# TopSpin

● GxP - Regulatory Compliance

User Manual

Version 002

Innovation with Integrity

NMR

Document Number:

P/N: H178131

# Contents

**1 Purpose of TopSpin’s GxP Extension ........ 5**

**2 Working with TopSpin ........ 7**

**3 Installation ........ 9**

3.1 Server Installation ........ 10

3.2 Client Installation ........ 13

**4 Central Audit Trail ........ 17**

**5 Data Set Audit Trail ........ 21**

5.1 The Raw Data Audit Trail ........ 21

5.2 The Processed Data Audit Trail ........ 21

5.3 Viewing Audit Trails ........ 22

5.4 Audit Trail Contents ........ 24

5.5 Adding a Comment to an Audit Trail ........ 24

5.6 Auditing User Defined Data Manipulations ........ 25

5.7 Audit Trails in JCAMP-DX and ZIP Archives ........ 25

**6 GUI Settings and Commands ........ 27**

6.1 Preferences for Regulated Environments ........ 27

6.1.1 GUI Restrictions and Protection of Setup Preferences ........ 27

6.1.2 Deletion of Data ........ 27

6.2 Logoff ........ 27

6.3 Locking TopSpin's Graphical User Interface ........ 27

**7 Identity Management ........ 29**

7.1 User Accounts ........ 30

7.1.1 User Attributes ........ 31

7.1.2 Password Expiration for Local Users ........ 32

7.2 Roles ........ 33

7.3 Electronic Signatures ........ 35

7.3.1 Signing a Dataset ........ 35

7.3.2 Structure of a Signature ........ 35

7.3.3 Displaying the Electronic Signature in the Dataset Window ........ 36

7.3.4 Plotting the Electronic Signature ........ 36

7.3.5 Multiple Signatures ........ 36

7.3.6 Validity and Security of Signatures ........ 36

7.4 Using Windows Active Directory Accounts for Identity Management ........ 36

7.5 Create Another Administrative User Account ........ 39

7.6 How to Change/Reset the Password of a User ........ 42

**8 Advanced Topics ........ 43**

8.1 Managing Users with Groups ........ 43

8.2 Remove Warning on Opening Keycloak Administration Console ........ 43

8.2.1 Firefox ........ 43

8.2.2 Edge (Chromium) ........ 46

8.2.3 Chrome ........ 46
8.2.4 Edge (Legacy Version) ........ 46
8.2.4.1 What if Edge Prevents Opening Keycloak? ........ 47
8.3 Extended Documentation........ 48

**9 Contact ........ 49**

# 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. TopSpin complies with the FDA 21 CFR Part 11 regulations. Please refer to the document, accessible under **Help | Manuals | Good Laboratory Practice | 21 CFR Part 11 compliance**.

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.

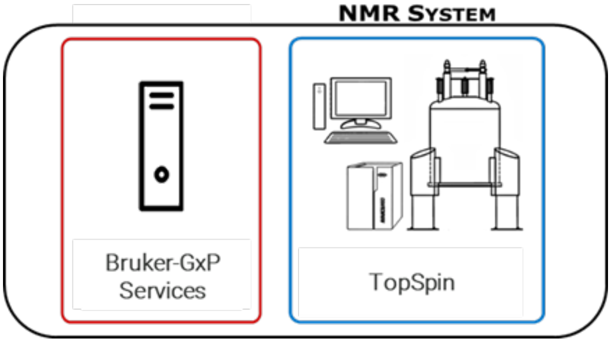
In order to use the GxP extension, a TOPSPIN_GXP_4 license key is required. Topspin installed with the GxP extension does not not start without this license; instead a corresponding error message is shown.

# 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.

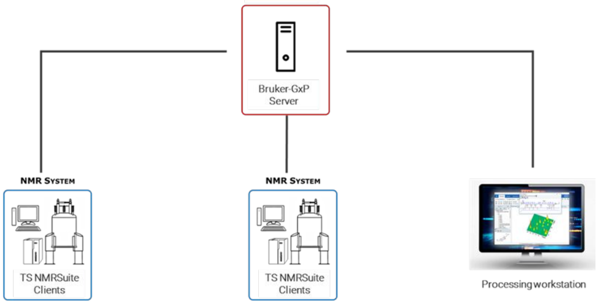
There are two possible deployment scenarios:

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, in such a scenario only Windows OS is supported.

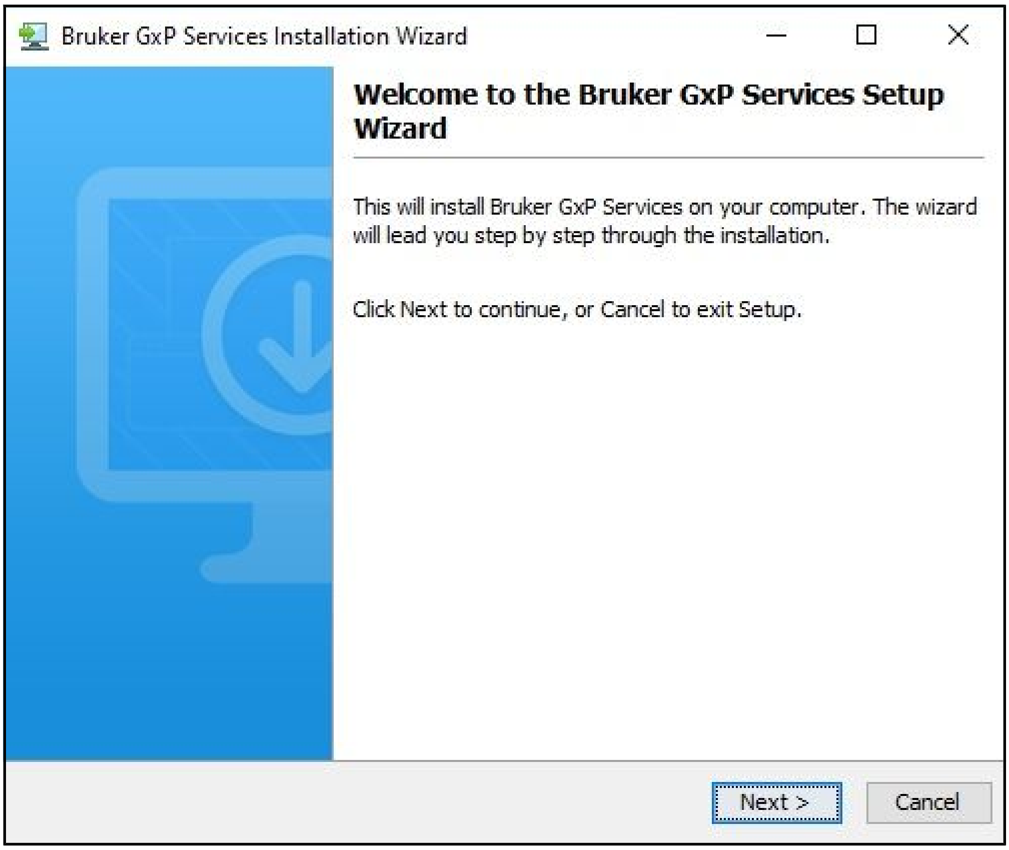
The 2nd case uses a central server for the TopSpin GxP services. Several clients may be connected to this server. All clients share the same Identity Management and write audit records to the same audit trail.



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 must be installed first.



Bruker GxP Services Installation Wizard

**Welcome to the Bruker GxP Services Setup Wizard**

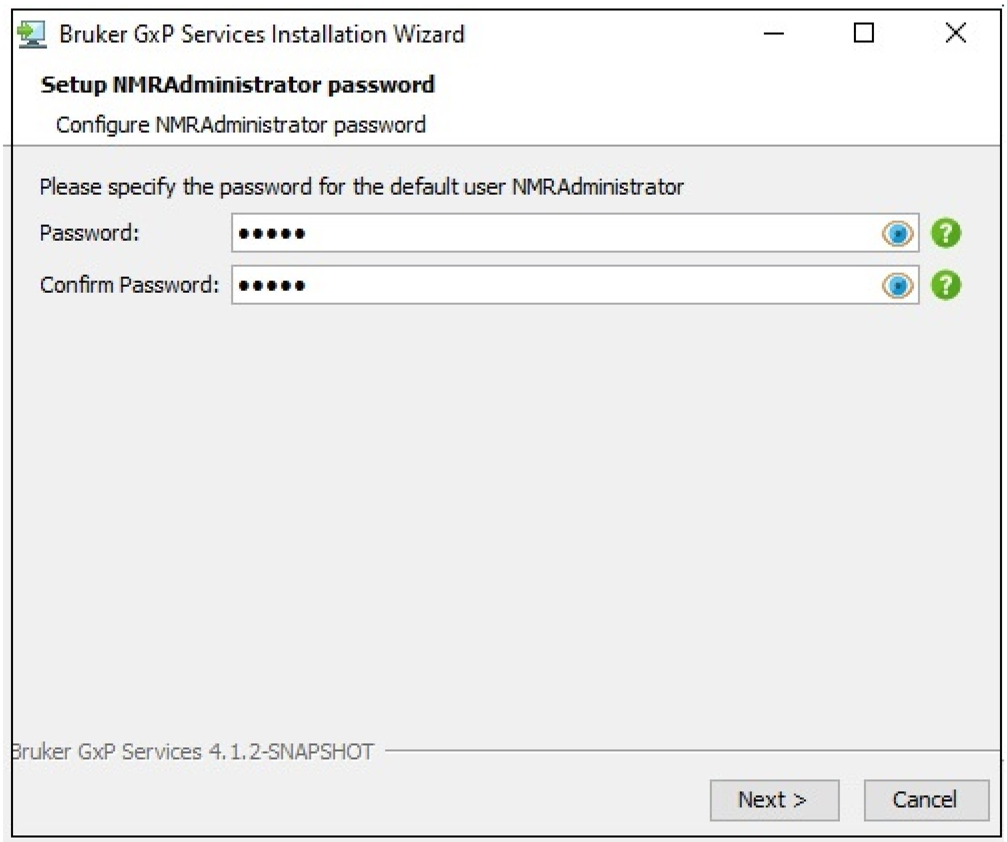
This will install Bruker GxP Services on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

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.



Bruker GxP Services Installation Wizard

**Setup NMRAdministrator password**

Configure NMRAdministrator password

Please specify the password for the default user NMRAdministrator

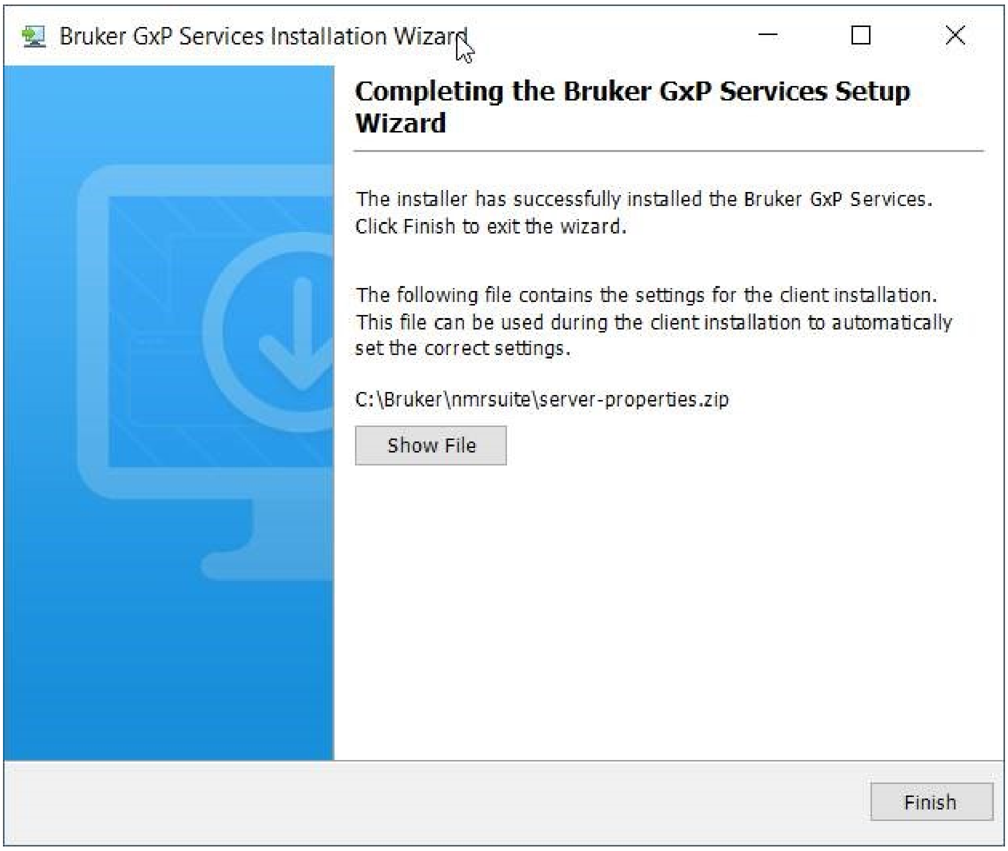
Password: •••••

Confirm Password: •••••

Bruker GxP Services 4.1.2-SNAPSHOT

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 (see *GUI Settings and Commands [▸ 27]* for more details).

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



**Completing the Bruker GxP Services Setup Wizard**

The installer has successfully installed the Bruker GxP Services.
Click Finish to exit the wizard.

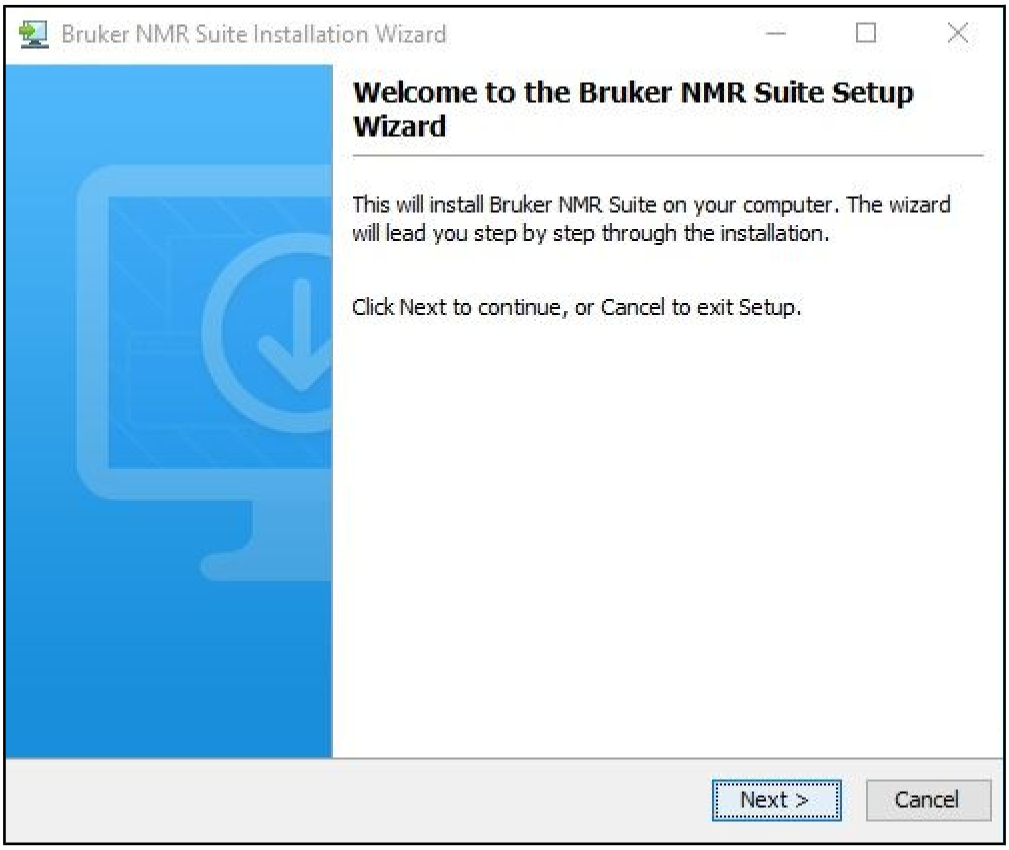
The following file contains the settings for the client installation.
This file can be used during the client installation to automatically set the correct settings.

