:** Name des Verbindungs-Profiles (frei wählbar)
 - **Server:** IP-Adresse oder Host-Name des *X4 Servers* (Beispiel: *localhost*)
 - **Port:** Port-Nummer
 - **Proxy Settings:** Standardeinstellungen zu Proxy-Servern und Internet-Verbindung
 - **User:** Name des Repository-Benutzers
 - **Password:** Zugehöriges Passwort
 - **Color:** Farbe für die Verbindungseinstellung (optional)
 - ❗ Die gewählte Farbe wird in der Statusleiste des *X4 Designers* beim nächsten erfolgreichen Verbindungsversuch angezeigt. Damit lassen sich verschiedene *X4 Server* besser unterscheiden.
4. **Test Connection** klicken, um zu prüfen, ob die Verbindung korrekt aufgebaut wird.
5. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

3.2.2 Process Editor konfigurieren

Unter **Process Editor** können Einstellungen zur Darstellung von Prozessen im Process Editor hinterlegt werden.

1. Menü **Tools > Options** aufrufen.
2. Auf der linken Seite **X4 Designer** doppelklicken und **Process Editor** wählen, um die Process-Editor-Konfiguration zu öffnen.

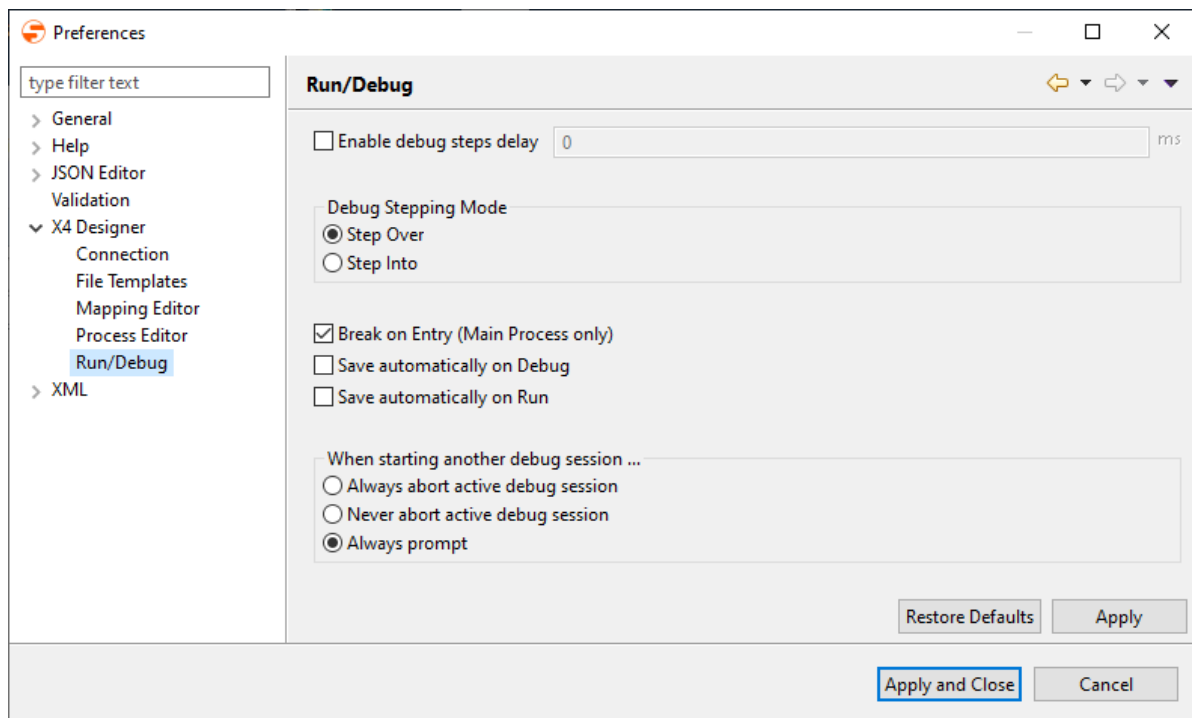


3. Gewünschte Einstellungen in **Default Process Properties** vornehmen:
 - **Can Stop:** Zulassen, dass der Prozess abgebrochen werden kann
 - **Stop on Error:** Prozess-Ausführung automatisch stoppen, wenn ein Fehler auftritt
 - **Public/Private:** Prozess darf ausgeführt werden
 - **Instance Limit:** Anzahl der Prozessinstanzen begrenzen
 - **Show grid and snap to grid:** Raster im Process Editor anzeigen und die Symbole am Raster ausrichten
 - **Show component label:** Beschriftungstext unterhalb von Prozessbaustein-Symbolen anzeigen
 - **Show file extension:** Prozessbausteine mit Dateinamensendung anzeigen (standardmäßig deaktiviert)
4. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

3.2.3 Run-/Debug-Modus konfigurieren

Sie können festlegen, wie sich Prozesse verhalten, wenn Sie im *X4 Designer* im Run- oder Debug-Modus ausgeführt werden.

1. Menü **Tools > Options** aufrufen.
2. Auf der linken Seite **X4 Designer** doppelklicken und **Run/Debug** wählen.



3. Gewünschte Einstellungen vornehmen:

- **Enable debug steps delay:** Verzögerung (in Millisekunden) zwischen jedem ausgeführten Prozess-Schritt im Debug-Modus in **Debug steps delay** einstellen
 ⓘ Die Verzögerung findet nur dann statt, wenn die Prozessausführung über **Resume** wieder fortgesetzt wird.
 - **Debug Stepping Mode:** Standard-Anzeigeverhalten beim Debugging der Prozess-Schritte:
 - **Step Over:** Schritte ausführen und jeden Subprozess als einen Prozessschritt debuggen
 - **Step Into:** Schritte ausführen und in Subprozesse springen und auch deren Schritte beim Debugging anzeigen
 - **Break on Entry (Main Process only):** Nach dem ersten Prozess-Schritt das Debugging anhalten
 - **Save automatically on Debug:** Prozess automatisch vor dem Start des Debug-Modus speichern
 - **Save automatically on Run:** Prozess automatisch vor dem Start des Run-Modus speichern
 - **When starting another debug session:** Verhalten des Debuggers, wenn bereits ein anderer Debugging-Vorgang ausgeführt wird
 - **Always abort active debug session:** Immer den aktiven Debugging-Vorgang abbrechen und sofort mit dem Debugging beginnen.
 - **Never abort active debug session:** Niemals den aktiven Debug-Vorgang abbrechen (diese muss dann vom Benutzer manuell abgebrochen werden).
 - **Always prompt:** Beim Starten des Debug-Modus werden Sie ggf. befragt.
- ⓘ Das Debugging lässt sich auch über die F4-Taste neu starten.

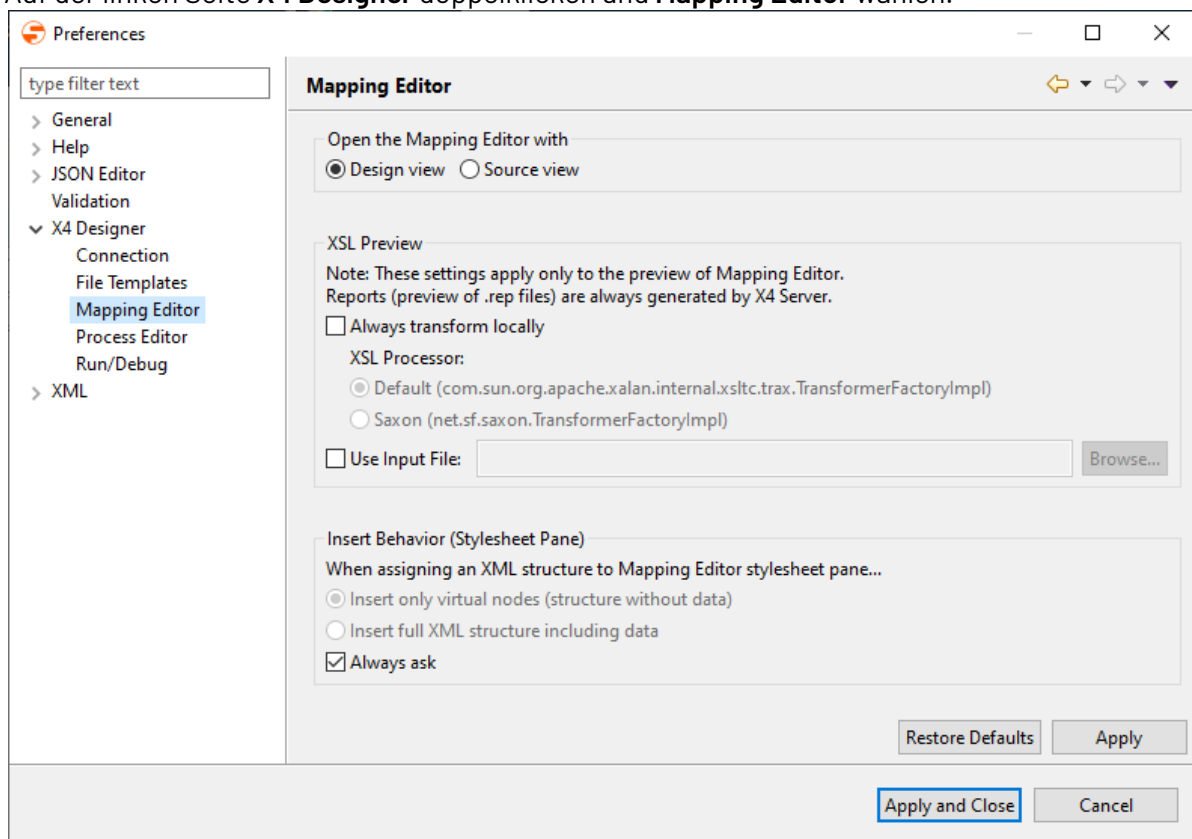
4. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

3.2.4 Mapping Editor konfigurieren

Für den Mapping Editor lässt sich für dessen Vorschau festlegen, ob XSL-Stylesheets auf dem X4 Server oder im X4 Designer transformiert werden sollen. Zudem können Sie einstellen, ob im Mapping Editor XML-Strukturen mit oder ohne Inhalt eingefügt werden sollen.

 Die Vorschau-Einstellungen gelten ausschließlich für den Mapping Editor, wenn Sie auf  klicken oder **F9** drücken! XSL-Mappings in ausgeführten Prozessen werden immer auf dem X4 Server transformiert!

1. Menü **Tools > Options** aufrufen.
2. Auf der linken Seite **X4 Designer** doppelklicken und **Mapping Editor** wählen.



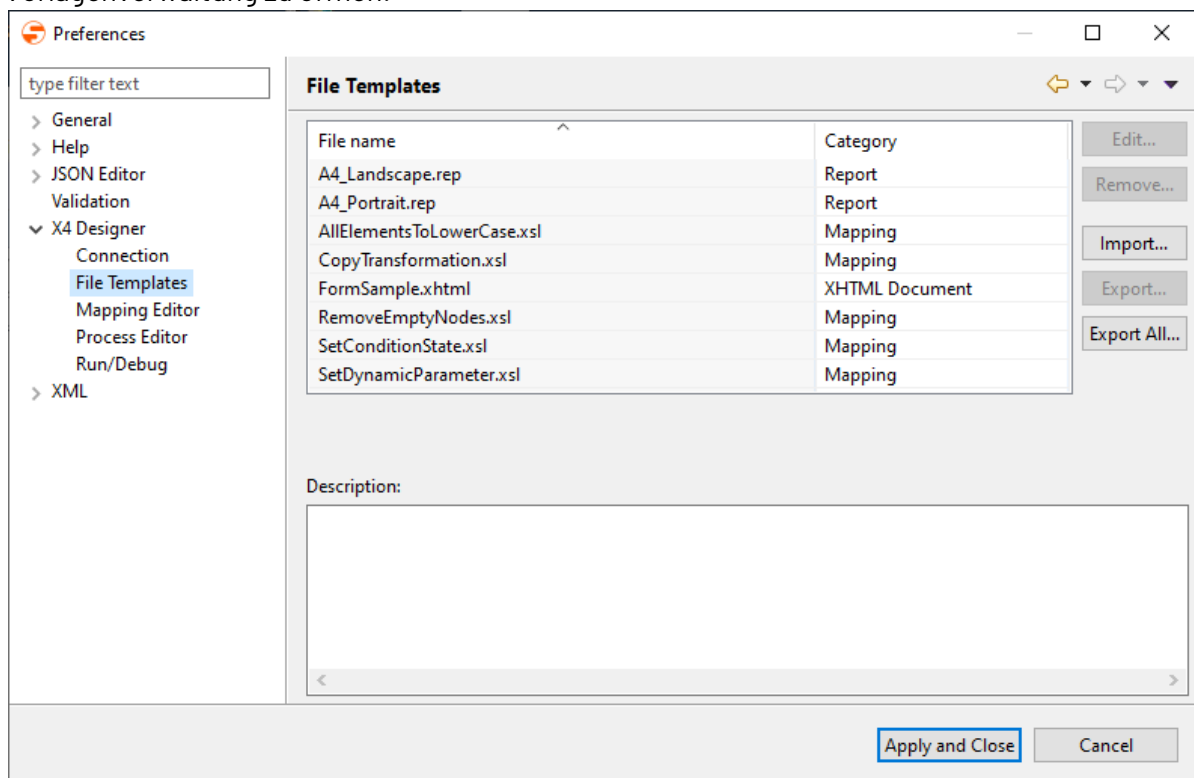
3. Verhalten des Mapping Editors konfigurieren:
 - In **Open the Mapping Editor with** einstellen, wie XSL-Mappings geöffnet werden sollen:
 - **Design view:** In der grafischen Mapping-Ansicht öffnen (Standard)
 - **Source view:** In der Quellcode-Ansicht öffnen
 - In **XSL Preview** das Verhalten der XSL-Transformationsvorschau einstellen
 - In **Insert Behavior (Stylesheet Pane)** das Standard-Einfügeverhalten von XML einstellen:
 - **Insert only virtual nodes:** Lediglich die Struktur als virtuelle Knoten im Stylesheet-Bereich anzeigen
 - **Insert full XML structure including data:** Komplette XML-Dokumentstruktur inklusive Werte einfügen

- **Always ask:** Bei jedem Einfügen von XML via Drag&Drop, per Kontextmenü oder über **Strg+V** fragen (standardmäßig aktiv)
4. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

3.2.5 Vorlagen für Repository-Elemente verwalten

Im X4 Designer können Sie Vorlagen für Prozesse, Prozessbausteine oder Ordner definieren, um wiederkehrende Muster schnell abzubilden.

1. Menü **Tools > Options** aufrufen.
2. Auf der linken Seite **X4 Designer** doppelklicken und **File templates** wählen, um die Vorlagenverwaltung zu öffnen.

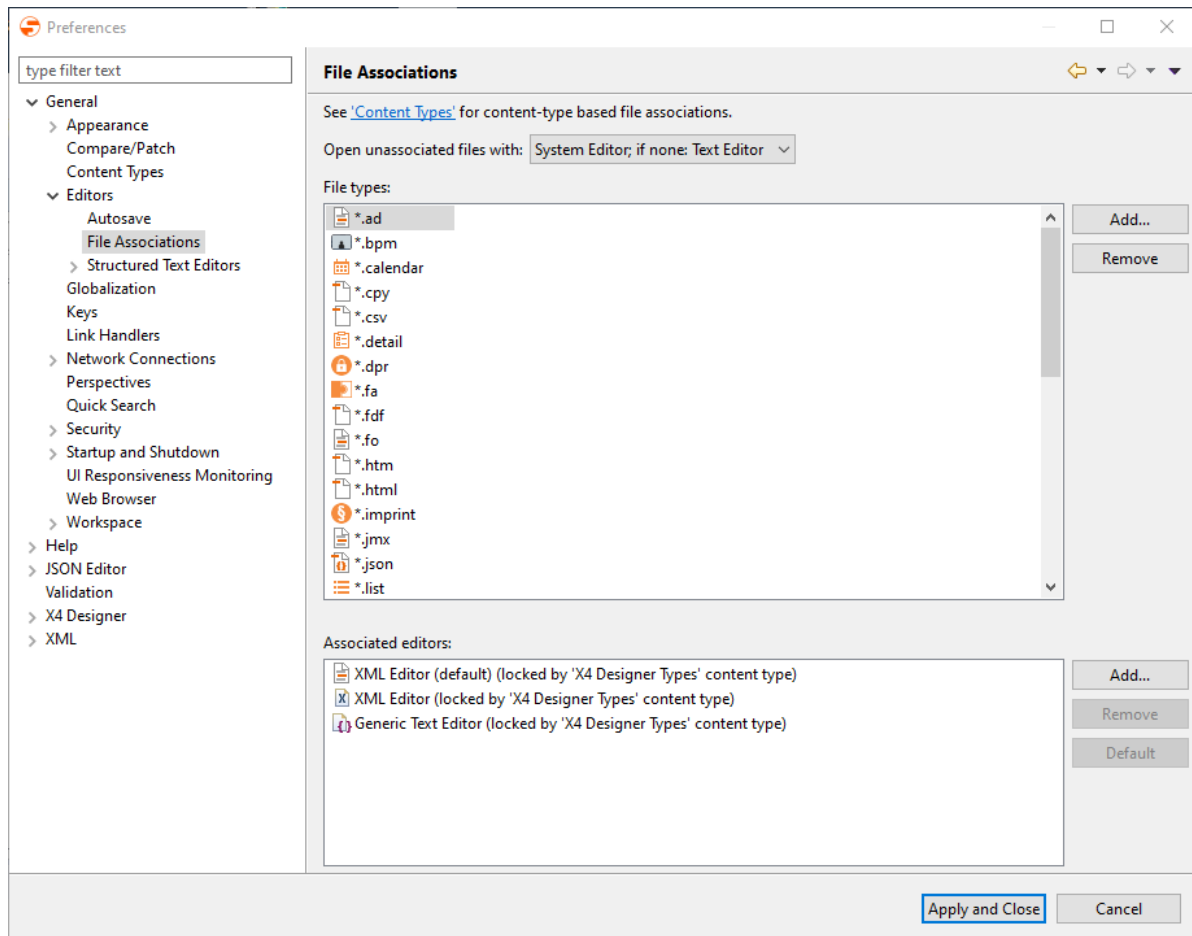


3. Vorlagen wie gewünscht verwalten:
 - **Edit:** Dateinamen und/oder den Beschreibungstext bearbeiten
 - **Remove:** Markierte Vorlage löschen
 - **Import:** Einen bestehenden Vorlagen-Ordner importieren
 - Zulässig sind nur Vorlagen-Ordner, welche die gleiche Struktur wie der Ordner <X4>/X4DB/0/Templates aufweisen.
 - **Export** bzw. **Export All:** Eine markierte Vorlage bzw. alle Vorlagen als Vorlagen-Ordner exportieren
4. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

3.2.6 Dateitypen zu internen und externen Editoren zuordnen

Im X4 Designer lassen sich beliebige Dateitypen mit Editoren und anderen Programmen verknüpfen.

1. Menü **Tools > Options** aufrufen.
2. Auf der linken Seite **General > Editors > File Associations** wählen.



3. in **File types** einen bestehenden Dateityp wählen oder über **Add** einen neuen Dateityp hinzufügen.

i Sie können entweder eine Dateinamensendung mit *-Platzhalter oder einen kompletten Dateinamen als Dateityp definieren. Beispiel: *.xyz oder Filename.xyz

4. In **Associated editors** für den markierten Dateityp einen Editor wählen oder über **Add** das Fenster **Editor Selection** öffnen und dort den gewünschten Editor aus einer Liste der verfügbaren Editoren wählen.

i Wenn Sie einen externen Editor verwenden möchten: in Fenster **Editor Selection** die Option **External programs** wählen und über **Browse** die Datei der gewünschten externen Anwendung wählen.
Beispiel: C:\Program Files\Notepad++\notepad++.exe wählen.

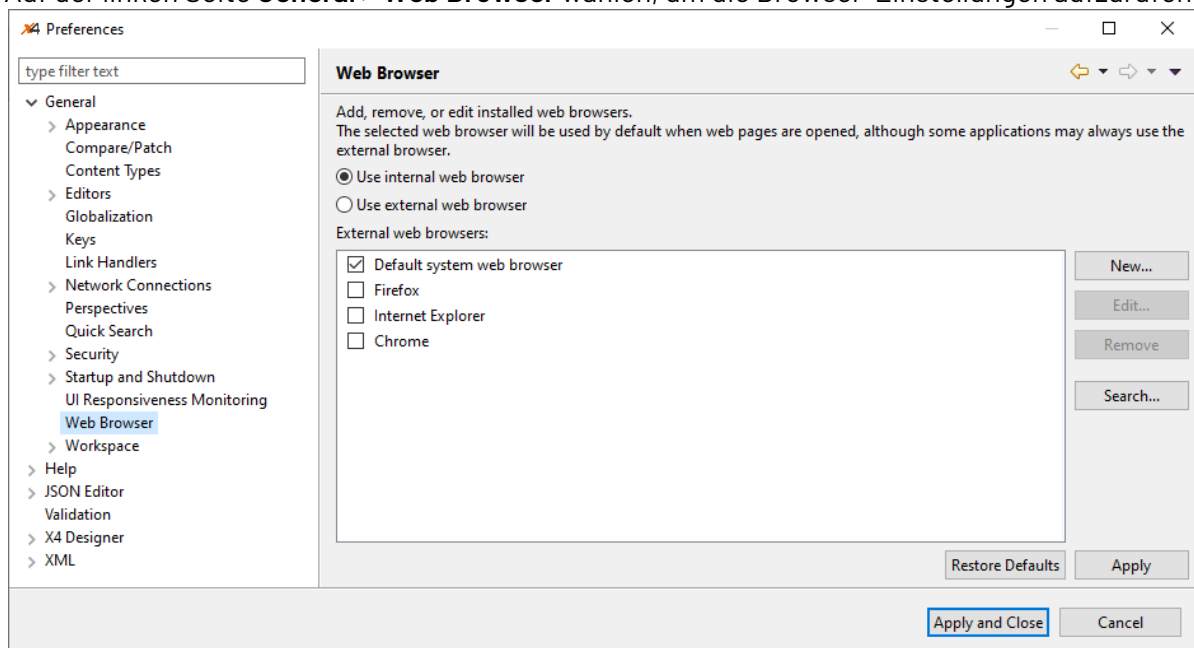
✓ Wenn der Dateityp standardmäßig mit dem gewählten Editor geöffnet werden soll, auf **Default** klicken.

5. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.
Im Kontextmenü des **Repository Navigators** sind nun unter **Open with** alle mit dem Dateityp verknüpften internen oder externen Editoren auswählbar.

3.2.7 Web Browser konfigurieren

Für die Anzeige der browserbasierten Komponenten der X4 BPMS können verschiedene Browser verwendet werden (siehe [Systemvoraussetzungen](#)). Der verwendete Browser kann in der X4 BPMS festgelegt werden.

1. Menü **Tools> Options** aufrufen.
2. Auf der linken Seite **General > Web Browser** wählen, um die Browser-Einstellungen aufzurufen.



3. Einen der definierten Browser auswählen oder auf **New** klicken.
4. Wenn **New** geklickt wurde:
 - **Name:** Anzeigename der Browserkonfiguration
 - **Location:** Dateipfad zum Browser
 - **Parameters:** Parameter, die beim Aufruf des Browsers verwendet werden sollen.

