

TopSpin GxP

- Quick Start Guide
User Manual
Version 012



Copyright © by Bruker Corporation

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means without the prior consent of the publisher. Product names used are trademarks or registered trademarks of their respective holders.

© May 17, 2021 Bruker Corporation

Document Number:

P/N: 1880068

Contents

1	Purpose of TopSpin's GxP Extension	5
2	Working with TopSpin.....	5
3	Installation.....	5
3.1	Server Installation	6
3.2	Client Installation.....	8
4	Audit Trail.....	12
5	Identity Management.....	16
5.1	User Accounts.....	17
5.1.1	User Attributes	19
5.1.2	Password Expiration for Local Users	19
5.2	Roles.....	20
5.3	Using Windows Active Directory Accounts for Identity Management	24
5.4	Create Another Administrative User Account	27
5.5	How to Change/Reset the Password of a User	30
6	Advanced Topics.....	30
6.1	Managing Users with Groups.....	30
6.2	Remove Warning on Opening Keycloak Administration Console	31
6.2.1	Firefox	31
6.2.2	Edge (Chromium).....	33
6.2.3	Chrome	34
6.2.4	Edge (Legacy Version)	34
6.2.4.1	What if Edge Prevents Opening Keycloak?	35
6.3	Extended Documentation.....	36
7	Contact	37

1 Purpose of TopSpin's GxP Extension

TopSpin provides a multitude of functionalities to support experimental NMR spectroscopy. With the growing usage of NMR in regulated industries (especially pharmaceuticals but also personal care and food), multiple requirements to operate TopSpin in regulated environments have been made during recent years.

TopSpin's GxP extension aims to provide significant functionalities that make NMR much easier to be used in situations where compliance with Good Laboratory Practice, Good Manufacturing Practice or 21CFR part 11 etc. is necessary.

The GxP extension is deliberately implemented to be a separate addition to the standard TopSpin software. The extension incorporates several useful features for example:

- It introduces a comprehensive approach to user identity management and enables exquisite control of users and their rights.
- The user accounts and their rights are generally designed to be consistent with GxP workflows.
- A significantly improved set of tools for retrieving, filtering and printing audit trail entries.

2 Working with TopSpin

Preparation

The decision on whether or not to use the GxP option has to be taken during installation of TopSpin, since activation (and deactivation) of the GxP extension is not possible after installation has been completed.

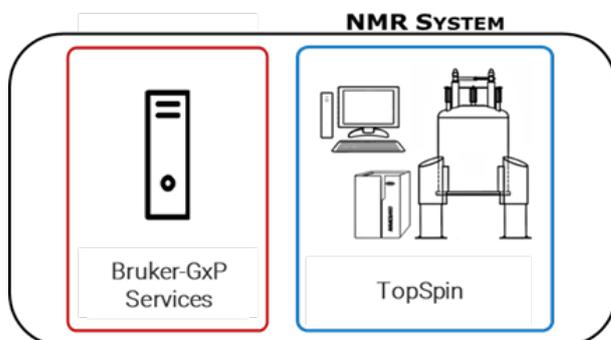
In order to use the GxP extension, a TOPSPIN_GXP_4 license key is required. Topspin installed with the GxP extension does not start without this license; instead a corresponding error message is shown.

3 Installation

The TopSpin GxP extension consists of several components implementing the required functionality. The server component includes Identity management, Central Audit Trail and supporting infrastructure. The client component is a GxP-capable version of Topspin.

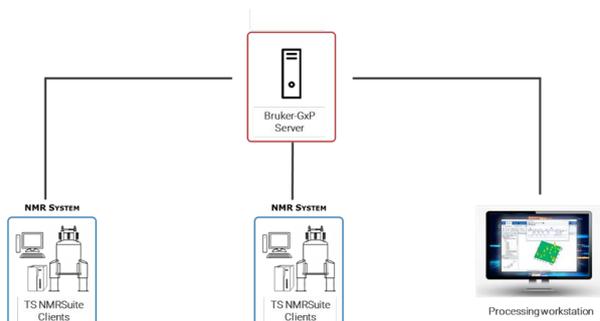
There are two possible deployment scenarios:

In the first, simple case, all components are installed on the same computer, typically the spectrometer controlling workstation.



This layout is appropriate for small labs with only one instrument, only Windows OS is supported.

The 2nd case uses a central server for the Topspin GxP services. Several clients may be connected to this server. All clients share the same Identity Management and write audit records to the same audit trail.



The server may be either physical, or virtual machine running MS Windows. The clients are either spectrometer or processing workstations. Both Windows and Linux (Cent OS) are supported for the clients.

3.1 Server Installation

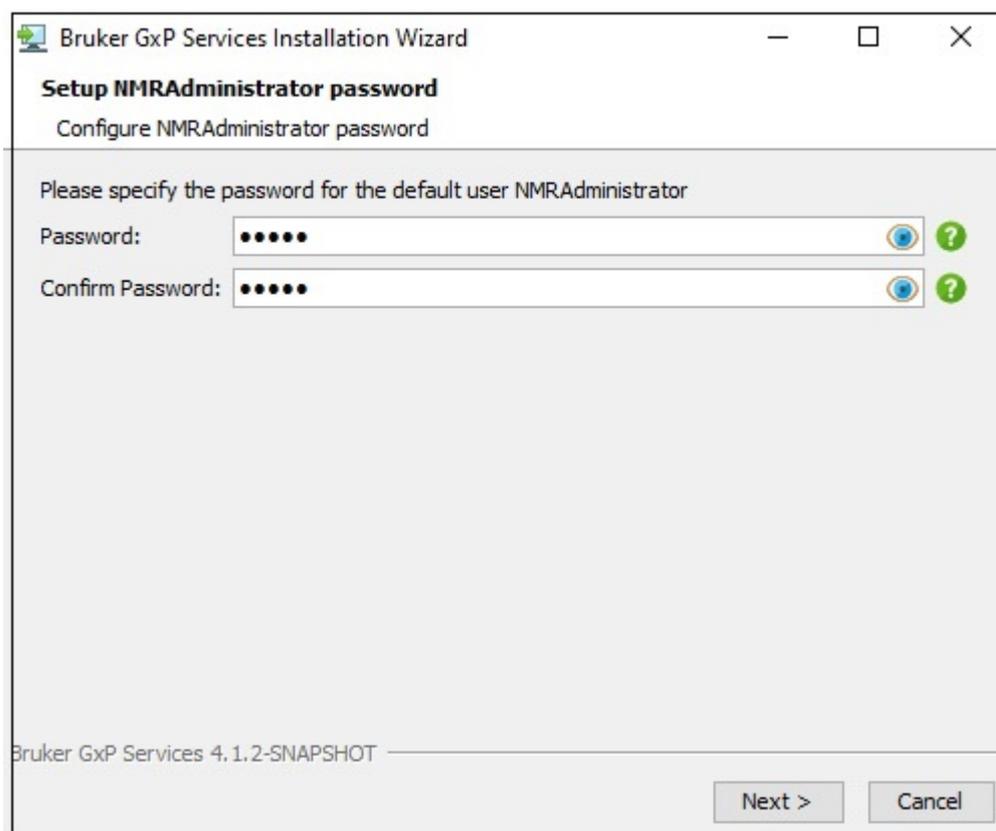
Independent on the deployment, GxP Services should be installed first.



The installation wizard prompts to define passwords for GxP users and services, as well as port numbers to define the communication channels between the GxP components. Bruker recommends using the preset default ports.

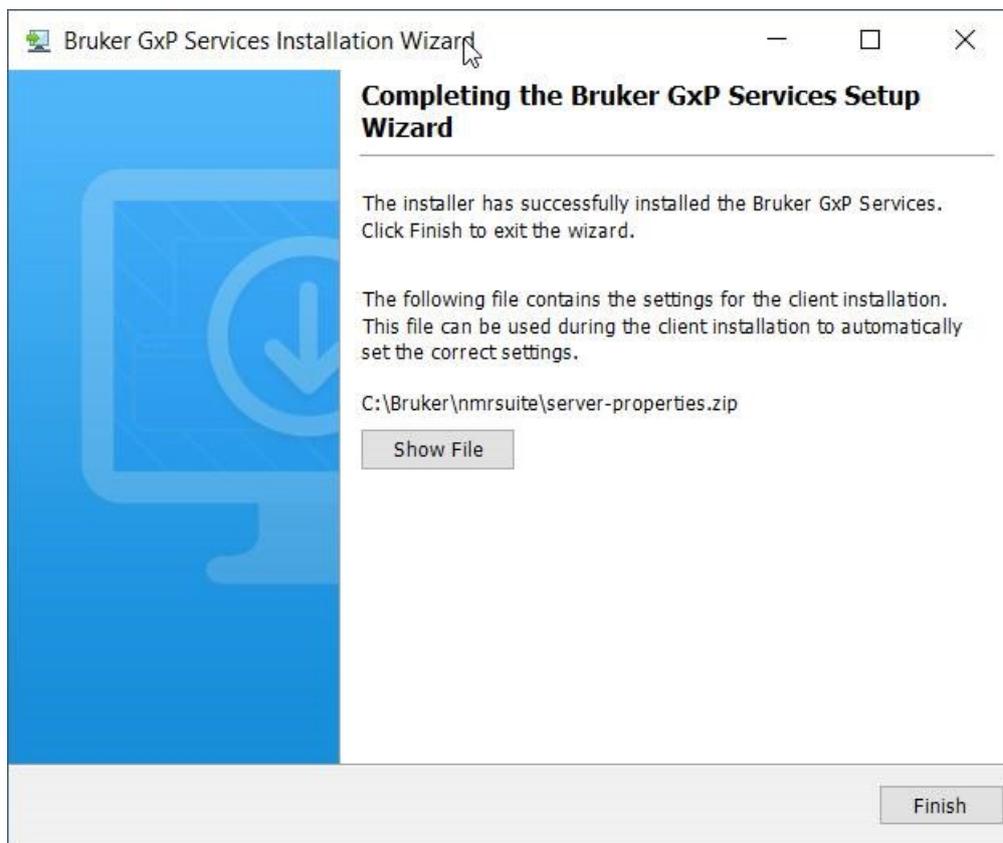
Bruker strongly recommends that these entries are recorded and kept confidential according to your local general instructions (paper file, sealed text file etc.) so that they can be used later.

The identity management creates two default accounts – NMRUser and NMRAdministrator.



These two default users own all rights necessary to operate the NMR spectrometer. They may be used during NMR system installation or maintenance before additional, laboratory specific user accounts will be added.

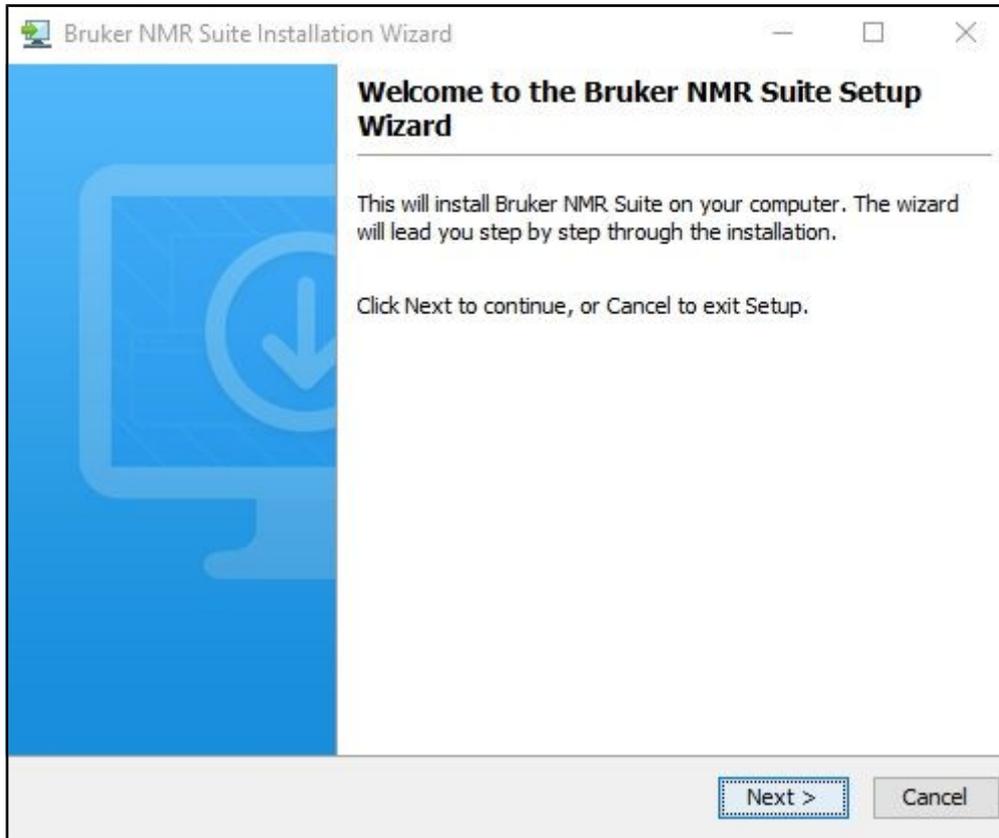
After the service installation finished, the following screen is shown:



