X4 Administration Guide

SoftProject

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

Inhaltsverzeichnis

1 Einführung

1.1 Welche Information finde ich im X4 Administration Guide?

Dieses Dokument richtet sich an Administratoren, die den X4 Server installieren, konfigurieren und administrieren möchten.

Folgende Inhalte werden beschrieben:

- Konfiguration des X4 Servers und Designers
- Administration des X4 Servers
- Hochverfügbarkeit mit geplanten Prozessausführungen, Lastverteilung und Ausfallsicherheit
- Authentifizierungsprovider Keycloak

1.2 Welches Wissen ist erforderlich?

Für die Installation, Konfiguration und Administration des X4 Servers wird neben detailliertem fachlichem Wissen der bestehenden IT-Infrastruktur auch grundsätzliches Wissen über Java EE, XML-Technologien und den Applikations-Server benötigt.

2 Konfiguration

2.1 X4 Server konfigurieren

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

2.1.1 Datenbank einrichten

- Oracle-Datenbank einrichten
- Konfiguration für MSSQL und PostgreSQL

2.1.1.1 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 Systemdatenbank 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 entragen -->
      <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 entragen -->
      <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>
```

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

2.1.1.2 Konfiguration für MSSQL und PostgreSQL

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

Migrations-/Installationswerkzeug ausführen

> Das Migrations-/Installationswerkzeug muss ausgeführt werden, auch wenn keine Migration einer vorhandenen Installation der X4 BPMS beabsichtigt ist. Weitere Informationen finden Sie unter Installation und Migration der Systemdatenbank und der X4DB.
> Vor dem Ausführen des Migrations-/Installationswerkzeugs muss zunächst eine leere Datenbank mit dem Namen `X4` angelegt werden.

Datasources konfigurieren

> **Hinweis:**
> Bitte beachten Sie beim Konfigurieren einer MSSQL-Datenbank in einer lokalen Entwicklungsumgebung Folgendes:
> Vergewissern Sie sich, dass Sie in der JDBC-URL `encrypt=false` verwenden. Andernfalls ist ein Start des Servers und/oder eine Migration der Datenbank aufgrund eines TLS-Fehlers nicht möglich.

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;encrypt=false</
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;encrypt=false</
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>
```

2.1.2 Konfiguration über X4config.xml

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

2.1.2.1 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:** • *on*: SNMP-Dienst aktivieren • *off*: SNMP-Dienst deaktivieren (Standard)
`<jcoserver>`	SAP Java Connector-Dienst aktivieren **Mögliche Werte:** • *on*: JCo-Dienst aktivieren • *off*: JCo-Dienst deaktivieren (Standard)

2.1.2.2 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.

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

2.1.2.3 Platzhalter-Speicher-Konfiguration

Die Konfiguration eines Platzhalter-Speichers erfolgt in der `X4config.xml`. Innerhalb des Wurzelelements `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>
```

2.1.2.3.1 Vorhandene Platzhalter-Speicher

Standardmäßig sind die folgenden drei Platzhalter-Speicher enthalten:

Name	Klassenname	Beschreibung
Properties Placeholder Storage	de.softproject.integration.engine.placeholder.PropertiesPlaceholderStorage	Platzhalter werden auf dem Dateisystem in `Properties`-Dateien abgelegt. Das Verzeichnis, das die Dateien enthält, ist konfigurierbar.
SQL Placeholder Storage	de.softproject.integration.engine.placeholder.SQLPlaceholderStorage	Platzhalter werden in einer SQL-Datenbank abgelegt. Die Ziel-Datenbank ist konfigurierbar.
In-Memory Placeholder Storage	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.

2.1.2.3.2 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.PropertiesPlaceholderSto
rage</class>
        <config>
            <path>C:/X4/PlaceholderStorage/</path>
        </config>
    </storage>
</placeholder>
```

2.1.2.3.3 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>
```

2.1.2.4 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>
```

2.1.3 Logging/Protokollierung konfigurieren

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

2.1.3.1 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 *Mögliche Werte:* • *`filesystem`*: Save Points werden ins Dateisystem, in das Server-Verzeichnis `savepoints` geschrieben • *`database`*: Save Points werden in die X4-Systemdatenbank geschrieben

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

2.1.3.2 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.

2.1.3.3 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.

2.1.3.3.1 Konfiguration

Das Protkollierverhalten kann über die `tracelog.properties`-Datei unter `X4\Server\X4DB\0` geste uert 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.

2.1.3.3.2 Beispielkonfigurationen

2.1.3.3.2.1 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*

2.1.3.3.2.2 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*

2.1.4 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

2.1.4.1 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.

2.1.4.2 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.

2.1.4.3 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.

2.1.4.4 https-listener anpassen

1. Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
2. Bearbeiten Sie folgende Zeilen ein.
3. 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.

2.1.4.5 socket-binding anpassen

1. Öffnen Sie die **standalone.xml** im Serververzeichnis unter **\wildfly\standalone\configuration**.
2. 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-ssltls.

2.1.5 Workspace erstellen

Das X4 Repository kann aus mehreren Workspaces bestehen. In einem Workspace werden die Projekte verwaltet.

Das X4 Repository ist der **X4DB**-Ordner im Serververzeichnis. Die Workspaces sind die einzelnen Ordner innerhalb des **X4DB**-Ordners.

> Die Ordner **0** und **X4modules** sind Systemordner und dürfen nicht gelöscht werden.

1. Erstellen Sie einen neuen Ordner im **X4DB**-Ordner, um einen neuen Workspace zu erstellen.
2. Starten Sie den X4 Server neu, damit der Workspace im X4 Designer zur Auswahl steht.

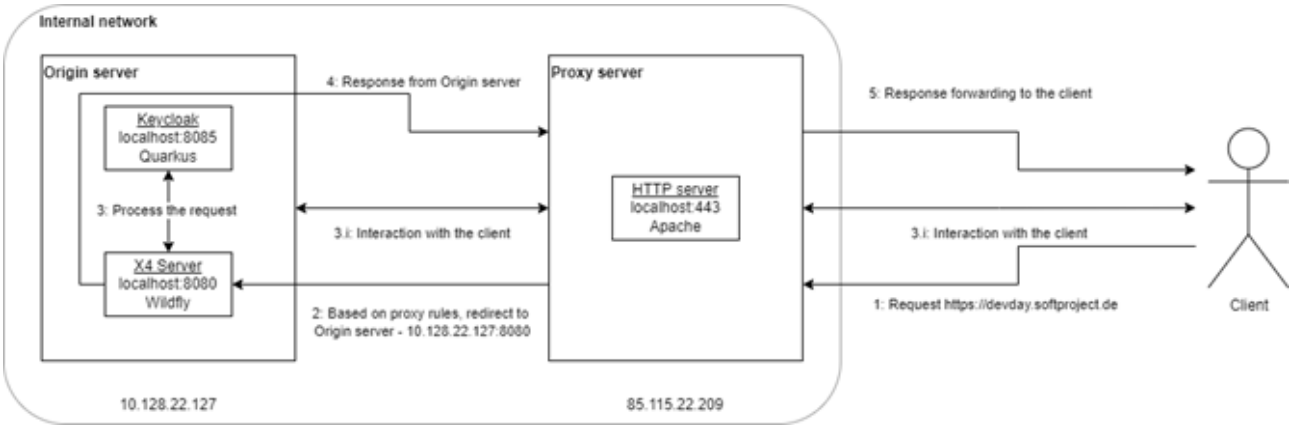
2.1.6 Reverse-Proxy-Server verwenden

Die Verwendung eines Reverse-Proxy-Servers zusammen mit Keycloak und dem X4 Server bietet Vorteile im Hinblick auf Sicherheit und Stabilität.

In diesem Kapitel finden Sie alle Schritte, die Sie ausführen müssen, um eine Installation mit Keycloak und dem X4 Server für den Einsatz mit einem Reverse-Proxy-Server zu konfigurieren:

- Reverse-Proxy-Server konfigurieren
- X4 Server für die Verwendung eines Reverse-Proxy-Servers einrichten
- Keycloak für die Verwendung eines Reverse-Proxy-Servers einrichten

Die beschriebenen Schritte beziehen sich auf eine einfache Reverse-Proxy-Einrichtung mit *einem* Proxy-Server und *einem* Origin-Server. Die Konfiguration der Netzwerkeinrichtung ist in folgendem vereinfachten Diagramm dargestellt:



2.1.6.1 Reverse-Proxy-Server konfigurieren

Die folgende Konfiguration muss auf dem Reverse-Proxy-Server selbst vorgenommen werden, insbesondere auf dem HTTP-Server, der für das Proxying verantwortlich ist (z. B. Apache oder NGINX).

1. Setzen Sie die folgenden HTTP-Header:

- `X-Forwarded-For`
- `X-Forwarded-Proto`
- `X-Forwarded-Host`

> **Hinweis:**
> Wenn diese Header nicht korrekt konfiguriert sind, kommt es zu Sicherheitsproblemen. Weitere Informationen hierzu finden Sie in der Keycloak-Dokumentation (http://www.keycloak.org) im Kapitel zur Verwendung von Reverse-Proxy-Servern.

2. Aktivieren Sie die Endpunkte, die von außen verfügbar sein sollen.

> Diese Einstellung hängt von den Anforderungen der Benutzer und den Sicherheitsvorgaben des Administrators ab.
> Beispiel: Der Zugriff auf die Keycloak-Administrationskonsole ist nicht standardmäßig verfügbar. Für den Zugriff müssen explizite Weiterleitungsregeln angelegt werden.

Die folgenden Abbildungen zeigen eine Beispielkonfiguration für den Apache-HTTP-Server:

```
RequestHeader set X-Forwarded-Host $HOST
RequestHeader set X-Forwarded-Server $HOST
RequestHeader set X-Forwarded-Port "443"
```

Abbildung 1: Header-Einstellungen in Apache

```
ProxyPass /auth http://10.128.22.127:8085/auth
ProxyPassReverse /auth http://10.128.22.127:8085/auth

#ProxyPass /auth/resources http://10.128.22.127:8085/auth/resources
#ProxyPassReverse /auth/resources http://10.128.22.127:8085/auth/resources

#ProxyPass /auth/js http://10.128.22.127:8085/auth/js
#ProxyPassReverse /auth/js http://10.128.22.127:8085/auth/js

#ProxyPass / http://10.128.22.127:8080/X4/webapp/DevDay22_Registration_WebApp/Module/Registration
#ProxyPassReverse / http://10.128.22.127:8080/X4/webapp/DevDay22_Registration_WebApp/Module/Registration

ProxyPass /X4/webapp http://10.128.22.127:8080/X4/webapp
ProxyPassReverse /X4/webapp http://10.128.22.127:8080/X4/webapp

ProxyPass /X4/httpstarter/ReST  http://10.128.22.127:8080/X4/httpstarter/ReST
ProxyPassReverse /X4/httpstarter/ReST  http://10.128.22.127:8080/X4/httpstarter/ReST

ProxyPass /download http://10.128.22.127:8080/download
ProxyPassReverse /download http://10.128.22.127:8080/download
```

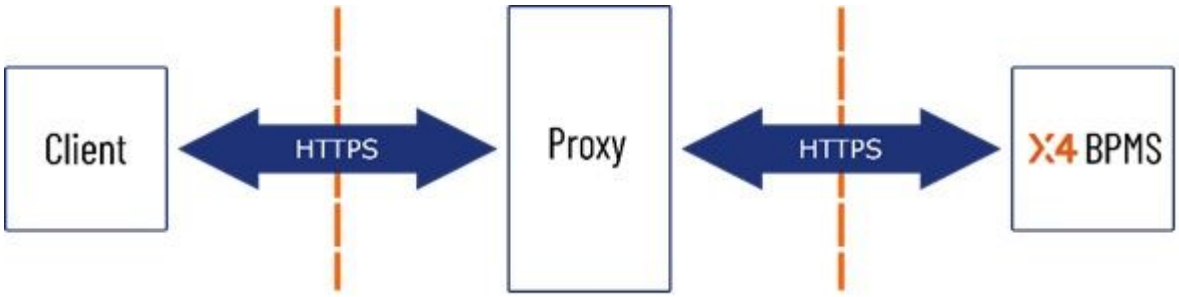
Abbildung 2: Beispiel für Routing-Regeln in Apache

2.1.6.2 X4 Server für die Verwendung eines Reverse-Proxy-Servers einrichten

Wenn für die Bereitstellung einer Web App mit dem zugehörigen Keycloak über das Internet ein Proxy-Server eingesetzt wird, muss der Reverse-Proxy-Server in X4 WildFly konfiguriert werden.

Voraussetzung

- Sie setzen einen Reverse-Proxy-Server ein.



So richten Sie WildFly für die Verwendung Ihres Reverse-Proxy-Servers ein

1. Öffnen Sie die Datei **standalone.xml** im Ordner **<Serververzeichnis>\wildfly\standalone\configuration**.
2. Suchen Sie nach `http-listener`.

3. Ändern Sie den Eintrag `redirect-socket="https"` in `redirect-socket="proxy-https"`.
4. Fügen Sie den Eintrag `proxy-address-forwarding="true"` hinzu.
   Nach den Änderungen muss die Zeile wie folgt aussehen:

```
<http-listener name="default" socket-binding="http" redirect-socket="proxy-
https" enable-http2="true" proxy-address-forwarding="true"/>
```

5. Suchen Sie nach `socket-binding-group`.
6. Fügen Sie folgende Zeile hinzu:

```
<socket-binding name="proxy-https" port="443"/>
```

7. Speichern Sie die Datei.

2.1.6.3 Keycloak für die Verwendung eines Reverse-Proxy-Servers einrichten

In diesem Abschnitt finden Sie alle Einrichtungsschritte, die Sie ausführen müssen, um den Keycloak für die Verwendung eines Reverse-Proxy-Servers anzupassen:

Administratorbenutzer in Keycloak anlegen

Root-URL für den X4 Client in Keycloak anpassen

Proxy-Konfiguration in Keycloak übernehmen

Keycloak starten

2.1.6.3.1 Administratorbenutzer in Keycloak anlegen

Dieser Schritt ist nur erforderlich, wenn kein Administratorbenutzer angelegt wurde. Für den Zugriff auf die Keycloak-Administrationskonsole ist ein Administratorbenutzer erforderlich.

So legen Sie den Administratorbenutzer lokal über die Keycloak-Administrationskonsole an

1. Wenn eine grafische Benutzeroberfläche verfügbar ist, können Sie lokal auf die Keycloak-Administrationskonsole zugreifen:
2. Navigieren Sie in einem Webbrowser zu **http://localhost:8085/auth**.
3. Wählen Sie **Administration Console**, und befolgen Sie die Anweisungen.

So legen Sie den Administratorbenutzer mithilfe von Umgebungsvariablen an, wenn keine lokale Benutzeroberfläche vorhanden ist

1. Fügen Sie die Umgebungsvariablen `KEYCLOAK_ADMIN` und `KEYCLOAK_ADMIN_PASSWORD` zur Datei `/etc/environment` hinzu. Diese Werte geben Benutzernamen und Passwort des Administrators an.
2. Starten Sie den Keycloak neu.
   Der Administratorbenutzer wird automatisch mit den angegebenen Zugangsdaten angelegt. Die Konsole (oder Logdatei) enthält einen Eintrag, der bestätigt, dass der Administratorbenutzer erfolgreich angelegt wurde.

   > **Hinweis:**
   > Wenn Sie den Administratorbenutzer angelegt haben, können Sie die Umgebungsvariablen löschen.

2.1.6.3.2 Root-URL für den X4 Client in Keycloak anpassen

Sobald die Anfragen an den Proxy gesendet werden, muss die Root-URL in der Keycloak-Oberfläche angepasst werden. So ist sichergestellt, dass Keycloak alle eingehenden Requests filtert und nur die Requests zulässt, die mit der festgelegten Root-URL übereinstimmen.

So passen Sie die Root-URL an

1. Öffnen Sie die Keycloak-Oberfläche über localhost:8085/auth.
2. Wählen Sie oben links in der Dropdown-Liste für die Realm-Auswahl den Eintrag **X4 Realm** aus.
3. Wählen Sie unter **Clients** auf der Registerkarte **Clients list** in der Spalte **Client ID** den Eintrag **X4** aus.
4. Geben Sie auf der Registerkarte **Settings** unter **Access Settings** den Wert für die Root-URL ein. Am Ende der Domain muss eine Referenz auf **/X4** enthalten sein.

> **Hinweis:**
> Wenn diese Einstellung geändert wurde, ist die Authentifizierung mit dem Zugriffstyp **Authorization Code Flow** in einer Web App nicht mehr möglich, da nur der Zugriff über die festgelegte Root-URL (in unserem Beispiel https://example.com/X4) aktiviert ist. Wenn die lokale Authentifizierung erneut aktiviert werden muss, setzen Sie die Domain auf ihren ursprünglichen Wert zurück: http://localhost:8080/X4.

2.1.6.3.3 Proxy-Konfiguration in Keycloak übernehmen

Wenn die Root-URL festgelegt wurde, fügen Sie im nächsten Schritt die Proxy-Konfiguration im Keycloak hinzu.

Öffnen Sie im Installationsverzeichnis des X4 Servers den Ordner `keycloak/conf/keycloak.conf`, und führen Sie die folgenden Schritte aus:

1. Legen Sie den Hostnamen basierend auf Ihrer externen URL fest: `hostname=example.com`.
2. Fügen Sie die Proxy-Konfigurationsoption hinzu: `proxy=edge`.
3. Setzen Sie den Wert der Konfigurationsoption `http-host` entsprechend, um externe Kommunikation zuzulassen. Sie können den Standardwert `http-host=0.0.0.0` verwenden, dieser bietet jedoch nur eine eingeschränkte Sicherheit.

> **Hinweis:**
> Wenn Sie diese Schritte ausgeführt haben, ist die Keycloak-Administrationskonsole auf dem lokalen Computer nicht verfügbar. Wenn Sie auf die Konsole zugreifen müssen, müssen Sie diese Einstellungen zurücksetzen. Weitere Informationen zum Wiederherstellen des lokalen Zugriffs auf die Keycloak-Administrationskonsole finden Sie im Abschnitt Bekannte Probleme.

Nach dem Einrichten sollte die Konfiguration in der Datei `keycloak.conf` wie folgt aussehen (nur aktivierte Konfigurationsoptionen sind dargestellt):

```
# Proxy configuration
hostname=example.com
proxy=edge

# Used HTTP host.
http-host=0.0.0.0

# Resources path prefix.
http-relative-path=/auth

# HTTP and HTTPS ports.
http-port=8085
https-port=8448

# Logging.
log=console,file
```

2.1.6.3.4 Keycloak starten

Wenn der Keycloak in einem anderen Modus gestartet wird (Wechsel vom Entwicklungsmodus in den Produktivmodus oder umgekehrt), ist ein zusätzlicher Schritt erforderlich. Keycloak X basiert auf Quarkus und kompiliert Konfigurationsdateien im Vorfeld, um einen schnelleren Start und eine bessere Performance zu ermöglichen. Dieser Schritt wird als „Erstellen" der Anwendung bezeichnet. Wenn der Schritt nicht nach den Konfigurationsänderungen (z. B. Datenbankkonfiguration) erfolgt, werden die letzten Konfigurationsänderungen unter Umständen nicht übernommen.

In der hier beschriebenen Proxy-Einrichtung muss der Keycloak im Produktionsmodus gestartet werden, obwohl keine Zertifikate und keine HTTPS-Konfiguration bereitgestellt werden müssen. Die in der X4 BPMS enthaltenen Keycloak-Startskripte starten den Keycloak in der Regel im Entwicklungsmodus. Wenn das der Fall ist, können Sie den Keycloak mit den folgenden Optionen im Produktivmodus starten:

So starten Sie den Keycloak manuell

1. Führen Sie `/c:/X4/keycloak/bin/kc.sh build` aus, um die Keycloak-Konfiguration vorab zu kompilieren.
2. Führen Sie `/c:/X4/keycloak/bin/kc.sh start` aus, um den Keycloak im Produktivmodus zu starten.

So ändern Sie die Startskripte

1. Führen Sie `/c:/X4/keycloak/bin/kc.sh build` aus, um die Keycloak-Konfiguration vorab zu kompilieren.
2. Ändern Sie in `/c:/X4/startKeycloak.sh` den Eintrag `start-dev` in `start`. Jetzt wird der Keycloak bei jeder Ausführung des Skripts im Produktivmodus gestartet.

So ändern Sie die Daemon-Konfigurationsdatei

1. Führen Sie `/opt/X4/keycloak/bin/kc.sh build` aus, um die Keycloak-Konfiguration vorab zu kompilieren.
2. Ändern Sie den Abschnitt `ExecStart` in der Datei `/etc/systemd/system/X4-Authentication-Provider.service`: Ersetzen Sie `start-dev` durch `start`.

2.1.6.3.5 Praktische Hinweise

Hier finden Sie einige praktische Hinweise, um Ihnen die Einrichtung eines Reverse-Proxy-Servers zu erleichtern.

Szenario:

- Verwendung von Authorization Code Flow
- Anbindung an externen Identity Provider (z. B. Azure)
- Verwendung des Adapters Keycloak Management
- Einsatz der Admin-UI aus internem Netzwerk

Umsetzung:

- **keycloak_config.xml im X4-Installationsverzeichnis:**

```
{
"connection": {
 "realm": "X4Realm",
 "auth-server-url": "https://[INTERN_HOST]/auth/",
 "resource": "X4",
  "credentials": {
"secret": "[SECRET]"
}
},
"webAppKeycloakAuthUrl": "https://[EXTERN_URL]/auth/"
}
```

Wenn `INTERN_HOST = EXTERN_URL`, fügen Sie `EXTERN_URL` zur Datei `/ect/hosts` mit dem lokalen IP hinzu.

- **Keycloak.conf in Keycloak:**

```
# Basic settings for running in production. Change accordingly before deploying the
server.

# Database



# The database vendor.

#db=postgres



# The username of the database user.

#db-username=keycloak



# The password of the database user.

#db-password=password



# The full database JDBC URL. If not provided, a default URL is set based on the
selected database vendor.

#db-url=jdbc:postgresql://localhost/keycloak



# Observability



# If the server should expose metrics and healthcheck endpoints.

#metrics-enabled=true



# HTTPS

https-key-store-file=${kc.home.dir}/conf/kc.keystore

https-key-store-password=secret

https-port=443



# HTTP
```

```
# The proxy address forwarding mode if the server is behind a reverse proxy.

#proxy=edge


# Do not attach route to cookies and rely on the session affinity capabilities from
reverse proxy

#spi-sticky-session-encoder-infinispan-should-attach-route=false


# Hostname for the Keycloak server.

#hostname=[EXTERN_URL]         <- Can be uncommented, if /etc/hosts entry is made

#hostname-admin=[INTERN_HOST]

hostname-strict=false


# Used HTTP host.

#http-host=[INTERN_HOST]

#http-enbaled=false


# Resources path prefix.

http-relative-path=/auth


# HTTP and HTTPS ports.

#http-port=8085

#https-port=8448


# Logging.

log=console,file

#log-file=${kc.home.dir}/log/keycloak.log
```

Weitere Hinweise:

- Verwenden Sie ein SSL-Zertifikat für den Keycloak.
  Laden Sie bei Verwendung eines selbstsignierten Zertifikats die öffentliche `.crt`-Datei in dieses Verzeichnis: `/c:/X4/jdk/bin/keytool -importcert -keystore cacerts -storepass changeit -alias kc -file kc.crt`.
  Schalten Sie außerdem die Zertifikatvalidierung im Proxy-Server für die Keycloak-Weiterleitung ab.

So können Sie ein selbstsigniertes Zertifikat für die Verwendung in Keycloak anlegen:

1. Legen Sie das Zertifikat an:

```
sudo openssl req -x509 -nodes -days 530 -newkey rsa:2048 -keyout kc.key
-out kc.crt -subj "/C=DE/ST=Baden-Württemberg/L=Ettlingen/O=SoftProject/
CN=localhost"
```

2. Importieren Sie das Zertifikat in den Keystore:

```
sudo openssl pkcs12 -inkey kc.key -in kc.crt -export -out kc.p12
-passout pass:changeit -name kc
```

3. Konvertieren Sie `p12` in einen Java-Keystore:

```
/c:/X4/jdk/bin/keytool/keytool -importkeystore -srckeystore <source_keys
toreFile> -srcstoretype PKCS12 -destkeystore <destination_keystoreFile>
-deststoretype JKS -srcstorepass mysecret -deststorepass mysecret
-srcalias myalias -destalias myalias -srckeypass mykeypass -destkeypass
mykeypass -noprompt
```

- Führen Sie den Keycloak im Produktivmodus (PROD) aus.
- Fügen Sie die folgenden Header zum Proxy hinzu:

  X-Forwarded-For=$HOST

  X-Forwarded-Proto=„https“

  X-Forwarded-Host=$HOST

- Legen Sie die Root-URL für X4 Client in Keycloak wie folgt fest: `https://[EXTERN_URL]/X4`

Weitere Informationen:

- https://www.keycloak.org/server/reverseproxy
- https://www.keycloak.org/server/configuration
- https://www.keycloak.org/server/configuration-production
- https://www.keycloak.org/server/hostname
- https://www.keycloak.org/server/configuration#_starting_keycloak

2.1.6.4 Bekannte Probleme

Problem	Lösung
Konfigurationsänderung wird nicht übernommen	Wenn Konfigurationsänderungen im Keycloak beim Ausführen des Keycloaks nicht angewendet werden, kann das daran liegen, dass Sie die Keycloak-Konfiguration nicht vorkompiliert haben. Um dieses Verhalten zu vermeiden, empfiehlt es sich, den `build`-Befehl jedes Mal auszuführen, wenn Sie den Ausführungsmodus des Keycloak ändern. Weitere Informationen hierzu finden Sie im Abschnitt Keycloak starten.

Zugriff auf die Keycloak-Administrationskonsole ist von außen nicht möglich	Wenn der Zugriff auf den Netzwerkendpunkt für die Keycloak-Administrationskonsole (**/admin**) von außen nicht möglich ist, ist der Zugriff auf die Keycloak-Administrationskonsole nur über den Computer möglich, auf dem der Keycloak installiert ist. **So stellen Sie den Zugriff auf die Keycloak-Administrationskonsole lokal wieder her** 1. Führen Sie in der Datei `/c:/X4/keycloak/conf/keycloak.conf` die folgenden Aktionen aus: • Kommentieren Sie `proxy=edge` ein. • Ändern Sie den Eintrag `hostname=example.com` in `hostname=localhost`. 2. Starten Sie den Keycloak im Entwicklungsmodus (siehe Keycloak starten). Jetzt können Sie wie gewohnt durch Eingabe von http://localhost:8085/auth in einem Web-Browser auf den Keycloak zugreifen. Je nach Ihren Konfigurationseinstellungen kann sich diese URL ändern. --- Wenn Sie alle Aktionen in der Keycloak-Administrationskonsole ausgeführt haben, müssen Sie die Proxy-Konfiguration in Keycloak erneut zuweisen, damit der Zugriff auf den X4 Server und die X4 Web Apps über den Proxy-Server wieder möglich ist. Führen Sie dazu die folgenden Schritte aus: 1. Machen Sie die zuvor in der Datei `/c:/X4/keycloak/conf/keycloak.conf`vorgenommenen Änderungen rückgängig: • Kommentieren Sie `proxy=edge` aus. • Ändern Sie `hostname=localhost` in `hostname=example.com`. 2. Starten Sie den Keycloak im Produktivmodus.

Datei `build-system.properties` fehlt	In einigen Fällen wird die Datei `build-system.properties` vom Dateisystem entfernt. Das führt beim Ausführen des `build`-Befehls zu einem Fehler mit dieser Fehlermeldung:
	`ERROR: Failed to run "build" command.`
	`ERROR: /opt/X4/Keycloak/lib/quarkus/build-system.properties`
	`For more details run the same command passing the "--verbose" option. Also you can use "--help" to see the details about the usage of the particular command.`
	
	Die Datei liegt im Verzeichnis `/c:/X4/Keycloak/lib/quarkus/build-system.properties` und enthält Metadaten zur Keycloak-Anwendung, die während der Vorkompilierung der Konfiguration verwendet werden.
	
	Um diesen Fehler zu beheben, legen Sie die Datei `/c:/X4/Keycloak/lib/quarkus/build-system.properties` an, und fügen Sie die folgenden Daten ein:
	
	`quarkus.application.name=keycloak-quarkus-server-app`
	`quarkus.application.version=19.0.1`
	`quarkus.version=2.7.6.Final`
	
	Hinweis:
	Wenn sich die Keycloak-Version ändert, sind diese Daten nicht gültig. Verwenden Sie in diesem Fall den Inhalt der Datei `build-system.properties` aus einer funktionsfähigen Keycloak-Instanz.

2.2 X4 Designer konfigurieren

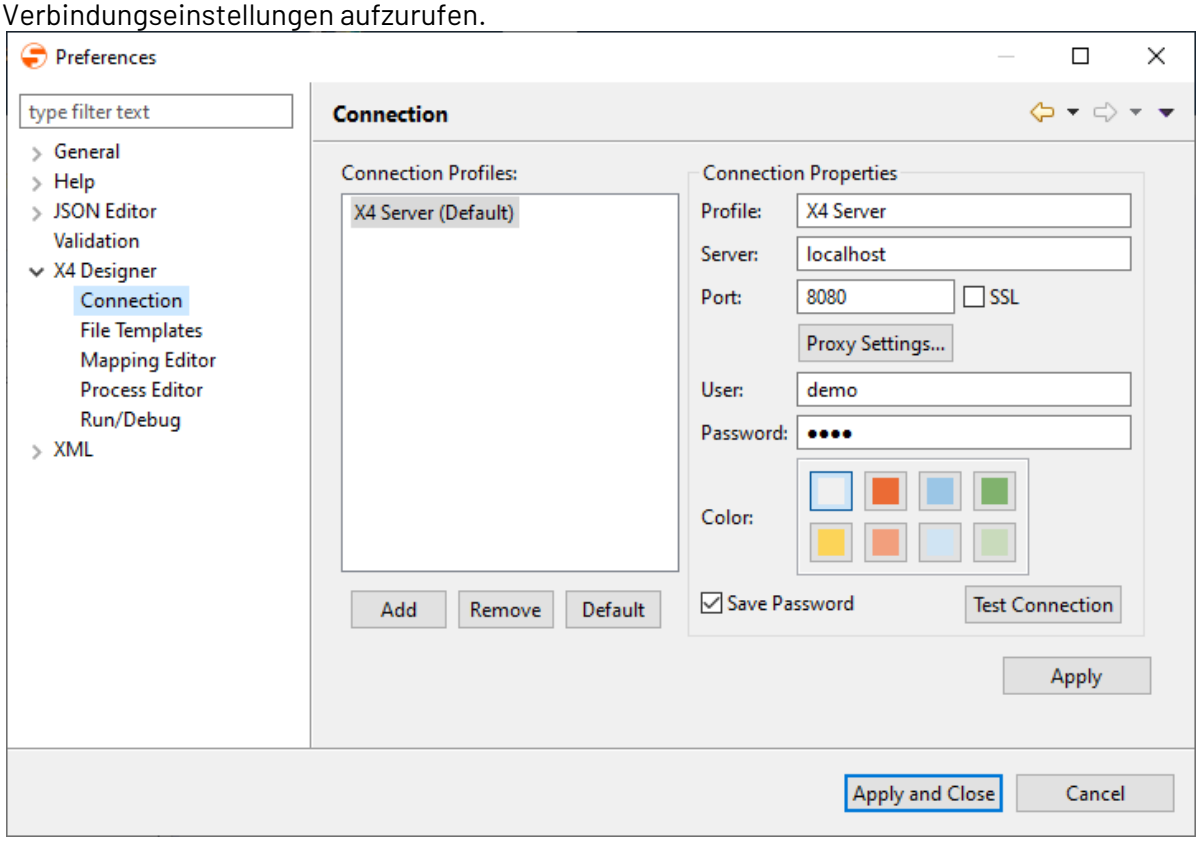
Wie sich Darstellung und das Verhalten einiger Komponenten des *X4 Designers* anpassen lassen

2.2.1 Verbindungskonfiguration bearbeiten

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

1. Menü **Tools> Options** aufrufen.

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



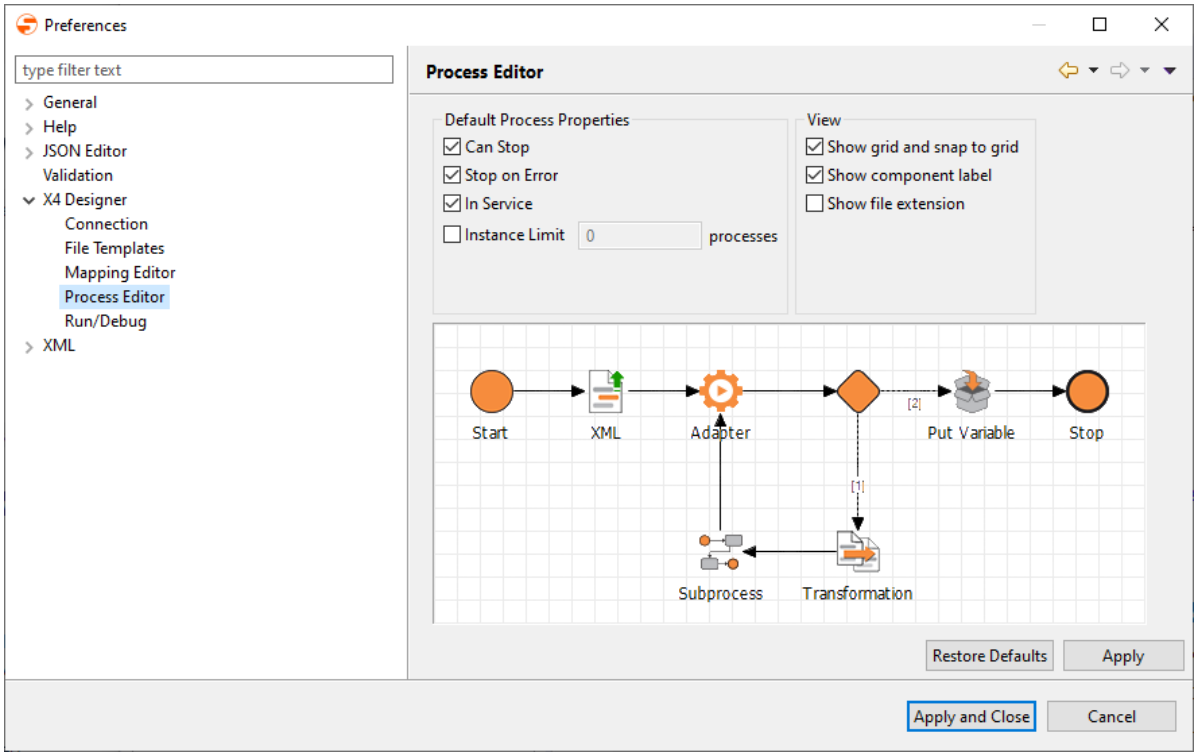
3. Gewünschte Verbindungseinstellungen vornehmen:
   - **Profile:** Name des Verbindungs-Profils (frei wählbar)
   - **Server:** IP-Adresse oder Host-Name des *X4 Servers* (Beispiel: *localhost*)
   - **Port:** Port-Nummer
   - **Proxy Settings:** Standardeinstellungen zu Proxy-Servern und Internet-Verbindung
   - **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.

