SAML authentication for Brainloop Secure Dataroom as of version 8.40.200 – Setup Guide

Content

1 Introduction

Security Assertion Markup Language 2.0 (SAML 2.0) provides an additional degree of security by requiring users to authenticate themselves via an Identity Provider. This Identity Provider confirms that users are indeed who they claim to be.
SAML 2.0 is a version of the SAML standard for exchanging authentication and authorization data between security domains. This XML-based protocol uses security tokens containing assertions to pass information about a user login between a SAML authority (an Identity Provider) and a SAML consumer (a service provider). SAML 2.0 enables web-based authentication and authorization scenarios including cross-domain single sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user.

There are three main players in SAML:

- **Service Provider (Brainloop Secure Dataroom):** This is the web server the user wants to access.
- **Client:** A service that interacts with the Service Provider. A client can be, for example, a web app being accessed through a web browser.
- **Identity Provider:** This is the server that owns the user identities and credentials. Users authenticate themselves with the Identity Provider.

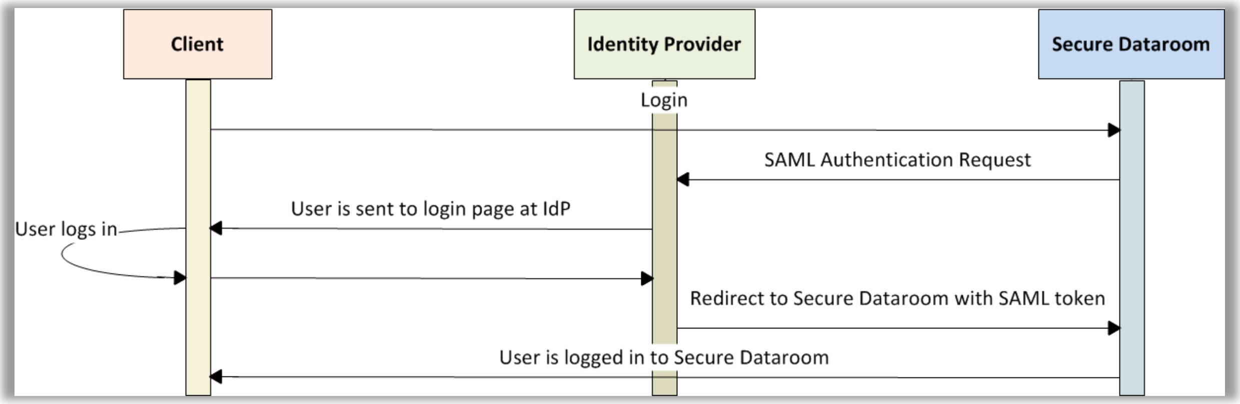

Client
Identity Provider
Secure Dataroom
Login
SAML Authentication Request
User is sent to login page at IdP
User logs in
Redirect to Secure Dataroom with SAML token
User is logged in to Secure Dataroom

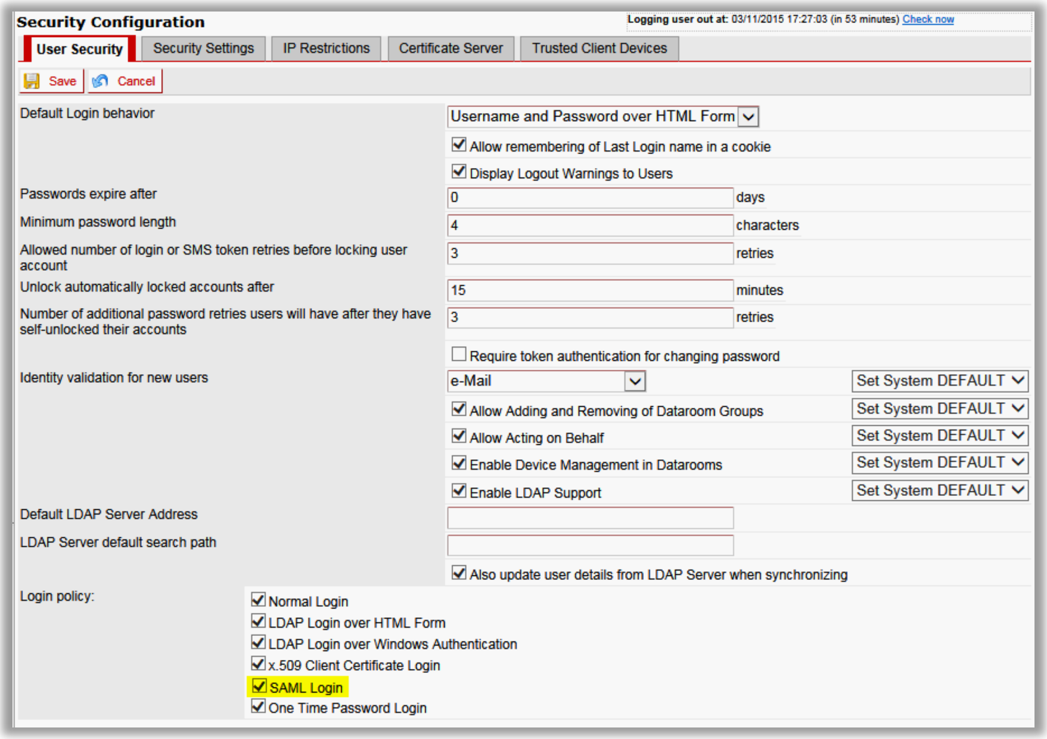
Figure 1: SP (Service Provider)-initiated scenario