C:\Bruker\nmrsuite\server-properties.zip

Please note the server settings file. It contains all 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 a different folder.



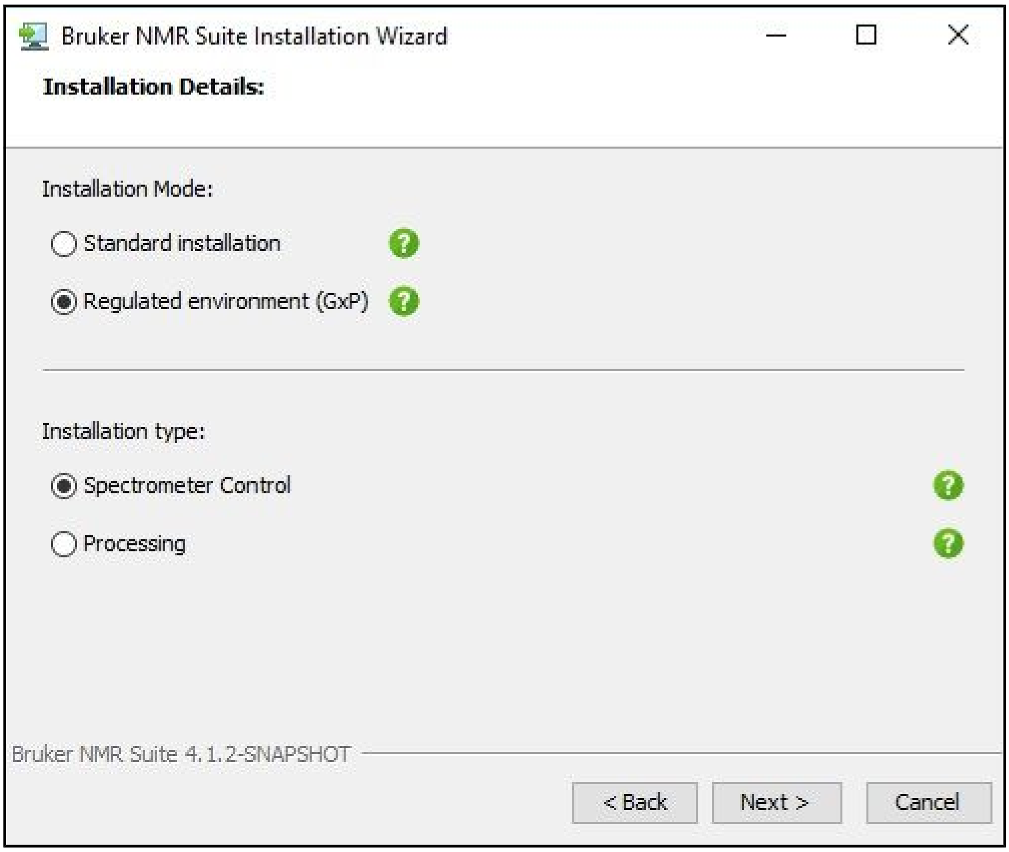
Bruker NMR Suite Installation Wizard

**Welcome to the Bruker NMR Suite Setup Wizard**

This will install Bruker NMR Suite on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

The next step is the selection of installation details.



Bruker NMR Suite Installation Wizard

**Installation Details:**

Installation Mode:

○ Standard installation

● Regulated environment (GxP)

Installation type:

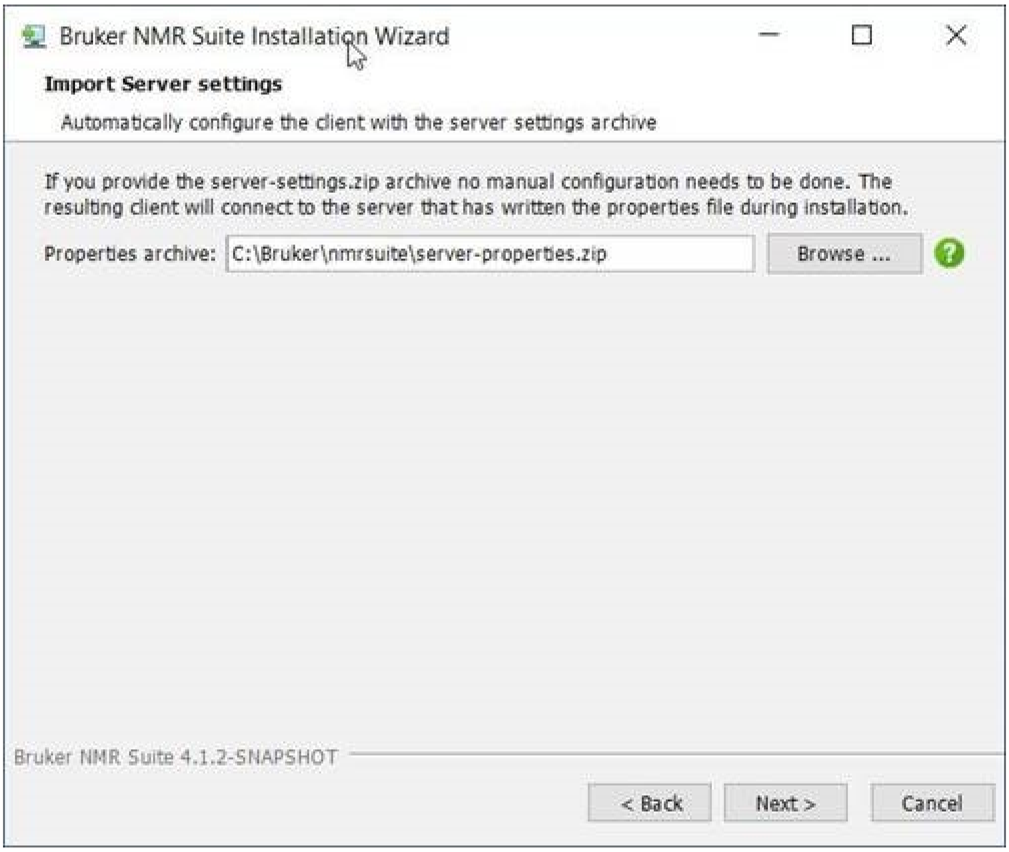
● Spectrometer Control

○ Processing

Bruker NMR Suite 4.1.2-SNAPSHOT

The installation mode (GxP or Standard Installation) cannot be changed if you are upgrading an 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 the server installation. You need to copy this file to the current machine and select its location.



Bruker NMR Suite Installation Wizard

**Import Server settings**

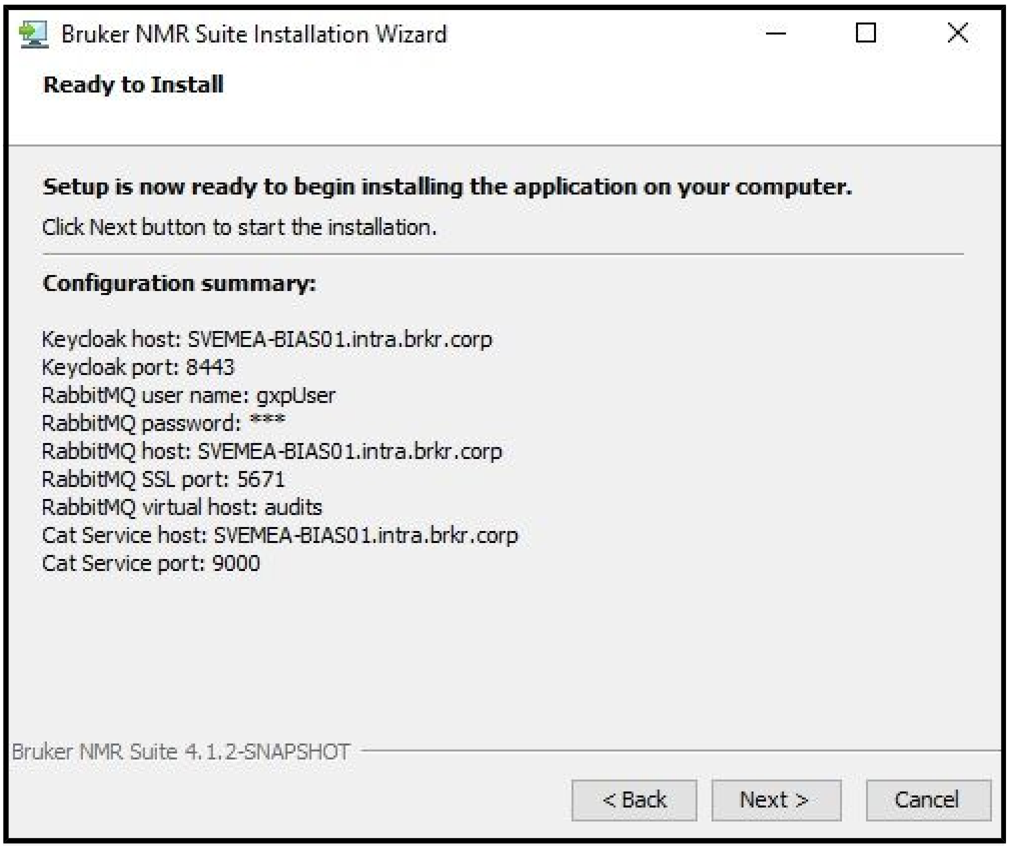
Automatically configure the client with the server settings archive

If you provide the server-settings.zip archive no manual configuration needs to be done. The resulting client will connect to the server that has written the properties file during installation.

Properties archive: C:\Bruker\nmrsuite\server-properties.zip

Browse ...
Bruker NMR Suite 4.1.2-SNAPSHOT
< Back
Next >
Cancel

The next screen summarizes the used server configuration.



**Ready to Install**

**Setup is now ready to begin installing the application on your computer.**

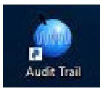
Click Next button to start the installation.

**Configuration summary:**

Keycloak host: SVEMEA-BIAS01.intra.brkr.corp
Keycloak port: 8443
RabbitMQ user name: gxpUser
RabbitMQ password: ***
RabbitMQ host: SVEMEA-BIAS01.intra.brkr.corp
RabbitMQ SSL port: 5671
RabbitMQ virtual host: audits
Cat Service host: SVEMEA-BIAS01.intra.brkr.corp
Cat Service port: 9000

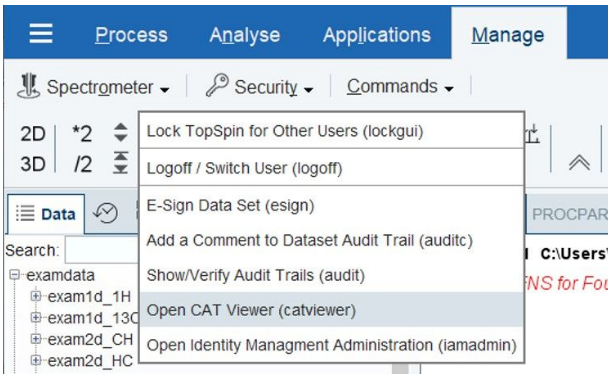
Pressing Next starts the installation of TopSpin GxP.

# 4 Central Audit Trail

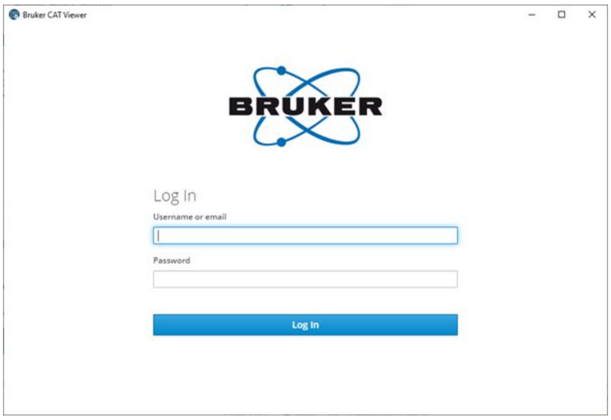


User interactions that create or change data in TopSpin are recorded in a central audit trail database to document who did what and at which point of time. The central audit trail (CAT) collects the data-changing actions of all users referring to any dataset.

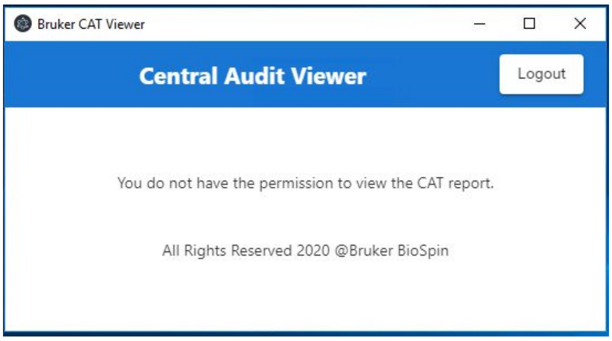
To examine the audit trail records, either launch the central audit trail viewer by double-clicking on the Windows desktop shortcut or directly from TopSpin’s user menu item.


Process
Analyse
Applications
Manage
Spectrometer
Security
Commands
2D
3D
*2
/2
Lock TopSpin for Other Users (lockgui)
Logoff / Switch User (logoff)
E-Sign Data Set (esign)
Add a Comment to Dataset Audit Trail (auditc)
Show/Verify Audit Trails (audit)
Open CAT Viewer (catviewer)
Open Identity Managment Administration (iamadmin)
Data
PROCPAR
Search:
C:\Users
NS for Fou
examdata
exam1d_1H
exam1d_13C
exam2d_CH
exam2d_HC

The central audit trail viewer requires credentials for logging in. Also, not every user account in TopSpin has automatic rights to login to the central audit trail viewer. Please check chapter *Roles [▹ 33]* for detailed information.