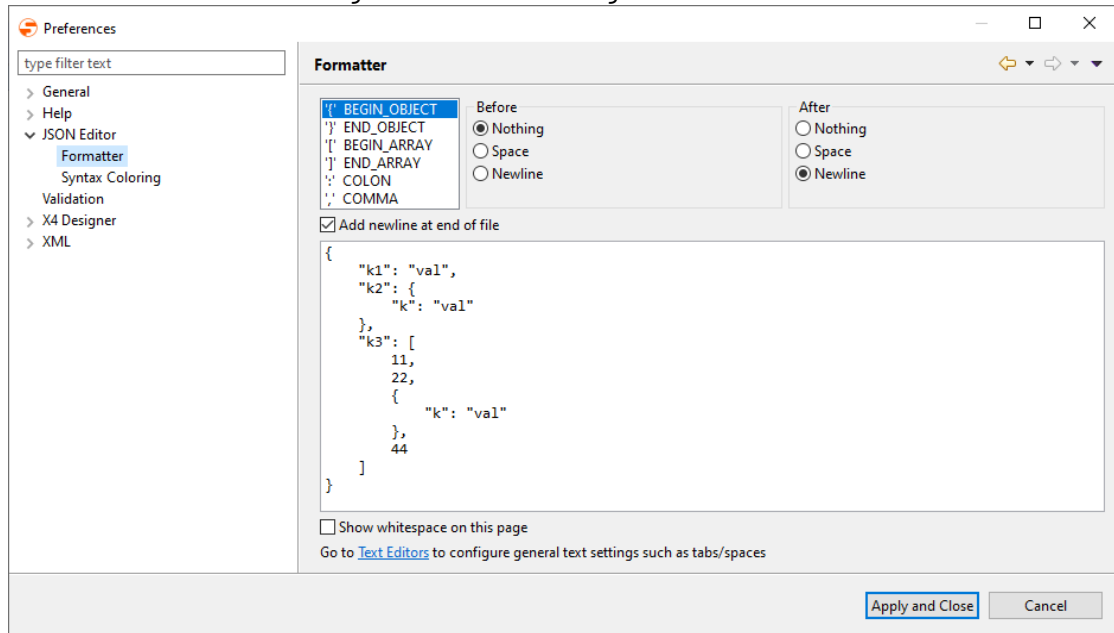
 Um Microsoft Edge verwenden zu können, muss folgendes eingetragen werden:
Location: Speicherort der Windows-Eingabeaufforderung, z. B. *C:\Windows\System32\cmd.exe*
Parameters: */c "start microsoft-edge:%URL%"*

5. Einstellungen mit **OK** bestätigen.
6. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

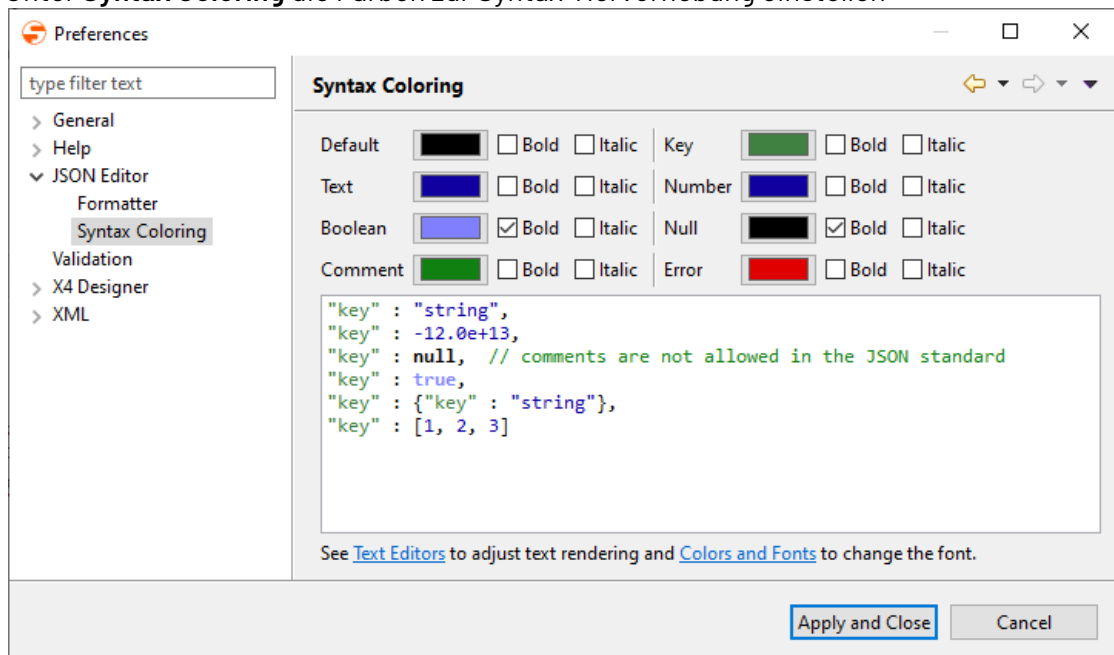
3.2.8 JSON-Editor konfigurieren

Unter **JSON Editor** können Einstellungen zum JSON-Editor hinterlegt werden.

1. Menü **Tools> Options** aufrufen.
2. Auf der linken Seite **JSON Editor** doppelklicken, um die Editor-Konfiguration zu öffnen.
3. Gewünschte Einstellungen vornehmen:
 - Unter **Formatter** Einstellungen zur Formatierung des JSON-Codes vornehmen



- Unter **Syntax Coloring** die Farben zur Syntax-Hervorhebung einstellen



4. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

3.2.9 Sprache der Hilfe umschalten

Über das Menü **Help > Help Contents** lässt sich die integrierte Hilfe in einem gesonderten Fenster aufrufen. Die Hilfe ist in Bücher unterteilt, die jeweils auf unterschiedliche Themen im Kontext der X4 BPMS eingehen.

Standardmäßig richtet sich die Sprache der angezeigten Hilfe nach der Systemsprache, es besteht jedoch die Möglichkeit, diese bei Bedarf zu ändern. Sollte die Systemsprache weder deutsch noch englisch sein, wird die Hilfe standardmäßig auf englisch angezeigt.

Die Sprache lässt sich derzeit über die `X4Designer.ini` unter `<X4>/Designer` anpassen. Für die Sprachumschaltung muss die Sprachangabe `en` für englisch oder `de` für deutsch angepasst werden.

Beispiel: Anpassung für englischsprachige Hilfe

```
-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
```

Nach dem Neustart des X4 Designers steht die Hilfe in der entsprechend eingestellten Sprache zur Verfügung.

4 Administration des X4 Servers

Hier erfahren Sie, wie Sie eine produktiv eingesetzte Installation der X4 BPMS über JMX administrieren.

4.1 X4 Repository im Production Mode aktualisieren

Im Production Mode des X4 Servers ist das Caching für das X4 Repository aktiviert. Sie können Repository-Projekte aktualisieren, ohne den X4 Server neu zu starten.

Damit nach der Aktualisierung des X4 Repositorys keine veralteten Dateien im Cache verwendet werden, muss dieser zurückgesetzt werden. Dies erfolgt über eine JMX Management Bean (MBean) mit Namen `X4Management`, die der X4 Server bereitstellt.

Tipp

Die JMX MBean `X4Management` ermöglicht neben dem Zurücksetzen des Caches über die Methode `resetCache()` u. a. auch die Betrachtung von Cache-Statistiken (Methode `cacheStatistics()`) und die Möglichkeit, einen *SAP JCo*-Server neuzustarten (Methode `restartSAPJcoServer()`).

1. Das X4 Repository aktualisieren.
2. Die JMX MBean `X4Management` aufrufen:
 - Das Werkzeug `jconsole` starten.
 - JMX MBean `X4Management` in einer Domain `de.softproject.X4` aufrufen.
3. Die MBean-Methode `resetCache()` ausführen.
Der Cache wird nun zurückgesetzt.

4.2 X4 Server kontrolliert herunterfahren (via JMX)

Wie Sie den *X4 Server* im laufenden Betrieb mit ausgeführten Prozessen kontrolliert herunterfahren

Voraussetzungen zum Herunterfahren

Ein kontrolliertes Herunterfahren des X4 Servers stellt sicher, dass alle aktuell ausgeführten Prozesse vollständig ausgeführt und keine Prozesse mehr gestartet werden. Dafür muss bei allen Prozessen, die nicht während der Ausführung abgebrochen werden dürfen, die Eigenschaft `Can Stop` deaktiviert sein. Zudem müssen Endlosprozesse so modelliert sein, dass sie in regelmäßigen Abständen die Verarbeitung unterbrechen, damit sie gestoppt werden können.

Je nach Warteschlangen-Adapter ist dies wie folgt möglich:

- *JMS* und *RequestReply Transfer*: In Parameter `timeout` eine entsprechende Zeitbeschränkung setzen. Wenn der Adapter den Status `0` zurückgibt, ist die Warteschlange leer und die Prozesskontrolle wird dem Adapter zurückgegeben, sodass der Prozess anhalten kann.
- *MQ Series Transfer* und *WebSphere MQ*: Parameter `MQGetMessageOptions.options.MQC.MQGM0_WAIT` aktivieren, um das Warten auf eine Nachricht zu aktivieren, und in Parameter `MQGetMessageOptions.waitInterval` eine Zeitdauer in Millisekunden angeben, die beim Auslesen gewartet wird, bis eine geeignete Nachricht ankommen kann.

1. Die MBean `X4Management` aufrufen:
 - Das Werkzeug `jconsole` starten.
 - JMX MBean `X4Management` in einer Domain `de.softproject.X4` aufrufen.
2. Die MBean-Methode `setAllOutOfService()` ausführen.
Für alle Prozesse wird damit die Eigenschaft `OutOfService` gesetzt. Dies bewirkt, dass keine Prozesse mehr gestartet werden.
3. Die MBean-Methode `stopAllProcesses()` ausführen.
Alle momentan ausgeführten Prozesse, die abgebrochen werden dürfen, werden damit beendet.
4. Warten, bis die MBean-Methode `runningWorkflowCount()` `0` anzeigt.
Nun wird kein Prozess mehr ausgeführt.

 Alternativ können Sie auch die Methode `shutdownAllProcesses(longtimeoutInMS)` aufrufen. Dies bewirkt, dass die MBean-Methoden `setAllOutOfService()`, `stopAllProcesses()` und `runningWorkflowCount()` nacheinander ausgeführt werden.

- In **ParamValue** eine Zeitbegrenzung in Millisekunden angeben, die die Methode als Parameter `longtimeoutInMS` erhält.
- Auf **Invoke** klicken, um die Methode auszuführen. Diese gibt `True` zurück, wenn `runningWorkflowCount()` innerhalb der Zeitbeschränkung `0` anzeigt.

5. X4 Server herunterfahren.

4.3 Prozess-Bibliotheken bereitstellen

Prozess-Bibliotheken bieten eine einfache Möglichkeit, um fachliche und technische Prozessmodelle benutzerübergreifend zu verwenden. Das Know-how lässt sich dadurch bündeln, zentral ablegen und gezielt wiederverwenden.

Zur Bereitstellung von Prozess-Bibliotheken sind folgende Schritte notwendig:

1. *Prozess-Bibliothek installieren*: Prozess-Bibliothek als ZIP- oder jar-Datei unter `Server\X4DB\X4modules` ablegen.
2. *Prozess-Bibliothek konfigurieren und bereitstellen*: Prozess-Bibliothek über die Datei `modules.xml` (`Server\X4DB\X4modules\`) konfigurieren und auf dem Server bereitstellen.