2 Configure SAML authentication in Brainloop Secure Dataroom

2.1 Enable SAML authentication for the platform

To use SAML, it needs to be enabled at platform level by selecting the **SAML Login** option in the **Security Settings** of Application Administration:

1. Open **Application Administration**.
2. Select **Security Settings > User Security**.



Security Configuration

Logging user out at: 03/11/2015 17:27:03 (in 53 minutes) Check now

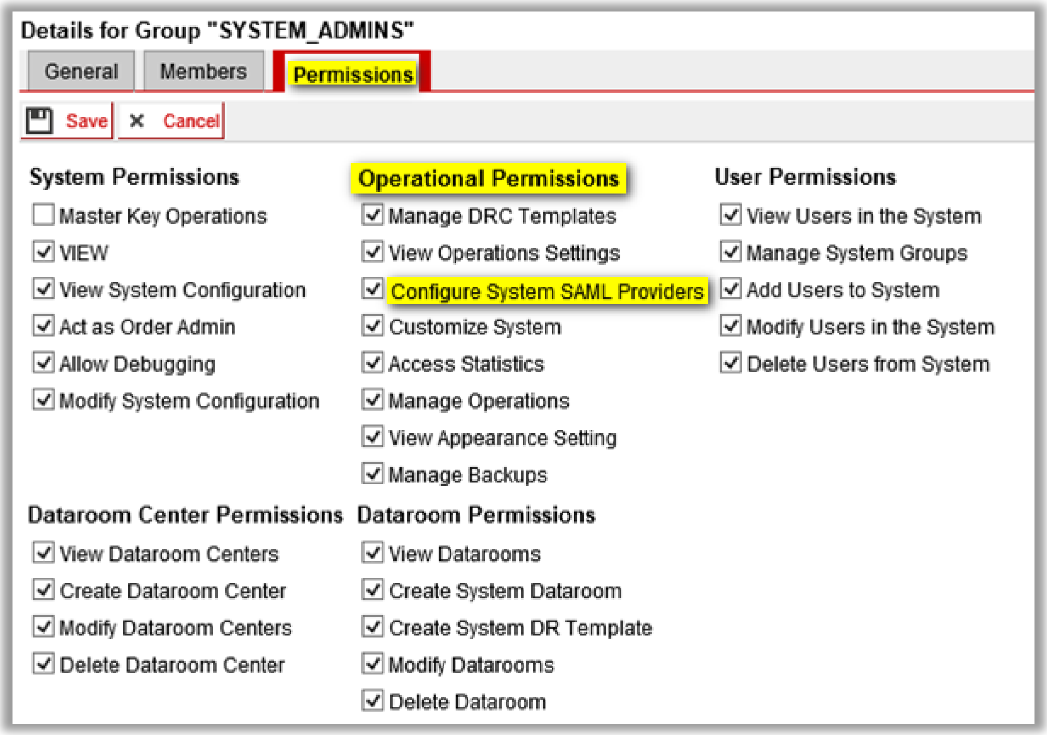
Default Login behavior	Username and Password over HTML Form
	☑ Allow remembering of Last Login name in a cookie
	☑ Display Logout Warnings to Users
Passwords expire after	0 days
Minimum password length	4 characters
Allowed number of login or SMS token retries before locking user account	3 retries
Unlock automatically locked accounts after	15 minutes
Number of additional password retries users will have after they have self-unlocked their accounts	3 retries
	☐ Require token authentication for changing password
Identity validation for new users	e-Mail — Set System DEFAULT
	☑ Allow Adding and Removing of Dataroom Groups — Set System DEFAULT
	☑ Allow Acting on Behalf — Set System DEFAULT
	☑ Enable Device Management in Datarooms — Set System DEFAULT
	☑ Enable LDAP Support — Set System DEFAULT
Default LDAP Server Address	
LDAP Server default search path	
	☑ Also update user details from LDAP Server when synchronizing
Login policy:	☑ Normal Login ☑ LDAP Login over HTML Form ☑ LDAP Login over Windows Authentication ☑ x.509 Client Certificate Login ☑ SAML Login ☑ One Time Password Login