2.2.2 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.

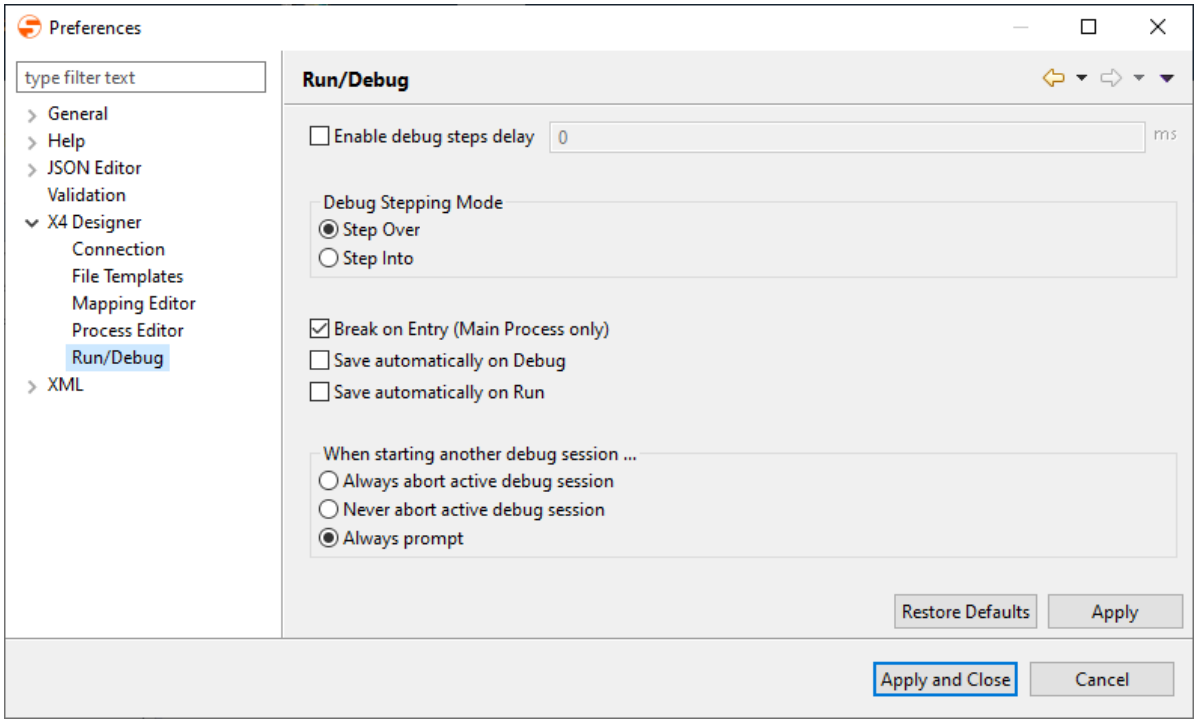


3. Gewünschte Einstellungen in **Default Process Properties** vornehmen:
   - **Can Stop:** Zulassen, dass der Prozess abgebrochen werden kann
   - **Stop on Error:** Prozess-Ausführung automatisch stoppen, wenn ein Fehler auftritt
   - **Public/Private:** Prozess darf ausgeführt werden
   - **Instance 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.

2.2.3 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.

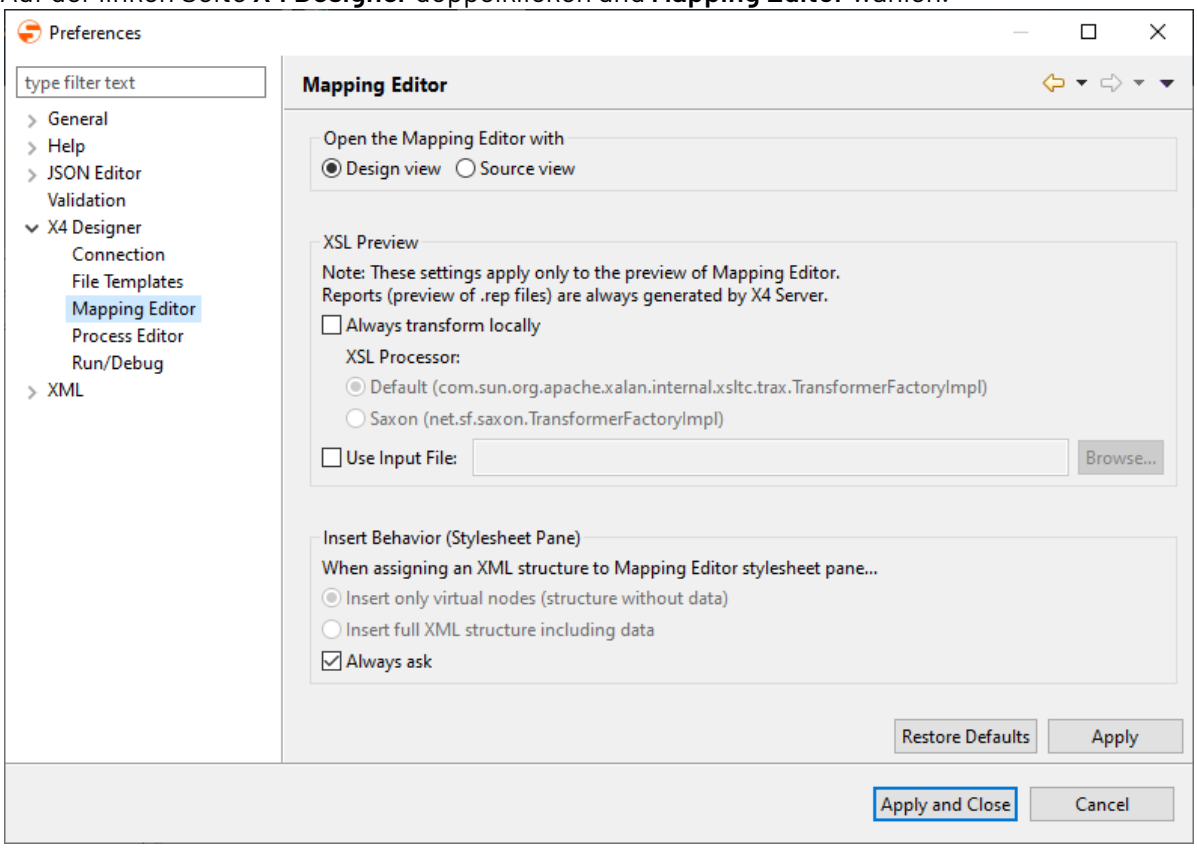
4. **Apply and Close** klicken, um die Einstellungen zu speichern und das Fenster zu schließen.

2.2.4 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

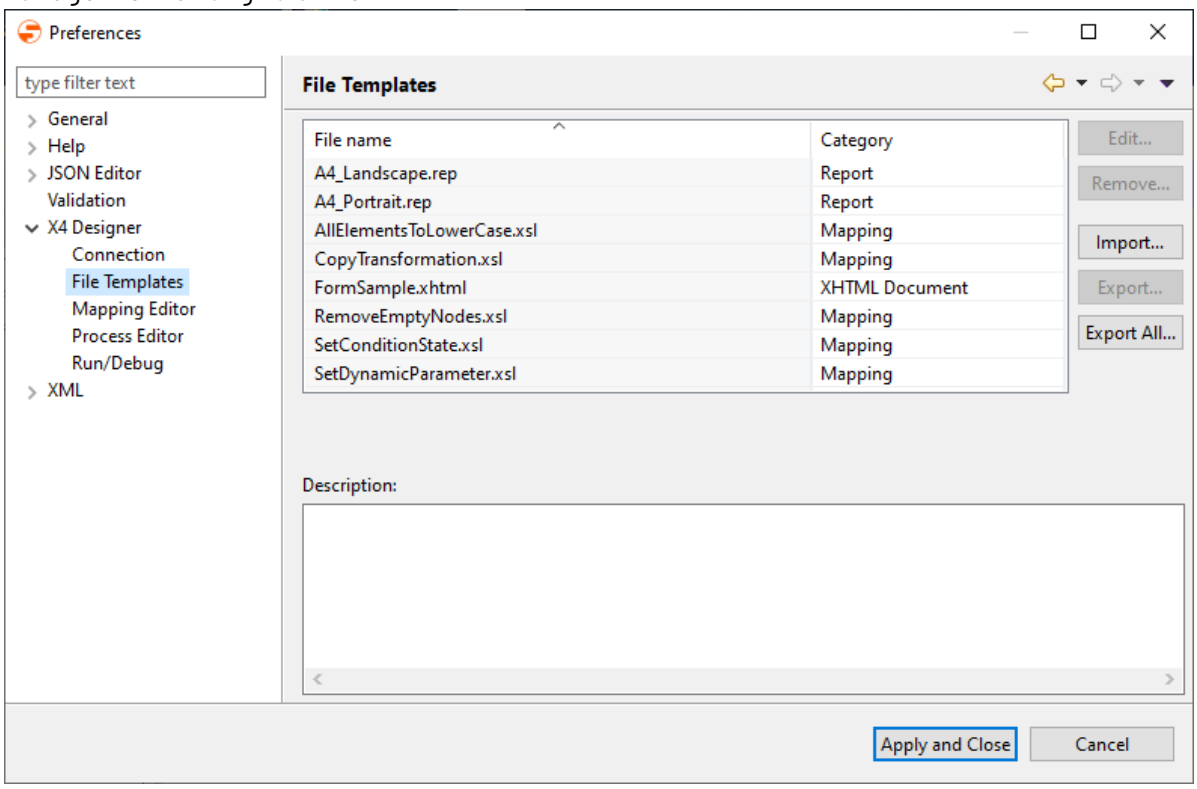
- **Always ask:** Bei jedem Einfügen von XML via Drag&Drop, per Kontextmenü oder über **Strg+V** fragen (standardmäßig aktiv)

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

2.2.5 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.

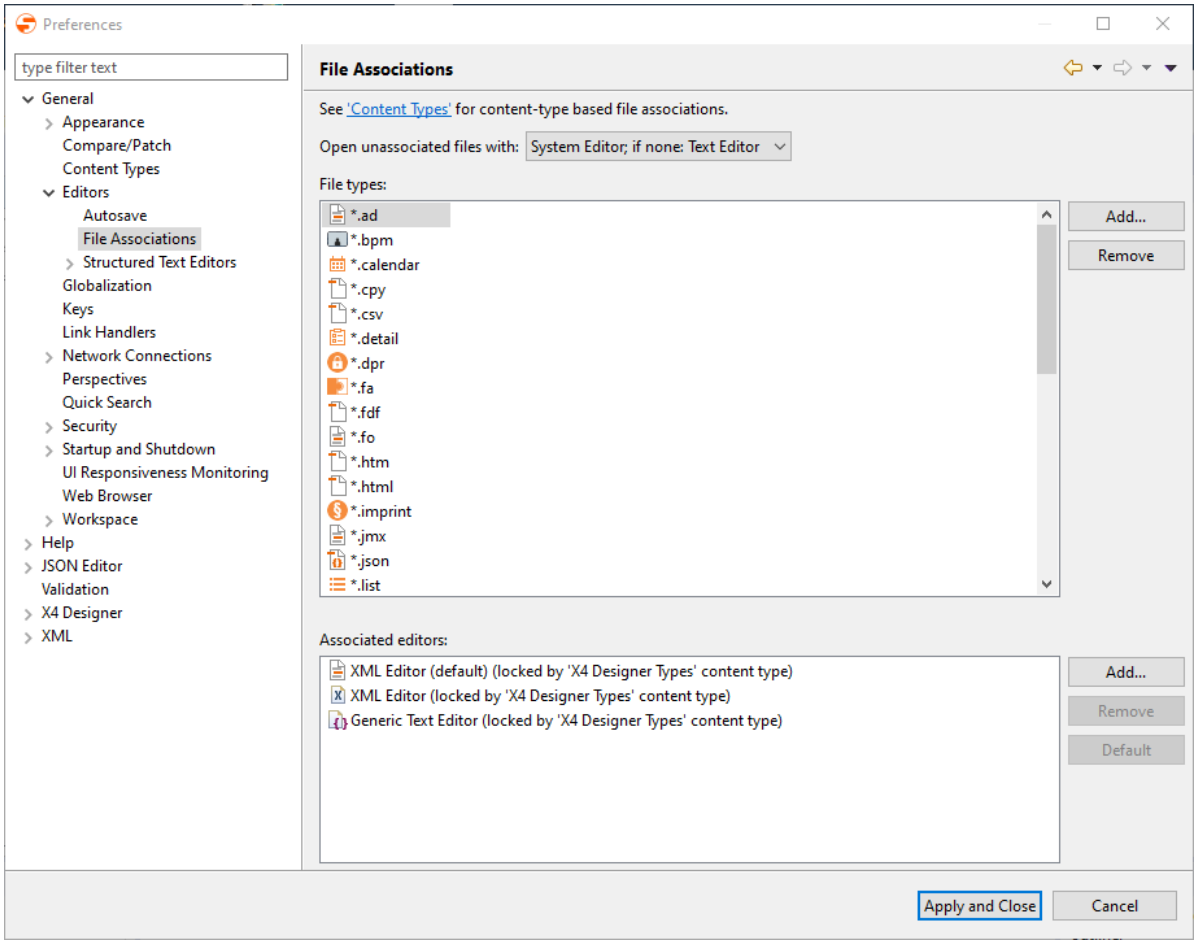


3. Vorlagen wie gewünscht verwalten:
   - **Edit:** Dateinamen und/oder den Beschreibungstext bearbeiten
   - **Remove:** Markierte Vorlage löschen
   - **Import:** Einen bestehenden Vorlagen-Ordner importieren
     ℹ Zulässig sind nur Vorlagen-Ordner, welche die gleiche Struktur wie der Ordner `<X4>/X4DB/0/Templates` 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.

2.2.6 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.

> ⓘ 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.

> ⓘ 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.

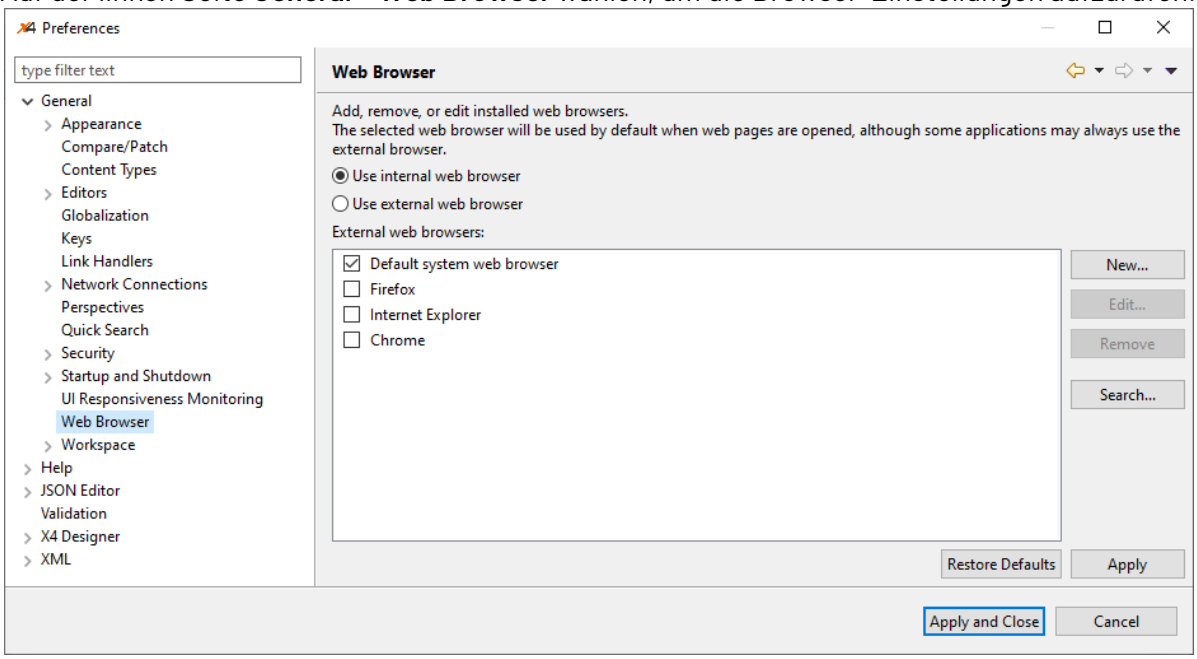
> ✔ Wenn der Dateityp standardmäßig mit dem gewählten Editor geöffnet werden soll, auf **Default** klicken.

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.

2.2.7 Web Browser konfigurieren

Für die Anzeige der browserbasierten Komponenten der X4 BPMS können verschiedene Browser verwendet werden (siehe X4 BPMS-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.

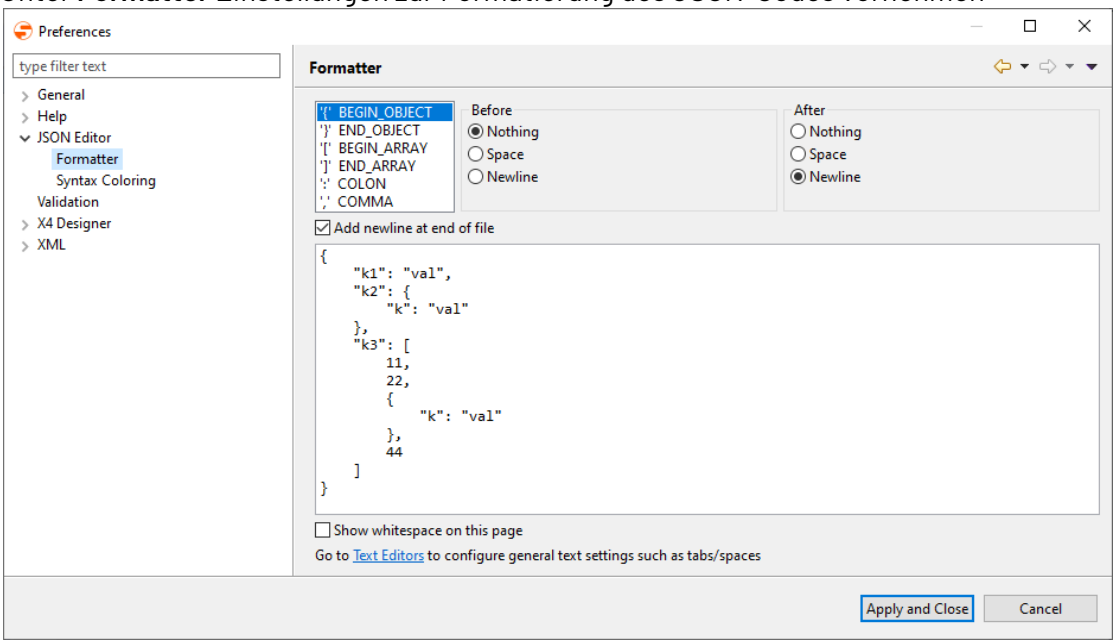
   > Um Microsoft Edge verwenden zu können, muss folgendes eingetragen werden:
   > **Location:** Speicherort der Windows-Eingabeaufforderung, z. B. *C:\Windows\System32\cmd.exe*
   > **Parameters:** /c "start microsoft-edge:%URL%"

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

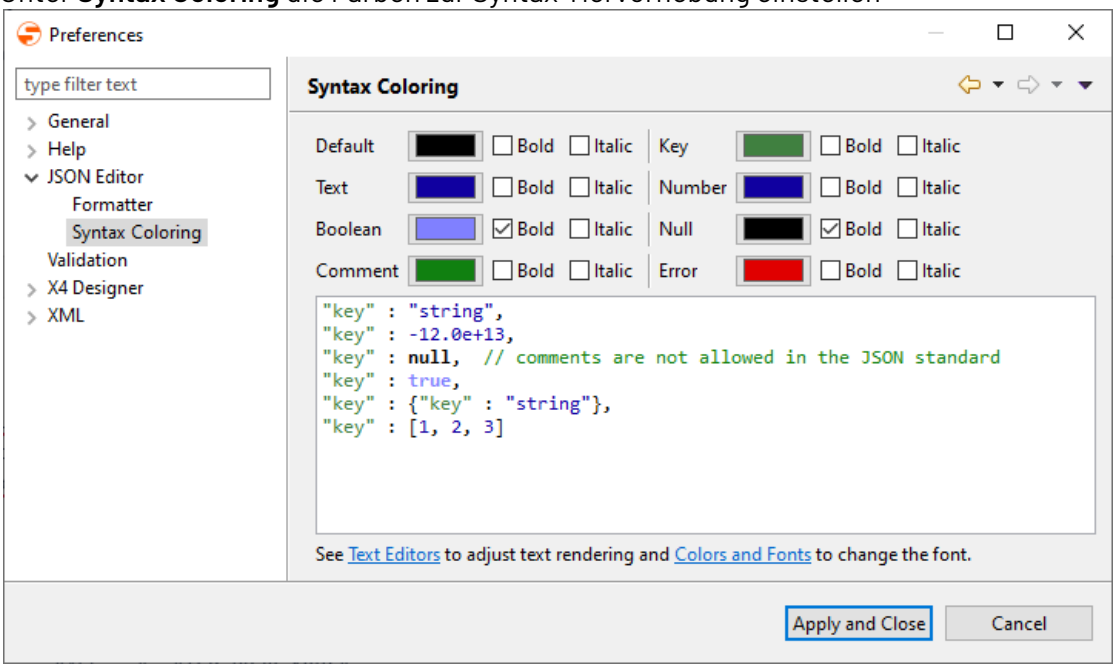
2.2.8 JSON-Editor konfigurieren

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.

2.2.9 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.

3 Administration des X4 Servers

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

3.1 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.

3.2 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.MQGMO_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.

3.3 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

4 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.

4.1 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 geschalten 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.

4.1.1 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.

4.1.1.1 Einfach – Direkter Datenbankzugriff

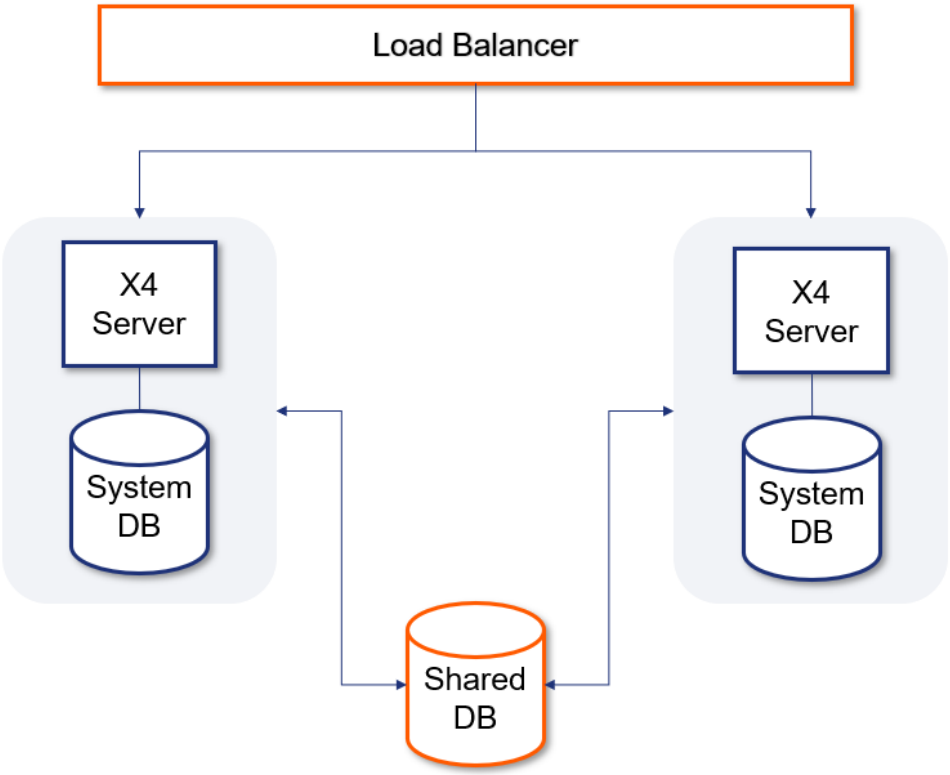


Abb. Direkter Datenbankzugriff

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.

4.1.1.2 Komplex – Gemeinsamer Zugriff über eine X4 Instanz

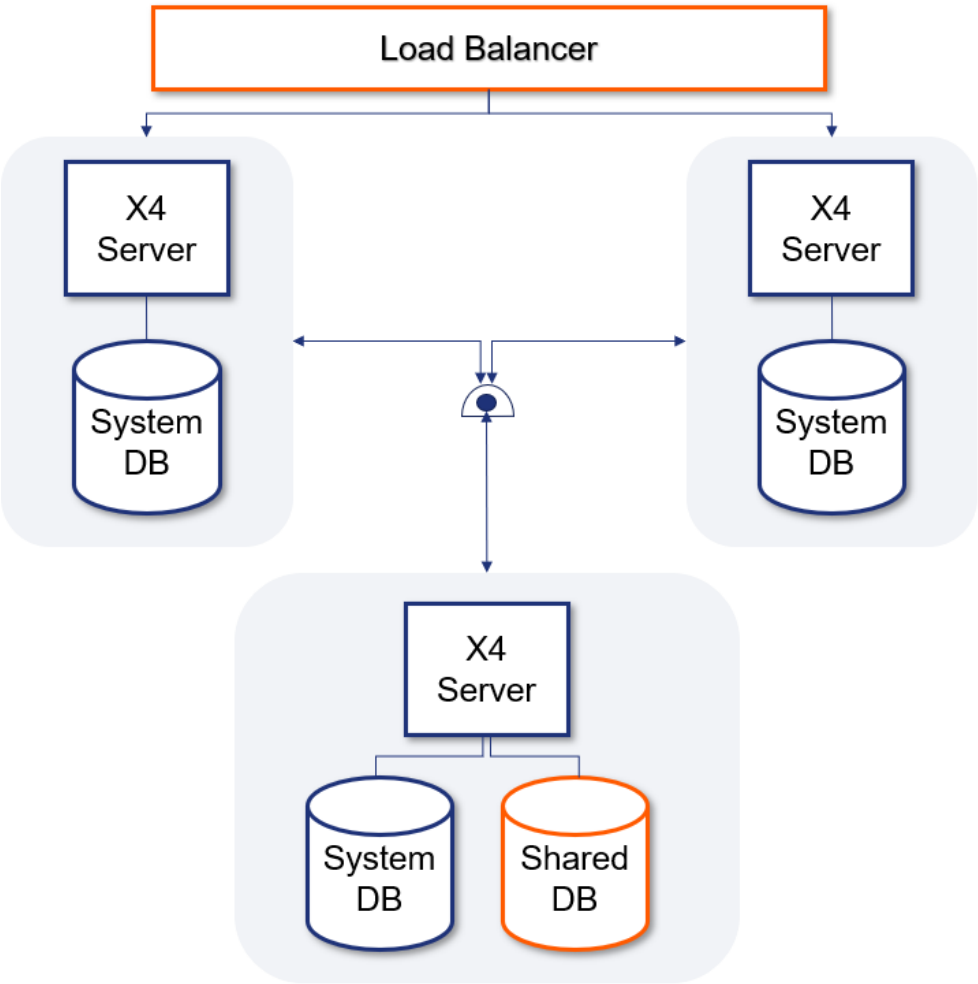


Abb. Gemeinsamer Datenbankzugriff über eine X4 Instanz

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.

4.1.2 Szenario – Gemeinsamer Zugriff über Message Queue

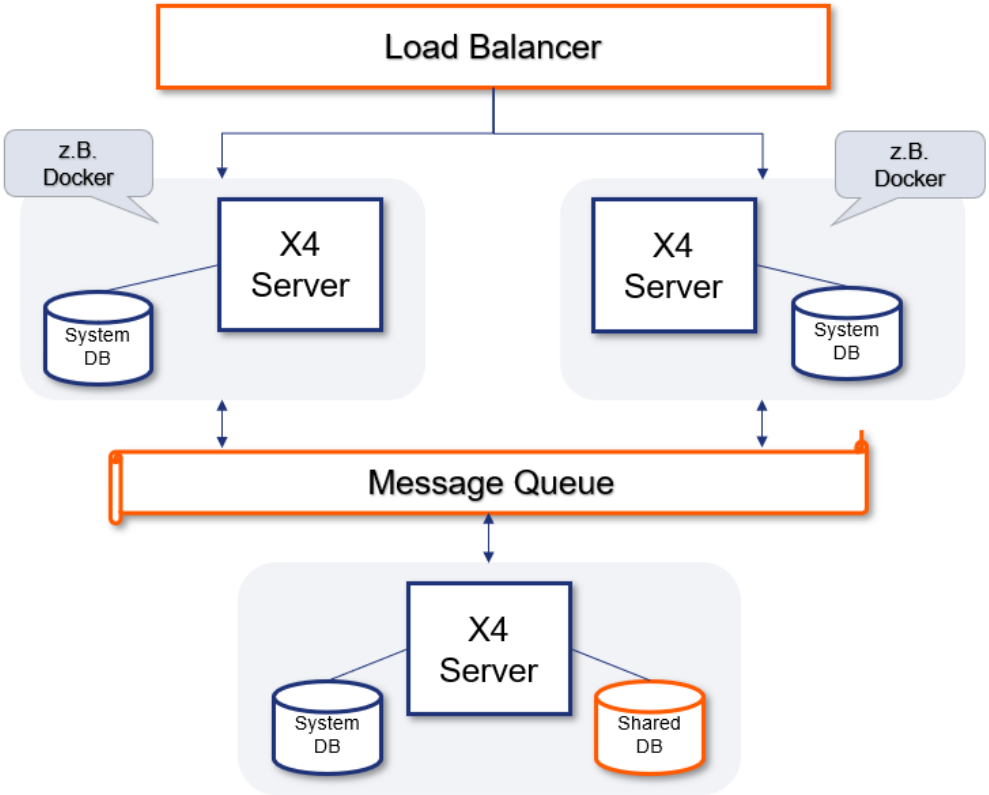


Abb. Gemeinsamer Zugriff über Message Queue

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.

4.2 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.

