

TopSpin GxP

Quick Start Guide
 User Manual
 Version 012

Innovation with Integrity

NMR

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 o	of TopSpin's GxP Extension	5
2	Working	with TopSpin	5
3	Installatio	n	5
	3.1	Server Installation	6
	3.2	Client Installation	8
4	Audit Trai	I	12
5	Identity M	anagement	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	I 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 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.

Bruker GxP Services Insta	lation Wizard	5 <u>98</u>		×
	Welcome to the Bru Wizard	ker GxP Servi	es Set	up
	This will install Bruker GxP Ser will lead you step by step thr	vices on your comp ough the installatior	uter. The n.	wizard
	Click Next to continue, or Car	ncel to exit Setup.		
		Next >	С	ancel



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 Servi	ices Installation	Wizard		_		×
Setup NMRAdmir	nistrator passw	ord				
Configure NMRAd	ministrator passwo	ord				
Please specify the p	assword for the d	lefault user NMRA	dministrator			
Password:	•••••				۲	0
Confirm Password:	•••••				۲	0
Bruker GxP Services 4.	1.2-SNAPSHOT -					
				Next >	Car	ncel

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:



Completing the Bruker G Wizard	CP Service	s Setup
The installer has successfully installed Click Finish to exit the wizard. The following file contains the setting This file can be used during the client set the correct settings. C:\Bruker\nmrsuite\server-properties Show File	ed the Bruker (gs for the clien nt installation t es.zip	SxP Services. nt installation. to automatically

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.



Installation Moder			
	0		
Regulated environment (GxP)	0		
Installation type:			
Spectrometer Control			0
			0

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.



	te instandulun wizard				-
Import Server se	ttings				
Automatically conf	figure the client with the server settings archive				
If you provide the se resulting client will o	erver-settings.zip archive no manual configuratio connect to the server that has written the proper	on needs rties file	to be do during ir	one. The Installation.	
Properties archive:	C:\Bruker\nmrsuite\server-properties.zip		Br	owse	0
ker NMR Suite 4.1.2	-SNAPSHOT				
ker NMR Suite 4.1.2	-SNAPSHOT				

The next screen summarizes the used server configuration.



🛃 Bruker NMR Suite Installation Wizard	8 <u>9</u>	<u>764</u>		×					
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									
Bruker NMR Suite 4.1.2-SNAPSHOT	ack Nex	ct >	Ci	ancel					

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 datachanging 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.

Bruker CAT Viewer		-	×
	BRUKER		
	Log In		
	Username or email		
	Log In		

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

bruker C/	AT Viewer			>
	Central Audit Viewer		Logo	ut
	You do not have the permission to view the CA	AT report.		

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).

Bruker CAT Viewer										1-1	ð X
					Central Audit Tr	ail				± 0	BRUKER
From: 1/23/2021	To: 4/23/2021	🖲 Searc	h Export Reset Sea	irch Fields				Records available	e: 66 Last search perfor	med: Apr 23, 2021, 1	12:22:25 PM
	Category	Who	User Uuid	Where	Client	What	Dataset Path	Dataset Uuid	Original Value	New Value	
When ↓	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 - 6	3 of 66 < <	> >1

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.

m: 23/2020	To:	🗉 Sea	rch Export
	Category	Who	User Uuid
When	AUTH	Search for	Search for
23.07.20, 09:11:33	AUTHENTICATE	nmruser	3aed533f-b3 9605-faecaf2
23.07.20, 09:11:44	AUTHENTICATE	dirk.hoelzer	e4c2b3cb-d5 9438-646aaa
23.07.20, 09:42:02	AUTHENTICATE	dirk.hoelzer	e4c2b3cb-d5 9438-646aaa
23.07.20, 09:42:09	AUTHENTICATE	john smith	a4a84f05-53 9925-f0be1e
23.07.20, 09:44:43	AUTHENTICATE	john smith	a4a84f05-53 9925-f0be1e
23.07.20, 09:47:25	AUTHENTICATE	john smith	a4a84f05-53 9925-f0be1e
23.07.20, 09:48:35	AUTHENTICATE	john smith	a4a84f05-53 9925-f0be1e
00 NT ON NO.40.40	ALITUENTIOATE	iohn amith	a4a84f05-53

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.