3. In the **Login policy** area, enable the **SAML Login** option.

2.2 Enable Operational Permissions to configure SAML Identity Providers

Application Administrators as well as Dataroom Center Administrators can register SAML Identity Providers centrally in the Security Configuration. To configure and manage SAML Identity Providers at platform level, make sure that the **Operational Permissions** are enabled in the **Application Administration**:

1. Open **Application Administration**.
2. Search for the username of the user or user group you would like to edit and select it from the results list.
3. Select the **Permissions** tab.



Details for Group "SYSTEM_ADMINS"

System Permissions

- □ Master Key Operations
- ☑ VIEW
- ☑ View System Configuration
- ☑ Act as Order Admin
- ☑ Allow Debugging
- ☑ Modify System Configuration

Operational Permissions

- ☑ Manage DRC Templates
- ☑ View Operations Settings
- ☑ Configure System SAML Providers
- ☑ Customize System
- ☑ Access Statistics
- ☑ Manage Operations
- ☑ View Appearance Setting
- ☑ Manage Backups

User Permissions

- ☑ View Users in the System
- ☑ Manage System Groups
- ☑ Add Users to System
- ☑ Modify Users in the System
- ☑ Delete Users from System

Dataroom Center Permissions

- ☑ View Dataroom Centers
- ☑ Create Dataroom Center
- ☑ Modify Dataroom Centers
- ☑ Delete Dataroom Center

Dataroom Permissions

- ☑ View Datarooms
- ☑ Create System Dataroom
- ☑ Create System DR Template
- ☑ Modify Datarooms
- ☑ Delete Dataroom

4. In the **Operational Permissions** area, enable the **Configure System SAML Providers** option.

2.3 Add and configure SAML Identity Providers for the platform

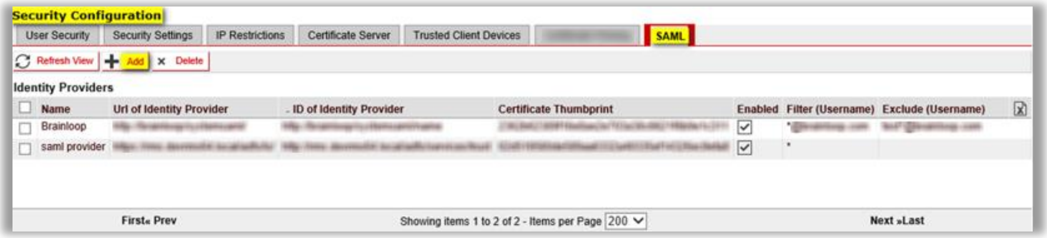
To centrally register and manage SAML Identity Providers in the Security Configuration, follow the steps described in this section.

Note: Application Administrators can register SAML Identity Providers centrally in the Security Configuration. At that stage, the Identity Provider's status is *Disabled* for Dataroom Centers.

To enable or disable an Identity Provider for a Dataroom Center, the Dataroom Center Administrator must select an available Identity Provider for a Dataroom Center and enable or disable the Identity Provider as needed.