Beispielkonfiguration über die `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>
```

Erläuterung:

Element	Beschreibung
global	Die Bibliothek ist global und damit für alle Benutzer verfügbar
local	Die Bibliothek ist lokal und damit nur für einen ausgewählten Benutzer verfügbar
userId	Benutzer, für den die Bibliothek verfügbar sein soll
project	Name des Projektes; Dieser muss dem Projektnamen der Prozess-Bibliothek entsprechen.
jar	Verweis auf die ZIP- oder jar-Datei der Prozess-Bibliothek

5 Hochverfügbarkeit

In Systemen mit hoher Auslastung oder kritischen Services ist Hochverfügbarkeit ein wichtiger Bestandteil der Systemlandschaft. Mit der X4 BPMS gibt es eine Reihe von Szenarien zur Realisierung von Hochverfügbarkeit.

Grundsätzlich werden drei unterschiedliche Anwendungsfälle beschrieben: Lastverteilung, Ausfallsicherheit und Hochverfügbarkeit mit geplanten Prozessausführungen.

Bei der Hochverfügbarkeit spielt häufig die Datenintegrität eine Rolle und muss daher gewährleistet sein. Aus diesem Grund ist es wichtig, die Datenbank in der Systemlandschaft zu betrachten.

Der Lastverteiler ist eine externe Systemkomponente, die abhängig von der Umgebung eingerichtet werden muss. Er nimmt die externen Anfragen entgegen und leitet sie an die entsprechende X4 Server-Instanz weiter. Dadurch sind externe Aufrufer unabhängig von der darunter liegenden Systemlandschaft und es können Erweiterungen durchgeführt werden, ohne Änderungen auf Clientseite vornehmen zu müssen.

5.1 Lastverteilung (Load Balancing)

Bei der Lastverteilung wird das Problem von vielen gleichzeitigen Anfragen und deren Bearbeitung adressiert. Es sollen mehr Anfragen gleichzeitig bearbeitet werden, indem mehrere X4 Server-Instanzen hinter einem lasterverteilenden System geschaltet sind und dadurch eine höhere Rechenleistung erreicht wird. Dies ermöglicht eine hohe, bedarfsgerechte Skalierbarkeit. Es muss jedoch gewährleistet sein, dass die geteilten Daten der X4 Systeme allen Systemen bekannt sind. Hierfür gibt es je nach Anwendungsfall unterschiedliche Szenarien.

5.1.1 Szenario – Wenige hauptsächlich lesende Datenbankzugriffe

Wenn hauptsächlich Berechnungen in den Prozessen vorhanden sind oder weitere Services angesprochen werden, kann eine Lastverteilung über mehrere X4 Server, die jeweils ihre Systemdatenbank verwalten, und einer weiteren Datenbank, die die gemeinsamen Daten enthält, realisiert werden. Hierbei kann man zwei Ausbaustufen unterscheiden.

5.1.1.1 Einfach – Direkter Datenbankzugriff

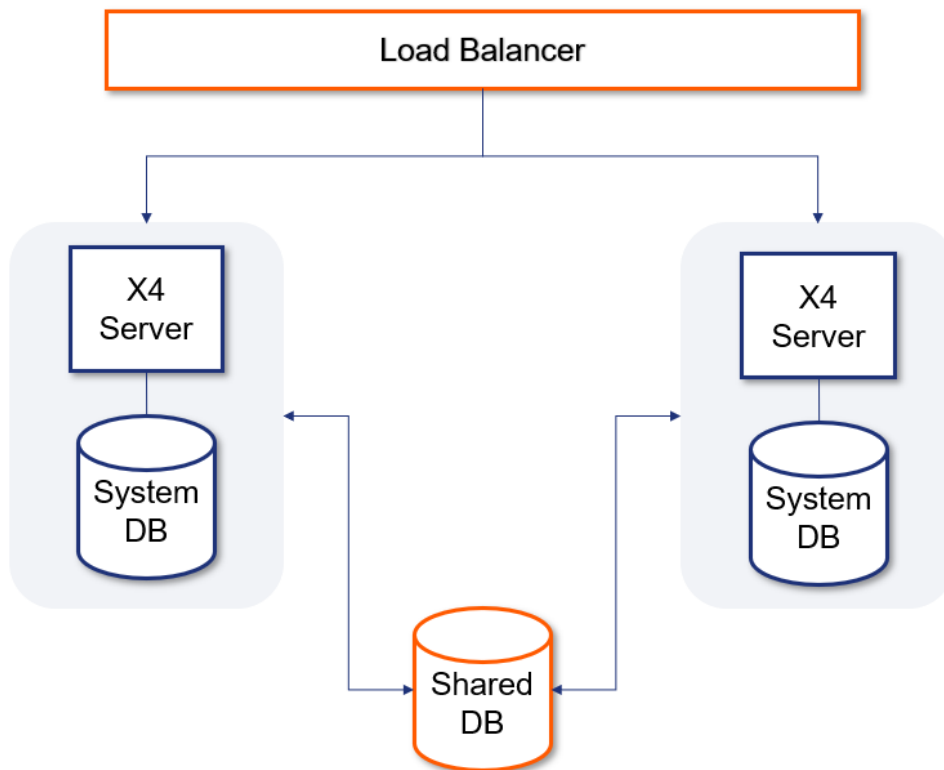


Abb. Direkter Datenbankzugriff

Man kann den Zugriff auf die gemeinsamen Daten direkt über die Zugriffsschicht der Datenbank regeln. Dies ist die einfachste Lösung des Problems und ist für kleine Systeme eine gute Lösung, da die Datenbank selbst nicht ohne weiteres entkoppelt werden kann.

5.1.1.2 Komplex – Gemeinsamer Zugriff über eine X4 Instanz

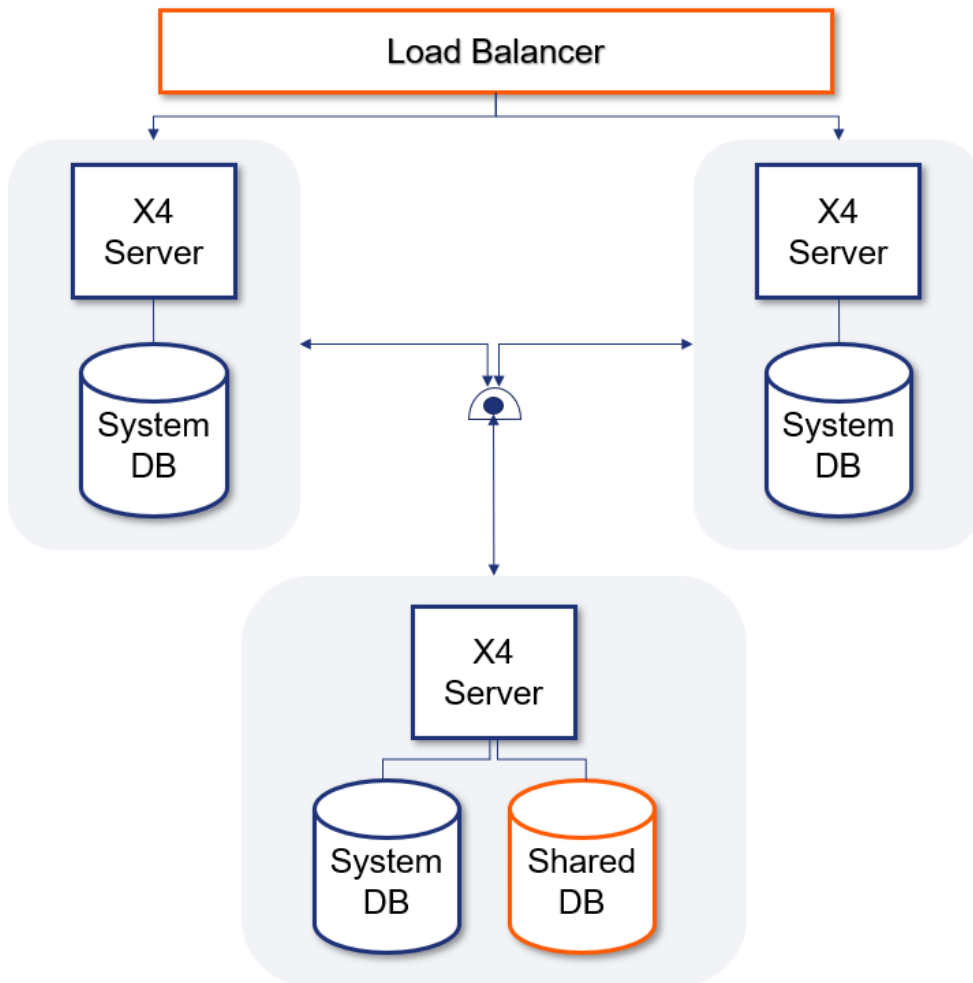


Abb. Gemeinsamer Datenbankzugriff über eine X4 Instanz

Möchte man die Datenbank entkoppeln, so bietet es sich an, eine Service-Schicht zwischen die Datenbank und den X4 Servern einzuziehen. Diese kapselt die gemeinsame Datenbank und macht dadurch die Datenhaltungsschicht austauschbar. Dies ist für größere Systeme von Bedeutung, um dort die Wartbarkeit, Testbarkeit und Integrität besser gewährleisten zu können.

5.1.2 Szenario – Gemeinsamer Zugriff über Message Queue

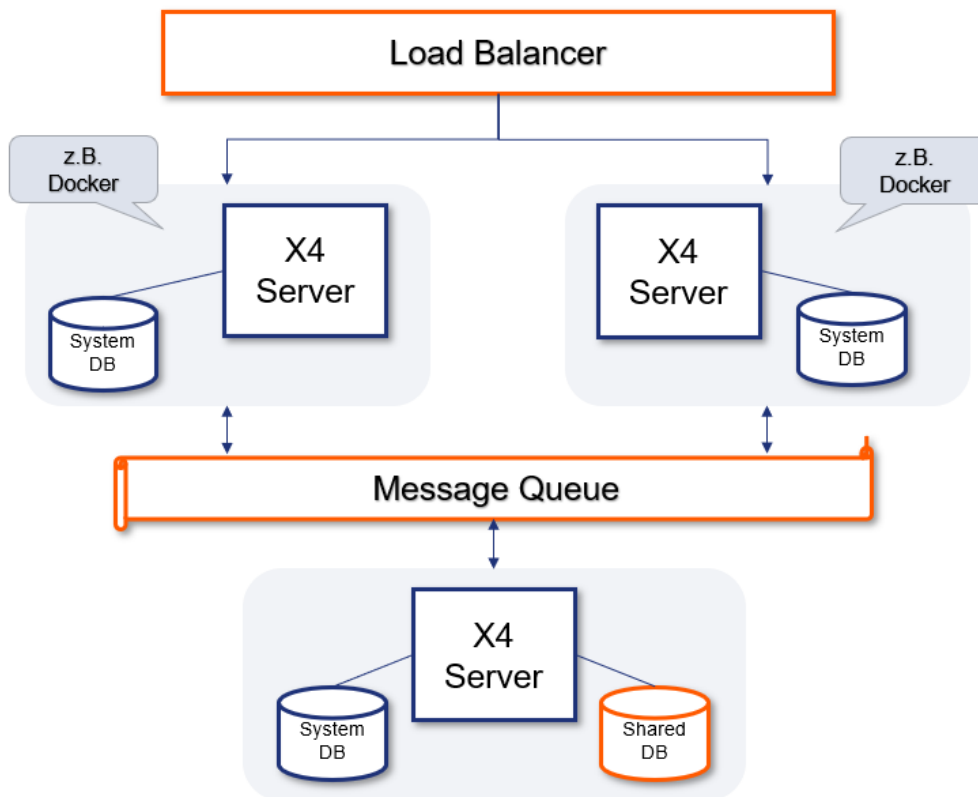


Abb. Gemeinsamer Zugriff über Message Queue

Eine weitere Möglichkeit, die Datenbank zu entkoppeln, besteht über eine Middleware. Dies ist bei kritischen Anwendungen zu empfehlen, wenn keine Nachrichten zwischen den X4 Servern und dem X4 Server der geteilten Datenbank verloren gehen dürfen. Die Middleware stellt sicher, dass Nachrichten so lange persistent gehalten werden, bis sie von dem Empfänger abgearbeitet wurden.

5.2 Ausfallsicherheit (Fail Over)

Im Gegensatz zur Lastverteilung ist bei der Ausfallsicherheit zu gewährleisten, dass das System jederzeit erreichbar ist. Es wird in der Regel jedoch nur ein Server primär mit Anfragen belastet. Fällt dieser aus, wird der zweite Server belastet und der Endanwender bemerkt den Ausfall nicht.

Ein *Keep-Alive-Service* sorgt dafür, dass der Lastverteiler benachrichtigt wird, wenn es zu einem Systemausfall kommt. Dadurch kann sofort auf den zweiten Server ausgewichen werden.

5.2.1 Szenario – Eine exklusive Datenbank

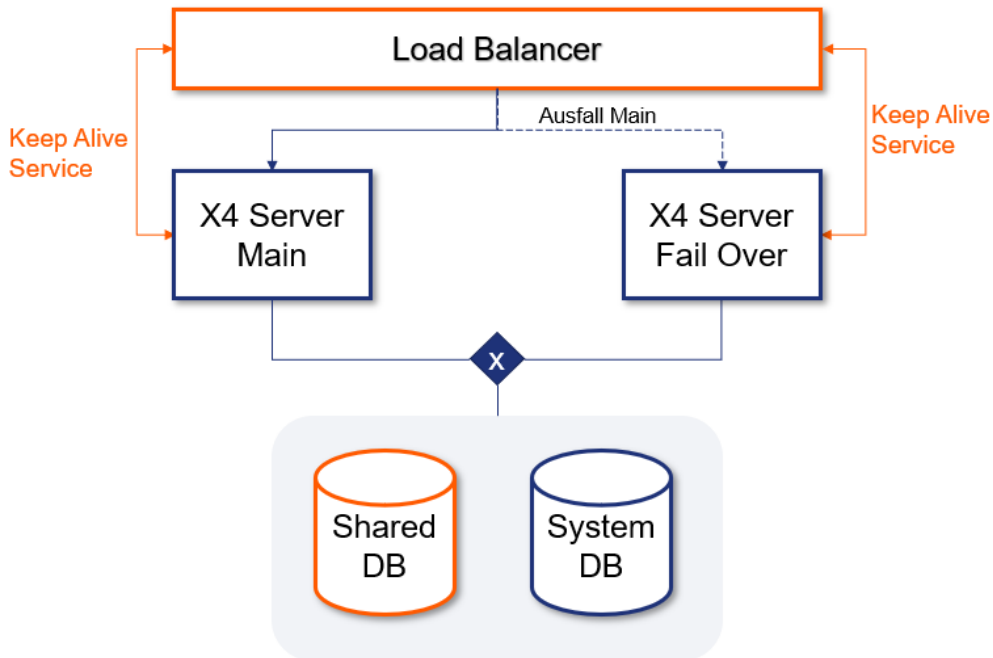


Abb. Eine Datenbank mit exklusivem Zugriff

Das einfachste System enthält zwei X4 Server-Instanzen, die beide Anfragen entgegennehmen können. Es wird eine Datenbank für beide Server benutzt, deshalb muss für die Datenintegrität darauf geachtet werden, dass nur jeweils einer der beiden Server Zugriff auf die Datenbank hat.

Scheduled Services können über einen externen Scheduler oder mithilfe eines logischen Locks auf eine Tabelle der gemeinsamen Datenbank *Shared DB* realisiert werden.

5.2.2 Szenario – Systemdatenbank pro X4 Server

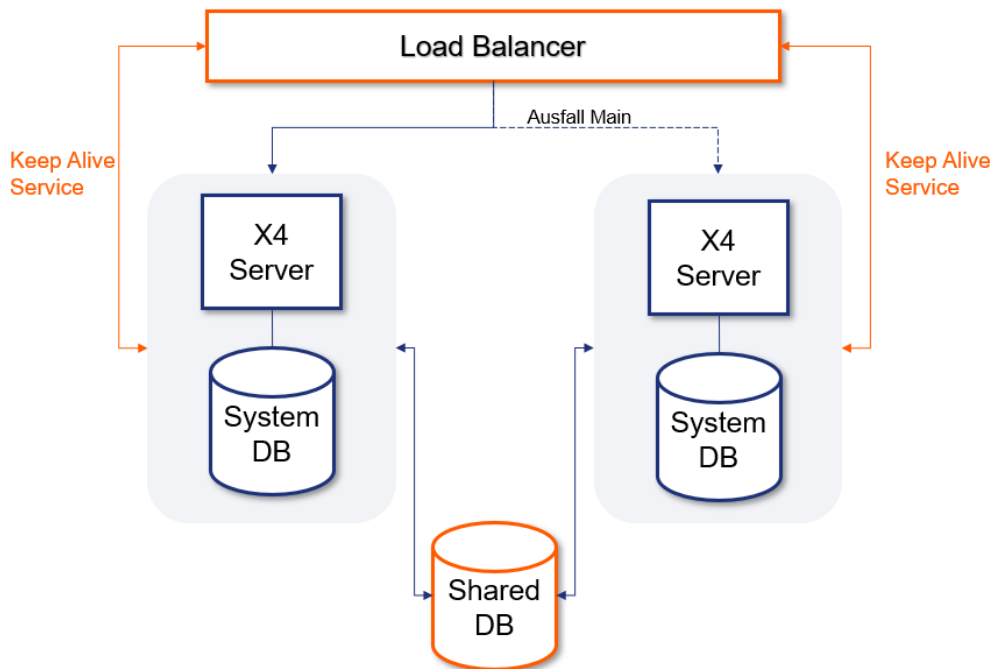


Abb. Getrennte Systemdatenbanken

Möchte man die Lastverteilung und Ausfallsicherheit durch den Systemaufbau ermöglichen, benötigt jeder X4 Server eine eigene Systemdatenbank. Dadurch kann jeder X4 Server Anfragen beantworten. Möchte man ausschließlich Ausfallsicherheit gewährleisten, so leitet man alle Anfragen nur auf einen der beiden X4 Server um.

Scheduled Services können über einen externen Scheduler oder mithilfe eines logischen Locks auf eine Tabelle der gemeinsamen Datenbank *Shared DB* realisiert werden.

5.3 Load Balancing mit Scheduler

Sollen neben der Lastverteilung auch Prozesse durch einen Scheduler automatisch gestartet werden, muss sichergestellt sein, dass die Ausführung nicht mehrfach angestoßen wird.

5.3.1 Szenario – Dedizierter X4 Server für Scheduling

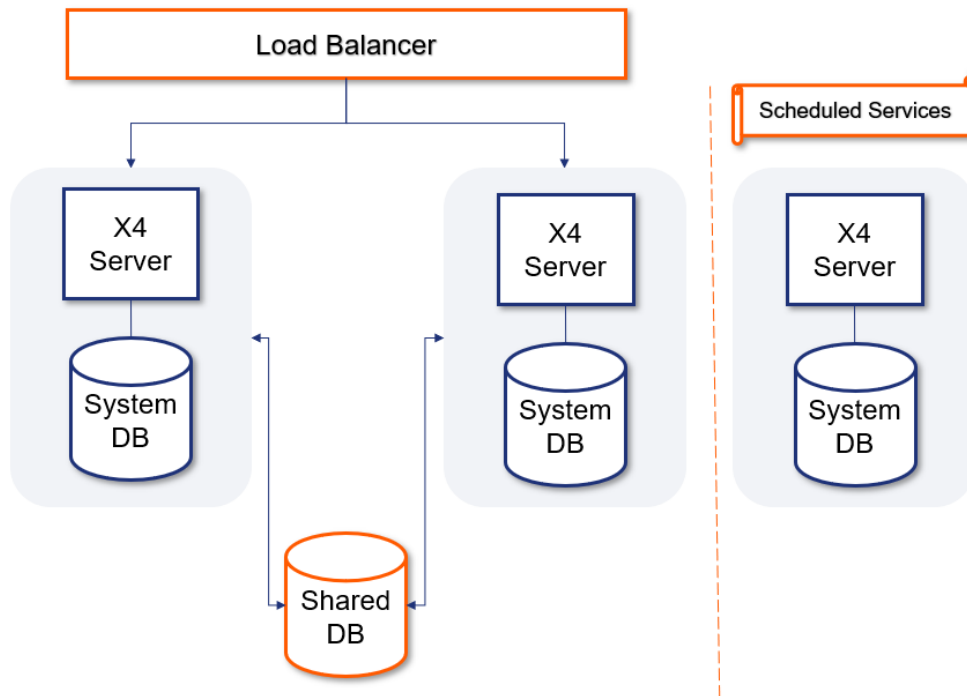


Abb. Dedizierter Scheduler X4 Server