Auditor: nmruser Search criteria: Fron	n: 2020-04-13, Te	o: 2020-07-14								
Number of Entries: 9	•				1	Signature:				
shen	Category	Who	Where	Client	Hhat	Dataset Path	Original Value	New Value		
13.07.20, 17:24:08	AUTHENTICATE	nmradministrato	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	login					
13.07.20, 17:29:43	AUTHENTICATE	nmradministrato	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	logoff					
13.07.20, 17:29:52	AUTHENTICATE	nmruser	NBRHE01-G7Q3QV2	TopSpin 4 0 10 a	login			1		
13.07.20, 17:29:54	PROCESSING	naruser	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	Start of raw data processing em LB = 0.3 SI = 32K data hash H05: 32K E1 20 05 7B C2 CB 56 BF 41 FA 08 60 20 45 60 90	C:/Bruker/Relea ses/TopSpin4.0. 9/examdata/exam 1d_1H/1/pdata/1				
13.07.20, 17:29:54	PROCESSING	naruser	NBRHE01-G7Q3QV2	TopSpin 4.0.10.a	ft FT_Mod = 6 FKNL = 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/Relea ses/TopSpin4.0, 9/examdata/exam 1d_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/Relea ses/TopSpin4.0. 9/examdata/exam 1d_1H/1/pdata/1				

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.



BRUKER		
Bruker v	Bruker 👕	
Configure	General Login Keys	Email Themes Cache Tokens Client Registration Security Defenses
🚻 Realm Settings	* Name	Bruker
Clients	Display name	Proter
🚷 Client Scopes	Display hame	bi unei
Roles	HTML Display name	
🚍 Identity Providers	Frontend URL 🚱	
User Federation	Enabled Ø	
Authentication	User-Managed Access 🚱	OFF
Manage	_	
🐇 Groups	Endpoints 🔞	OpenID Endpoint Configuration
		SAME 2.0 Identity Provider Metadata
		Save Cancel
O Sessions		
Events		
Import		
🖾 Export		

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.



BRUKER								Admin 🗸
\sim								2
Bruker 🗸 🗸	Users							
Configure	Lookup							
👫 Realm Settings	Şearch	Q View all users					Unlock users	Add user
Clients	ID	Username	Email	Last Name	First Name	Actions		
🚓 Client Scopes	3aed533f-b374-4bfc-9605	nmruser				Edit	Impersonate	Delete
Roles	1f783049-2ebd-4a5e-ba01	nmradministrator				Edit	Impersonate	Delete
⇒ Identity Providers								
User Federation								
 Authentication 								
Manage								
🐁 Groups								
💄 Users								
 Sessions 								
🛗 Events								
Import								
Export								

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].

BRUKER			Admin ~
Bruker ~	Users > Add user		
Master	Add user		
Add realm	ID		
📦 Clients	Created At		
🚓 Client Scopes	Username *	John Smith	
Roles Identity Providers	Email	john.smith@myCompany.com	
User Federation	First Name	John	
Authentication	Last Name	Smith	
Manage	User Enabled 😡	ON	
k Groups	Email Verified 😡	OFF	
🛓 Users	Required User Actions 😡	Select an action	
② Sessions			
Events		Save Cancel	
Import			
LN Export			

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.

Jsers → john		
ohn 👕		
Details Attributes Credentials	s Role Mappings Groups Consents Sessions	
Кеу	Value	Actions
ESIGN	Sample Identity confirmed##Analysis approved	Delete
SPECTROMETER_BLACKLIST	BLOB##NBRHE01-F07NSQ2	Delete

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.

🖕 Lo	ogin forbidden	×
8	You are not allowed to work on this instrument. Please contact laboratory manager The instrument name is NBRHE01-F07NSQ2	for access.
		Close

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



в	RUKER								Admin 🗸
Bruk	er 🗸	Authentication	Required Actions	Password Policy	OTP Policy	WebAuthn Policy			
**	Realm Settings Clients	Policy Type		Policy Value			Actions	Add policy	~
& =	Client Scopes Roles	Save Cancel							
11	Identity Providers User Federation								
 Mana	Authentication								

- 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**.