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

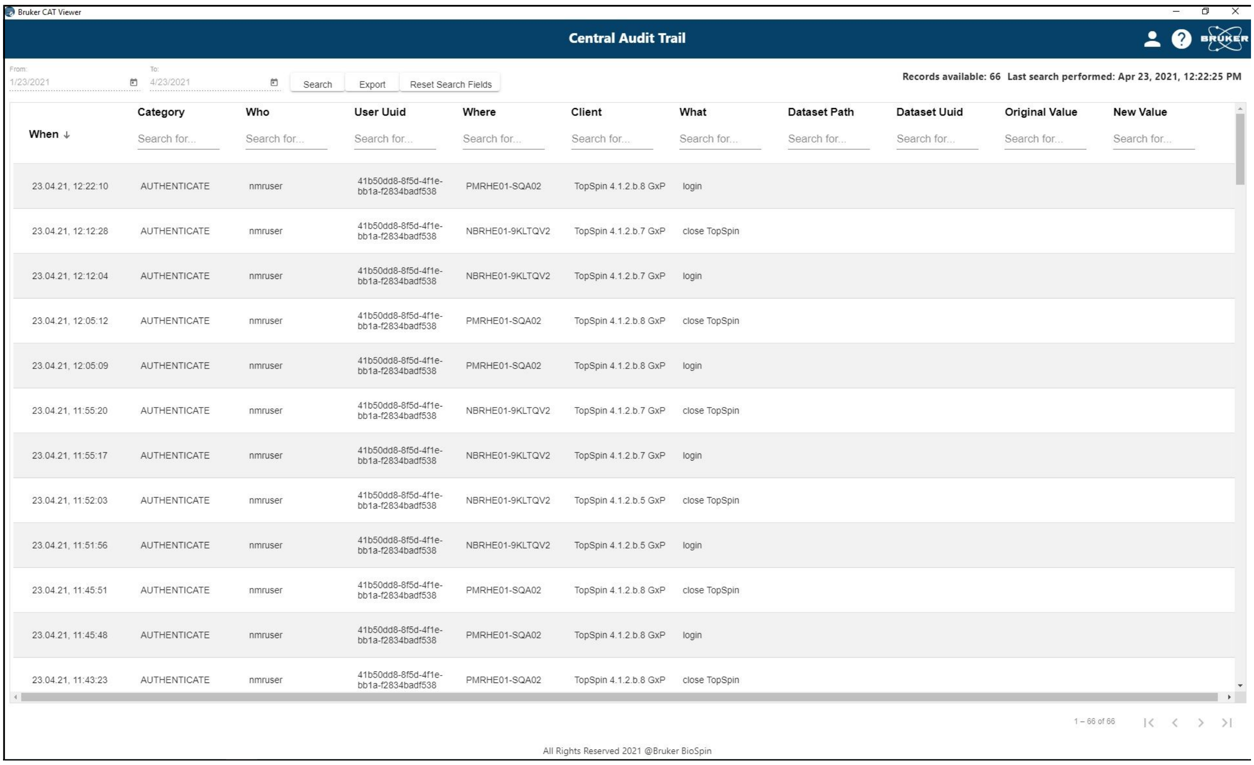


You do not have the permission to view the CAT report.

All Rights Reserved 2020 @Bruker BioSpin

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).



From: 1/23/2021

To: 4/23/2021

Records available: 66  Last search performed: Apr 23, 2021, 12:22:25 PM

| When ↓ | Category | Who | User Uuid | Where | Client | What | Dataset Path | Dataset Uuid | Original Value | New Value |
|---|---|---|---|---|---|---|---|---|---|---|
| | Search for... | Search for... | Search for... | Search for... | Search for... | Search for... | Search for... | Search for... | Search for... | Search for... |
| 23.04.21, 12:22:10 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | PMRHE01-SQA02 | TopSpin 4.1.2.b.8 GxP | login | | | | |
| 23.04.21, 12:12:28 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | NBRHE01-9KLTQV2 | TopSpin 4.1.2.b.7 GxP | close TopSpin | | | | |
| 23.04.21, 12:12:04 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | NBRHE01-9KLTQV2 | TopSpin 4.1.2.b.7 GxP | login | | | | |
| 23.04.21, 12:05:12 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | PMRHE01-SQA02 | TopSpin 4.1.2.b.8 GxP | close TopSpin | | | | |
| 23.04.21, 12:05:09 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | PMRHE01-SQA02 | TopSpin 4.1.2.b.8 GxP | login | | | | |
| 23.04.21, 11:55:20 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | NBRHE01-9KLTQV2 | TopSpin 4.1.2.b.7 GxP | close TopSpin | | | | |
| 23.04.21, 11:55:17 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | NBRHE01-9KLTQV2 | TopSpin 4.1.2.b.7 GxP | login | | | | |
| 23.04.21, 11:52:03 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | NBRHE01-9KLTQV2 | TopSpin 4.1.2.b.5 GxP | close TopSpin | | | | |
| 23.04.21, 11:51:56 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | NBRHE01-9KLTQV2 | TopSpin 4.1.2.b.5 GxP | login | | | | |
| 23.04.21, 11:45:51 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | PMRHE01-SQA02 | TopSpin 4.1.2.b.8 GxP | close TopSpin | | | | |
| 23.04.21, 11:45:48 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | PMRHE01-SQA02 | TopSpin 4.1.2.b.8 GxP | login | | | | |
| 23.04.21, 11:43:23 | AUTHENTICATE | nmruser | 41b50dd8-8f5d-4f1e-bb1a-f2834badf538 | PMRHE01-SQA02 | TopSpin 4.1.2.b.8 GxP | close TopSpin | | | | |

1 – 66 of 66

All Rights Reserved 2021 @Bruker BioSpin

Each record in the CAT contains a series of meta data items, which are listed here from left to right.

Each record contains a timestamp (When), a Category to which user interactions belong and the name of the user account (Who) 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.

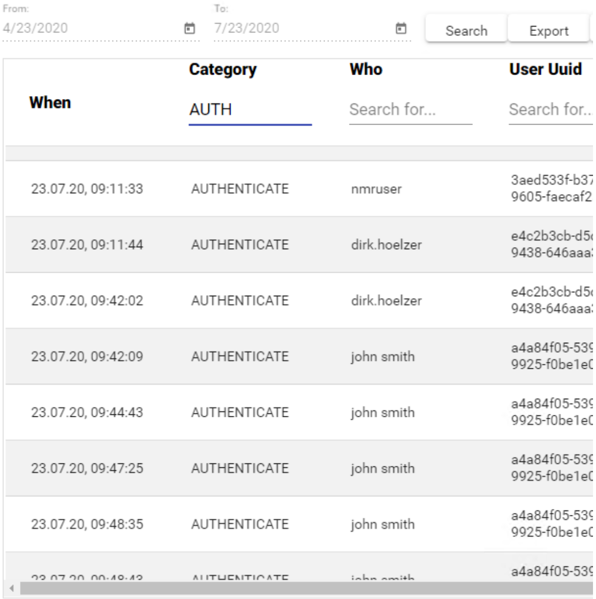
**Where**: The central audit trail can be the common audit trail database for all Bruker NMR spectrometers in a laboratory or on a site. Therefore, the column **Where** specifies which workstation was used to execute the action described in the **What** column.

**Client** defines the software the user interacted with. This is typically TopSpin but other Bruker products will also write to the central audit trail file in the future.

**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 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.



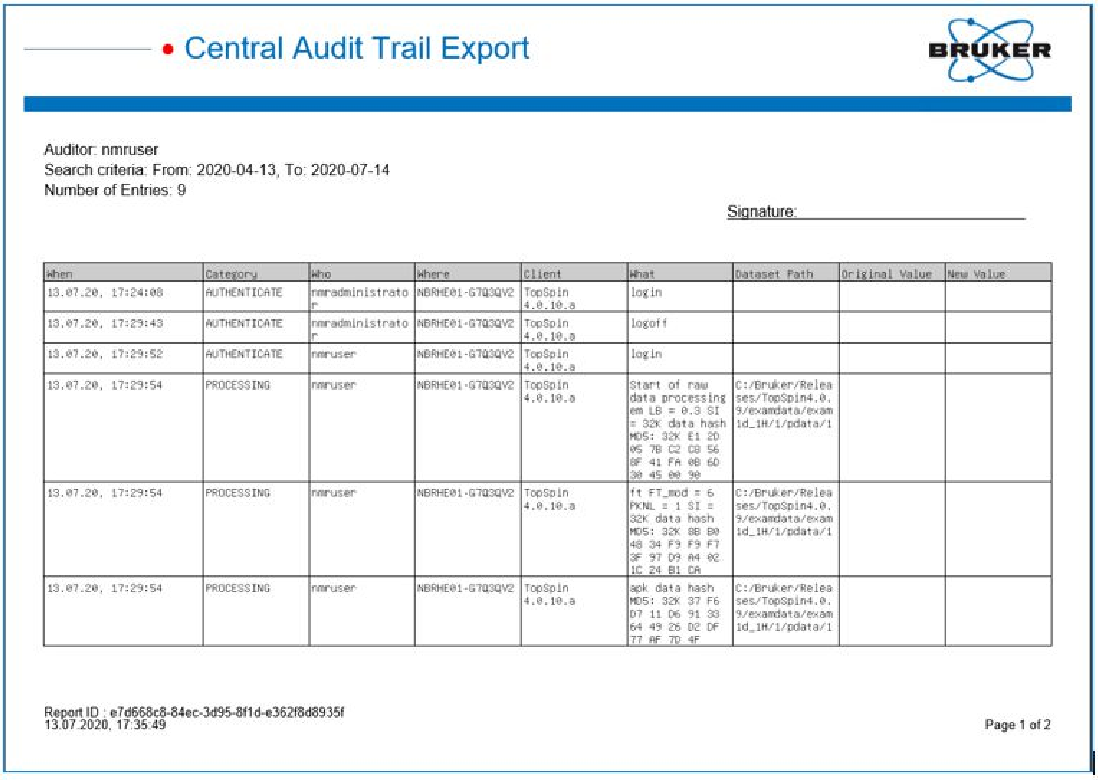
| When | Category | Who | User Uuid |
|---|---|---|---|
| | AUTH | Search for... | Search for.. |
| 23.07.20, 09:11:33 | AUTHENTICATE | nmruser | 3aed533f-b37<br>9605-faecaf2 |
| 23.07.20, 09:11:44 | AUTHENTICATE | dirk.hoelzer | e4c2b3cb-d5<br>9438-646aaa |
| 23.07.20, 09:42:02 | AUTHENTICATE | dirk.hoelzer | e4c2b3cb-d5<br>9438-646aaa |
| 23.07.20, 09:42:09 | AUTHENTICATE | john smith | a4a84f05-539<br>9925-f0be1e |
| 23.07.20, 09:44:43 | AUTHENTICATE | john smith | a4a84f05-539<br>9925-f0be1e |
| 23.07.20, 09:47:25 | AUTHENTICATE | john smith | a4a84f05-539<br>9925-f0be1e |
| 23.07.20, 09:48:35 | AUTHENTICATE | john smith | a4a84f05-539<br>9925-f0be1e |
| 23.07.20, 09:48:43 | AUTHENTICATE | john smith | a4a84f05-539 |

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 can be exported to a PDF document in order to store it separately or to 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 | logoff | | | |
| 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 MD5: 32K E1 2D 05 7B C2 C8 56 8F 41 FA 0B 6D 30 45 00 90 | C:/Bruker/Releases/TopSpin4.0.9/examdata/exam1d_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 MD5: 32K 8B B0 48 34 F9 F9 F7 3F 97 D9 A4 02 1C 24 B1 CA | C:/Bruker/Releases/TopSpin4.0.9/examdata/exam1d_1H/1/pdata/1 | | |
| 13.07.20, 17:29:54 | PROCESSING | nmruser | NBRHE01-G7Q3QV2 | TopSpin 4.0.10.a | apk data hash MD5: 32K 37 F6 D7 11 D6 91 33 64 49 26 D2 DF 77 AF 7D 4F | C:/Bruker/Releases/TopSpin4.0.9/examdata/exam1d_1H/1/pdata/1 | | |

Report ID : e7d668c8-84ec-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 Data Set Audit Trail

## 5.1 The Raw Data Audit Trail

Each *expno* sub-directory contains a text file *audita.txt*, the audit trail of the raw data. This reflects the acquisition state of the raw data and contains a checksum for the file itself (audita.txt) and one for the raw data file (fid or ser). The latter checksum links the audit file with the raw data. By means of the checksums, any illegal manipulation of the audit file or the raw data file can be detected, using the TopSpin commands **audit** or **auditcheck**. Whenever an acquisition is started, the possibly existing audit file is overwritten by a new one, belonging to the new raw data file. By default, the user is warned when the current dataset already contains raw data, thus preventing accidental overwriting (The option “Override existing fid without inquiry” is, by default, **OFF**.

To change this option,

- Check **Setup Preferences  | Acquisition | Overwrite existing FID without inquiry (ZG safety off)**.

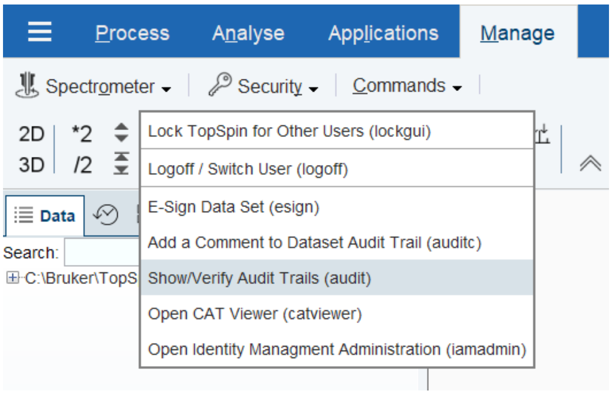
## 5.2 The Processed Data Audit Trail

Each *procno* sub-directory contains a text file *auditp.txt*, the audit trail of the processed data. It reflects the processing state of the processed data and contains a checksum for the file itself (*auditp.txt*), and a checksum for the real processed data files (*1r*, *2rr*, *3rrr*, ...). The latter checksum links the audit file with the processed data. By means of the checksums, any illegal manipulation of the audit file or the processed data file can be detected, using the TopSpin commands **audit** or **auditcheck**. Whenever a processing command is performed, the current audit file is updated with this command and its associated parameters. When processing starts from scratch (from a raw data file), the existing audit file is overwritten. As such, the processed data can always be regenerated from raw data by applying the commands and parameters listed in the audit trail.

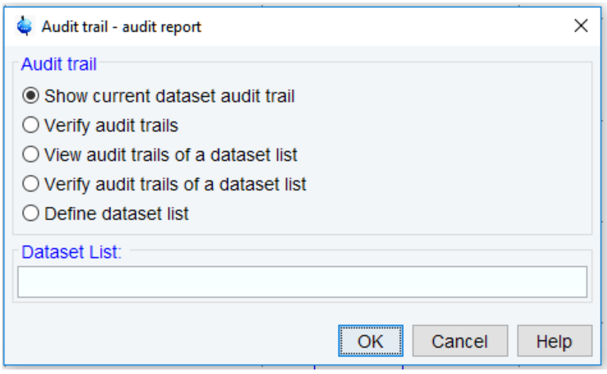
If the laboratory management does not allow data files or audit trails to be deleted, a respective saving procedure must be established. For this purpose, TopSpin provides data copying commands, which may be called in a user defined macro or AU program, before a new acquisition or processing starts.