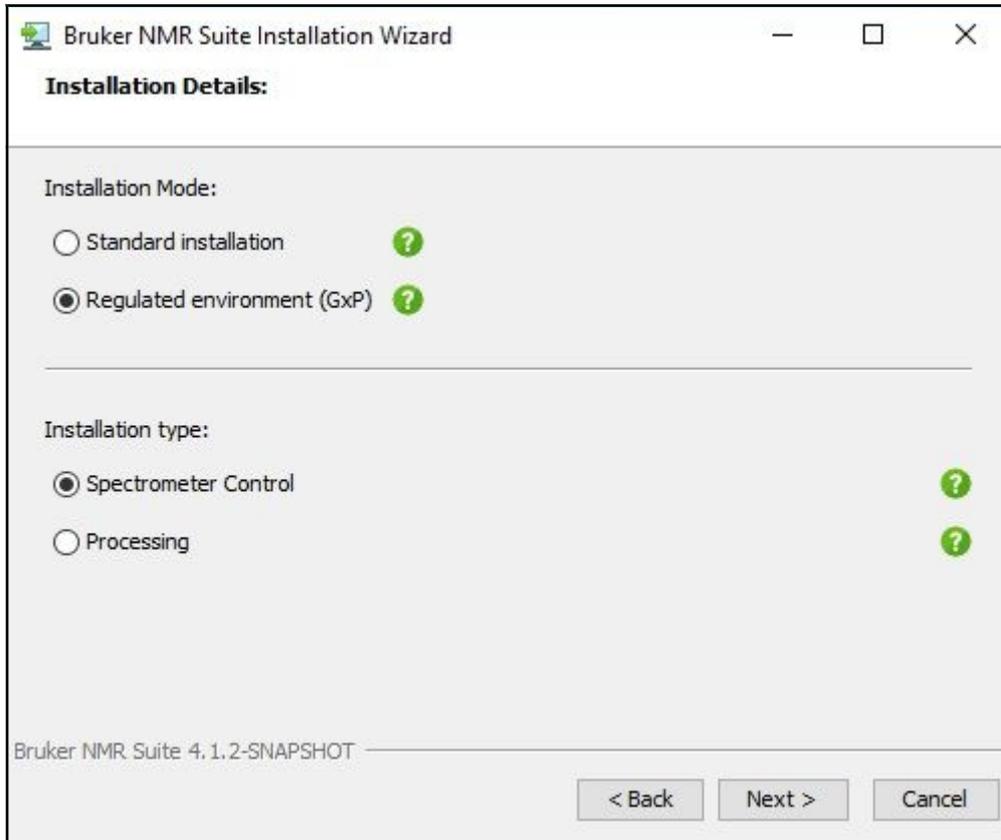
Please note the server settings file. It contains any information about the server setup (users, passwords, ports) which you will need during the client installation.

3.2 Client Installation

The client installer (Windows or Linux) allows to update an existing installation, or to install the software in different folder.

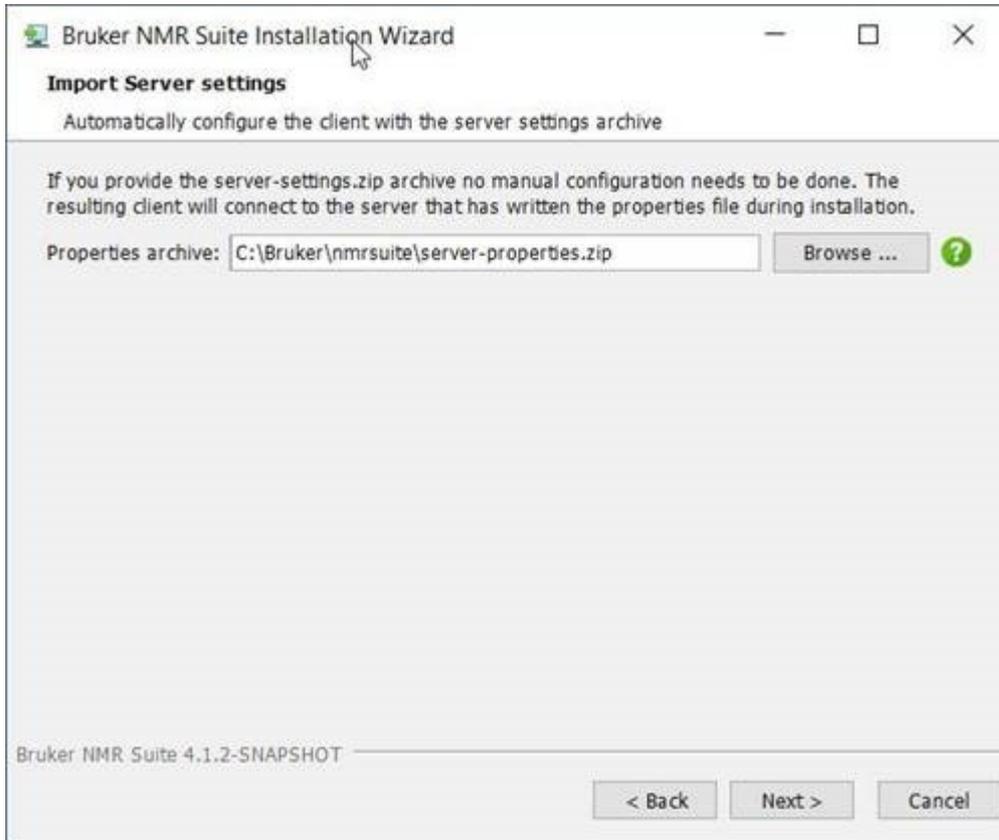


The next step is the selection of installation details.

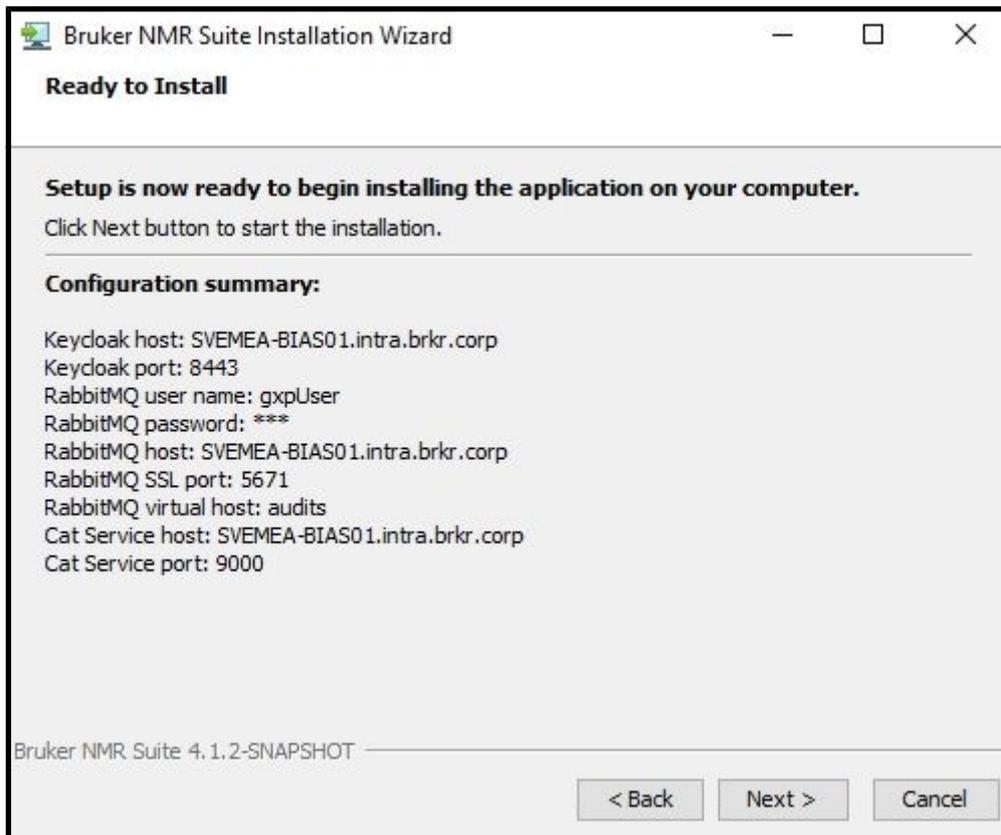


The installation mode (GxP or Standard Installation) cannot be changed if you are upgrading existing installation. The installation type discriminates between Processing and Spectrometer Control. In the latter case all necessary components (automation, spectrometer OS...) are also installed.

The client installation needs the information about the server location and corresponding access credentials. This information is stored in the *server-properties.zip* file created at the end of server installation. You need to copy this file to the current machine and select its location.



The next screen summarizes the used server configuration.



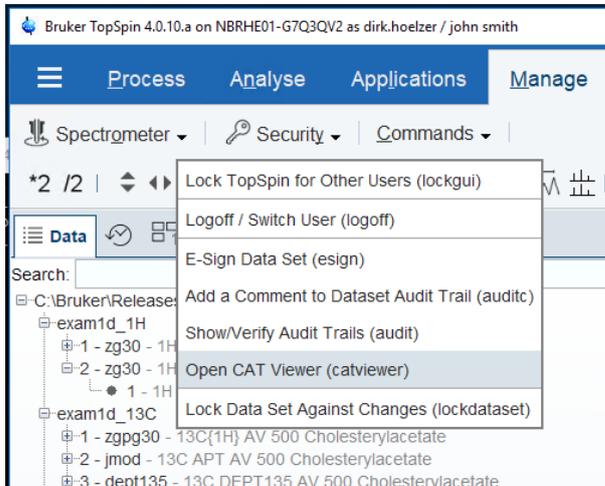
Pressing Next starts the installation of Topspin GxP.

4 Audit Trail

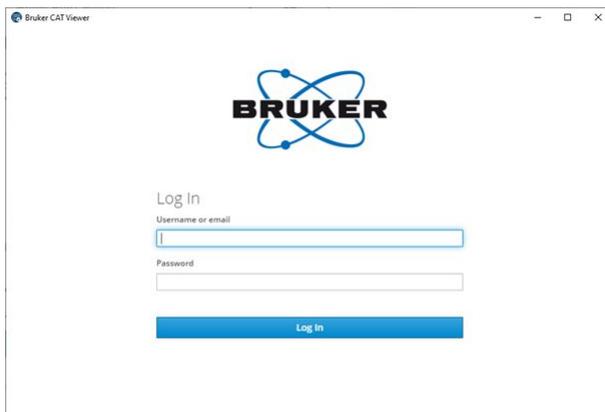


User interactions that create or change data in TopSpin are recorded in a central audit trail database to document who did what and at which point of time. The central audit trail (CAT) collects the data-changing actions of all users referring to any dataset.

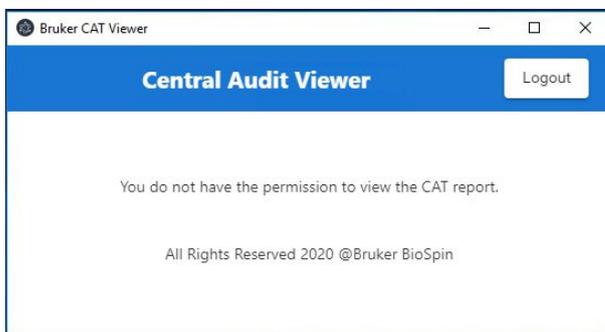
To examine the audit trail records, either launch the central audit trail viewer by double-clicking on the Windows desktop shortcut or directly from TopSpin's user menu item.



The central audit trail viewer also requires credentials for logging in. Also, it needs to be borne in mind that not every user account in TopSpin has automatic rights to login to the central audit trail viewer. Please check chapter [Roles \[20\]](#) for detailed information.