Soll das Scheduling unabhängig von der laufenden Lastverteilung geschehen, wird ein dedizierter X4 Server eingerichtet, auf dem nur die automatisch gestarteten Prozesse installiert sind. Diese X4 Server-Instanz hat die Möglichkeit, über die geteilte Datenbank die anderen X4 Systeme zu benachrichtigen. Hierbei gibt es, wie im Abschnitt *Szenario – Gemeinsamer Zugriff über Message Queue* angegeben, auch die Möglichkeit, Nachrichten über eine Message Queue mit der geteilten Datenbank auszutauschen.

5.3.2 Szenario – Ein Server zuständig für Scheduling

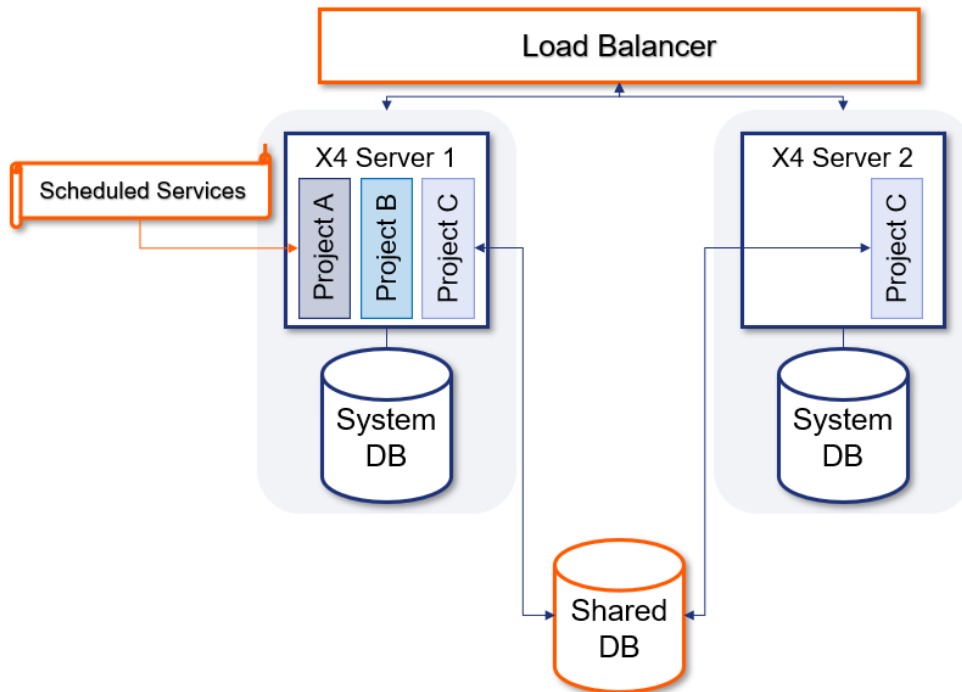


Abb. Geplante Prozesse in X4 Projekt

Möchte man keine zusätzliche X4 Server-Instanz für die automatische Ausführung von Prozessen verwenden, so kann man innerhalb der X4 Projekte ein eigenes Projekt für diese Prozesse verwenden. Dieses Projekt wird dann ausschließlich auf einem der beiden X4 Server installiert. Dadurch ist gewährleistet, dass nur diese Server-Instanz die Prozesse ausführt.

5.3.3 Szenario – Externer Scheduler

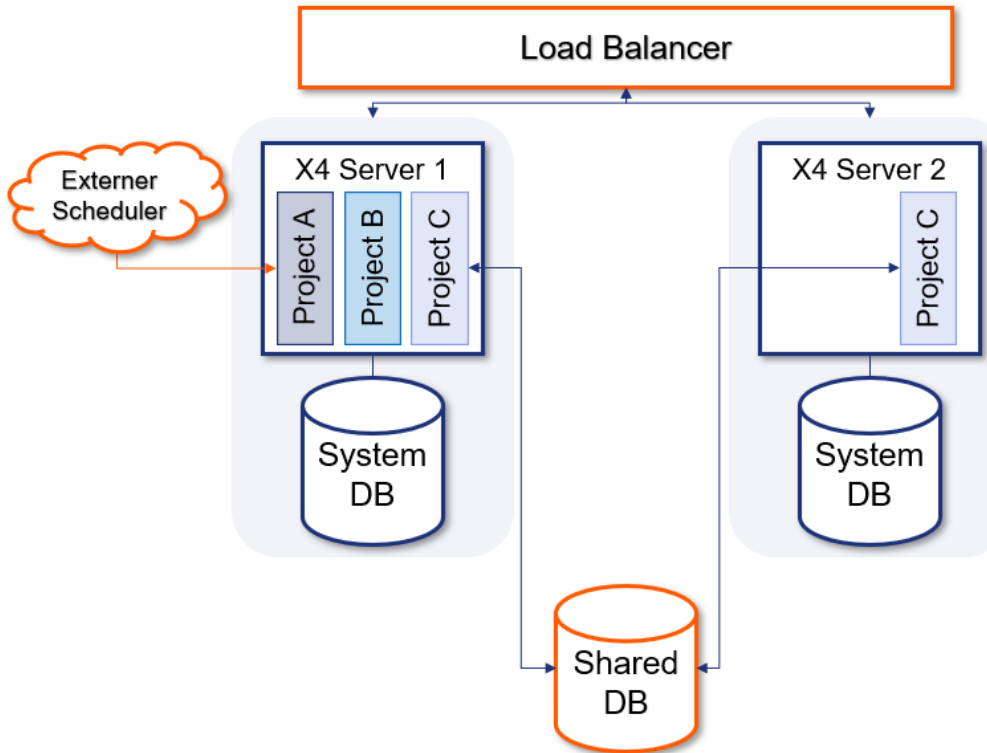


Abb. Geplante Prozesse durch externen Scheduler-Dienst

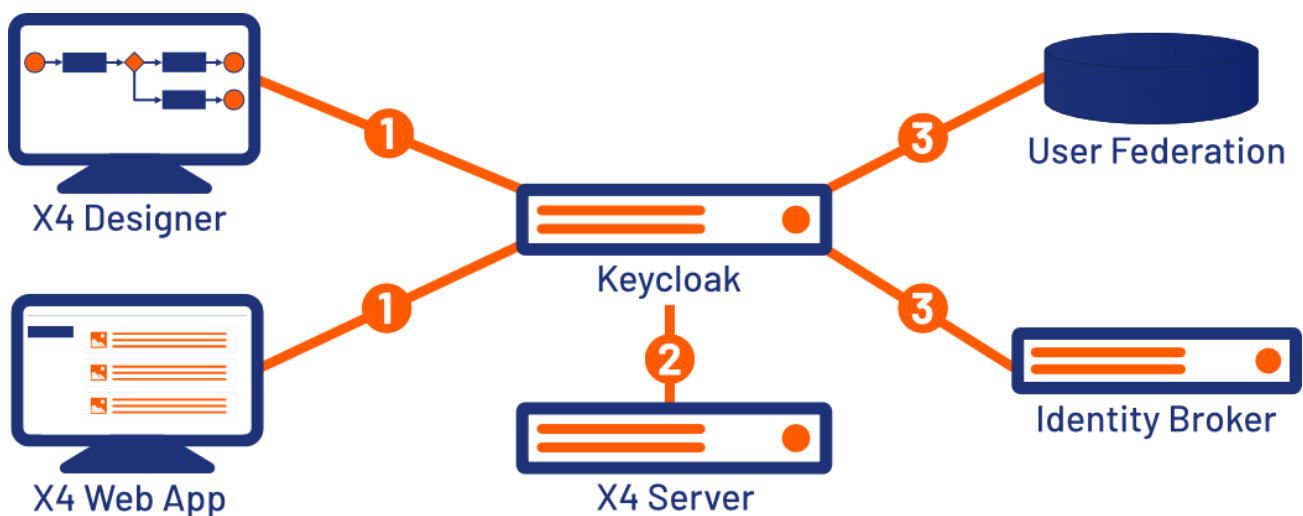
Neben der im X4 Server vorhandenen Scheduler-Implementierung kann auch ein externer Dienst Prozesse automatisiert starten. Dieser spricht die auszuführenden Prozesse direkt auf dem Server an, auf dem das Projekt A installiert ist.

6 Keycloak

⚠ Der Authentifizierungsprovider Keycloak muss installiert sein, um die X4 BPMS verwenden zu können.

Alle Komponenten der X4 BPMS verwenden den Authentifizierungsprovider Keycloak für die Authentifizierung und Autorisierung. Die Benutzer, Gruppen und Rollen werden in Keycloak verwaltet. Der mitgelieferte Keycloak ist bereit mithilfe einer zentralen Konfiguration angebunden.

Sie haben jedoch auch die Möglichkeit, bereits existierende Identity Provider wie zum Beispiel LDAP oder Active Directory mithilfe des mitgelieferten Keycloaks anzubinden. Keycloak unterstützt auch die Anbindung von externen Providern wie zum Beispiel Microsoft, Google oder Facebook.



1	Authentifizieren
2	Token-Erstellung und Validierung
3	Anbinden

Die Keycloak Administrationskonsole kann über die URL <http://localhost:8085/auth/admin/> geöffnet werden.

⚠ Potenzielle Sicherheitslücke

In der Testversion der X4 BPMS ist ein Defaultbenutzer mit Administrationsrechten vorinstalliert. Der Defaultbenutzer stellt bei einer Produktivnahme des Systems eine potenzielle Sicherheitslücke dar, sodass der Defaultbenutzer zwingend abgesichert werden muss. Deaktivieren Sie den Defaultbenutzer oder ändern Sie das Passwort in der Administrationskonsole von Keycloak.

Keycloak**Defaultbenutzer**

- Benutzername: admin
- Passwort: demo

Verfügbare Rollen

Rolle	Beschreibung
x4_admin_access	Gewährt Zugriff auf die X4 ReST-API.
x4_dev_access	Gewährt Zugriff auf den X4 Designer.
x4_dev_access_*	Gewährt Zugriff auf alle X4 Repositories.

X4 Designer**Defaultbenutzer**

- Benutzername: demo
- Passwort: demo

X4 Web Apps**Defaultbenutzer**

- Benutzername: demo
- Passwort: demo

Die offizielle Keycloak-Dokumentation ist über die URL <https://www.keycloak.org/documentation.html> erreichbar.

6.1 Hinweise zur verwendeten Datenbank

Keycloak wird standardmäßig mit einer H2-Datenbank ausgeliefert, damit das Keycloak ohne weitere Konfiguration verwendet werden kann. Die H2-Datenbank ist jedoch aufgrund von Sicherheitsmängeln und eingeschränkter Skalierbarkeit nicht für den produktiven Betrieb geeignet. Daher empfehlen wir den Einsatz einer alternativen Datenbank. Vor dem produktiven Einsatz des Keycloaks sollten Sie daher eine alternative Datenbank anbinden.

Wie Sie Datenbanken an Keycloak anbinden, wird in der offiziellen Keycloak-Dokumentation beschrieben.

- ✓ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_installation/index.html#_database.

6.2 Einrichten

6.2.1 Docker-Image laden und Container starten

In diesem Abschnitt erfahren Sie, wie sich der Authentifizierungsprovider Keycloak in Docker laden und als Container starten lässt.

Voraussetzungen

- Docker muss auf dem System installiert und eingerichtet sein. Informationen hierzu finden Sie in der Docker-Dokumentation unter <https://docs.docker.com/>.
- Kenntnisse der Docker-Funktionsweise werden vorausgesetzt.

1. Das von SoftProject bereitgestellte Installationspaket `keycloak-image.tar` mit dem Kommando `docker load -i keycloak-image.tar` auf Ihr System laden.
2. Docker mit dem Kommando `docker run -d -p 8085:8085 --name keycloak softprojectgmbh/keycloak` ausführen.

6.2.2 Eigene Keycloak-Installation anbinden

Falls die enthaltene Keycloak-Installation durch eine eigene Keycloak-Installation ersetzt werden soll, muss eine Keycloak-Konfigurationsdatei im Serververzeichnis unter **\configurations\keycloak_config.json** erstellt werden.

Die Konfiguration wird in dem `connection` Element vorgenommen.

Beispiel

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

Folgende Rollen müssen in Keycloak erstellt werden:

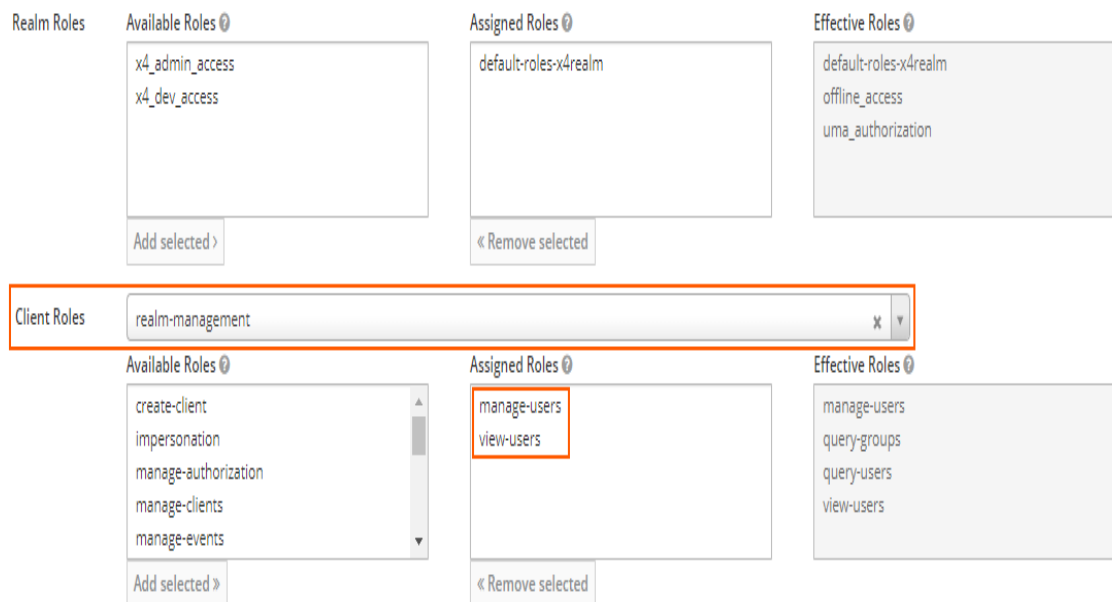
Rolle	Beschreibung
x4_admin_access	Gewährt Zugriff auf die X4 ReST-API.
x4_dev_access	Gewährt Zugriff auf den X4 Designer.
x4_dev_access_*	Gewährt Zugriff auf alle X4 Repositories.

Um die X4 ReST-API zu verwenden, muss dem entsprechenden Benutzer die folgenden Rechte erteilt werden:

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

System 

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



The screenshot shows the 'Role Mappings' tab for a client. It displays four panels: 'Realm Roles' (x4_admin_access, x4_dev_access), 'Available Roles' (x4_admin_access, x4_dev_access), 'Assigned Roles' (default-roles-x4realm), and 'Effective Roles' (default-roles-x4realm, offline_access, uma_authorization). Below these, the 'Client Roles' dropdown is set to 'realm-management'. Underneath, the 'Assigned Roles' list is highlighted with an orange box and contains 'manage-users' and 'view-users'.



Weitere Informationen zur Konfigurationsdatei finden Sie unter https://www.keycloak.org/docs/latest/securing_apps/index.html#_java_adapter_config.

6.3 Konfigurieren

6.3.1 Authorization Code Flow anwenden

Die X4 BPMS unterstützt verschiedene Autorisierungsabläufe und das Single Sign-on-Authentifizierungsverfahren. Um die Autorisierungsabläufe für X4 Web Apps anzuwenden, müssen Sie in der Administrationskonsole von Keycloak im Bereich **Client** den Pfad zur Web App unter **Valid Redirect URIs** eintragen.