## 5.3 Viewing Audit Trails

Since audit trails are regular ASCII text files, they can be viewed or printed with any text editor, outside of TopSpin. Within TopSpin, you can use the command **audit** or click **Manage | Security | Show/Verify Audit Trails**.


Process
Analyse
Applications
Manage
Spectrometer
Security
Commands
2D
3D
*2
/2
Data
Search:
C:\Bruker\TopS
Lock TopSpin for Other Users (lockgui)
Logoff / Switch User (logoff)
E-Sign Data Set (esign)
Add a Comment to Dataset Audit Trail (auditc)
Show/Verify Audit Trails (audit)
Open CAT Viewer (catviewer)
Open Identity Managment Administration (iamadmin)

This opens the dialog box:

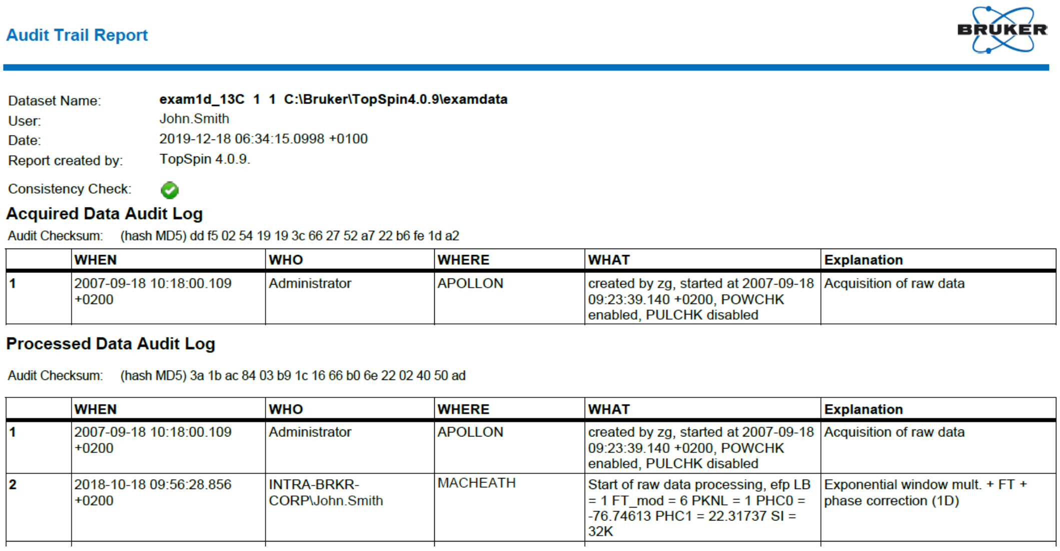

Audit trail - audit report

Audit trail

● Show current dataset audit trail
○ Verify audit trails
○ View audit trails of a dataset list
○ Verify audit trails of a dataset list
○ Define dataset list

Dataset List:

Selection **Show current dataset audit trail** provides an Audit Trail Report PDF, for example:


Audit Trail Report

| | |
|---|---|
| Dataset Name: | **exam1d_13C 1 1 C:\Bruker\TopSpin4.0.9\examdata** |
| User: | John.Smith |
| Date: | 2019-12-18 06:34:15.0998 +0100 |
| Report created by: | TopSpin 4.0.9. |
| Consistency Check: | ✓ |

**Acquired Data Audit Log**

Audit Checksum: (hash MD5) dd f5 02 54 19 19 3c 66 27 52 a7 22 b6 fe 1d a2

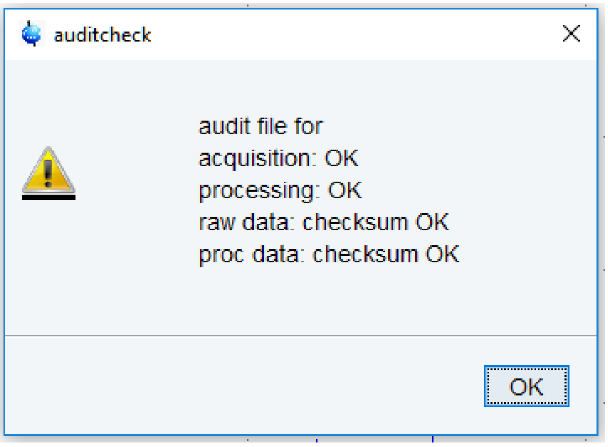
| | WHEN | WHO | WHERE | WHAT | Explanation |
|---|---|---|---|---|---|
| **1** | 2007-09-18 10:18:00.109 +0200 | Administrator | APOLLON | created by zg, started at 2007-09-18 09:23:39.140 +0200, POWCHK enabled, PULCHK disabled | Acquisition of raw data |

**Processed Data Audit Log**

Audit Checksum: (hash MD5) 3a 1b ac 84 03 b9 1c 16 66 b0 6e 22 02 40 50 ad

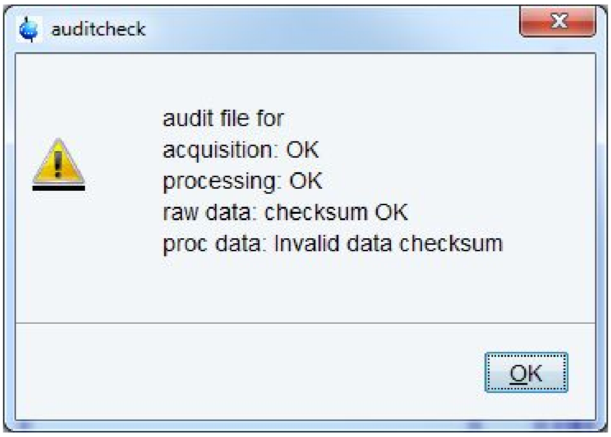
| | WHEN | WHO | WHERE | WHAT | Explanation |
|---|---|---|---|---|---|
| **1** | 2007-09-18 10:18:00.109 +0200 | Administrator | APOLLON | created by zg, started at 2007-09-18 09:23:39.140 +0200, POWCHK enabled, PULCHK disabled | Acquisition of raw data |
| **2** | 2018-10-18 09:56:28.856 +0200 | INTRA-BRKR-CORP\John.Smith | MACHEATH | Start of raw data processing, efp LB = 1 FT_mod = 6 PKNL = 1 PHC0 = -76.74613 PHC1 = 22.31737 SI = 32K | Exponential window mult. + FT + phase correction (1D) |

Selection **Verify audit trails** performs an audit trail check, i.e. a data consistency check. If both raw and processed data are consistent, a message is displayed:



audit file for
acquisition: OK
processing: OK
raw data: checksum OK
proc data: checksum OK

If the data have been manipulated outside of TopSpin, e.g. with third party software, the checksum will be inconsistent. The next figure shows the message for inconsistent processed data.

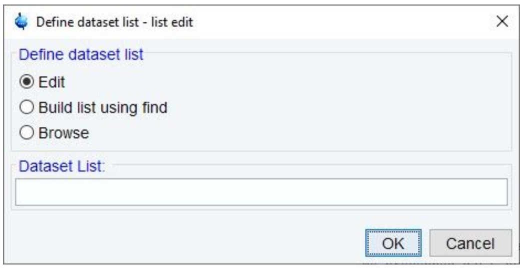


audit file for
acquisition: OK
processing: OK
raw data: checksum OK
proc data: Invalid data checksum

Selection **View audit trails of a dataset list** provides an Audit Trail Report PDF of a list of datasets. This list can be created using the option **Define dataset list**.

Selection **Verify audit trails of a dataset list** performs an audit trail check, i.e. a data consistency check, on a list of datasets. This list can be created using the option **Define dataset list**.

Selection **Define dataset list** allows to create a dataset list in three different ways as shown in the screenshot below.



## 5.4 Audit Trail Contents

The contents of an audit file are grouped in the following way:

(NUMBER, WHEN, WHO, WHERE, PROCESS, VERSION, WHAT)

These entries have the following meaning:

**NUMBER**

Running number of an entry, starting with 1.

**WHEN**

Date of the entry, e.g. <2004-03-30 10:55:36.171 +0200>, where the last value represents the offset in hours to Universal Time (UTC).

**WHO**

The user logged in, at the time the entry was generated. It has one of the two forms: <user1> or <user1/user2>. The user <user1> is always the user who is logged into the operating system (Windows or Linux user), and who started TopSpin. <user2> is the internal username with which Topspin was started (see *Identity Management [▸ 29]* for more details).

**WHERE**

The network name of the current computer, e.g. <EOS2>.

**PROCESS**

The TopSpin process (module) which performed the acquisition or processing.

**VERSION**

The TopSpin version which performed the acquisition or processing.

**WHAT**

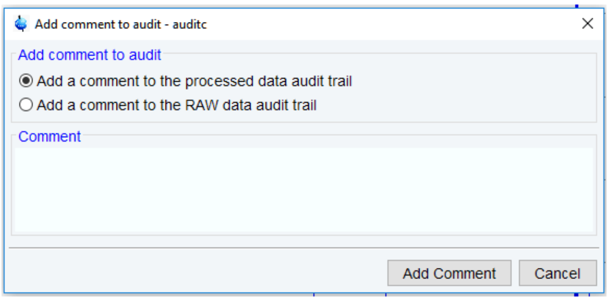
The type of acquisition or data manipulation performed.

Note that if only the entries NUMBER, WHEN, WHO, WHERE, WHAT are present, then the audit trail was created by TopSpin 1.3 or older.

## 5.5 Adding a Comment to an Audit Trail

Audit trail entries are normally generated automatically by a respective acquisition or processing command. However, a user can also add a comment manually, using the **auditc** command. This is available either from the command line, or from the menu under **Manage | Security | Add a comment to dataset audit trail (auditc)**.

A dialog is opened allowing to enter the comment and the target component (RAW or processed data).



Add comment to audit - auditc

Add comment to audit

● Add a comment to the processed data audit trail
○ Add a comment to the RAW data audit trail

Comment

You may also add a comment to the raw data or processed data audit trail from an AU program, using the macros AUDITCOMMENTA(comment) or AUDITCOMMENTP(comment), respectively.

## 5.6 Auditing User Defined Data Manipulations

Customer using their own AU programs to manipulate the data in any way may write their own audit entries. The details are described in the AU programming manual under **Help | Manuals | Programming Manuals | AU programming.**

## 5.7 Audit Trails in JCAMP-DX and ZIP Archives

The TopSpin commands **tojdx** and **tozip** allow to store a dataset into a single file in the internationally standardized ASCII-type JCAMP-DX format or in the well-known ZIP format. Both storage formats retain the audit trails. When unpacking such files with **fromjdx** or **fromzip**, the original dataset in standard Bruker format is restored. The command **auditcheck** may be used to check whether the data are still consistent. If, for example, JCAMP-DX or ZIP file have been manipulated, the data might not be consistent.

# 6 GUI Settings and Commands

## 6.1 Preferences for Regulated Environments

### 6.1.1 GUI Restrictions and Protection of Setup Preferences

To avoid that everyone can access and administer the setup preferences you can

- enable **Setup Preferences | Regulated Environments | Enable GUI restrictions and protection of preferences**

This assures that modifications in the setup preferences are possible only for users who know the NMR administration password.

### 6.1.2 Deletion of Data

By default, data deletion is not possible when TopSpin has been installed with the GxP extension. Nevertheless, there are some used cases for specific applications that are linked to certain users and their roles where data deletion may be permitted. Two different delete options can be allowed by checking the respective item in the Preferences.

- Check **Setup Preferences | Regulated Environments | Disable options for deletion of RAW data**

if you want to permit to only delete raw (acquired) data.

- Check **Setup Preferences | Regulated Environments | Disable options for deletion of data sets in general**

if you want to permit to delete raw (acquired) and processed data.

## 6.2 Logoff

To log off the internal user:

- Click **Manage | Security | Logoff / Switch User (logoff)**

or

- enter **logoff**.

TopSpin will immediately log the current user off and prompt with a new login window. TopSpin is locked until a user logs in.

## 6.3 Locking TopSpin's Graphical User Interface

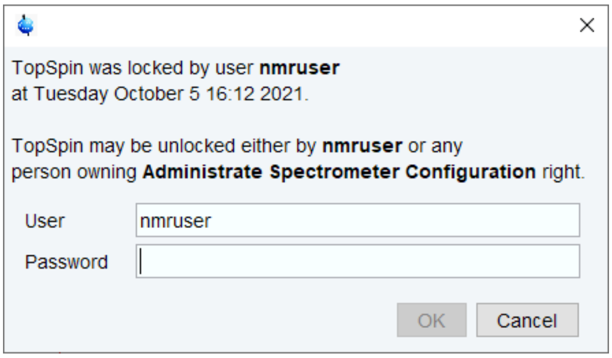
TopSpin can be locked, such that it does no longer accept user input via mouse or keyboard.

- Click **Manage | Security | Lock TopSpin for Other Users**

  or

- enter **lockgui**.

A window will appear indicating the locked status and the user name who will be allowed to unlock TopSpin again. Note that also the NMRAdministrator can unlock TopSpin.



TopSpin was locked by user **nmruser**
at Tuesday October 5 16:12 2021.

TopSpin may be unlocked either by **nmruser** or any person owning **Administrate Spectrometer Configuration** right.

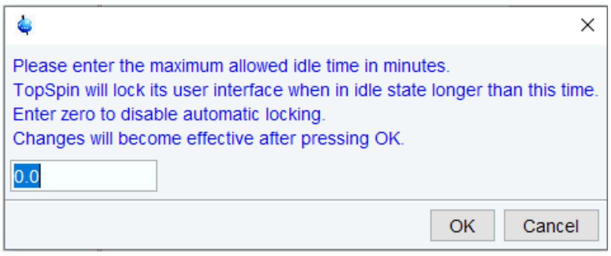
User nmruser

Password

While TopSpin is locked, all background activities such as data acquisition and processing continue.

For safety reasons TopSpin can be forced to execute **lockgui** automatically when no commands from the command line, menus or toolbar buttons have been entered for a certain period (for instance because the current user has left). In order to enable automatic locking:

- Click **Setup Preferences Administration Items | Automatic locking of TopSpin when idle time exceeded | Change**
- Enter the maximum allowed idle time (in minutes) in the dialog and click **OK**.

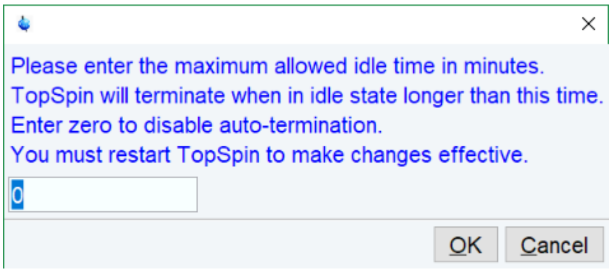


Please enter the maximum allowed idle time in minutes.
TopSpin will lock its user interface when in idle state longer than this time.
Enter zero to disable automatic locking.
Changes will become effective after pressing OK.