4.2.1 Szenario – Eine exklusive Datenbank

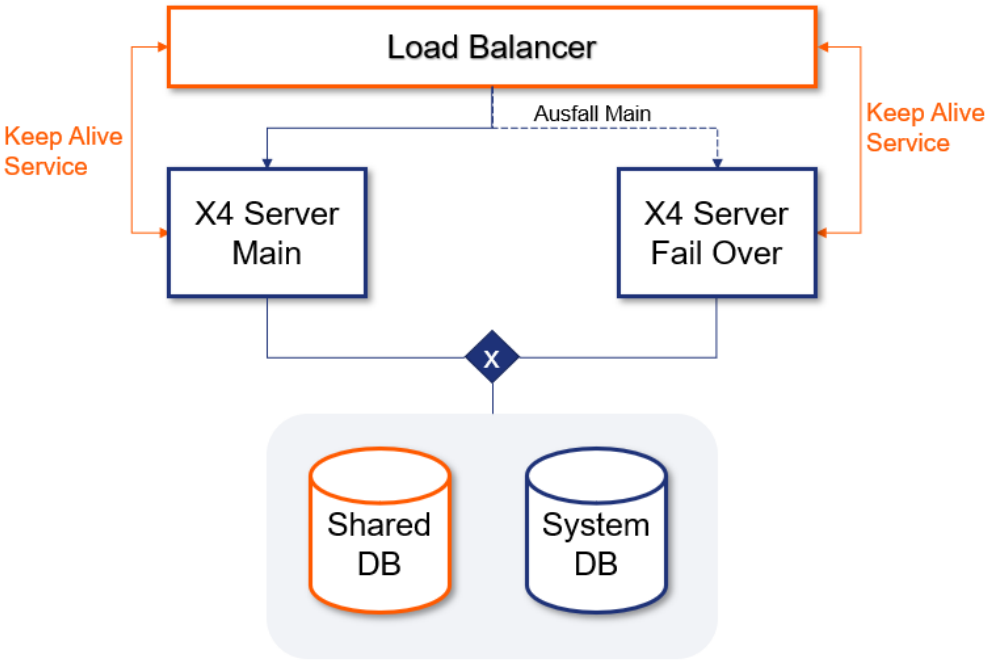


Abb.Eine Datenbank mit exklusivem Zugriff

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.

4.2.2 Szenario – Systemdatenbank pro X4 Server

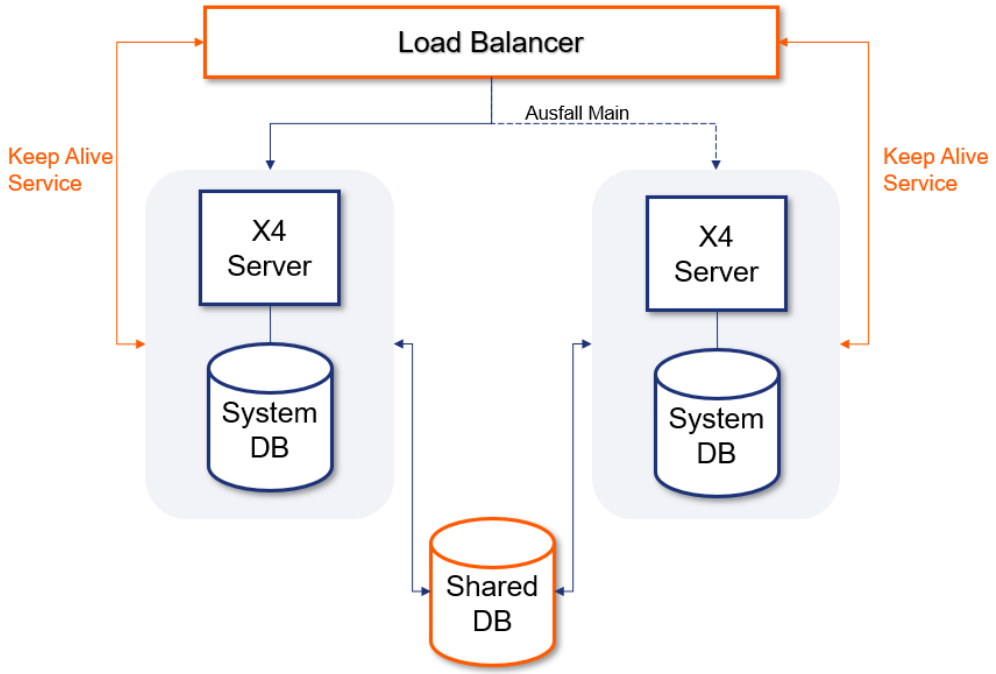


Abb. Getrennte Systemdatenbanken

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 gewährleisen, 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.

4.3 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.

4.3.1 Szenario – Dedizierter X4 Server für Scheduling

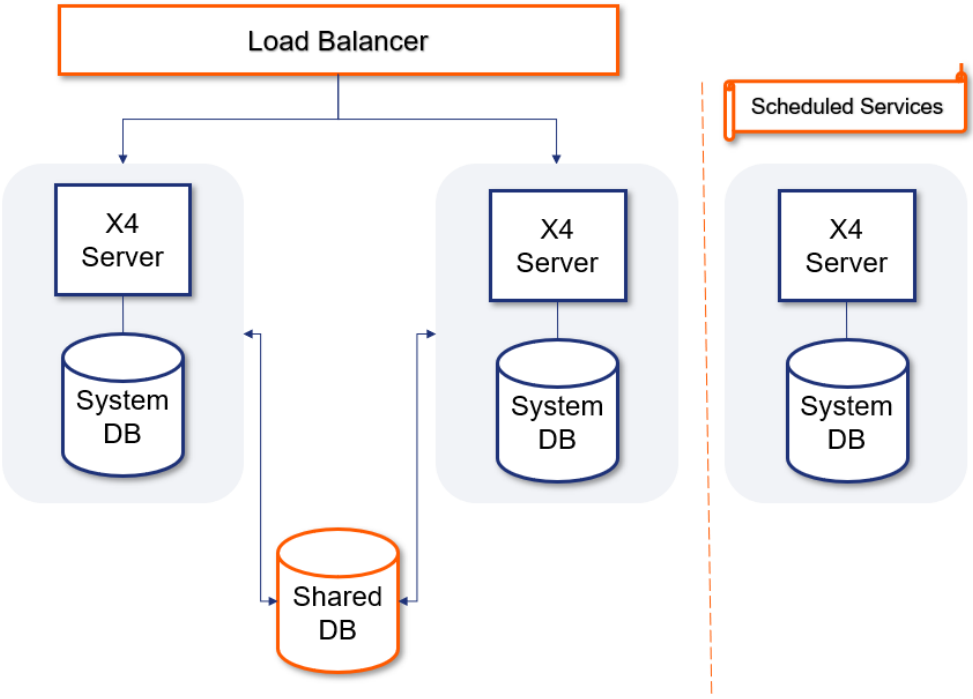


Abb. Dedizierter Scheduler X4 Server

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.

4.3.2 Szenario – Ein Server zuständig für Scheduling

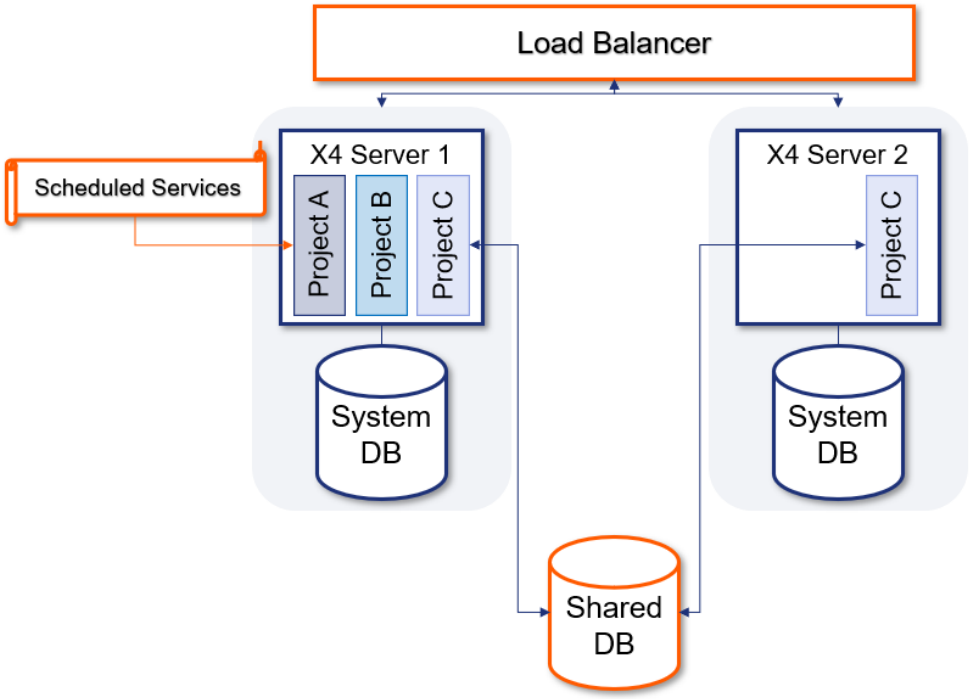


Abb. Geplante Prozesse in X4 Projekt

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.

4.3.3 Szenario – Externer Scheduler

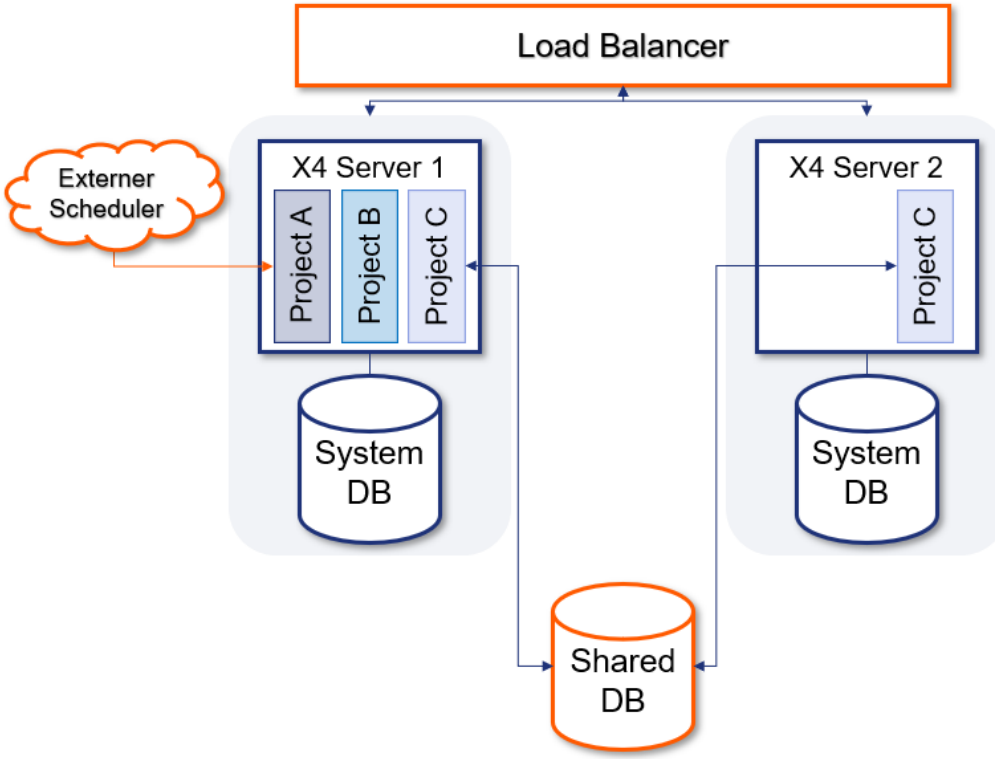


Abb. Geplante Prozesse durch externen Scheduler-Dienst

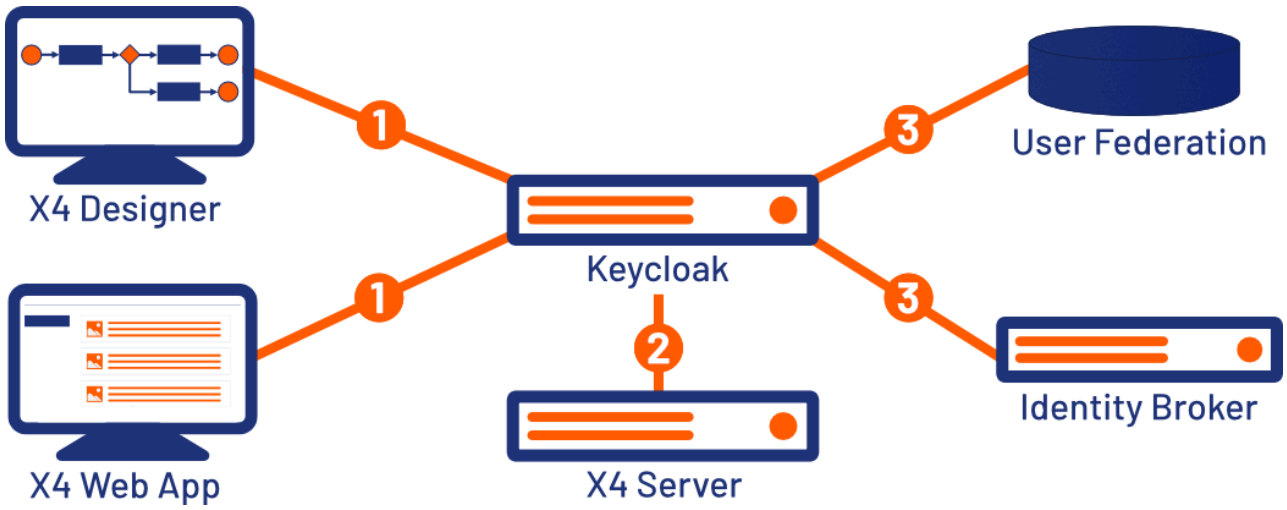
Neben der im X4 Server vorhandenen Scheduler-Implementierung kann auch ein externer Dienst Prozesse automatisiert starten. Dieser spricht die auszuführenden Prozesse direkt auf dem Server an, auf dem das Projekt *A* installiert ist.

5 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 bereits 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

Keycloak wird standardmäßig mit einer H2-Datenbank ausgeliefert, damit der 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/server/db.

5.1 Keycloak für produktiven Betrieb konfigurieren

Keycloak wird standardmäßig mit einer H2-Datenbank ausgeliefert, damit Keycloak ohne weitere Konfiguration verwendet werden kann. Die H2-Datenbank ist jedoch aufgrund von Sicherheitsmängeln und eingeschränkter Skalierbarkeit nicht für den produktiven Betrieb geeignet.

Um Keycloak für einen sicheren produktiven Betrieb nutzen können, sollten Sie zuvor Folgendes konfigurieren:

- TLS (Transport Layer Security)
- Hostname
- Reverse-Proxy/Load-Balancer-Komponente
- SQL-Datenbank

Hinweis:
Weitere Informationen zum Anbinden von Datenbanken an Keycloak finden Sie in der offiziellen Keycloak-Dokumentation (https://www.keycloak.org):

- alternative Datenbank an Keycloak anbinden für den produktiven Betrieb: https://www.keycloak.org/server/configuration-production *(Guides > Server > Configuring Keycloak for Production)*
- Datenbank an Keycloak anbinden: https://www.keycloak.org/server/db (*Guides > Server > Configuring the Database)*

Hinweis:
Bitte beachten Sie, dass die Einstellungen je nach Art der Datenbank unterschiedlich sind.
Um eine alternative Datenbank mit Keycloak einzurichten, müssen Sie den Standard Keycloak X4Realm und die Benutzer importieren.
Verwenden Sie dazu die Skripte, die im Ordner **<Serververzeichnis>\keycloak\data\import** enthalten sind (`X4Realm-realm.json` und `X4Realm-users-0.json`).
Beide Skripte können über einen Include-Mechanismus importiert werden, der in der offiziellen Keycloak-Dokumentation beschrieben ist: https://www.keycloak.org/server/importExport (*Guides > Server > Importing and Exporting Realms*).

5.2 Keycloak-Administrationskonsole aufrufen

> **Hinweis**
> Um die Keycloak-Administrationskonsole aufrufen zu können, muss ein initialer Admin-Benutzer in Keycloak vorhanden sein. Diesen können Sie über http://localhost:8085/auth/ anlegen.
> Weitere Information hierzu finden Sie im *Keycloak Server Administration Guide* im Abschnitt „Creating the first administrator" (https://www.keycloak.org/docs/latest/server_admin/index.html#creating-first-admin_server_administration_guide).

Die Keycloak-Administrationskonsole kann dann erreicht werden über:

- Direktlink (http://localhost:8085/auth/admin/)
- die Schaltfläche **User Management** im X4 Control Center (http://localhost:8080/)

> **Hinweis**
> Wenn Sie nicht über eine `localhost`-Adresse auf den Server zugreifen können oder Keycloak über die Befehlszeile starten möchten, können Sie den initialen Admin-Benutzer auch remote anlegen.
> Weitere Informationen hierzu finden Sie im *Keycloak Server Administration Guide* im Abschnitt „Creating the account remotely" (https://www.keycloak.org/docs/latest/server_admin/index.html#creating-the-account-remotely).

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

> **Weitere Informationen**:
> - Hinweise zur Keycloak-Administrationskonsole

5.2.1 Hinweise zur Keycloak-Administrationskonsole

Nach der Keycloak-Installation (und ggf. nach Anlegen des initialen Admin-Benutzers) können Sie sich als Admin in der Keycloak-Administrationskonsole (**User Management**) anmelden über:

- X4 Control Center (URL: http://localhost:8080/) über die Schaltfläche **User Management**
- Direktlink zum **User Management** (http://localhost:8085/auth/admin/master/console/#/X4Realm/users)

Dort können Sie den bereits vorhandenen Default-Benutzer aufrufen bzw. weitere Benutzer anlegen. Der Default-Benutzer ist vorhanden, um den Designer und Web Apps zu verwenden.

> **Hinweis**
> Achten Sie beim Aufrufen des Default-Benutzers sowie beim Anlegen neuer Benutzer darauf, dass Sie im entsprechenden Realm sind. Der Default-Benutzer ist im **X4Realm** angelegt.
> Der Direktlink zum Realm enthält den Namen des Realms, hier am Beispiel **X4Realm**: http://localhost:8085/auth/admin/master/console/#/**X4Realm**

5.3 Einrichten

5.3.1 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 Element `<connection>` vorgenommen.

Beispiel

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

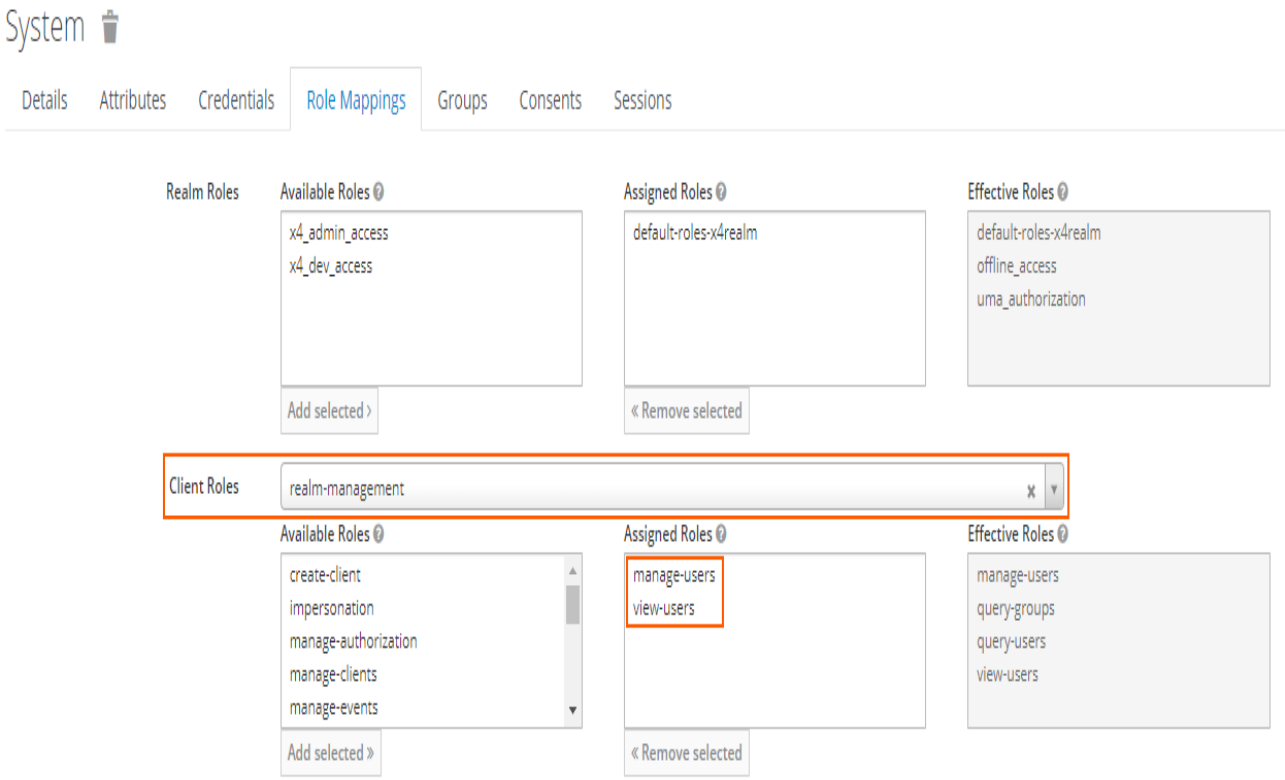
Folgende Rollen müssen in Keycloak erstellt werden:

Rolle	Beschreibung
x4_admin_access	Gewährt Zugriff auf die X4 ReST-API.
x4_control_center	Gewährt in Zukunft Zugriff auf das X4 Control Center.
x4_dev_access	Gewährt Zugriff auf den X4 Designer.
x4_dev_access_*	Gewährt Zugriff auf alle X4 Repositorys.

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

Client Roles	• realm-management

Assigned Roles	• manage-users • view-users



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

5.4 Konfigurieren

5.4.1 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.

Weitere Informationen finden Sie im Abschnitt Configuration.

5.4.2 Zugriff auf Workspaces 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.

5.4.2.1 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.

5.4.3 Standardkonfiguration

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

5.4.3.1 Realm Settings

5.4.3.1.1 General

Label	Wert
Name	X4Realm
Enabled	`ON`

5.4.3.1.2 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`

5.4.3.1.3 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

5.4.3.1.4 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

5.4.3.2 Clients

5.4.3.2.1 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`

5.4.3.2.1.1 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`

5.4.3.2.1.2 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`

5.4.3.2.1.3 Advanced Settings

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

5.4.3.2.2 Credentials

Label	Wert
Client Authenticator	`Client Id and Secret`

5.4.3.2.3 Client Scopes

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

5.4.3.2.4 Mappers

5.4.3.2.4.1 Group Membership Mapper

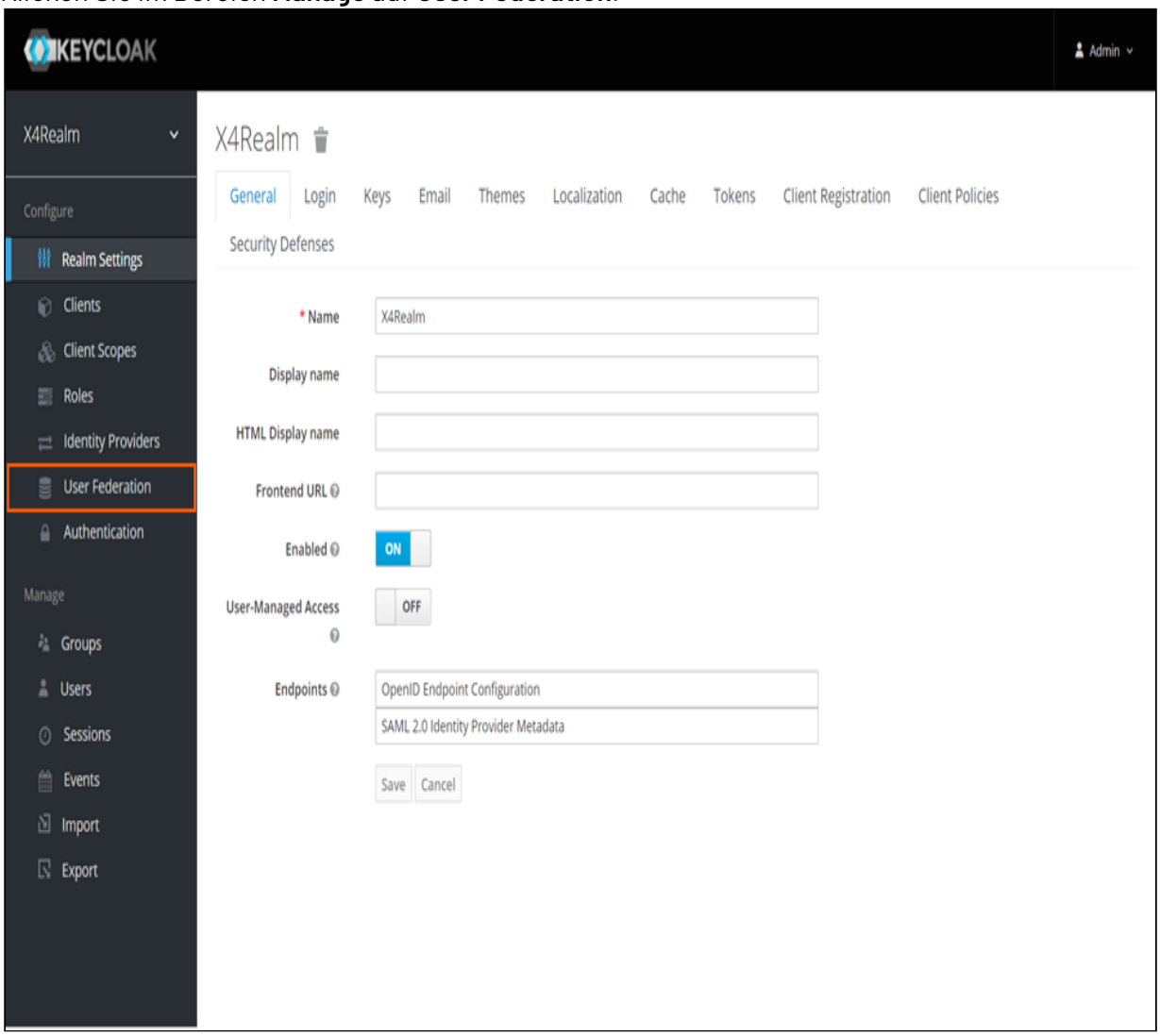
Label	Wert
Name	Group Membership Mapper
Mapper Type	Group Membership
Token Claim Name	groups
Full group path	OFF
Add to ID token	ON
Add to access token	ON
Add to userinfo	ON

5.4.4 LDAP anbinden

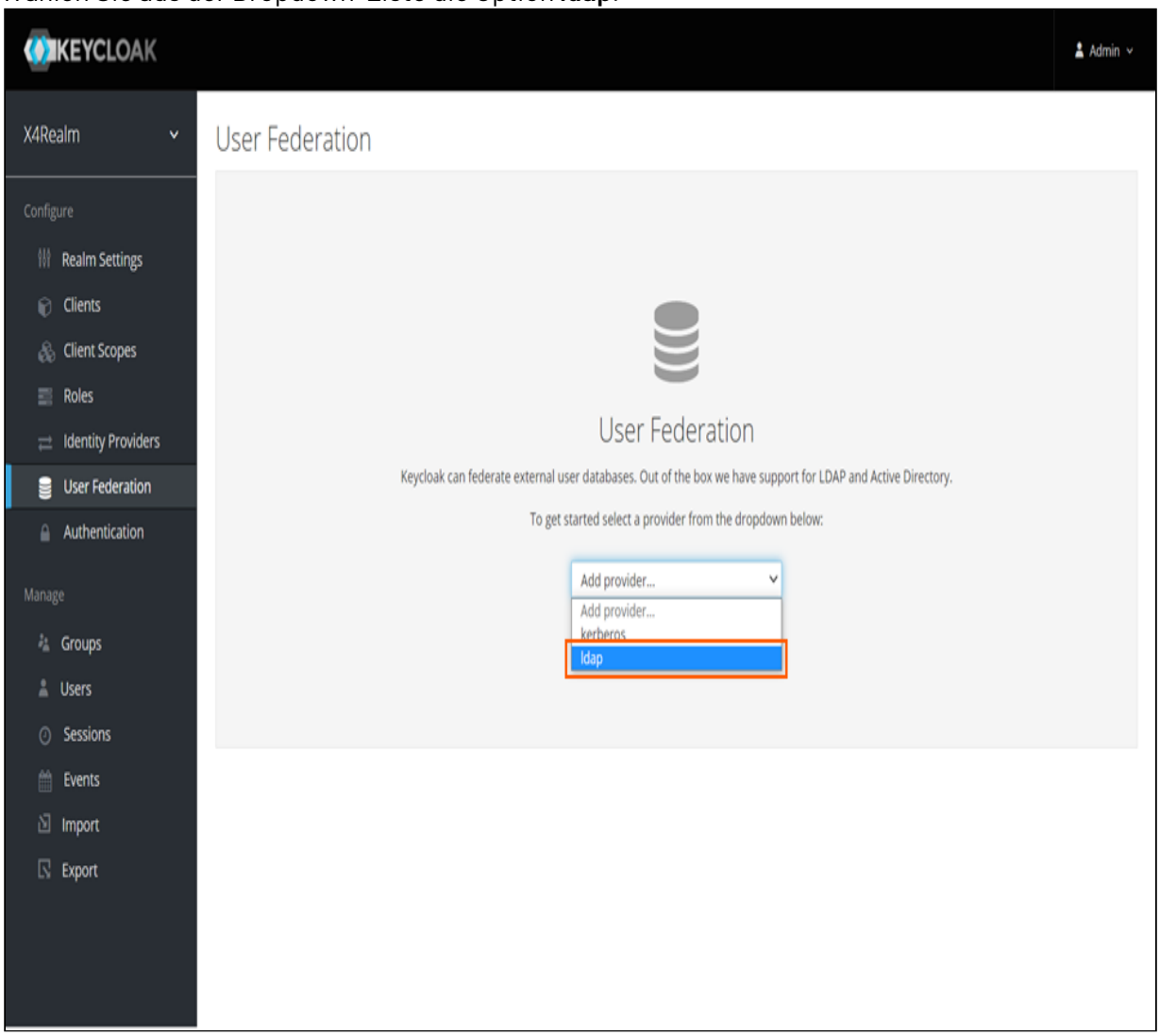
In Keycloak können Sie ein bestehendes LDAP anbinden. Keycloak verfügt über einen eingebauten LDAP/AD-Anbieter. Es ist möglich, mehrere verschiedene LDAP-Server in denselben Keycloak-Realm einzubinden.

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

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



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



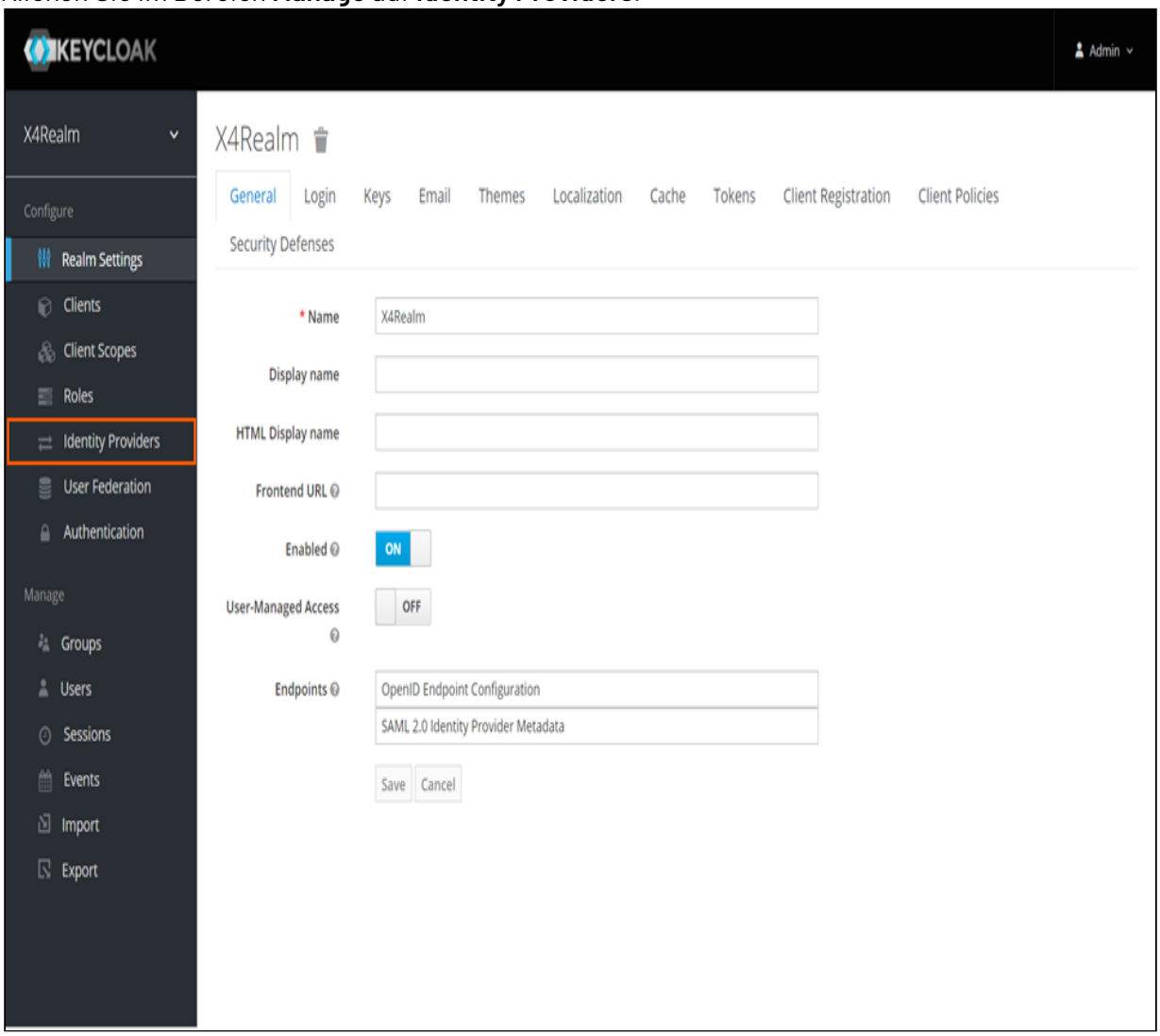
Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_ldap.