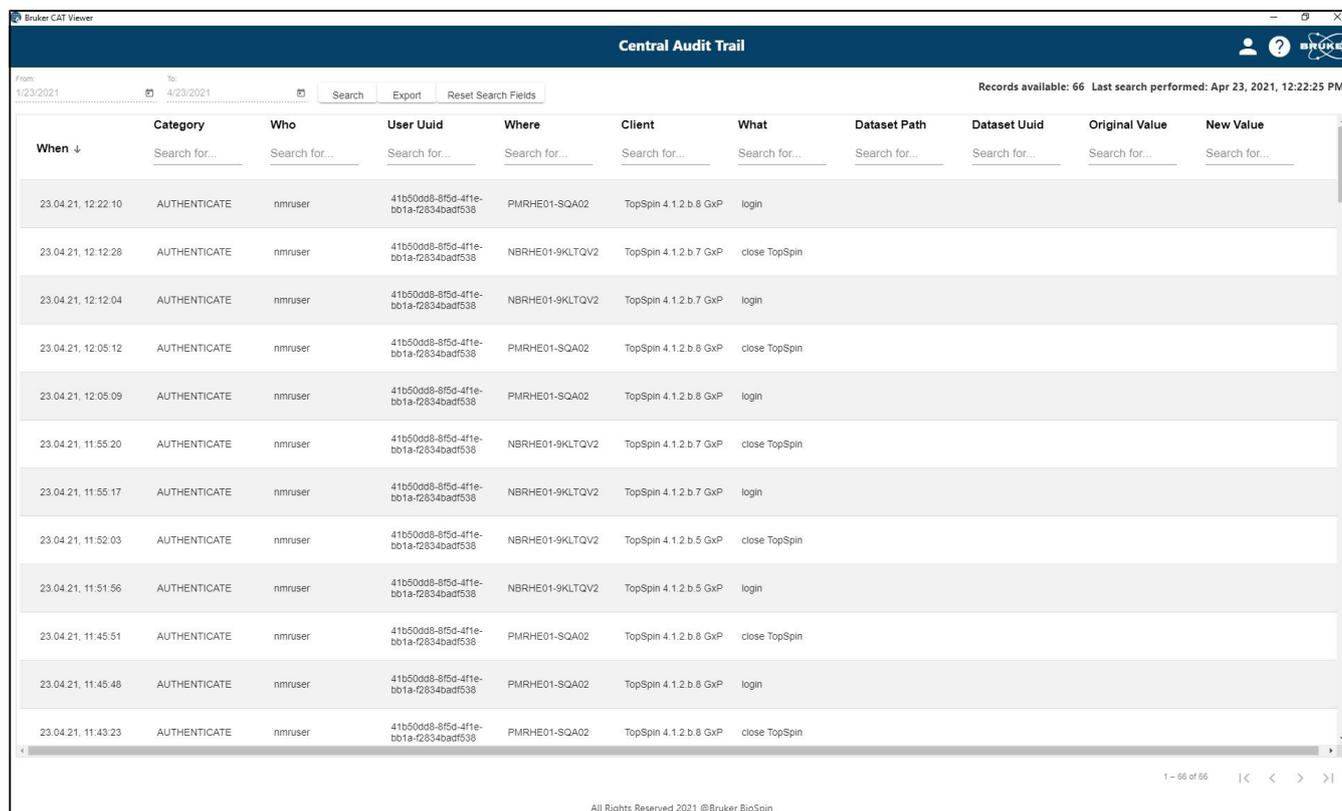


The user account needs the "review" right in order to log in, otherwise the login is refused:



Right after the installation, the default account nmruser owns this right. Therefore you can log in with the account nmruser and its default password "NMRUser".

Once logged in, the central audit trail viewer lists the current records of the last three months. If investigation of older records is required or there is a need to retrieve fewer records, the **From** and **To** dates can be changed to view alternative timespans. This change is visible after the **Search** button is clicked (this applies also for any filter described below).



When ↓	Category	Who	User Uuid	Where	Client	What	Dataset Path	Dataset Uuid	Original Value	New Value
23.04.21, 12:22:10	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	PMRHE01-SQA02	TopSpin 4.1.2.b.8 GxP	login				
23.04.21, 12:12:28	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	NBRHE01-9KLTQV2	TopSpin 4.1.2.b.7 GxP	close TopSpin				
23.04.21, 12:12:04	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	NBRHE01-9KLTQV2	TopSpin 4.1.2.b.7 GxP	login				
23.04.21, 12:05:12	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	PMRHE01-SQA02	TopSpin 4.1.2.b.8 GxP	close TopSpin				
23.04.21, 12:05:09	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	PMRHE01-SQA02	TopSpin 4.1.2.b.8 GxP	login				
23.04.21, 11:55:20	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	NBRHE01-9KLTQV2	TopSpin 4.1.2.b.7 GxP	close TopSpin				
23.04.21, 11:55:17	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	NBRHE01-9KLTQV2	TopSpin 4.1.2.b.7 GxP	login				
23.04.21, 11:52:03	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	NBRHE01-9KLTQV2	TopSpin 4.1.2.b.5 GxP	close TopSpin				
23.04.21, 11:51:56	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	NBRHE01-9KLTQV2	TopSpin 4.1.2.b.5 GxP	login				
23.04.21, 11:45:51	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	PMRHE01-SQA02	TopSpin 4.1.2.b.8 GxP	close TopSpin				
23.04.21, 11:45:48	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	PMRHE01-SQA02	TopSpin 4.1.2.b.8 GxP	login				
23.04.21, 11:43:23	AUTHENTICATE	nmruser	41b50d98-8f5d-4f1e-bb1a-f2834badf538	PMRHE01-SQA02	TopSpin 4.1.2.b.8 GxP	close TopSpin				

Each record in the CAT contains a series of meta data items:

From the left:

Each record contains a timestamp, a category to which user interactions belong and the name of the user account that initiated the action.

UUID: It is noted that a user account may be deleted (for example if an employee leaves the organization) and at some time in the future, a new user account with the same user name could be created. It is important to be able to distinguish between these two different accounts as they relate to different people. This can be done by checking the unique user id (Uuid) which is not easily readable but ensures – as it says – uniqueness.

Where: The central audit trail can be the common audit trail database for all Bruker NMR spectrometers in a laboratory or on a site. Therefore, the column **Where** specifies which workstation was used to execute the action described in the **What** column.

Client defines the software the user interacted with. This is typically TopSpin but other Bruker products (for example IconNMR or GoScan may be used for GxP – planned).

Data Set Path describes to which experiment/processing data the **What** applies. If a data set is affected, the audit trail record is also written into the data set's specific audit trail file (can be inspected via **Manage | Security | Show/Verify Audit Trails**).

The columns **Original Value** and **New Value** serve to illustrate specific data changes.

After some time of operation, the audit trail database will probably have grown to a substantial size and the user might want to narrow the number of retrieved records in order to easily investigate specific topics. For each column, filtering by any character is possible. After clicking the **Search** button, only the entries containing the substrings are displayed. In many cases, it is sufficient to enter the only a few letters of a keyword to filter out many unnecessary entries. In the case depicted below, the filter for **AUTH** in the **Category** column removes entries not related to authentication and yields typical login/logoff entries.

From: 4/23/2020 To: 7/23/2020 Search Export

When	Category	Who	User Uuid
	<u>AUTH</u>	Search for...	Search for..
23.07.20, 09:11:33	AUTHENTICATE	nrmuser	3aed533f-b379605-faecaf2
23.07.20, 09:11:44	AUTHENTICATE	dirk.hoelzer	e4c2b3cb-d5e9438-646aaa:
23.07.20, 09:42:02	AUTHENTICATE	dirk.hoelzer	e4c2b3cb-d5e9438-646aaa:
23.07.20, 09:42:09	AUTHENTICATE	john smith	a4a84f05-53f9925-f0be1eC
23.07.20, 09:44:43	AUTHENTICATE	john smith	a4a84f05-53f9925-f0be1eC
23.07.20, 09:47:25	AUTHENTICATE	john smith	a4a84f05-53f9925-f0be1eC
23.07.20, 09:48:35	AUTHENTICATE	john smith	a4a84f05-53f9925-f0be1eC
23.07.20, 09:49:42	AUTHENTICATE	john smith	a4a84f05-53f9925-f0be1eC

Multiple search entries are combined so that the result set contains only the records including both search criteria, i.e. more criteria help to narrow the search.

Clicking **Reset Search Fields** removes all user-defined filters.

When it is opened, the audit trail is always ordered by the **When** field i.e. with the most recent at the top.

Finally, the filtered result could be exported to a PDF document in order to store it separately or print it out with PDF viewer.

• Central Audit Trail Export


Auditor: nmruser
Search criteria: From: 2020-04-13, To: 2020-07-14
Number of Entries: 9

Signature: _____

When	Category	Who	Where	Client	What	Dataset Path	Original Value	New Value
13.07.20, 17:24:08	AUTHENTICATE	nmradministrator	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	login			
13.07.20, 17:29:43	AUTHENTICATE	nmradministrator	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	logout			
13.07.20, 17:29:52	AUTHENTICATE	nmruser	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	login			
13.07.20, 17:29:54	PROCESSING	nmruser	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	Start of raw data processing em LB = 0.3 SI = 32K data hash MDS: 32K E1 2D 05 7B C2 C8 56 BF 41 FA 0B 60 38 45 00 90	C:/Bruker/Releases/TopSpin4.0.9/exadata/examid_1H/1/pdata/1		
13.07.20, 17:29:54	PROCESSING	nmruser	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	ft FT_mod = 6 PKNL = 1 SI = 32K data hash MDS: 32K 8B B0 48 34 F9 F9 F7 3F 97 D9 A4 02 1C 24 B1 C8	C:/Bruker/Releases/TopSpin4.0.9/exadata/examid_1H/1/pdata/1		
13.07.20, 17:29:54	PROCESSING	nmruser	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	apk data hash MDS: 32K 37 F6 07 11 D6 91 33 64 49 26 DC DF 77 AF 7D 4F	C:/Bruker/Releases/TopSpin4.0.9/exadata/examid_1H/1/pdata/1		

Report ID : e7d666c8-84ec-3d95-8f1d-e362f8d8935f
13.07.2020, 17:35:49

Page 1 of 2

Once work with the audit trail viewer has been completed, click the button **Logout** in the upper right hand corner to close the session.

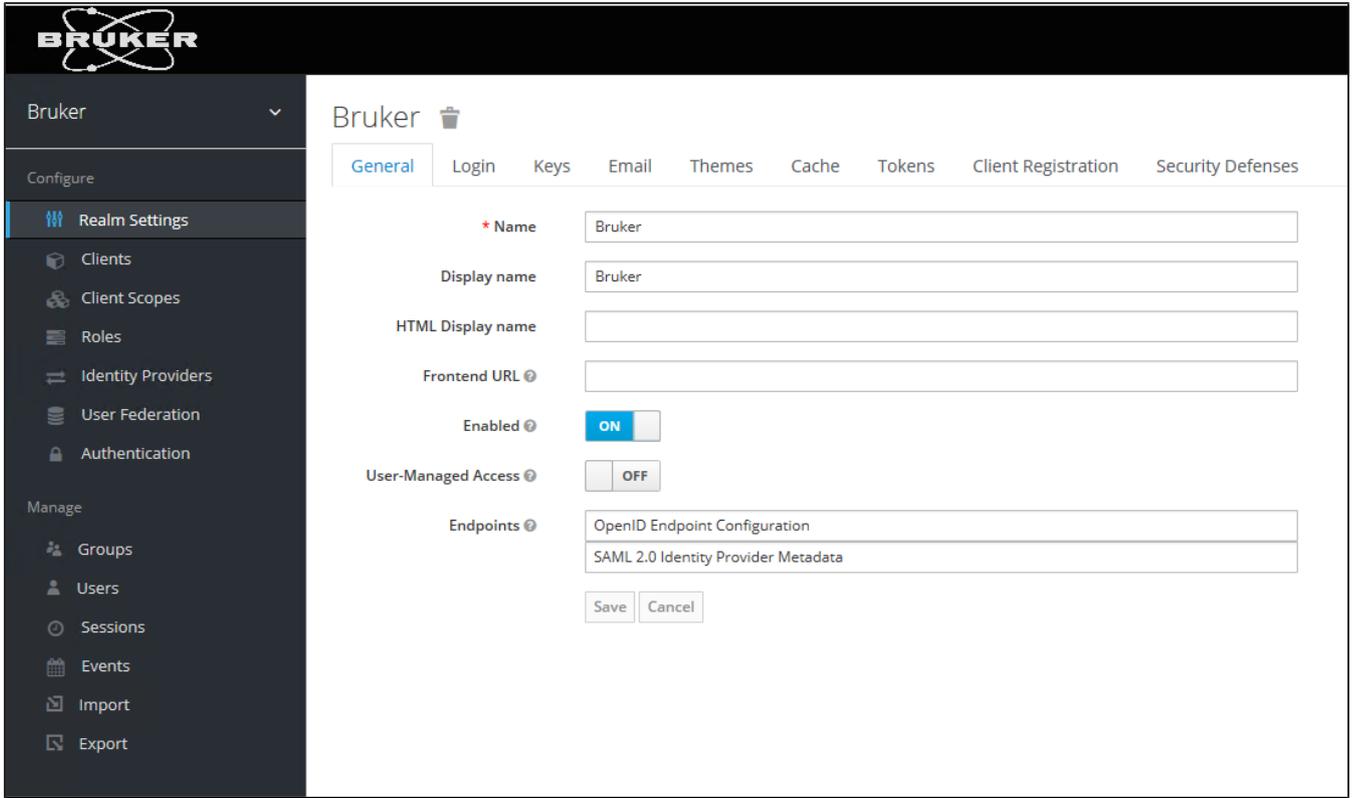
5 Identity Management



The TopSpin GxP extension provides a variety of options on how to configure user accounts and their specific rights. TopSpin GxP uses a widely used and proven component for identity management which is named Keycloak. Click the Bruker User Management shortcut on the desktop to launch the Identity Management Console. The default browser on the workstation starts and tries to open the Keycloak start page that contains the Bruker Identity Management. Depending on the browser settings, this may generate a security warning but this can be safely ignored.