0.0

Note that you can also set in Preferences a time after which TopSpin automatically exits.

- Click **Setup Preferences Administration Items | Automatic termination of TopSpin when idle time exceeded | Change**
- Enter the maximum allowed idle time (in minutes) in the dialog and click **OK**.



Please enter the maximum allowed idle time in minutes.
TopSpin will terminate when in idle state longer than this time.
Enter zero to disable auto-termination.
You must restart TopSpin to make changes effective.

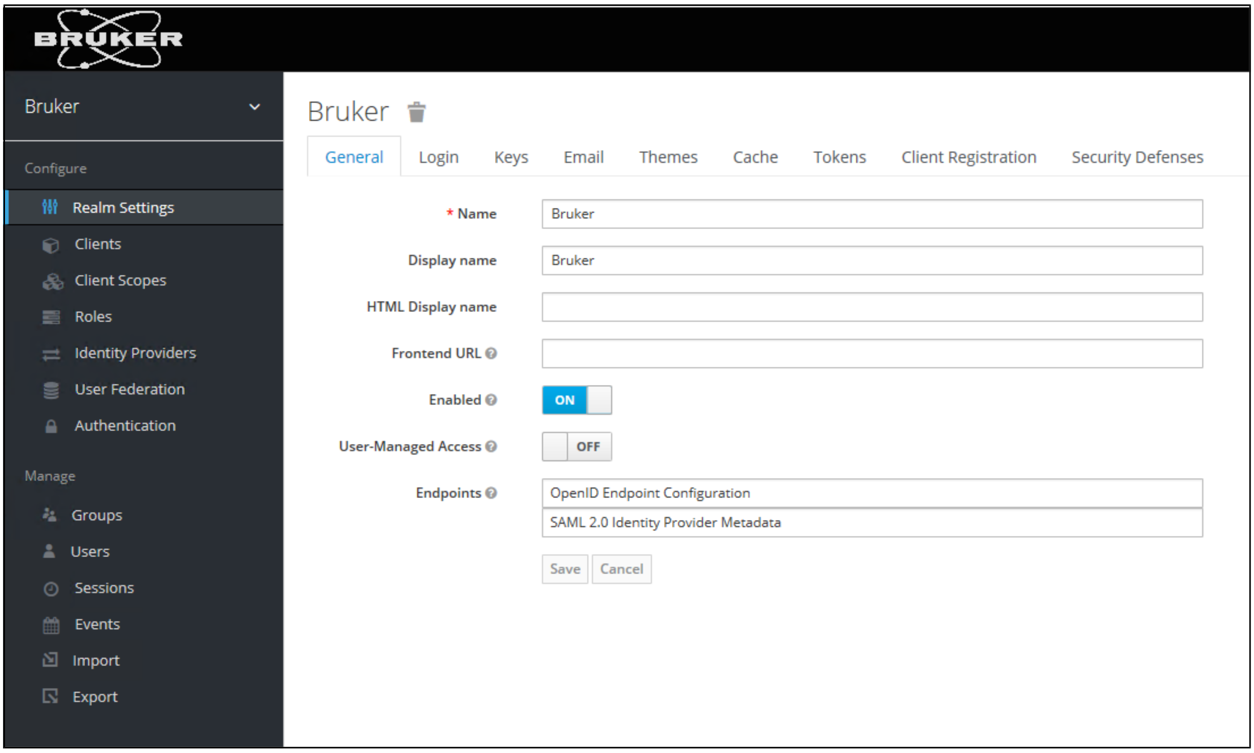
0

# 7 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* [▹ 9]).
- Select the realm “Bruker” which contains the necessary pre-configurations.



* Name: Bruker

Display name: Bruker

HTML Display name:

Frontend URL:

Enabled: ON

User-Managed Access: OFF

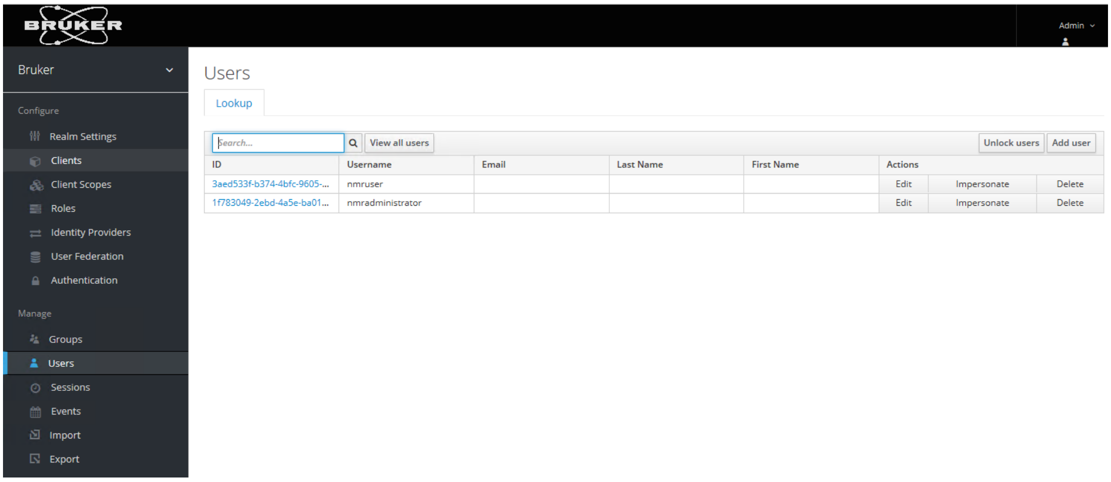
Endpoints: OpenID Endpoint Configuration<br>SAML 2.0 Identity Provider Metadata

## 7.1 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 *Server Installation* [▹ 10]).

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

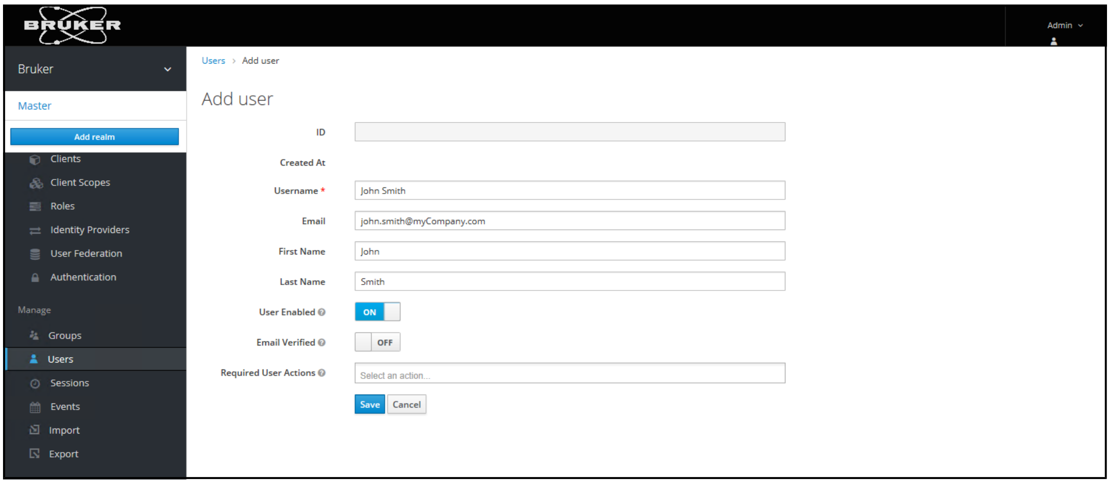
Note that TopSpin passwords are upper/lowercase sensitive.



| ID | Username | Email | Last Name | First Name | Actions | | |
|---|---|---|---|---|---|---|---|
| 3aed533f-b374-4bfc-9605-... | nmruser | | | | Edit | Impersonate | Delete |
| 1f783049-2ebd-4a5e-ba01... | nmradministrator | | | | Edit | Impersonate | Delete |

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* [▹ 33].



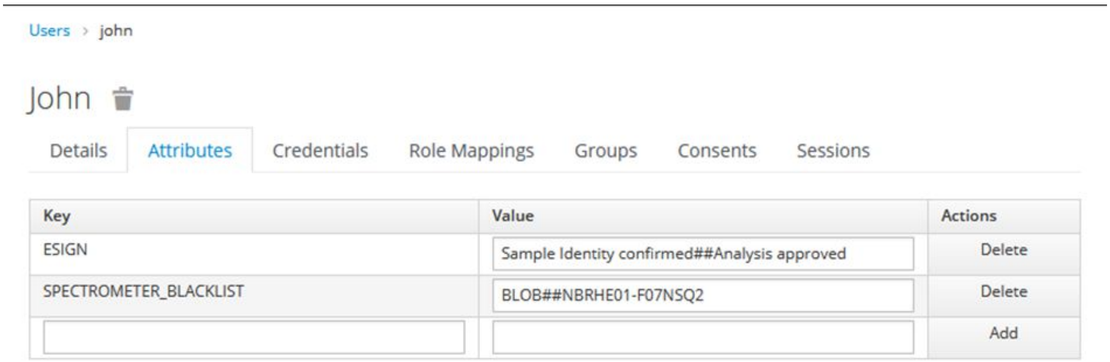
Add user

| | |
|---|---|
| ID | |
| Created At | |
| Username * | John Smith |
| Email | john.smith@myCompany.com |
| First Name | John |
| Last Name | Smith |
| User Enabled | ON |
| Email Verified | OFF |
| Required User Actions | Select an action... |

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

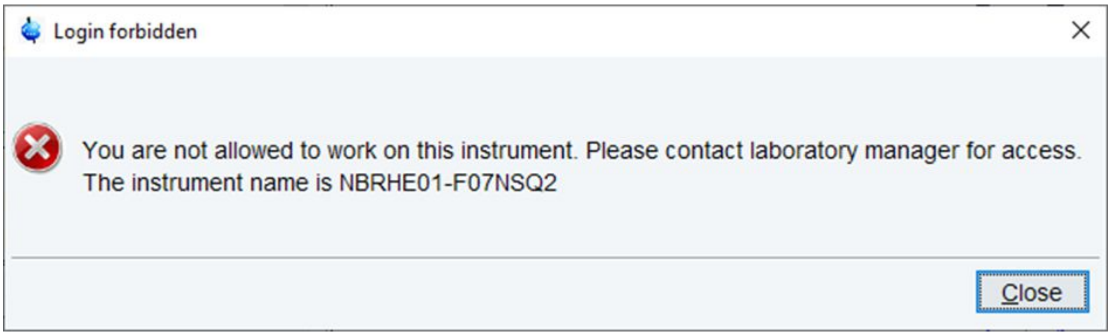
## 7.1.1 User Attributes

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.



| Key | Value | Actions |
|---|---|---|
| ESIGN | Sample Identity confirmed##Analysis approved | Delete |
| SPECTROMETER_BLACKLIST | BLOB##NBRHE01-F07NSQ2 | Delete |
| | | 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.



Login forbidden

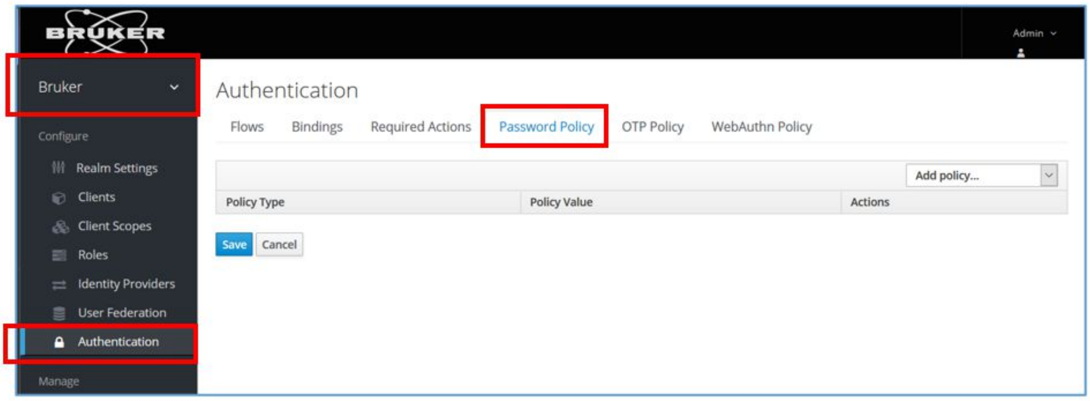
You are not allowed to work on this instrument. Please contact laboratory manager for access.
The instrument name is NBRHE01-F07NSQ2

## 7.1.2 Password Expiration for Local Users

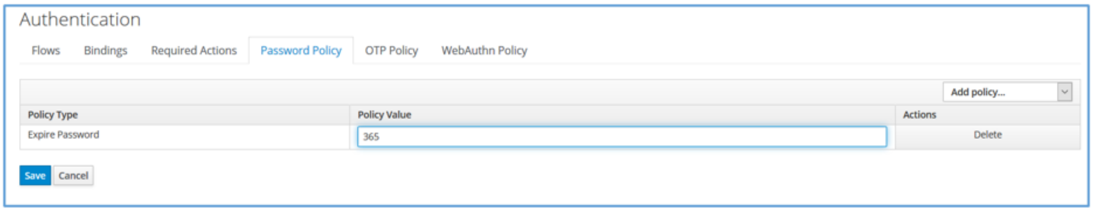
The definition of a time span for password expiration is done by a Windows Active Directory administrator for any LDAP user account integrated in Bruker GxP solution (see chapter *User Accounts [▷ 30]*).

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**.



| Policy Type | Policy Value | Actions |
|---|---|---|
| Expire Password | 365 | Delete |

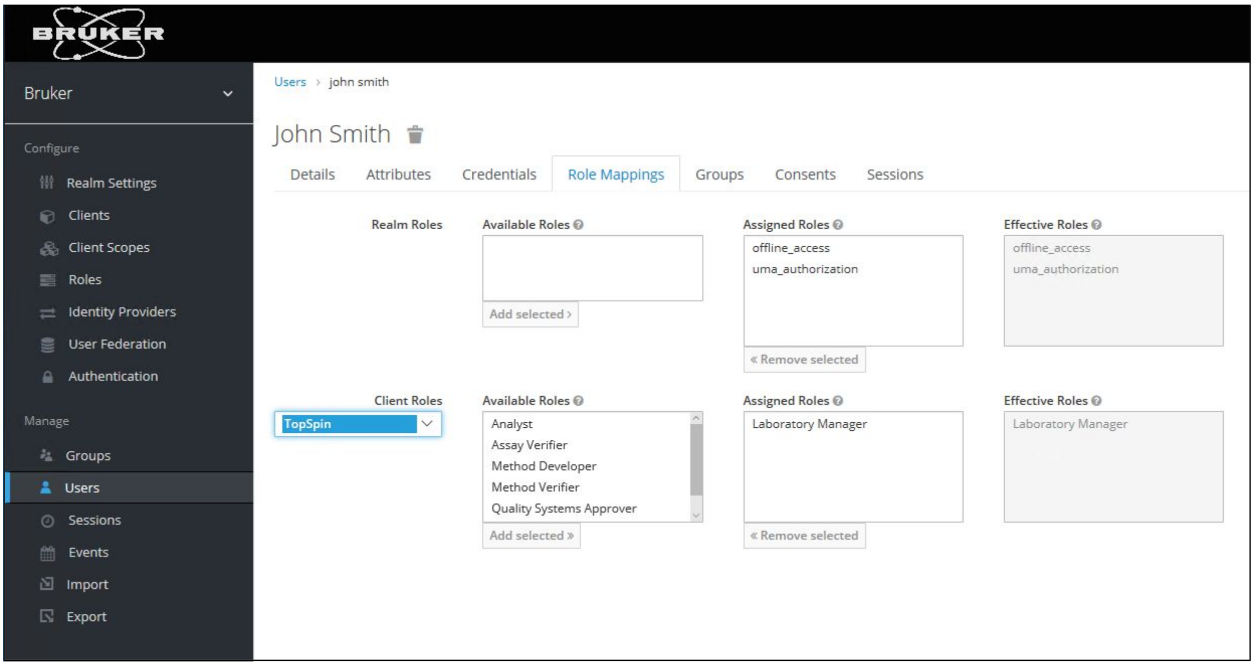
Setting no policy means that passwords will stay valid for an infinite amount of time.