Authorization Enabled  ☒ ON

Root URL 

* Valid Redirect URIs   

✔ Weitere Informationen finden Sie im Abschnitt Configuration.

6.3.2 Zugriff auf X4 Repository einschränken

Der Zugriff auf einzelne Workspaces kann mithilfe von Rollen eingeschränkt werden. Dazu muss in der Keycloak Administrator Konsole eine neue Rolle mit dem Namen **x4_dev_access_<Workspace-Name>** angelegt werden. Die Verknüpfung zum Workspace wird anhand des Rollennamens hergestellt.

6.3.2.1 Beispiel

Um den Workspace **2** mithilfe einer Rolle einzuschränken, wird in Keycloak die Rolle **x4_dev_access_2** erstellt. Nur Benutzer, die der Rolle **x4_dev_access_2** zugewiesen werden, haben Zugriff auf den Workspace.

6.3.3 Standardkonfiguration

In diesem Abschnitt wird die Standardkonfiguration des Authentifizierungsproviders im Auslieferungszustand beschrieben.

6.3.3.1 Realm Settings

6.3.3.1.1 General

Label	Wert
Name	X4Realm
Enabled	ON

6.3.3.1.2 Login

Label	Wert
User registration	OFF
Edit username	OFF
Forgot password	OFF
Remember Me	OFF

Verify email	OFF
Login with email	ON
Require SSL	external requests

6.3.3.1.3 Tokens

Label	Wert
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

6.3.3.1.4 Security Defenses

Label	Wert
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

6.3.3.2.1 Settings

Label	Wert
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

6.3.3.2.1.1 Fine Grain OpenID Connect Configuration

Label	Wert
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

6.3.3.2.1.2 OpenID Connect Compatibility Modes

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

6.3.3.2.1.3 Advanced Settings

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

6.3.3.2.2 Credentials

Label	Wert
Client Authenticator	Client Id and Secret

6.3.3.2.3 Client Scopes

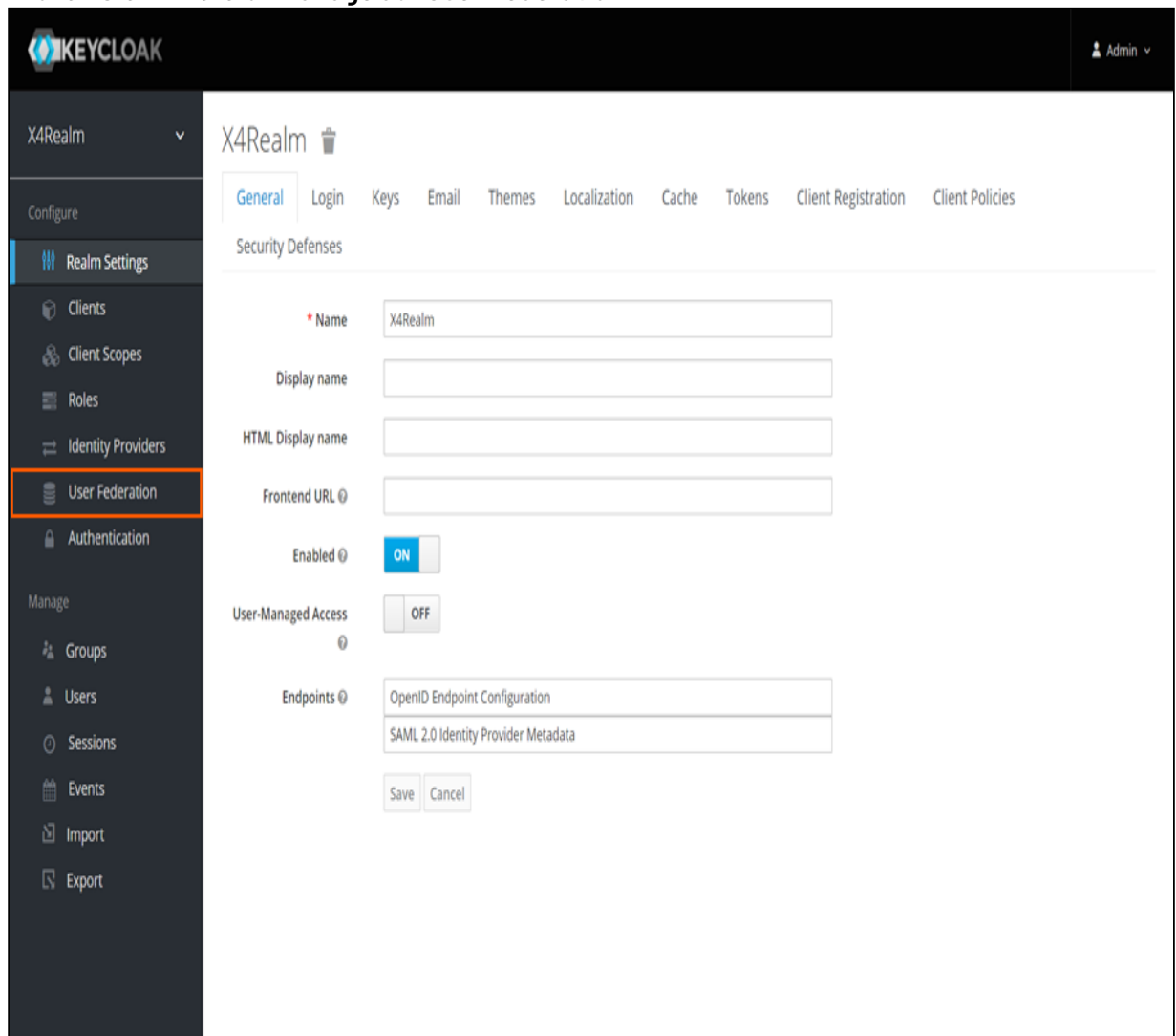
Label	Wert
Assigned Default Client Scopes	• email • profile • roles • web-origins
Assigned Optional Client Scopes	• address • microprofile-jwt • offline_access • phone

6.3.4 LDAP anbinden

In Keycloak können Sie ein bestehendes LDAP anbinden. Keycloak verfügt über einen eingebauten LDAP/AD-Anbieter. Es ist möglich, mehrere verschiedene LDAP-Server in denselben Keycloak-Realm einzubinden.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **User Federation**.

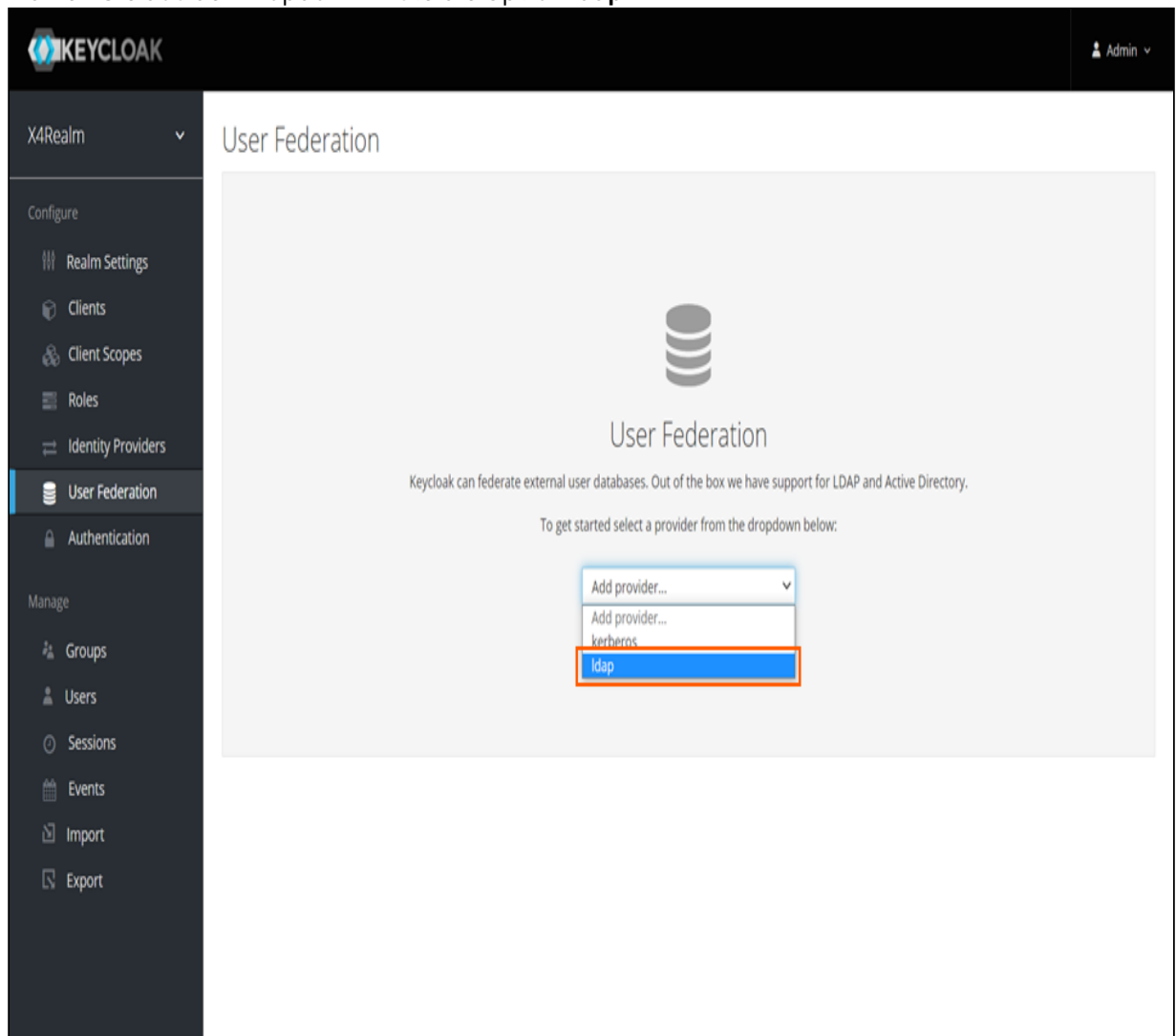


The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the Keycloak logo and the user 'Admin'. The left sidebar contains the 'Configure' section with 'Realm Settings' expanded, and the 'Manage' section with 'User Federation' highlighted. The main content area is titled 'X4Realm' and shows the 'General' tab 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 of the form are 'Save' and 'Cancel' buttons.

3. Wählen Sie aus der Dropdown-Liste die Option **ldap**.



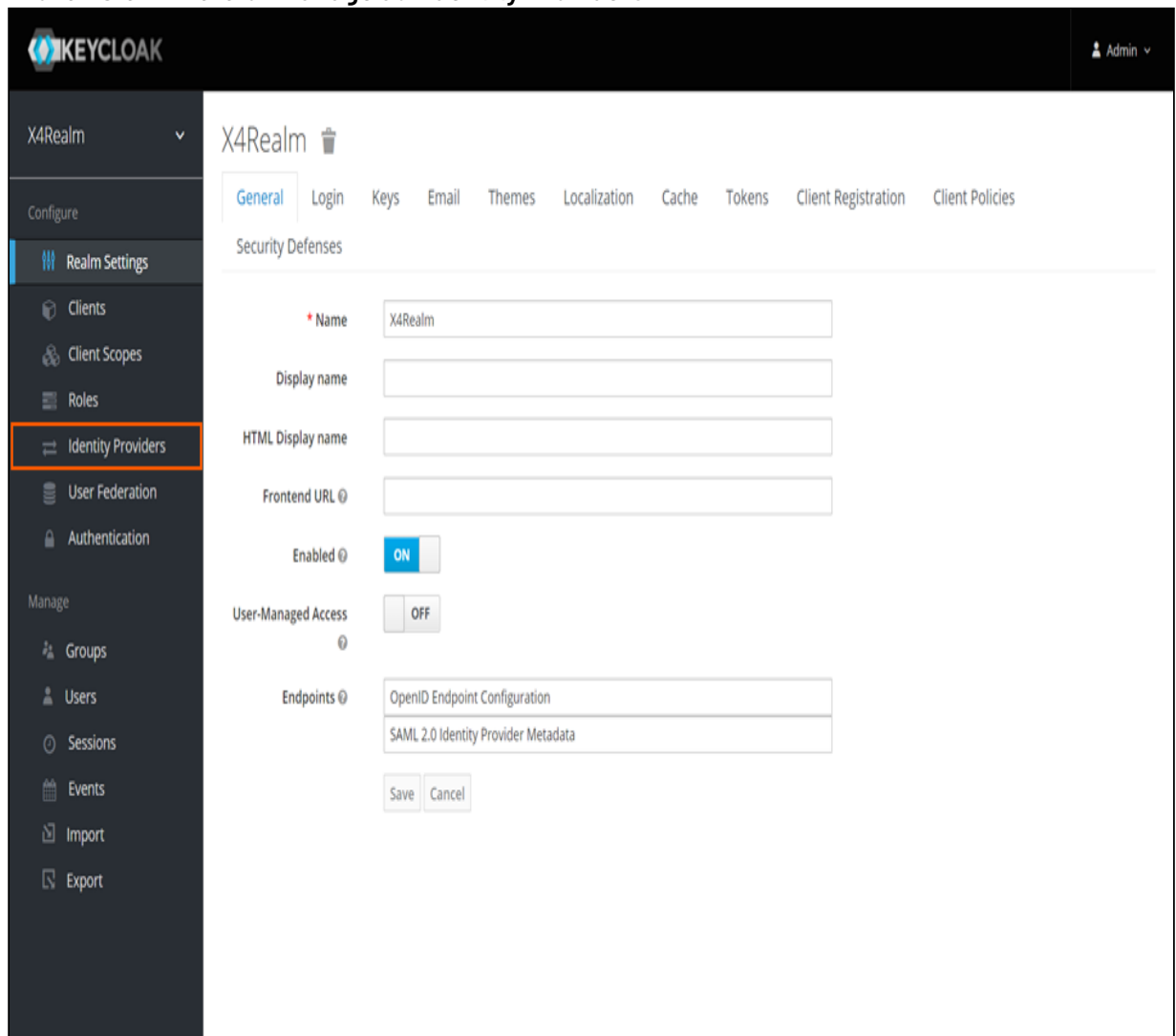
✓ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_ldap.

6.3.5 SAML v2.0 anbinden

In Keycloak können Sie ein bestehendes SAML v2.0 anbinden. Keycloak kann Identitätsanbieter vermitteln, die auf dem SAML v2.0 Protokoll basieren.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **Identity Providers**.



The screenshot displays the Keycloak administration console. The top navigation bar shows the 'KEYCLOAK' logo and the user 'Admin'. The left sidebar is divided into 'Configure' and 'Manage' sections. Under 'Configure', 'Realm Settings' is selected, and 'Identity Providers' is highlighted with an orange box. 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. The configuration fields include: 'Name' (X4Realm), 'Display name' (empty), 'HTML Display name' (empty), 'Frontend URL' (empty), 'Enabled' (toggle set to ON), 'User-Managed Access' (toggle set to 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

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

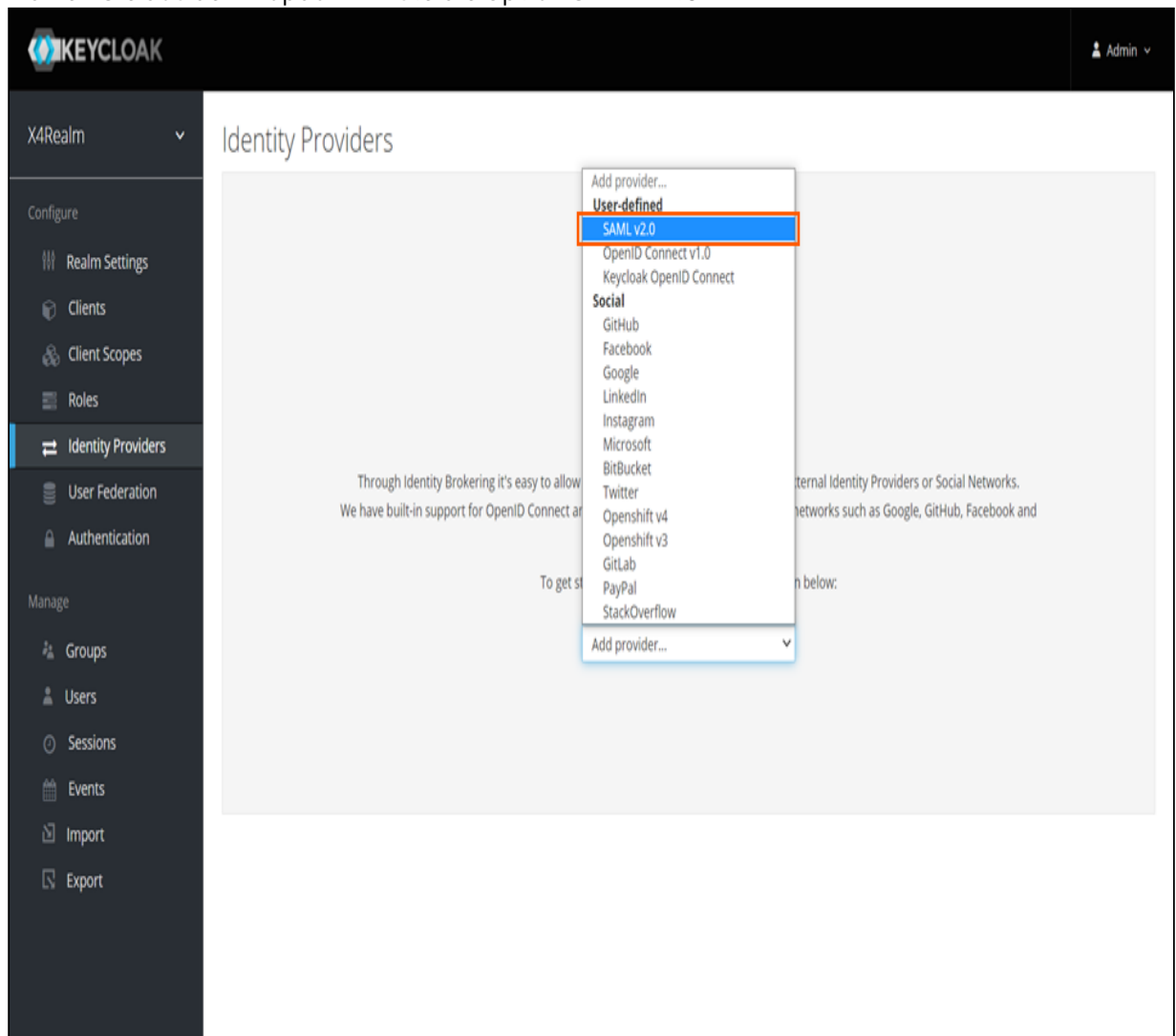
Enabled ON

User-Managed Access OFF

Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Save Cancel

3. Wählen Sie aus der Dropdown-Liste die Option **SAML v2.0**.



Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#saml-v2-0-identity-providers.

6.3.6 Kerberos anbinden

In Keycloak können Sie ein bestehendes Kerberos anbinden. Keycloak unterstützt die Anmeldung mit einem Kerberos-Ticket über das SPNEGO-Protokoll.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **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 'Configure' section with 'Realm Settings' expanded, and the 'Manage' section with 'User Federation' highlighted. The main content area is titled 'X4Realm' and shows the 'General' tab under 'Security Defenses'. The configuration fields include: 'Name' (X4Realm), 'Display name', 'HTML Display name', 'Frontend URL', '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

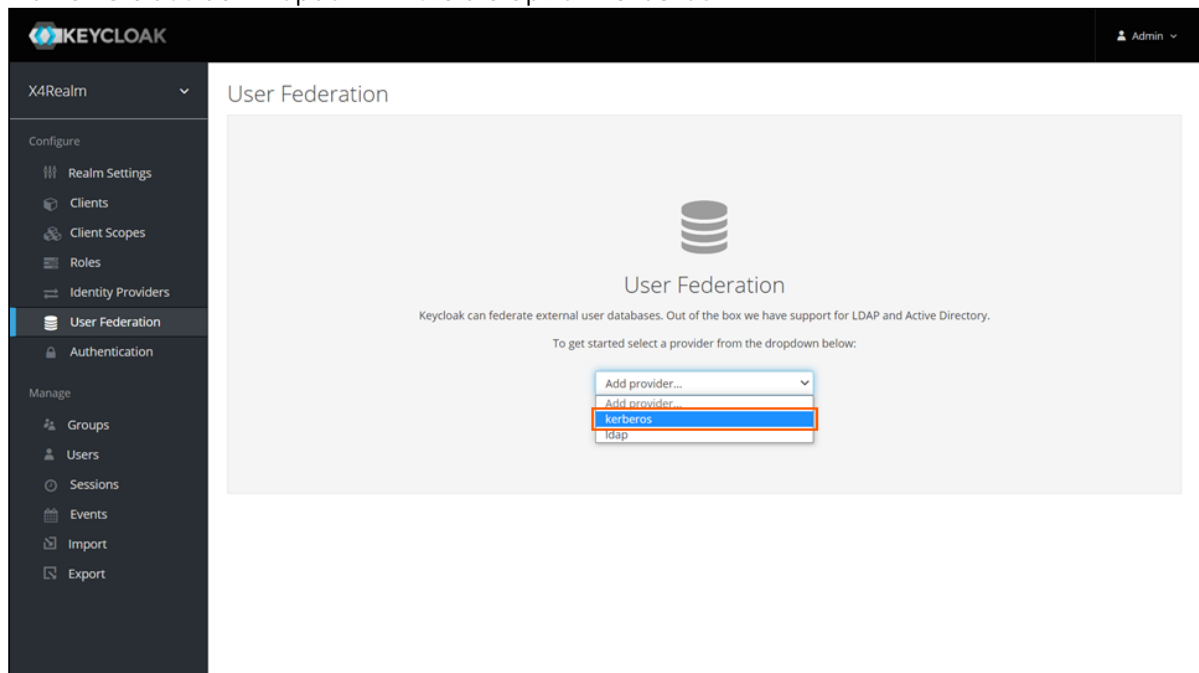
Enabled ON

User-Managed Access OFF

Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Save Cancel

3. Wählen Sie aus der Dropdown-Liste die Option **kerberos**.



- ✓ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_kerberos.

6.3.7 Social Identity-Anbieter anbinden

In Keycloak können Sie verschiedene Social Identity-Anbieter anbinden. Keycloak bietet integrierte Unterstützung für die gängigsten sozialen Netzwerke, wie Google, Facebook, Twitter, GitHub, LinkedIn, Microsoft und Stack Overflow.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **Identity Providers**.

The screenshot shows the Keycloak Administration Console interface. On the left, a sidebar menu is visible with the 'Identity Providers' option highlighted. The main content area displays the configuration for the 'X4Realm'. The 'General' tab is selected, showing fields for 'Name' (X4Realm), 'Display name', 'HTML Display name', and 'Frontend URL'. The 'Enabled' toggle is set to 'ON', and 'User-Managed Access' is set to 'OFF'. The 'Endpoints' section lists 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. 'Save' and 'Cancel' buttons are at the bottom.

3. Wählen Sie aus der Dropdown-Liste den gewünschten Social Identity-Anbieter.

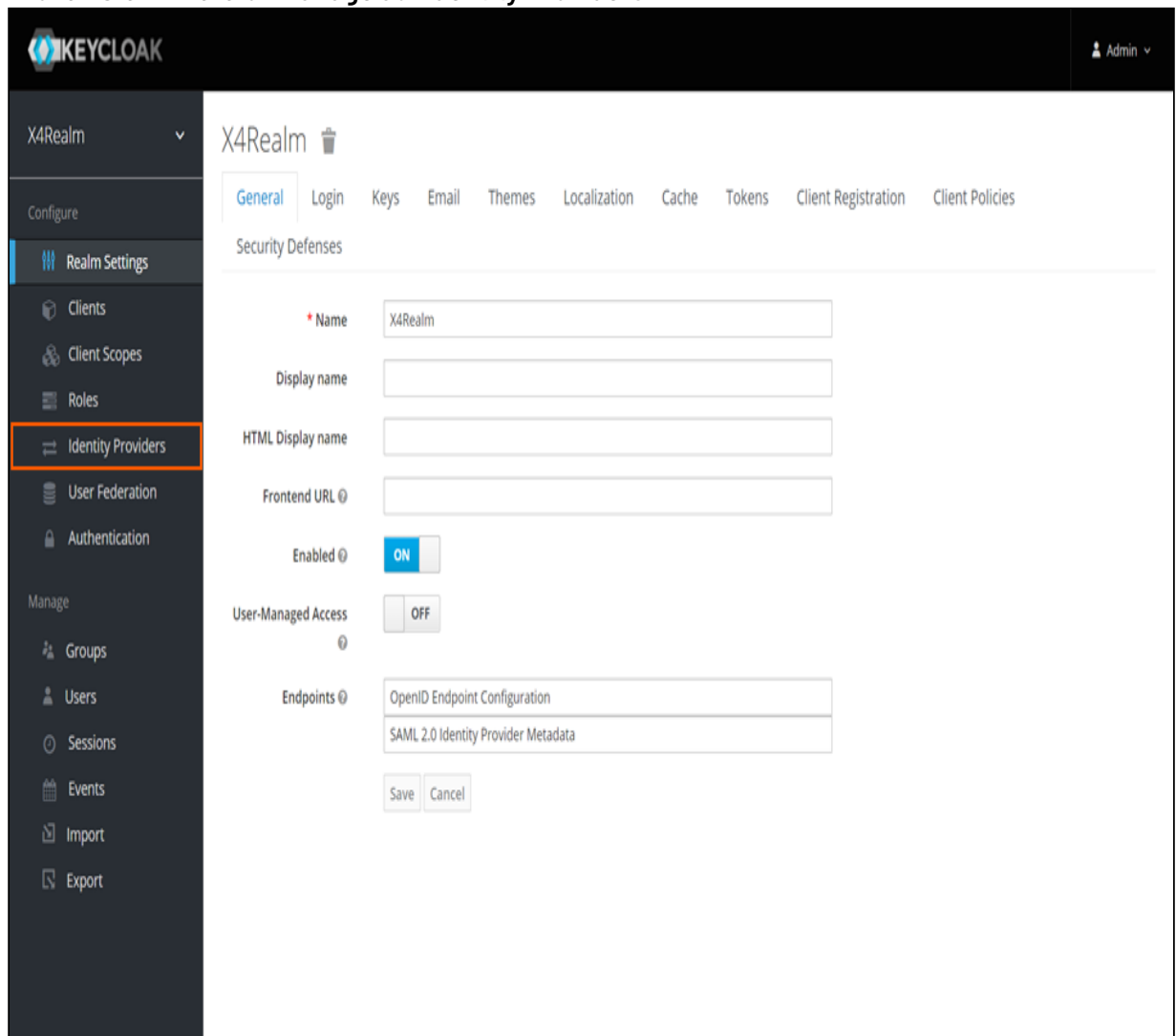