The Keycloak Identity Management features a multitude of options and settings that may be altered in order to comply with relevant SOPs and general requirements. However, for default usage, Bruker recommends only to change settings that are described below. Otherwise, the combination of Keycloak with TopSpin GxP and the Audit Trail Viewer might not work properly.

- On first login, use the Keycloak credentials that were entered and stored safely during the installation progress (see chapter [Installation](#) [5]).
- Select the realm “Bruker” which contains the necessary pre-configurations.



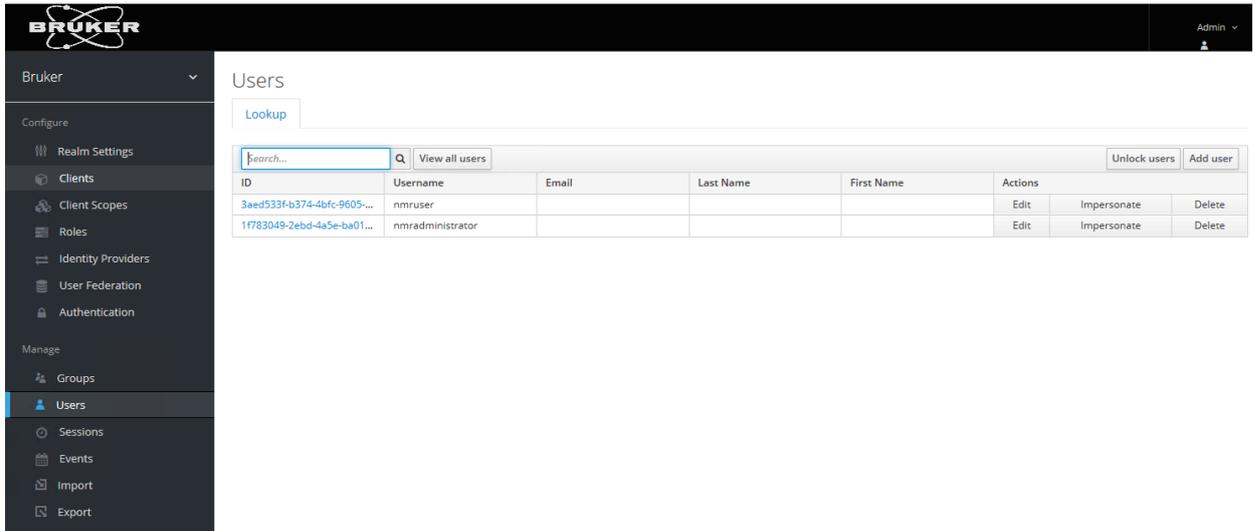
5.1 User Accounts

When **Users** is used for the first time, two pre-defined user accounts will appear – these have been included to enable a jump-start with TopSpin: **nmruser** and **nmradministrator**. **nmruser** has the default password “NMRUser” whereas the **nmradministrator** password is the one that was created during the installation (see [below](#) [5]).

If working with personalized accounts is preferred, these two default accounts are to be deleted.

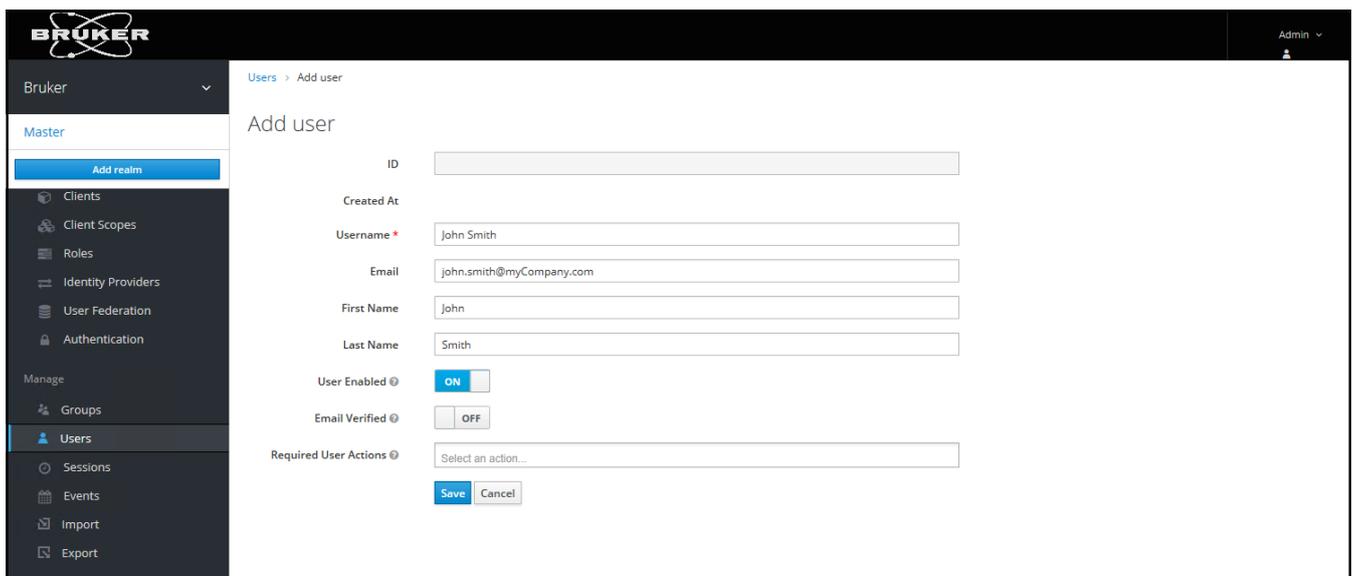


Note that TopSpin passwords are upper/lowercase sensitive.



For working in an GxP environment, specific personalized user accounts are often required. New accounts can be created by the following procedure:

- In the tab **User**, click on **View all users**, then on **Add user**.
- At minimum, fill out the field **Username**, then click on **Save**.
- On the next screen, select page **Credentials**. Define the initial password. Set the option **Temporary** to **Off**, then click **Set Password** and confirm.
- With these personal credentials, the new user will be able to login to TopSpin from now on.
- To be able to work with TopSpin, each user must have an assigned role. This is done in page **Role Mappings**. Detailed description is available in chapter [Roles](#) [▶ 20].



In the tab **Credentials** the user account's password is to be defined and changed, if necessary.

5.1.1 User Attributes

For each user who will use TopSpin's esign command you have to define signature meanings. After you created a new Top Spin user, open the tab Attributes and add an Attribute ESIGN, and as value, enter possible meanings for signatures, separated by ##, e.g. for Approved, Checked, Release or as depicted below.

Users > john

John 

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

Key	Value	Actions
ESIGN	Sample Identity confirmed##Analysis approved	Delete
SPECTROMETER_BLACKLIST	BLOB##NBRHE01-F07NSQ2	Delete
<input type="text"/>	<input type="text"/>	Add

SPECTROMETER_BLACKLIST is an additional, optional attribute. It allows to refuse user login on specified computer. The list consists of several hostnames separated by ##. This allows to use one common user management for the whole lab and in parallel restrict the usage of some instruments to selected user group. TopSpin login on a prohibited computer is denied and the following corresponding error message is shown.

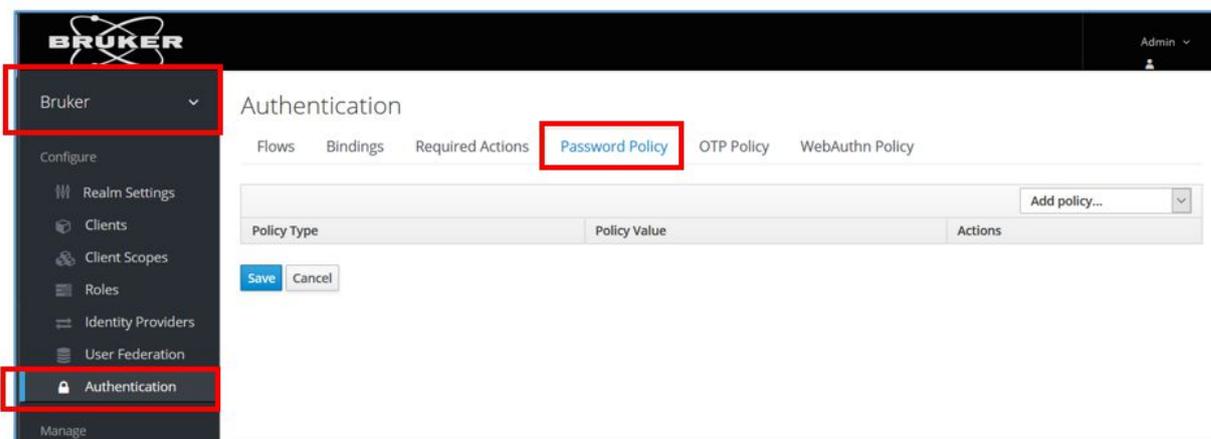


5.1.2 Password Expiration for Local Users

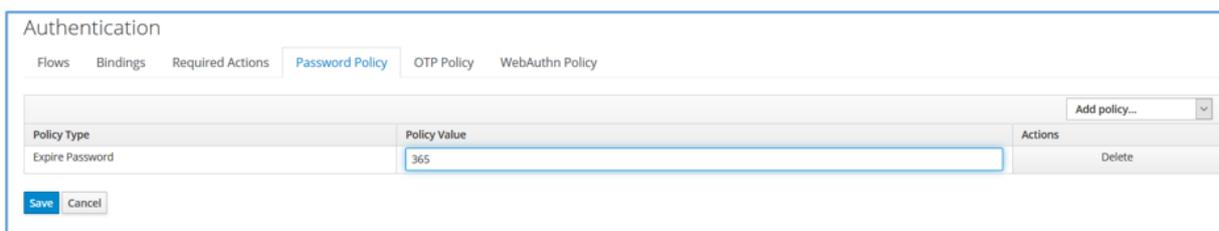
The definition of a time span for password expiration is done by a Windows Active Directory administrator for any LDAP user account integrated in Bruker GxP solution (see chapter [User Accounts](#) [17]).

For local user accounts, an expiration time span can be defined as follows:

1. When logged in to the Keycloak administration console, the Bruker realm has to be selected
2. Click on **Authentication** on the left-side menu and choose the **Password Policy** tab



1. From the **Add policy** drop-down menu, choose **Expire Password**
2. Enter the desired number of days until password expiration and click on **Save**.