Authentication		
Flows Bindings Required Actions Password Policy	OTP Policy WebAuthn Policy	
		Add policy 🗸
Policy Type	Policy Value	Actions
Expire Password	365	Delete
Save Cancel		

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



BRUKER Bruker ~	Users → john si	mith			
Configure	John Sm	ith 👕			
锴 Realm Settings	Details	Attributes	Credentials Role Mappings	Groups Consents Sessions	
📦 Clients	0	Realm Roles	Available Roles 🖗	Assigned Roles 😡	Effective Roles @
🚓 Client Scopes				offline_access	offline_access
Roles				uma_authorization	uma_authorization
≓ Identity Providers			Add selected >		
🍔 User Federation				« Remove selected	
Authentication				whentove selected	
Manage	TopSpin	Client Roles	Available Roles 🔞	Assigned Roles @	Effective Roles @
🐇 Groups			Assay Verifier	cubor actory manager	aborotory manager
Lusers			Method Developer Method Verifier		
 Sessions 			Quality Systems Approver	~	
Events			Add selected »	« Remove selected	
Import					
R Export					



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	Х					Х	
Setup method				Х		Х	
Customize experiment				Х		Х	
Start experiment		X		Х	Х	Х	
Process data		Х		Х	Х	Х	
Delete RAW data	Х						
Delete data	Х						
Access File System	Х						Х
Publish data		Х	Х	Х	Х	Х	Х
Review		Х	Х	Х	Х	Х	Х
Approve		Х	X			Х	Х

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

BRUKER				
Bruker 🗸 🗸	Users > john smith			
Configure	John Smith 🍵			
🚻 Realm Settings	Details Attributes	Credentials Role Mappings G	roups Consents Sessions	
Clients	Realm Roles	Available Roles 🚱	Assigned Roles 😡	Effective Roles @
🚓 Client Scopes			offline_access	offline_access
📰 Roles			uma_authorization	uma_authorization
💳 Identity Providers		Add selected >		
User Federation				
Authentication			« Remove selected	
	Client Roles	Available Roles 🔞	Assigned Roles 📀	Effective Roles 🚱
Manage	TopSpin-rights 🗸 🗸	Access File System		Administrate Spectrometer Configu ^
🐁 Groups		Delete data		Approve
		Elevate permissions	# Demous collected	Customize experiment
		Liefote permissions	« Remove selected	Publish data
O Sessions		Add selected »		<
🛗 Events				
Import				
F Creat				
LS Export				







The following roles are used for the predefined users:

nmruser

nmradministrator

Laboratory Manager 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.

BRUKER	Bruker 🗸
Bruker 🗸	User Federation
Configure Realm Settings Clients Client Scopes Roles Identity Providers User Federation Authentication Manage Scoups Users	User Federation 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: Add provider kerberos ldap

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: Idap://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).

Enabled ©	ON	Auf "diesem PC
Console Display Name 🗊	Idap	
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 ©	Idap://server.myDomain:389	Test connection
+ Users DN @	dc=myDomain	
* Bind Type 😡	simple 🗸	
Enable StartTLS ©	OFF	
• Bind DN @	admin@myDomain.com	
• Plad Conductial O		Test authentication



Custom User LDAP Filter @	(&(objectCategory=Person)(sAMAccountName=*))		
Search Scope 😡	Subtree	~	
Validate Password Policy ©	OFF		
Trust Email @	OFF		
Use Truststore SPI 😡	Only for Idaps	~	
Connection Pooling	ON		Connection Pooling Settings
Connection Timeout	Connection Timeout		
Read Timeout @	Read Timeout		
Pagination @	ON DE		
Kerberos Integra	tion		
Allow Kerberos authentication ©	OFF		
Use Kerberos For Password	OFF		
Sync Settings			
Batch Size @	1000		
Periodic Full Sync 🛛	OFF		
Periodic Changed Users Sync ⊕	OFF		
Cache Settings			
Cache Policy 😡	DEFAULT V Seve Cancel		

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.

P. C. Dispersional Dispersion	Reyclade 🖂 Reyclade Aplein Cancel 🛪 🔤 🗠				- o *
	the state of the second s	IL C. MARINE WERE DEVELOPING			5 B L 11 -
	2 (1000 - 1000)				
Matter	Test #				
144	Debath Attributes Dedentary Aules	Anarth Groups Corports Sessory			
111111-11-11-11-11-11-11-11-11-11-11-11	Real Prove	Australia Australia	Automatication of	Photos Area 0	
			affect in parts	Allen prove	
			one autoritaria	of the distribution	
		Act strategies			
a Administration	Concert State		+ Number concerns		
	Daris Rates	further county in county with the classes			
II tuet					
					Activate Windows
		10. De bisset him oos at 10 oos inter	and for the size over time?	and the second se	
		Man inte	in the second	New X	
the state of the s			a second s	and a second	
,D have here to exactly.	0 🖻 📰 🖬 🏥 💼 🐺 💠				· · · · · · · · · · · · · · · · · · ·

Navigate to section Users, then click on Add User.