✓ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#social-identity-providers.

6.3.8 OpenID Connect anbinden

In Keycloak können Sie einen bestehenden OpenID Connect-Anbieter anbinden. Der Identitätsanbieter muss den Authorization Code Flow unterstützen, um den Benutzer zu authentifizieren und den Zugriff zu autorisieren.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **Identity Providers**.

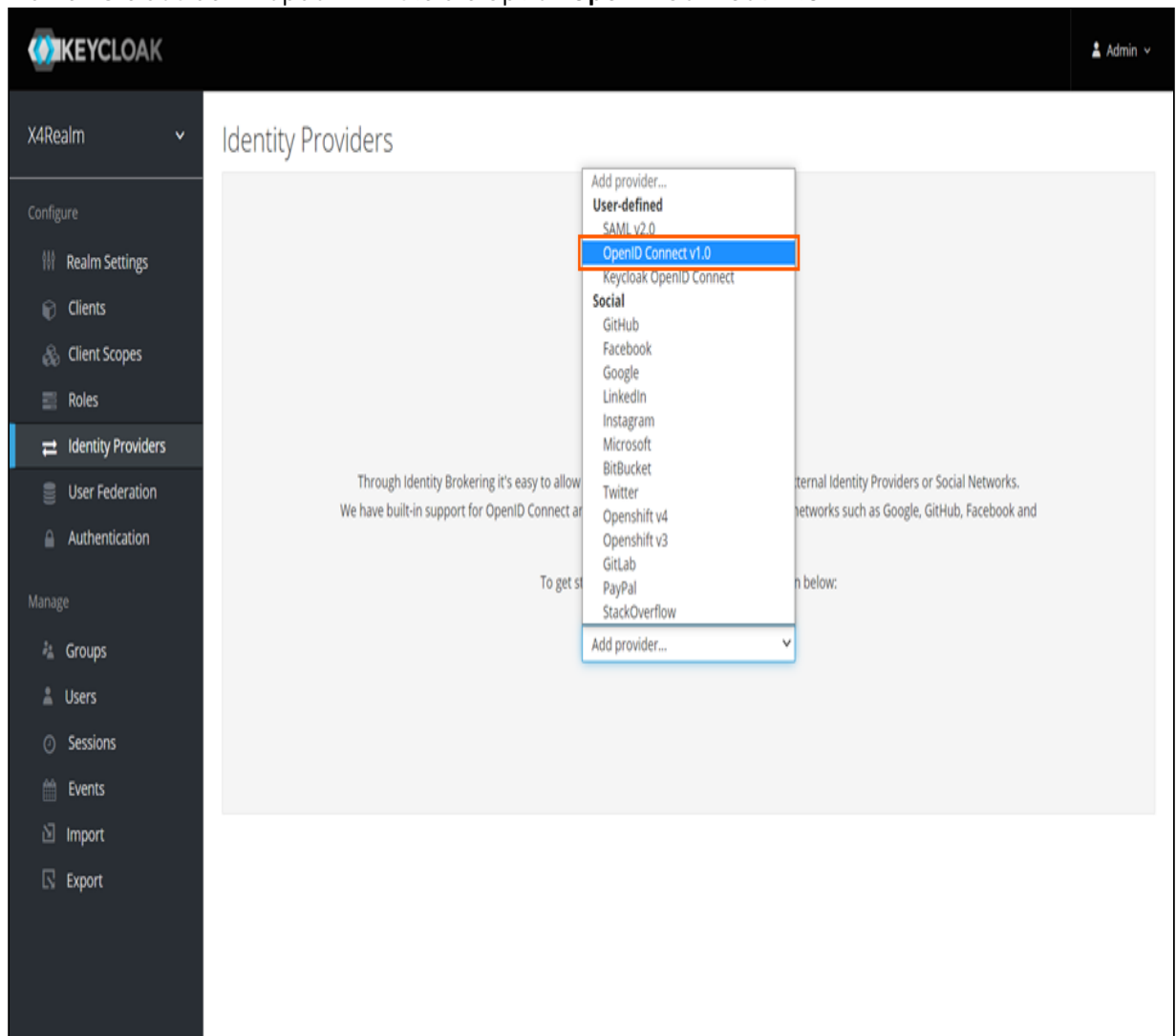


The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the 'KEYCLOAK' logo and the user 'Admin'. The left sidebar is divided into 'Configure' and 'Manage' sections. Under 'Configure', 'Realm Settings' is selected, and 'Identity Providers' is highlighted with an orange box. The main content area is titled 'X4Realm' and shows the 'General' tab for '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. Wählen Sie aus der Dropdown-Liste die Option **OpenID Connect v1.0**.



✔ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_identity_broker_oidc.

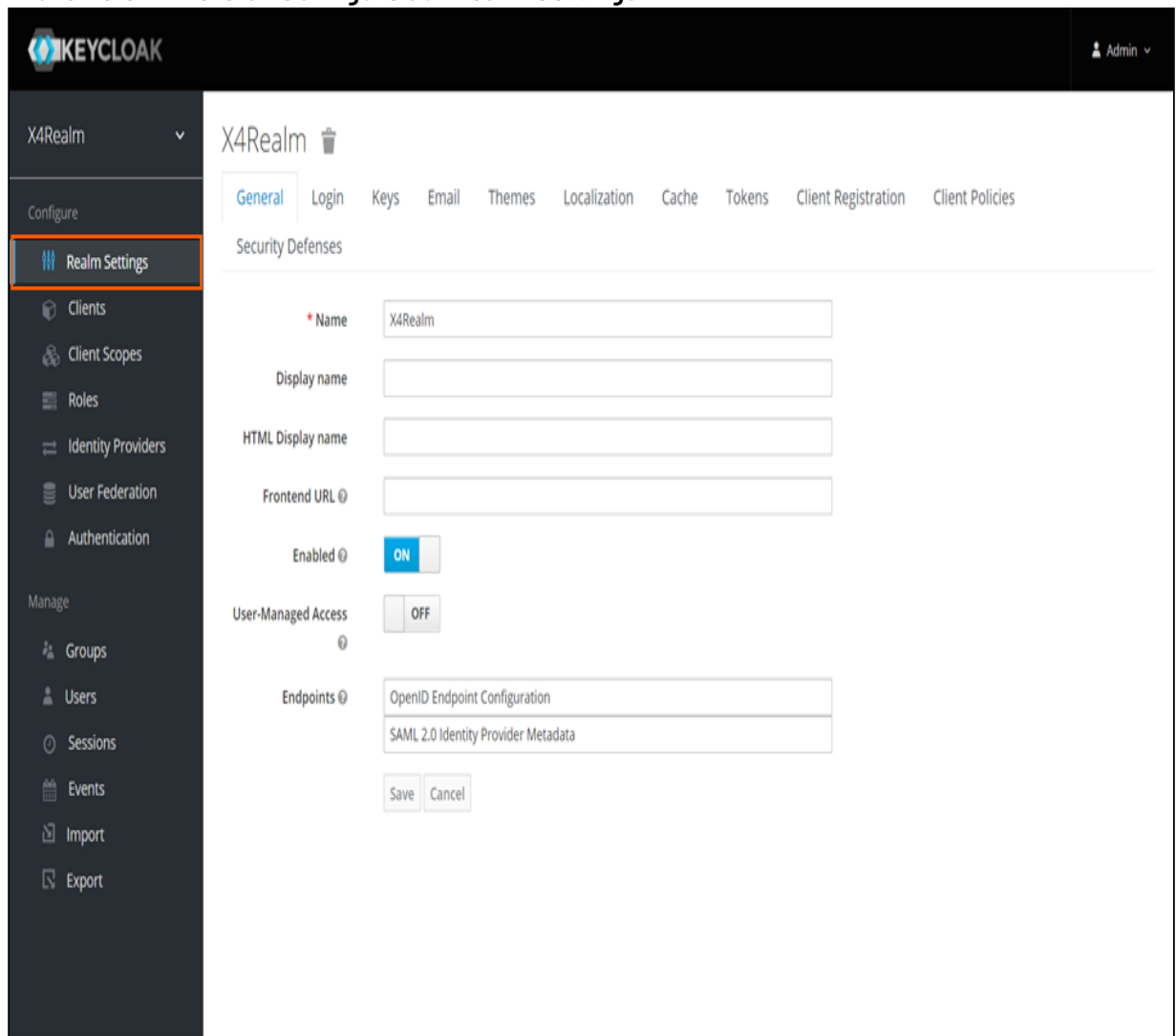
6.3.9 Anmeldeseite

6.3.9.1 Angemeldet bleiben-Schaltfläche

Die Angemeldet bleiben-Schaltfläche kann in der Keycloak Administrationskonsole im Realm Settings Menü aktiviert werden.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Configure** auf **Realm Settings**.



The screenshot displays the Keycloak Admin Console interface. The top navigation bar shows the Keycloak logo and the user 'Admin'. The left sidebar contains a 'Configure' section with 'Realm Settings' highlighted. The main content area is titled 'X4Realm' and features a tabbed interface with 'General' selected. Under the 'General' tab, the 'Security Defenses' section is visible, containing the following fields and controls:

- Name:** X4Realm
- Display name:** (empty text input)
- HTML Display name:** (empty text input)
- Frontend URL:** (empty text input)
- 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 form are 'Save' and 'Cancel' buttons.

3. Wechseln Sie in die Registerkarte **Login**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar contains a navigation menu with categories like 'Configure', 'Realm Settings', and 'Manage'. The 'Login' tab is selected and highlighted with a red box. The main content area displays the 'Security Defenses' section with various configuration fields: 'Name' (X4Realm), 'Display name', 'HTML Display name', 'Frontend URL', 'Enabled' (toggle ON), 'User-Managed Access' (toggle OFF), and 'Endpoints' (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK

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

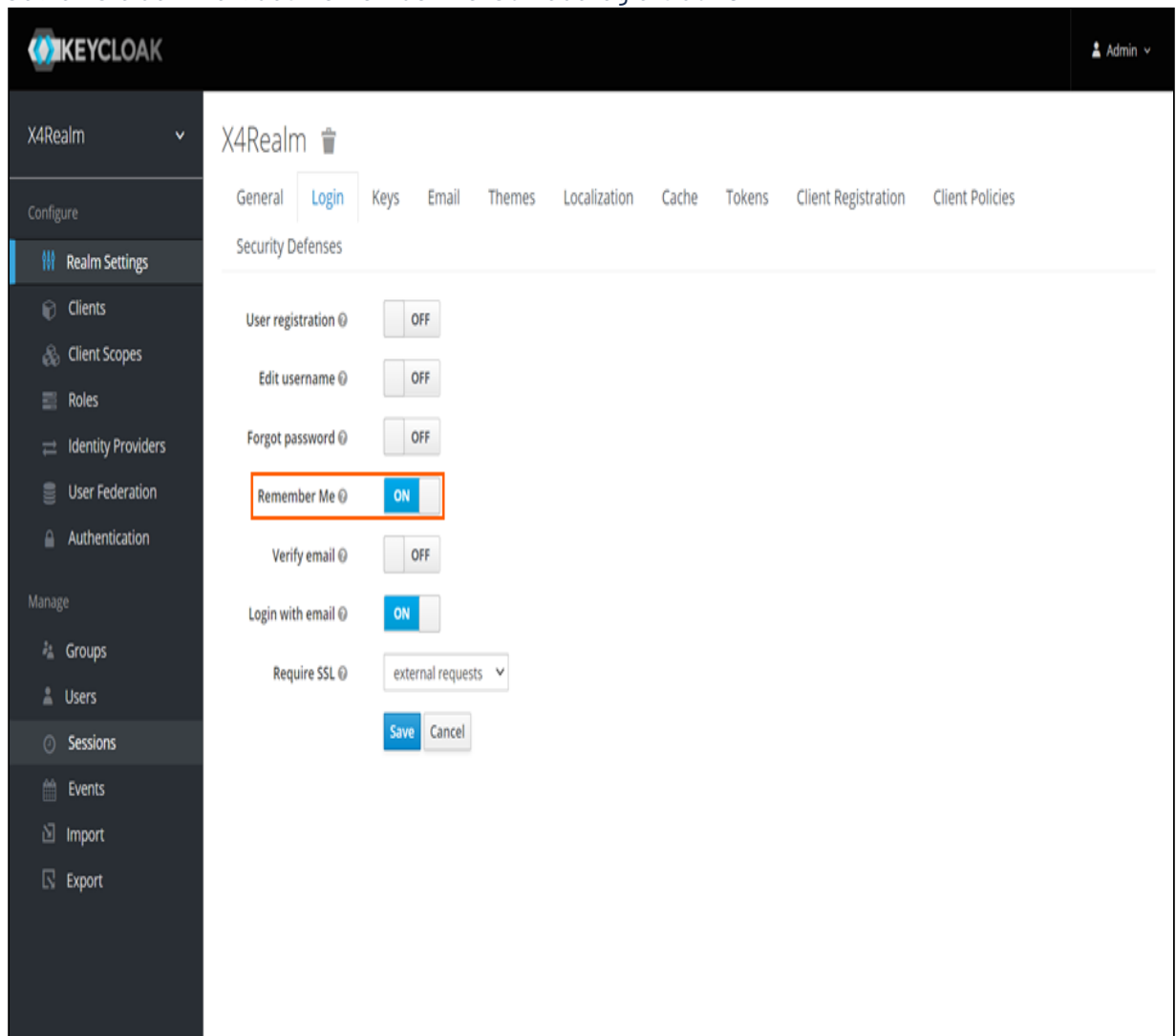
Endpoints

OpenID Endpoint Configuration

SAML 2.0 Identity Provider Metadata

Save Cancel

4. Setzen Sie den Wert des **Remember Me**-Schiebereglers auf **ON**.



5. Klicken Sie auf **Save**.

6.3.9.2 Passwort vergessen-Schaltfläche

Die Passwort vergessen-Schaltfläche kann in der Keycloak Administrationskonsole im Realm Settings Menü aktiviert werden.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Configure** auf **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. A sidebar on the left contains a 'Configure' section with 'Realm Settings' highlighted in orange. Below this, there are sections for 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', 'Authentication', and a 'Manage' section with 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The main content area is titled 'X4Realm' and features a tabbed interface with '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' (toggle set to ON), 'User-Managed Access' (toggle set to 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. Wechseln Sie in die Registerkarte **Login**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar contains a navigation menu with categories like 'Configure', 'Realm Settings', and 'Manage'. The 'Login' tab is selected and highlighted with a red box. The main content area displays the 'Security Defenses' section with various configuration fields: 'Name' (X4Realm), 'Display name', 'HTML Display name', 'Frontend URL', 'Enabled' (toggle ON), 'User-Managed Access' (toggle OFF), and 'Endpoints' (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK

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

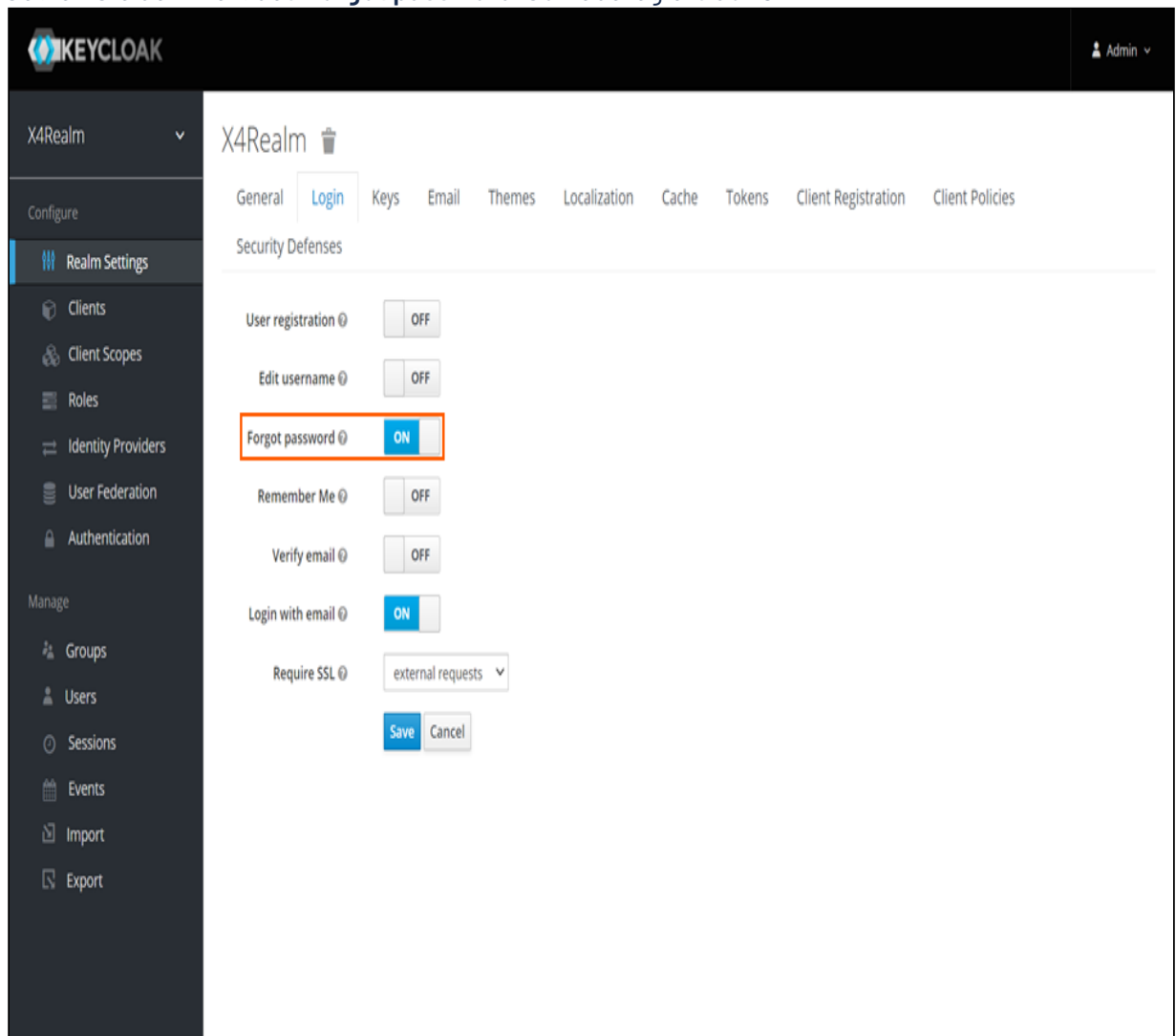
Endpoints

OpenID Endpoint Configuration

SAML 2.0 Identity Provider Metadata

Save Cancel

4. Setzen Sie den Wert des **Forgot password**-Schiebereglers auf **ON**.



5. Klicken Sie auf **Save**.

6.3.9.3 Registrierung aktivieren

Die Registrieren-Schaltfläche kann in der Keycloak Administrationskonsole im Realm Settings Menü aktiviert werden.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Configure** auf **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. A sidebar on the left contains a 'Configure' section with 'Realm Settings' highlighted by an orange border. Below 'Configure' are sections for 'Clients' and 'Manage' with various sub-items. The main content area is titled 'X4Realm' and features a tabbed interface with 'General' selected. The 'General' tab shows 'Security Defenses' settings, including 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' (OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata) and 'Save'/'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. Wechseln Sie in die Registerkarte **Login**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The left sidebar contains a navigation menu with categories like 'Configure', 'Realm Settings', and 'Manage'. The 'Login' tab is selected and highlighted with a red box. The main content area displays the 'Security Defenses' section with various configuration fields: 'Name' (X4Realm), 'Display name', 'HTML Display name', 'Frontend URL', 'Enabled' (toggle ON), 'User-Managed Access' (toggle OFF), and 'Endpoints' (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). 'Save' and 'Cancel' buttons are at the bottom.

KEYCLOAK

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

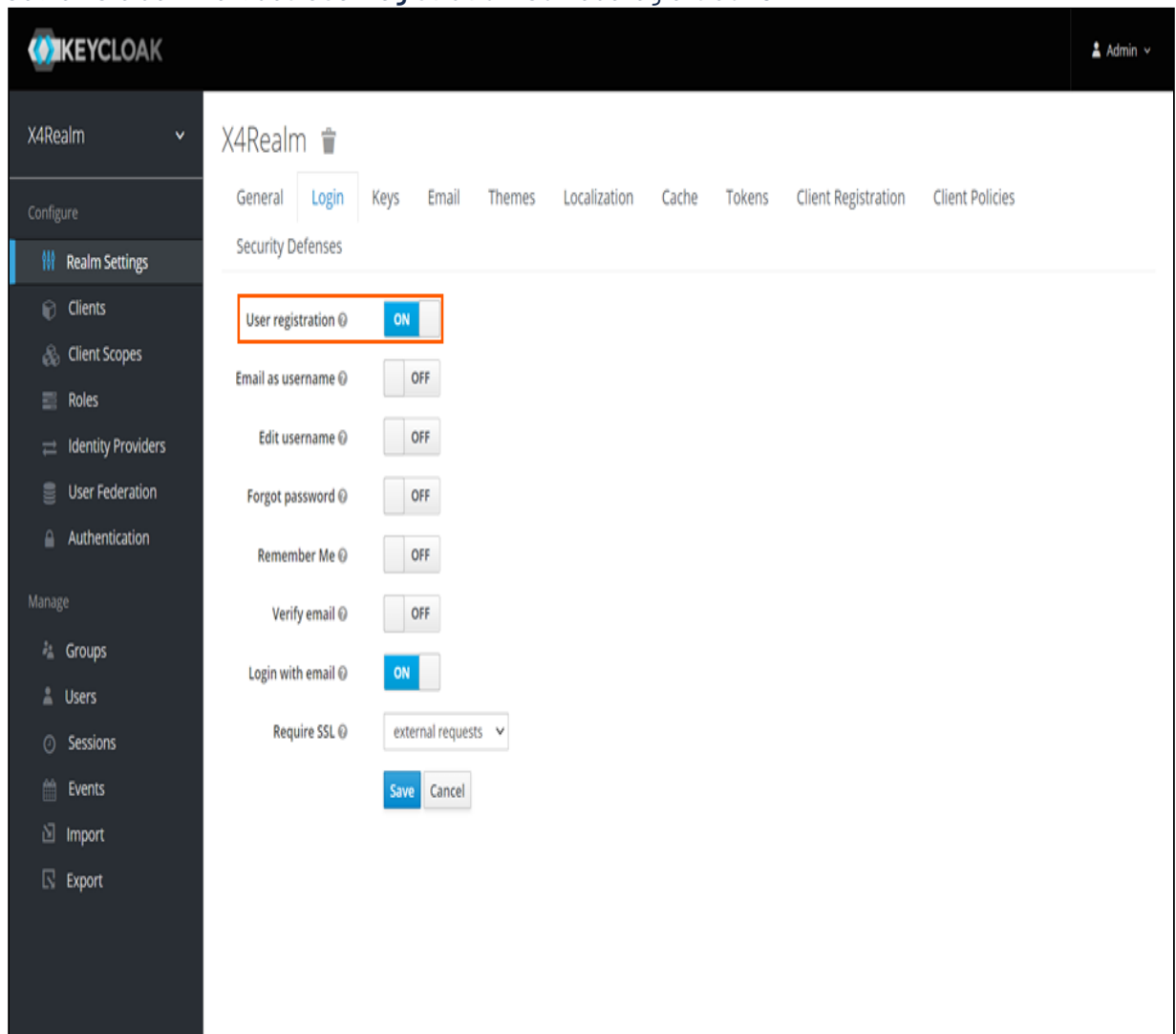
Endpoints

OpenID Endpoint Configuration

SAML 2.0 Identity Provider Metadata

Save Cancel

4. Setzen Sie den Wert des **User registration**-Schiebereglers auf **ON**.