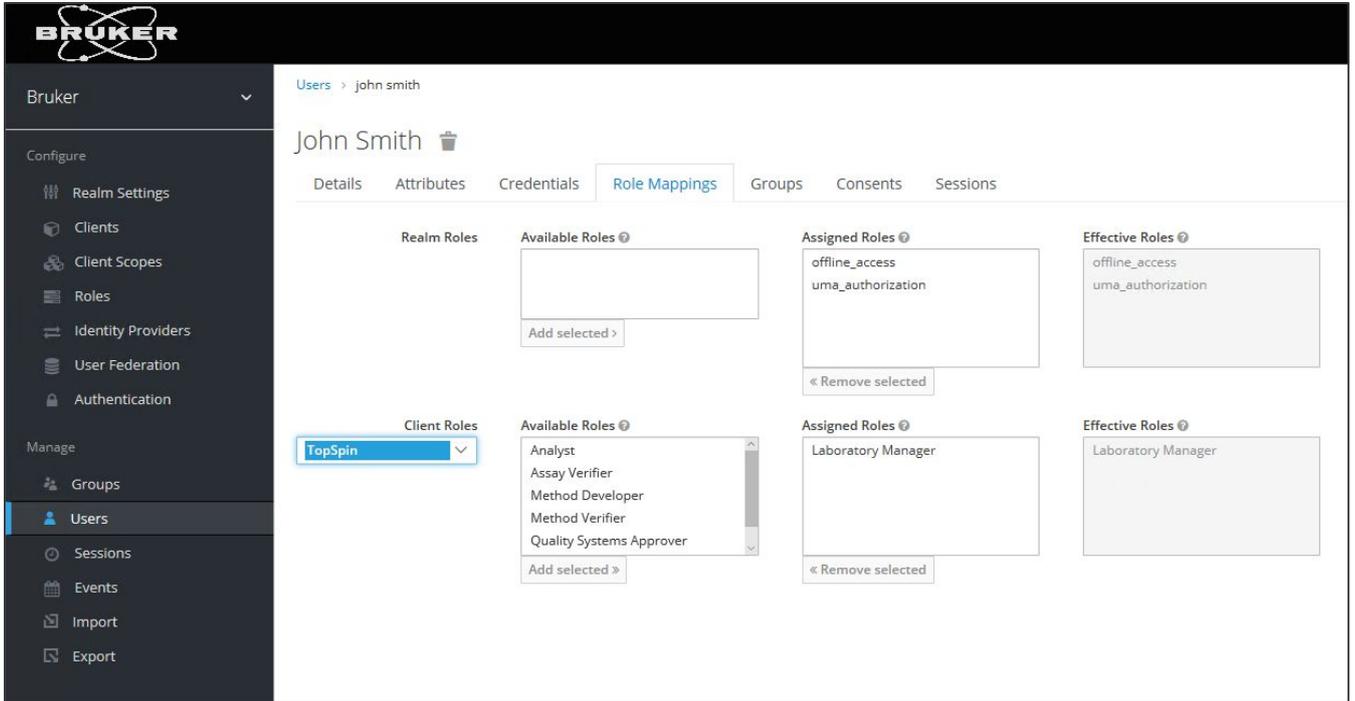
Setting no policy means that passwords will stay valid for an infinite amount of time.

5.2 Roles

Click on the tab **Role Mappings**, then select from the box **Client Roles** the entry **TopSpin** in order to show the list of available roles. Selecting them for a given user defines his/her interactions with TopSpin.

The predefined roles are:

- Spectrometer Administrator
- Analyst
- Assay Verifier
- Method Developer
- Method Verifier
- Laboratory Manager
- Quality Systems Approver

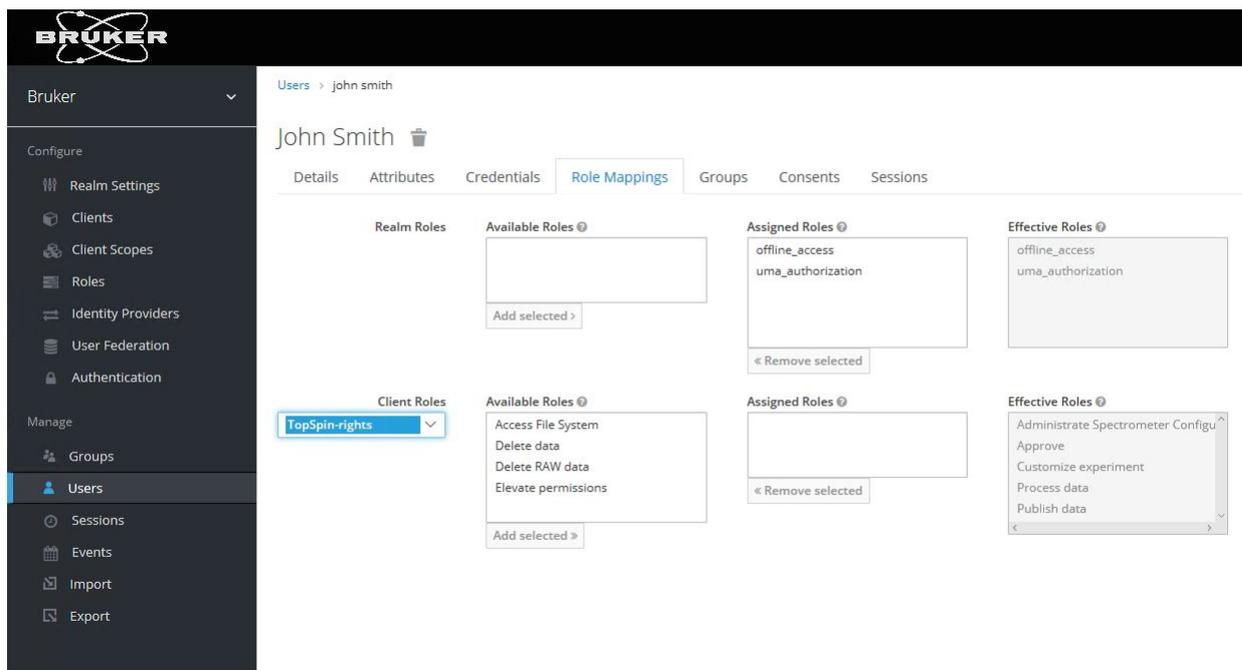


The screenshot displays the Bruker user management interface for user John Smith. The left sidebar contains navigation options under 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The main content area is titled 'John Smith' and includes tabs for 'Details', 'Attributes', 'Credentials', 'Role Mappings', 'Groups', 'Consents', and 'Sessions'. The 'Role Mappings' tab is active, showing two sections: 'Realm Roles' and 'Client Roles'. The 'Client Roles' section is expanded for the 'TopSpin' client. Each section contains an 'Available Roles' list, an 'Assigned Roles' list, and an 'Effective Roles' list. In the 'Client Roles' section, the 'Available Roles' list includes Analyst, Assay Verifier, Method Developer, Method Verifier, and Quality Systems Approver. The 'Assigned Roles' list contains 'Laboratory Manager', which is also reflected in the 'Effective Roles' list.

The following table shows which TopSpin rights are granted to what user roles:

Right	Spectrometer Administrator	Analyst	Assay Verifier	Method Developer	Method Verifier	Laboratory Manager	Quality Systems Approver
Administrate Spectrometer Configuration	X					X	
Setup method				X		X	
Customize experiment				X		X	
Start experiment		X		X	X	X	
Process data		X		X	X	X	
Delete RAW data	X						
Delete data	X						
Access File System	X						X
Publish data		X	X	X	X	X	X
Review		X	X	X	X	X	X
Approve		X	X			X	X

Selecting the **Client Roles** combo box item **TopSpin rights** shows the corresponding rights in the **Effective Roles** combo box.



The following roles are used for the predefined users:

nmruser	Laboratory Manager
nmradministrator	Spectrometer Administrator

These predefined accounts provide a minimum of roles and rights management as a starting environment. So you can login as nmradministrator immediately upon first start of TopSpin. Due to the role as Laboratory Manager, you have the right to perform important configuration steps.

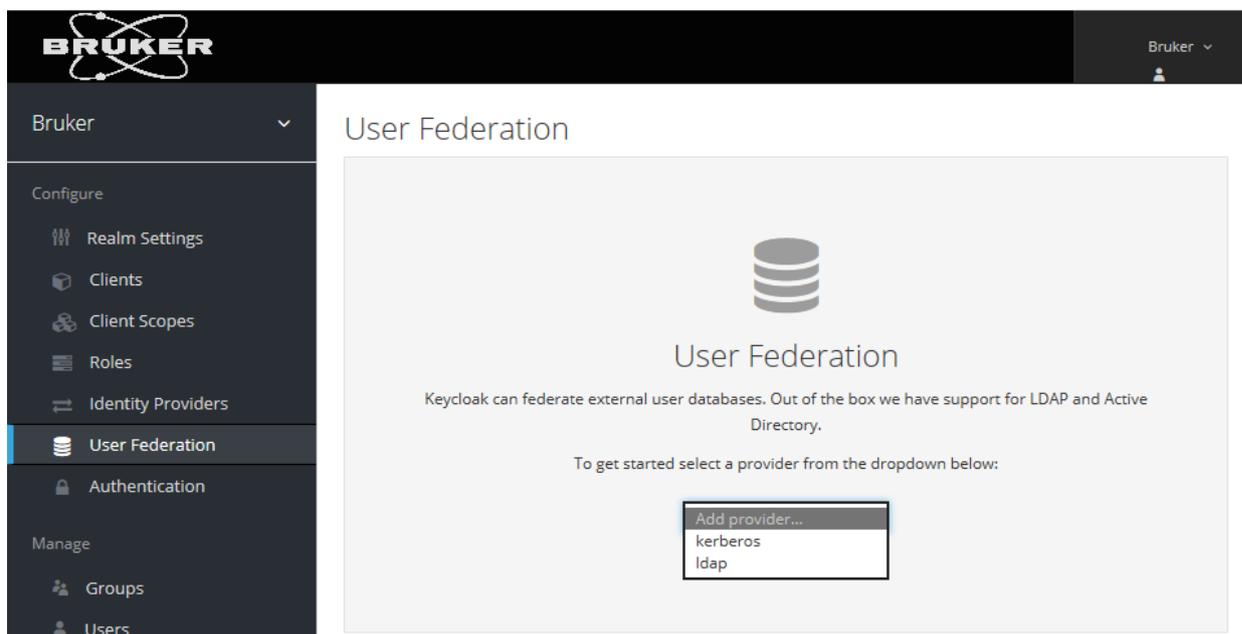
When logged in as nmruser, you have more restricted rights according to the table shown above.

This assignment may be changed anytime, the Bruker predefined user accounts may even be disabled.

5.3 Using Windows Active Directory Accounts for Identity Management

When the spectrometer workstation is in a Windows Active Directory / LDAP Domain, it is recommended to map the TopSpin user account defined at this stage with an existing Active Directory/LDAP account. This enables the user to login to TopSpin with the same credentials that he/she uses for his/her workstation login. Access to TopSpin GxP is therefore controlled by the overarching user access control system, and therefore user identity, password validity, password complexity etc.

To integrate the accounts in the Windows Active Directory, navigate to **User Federation** in the Keycloak Console and select LDAP as provider for the user accounts.



The following screenshot serves as an example for how to set up the connection between the Active Directory and the Bruker Identity Management. Please replace the placeholders 'server', 'myDomain' by the real names of your server and your domain. The Bind DN is your domain e-mail address (e.g. John.Smith@bruker.com) and the credentials are your password: i.e. John's Smith domain password.

To ensure the right data is entered in these fields, click on test connection and test authentication afterwards.:

- **ConnectionURL:** ldap://server.myDomain

- **Users DN:** dc=myDomain
- **Bind DN:** admin@myDomain (and the according password for **Bind Credential**)

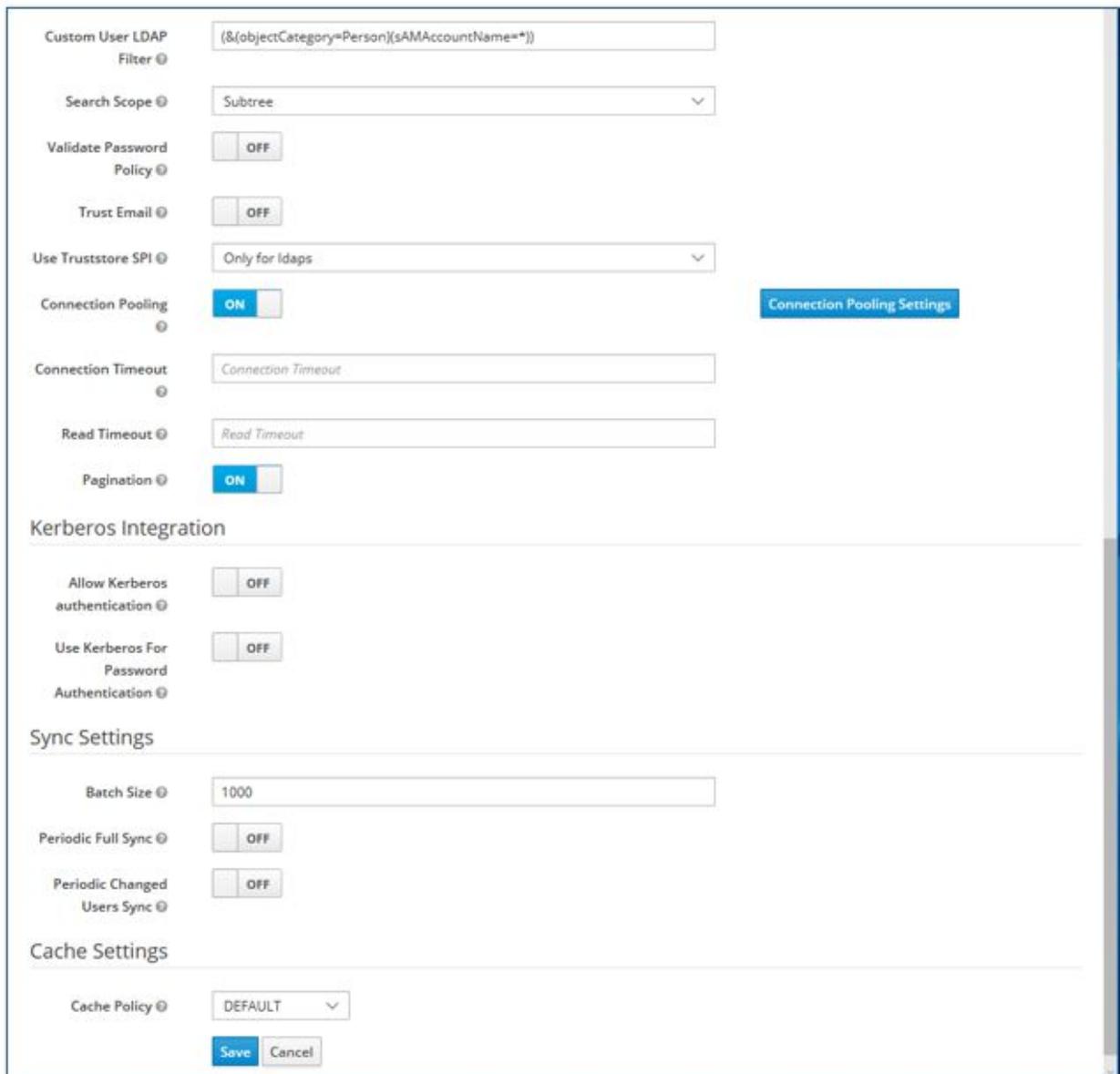
In the field **Connection URL**, use 389 or 10389 for LDAP, 636 or 10636 for LDAPS (LDAP over SSL).