BRUKER			Admin	×
Bruker 🗸	Users > Add user			
Master	Add user			
Add realm	ID			
Clients	Created At			
🙈 Client Scopes	Username *	John Smith		
Roles Identity Providers	Email	john.smith@myCompany.com		
User Federation	First Name	John		
Authentication	Last Name	Smith		
Manage	User Enabled Ø	ON		
🐁 Groups	Email Verified Ø	OFF		
🛓 Users	Required User Actions @	Select an action		
 Sessions Events 		Save Cancel		
Import				
Export				





Enter username and click on Save.

🔁 🖅 🖂 Keycloak Admin Console 🔄 Keycloak Admin G	Consol × 🖂 Keycloak Admin Console 🛛 + 🗸		- ø ×
← → Ů ŵ ▲ Certificate error https://localho	ost.8444/auth/admin/master/console/#/create/user/master		□☆ ☆ん ピ…
BRUKER			Kuder -
Master	Users > Add user		
Configure	Add user		
III Realm Settings	10		
© Clients	Created At		
🚓 Client Scopes	Uzername *	numbur ×	
Roles			
Identity Providers	Email		
User Federation	First Name		
Authentication	Last Name		
Manage	User Enabled @	ON	
²≞ Groups	Email Verified 0	OFF	
👗 Users	Resident Horse Automa ()		
 Sessions 	Required user Acours of	Select an action	
Events		Save Cancel	
i tmport			
Export			
			Activate Windows
F Dype here to search	o 🛱 🔁 🧮 🚖 😭 🚸		스 188 127 40 DNG 607 AM 특징

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

							_
Keycloak Admin Console	rsol × H Keydoak Admin Con	isole + ~				- Ø	×
← → ○ ᢙ ▲ Certificate error https://localhost8	8444/auth/admin/master/console/#	//realms/master/users/2730b/	1e-cc62-492a-ba59-e99813f0b32f/user-credentials			□ ☆ ☆ <i>£</i> ピ	
BRUKER						Kuse	
Master 🗸	Users > newadmin						
	Newadmin 👕						
III Realm Settings	Details Attributes	Credentials Role Ma	ppings Groups Consents Sessions				
Clients	Manage Credentials						
💩 Client Scopes	manage credendals						
E Roles	Position		Туре	User Label	Data	Actions	
Identity Providers	Set Password						
User Federation		Presented	[
Authentication							
11		Password Confirmation			æ		
Manage		Temporary Ø	OFF				
4. Groups			Set Password				
▲ Osers							
O Sessions							
Evens							
as import							
L's Export							
						Activate Windows	
# P Type here to search	o # 🤮 📕 🛱	i 💼 👰 🚸	● ♦ 至			∧ 🖮 💭 40 DNG 608 AM	5



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

🔁 📲 🗄 Log in to Keycloak 📄 Keycloak Admin Consol	× ⊟ Log in to Keycloak + ∨				- 0
\leftarrow \rightarrow \bigcirc $\hat{\omega}$ \triangle Certificate error https://localhost.84	4/auth/admin/master/console/#/realms/master/users/53afef3	-ad2b-405a-8409-64af5967d00e/role-mappings			
BRUKER					Vousier 1
Master ~	Users > newadmin				
Configure	Newadmin 👕				
iii Realm Settings	Details Attributes Credentials Role Ma	opings Groups Consents Sessions			
© Clients	Realm Roles	Available Roles (i)	Assigned Boles ()	Effective Boles (0	
A Client Scopes		edmin	offline_access	offline_access	
Roles		create-realm	uma_authorization	uma_authorization	
Identity Providers					
User Federation					
Authentication		Add selected >	< Remove selected		
Manage	Client Roles	Select client to view roles for client			
A. Groups	account				
Lusers	broker Broker-malm				
③ Sessions	master-realm security-admin-console				
🛗 Events	×				
Import					
🐼 Export					