5.4.5 SAML v2.0 anbinden

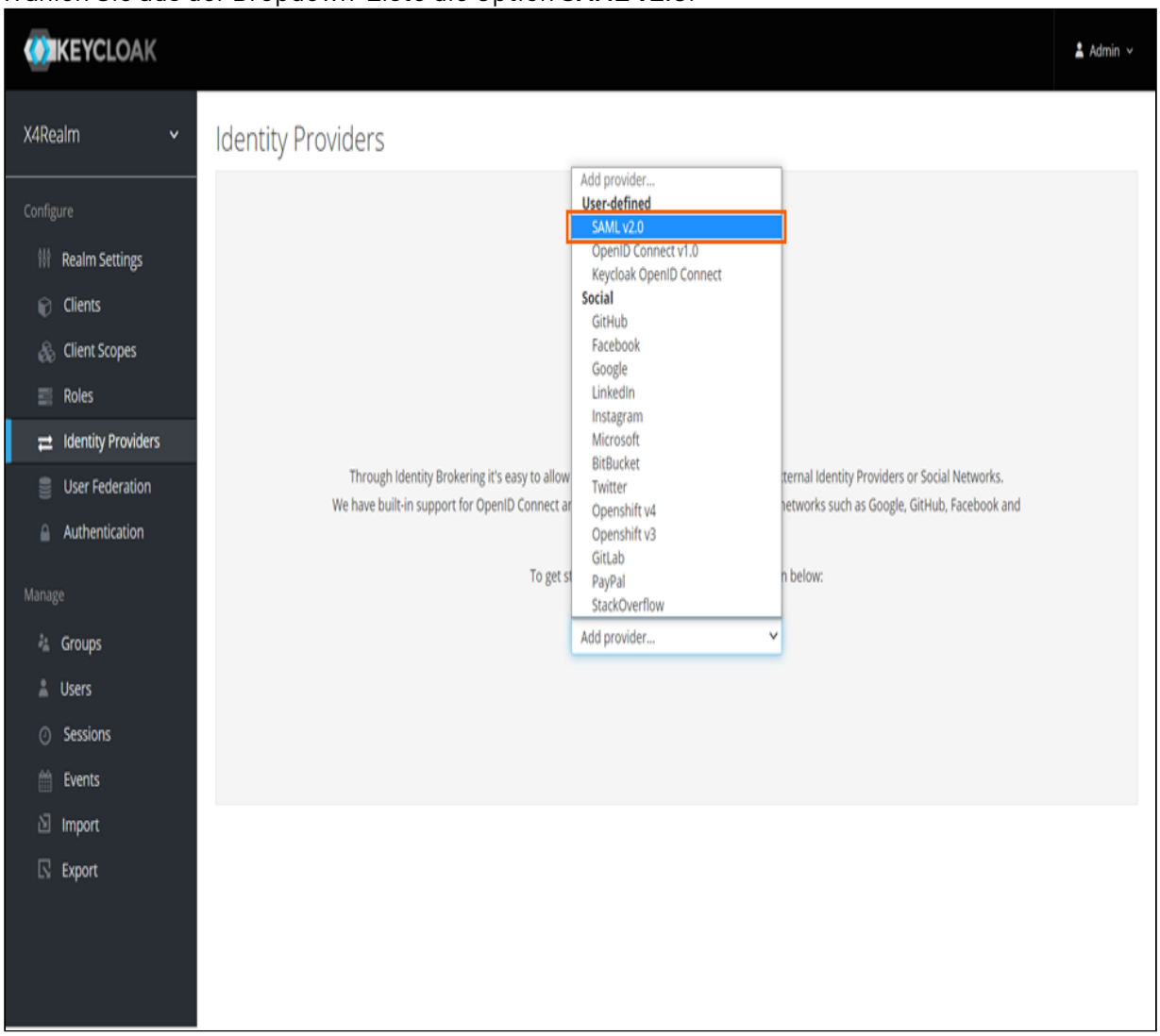
In Keycloak können Sie ein bestehendes SAML v2.0 anbinden. Keycloak kann Identitätsanbieter vermitteln, die auf dem SAML v2.0 Protokoll basieren.

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

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



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



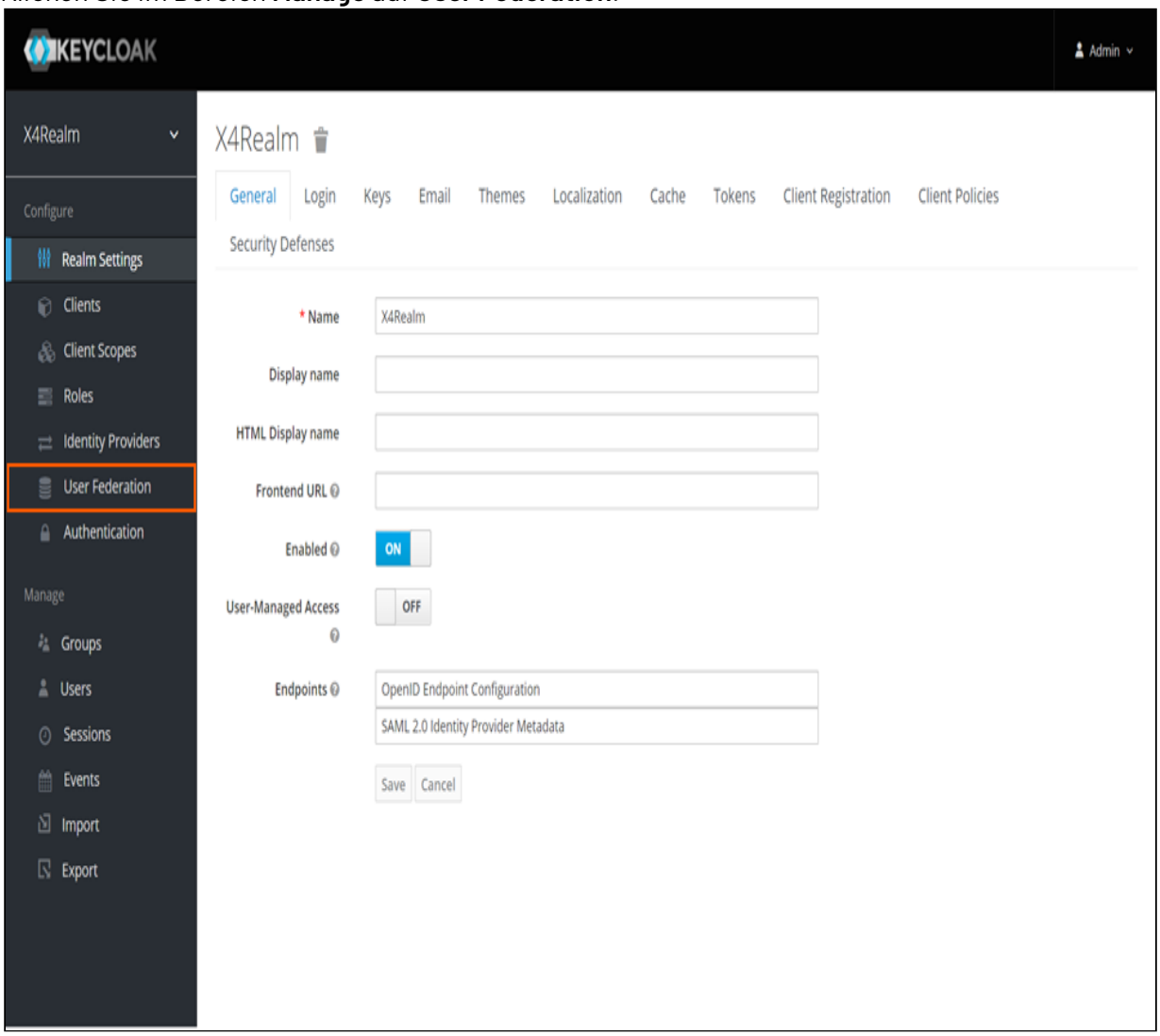
Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#saml-v2-0-identity-providers.

5.4.6 Kerberos anbinden

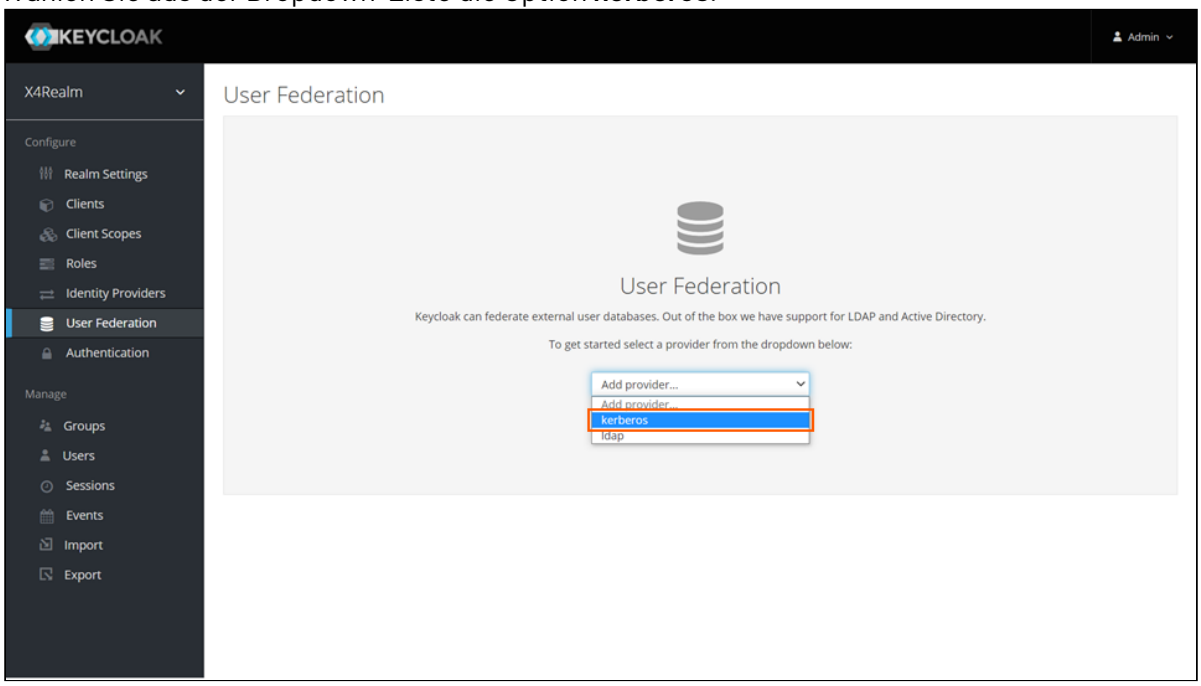
In Keycloak können Sie ein bestehendes Kerberos anbinden. Keycloak unterstützt die Anmeldung mit einem Kerberos-Ticket über das SPNEGO-Protokoll.

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

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



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



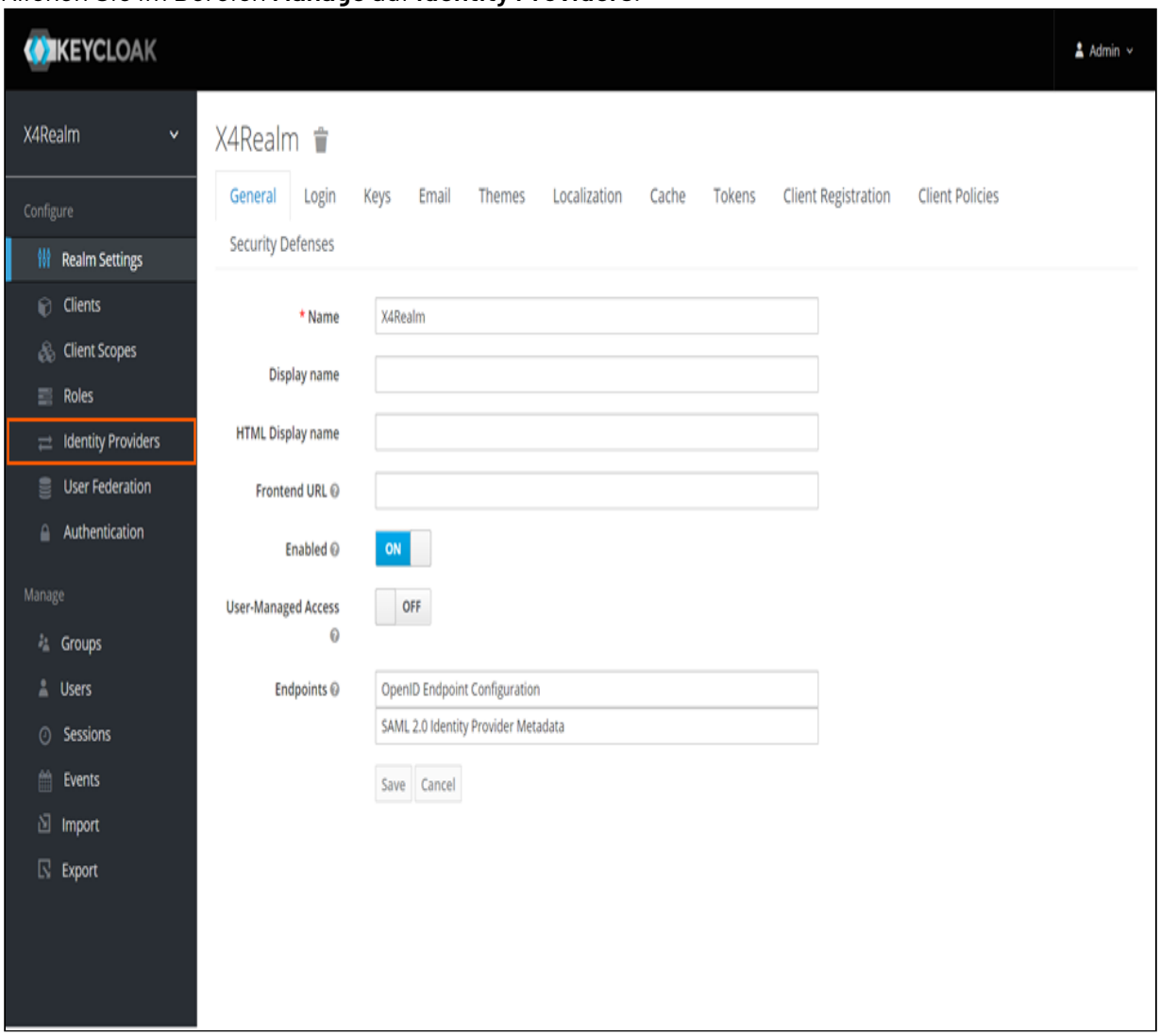
Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_kerberos.

5.4.7 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**.



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.

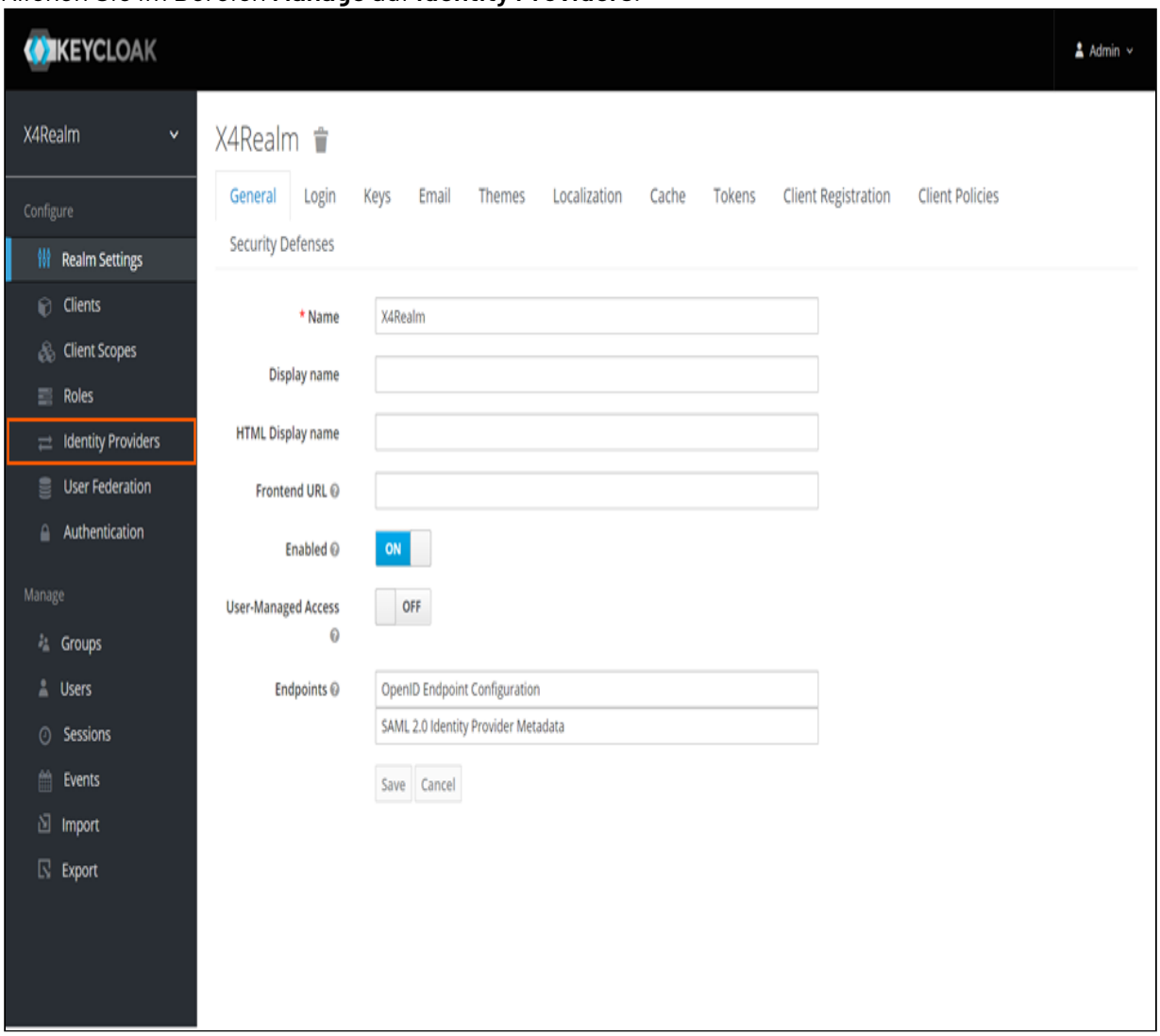
> Wenn Sie sich mit dem Benutzer eines Social Identity- Anbieter anmelden, können Sie das Passwort nicht über die Web Apps ändern.

5.4.8 OpenID Connect anbinden

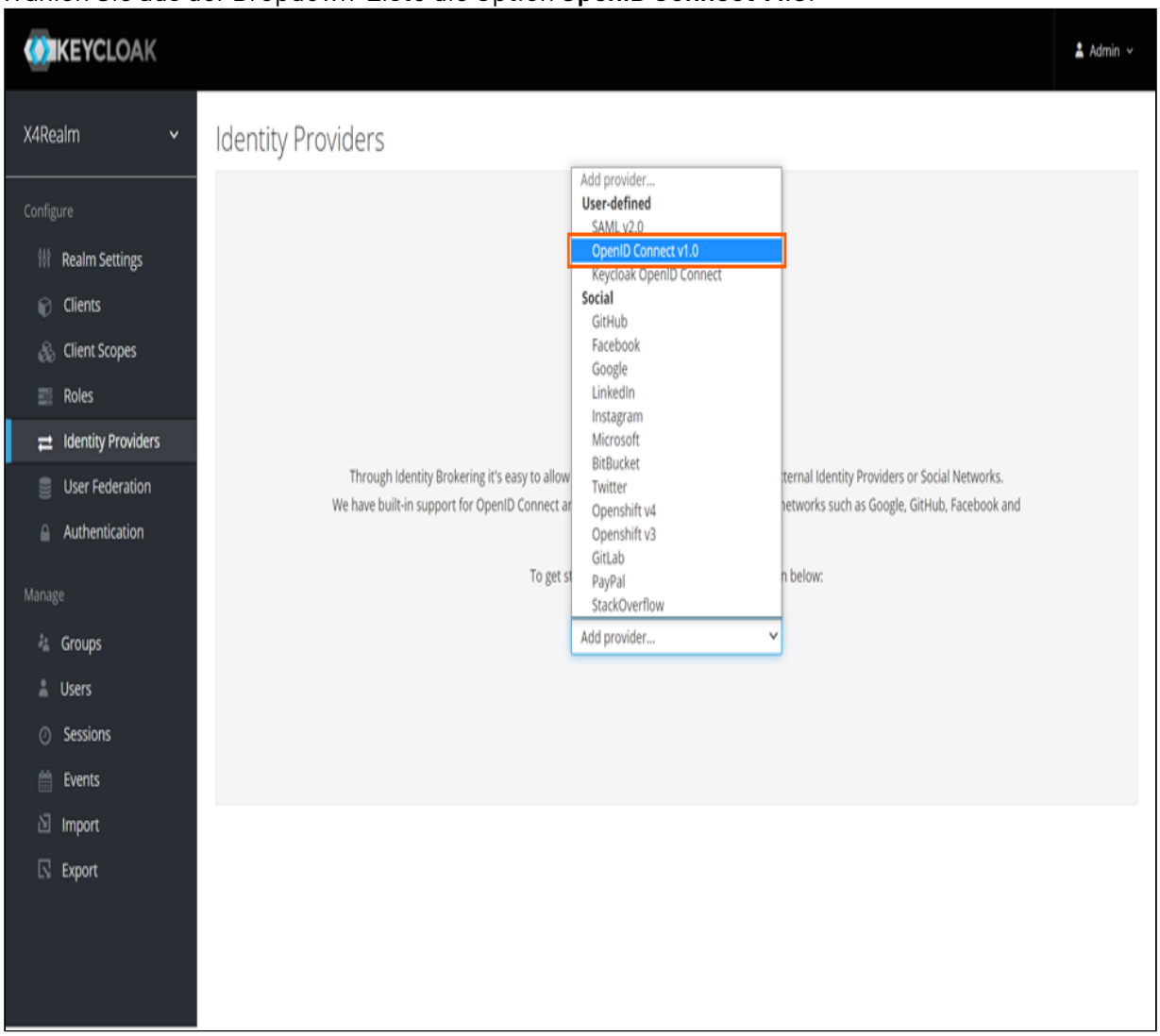
In Keycloak können Sie einen bestehenden OpenID Connect-Anbieter anbinden. Der Identitätsanbieter muss den Authorization Code Flow unterstützen, um den Benutzer zu authentifizieren und den Zugriff zu autorisieren.

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

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



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.

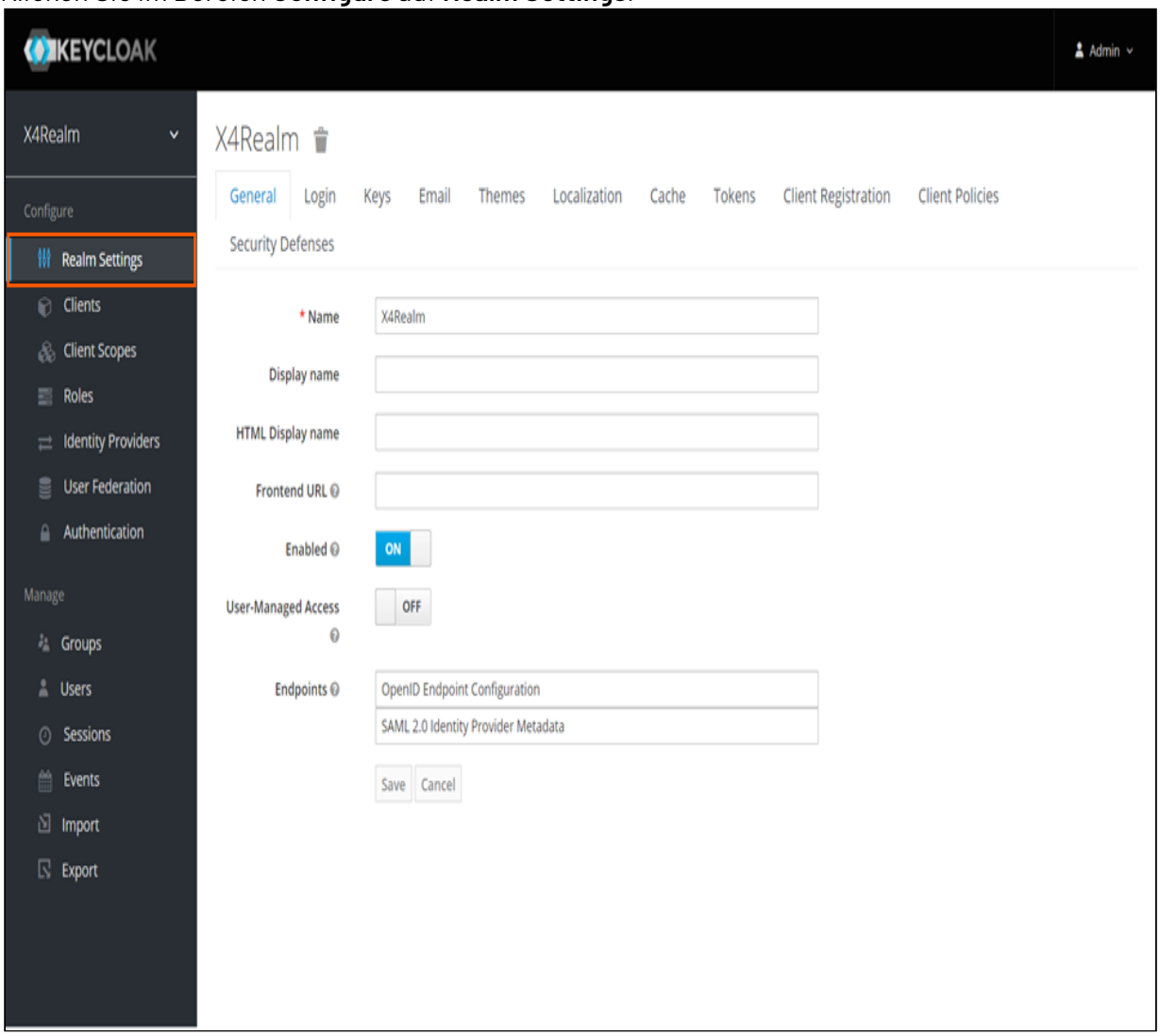
5.4.9 Anmeldeseite

5.4.9.1 Angemeldet bleiben-Schaltfläche

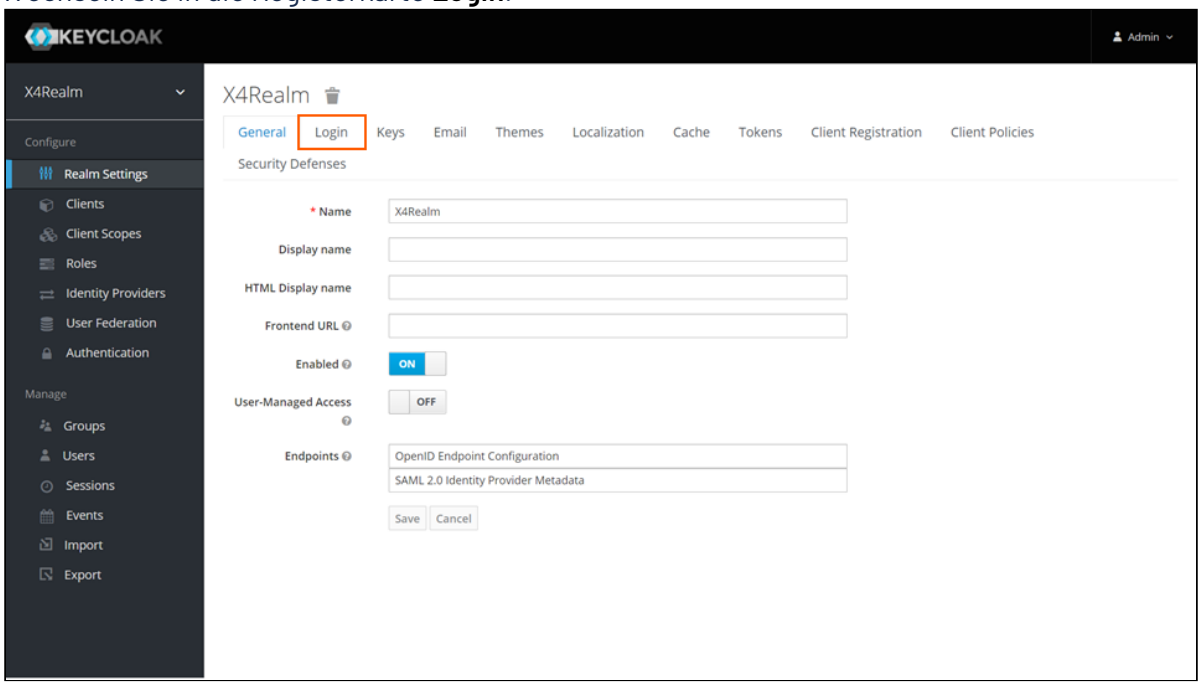
Die Angemeldet bleiben-Schaltfläche kann in der Keycloak Administrationskonsole im Realm Settings Menü aktiviert werden.

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

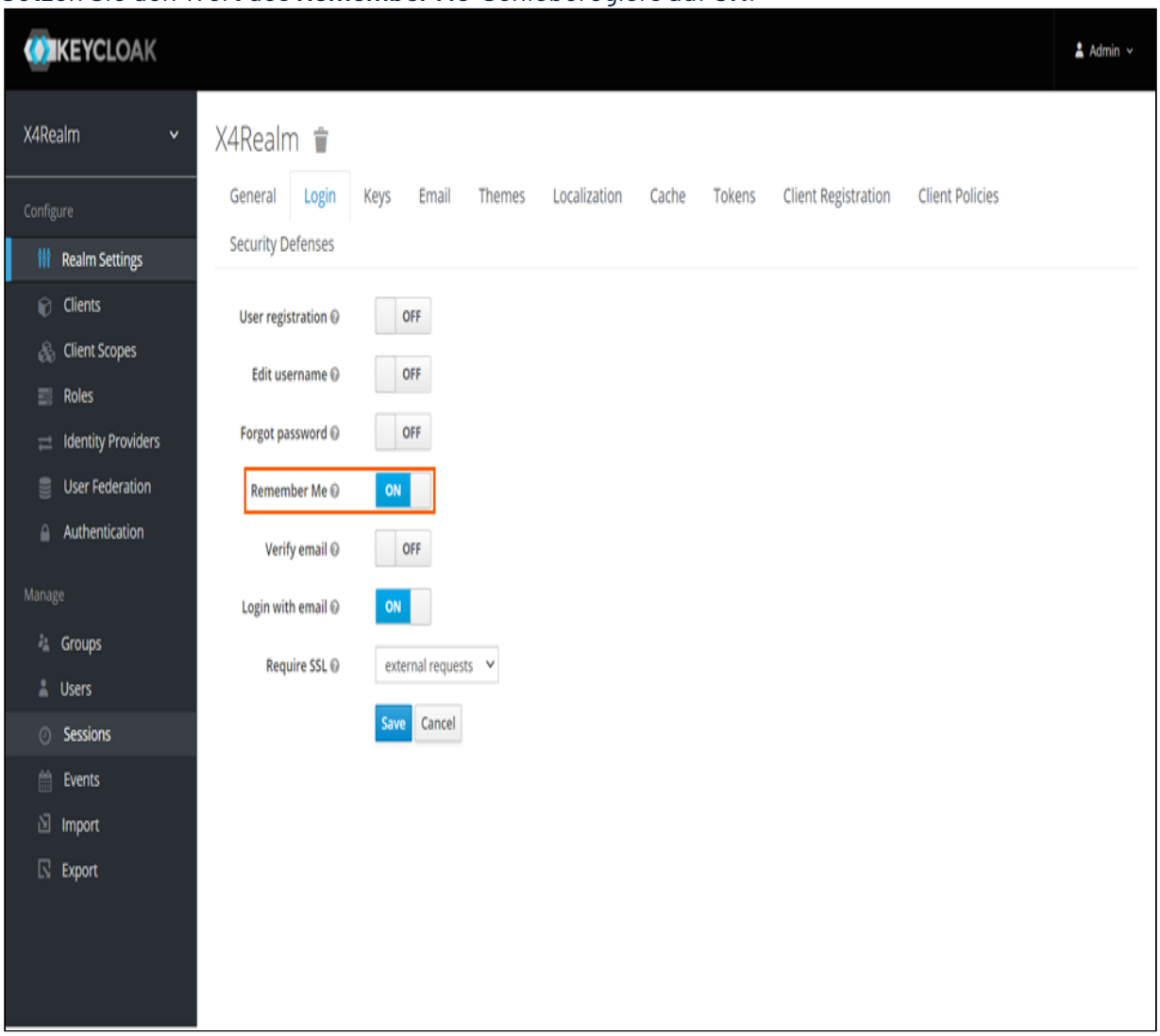
2. Klicken Sie im Bereich **Configure** auf **Realm Settings**.