Add user federation provider

Required Settings

Enabled	<input checked="" type="checkbox"/>	
Console Display Name	<input type="text" value="ldap"/>	
Priority	<input type="text" value="0"/>	
Import Users	<input checked="" type="checkbox"/>	
Edit Mode	<input type="text" value="UNSYNCED"/>	
Sync Registrations	<input type="checkbox"/>	
* Vendor	<input type="text" value="Active Directory"/>	
* Username LDAP attribute	<input type="text" value="cn"/>	
* RDN LDAP attribute	<input type="text" value="cn"/>	
* UUID LDAP attribute	<input type="text" value="objectGUID"/>	
* User Object Classes	<input type="text" value="user"/>	
* Connection URL	<input type="text" value="ldap://server.myDomain:389"/>	<input type="button" value="Test connection"/>
* Users DN	<input type="text" value="dc=myDomain"/>	
* Bind Type	<input type="text" value="simple"/>	
Enable StartTLS	<input type="checkbox"/>	
* Bind DN	<input type="text" value="admin@myDomain.com"/>	
* Bind Credential	<input type="password" value="*****"/>	<input type="button" value="Test authentication"/>

Auf "diesem PC"



The screenshot displays the configuration interface for TopSpin GxP, organized into several sections:

- LDAP Settings:**
 - Custom User LDAP Filter:
 - Search Scope:
 - Validate Password Policy:
 - Trust Email:
 - Use Truststore SPI:
 - Connection Pooling: (with a [Connection Pooling Settings](#) button)
 - Connection Timeout:
 - Read Timeout:
 - Pagination:
- Kerberos Integration:**
 - Allow Kerberos authentication:
 - Use Kerberos For Password Authentication:
- Sync Settings:**
 - Batch Size:
 - Periodic Full Sync:
 - Periodic Changed Users Sync:
- Cache Settings:**
 - Cache Policy:

At the bottom of the form, there are **Save** and **Cancel** buttons.

Click **Save** and then **Synchronize all Users**.

Navigate to **Users** to find all the user accounts of the Active Directory listed. By clicking on **Edit** you can, as described above, assign the according TopSpin roles to the Active Directory accounts.

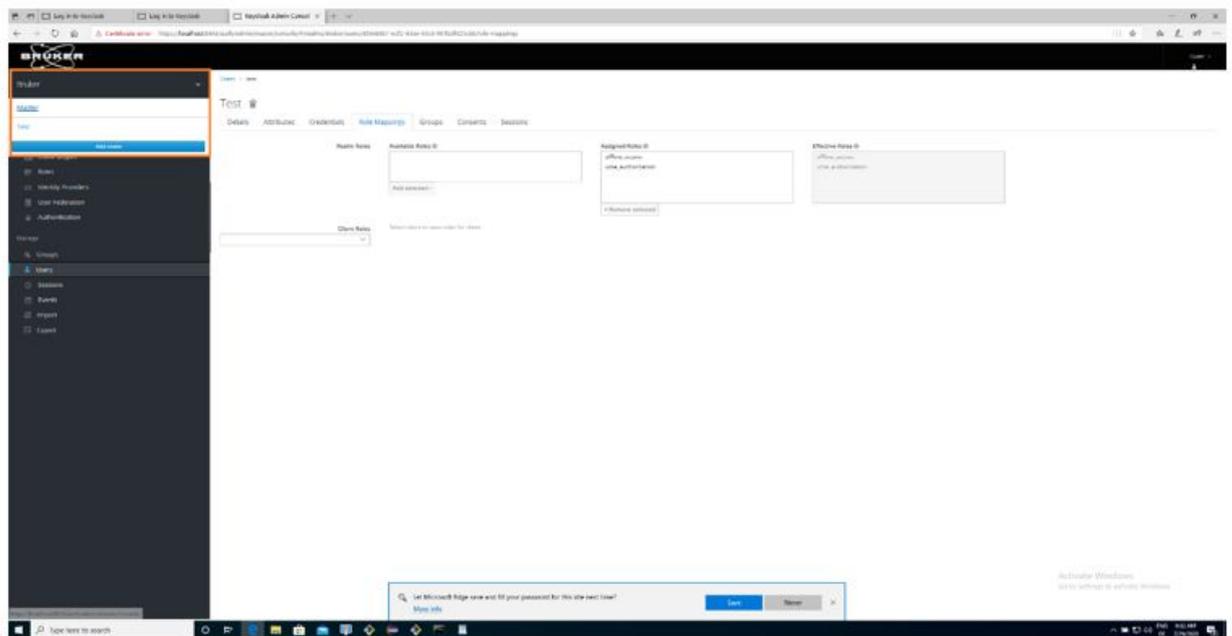
After this stage has been completed, login to TopSpin with Active Directory credentials is possible for all these users.

5.4 Create Another Administrative User Account

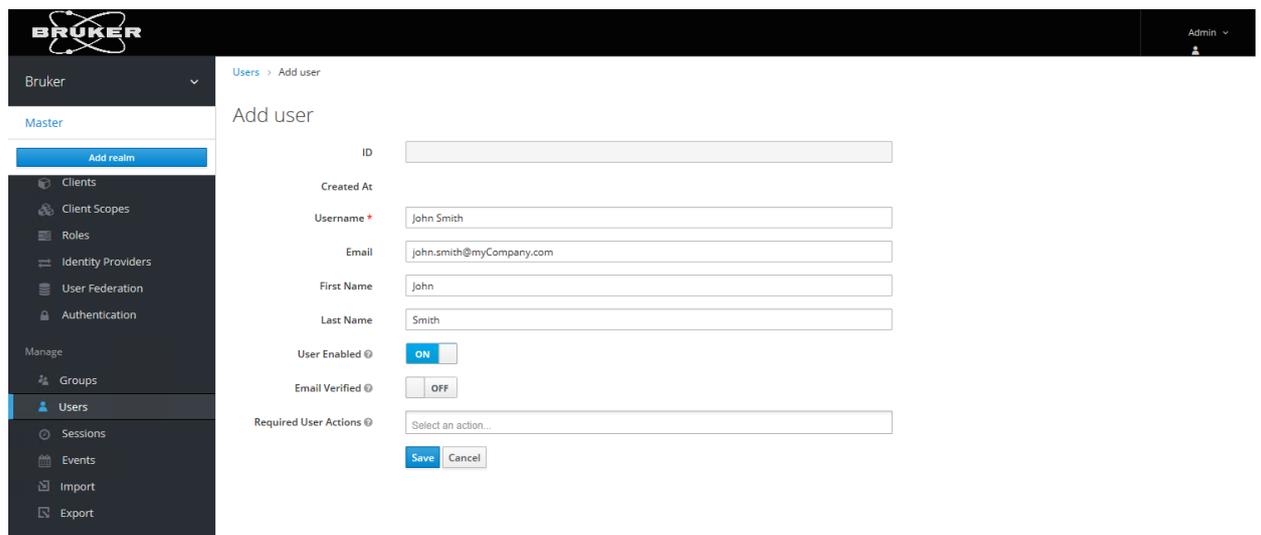
If the usage of the default admin account for identity management in Keycloak is undesirable, another account can be set up by following these steps:

Login to Keycloak (click icon **Identity Management** on Desktop) and enter admin user credentials (the credentials have been entered and stored safely during the installation progress).

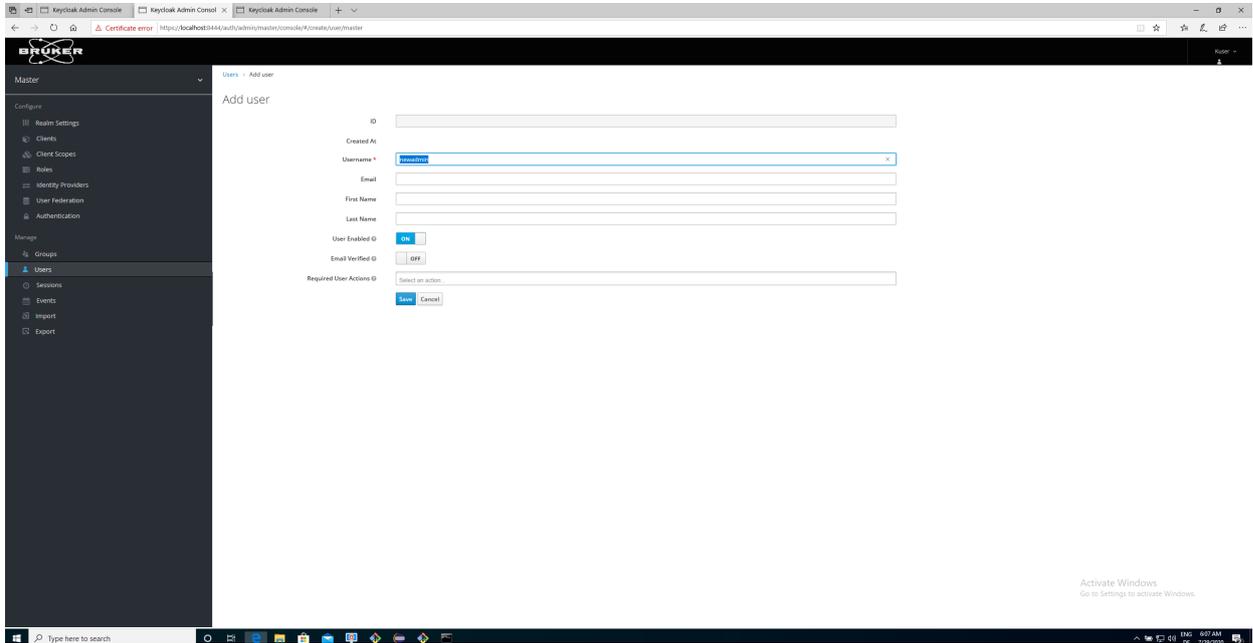
Switch to realm **Master**.



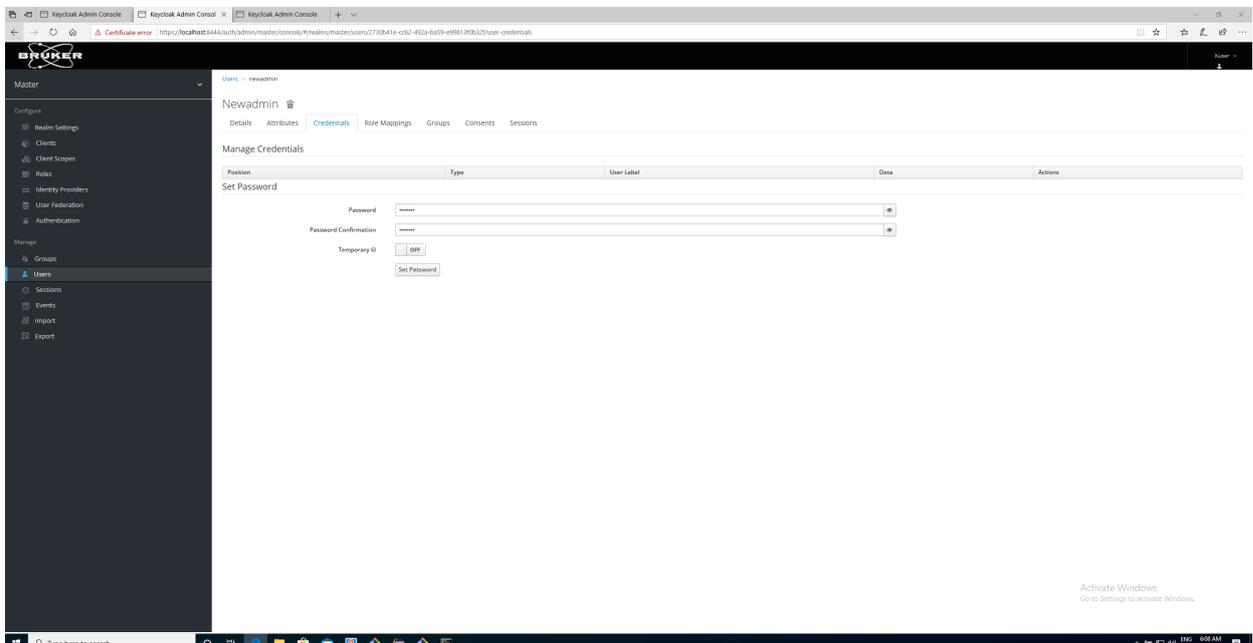
Navigate to section **Users**, then click on **Add User**.