Der **Email as username**-Schieberegler wird eingeblendet.

5. Wenn die zur Registrierung verwendete E-Mail als Benutzername verwendet werden soll, setzen Sie den Wert des **Email as username**-Schiebereglers auf **ON**.
6. Klicken Sie auf **Save**.

6.3.10 Passwörter

In Keycloak können Sie verschieden Einstellungen zu Passwörtern festlegen, wie zum Beispiel Passwortrichtlinien.

6.3.10.1 Passwortrichtlinien festlegen

In Keycloak können Sie verschiedene Passwortrichtlinien festlegen.

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Configure** auf **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

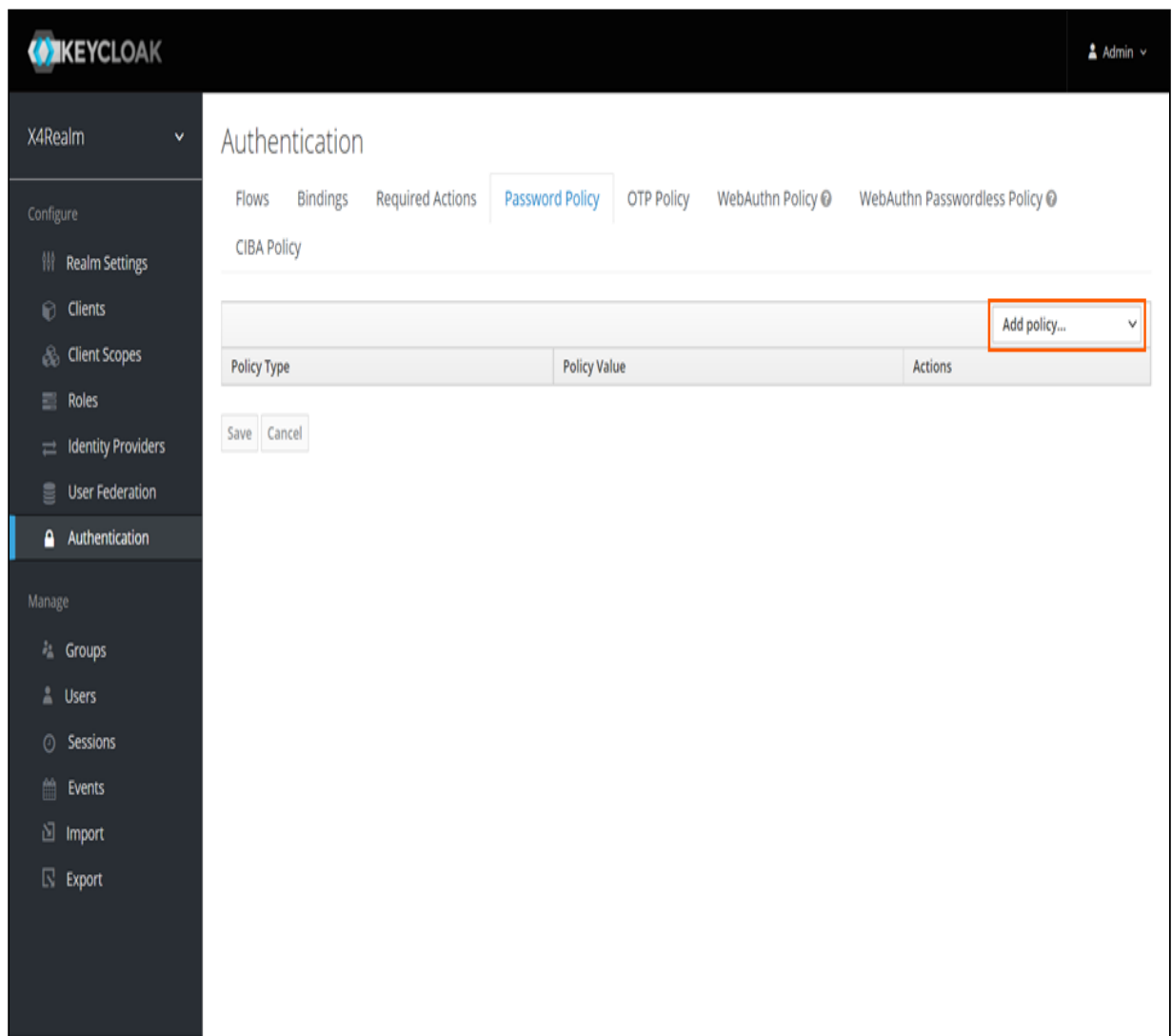
Save Cancel

3. Wechseln Sie in die Registerkarte **Password Policy**.

The screenshot shows the Keycloak Administration Console interface. The left sidebar contains navigation menus for 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The main content area is titled 'Authentication' and includes tabs for 'Flows', 'Bindings', 'Required Actions', 'Password Policy' (highlighted with an orange box), 'OTP Policy', 'WebAuthn Policy', and 'WebAuthn Passwordless Policy'. Below the tabs is a 'CIBA Policy' section. The main table displays authentication requirements for the 'Browser' flow. The table has columns for 'Auth Type', 'Requirement', and 'Actions'. The requirements listed are: Cookie, Kerberos, Identity Provider Redirector, Forms, Username Password Form, Browser - Conditional OTP, Condition - User Configured, and OTP Form. Each requirement has radio buttons for 'REQUIRED', 'ALTERNATIVE', and 'DISABLED' states. The 'Forms' requirement has an additional 'CONDITIONAL' state. The 'Actions' column shows a dropdown menu for each requirement.

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

4. Wählen Sie aus der Dropdown-Liste **Add policy** die Passwortrichtlinien aus, die Sie hinzufügen möchten.



5. Klicken Sie auf **Save**.

- ✓ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#password-policy-types.

6.3.11 Themes

Sie können in Keycloak ein vordefiniertes Theme für die Anmeldeseite verwenden oder eine individuelle Anmeldeseite gestalten.

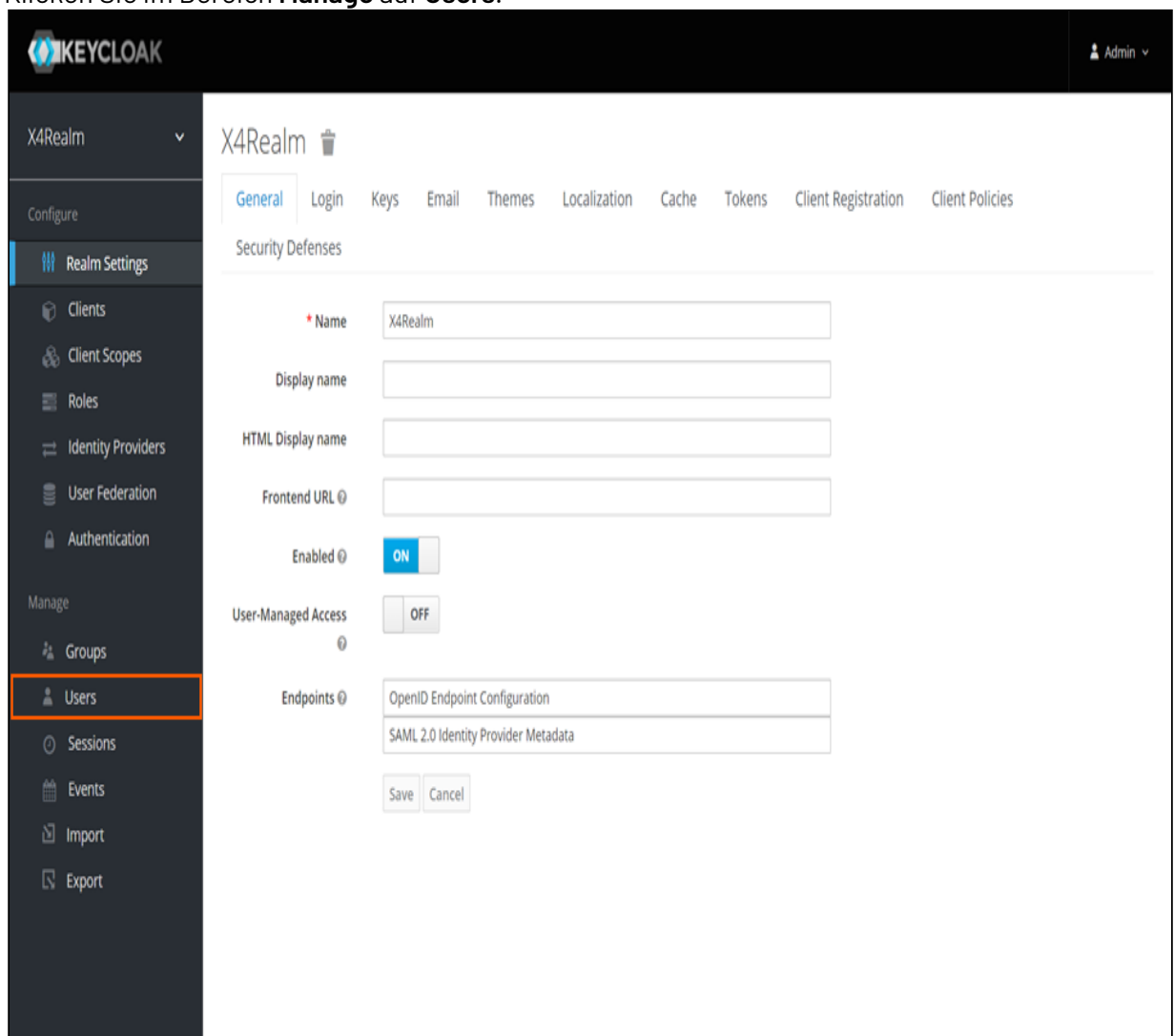
- ✓ Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_themes.

6.4 Benutzer

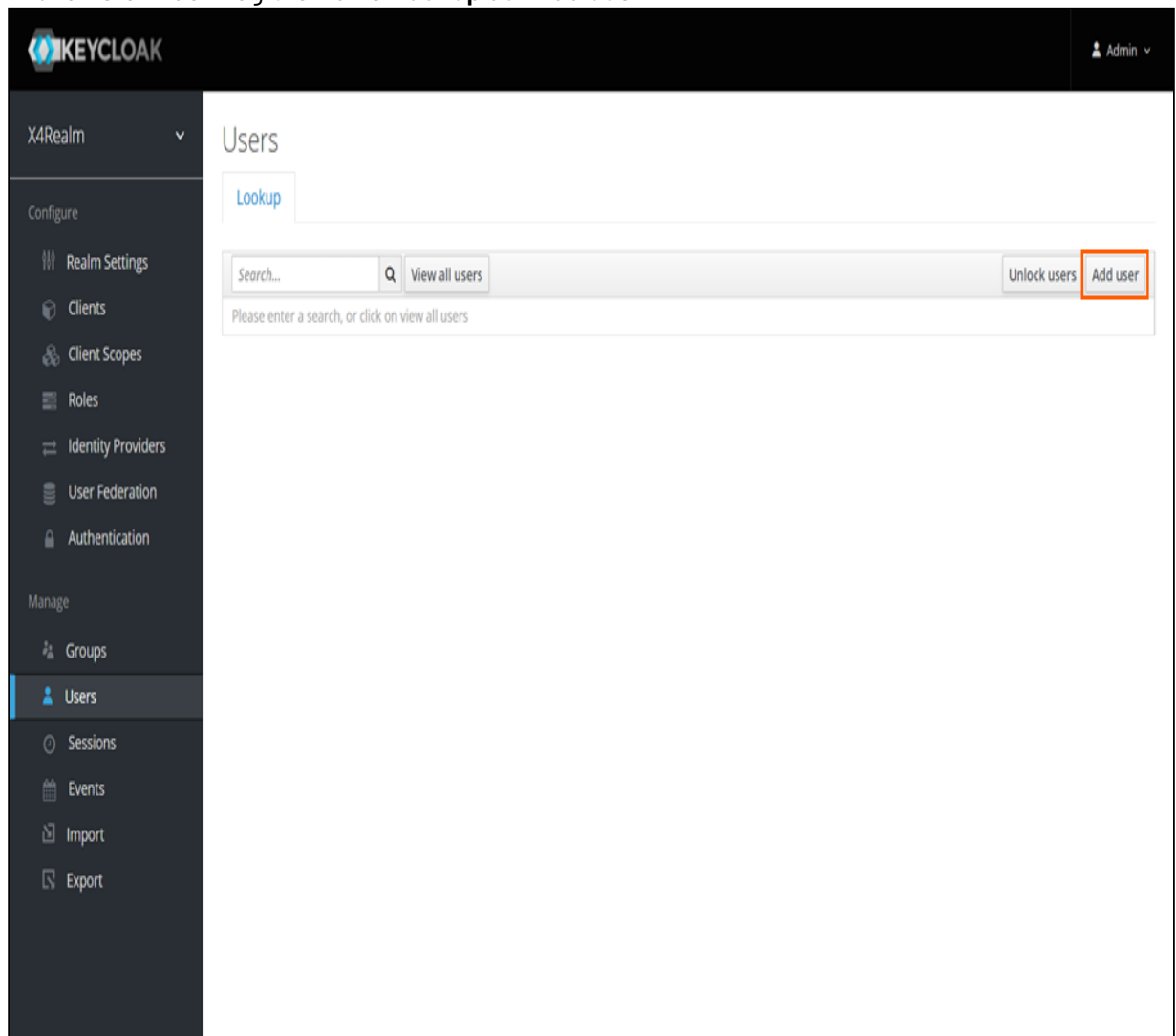
6.4.1 Benutzer erstellen

⚠ Wenn eine Web App den Autorisierungsablauf `Ressource Owner Password Flow` verwendet, kann sich ein Benutzer mit einem temporären Passwort nicht an dieser Web App anmelden.
Wenn Sie temporäre Passwörter einsetzen möchten, verwenden Sie den Autorisierungsablauf `Authorization Code Flow`.

1. Öffnen Sie die **Keycloak Administrationskonsole**.
2. Klicken Sie im Bereich **Manage** auf **Users**.



3. Klicken Sie in der Registerkarte **Lookup** auf **Add user**.



4. Tragen Sie die relevanten Daten ein.
5. Klicken Sie auf **Save**.

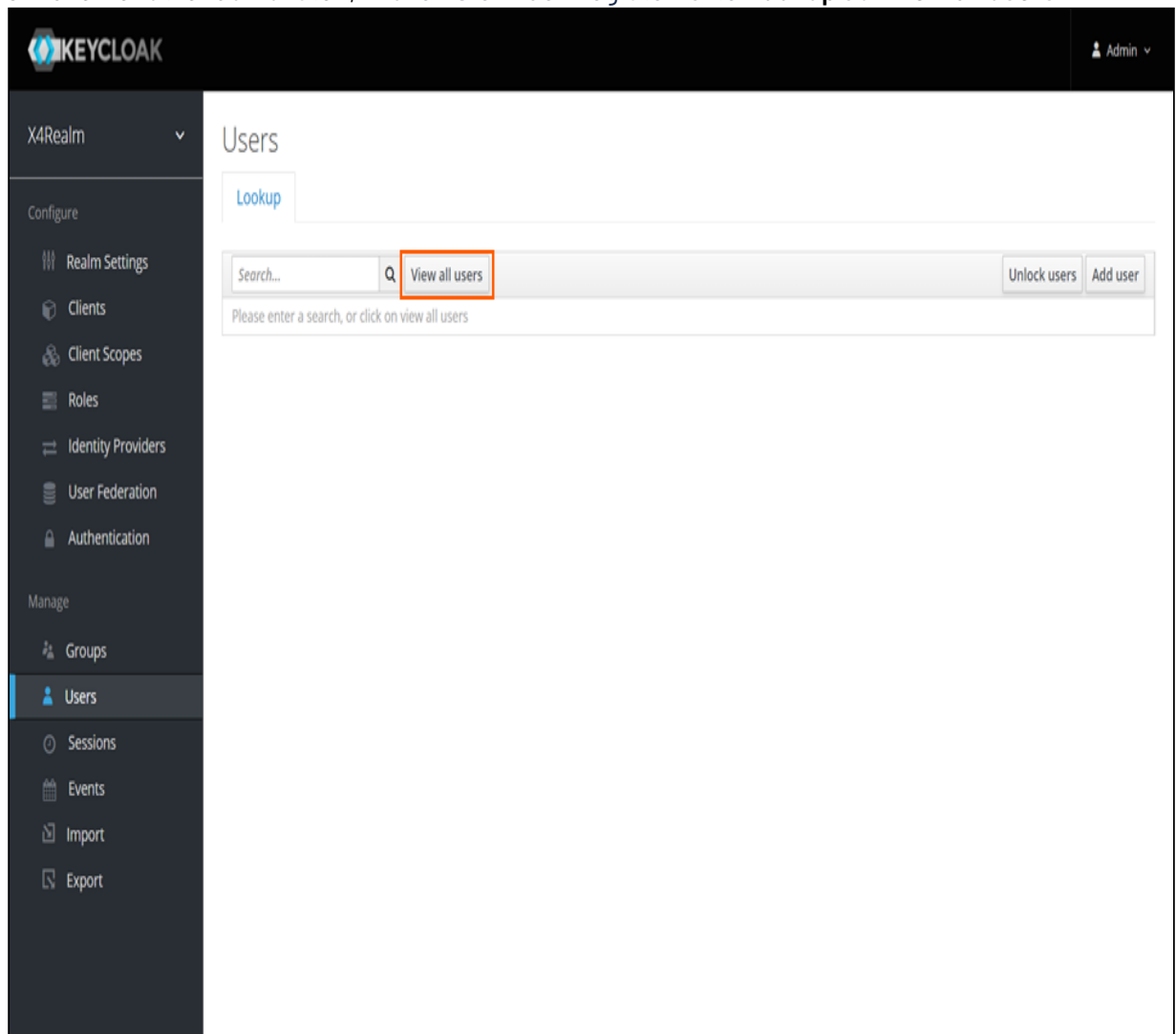
6.4.2 Benutzer eine Rolle zuweisen

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **Users**.

The screenshot displays the Keycloak administration interface for the 'X4Realm'. The top navigation bar includes the Keycloak logo and a user profile 'Admin'. 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, showing 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 fields for 'Endpoints' (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata) and 'Save'/'Cancel' buttons.

3. Um alle Benutzer aufzulisten, klicken Sie in der Registerkarte **Lookup** auf **View all users**.



4. Klicken Sie in der Zeile des gewünschten Benutzers in der Spalte **Actions** auf **Edit**.

The screenshot shows the Keycloak administration interface for the 'X4Realm'. The 'Users' section is active in the sidebar. The main content area shows a table of users. The 'Actions' column for each user contains 'Edit', 'Impersonate', and 'Delete' buttons. 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

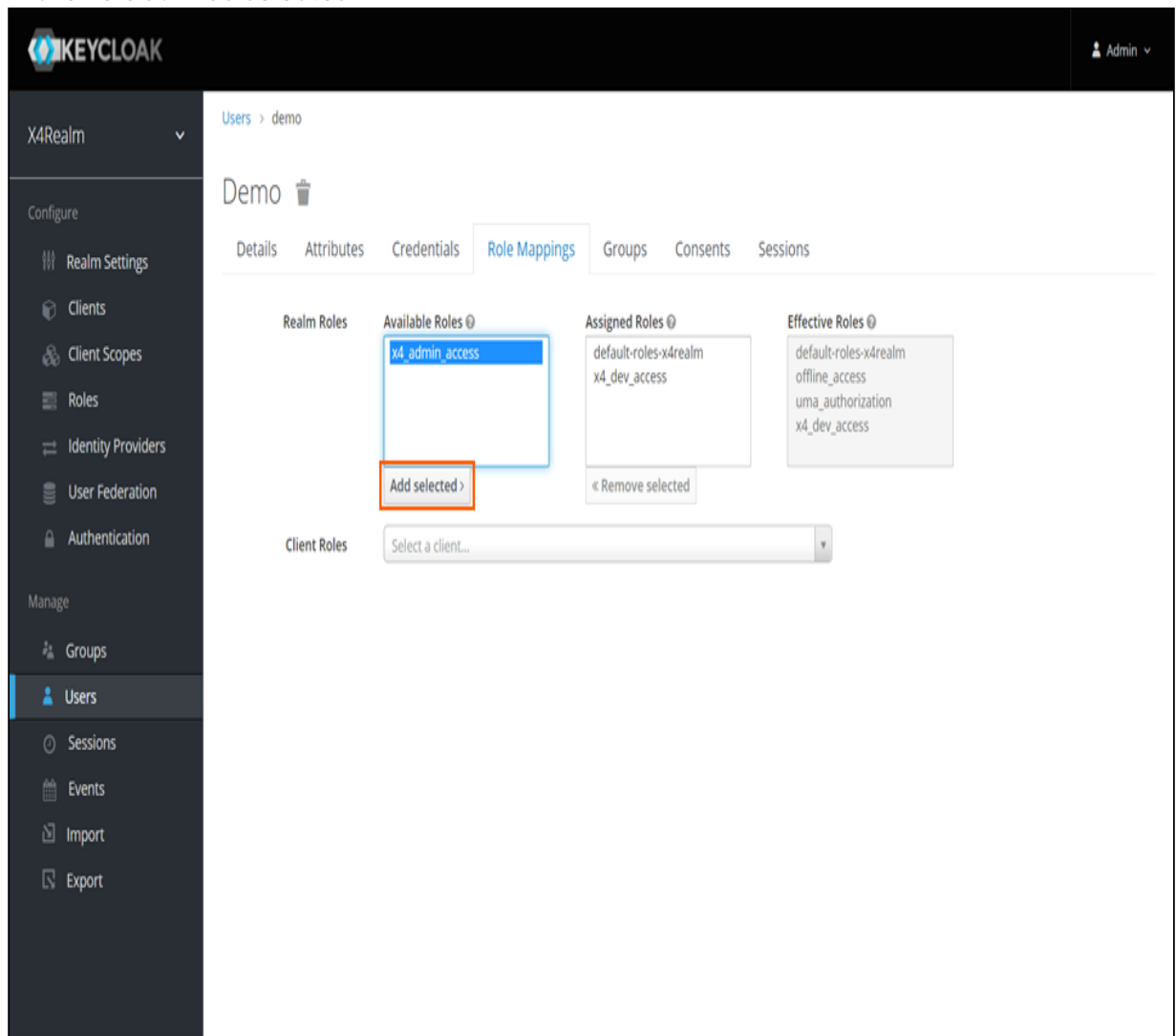
5. Wechseln Sie in die Registerkarte **Role Mappings**.

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' user information. Below this, a breadcrumb 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)
- Save and Cancel buttons at the bottom.

6. Wählen Sie im Bereich **Available Roles** die Rolle aus, die dem Benutzer zugewiesen werden soll.

The screenshot displays the Keycloak Admin Console interface. The left sidebar shows the navigation menu with 'Users' selected. The main content area is titled 'Demo' and shows the 'Role Mappings' tab. The 'Available Roles' list is highlighted with a red box, containing the role 'x4_admin_access'. Below this list is an 'Add selected >' button. The 'Assigned Roles' list contains 'default-roles-x4realm' and 'x4_dev_access', with a '< Remove selected' button below it. The 'Effective Roles' list contains '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. Klicken Sie auf **Add selected**.

6.4.3 Benutzer eine Gruppe zuweisen

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **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' with various configuration fields. The 'Security Defenses' section is expanded, showing fields for Name, Display name, HTML Display name, Frontend URL, Enabled status (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

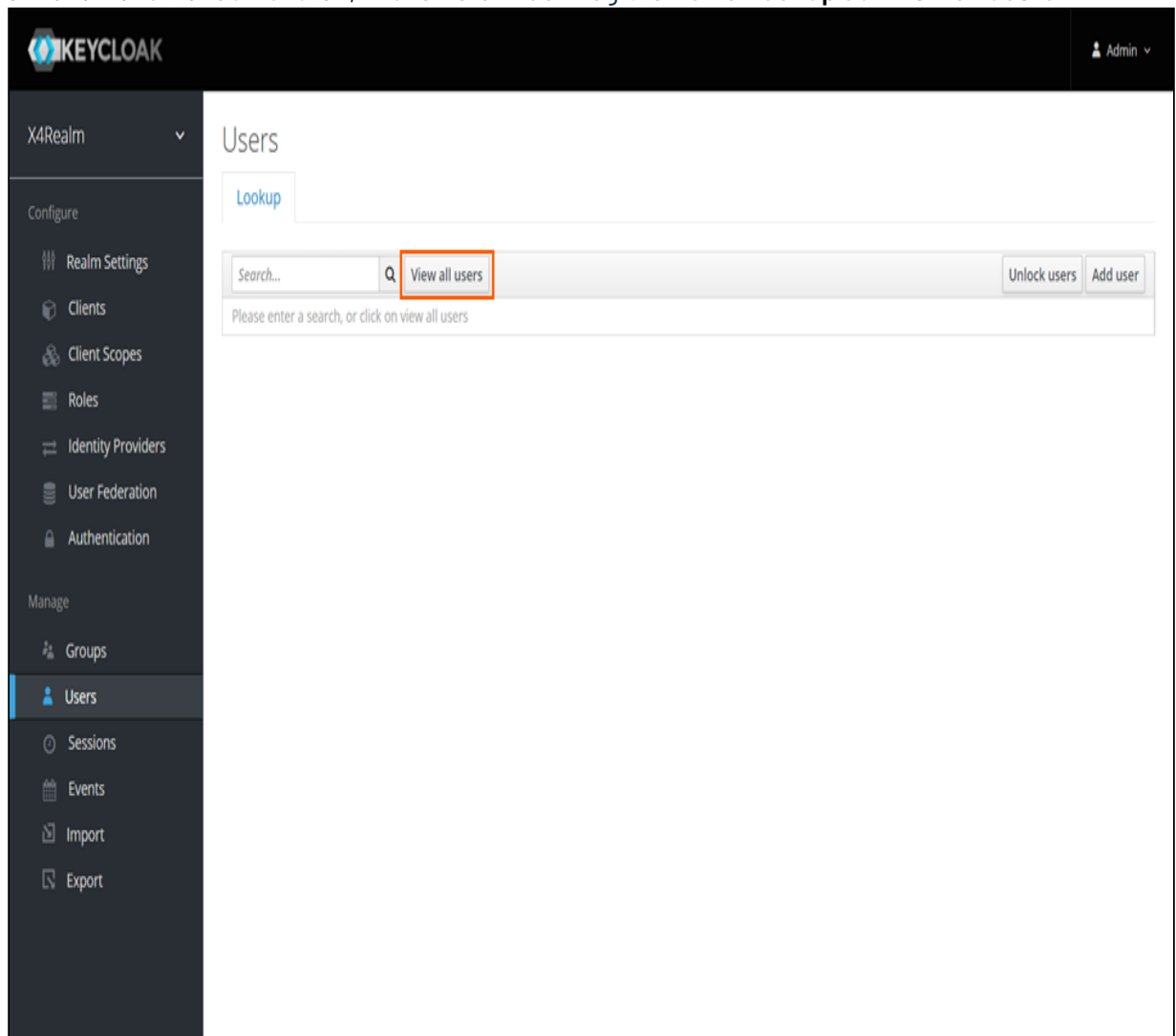
Enabled ON

User-Managed Access OFF

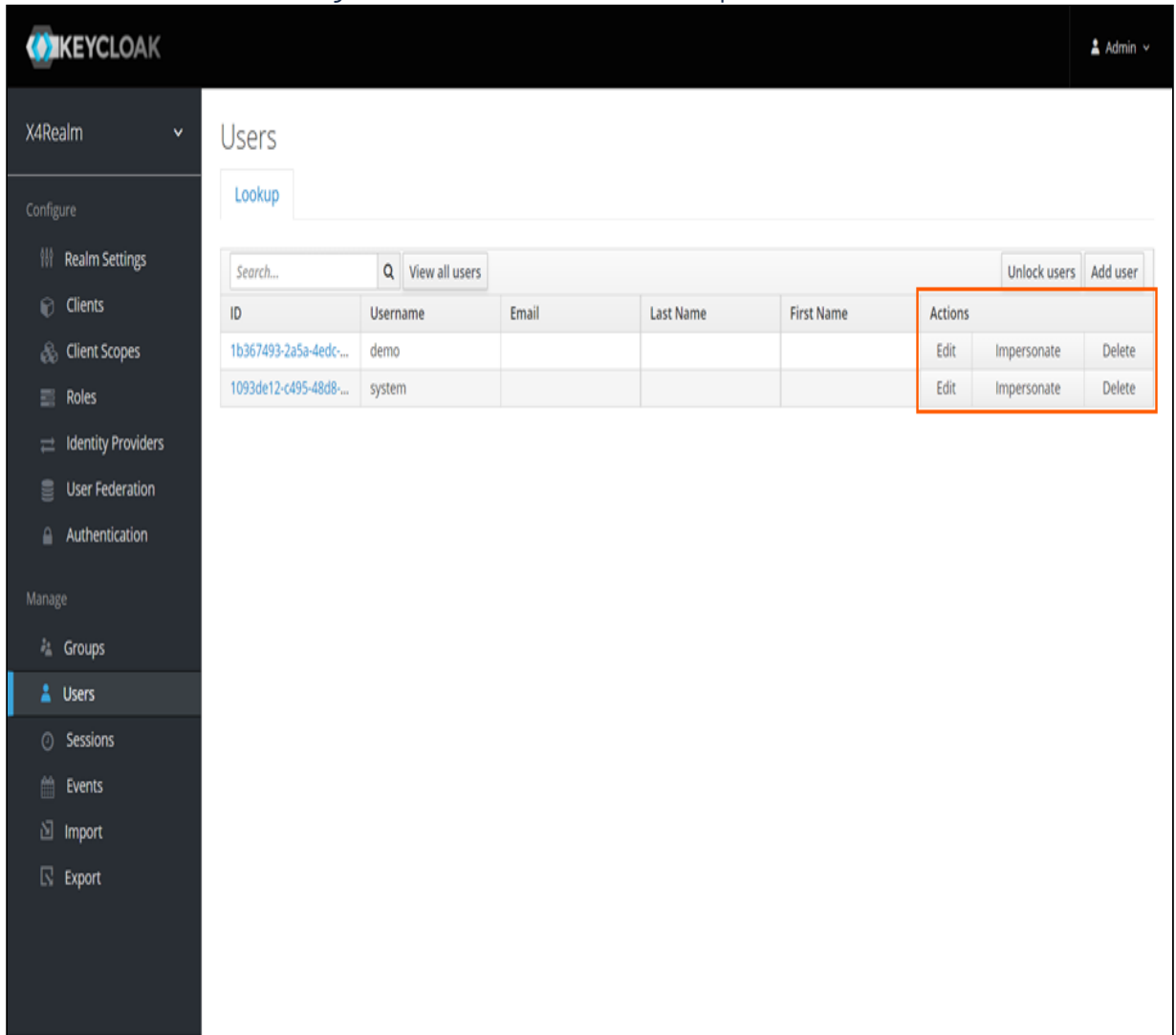
Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Save Cancel

3. Um alle Benutzer aufzulisten, klicken Sie in der Registerkarte **Lookup** auf **View all users**.



4. Klicken Sie in der Zeile des gewünschten Benutzers in der Spalte **Actions** auf **Edit**.



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 search bar and a 'View all users' button. To the right of the search bar are 'Unlock users' and 'Add user' buttons. The main table lists users with columns: ID, Username, Email, Last Name, First Name, and Actions. The 'Actions' column contains 'Edit', 'Impersonate', and 'Delete' buttons. The 'Edit' button for the first user is highlighted with a red box.

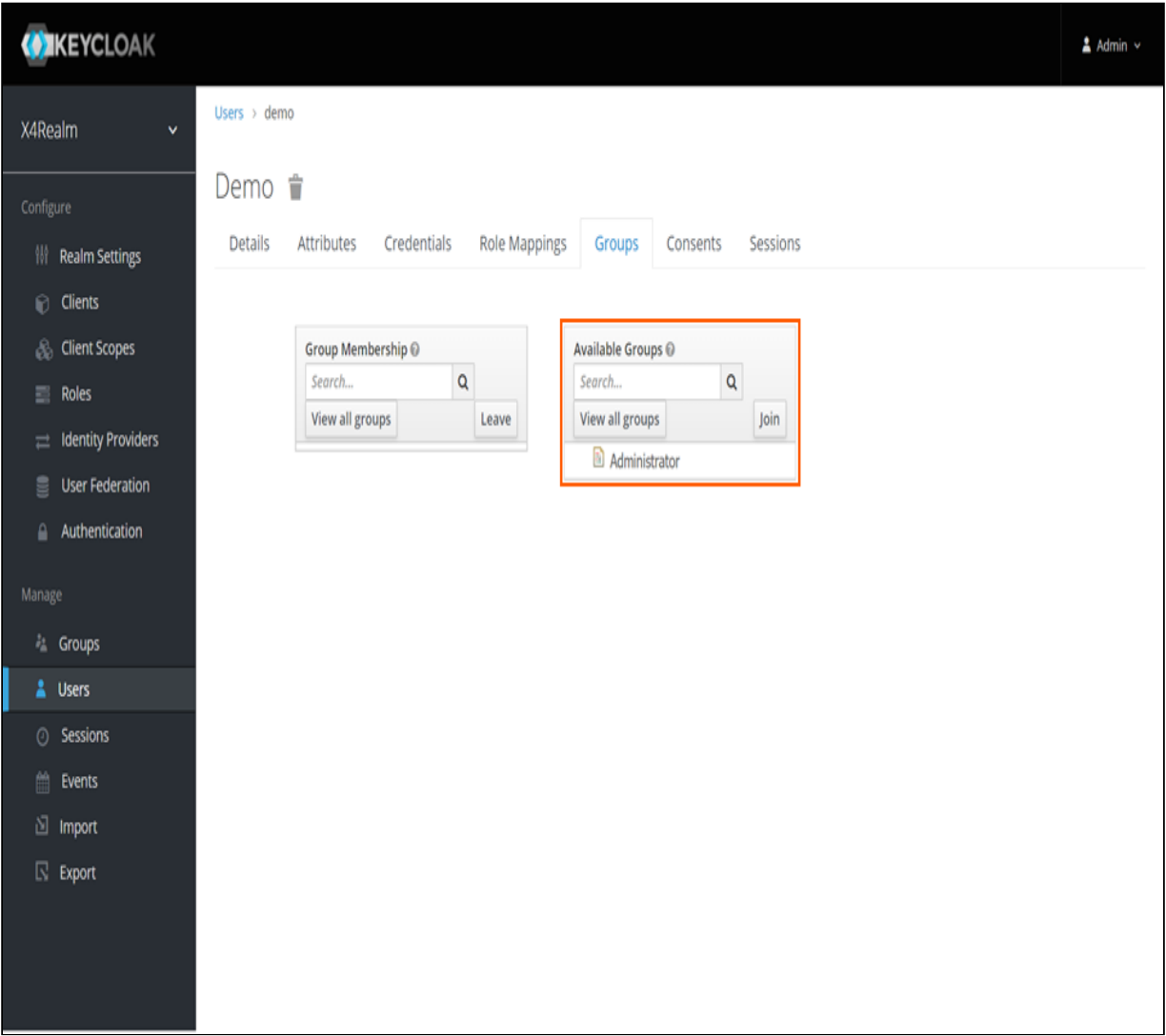
ID	Username	Email	Last Name	First Name	Actions