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



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



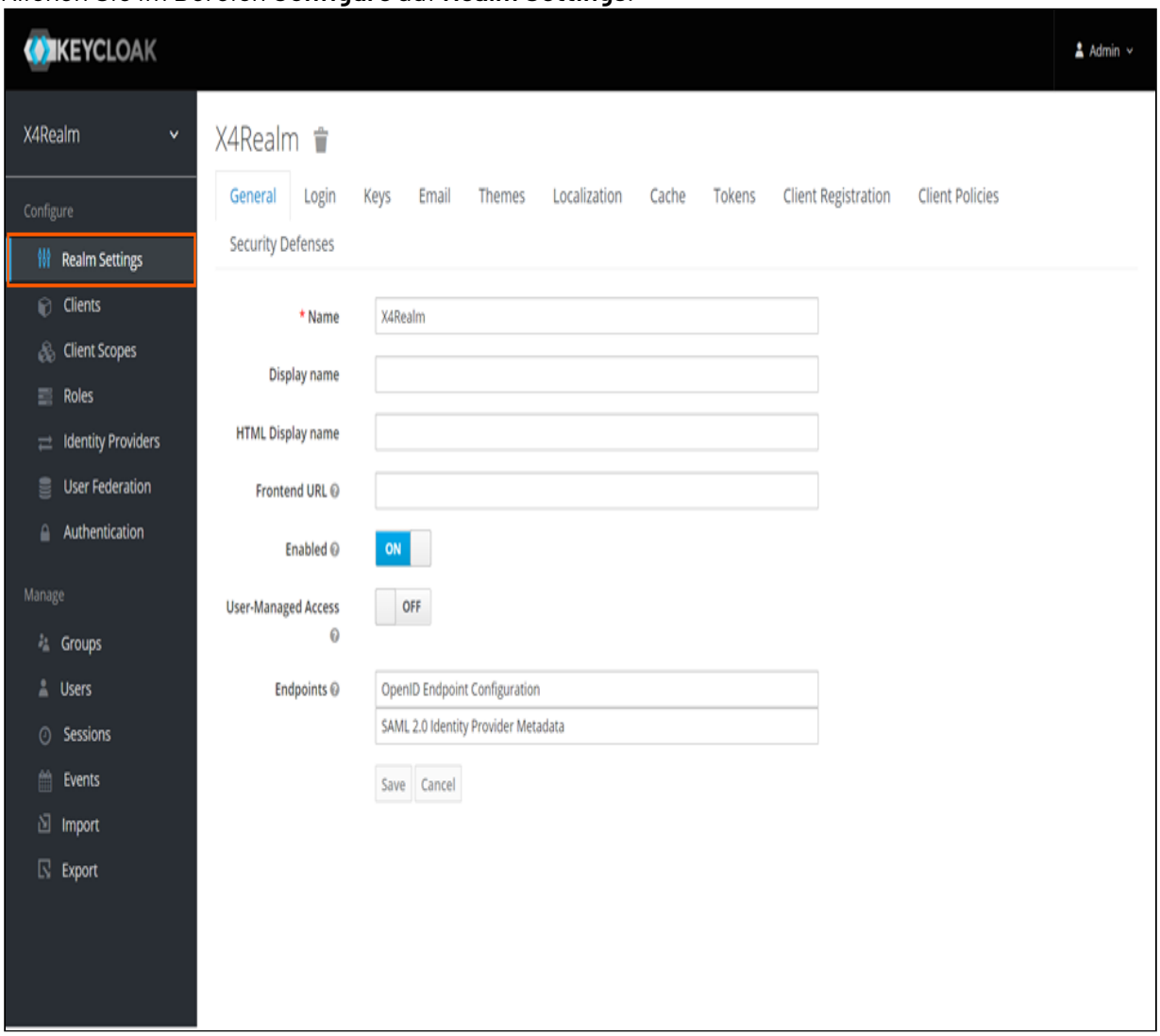
5. Klicken Sie auf **Save**.

5.4.9.2 Passwort vergessen-Schaltfläche

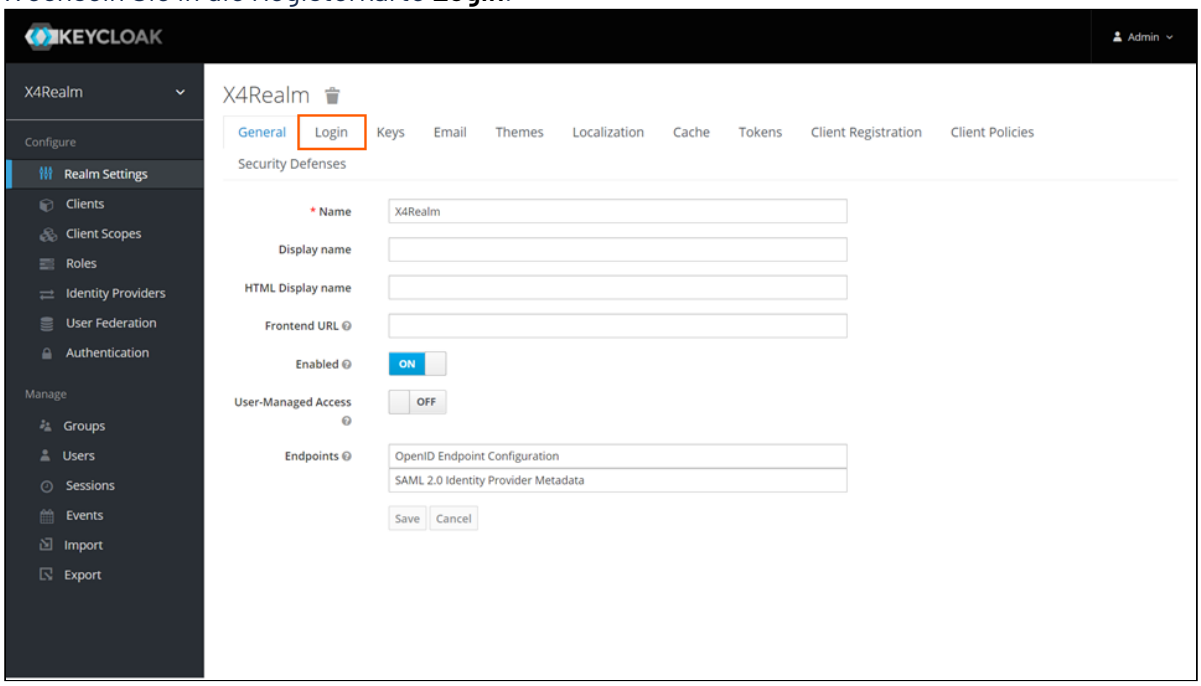
Die Passwort vergessen-Schaltfläche kann in der Keycloak Administrationskonsole im Realm Settings Menü aktiviert werden.

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

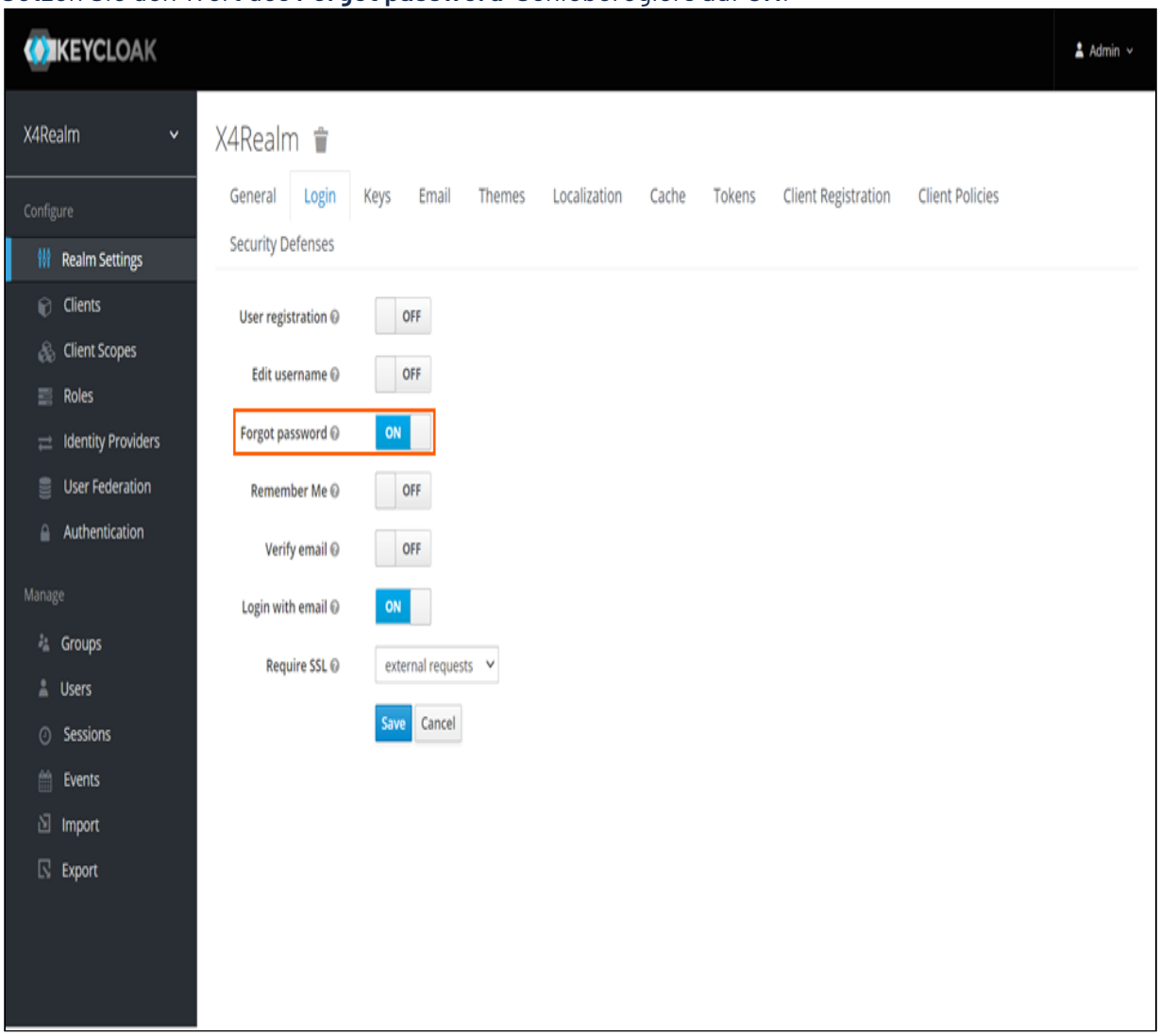
2. Klicken Sie im Bereich **Configure** auf **Realm Settings**.



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



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



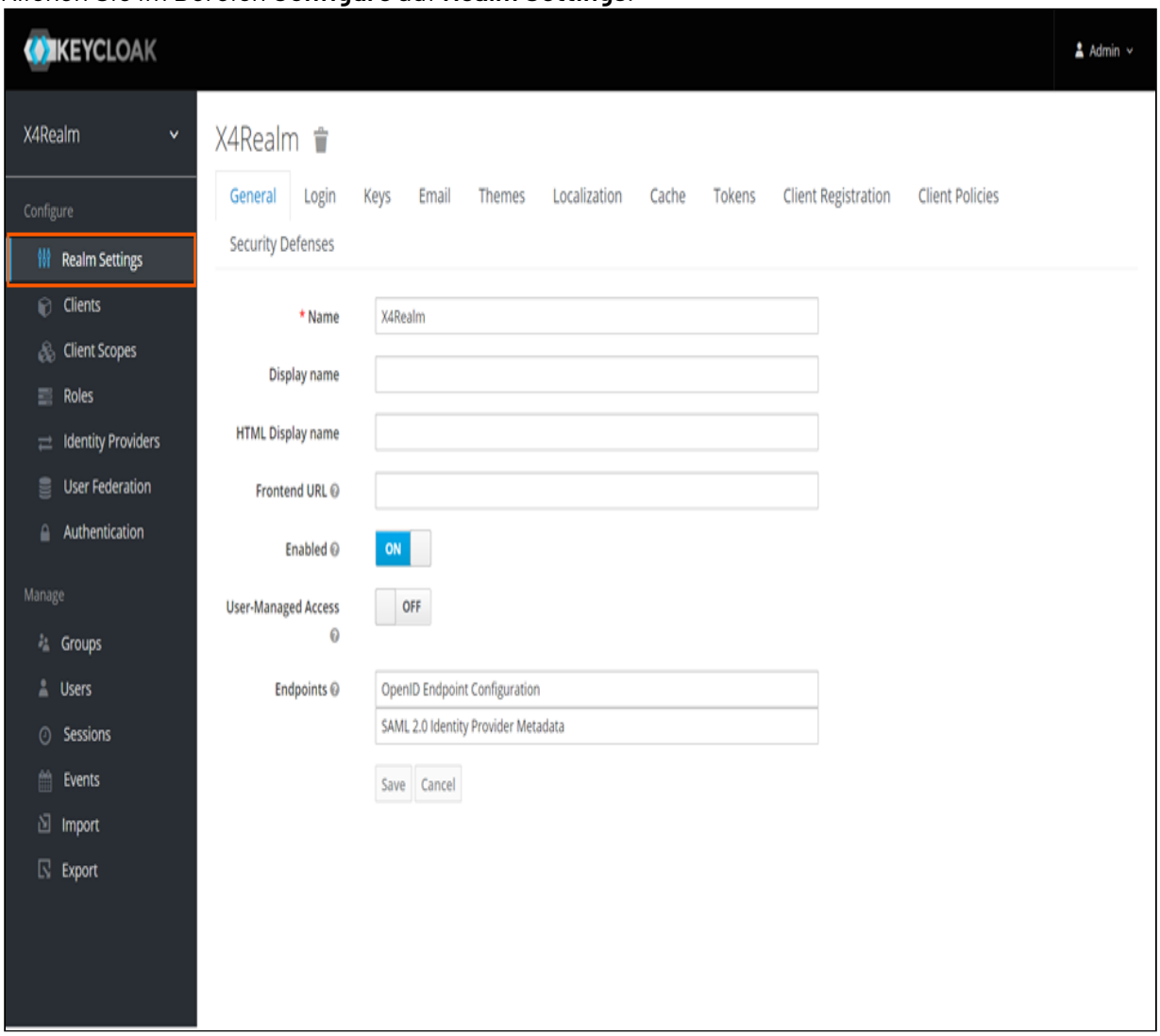
5. Klicken Sie auf **Save**.

5.4.9.3 Registrierung aktivieren

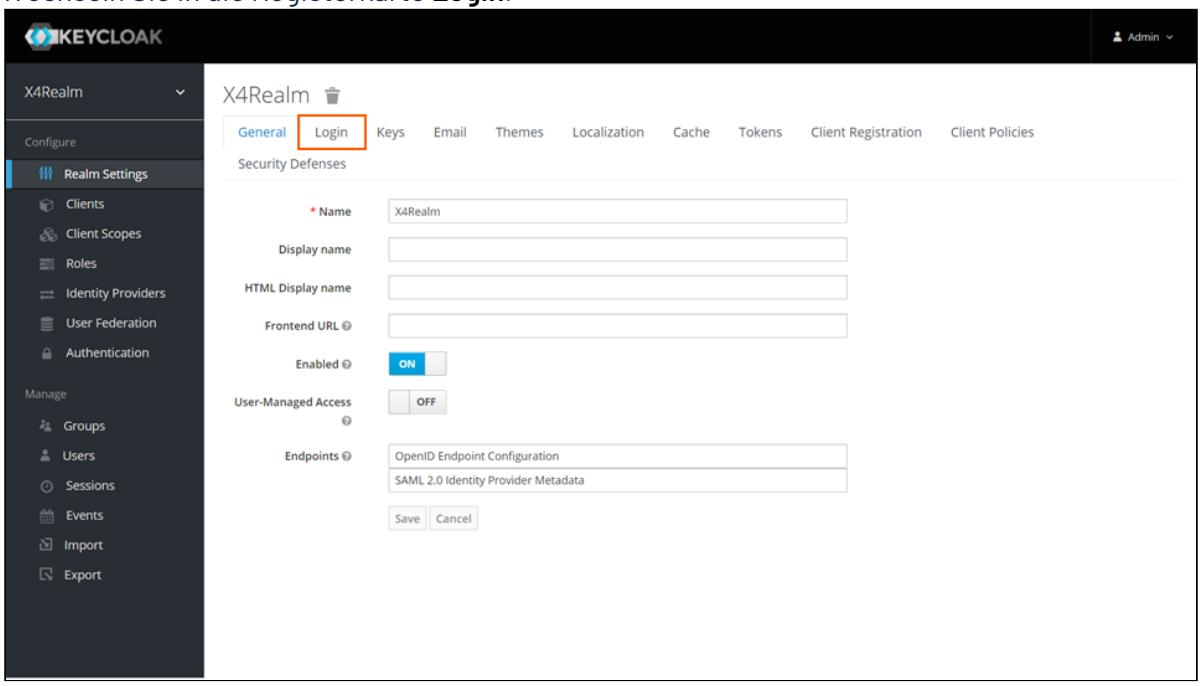
Die Registrieren-Schaltfläche kann in der Keycloak Administrationskonsole im Realm Settings Menü aktiviert werden.

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

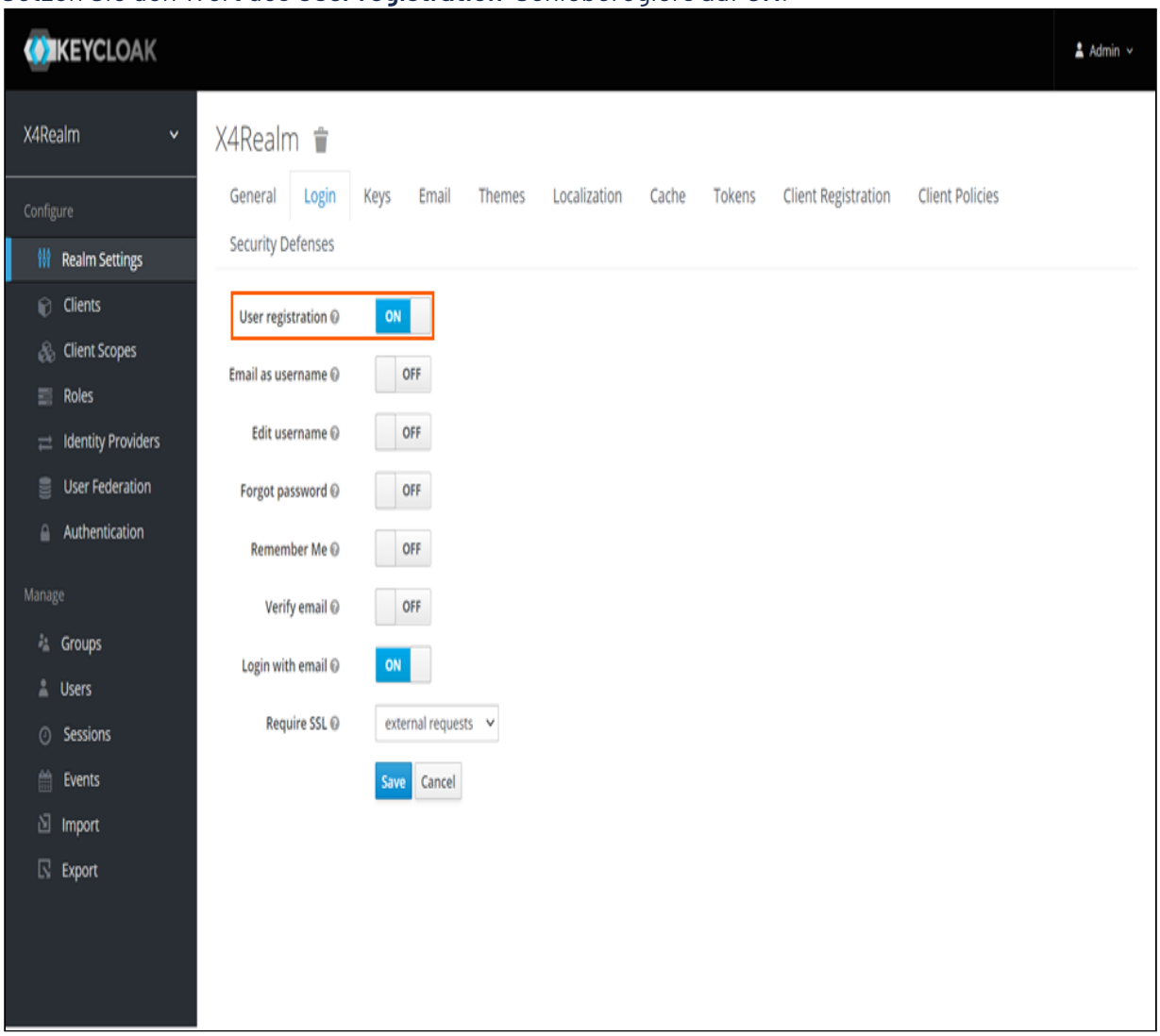
2. Klicken Sie im Bereich **Configure** auf **Realm Settings**.



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



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**.

5.4.10 Passwörter

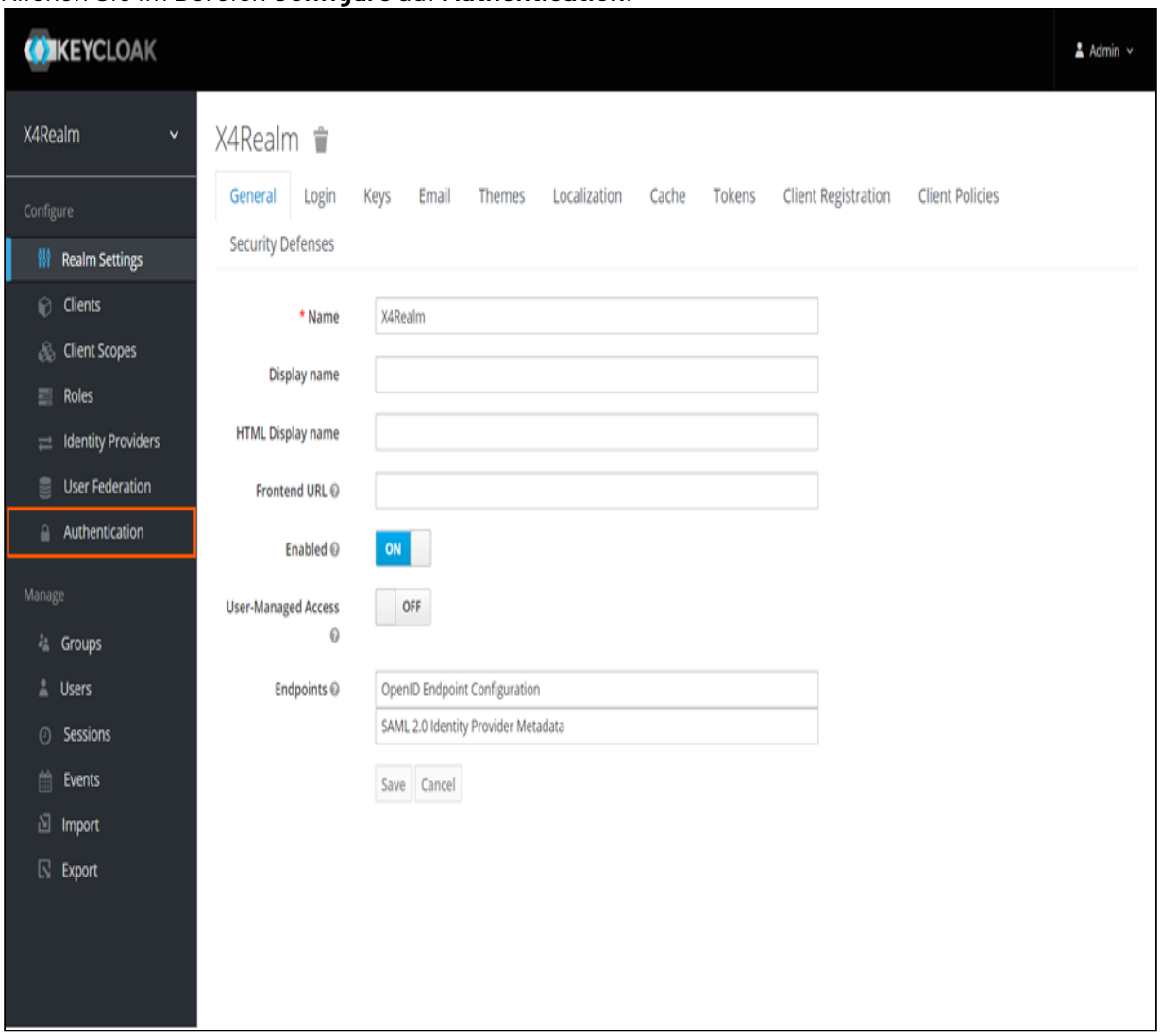
In Keycloak können Sie verschieden Einstellungen zu Passwörtern festlegen, wie zum Beispiel Passwortrichtlinien.

5.4.10.1 Passwortrichtlinien festlegen

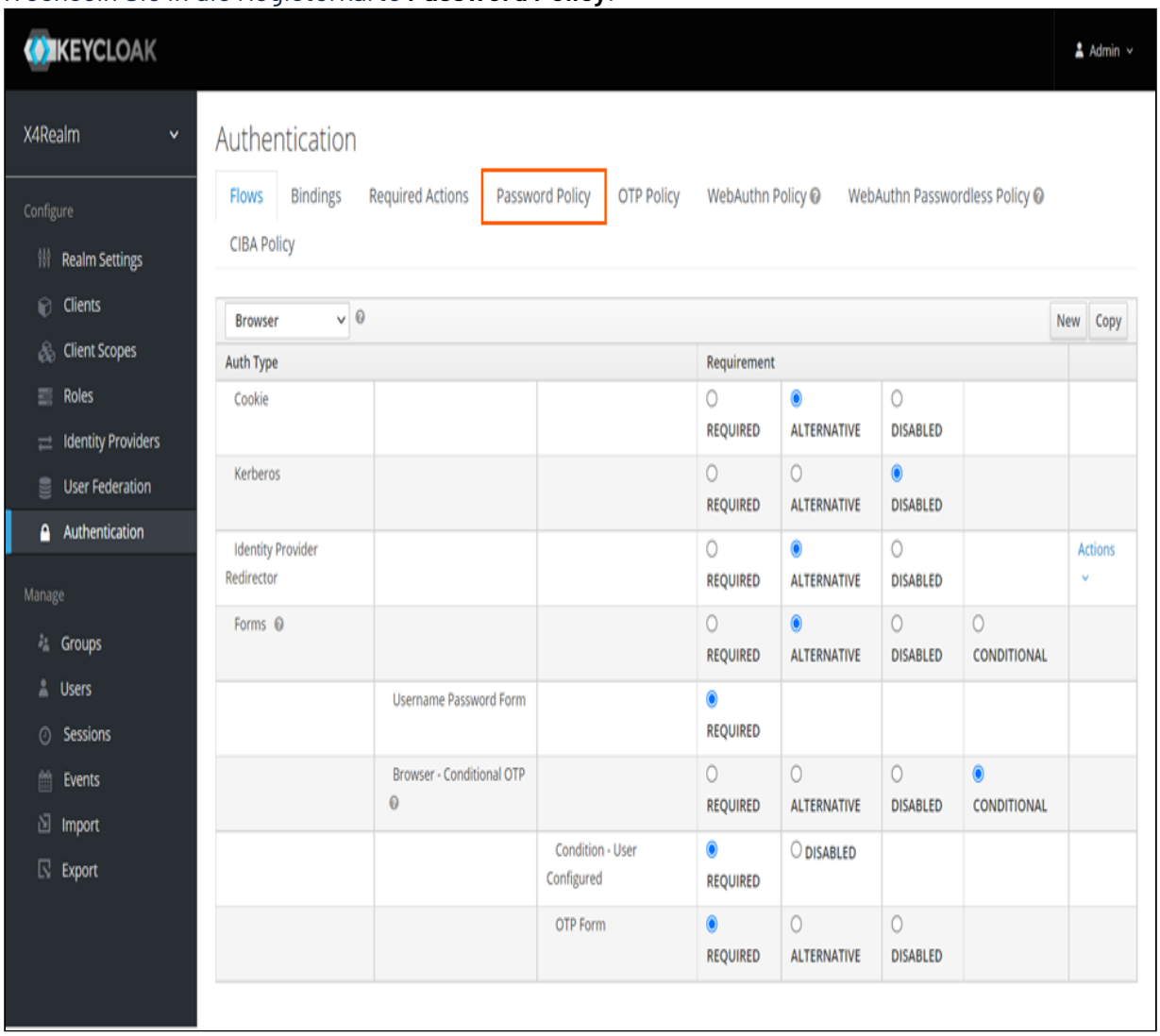
In Keycloak können Sie verschiedene Passwortrichtlinien festlegen.

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

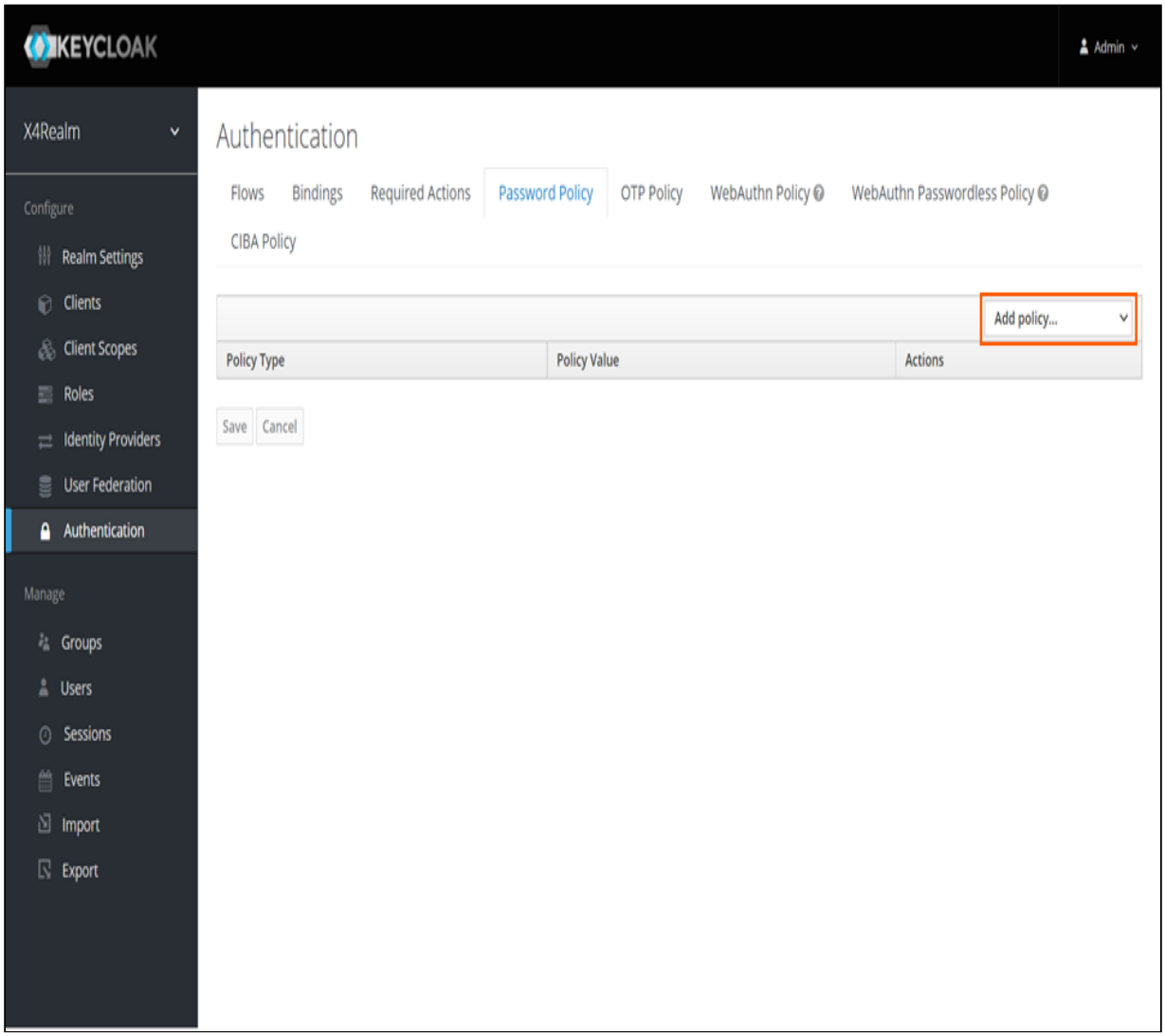
2. Klicken Sie im Bereich **Configure** auf **Authentication**.



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



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.