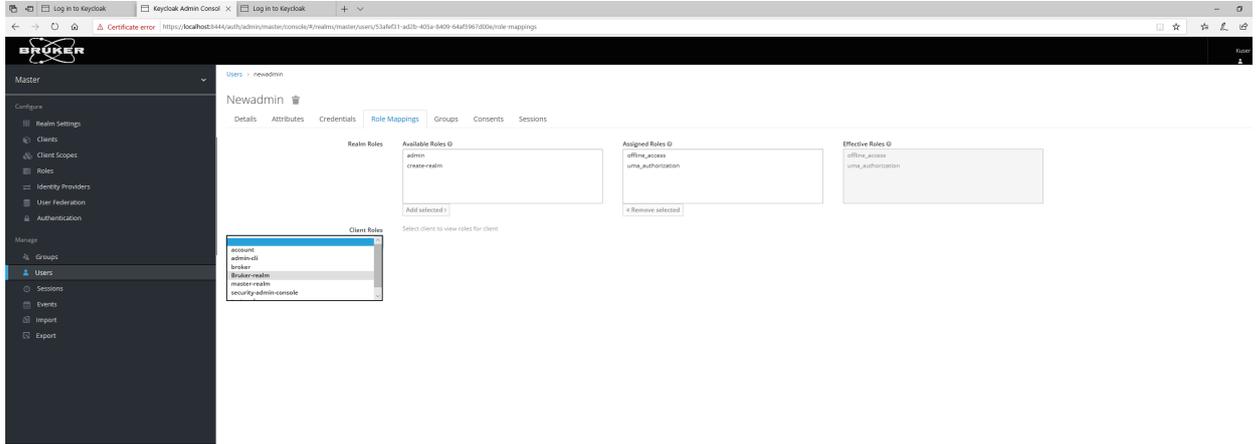
Enter username and click on **Save**.



Select the tab **Credentials**, define a password, and disable **Temporary**.

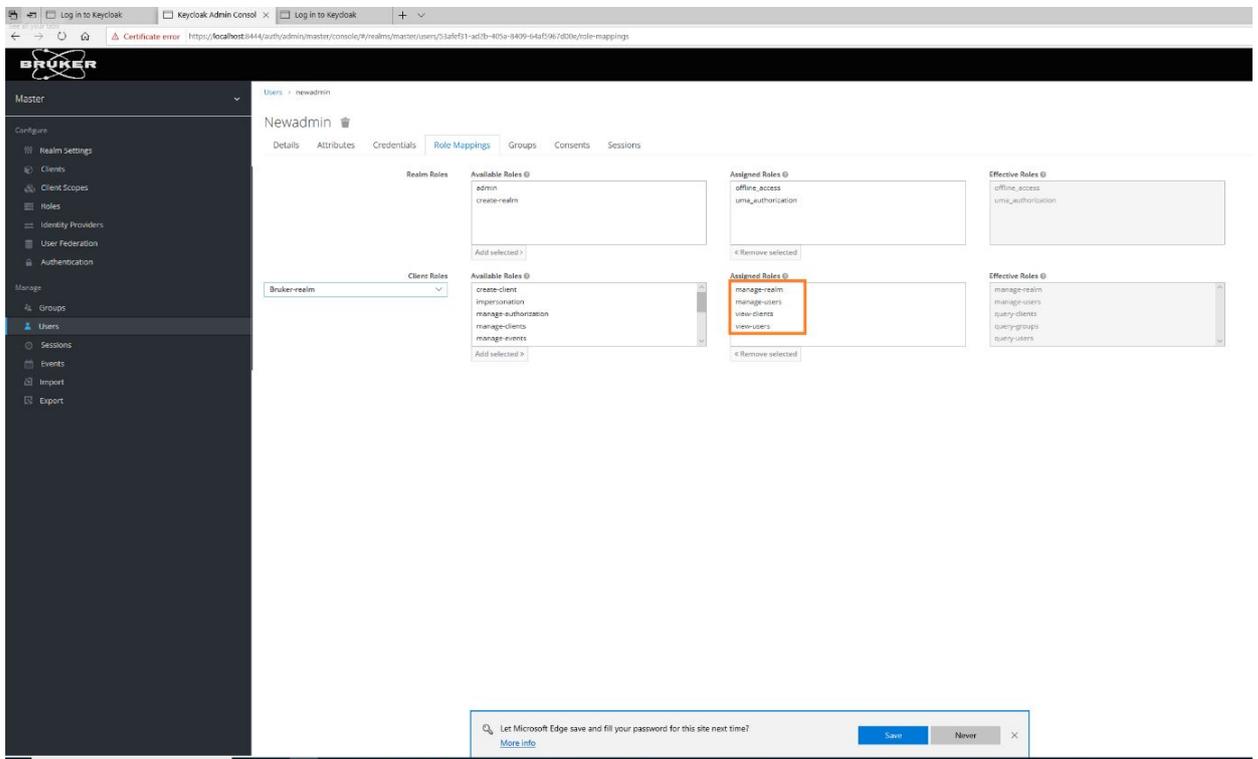


Select the tab **role mappings** and select the client roles for Bruker-realm.



Then add the roles

- manage-users
- view-users
- manage-realm
- view-clients



Switch the realm back to **Bruker**, then logoff the admin user.

Finally, click the link on the desktop to be directed to the login screen of Keycloak to login with the new account's credentials.

It is also possible to grant Keycloak administrator rights to an LDAP account for TopSpin users, which is analogous as described in the chapter above.

5.5 How to Change/Reset the Password of a User

Note that the icon **User Management** on the desktop only allows login for the administrator of Keycloak only, not for normal users. You can also open a web browser and go to the address <https://localhost:8443/auth/admin/> for accessing the identity management..

However, every known user can login for self-management and change the password of his/her own account at any time following the following steps:

- In a web browser enter the address <https://localhost:8443/auth/realms/Bruker/account/password>
- Log in with the personal username and password
- On the page **Password** enter the old and new password
- Click **Save** and then choose **Sign Out**.

User should apply this procedure in order to assign a confidential password which is only known to themselves. In case the password is forgotten, the administrator can reset it through administrator's access.

(The number 8443 stands for the default port number of the Keycloak component which has been set during the installation routine. Use the according number instead if changed during the installation.)

6 Advanced Topics

6.1 Managing Users with Groups

The basic collection of accounts which is set up by the installation routine of TopSpin GxP does not make use of user groups. The roles of the two accounts nmradministrator and nmruser have been directly assigned to the accounts itself. For a small number of accounts this is a suitable approach.

However, for a larger number of users this approach may quickly become inefficient. A best practice then is to manage the roles of users indirectly through user groups. The intended roles are assigned to the groups then, and users get their defined role by being added to the according user group.

Follow these steps in order to create the first group for users with the role Analyst:

- Log in to the Keycloak Administration console as Administrator
- Select the realm Bruker if not already selected
- Choose **Groups**
- Click on **New**, enter the new group name Analysts and click on **Save**
- Select the page **Role Mappings**, and from the box **Client Roles** select **TopSpin**
- Select Analyst from Available Roles and click on **Add selected**

Now all users who become member of the group Analysts will acquire the role Analyst automatically. Review the page **Members** to see all current members. Right after creation of the group this list will be empty, of course.

In order to manage the group membership of an account:

- Select **Users** on the left navigation bar, click **View all users**
- Select the user of your choice, switch to the page **Groups**

- Under the title Available Groups the group name Analysts should be visible. Select this group and click on **Join** in order to set a membership. The button **Leave** would end a membership, respectively.
- Note that accounts can be member of more than just one group.

If you establish this concept, no roles should be assigned to accounts directly in order to keep the overall setup transparent.

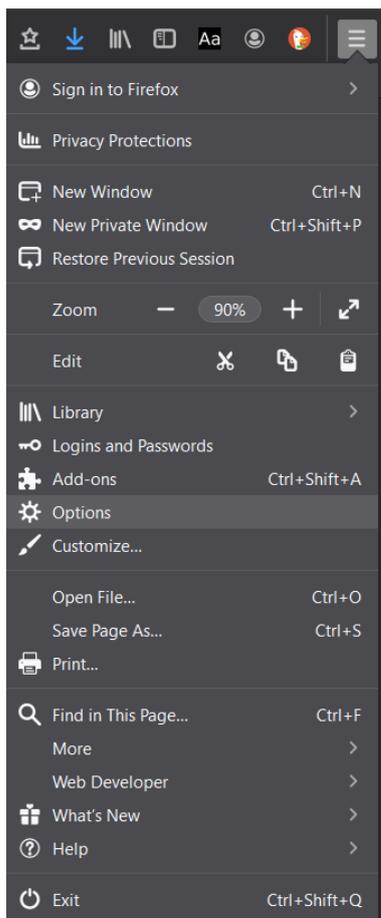
6.2 Remove Warning on Opening Keycloak Administration Console

To enhance internet security, current web browsers prompt security warnings when web pages of unknown origin are opened. Unfortunately this also applies to the local Keycloak administration page.

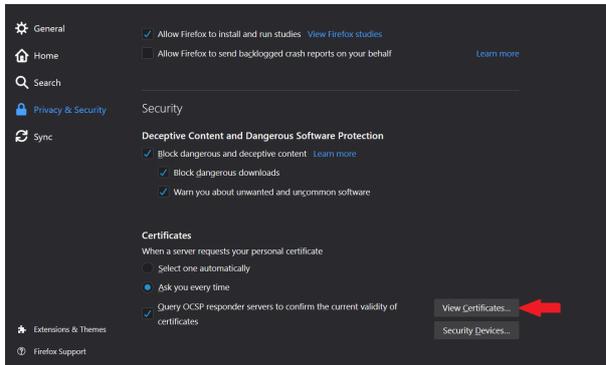
To suppress the warning messages the following steps for common browsers are recommended.

6.2.1 Firefox

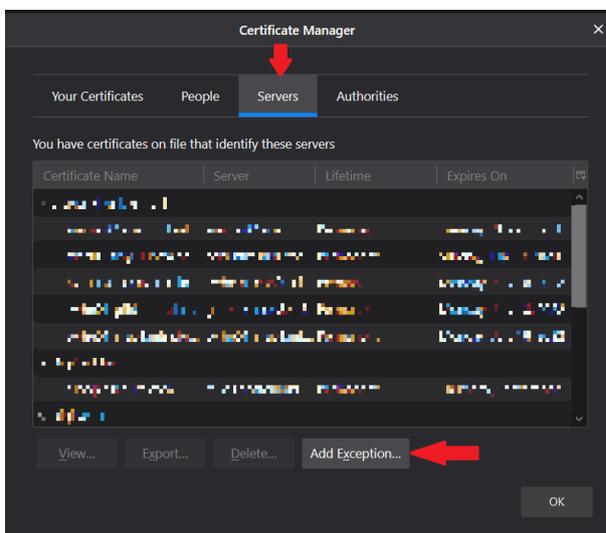
- Open Firefox, click on the menu button on the top right and select options.



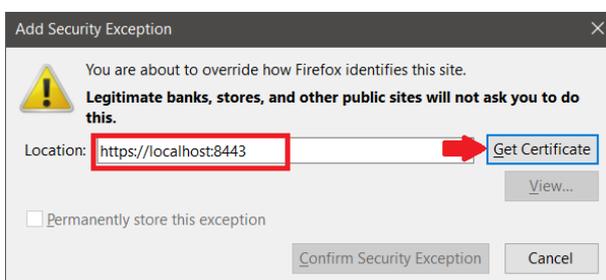
- On the left side bar, navigate to **Privacy and Security**, and scroll down to the Security section, then click on **View Certificates**.