Then add the roles

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

📇 🖅 🖂 Log in to Keycloak 🖂 Keycloak Admin	Consol 🗴 🔲 Log in to Keydloak 🛛 🕂 🗸			
← → O @ <u>A</u> Certificate error https://localh	iost 8444/auth/admin/master/console/#/realms/master/users/53afefs	81-ad2b-405a-8409-64af5967d00e/role-mappings		
\sim				
BRUKER				
11	Users > newadmin			
Master	×			
Configure	Newadmin 👕			
111 Realm Settings	Details Attributes Credentials Role M	appings Groups Consents Sessions		
E) Clents		a canonas	101 Julia - C	
- S. Client Scopes	Realm Roles	Available Roles @	Assigned Roles @	Effective Roles @
I Boles		create-realm	uma_authorization	uma_authorization
→ Identity Providers				
User Federation				
A Authentication		Add selected >	« Remove selected	
	Client Roles	Available Roles D	Assigned Roles @	Effective Roles ()
Marage	Bruker-realm 🗸	create-client	manage-realm	manage-realm ^^
A Groups		manage-authorization	view-clients	manage-users query-clients
🛔 Users		manage-clients	view-users	duery-groups
Sessions		manage-events	a Remove selected	direct-results in the second sec
🛗 Events		Hou selected #	< Remove selected	
团 Import				
🖾 Export				
		$\mathbb{Q}_{\!\!\boldsymbol{Q}}$. Let Microsoft Edge save and fill your password for this site	next time? Save	lever ×
		More info		

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 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.)

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. Unfortunatey 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.

	Certi	ficate Manager		×
		<u>+</u>		
Your Certificates	People Se	ervers Authori	ties	
You have certificates or	ı file that identify tl	hese servers		
				E\$
the second second second				Ê
	lad an aits	e Person	1 ···	- E
and available	an same		Same of a	10 0
Sec. 114, 1146-1	r le l'Anterne et	and means	www.good.com	1.2
- test pild	ala si ji teran	de la Remaine	Damap 1 - 2	. * 1 0
wheels a school	alas vieta a	elada. Penere a	Dana Auto	n.0
a legt at the				
improvince	s na staate	and a second	and a second second	
s djære				¥
		Add Exceptio	on	
				ОК

• 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**.

Add Security Exception	×
You are about to override how Legitimate banks, stores, and this.	v Firefox identifies this site. Id other public sites will not ask you to do
Location: https://localhost:8443	Get Certificate
	<u>V</u> iew
Permanently store this exception	
	Confirm Security Exception Cancel

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



Add Security Exception	×
You are about to override how Firefox identifies this site Legitimate banks, stores, and other public sites will a this.	e. not ask you to do
Location: https://localhost:8443	Get Certificate
This site attempts to identify itself with invalid information.	<u>V</u> iew
Unknown Identity The certificate is not trusted because it hasn't been verified as iss authority using a secure signature.	sued by a trusted
Permanently store this exception	
Confirm Security Except	tion Cancel

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

		Certificate	Manager		
Your Certificat	es Peo	ple Servers	Authorities		
′ou have certifica	tes on file th	at identify these s	ervers		
∽ Bruker					î
localhost		localhost:8443	Permanent	Wednesday, August 1	
e testas tigata					
nama 21 s	na Stata	worself some	. Permanent	basiy Beerin 1	ł
service day	u lanske	and in the selection	I VERSION DE	streaking unity on a stream	
SAKIRA V	an tatan s	wirw1 witW1	- Parrienal	Mundes Adv 18 2044	
and all all	l luha lu	gi tude de 88	S. Permanent	Minday July 18, 5977	
in the second second	u aven az	nmer spract m	I NEW MARK	executing any injection	
- Արֆունդ					
	Export	Delete	Add Exception		
View	Laportan	Deleter	nua L <u>x</u> ception		
<u>V</u> iew					
<u>V</u> iew				ОК	

• 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.



Edge edge:// flags /#allow-insecure-localhost	Z
Q Search flags	Reset all
Allow invalid certificates for resources loaded from localhost.	
Allows requests to localhost over HTTPS even when an invalid certificate is presented. –	Enabled N
Mac, Windows	
<u>#allow-insecure-localhost</u>	
Override software rendering list	
Overrides the built-in software rendering list and enables GPU-acceleration on unsupported	Disabled
system configurations. – Mac, Windows	Diction
<u>#ignore-gpu-denylist</u>	

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:

localhost:8443	
$\widehat{(\times)}$	This site is not secure
\checkmark	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.



6.2.4. 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 Previous Setting Next Setting					
O Not Configured	Comment:				~
O Enabled					
Disabled					\vee
	Supported on:	Microsoft Edge on Windows 10, Ver	sion 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.
OK Cancel Apply



6.3 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.





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