5.4.11 Themes

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

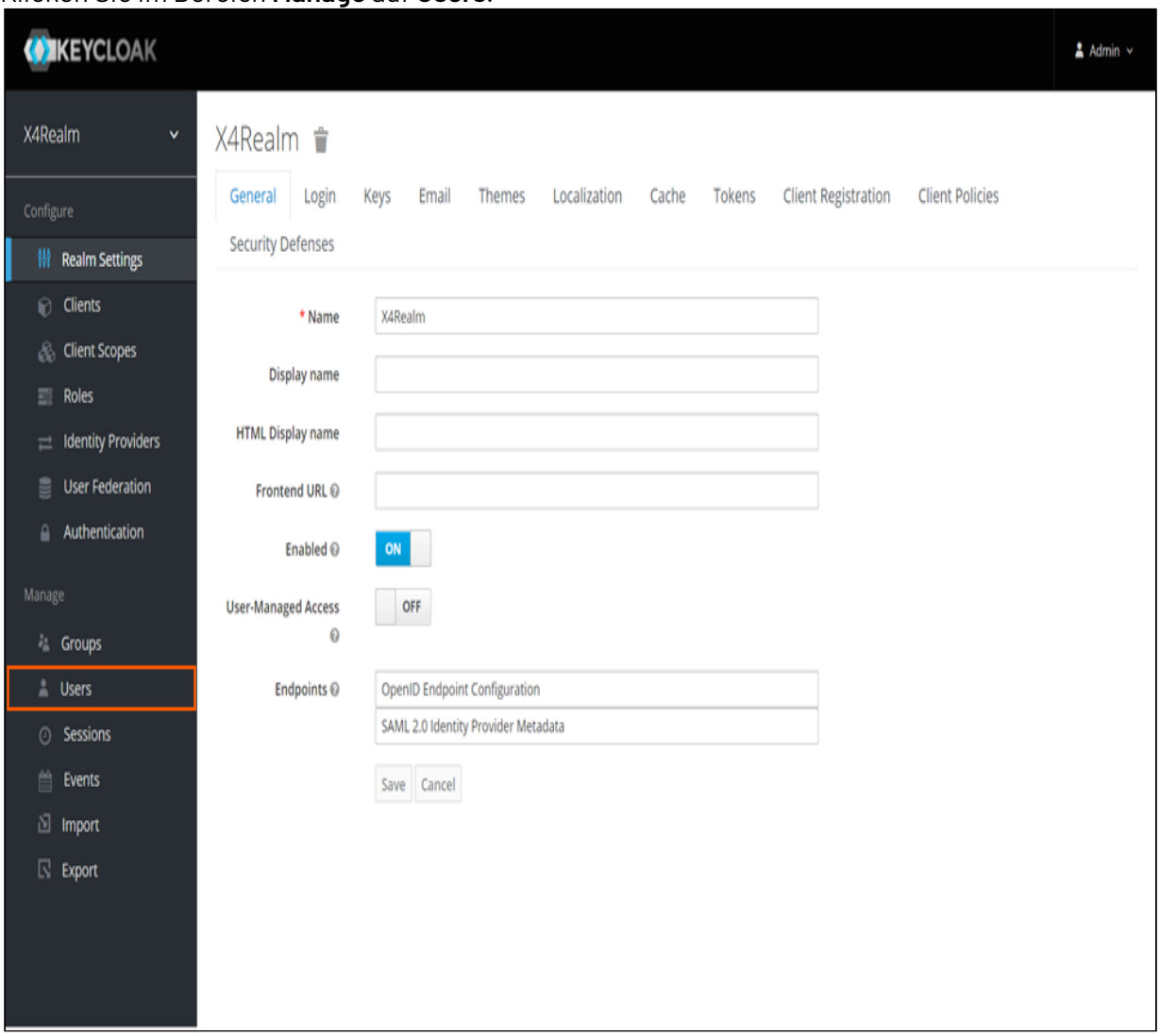
> Weitere Informationen finden Sie unter https://www.keycloak.org/docs/latest/server_admin/#_themes.

5.5 Benutzer

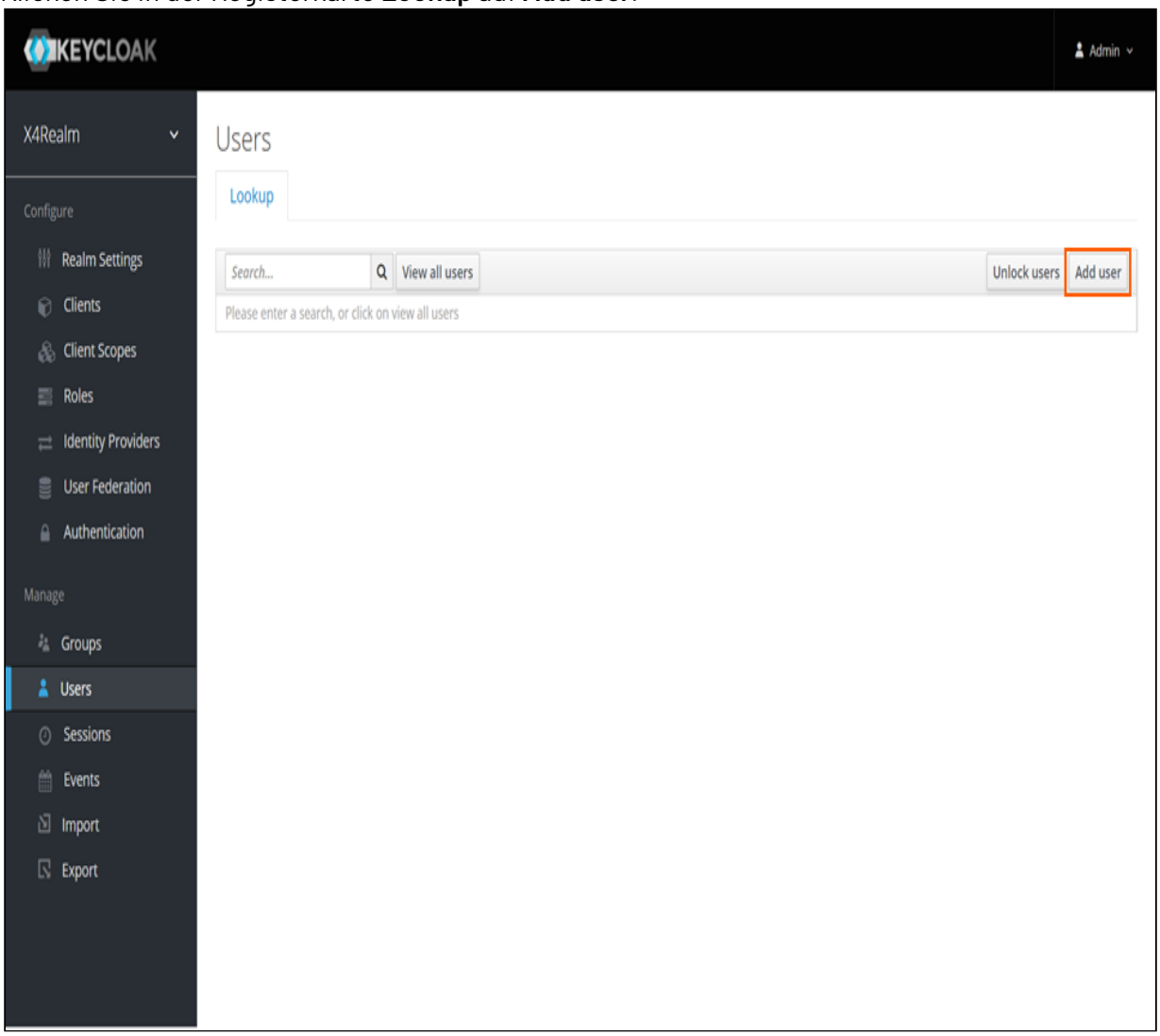
5.5.1 Benutzer erstellen

> ⚠ 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**.

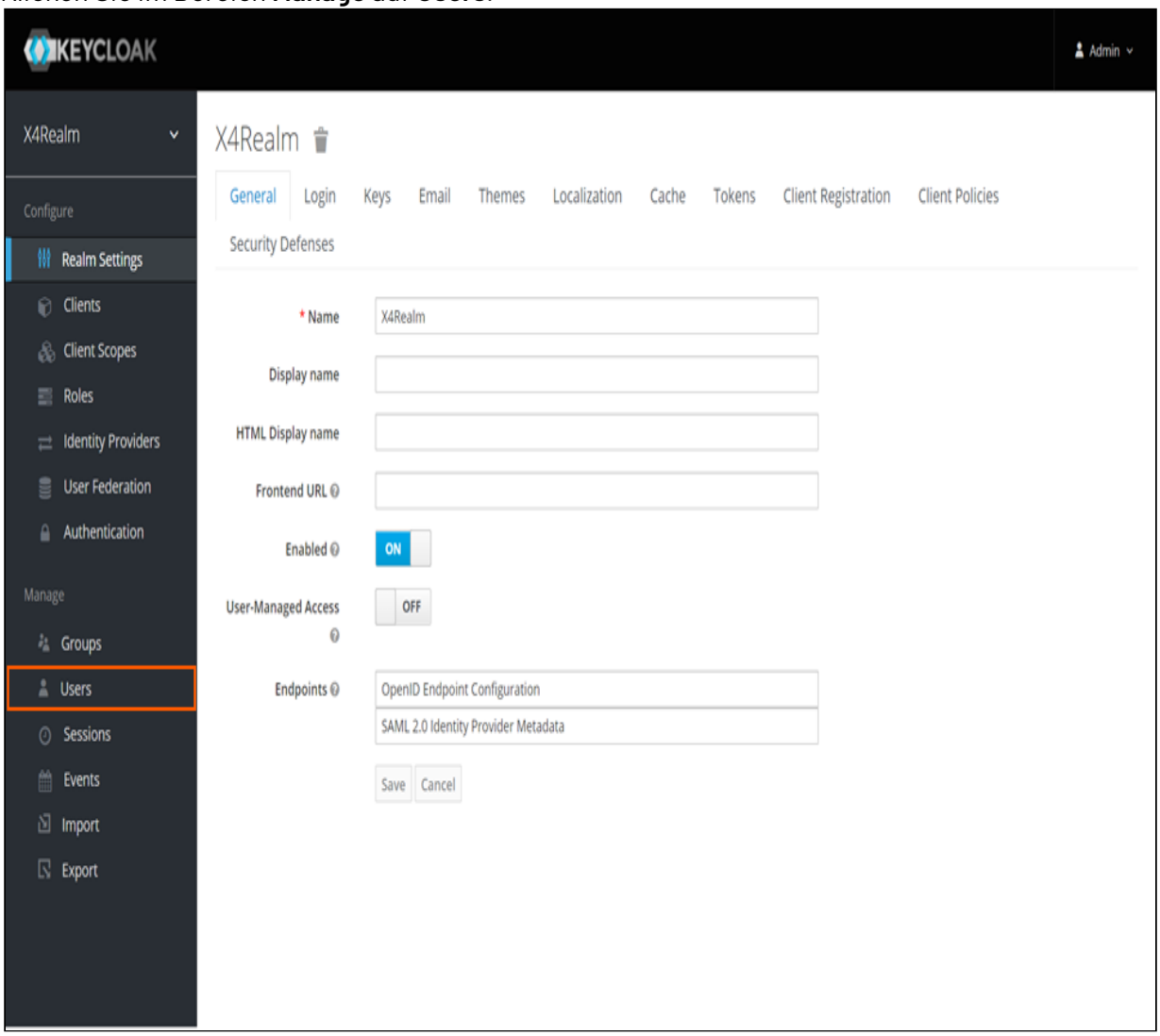


4. Tragen Sie die relevanten Daten ein.
5. Klicken Sie auf **Save**.

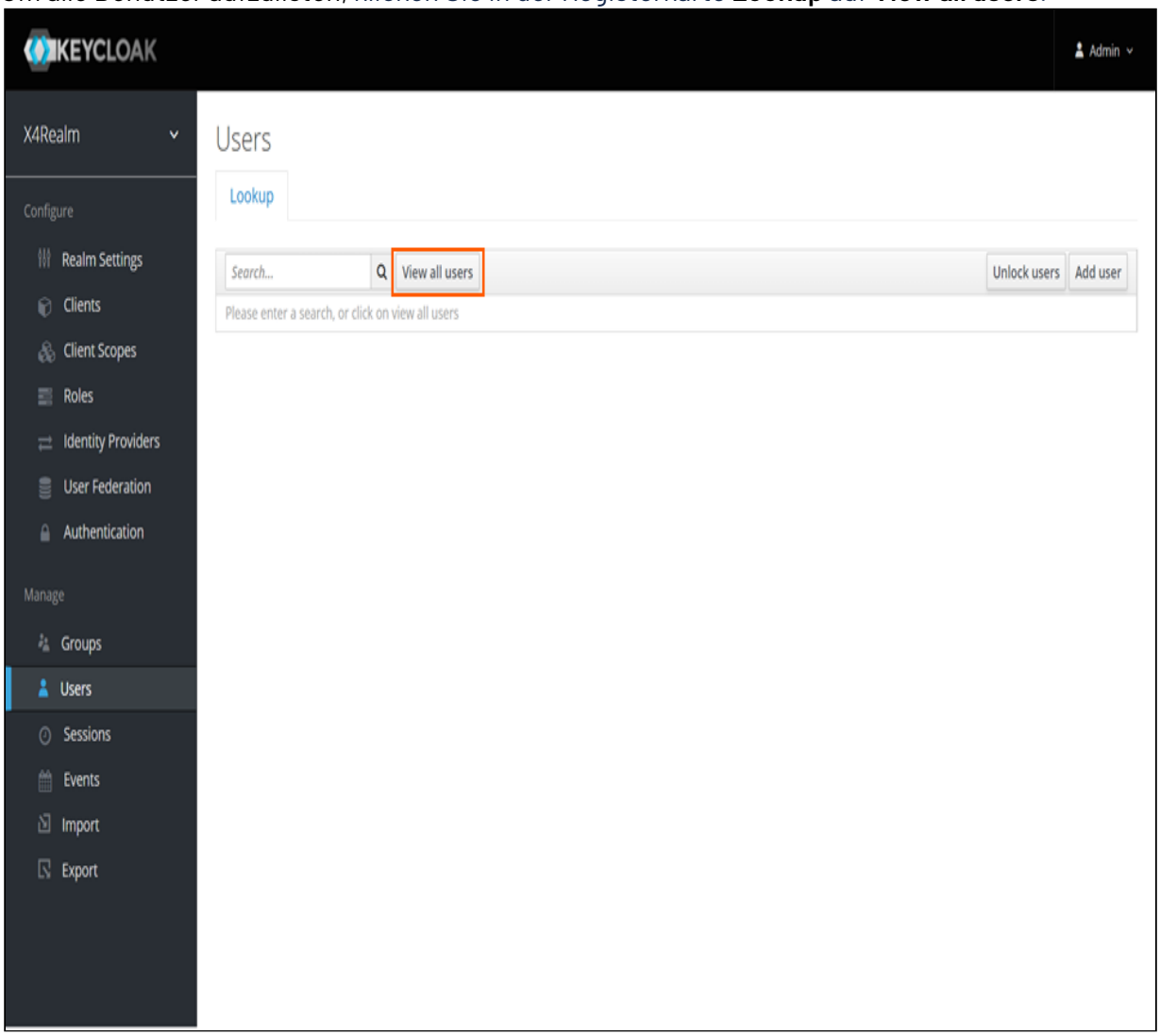
5.5.2 Benutzer eine Rolle zuweisen

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

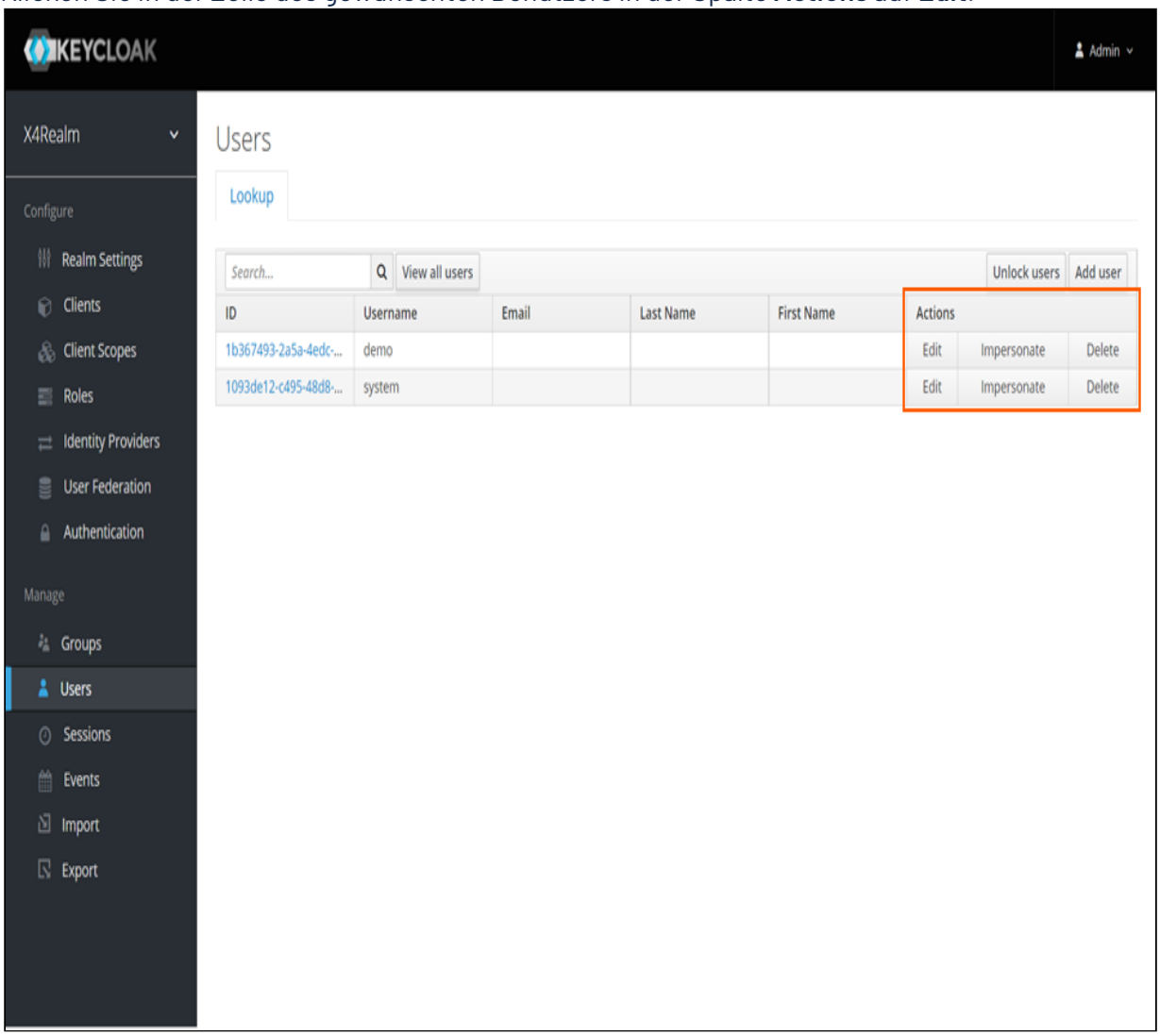
2. Klicken Sie im Bereich **Manage** auf **Users**.



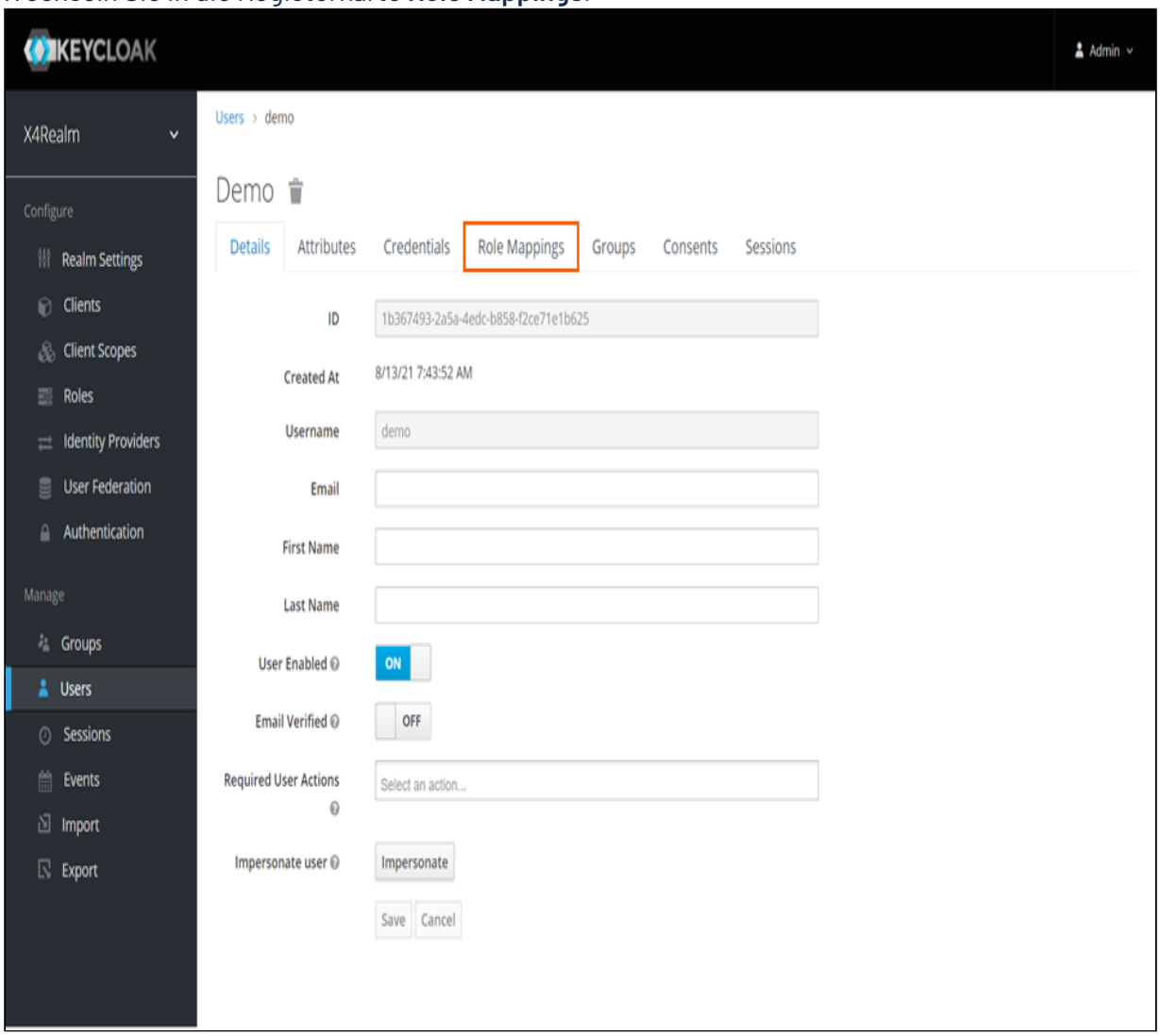
3. Um alle Benutzer aufzulisten, klicken Sie in der Registerkarte **Lookup** auf **View all users**.



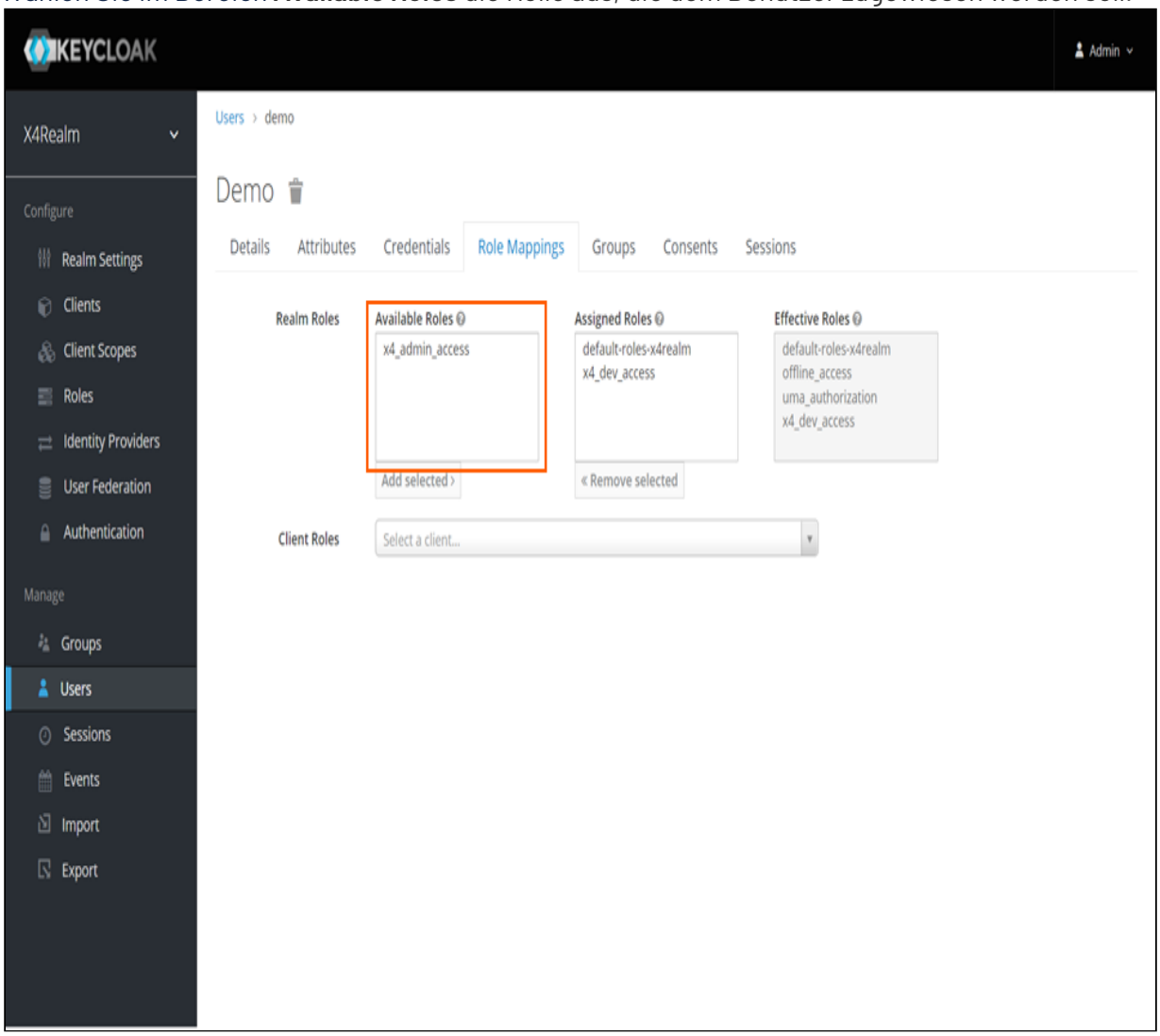
4. Klicken Sie in der Zeile des gewünschten Benutzers in der Spalte **Actions** auf **Edit**.



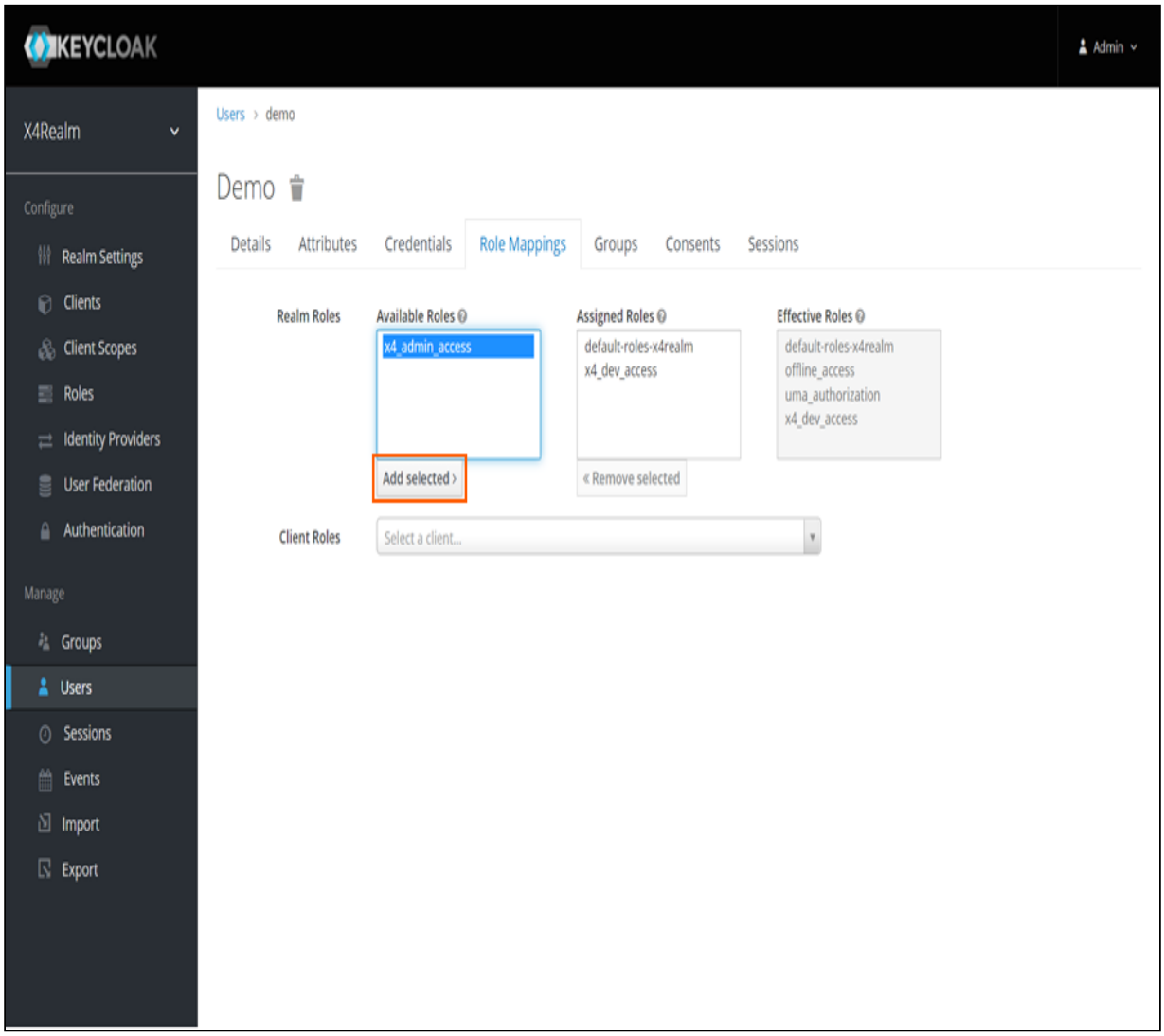
5. Wechseln Sie in die Registerkarte **Role Mappings**.



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



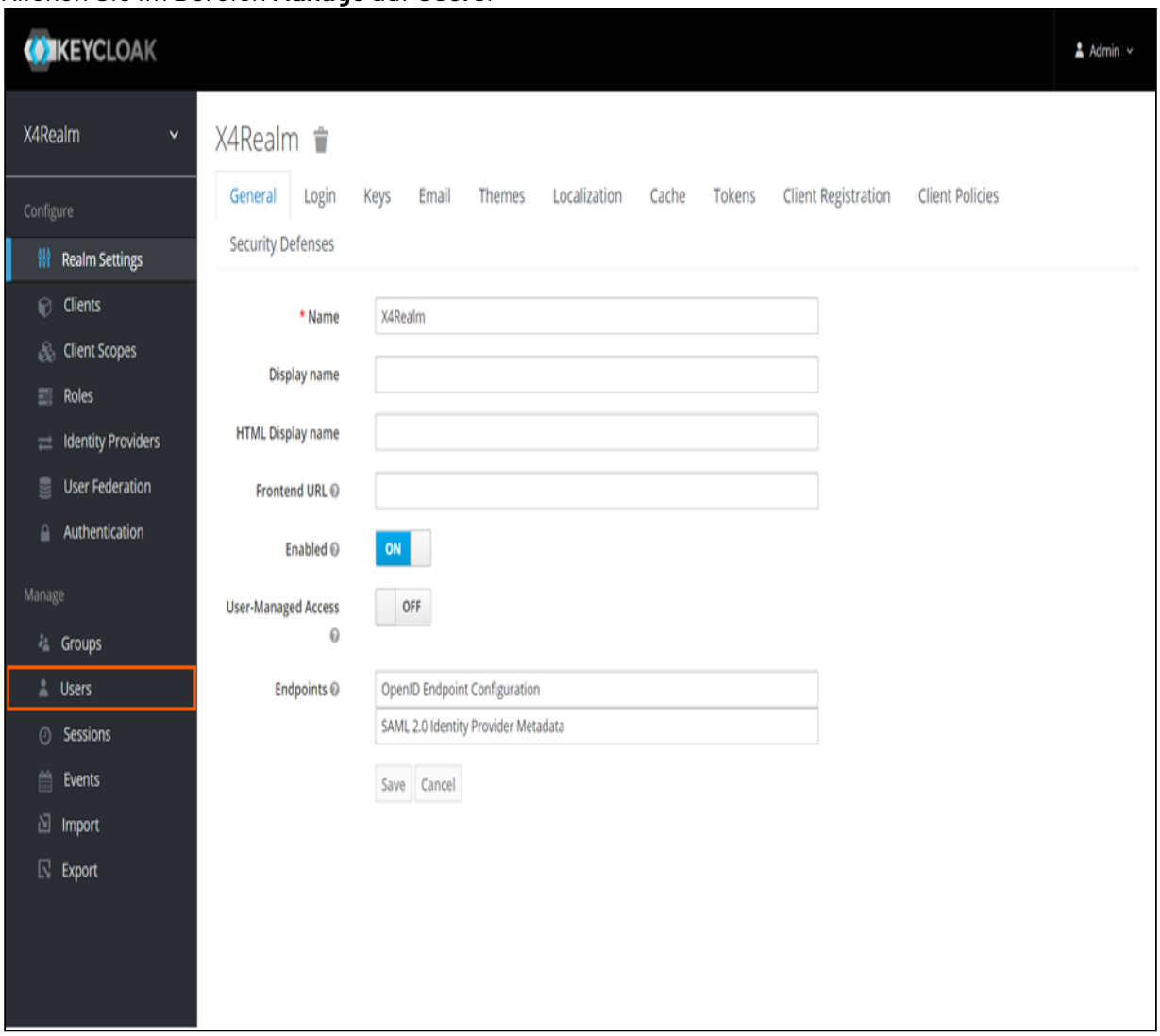
7. Klicken Sie auf **Add selected**.