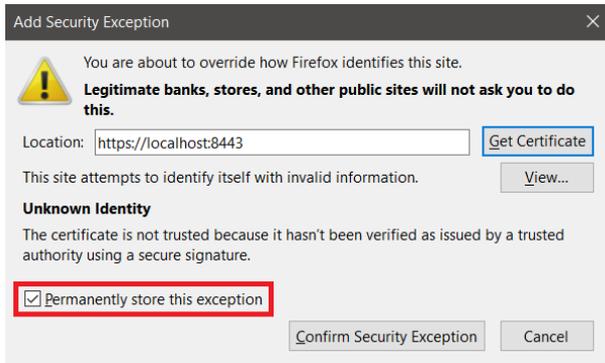
- On the **Certificate Manager** window select the **Servers** tab, and click on the button **Add Exception**.



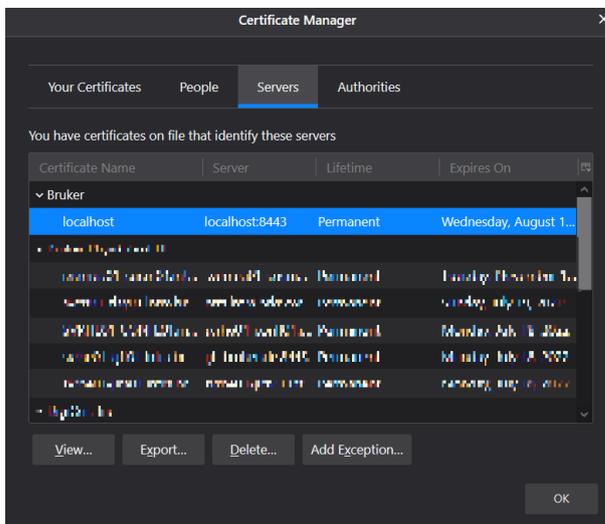
- Enter the URL for the Identity Management (Keycloak) in the **Location** field, using the port which specified for Keycloak during the installation process. If the default port was not changed during the installation, then use port 8443. Then click on **Get Certificate**.



- Keep the check mark for **Permanently store this exception**, or add it if it's not there, then click on **Confirm Security Exception**.



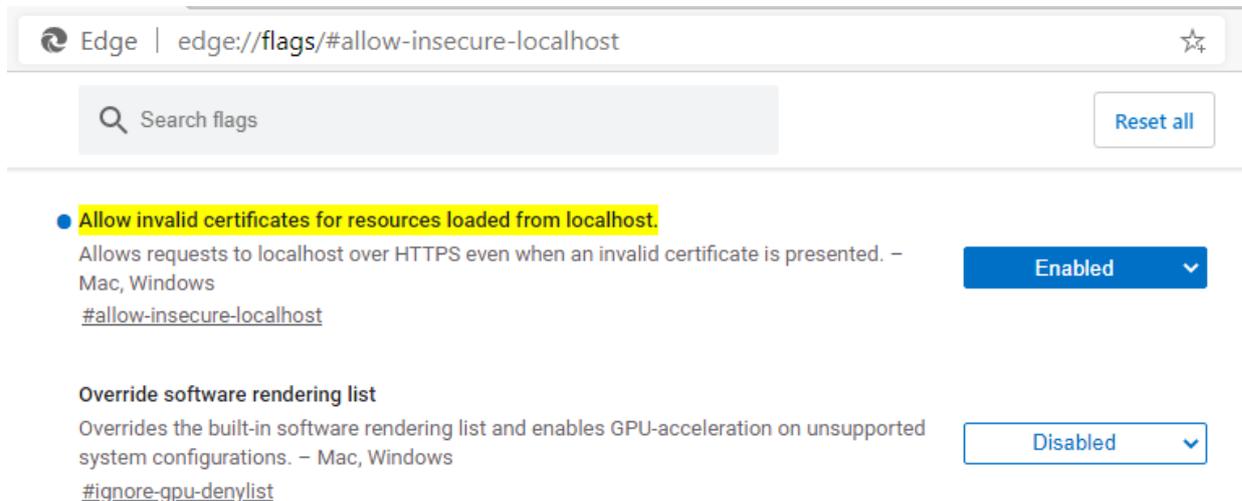
- The new exception should now be visible in the Certificate Manager:



- Now the Keycloak admin console opens directly by using the same location as the certificate. e.g. <https://localhost:8443>.

6.2.2 Edge (Chromium)

Invalid certificates for resources loaded from localhost must be allowed. Therefore, enter `edge://flags/#allow-insecure-localhost` into your browser and on the displayed page set the option **Allow invalid certificates for resources loaded from localhost** to enabled.



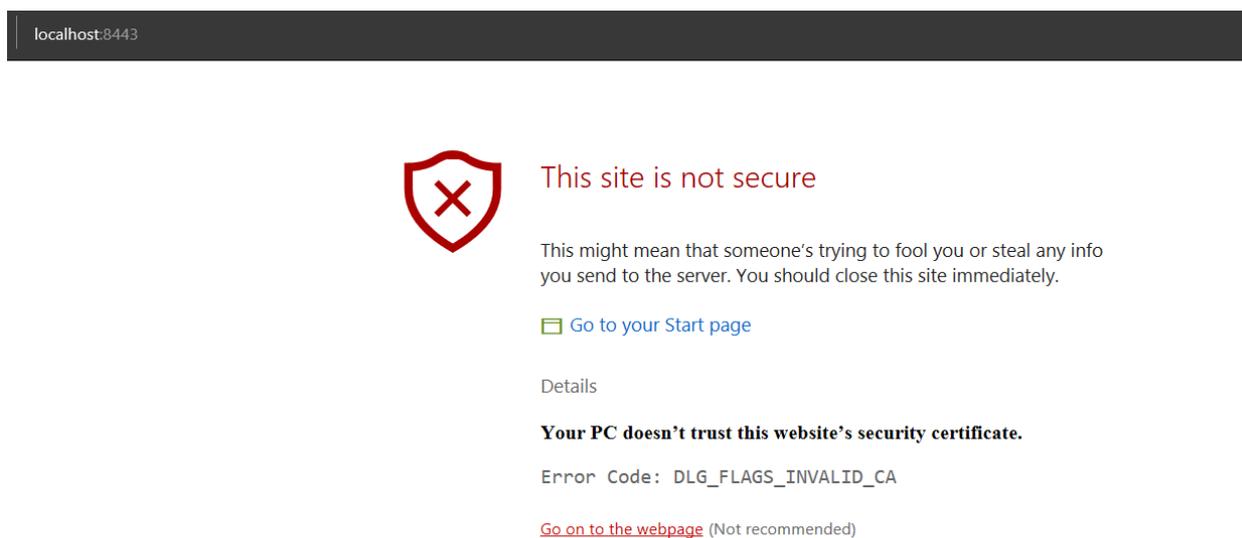
Afterwards Edge needs to be restarted.

6.2.3 Chrome

Same as Edge (Chromium), just enter `chrome://flags/#allow-insecure-localhost` instead.

6.2.4 Edge (Legacy Version)

Upon navigating to the Keycloak page, a warning is displayed:

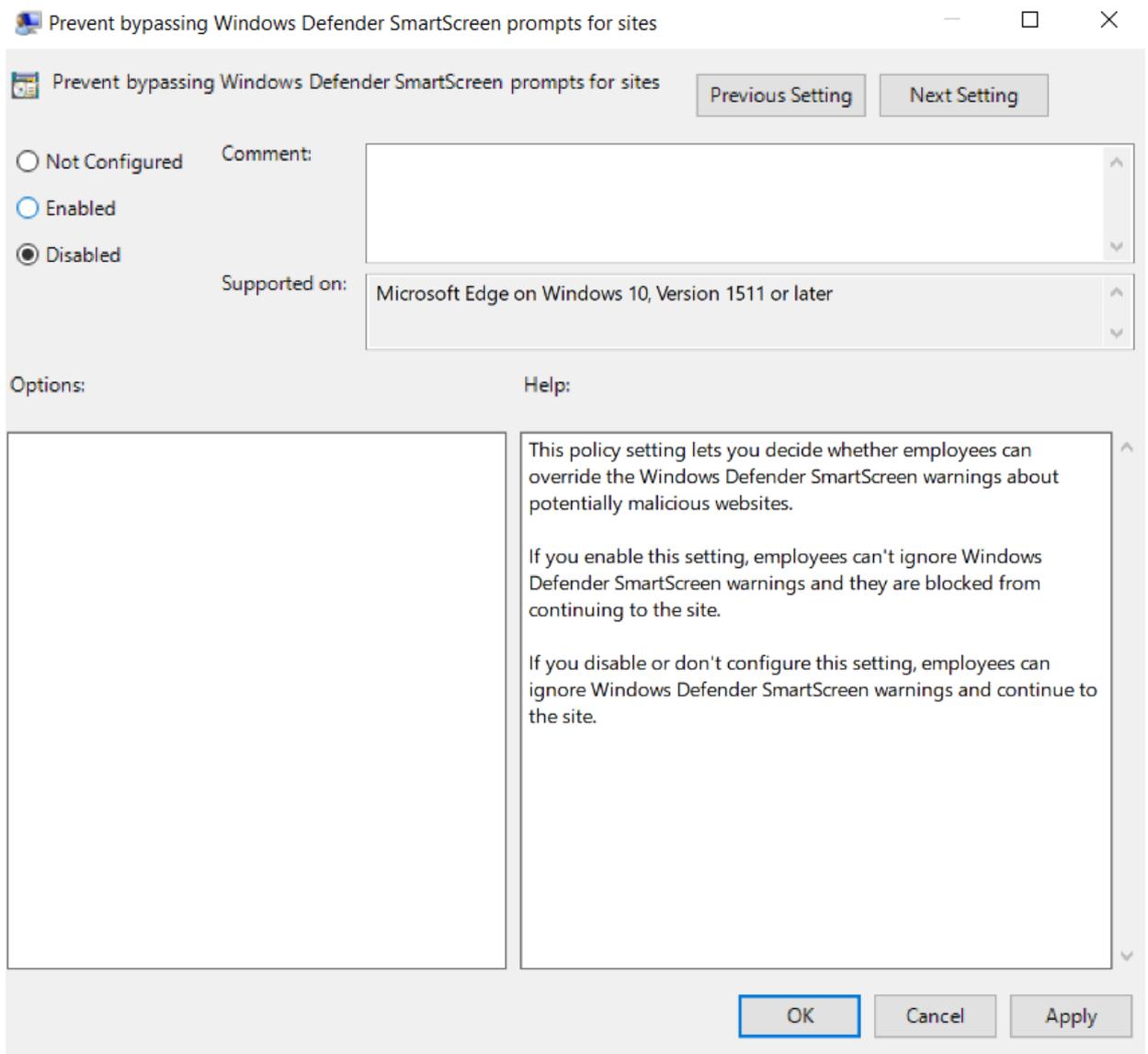


Clicking on the **Go on to the webpage** link at the bottom will open Keycloak, although the certificate warning will remain. In order to work without a security warning, it is recommended to upgrade to the new Chromium-based Edge, or install Firefox or Chrome and follow the instructions above.

6.2.4. What if Edge Prevents Opening Keycloak? 1

The local policy in MS Windows probably prevents overriding the certificate error. To change it:

1. Log in as an administrator
2. Open the **Local Group Policy Editor**, or **Edit Group Policy** from the Control Panel
3. Navigate to: **Computer Configuration\Administrative Templates\Windows Components\Microsoft Edge**
4. Choose **Prevent bypassing Windows Defender SmartScreen Prompts for Sites** and choose **Disabled**. (Depending on the windows version, this option might be named Prevent certificate error overrides.)
5. Apply the changes and close.



6.3 Extended Documentation

Keycloak's functionalities by far extend the ones needed for basic usage in TopSpin GxP. Further information can be found on Keycloak's website <https://www.keycloak.org/> or by searching for other resources on the internet.

7 Contact

Manufacturer

Bruker BioSpin GmbH
Silberstreifen 4
D-76287 Rheinstetten
Germany

E-Mail: nmr-support@bruker.com

<http://www.bruker.com>

WEEE DE43181702

Bruker BioSpin Hotlines

Contact our Bruker BioSpin service centers.

Bruker BioSpin provides dedicated hotlines and service centers, so that our specialists can respond as quickly as possible to all your service requests, applications questions, software or technical needs.

Please select the service center or hotline you wish to contact from our list available at:

<https://www.bruker.com/service/information-communication/helpdesk.html>

 **Bruker Corporation**

info@bruker.com
www.bruker.com



Order No: 1880068