## 7.2 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
- Laboratory Manager
- Analyst
- Assay Verifier
- Method Developer
- Method Verifier
- Quality Systems Approver



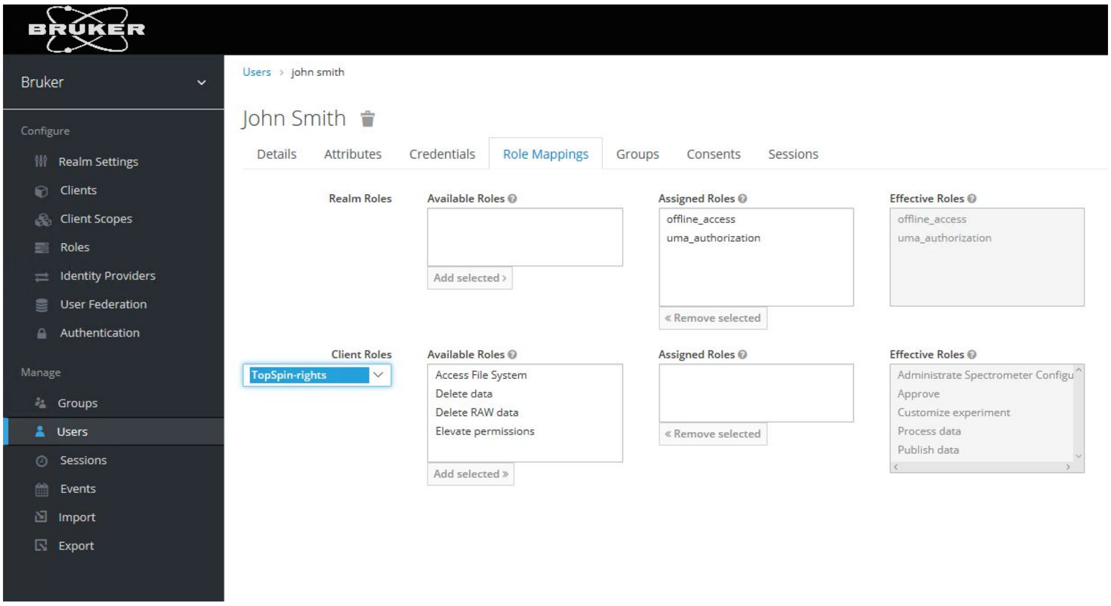
Realm Roles
Available Roles:
Assigned Roles: offline_access, uma_authorization
Effective Roles: offline_access, uma_authorization

Client Roles: TopSpin
Available Roles: Analyst, Assay Verifier, Method Developer, Method Verifier, Quality Systems Approver
Assigned Roles: Laboratory Manager
Effective Roles: Laboratory Manager

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.



Realm Roles

Available Roles

Assigned Roles: offline_access, uma_authorization

Effective Roles: offline_access, uma_authorization

Client Roles: TopSpin-rights

Available Roles: Access File System, Delete data, Delete RAW data, Elevate permissions

Assigned Roles

Effective Roles: Administrate Spectrometer Configu, Approve, Customize experiment, Process data, Publish data

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 Spectrometer Administrator, you have the right to perform important configuration steps.

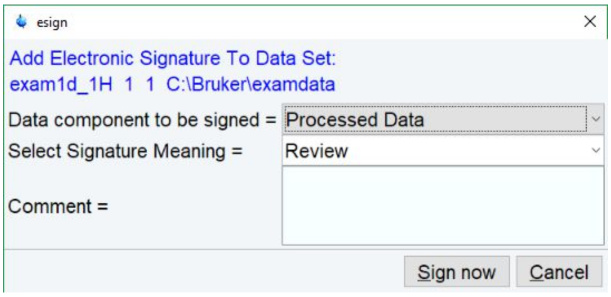
When logged in as nmruser, you have more restricted rights according to the table shown above.

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

## 7.3 Electronic Signatures

### 7.3.1 Signing a Dataset

The command **esign** adds an electronic signature to the raw data or to the processed data of a dataset. It opens a dialog where you can select the data component to be signed, the signature meaning and, optionally, add a comment. The command **esign** requires that the NMR administrator has set up a list of users who are allowed to sign a dataset, along with definitions of signature meanings (e.g. review, approval). See previous chapters for the definition of users, their roles, and signature meanings.



Add Electronic Signature To Data Set:
exam1d_1H 1 1 C:\Bruker\examdata

Data component to be signed = Processed Data

Select Signature Meaning = Review

Comment =

### 7.3.2 Structure of a Signature

In TopSpin, an electronic signature is realized as a special entry appended to the audit trail of the raw or processed data. It is therefore linked with the data and protected against manipulations just like any other audit trail entry. Signatures can be viewed with the command **audit**. An electronic signature consists of the following items:

**USER ID**

The ID of the user logged in at the time **esign** was executed. This is the internal user with whom TopSpin was started.

**USER NAME**

The complete name of the signer as specified by the NMR administrator during user administration.

**SIGNATURE MEANING**

The meaning of a signature e.g. Review or Approval. A user may only select meanings that were assigned to him by the NMR administrator during user administration.

**SIGNATURE COMMENT**

Any text.

### 7.3.3 Displaying the Electronic Signature in the Dataset Window

The electronic signature can be displayed in the dataset window by setting the corresponding display component.

- Right-click in the dataset window and select **Spectra Display Preferences...** [**.dopt**].
- In the group **Spectrum components** check **Electronic Signature** and click **Apply**.

The electronic signature will appear, at the upper left corner, below the title.

### 7.3.4 Plotting the Electronic Signature

When plotting a dataset using TopSpin's plot editor (commands **plot** and **autoplot**), an electronic signature is automatically plotted (unless this feature is disabled), if the last entry of the audit trail of the data to be plotted is an electronic signature. This ensures that after signing no more data manipulations have been performed.

### 7.3.5 Multiple Signatures

The command **esign** may be applied several times to a dataset, for instance if two persons (say an operator and an administrator) must sign in accordance with company regulations.

### 7.3.6 Validity and Security of Signatures

TopSpin electronic signatures of datasets must not be confused with digital signatures as defined in applicable law. Digital signature laws are usually country dependent. They require the administration of passwords (more general: electronic keys which authenticate the owner of the document) to be performed by authorized trust centers. In contrast, TopSpin uses OS-encrypted passwords or internal user passwords encrypted by TopSpin itself.

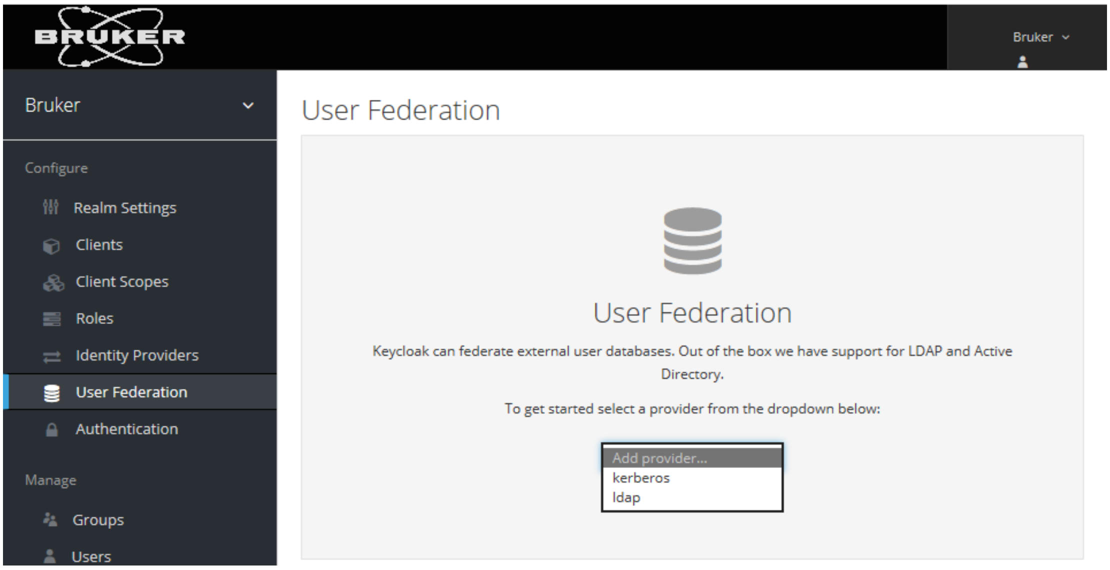
For this reason, companies and institutions that want to apply TopSpin signatures must have a Standard Operating Procedure (SOP), which defines the role of these signatures.

Note that digital signatures complying with respective laws requires special software, and the involvement of trust centers. Bruker refers to the respective commercial software for this purpose.

## 7.4 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 then controlled by the overarching user access control system, and hence 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.



User Federation

Keycloak can federate external user databases. Out of the box we have support for LDAP and Active Directory.

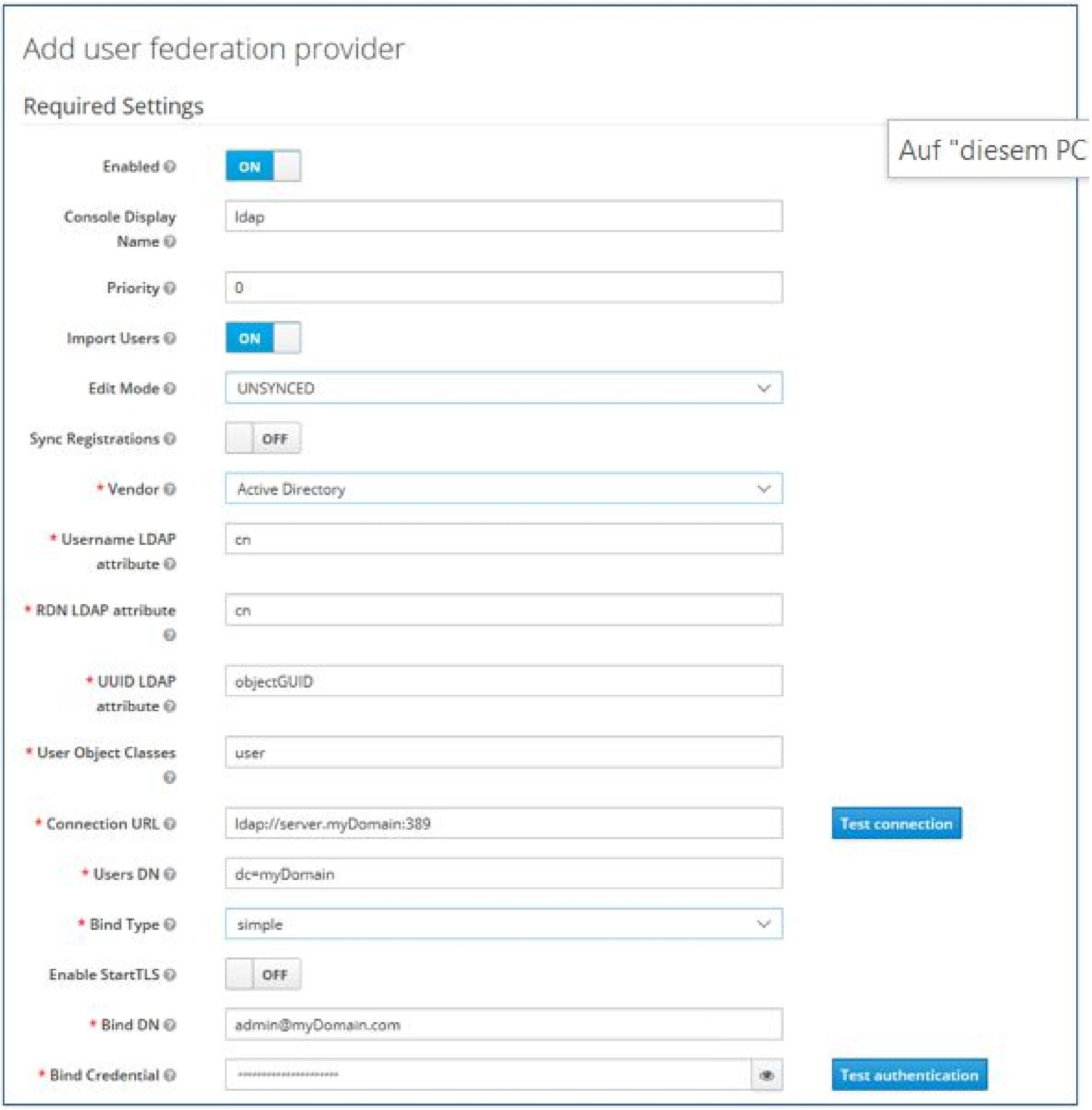
To get started select a provider from the dropdown below:

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).