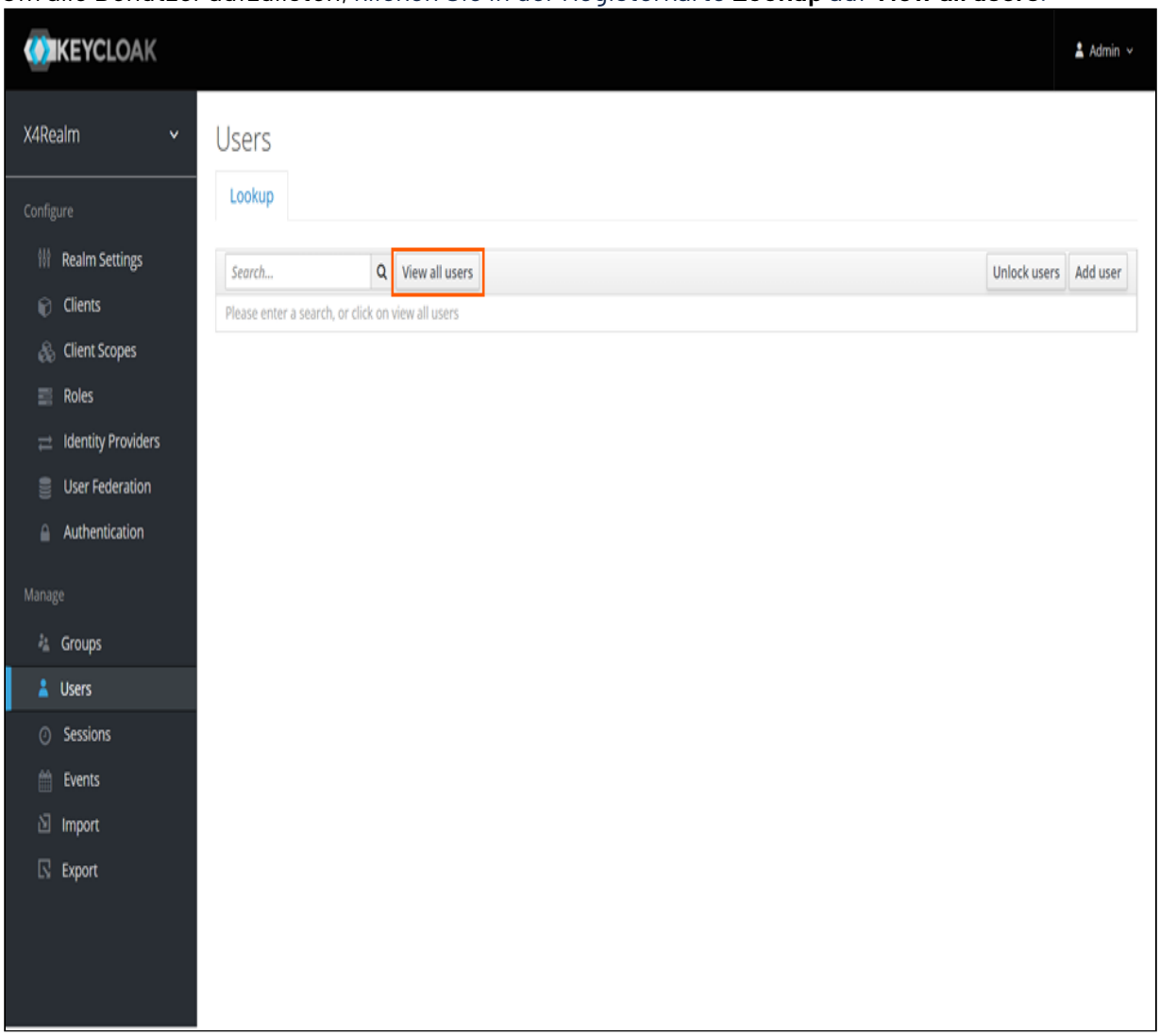
5.5.3 Benutzer eine Gruppe zuweisen

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

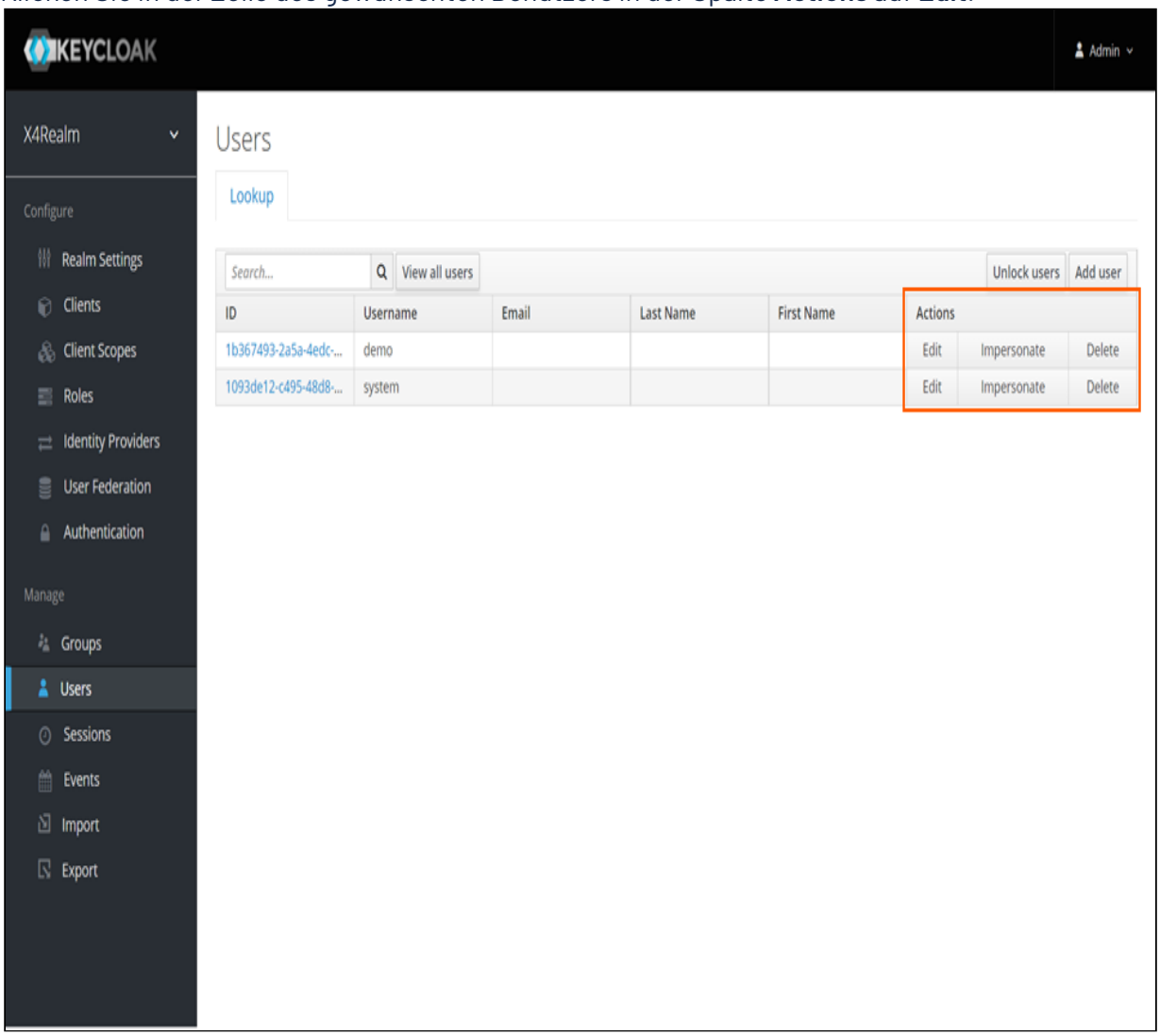
2. Klicken Sie im Bereich **Manage** auf **Users**.



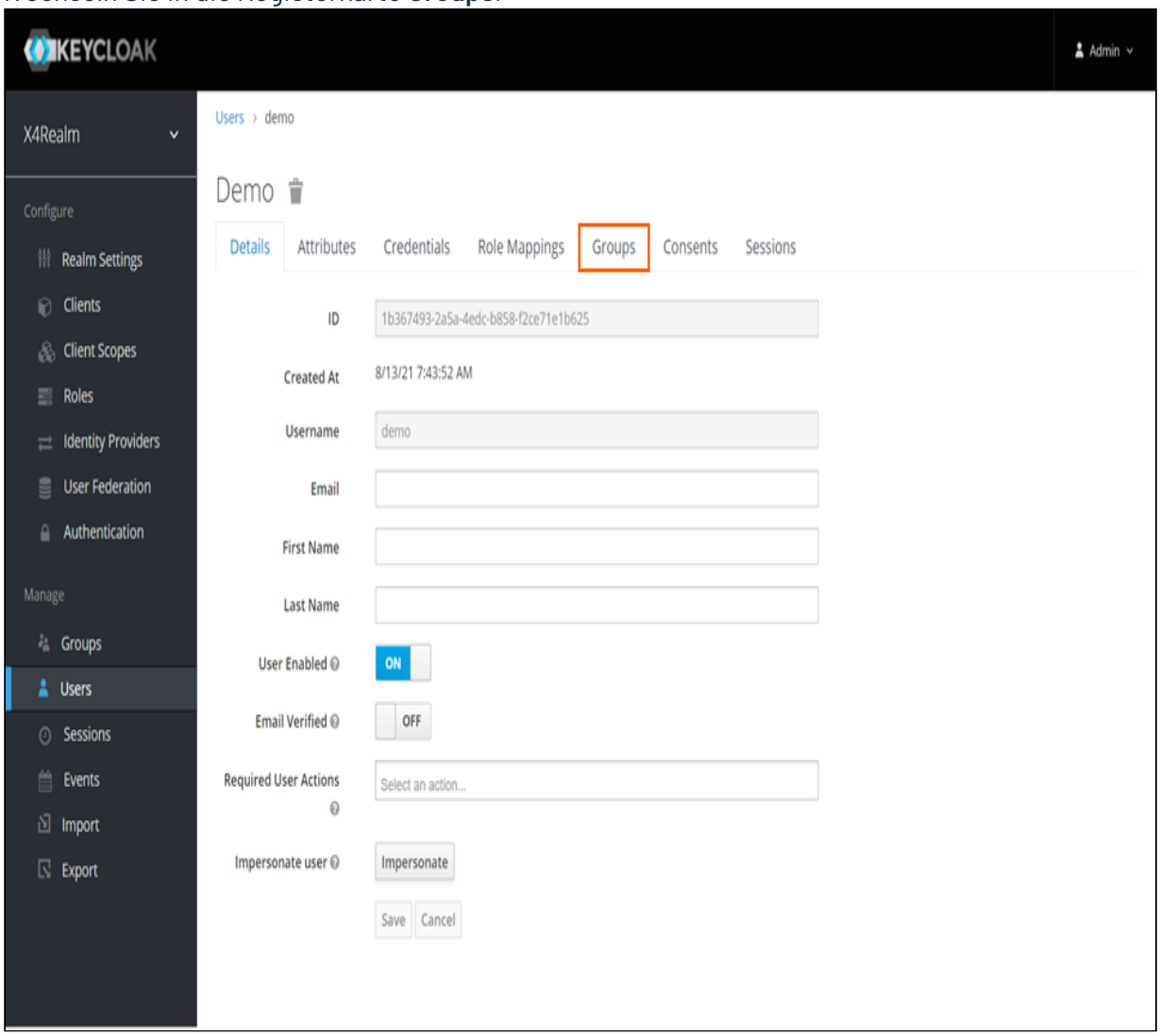
3. Um alle Benutzer aufzulisten, klicken Sie in der Registerkarte **Lookup** auf **View all users**.



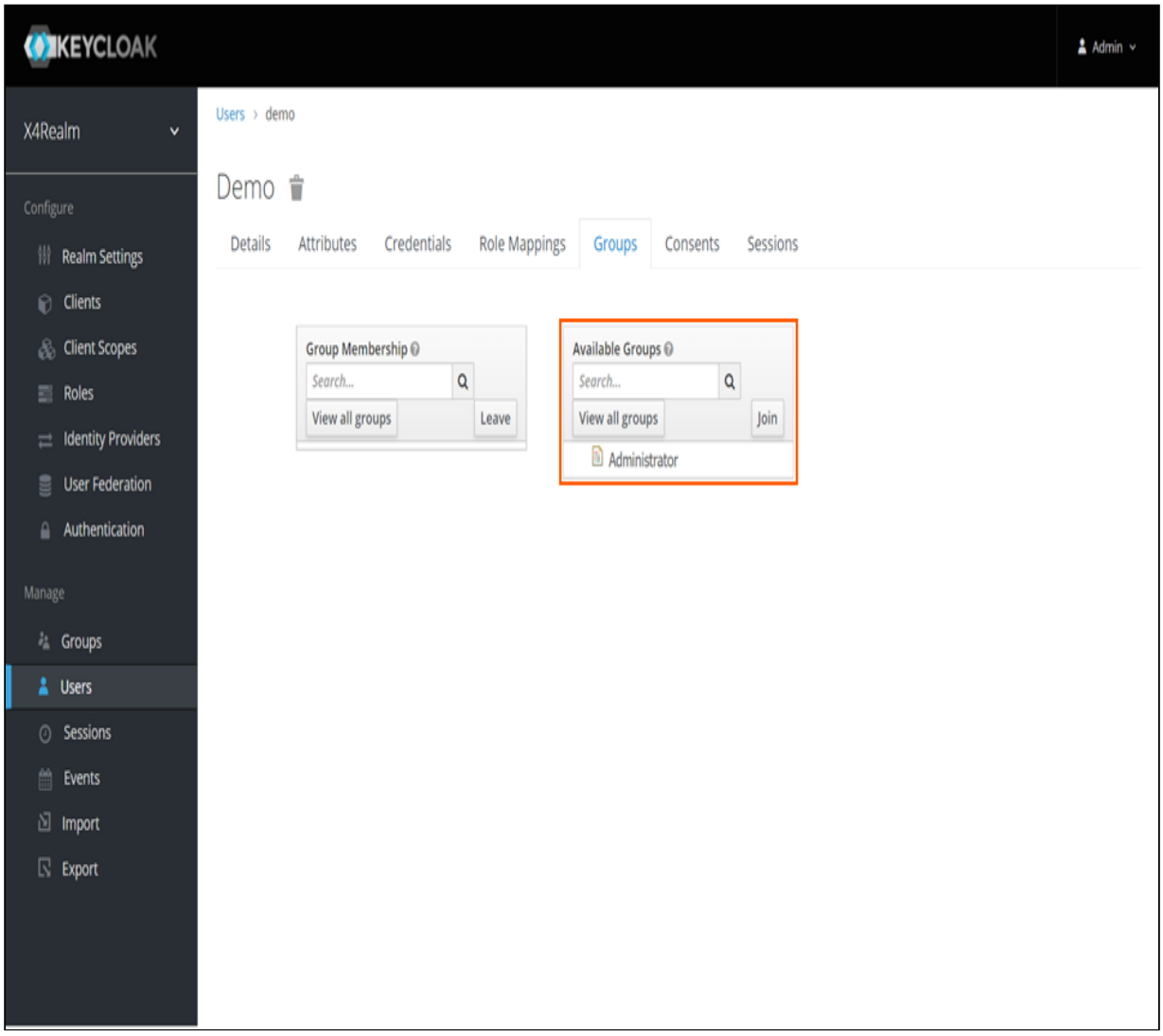
4. Klicken Sie in der Zeile des gewünschten Benutzers in der Spalte **Actions** auf **Edit**.



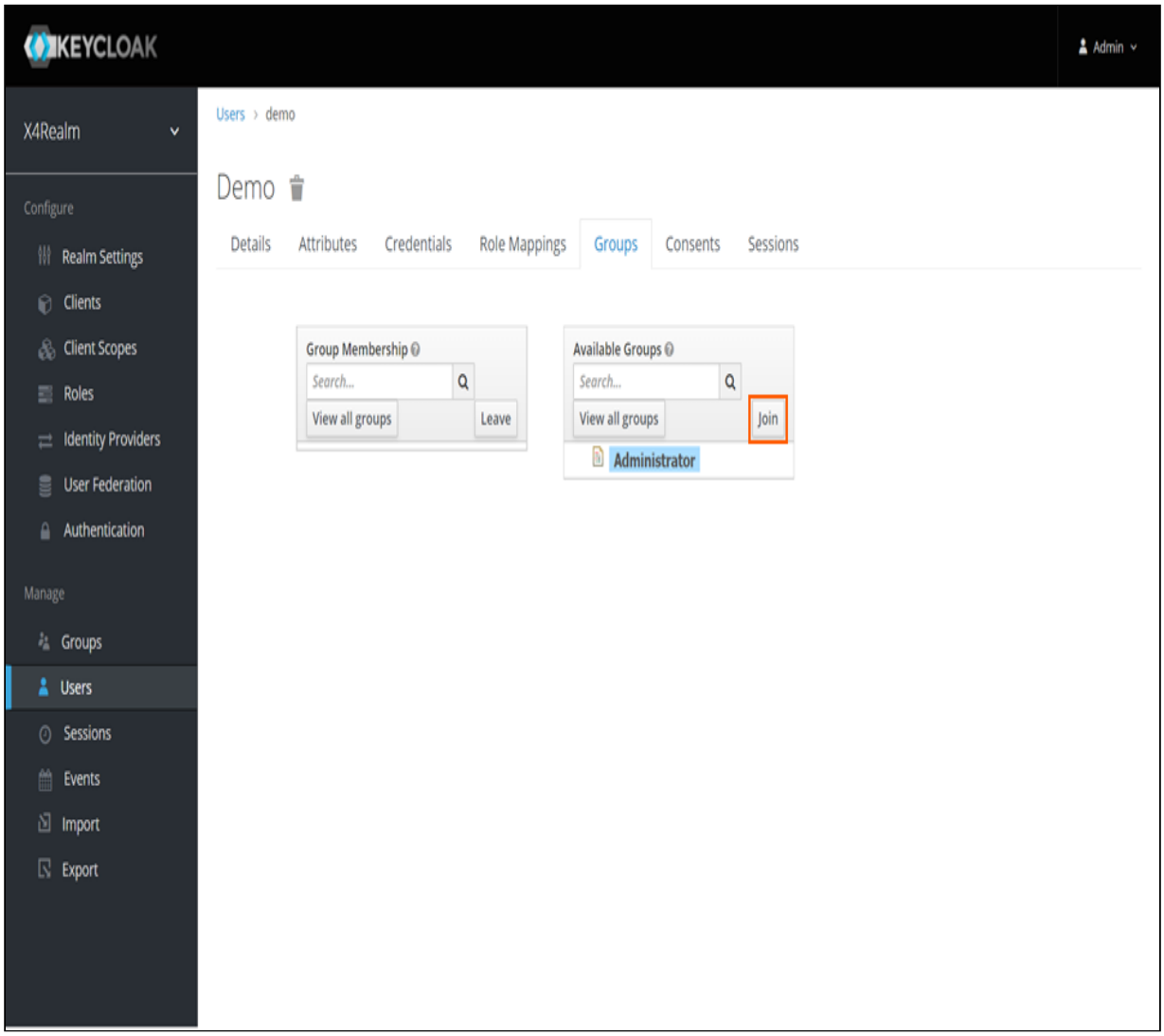
5. Wechseln Sie in die Registerkarte **Groups**.



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


KEYCLOAK
Admin
X4Realm
Configure
Realm Settings
Clients
Client Scopes
Roles
Identity Providers
User Federation
Authentication
Manage
Groups
Users
Sessions
Events
Import
Export
Users › demo
Demo
Details
Attributes
Credentials
Role Mappings
Groups
Consents
Sessions
Group Membership
Search...
View all groups
Leave
Available Groups
Search...
View all groups
Join
Administrator

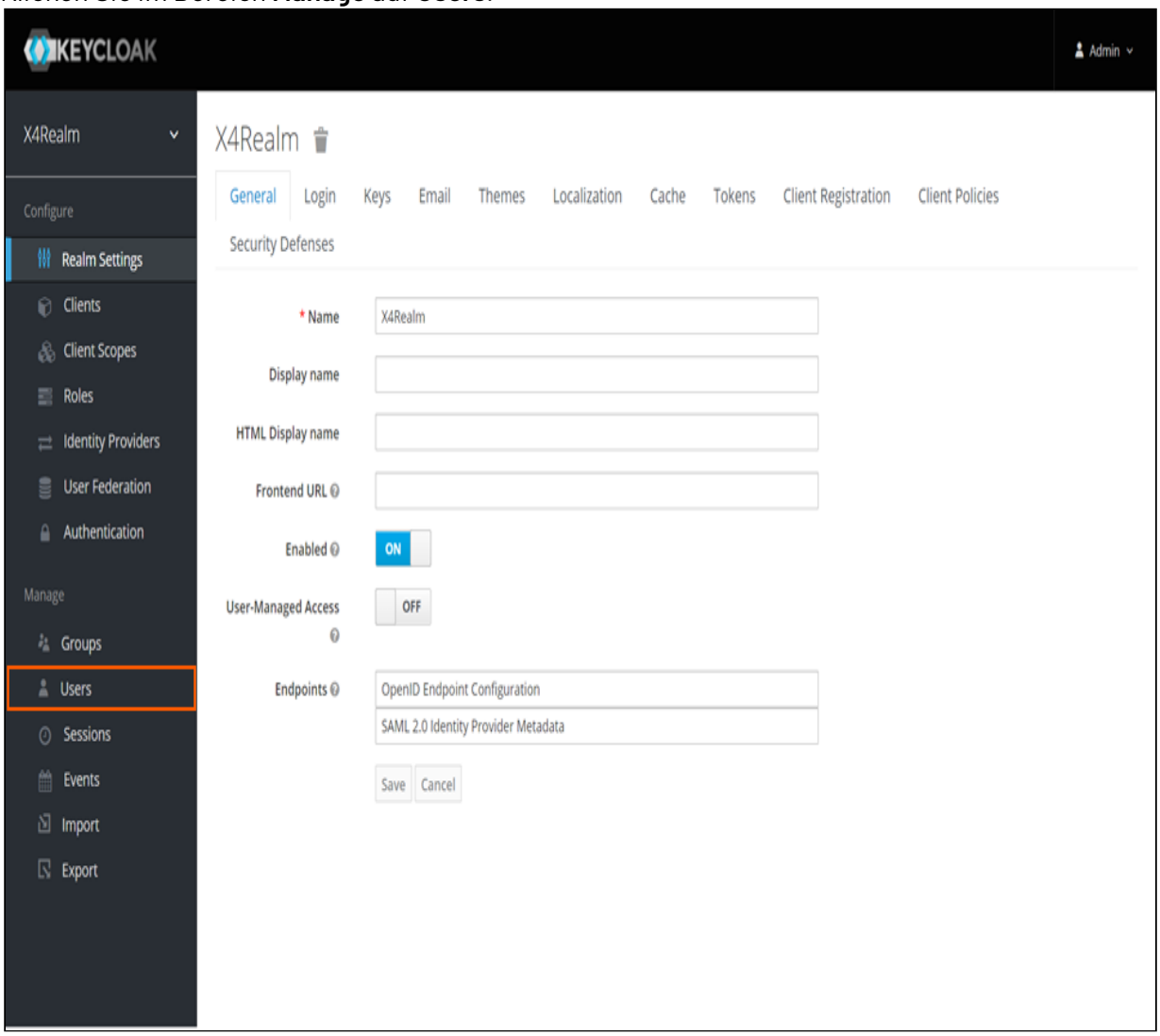
7. Klicken Sie auf **Join**.



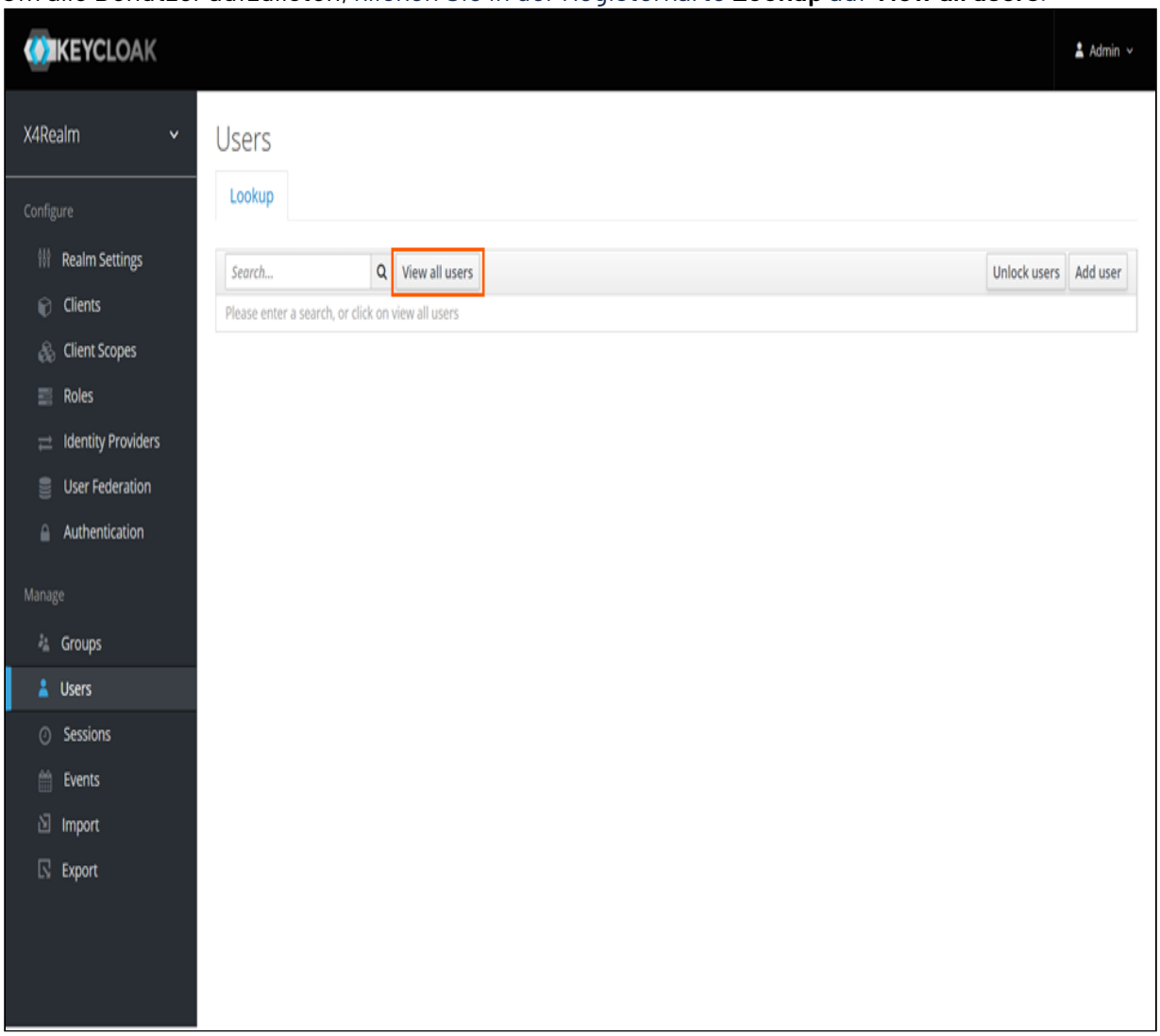
5.5.4 Benutzer aus einer Gruppe entfernen

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

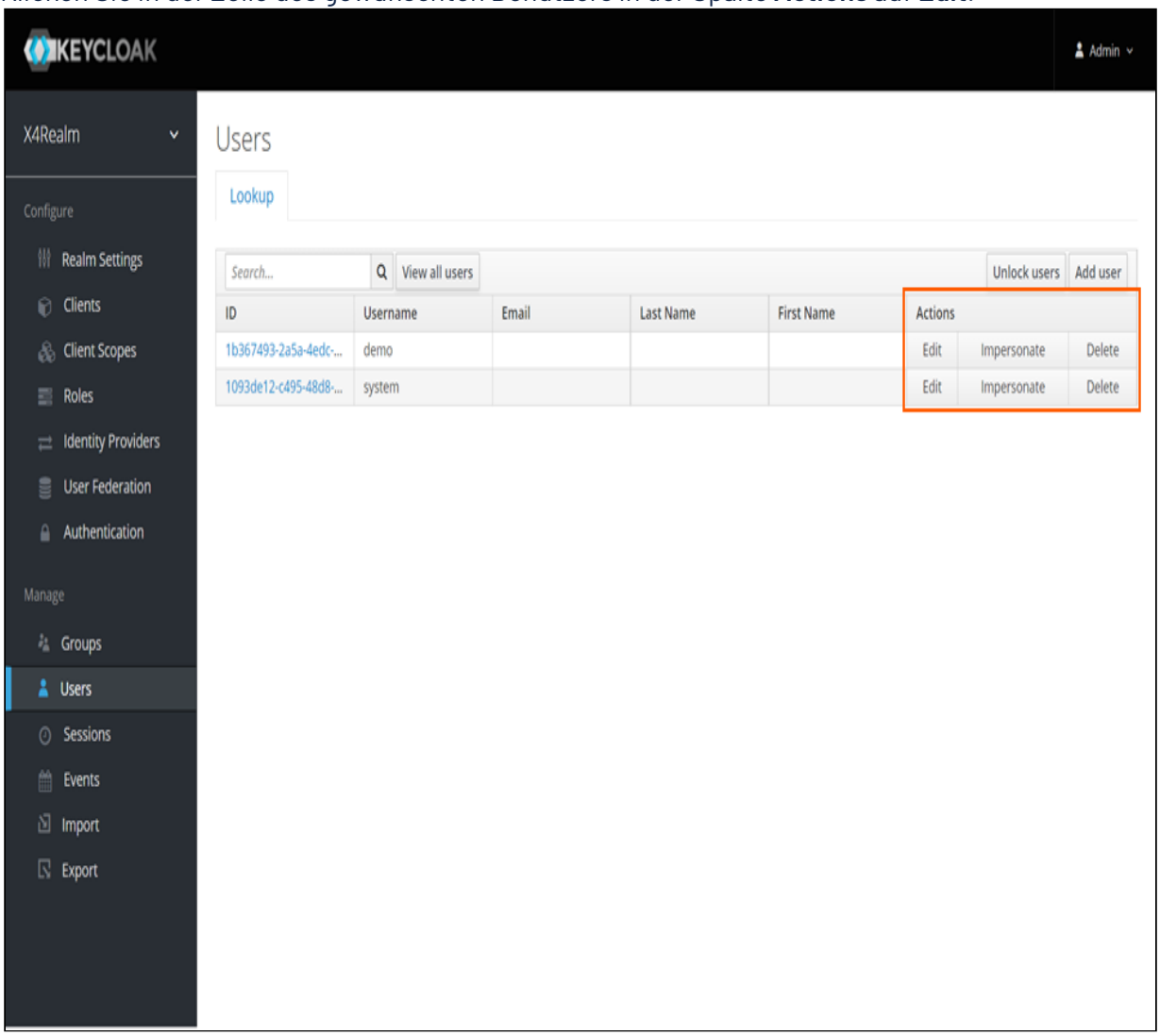
2. Klicken Sie im Bereich **Manage** auf **Users**.