1b367493-2a5a-4edc...	demo				Edit Impersonate Delete
1093de12-c495-48d8...	system				Edit Impersonate Delete

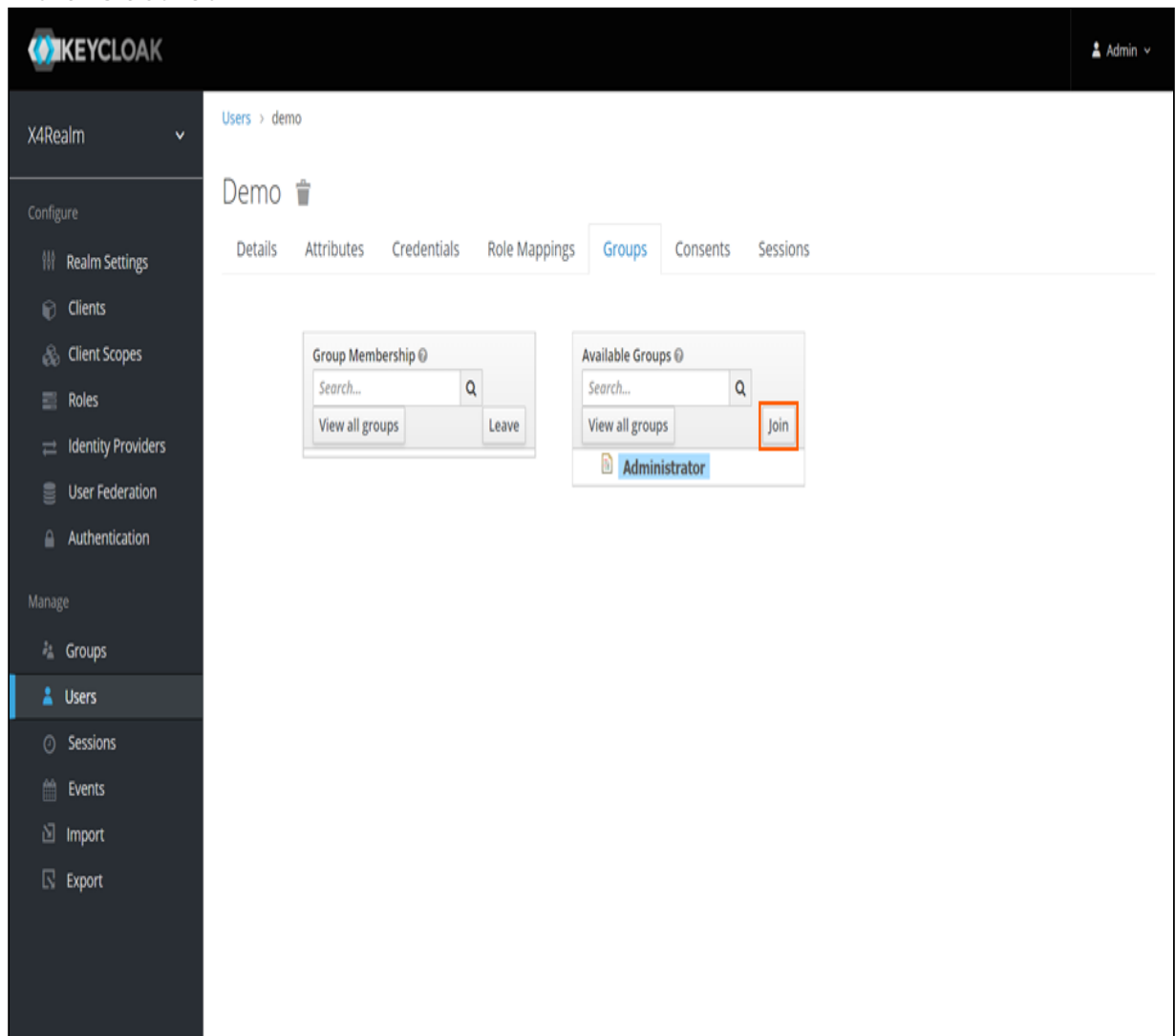
5. Wechseln Sie in die Registerkarte **Groups**.

The screenshot shows the Keycloak administration console. On the left is a dark sidebar with a menu. The 'Users' option is highlighted. The main area is titled 'Users > demo' and 'Demo'. Below the title are tabs: 'Details', 'Attributes', 'Credentials', 'Role Mappings', 'Groups' (which is selected and highlighted with an orange border), 'Consents', and 'Sessions'. The 'Groups' tab contains a list of available groups. At the bottom of the main area are buttons for 'Save' and 'Cancel'.

ID	Created At	Username	Email	First Name	Last Name	User Enabled	Email Verified	Required User Actions	Impersonate user
1b367493-2a5a-4edc-b858-f2ce71e1b625	8/13/21 7:43:52 AM	demo				ON	OFF	Select an action...	Impersonate

6. Wählen Sie im Bereich **Available Groups** die Gruppe aus, die dem Benutzer zugewiesen werden soll.



7. Klicken Sie auf **Join**.

6.4.4 Benutzer aus einer Gruppe entfernen

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **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' configuration. The 'Security Defenses' section includes fields for 'Name' (X4Realm), 'Display name', 'HTML Display name', and 'Frontend URL'. The 'Enabled' toggle is set to 'ON', and 'User-Managed Access' is set to 'OFF'. The 'Endpoints' section lists '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

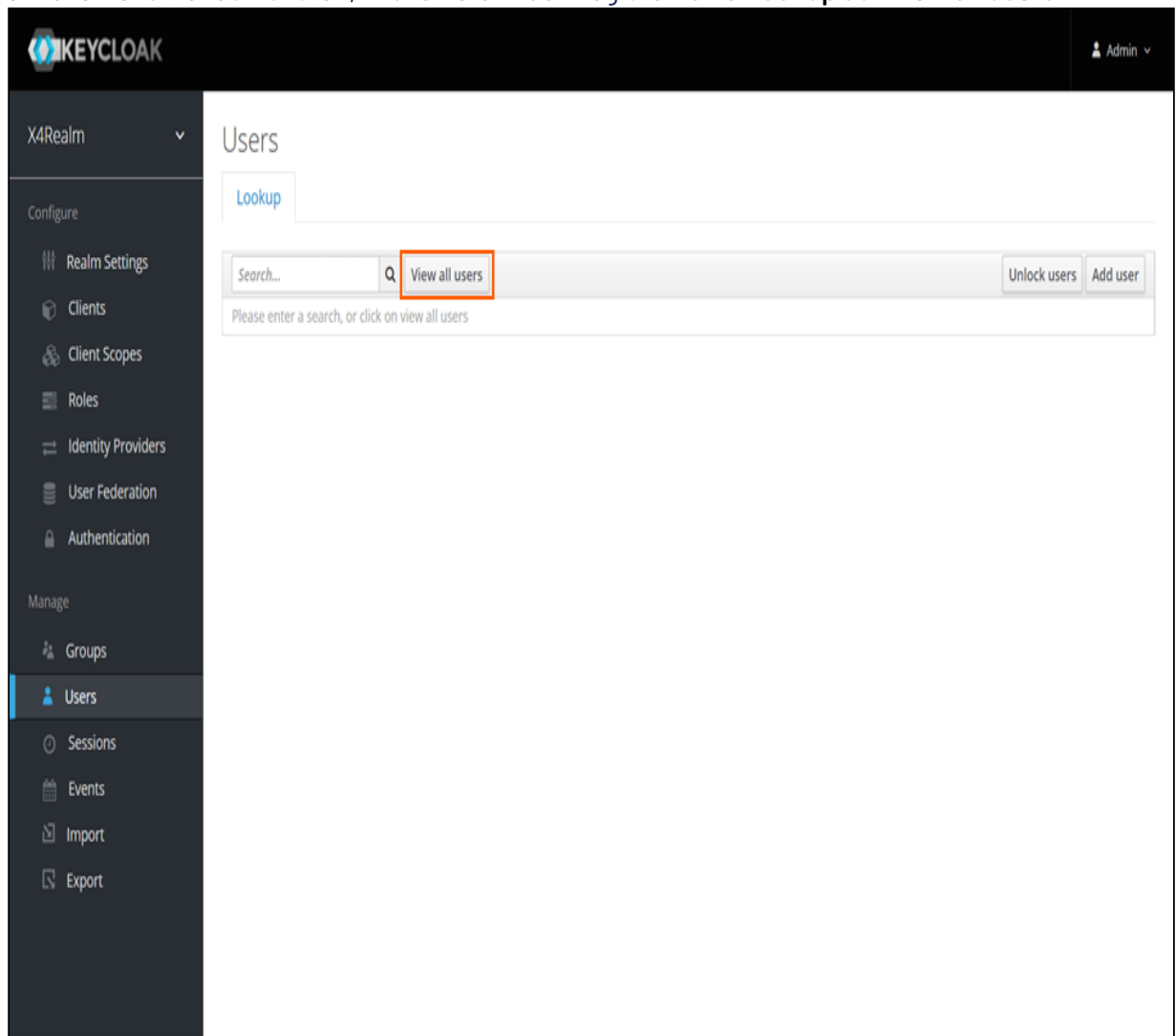
Endpoints

OpenID Endpoint Configuration

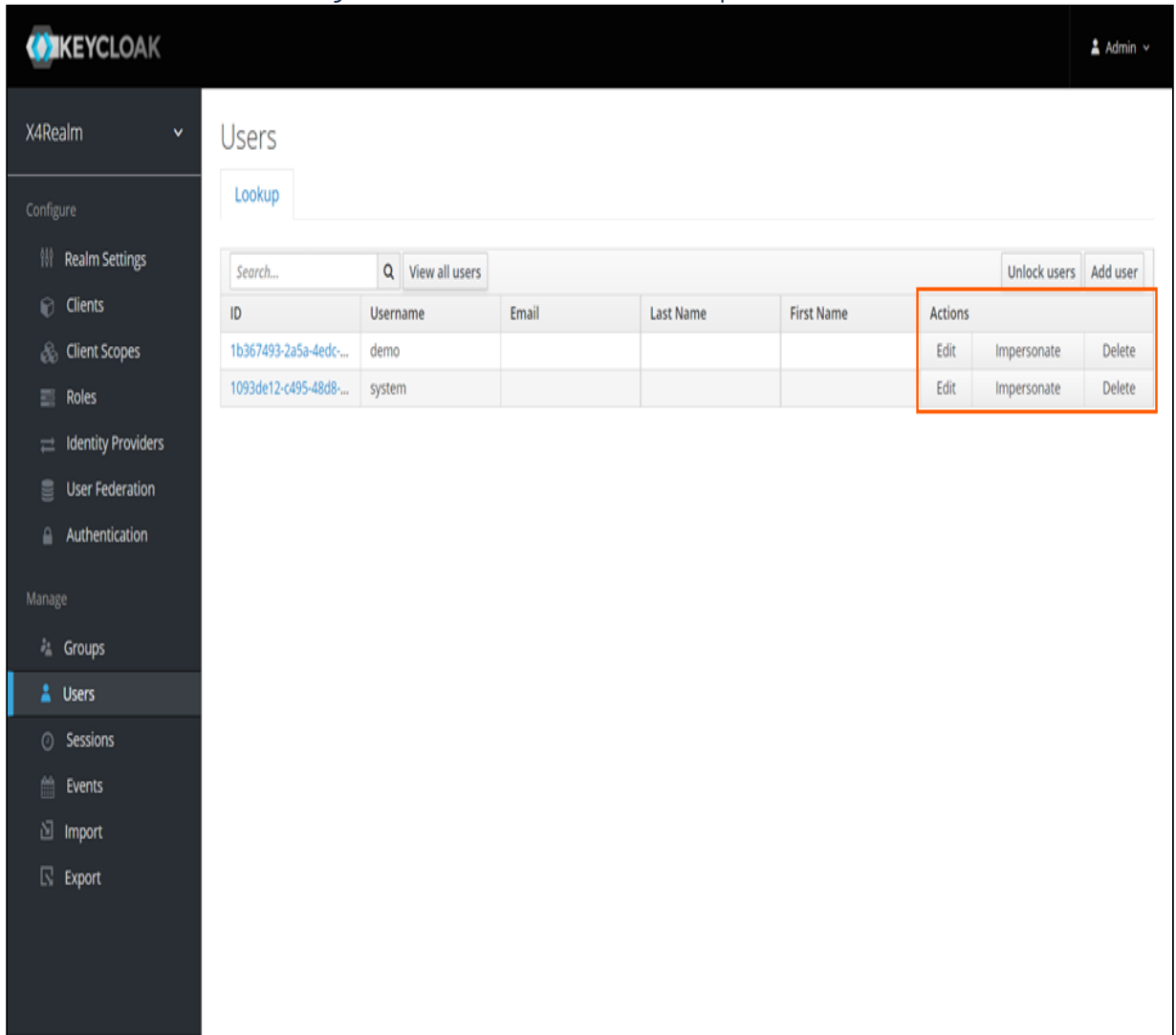
SAML 2.0 Identity Provider Metadata

Save Cancel

3. Um alle Benutzer aufzulisten, klicken Sie in der Registerkarte **Lookup** auf **View all users**.



4. Klicken Sie in der Zeile des gewünschten Benutzers in der Spalte **Actions** auf **Edit**.



The screenshot shows the Keycloak administration interface for the 'X4Realm'. The 'Users' menu item is selected in the left sidebar. The main content area displays a table of users. The 'demo' user is highlighted, and the 'Actions' column for this user is expanded, showing 'Edit', 'Impersonate', and 'Delete' options.

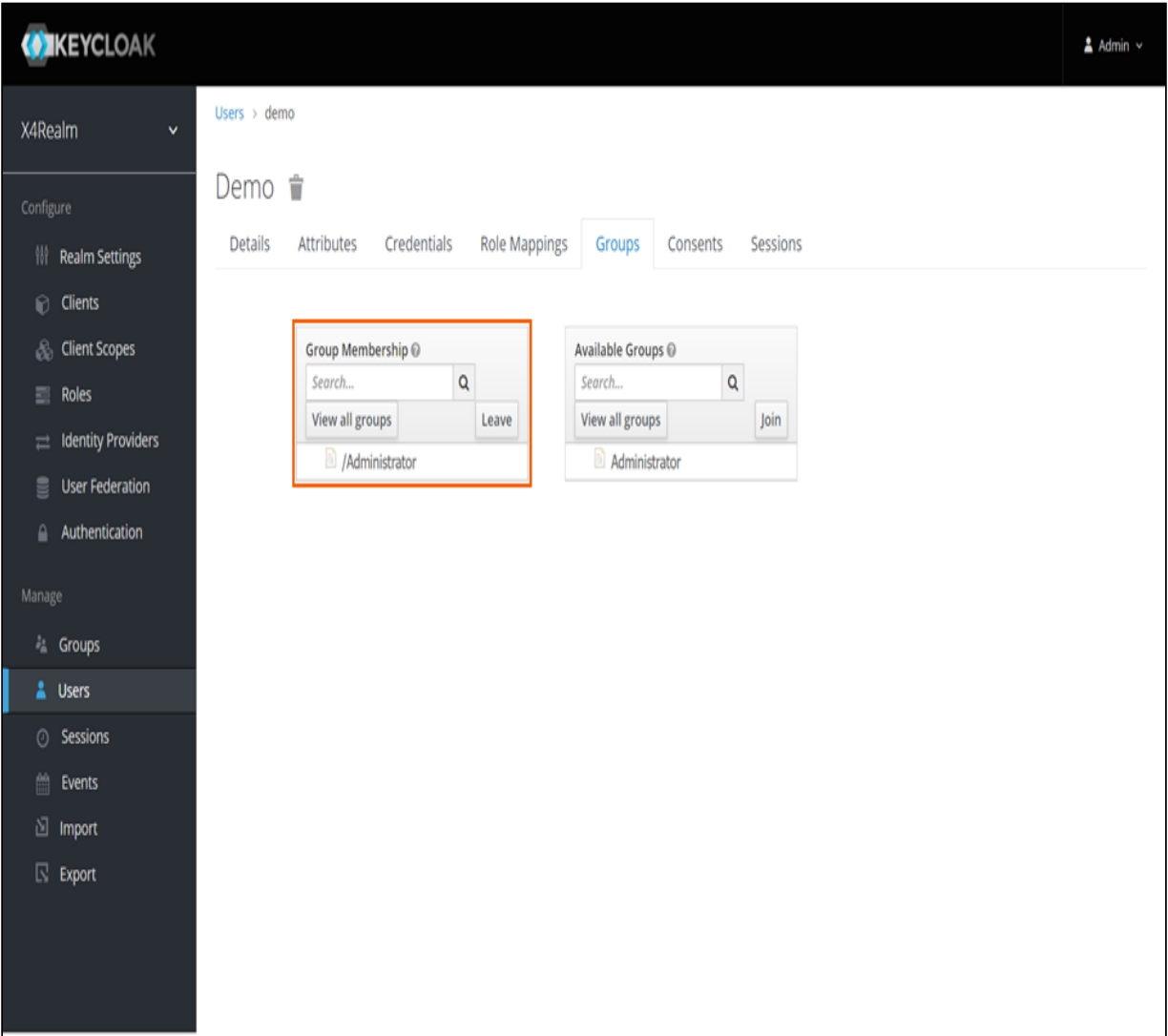
ID	Username	Email	Last Name	First Name	Actions
1b367493-2a5a-4edc...	demo				Edit Impersonate Delete
1093de12-c495-48d8...	system				Edit Impersonate Delete

5. Wechseln Sie in die Registerkarte **Groups**.

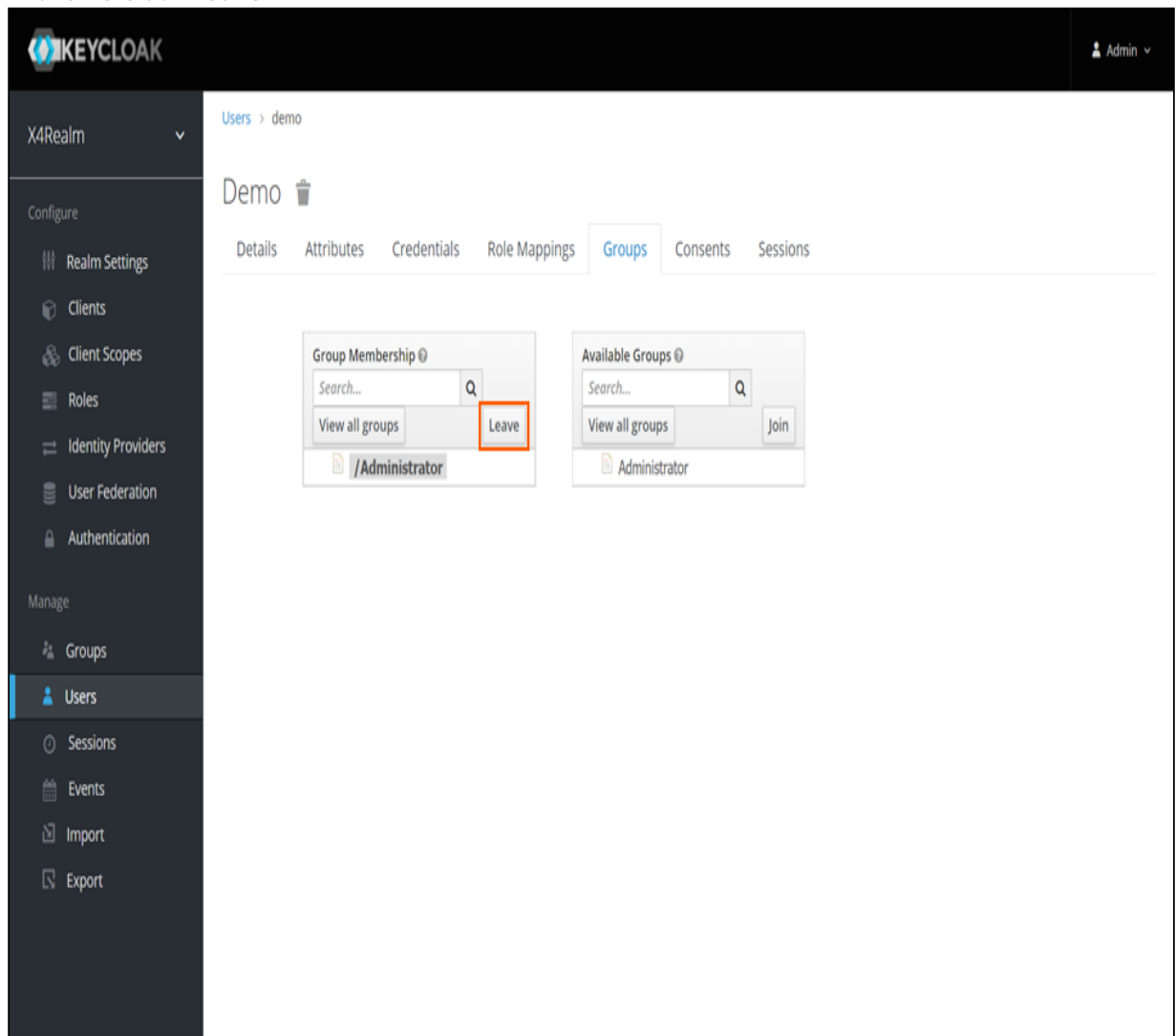
The screenshot shows the Keycloak administration console. On the left is a dark sidebar with a menu. The 'Users' option is highlighted. The main area is titled 'demo' and contains several tabs: 'Details', 'Attributes', 'Credentials', 'Role Mappings', 'Groups' (which is highlighted with an orange border), 'Consents', and 'Sessions'. The 'Groups' tab is active, displaying 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
- Email Verified: ☐ OFF
- Required User Actions: Select an action... (dropdown menu)
- Impersonate user:
- Buttons:

6. Wählen Sie im Bereich **Group Membership** die Gruppe, aus der der Benutzer entfernt werden soll.



7. Klicken Sie auf **Leave**.



6.5 Rollen

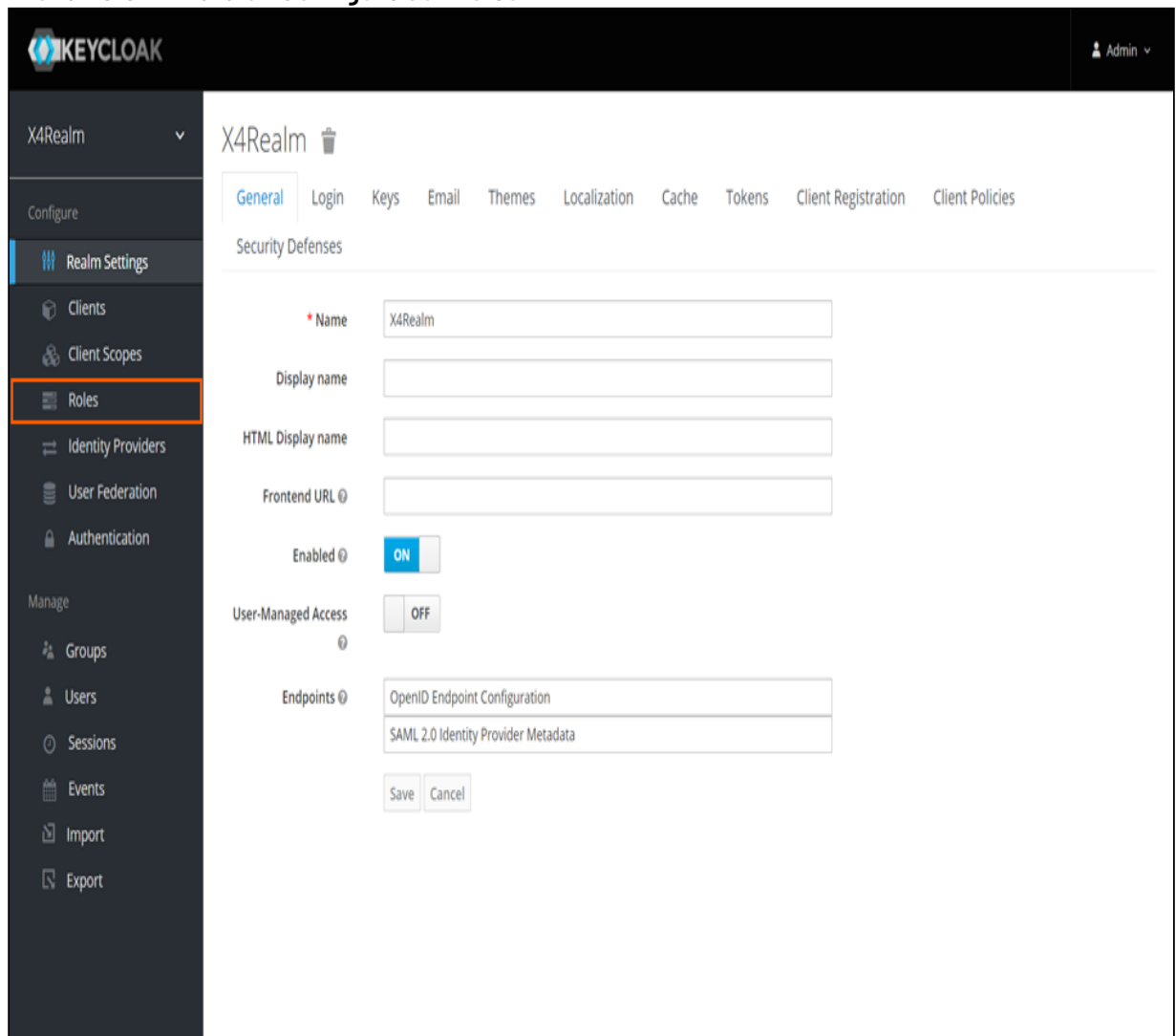
Rollen sind im Wesentlichen ein Namensraum, der einem Client zugeordnet ist. Jeder Client erhält seinen eigenen Namensraum.

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

6.5.1 Rolle erstellen

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Configure** auf **Roles**.

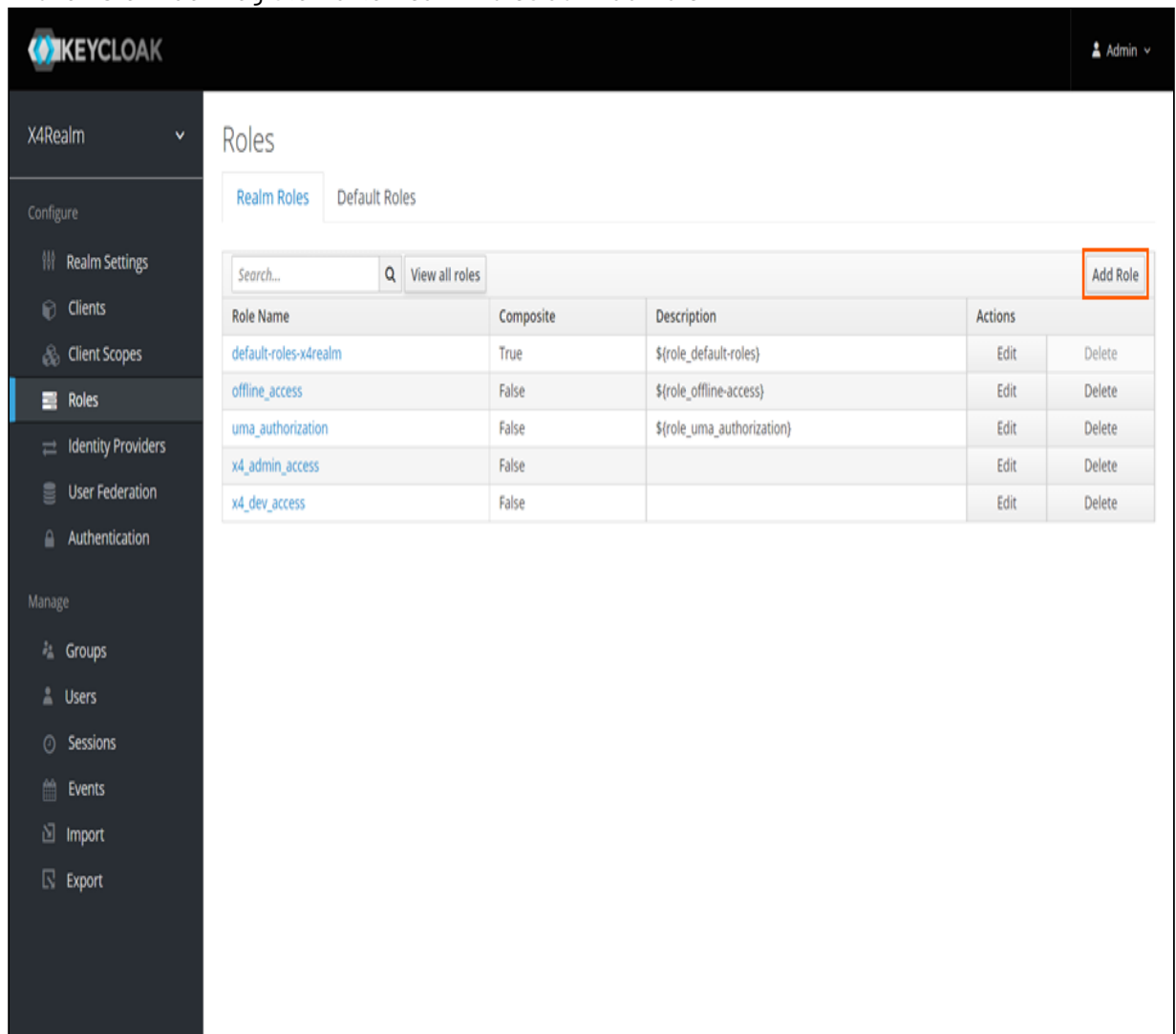


The screenshot displays the Keycloak administration interface. On the left, a dark sidebar contains a menu with the following items: 'X4Realm' (selected), 'Configure', 'Realm Settings', 'Clients', 'Client Scopes', 'Roles' (highlighted with an orange border), 'Identity Providers', 'User Federation', 'Authentication', 'Manage', 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The main content area is titled 'X4Realm' and features a horizontal tab bar with 'General' (active), 'Login', 'Keys', 'Email', 'Themes', 'Localization', 'Cache', 'Tokens', 'Client Registration', and 'Client Policies'. Below the tabs, the 'Security Defenses' section is visible, containing the following fields and controls:

- Name:** A text input field containing 'X4Realm'.
- Display name:** An empty text input field.
- HTML Display name:** An empty text input field.
- Frontend URL:** An empty text input field.
- Enabled:** A toggle switch currently set to 'ON'.
- User-Managed Access:** A toggle switch currently set to 'OFF'.
- Endpoints:** Two stacked text input fields containing 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'.

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

3. Klicken Sie in der Registerkarte **Realm Roles** auf **Add Role**.



4. Geben Sie im Textfeld **Role Name** einen Namen ein.
5. Klicken Sie auf **Save**.

6.6 Gruppen

Gruppen in Keycloak ermöglichen es Ihnen, einen gemeinsamen Datensatz von Attributen und Rollenzuordnungen für eine Gruppe von Benutzern zu verwalten. Benutzer können Mitglied von keiner oder mehreren Gruppen sein. Die Benutzer erben die Attribute und Rollenzuordnungen, die der jeweiligen Gruppe zugeordnet sind.

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

6.6.1 Gruppe erstellen

1. Öffnen Sie die **Keycloak Administrationskonsole**.

2. Klicken Sie im Bereich **Manage** auf **Groups**.

The screenshot displays the Keycloak administration console. The top navigation bar shows the 'KEYCLOAK' logo and the user 'Admin'. 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 is titled 'X4Realm' and contains a tabbed interface with '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' (toggle set to ON), 'User-Managed Access' (toggle set to OFF), and 'Endpoints' (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

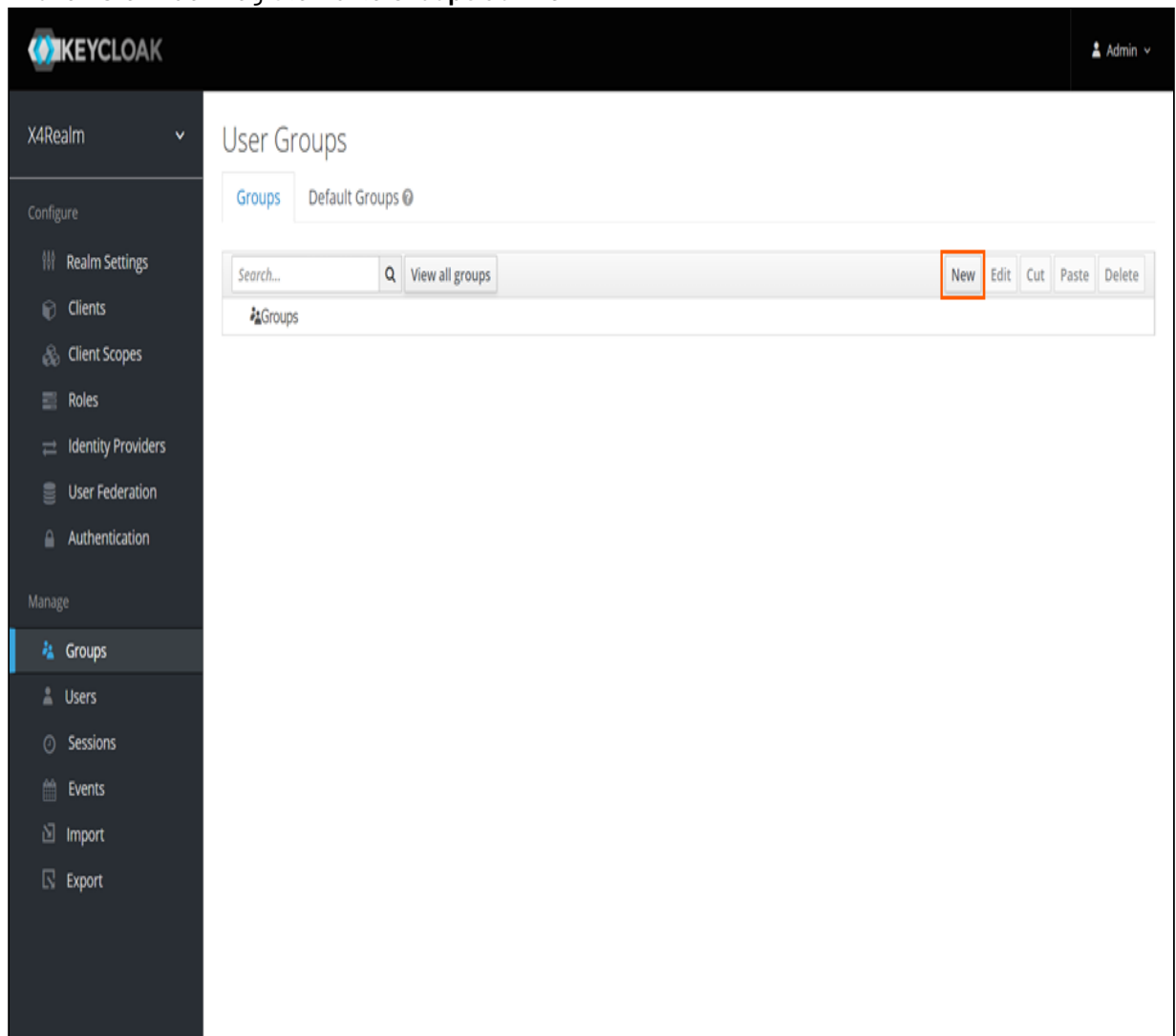
Enabled ON

User-Managed Access OFF

Endpoints OpenID Endpoint Configuration
SAML 2.0 Identity Provider Metadata

Save Cancel

3. Klicken Sie in der Registerkarte **Groups** auf **New**.



4. Geben Sie im Textfeld **Name** einen Namen ein.
5. Klicken Sie auf **Save**.