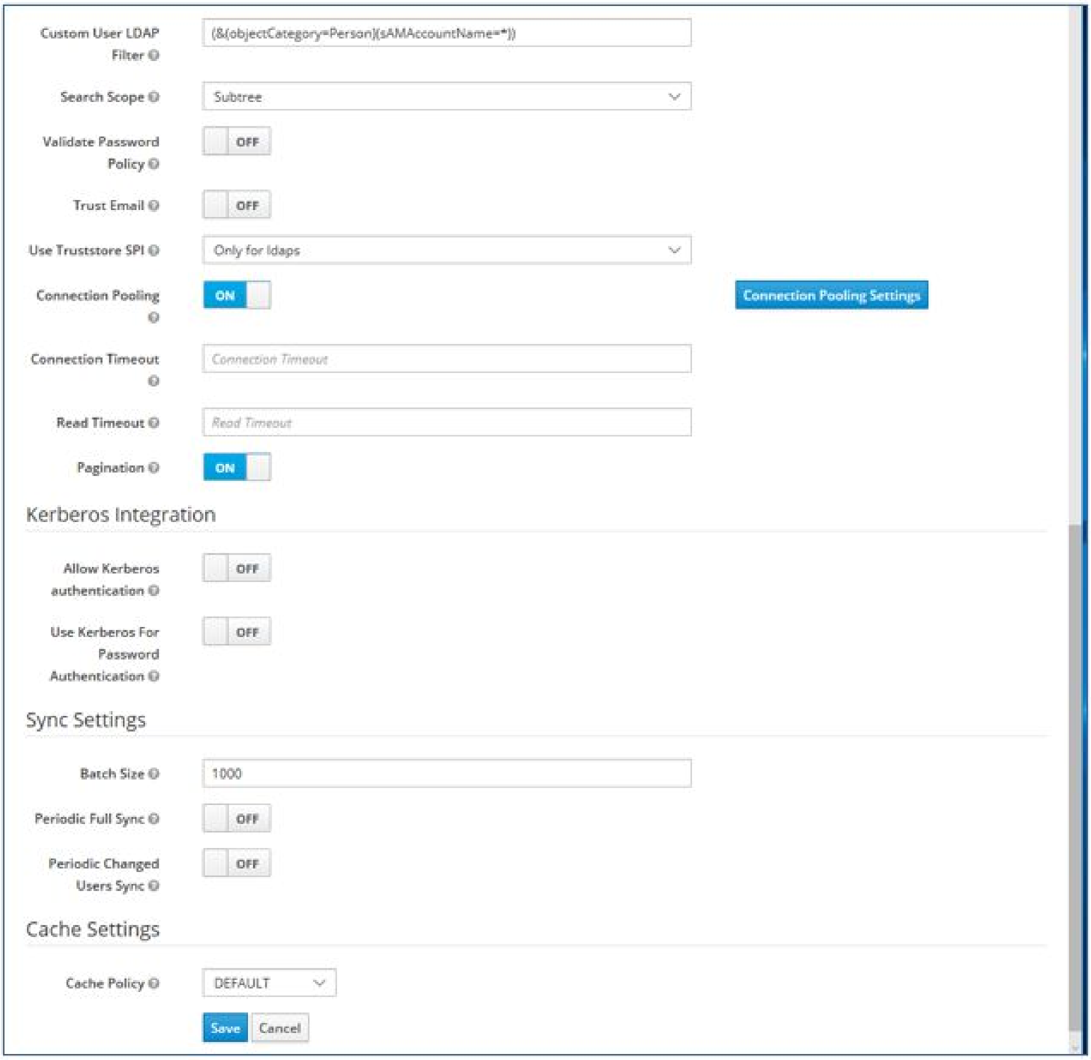


## Add user federation provider

### Required Settings

Auf "diesem PC

| | | |
|---|---|---|
| Enabled | ON | |
| Console Display Name | ldap | |
| Priority | 0 | |
| Import Users | ON | |
| Edit Mode | UNSYNCED | |
| Sync Registrations | OFF | |
| * Vendor | Active Directory | |
| * Username LDAP attribute | cn | |
| * RDN LDAP attribute | cn | |
| * UUID LDAP attribute | objectGUID | |
| * User Object Classes | user | |
| * Connection URL | ldap://server.myDomain:389 | Test connection |
| * Users DN | dc=myDomain | |
| * Bind Type | simple | |
| Enable StartTLS | OFF | |
| * Bind DN | admin@myDomain.com | |
| * Bind Credential | ******************** | Test authentication |



Custom User LDAP Filter (&(objectCategory=Person)(sAMAccountName=*))

Search Scope Subtree

Validate Password Policy OFF

Trust Email OFF

Use Truststore SPI Only for ldaps

Connection Pooling ON

Connection Timeout Connection Timeout

Read Timeout Read Timeout

Pagination ON

Kerberos Integration

Allow Kerberos authentication OFF

Use Kerberos For Password Authentication OFF

Sync Settings

Batch Size 1000

Periodic Full Sync OFF

Periodic Changed Users Sync OFF

Cache Settings

Cache Policy DEFAULT

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.

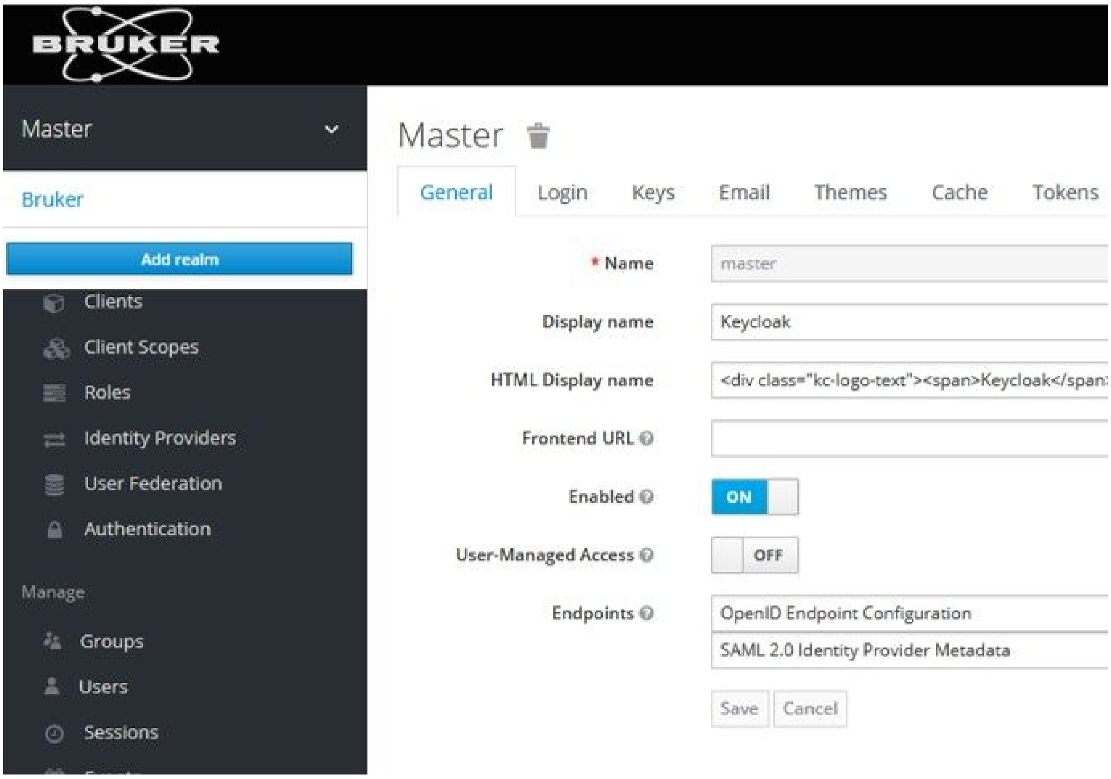
After this stage has been completed, login to TopSpin with Active Directory credentials is possible for all these users.

## 7.5 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).

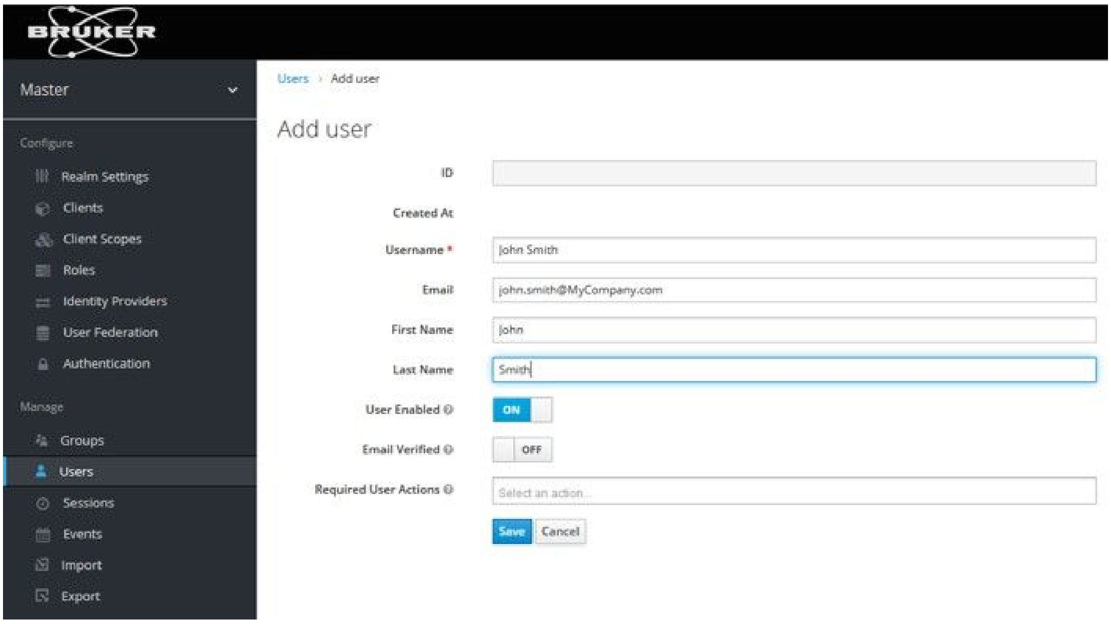
Switch to realm **Master**.



Master

| | |
|---|---|
| * Name | master |
| Display name | Keycloak |
| HTML Display name | <div class="kc-logo-text"><span>Keycloak</span |
| Frontend URL | |
| Enabled | ON |
| User-Managed Access | OFF |
| Endpoints | OpenID Endpoint Configuration<br>SAML 2.0 Identity Provider Metadata |

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

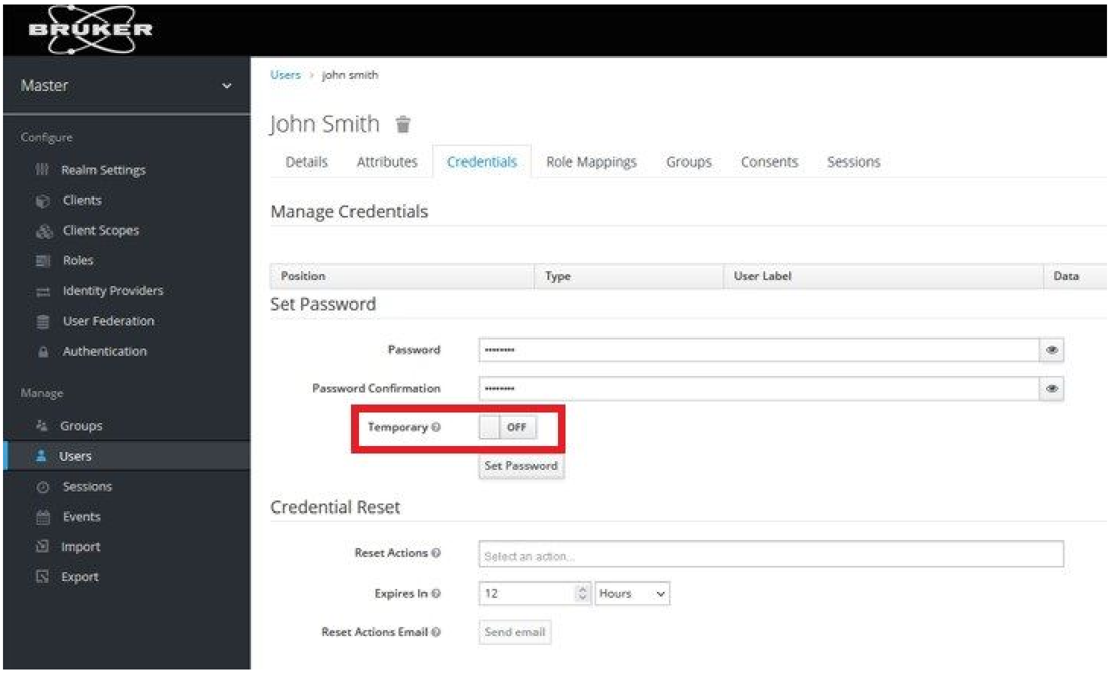


Add user

| | |
|---|---|
| ID | |
| Created At | |
| Username * | John Smith |
| Email | john.smith@MyCompany.com |
| First Name | John |
| Last Name | Smith |
| User Enabled | ON |
| Email Verified | OFF |
| Required User Actions | Select an action... |

Enter username and click on **Save.**

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



Password: ********

Password Confirmation: ********

Temporary: OFF

Reset Actions: Select an action...

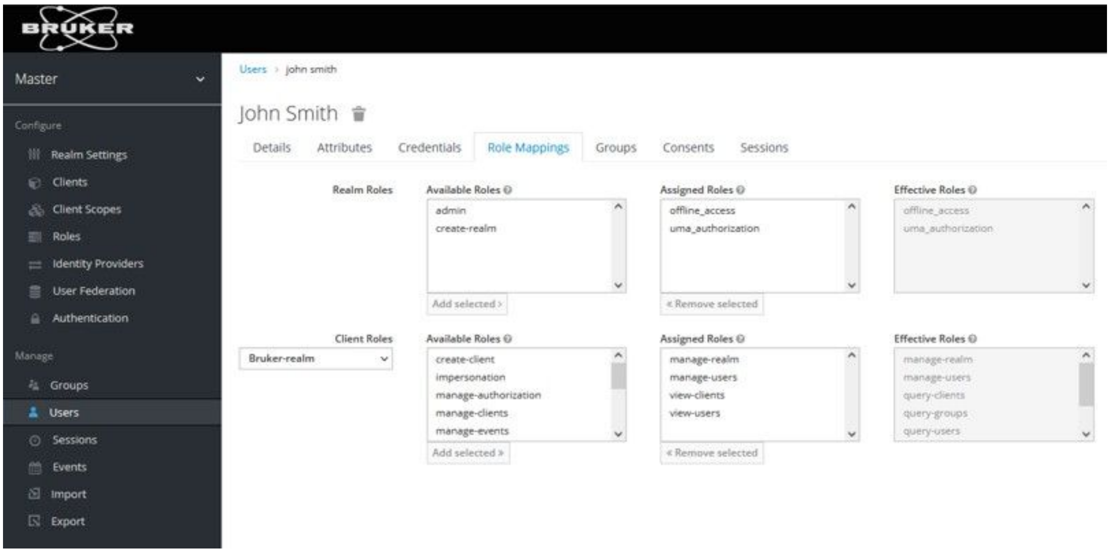
Expires In: 12 Hours

Reset Actions Email

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



Realm Roles

| Available Roles | Assigned Roles | Effective Roles |
|---|---|---|
| admin<br>create-realm | offline_access<br>uma_authorization | offline_access<br>uma_authorization |

Client Roles: Bruker-realm

| Available Roles | Assigned Roles | Effective Roles |
|---|---|---|
| create-client<br>impersonation<br>manage-authorization<br>manage-clients<br>manage-events | manage-realm<br>manage-users<br>view-clients<br>view-users | manage-realm<br>manage-users<br>query-clients<br>query-groups<br>query-users |

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.

## 7.6 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, 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 the 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.)

# 8 Advanced Topics

## 8.1 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 respective 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.