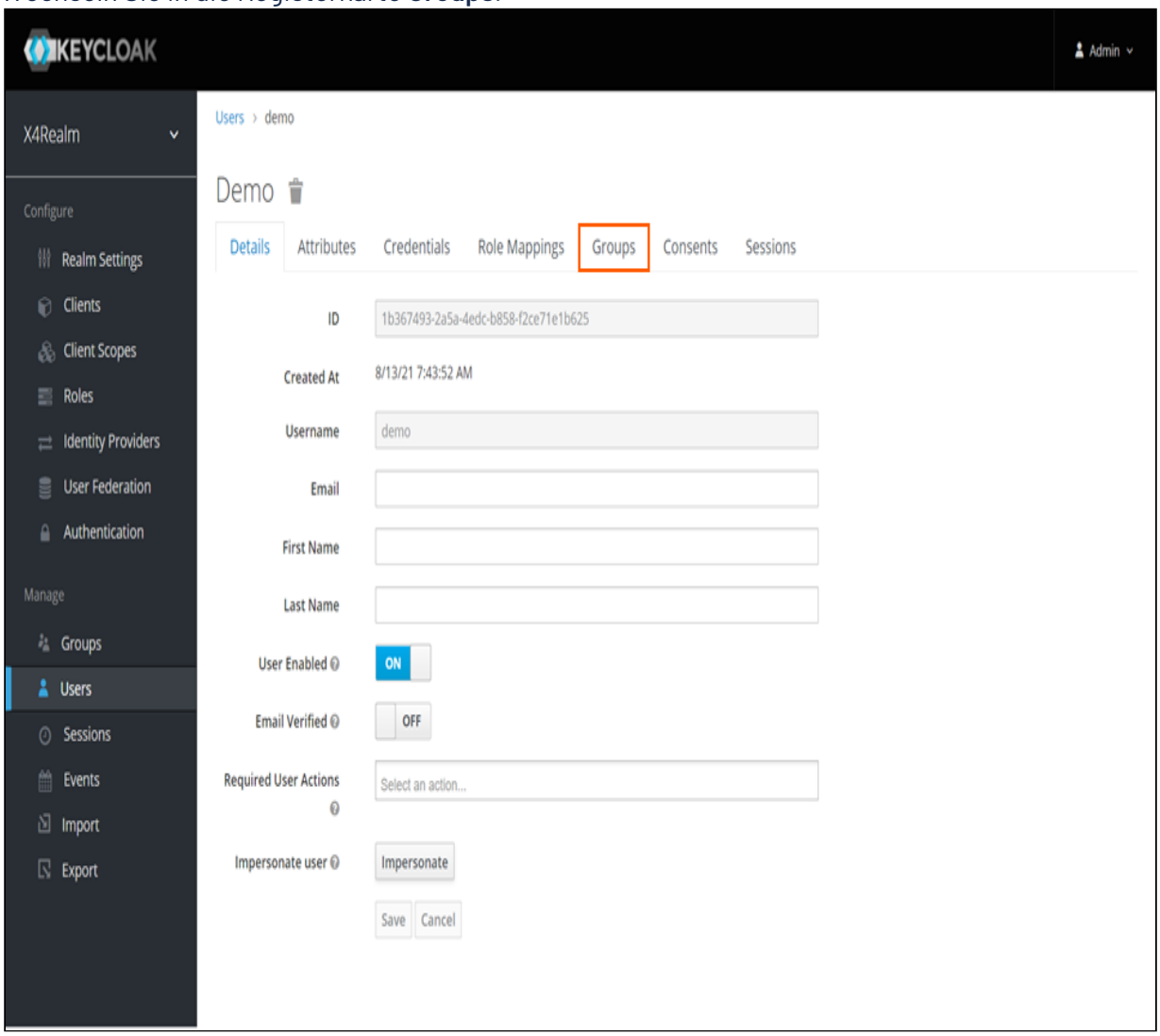
3. Um alle Benutzer aufzulisten, klicken Sie in der Registerkarte **Lookup** auf **View all users**.



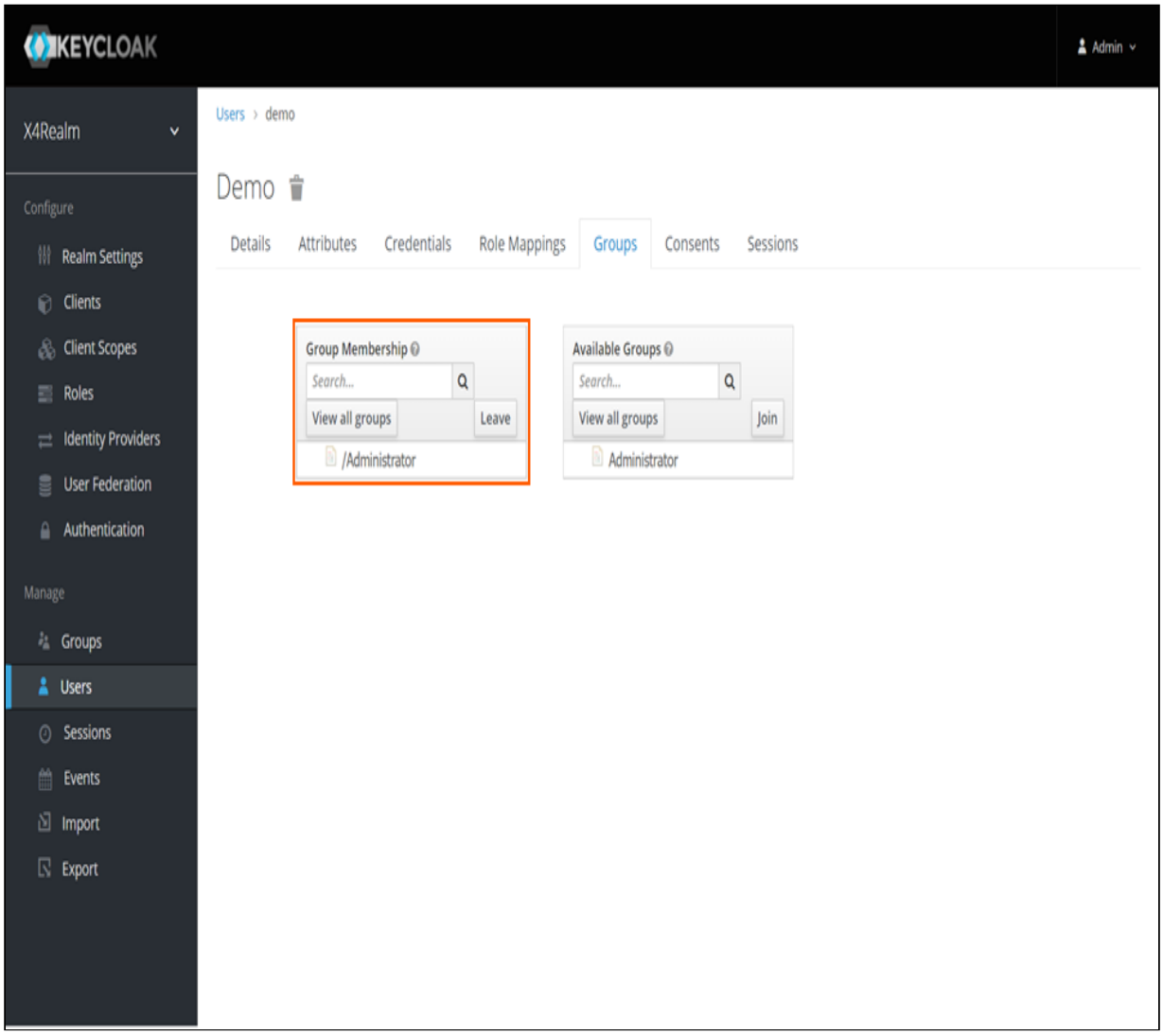
4. Klicken Sie in der Zeile des gewünschten Benutzers in der Spalte **Actions** auf **Edit**.



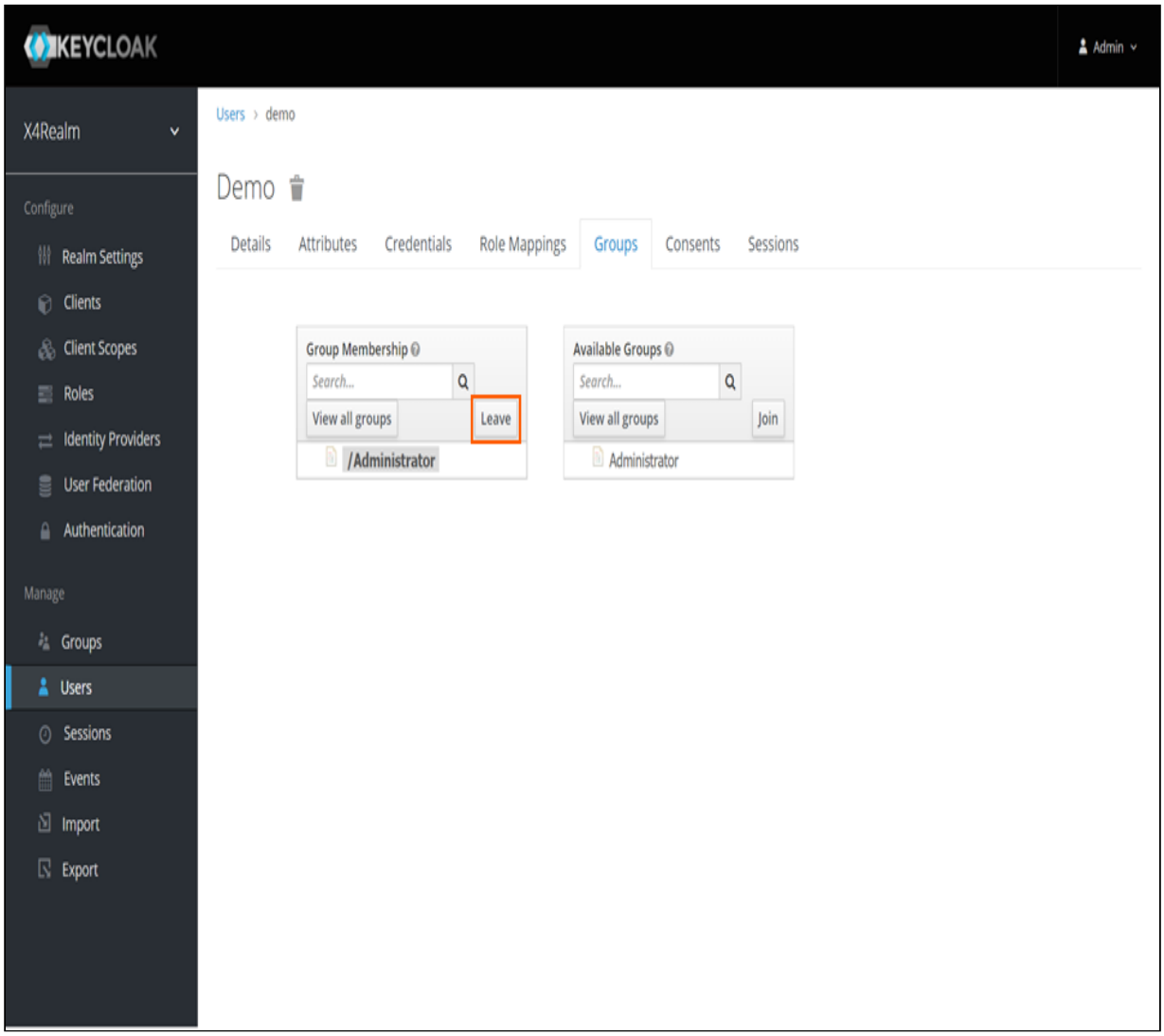
5. Wechseln Sie in die Registerkarte **Groups**.



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


KEYCLOAK
Admin
X4Realm
Configure
Realm Settings
Clients
Client Scopes
Roles
Identity Providers
User Federation
Authentication
Manage
Groups
Users
Sessions
Events
Import
Export
Users › demo
Demo
Details
Attributes
Credentials
Role Mappings
Groups
Consents
Sessions
Group Membership
Search...
View all groups
Leave
/Administrator
Available Groups
Search...
View all groups
Join
Administrator

7. Klicken Sie auf **Leave**.



5.6 Rollen

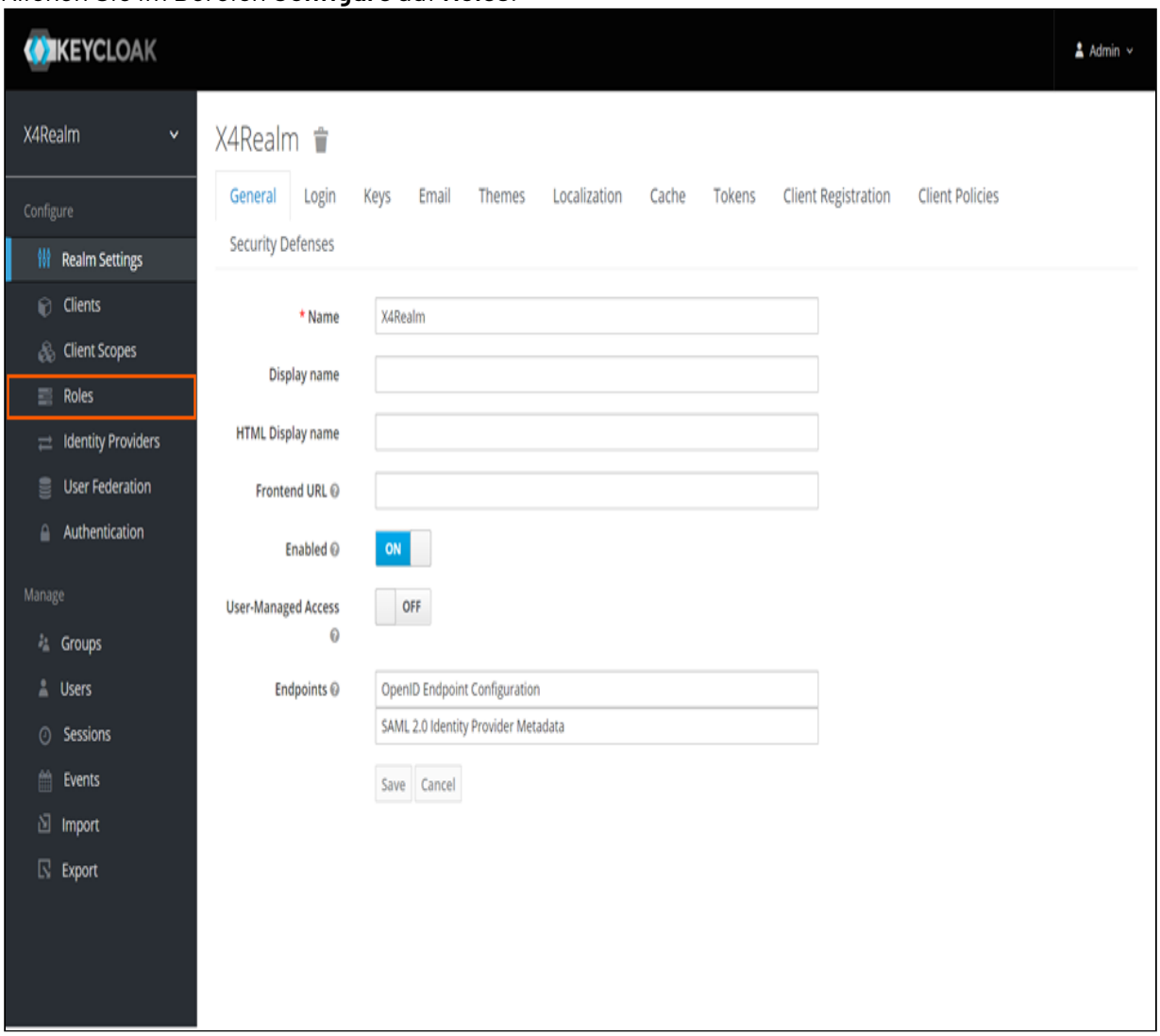
Rollen sind im Wesentlichen ein Namensraum, der einem Client zugeordnet ist. Jeder Client erhält seinen eigenen Namensraum.

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

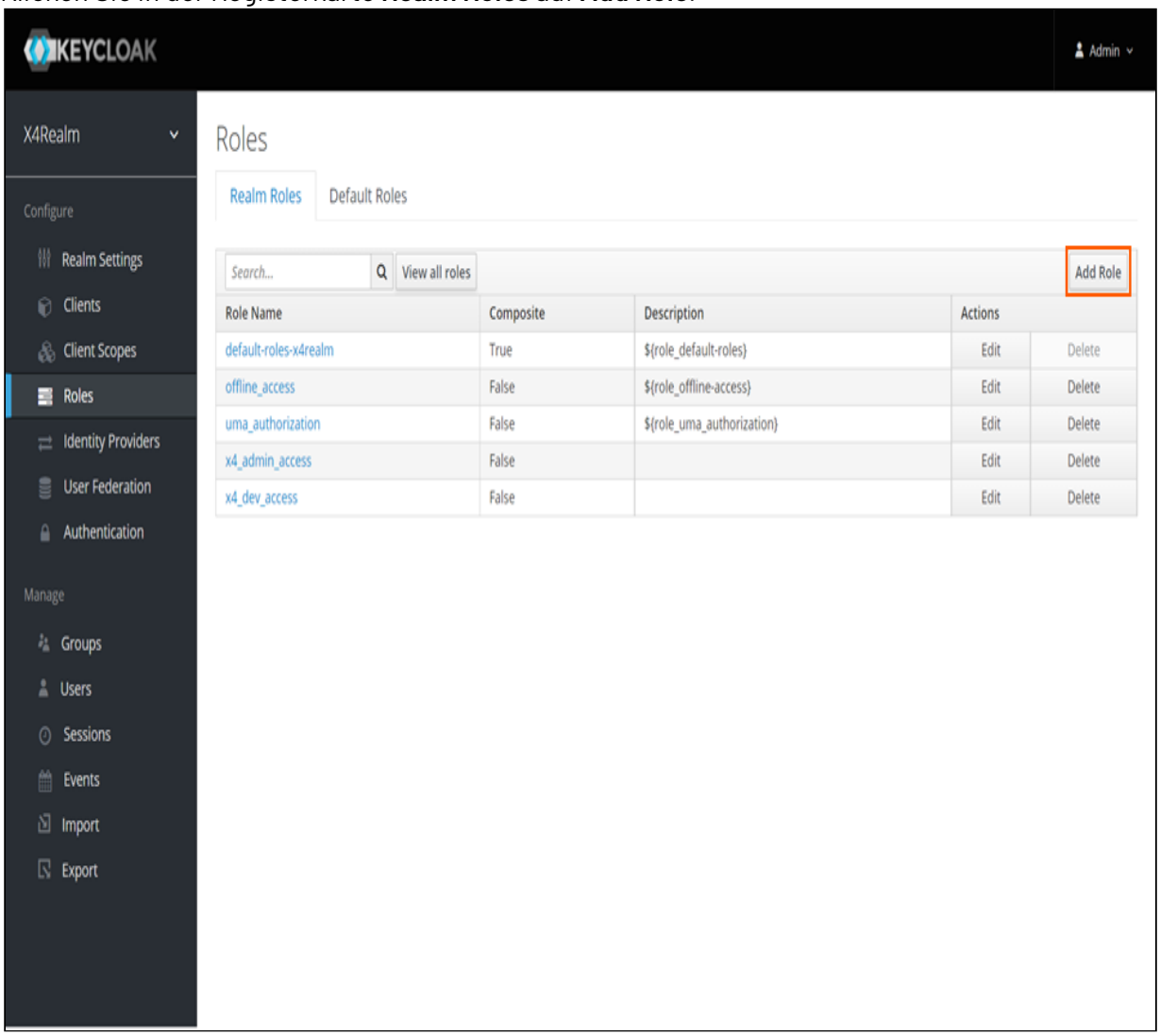
5.6.1 Rolle erstellen

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

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



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**.

5.7 Gruppen

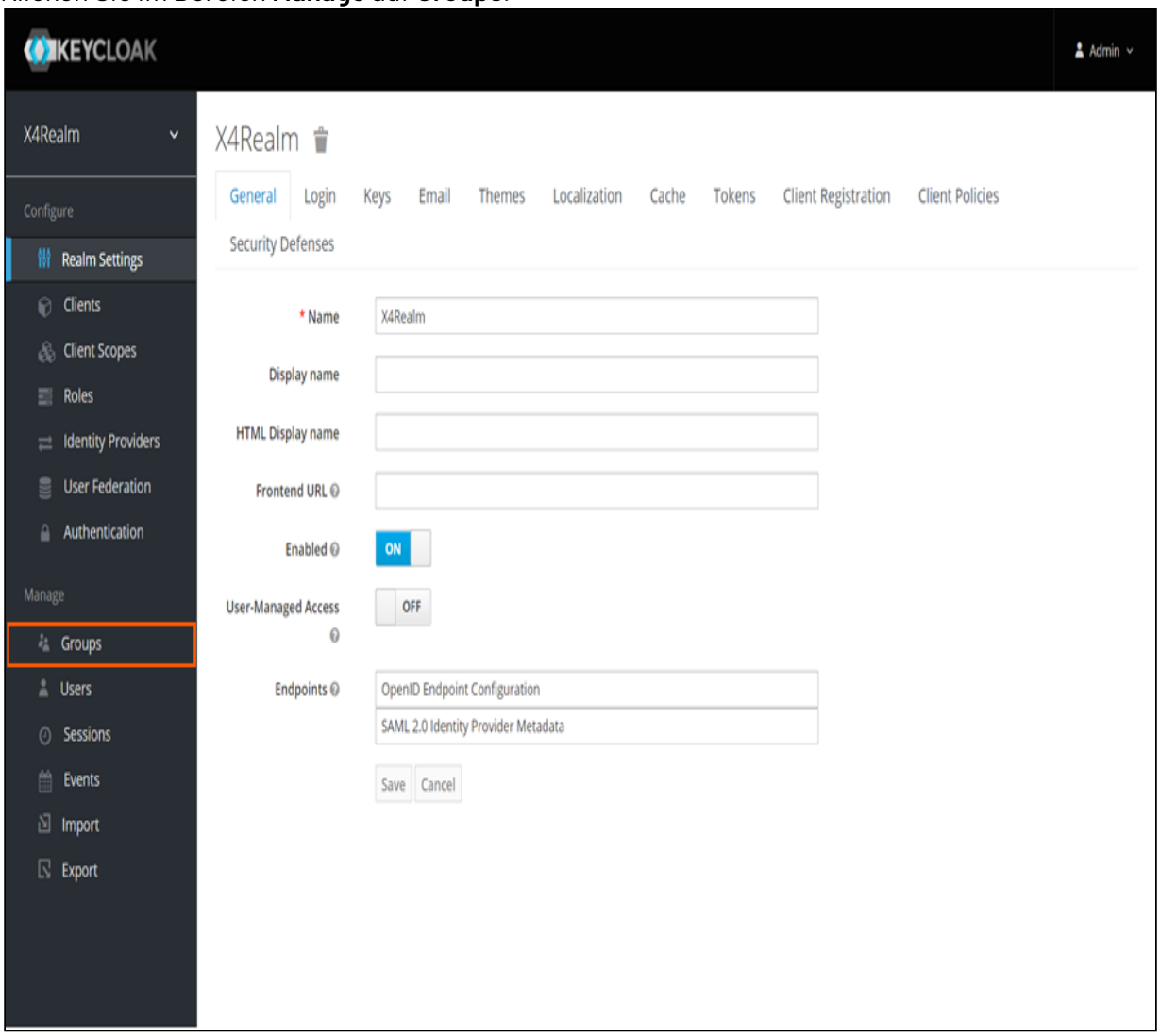
Gruppen in Keycloak ermöglichen es Ihnen, einen gemeinsamen Datensatz von Attributen und Rollenzuordnungen für eine Gruppe von Benutzern zu verwalten. Benutzer können Mitglied von keiner oder mehreren Gruppen sein. Die Benutzer erben die Attribute und Rollenzuordnungen, die der jeweiligen Gruppe zugeordnet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

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

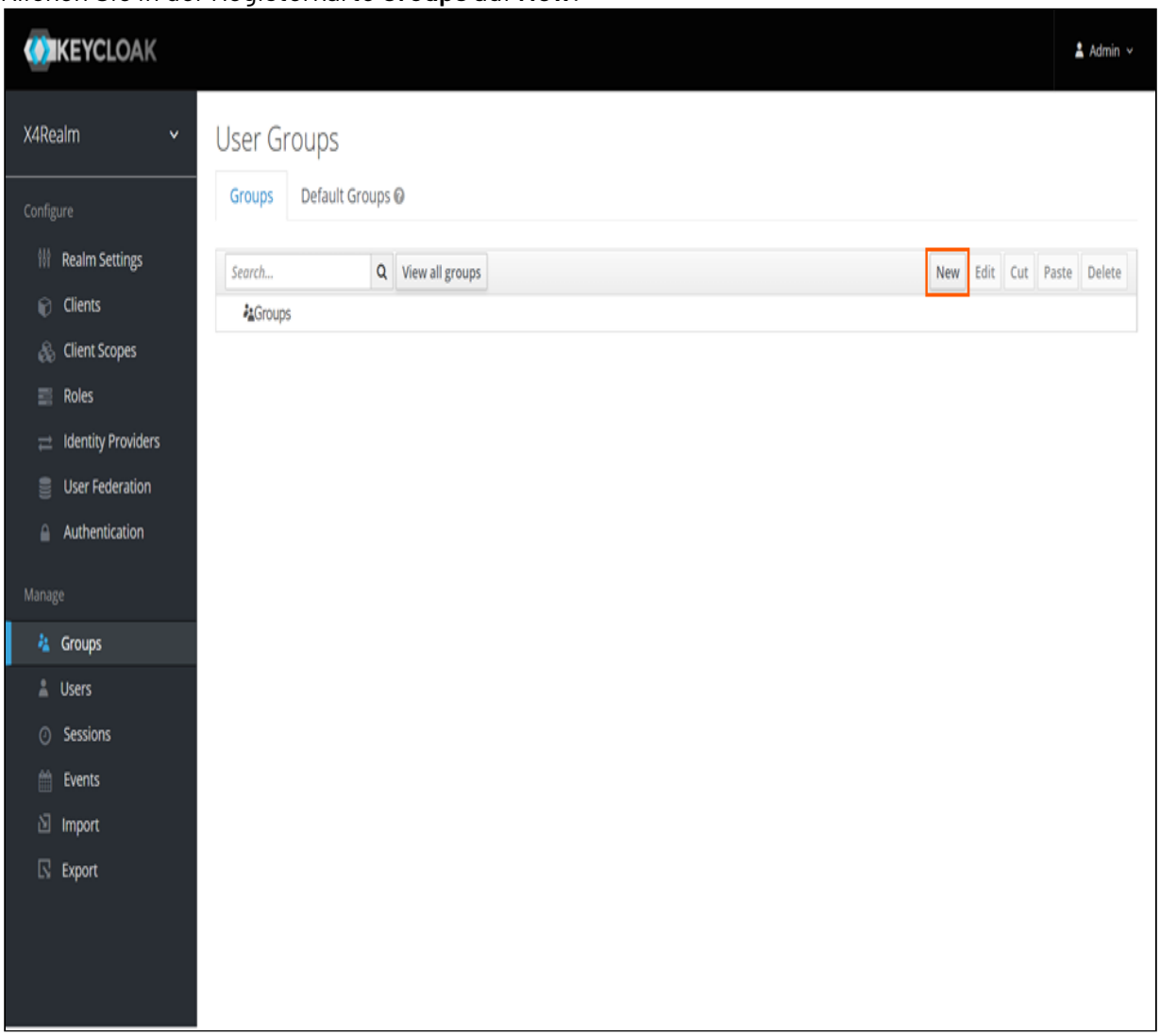
5.7.1 Gruppe erstellen

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

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



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

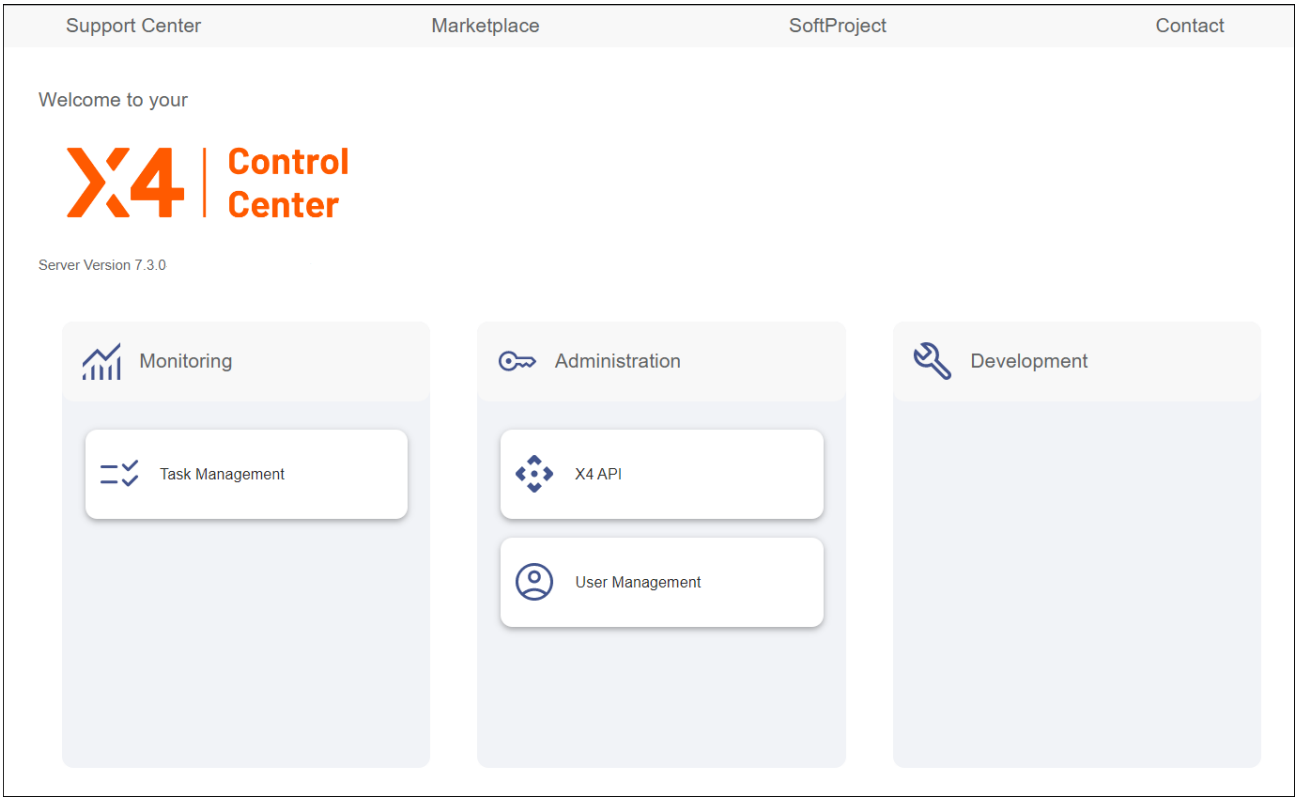


4. Geben Sie im Textfeld **Name** einen Namen ein.
5. Klicken Sie auf **Save**.

6 X4 Control Center

Das X4 Control Center ist ein Dashboard mit einem Überblick über die systemeigenen X4 Web Apps. Si e können das X4 Control Center über die URL http://localhost:8080/ aufrufen.

Folgende Startseite wird angezeigt:



Am oberen Rand befinden sich vier Schaltflächen:

Support Center	Über diese Schaltfläche können Sie auf das Support Center von Soft Project zugreifen, sofern Sie über einen Zugang verfügen. **Hinweis:** Bestandskunden, die noch keinen Zugang haben, können unter support@softproject.de einen Zugang beantragen.
Marketplace	Über diese Schaltfläche können Sie auf den SoftProject Marketplace zugreifen.
SoftProject	Über diese Schaltfläche gelangen Sie zur SoftProject-Website, auf der Sie ausführliche Informationen rund um die X4 BPMS finden.
Contact	Über diese Schaltfläche können Sie sich mit einem SoftProject-Ansprechpartner in Verbindung setzen.

Das X4 Control Center besteht aus den Kacheln **Monitoring**, **Administration** und **Development** mit folgenden Inhalten:

Monitoring	Die *Task Management* Web App bietet eine Oberfläche zur Abarbeitung der definierten Aufgaben (Human Tasks), denen Menschen in Business Processes zugeordnet sind. Die *Task Management* Web App besitzt bereits eine vordefinierte Struktur und vordefinierte Funktionen. Innerhalb des entsprechenden Business Processes und über verschiedene Einstellungen im *Human Task Editor* lassen sich jedoch weitere Einstellungen vornehmen. Weitere Informationen zu dieser App finden Sie im X4 BPM-Handbuch im Kapitel Task Management Web App.
Administration	Diese Kachel enthält zwei Schaltflächen, über die Sie administrative Funktionen ausführen können: • Über die Schaltfläche **X4 API** können Sie im Swagger Editor (Swagger UI) auf die X4 ReST API zugreifen, mit der Sie auf X4 zugreifen und mit X4 arbeiten können. • Über die Schaltfläche **User Management** können Sie auf die Keycloak-Administrationskonsole (http://localhost:8085/auth) zugreifen. Hier können Sie Benutzer, Gruppen und Rollen verwalten. Weitere Informationen hierzu finden Sie im X4 Administrationshandbuch unter Keycloak.
Development	Diese Kachel enthält keine systemeigenen X4 Web Apps. In dieser Kachel werden alle Web Apps angezeigt, die Sie mit der X4 BPMS erstellen.

Hinweis:
Sie können die Kacheln im X4 Control Center mit fünf weiteren vorkonfigurierten X4 Web Apps befüllen:

- App Configuration
- Parameter Editor
- Process Monitor
- Process Scheduler
- 3rd Party License Report

Diese Web Apps sind im Installationspaket All-in-One - Interaktive Installation enthalten. Sie können die Apps aber auch über ein eigenes Installationspaket für das X4 Control Center separat herunterladen.
Beide Installationspakete finden Sie auf der SoftProject-Website im Bereich **Ressourcen** > **Software X4 BPMS**.