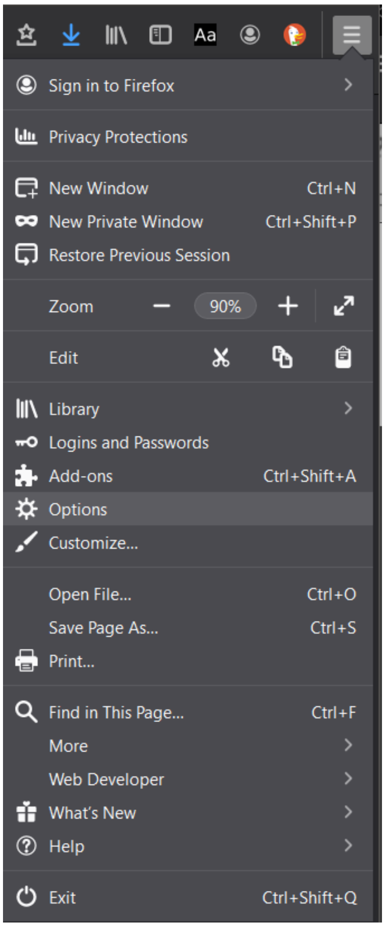
## 8.2 Remove Warning on Opening Keycloak Administration Console

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

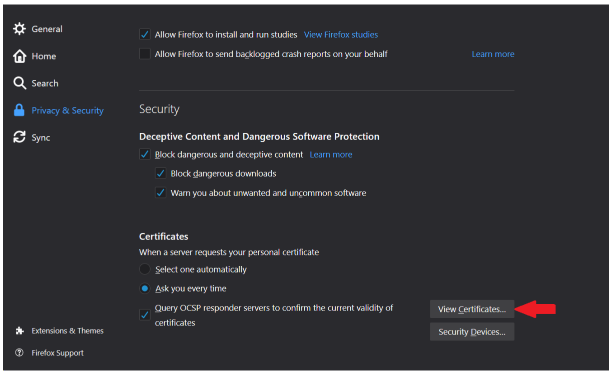
To suppress the warning messages the following steps for common browsers are recommended.

### 8.2.1 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**.



☑ Allow Firefox to install and run studies View Firefox studies

□ Allow Firefox to send backlogged crash reports on your behalf Learn more

Security

**Deceptive Content and Dangerous Software Protection**

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

**Certificates**

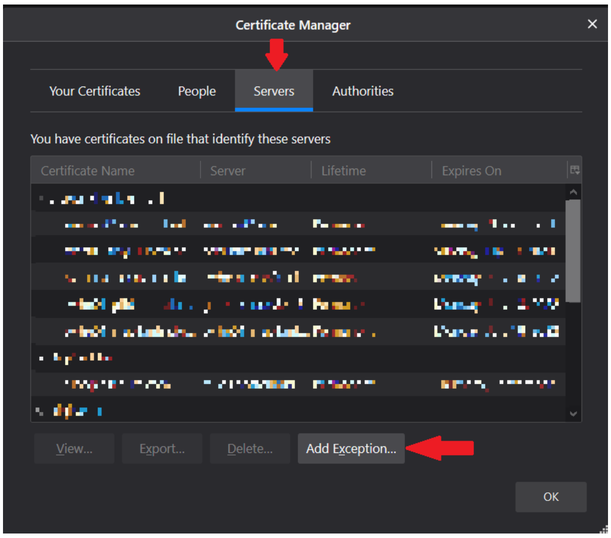
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

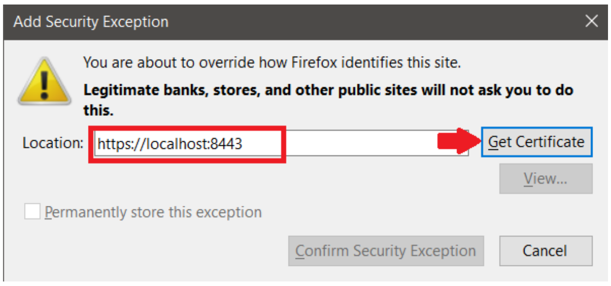
- On the **Certificate Manager** window select the **Servers** tab, and click on the button **Add Exception**.



You have certificates on file that identify these servers

| Certificate Name | Server | Lifetime | Expires On |
|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] |

- 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**.



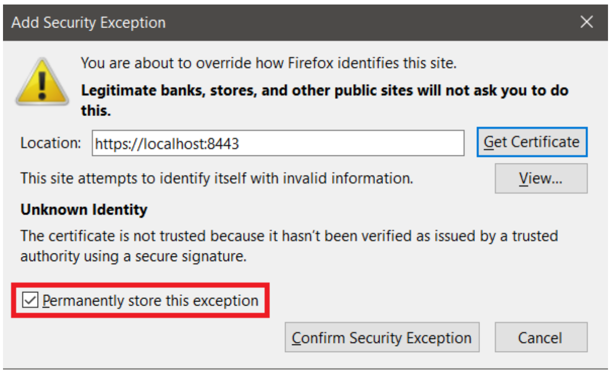
You are about to override how Firefox identifies this site.

**Legitimate banks, stores, and other public sites will not ask you to do this.**

Location: https://localhost:8443

□ Permanently store this exception

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



You are about to override how Firefox identifies this site.

**Legitimate banks, stores, and other public sites will not ask you to do this.**

Location: https://localhost:8443

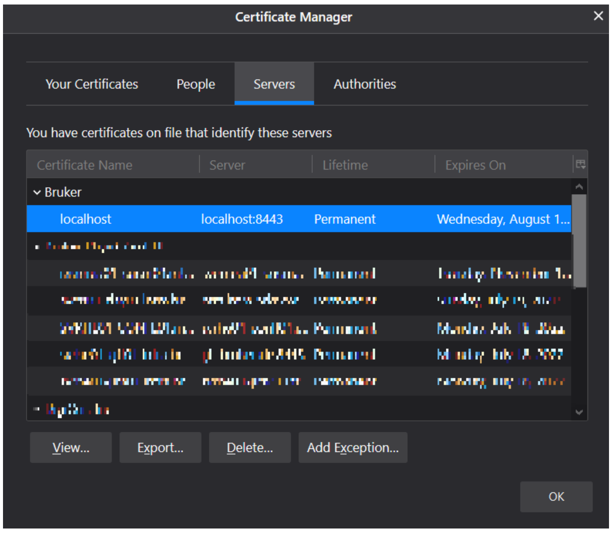
This site attempts to identify itself with invalid information.

**Unknown Identity**

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

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



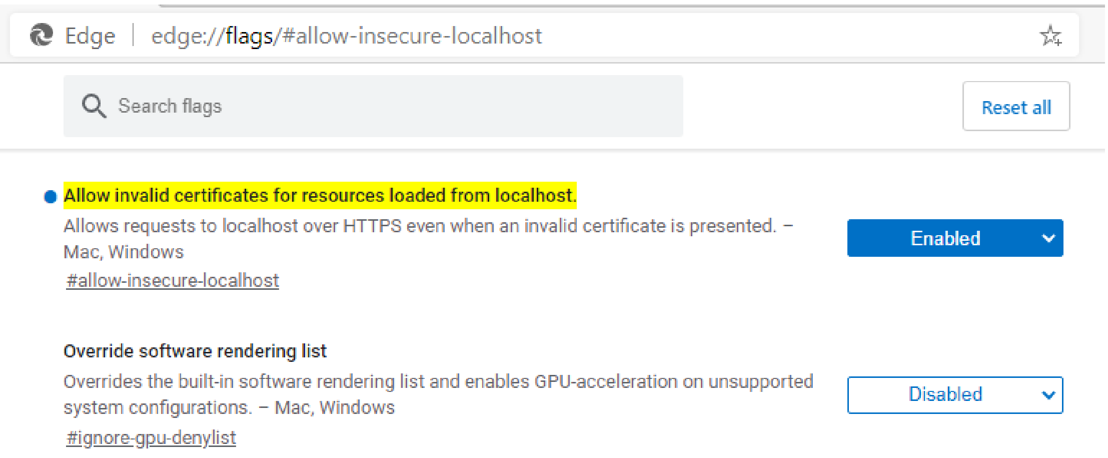
You have certificates on file that identify these servers

| Certificate Name | Server | Lifetime | Expires On |
|---|---|---|---|
| Bruker | | | |
| localhost | localhost:8443 | Permanent | Wednesday, August 1... |
| [redacted] | | | |

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

### 8.2.2 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.



Allow invalid certificates for resources loaded from localhost.
Allows requests to localhost over HTTPS even when an invalid certificate is presented. – Mac, Windows
#allow-insecure-localhost
Enabled

Override software rendering list
Overrides the built-in software rendering list and enables GPU-acceleration on unsupported system configurations. – Mac, Windows
#ignore-gpu-denylist
Disabled

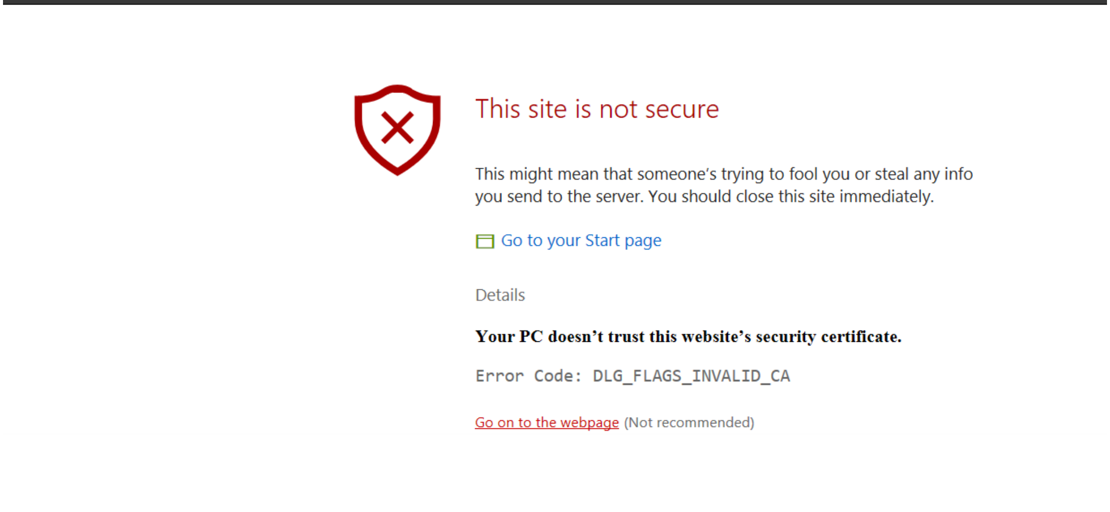
Afterwards Edge needs to be restarted.

### 8.2.3 Chrome

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

### 8.2.4 Edge (Legacy Version)

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



localhost:8443

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

**Your PC doesn't trust this website's security certificate.**

```
Error Code: DLG_FLAGS_INVALID_CA
```

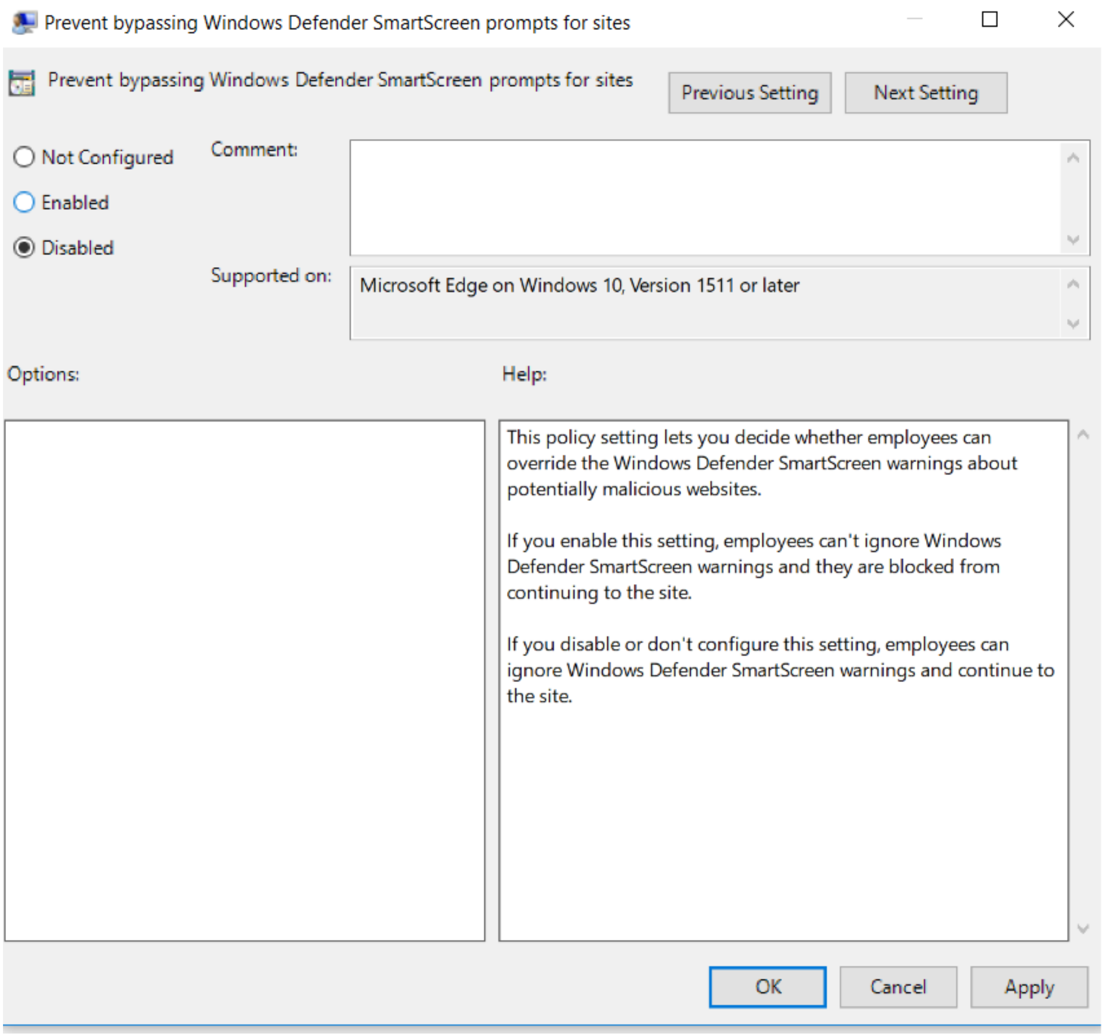
Go on to the webpage (Not recommended)

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.

### 8.2.4.1 What if Edge Prevents Opening Keycloak?

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.



Prevent bypassing Windows Defender SmartScreen prompts for sites

Prevent bypassing Windows Defender SmartScreen prompts for sites

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: Microsoft Edge on Windows 10, Version 1511 or later

Options:

Help:

This policy setting lets you decide whether employees can override the Windows Defender SmartScreen warnings about potentially malicious websites.

If you enable this setting, employees can't ignore Windows Defender SmartScreen warnings and they are blocked from continuing to the site.

If you disable or don't configure this setting, employees can ignore Windows Defender SmartScreen warnings and continue to the site.

## 8.3 Extended Documentation

Keycloak’s functionalites 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 ressources on the internet.

# 9 Contact

**Manufacturer**

Bruker BioSpin GmbH
Rudolf-Plank-Str. 23
D-76275 Ettlingen
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

Part No: H178131