2.3.1 Add a SAML Identity Provider

1. In the Application Administration, open **Security Settings**.
2. Select the **SAML** tab.

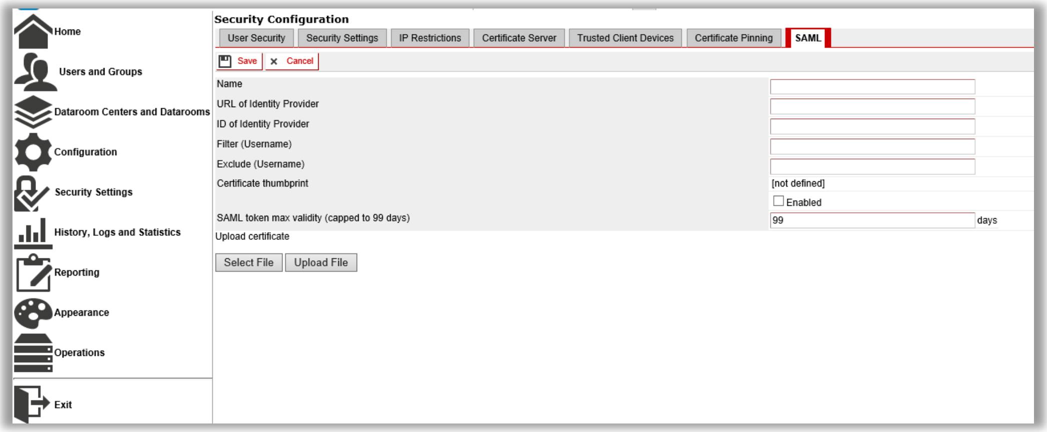


Identity Providers

□	Name	Url of Identity Provider	ID of Identity Provider	Certificate Thumbprint	Enabled	Filter (Username)	Exclude (Username)
□	Brainloop	[redacted]	[redacted]	[redacted]	☑	*[redacted]	[redacted]
□	saml provider	[redacted]	[redacted]	[redacted]	☑	*	

First« Prev Showing items 1 to 2 of 2 - Items per Page 200 Next »Last

3. Click **Add** to register a new SAML Identity Provider.
4. The following dialog is displayed.



Name	
URL of Identity Provider	
ID of Identity Provider	
Filter (Username)	
Exclude (Username)	
Certificate thumbprint	[not defined]
	□ Enabled
SAML token max validity (capped to 99 days)	99 days
Upload certificate	

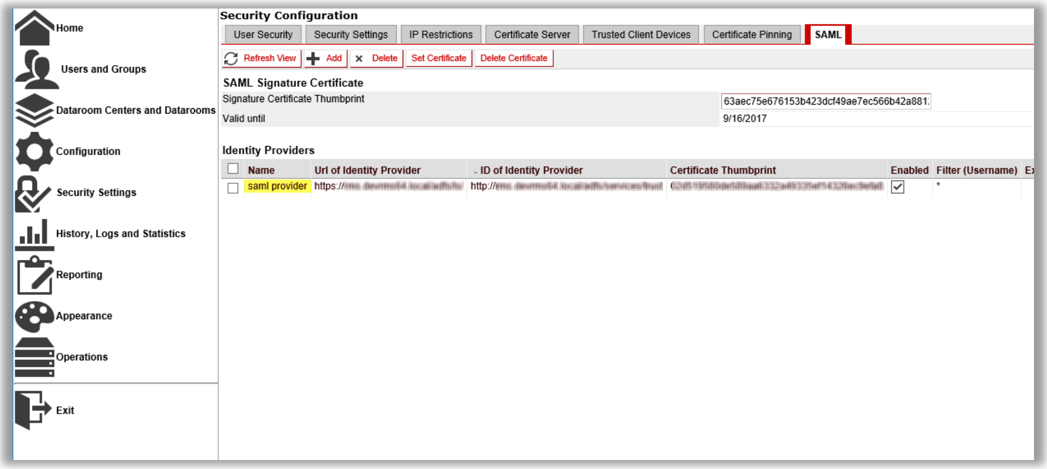
- **Name:** Enter a friendly name.
- **URL of Identity Provider**: Enter the URL that the SAML request is sent to.
- **ID of Identity Provider**: Enter the ID of the SAML Identity Provider. This ID is available on the ADFS server.
- **Filter (Username):** Add usernames of users and user groups to enable them to use this SAML Identity Provider to log into the Dataroom Center. Semicolons are used as separators.
- **Exclude (Username):** Add usernames of individual users or subgroups from the previously defined filter. This excludes these users from using this SAML Identity Provider to log into the Dataroom Center. This function is, for example, helpful when certain user groups need to use different SAML Identity Providers. It can also be used to ensure that only one specific Identity Provider is used for a particular user.
- **Certificate thumbprint:** This field is populated automatically when uploading a valid certificate.
- **Enabled:** Use this checkbox to enable or disable the registered Identity Provider for the platform.
- **SAML token max validity (capped to 99 days)**: This field specifies the time in days for which SAML authentication tokens are valid for the respective Brainloop Client.

5. Click on **Upload certificate** to upload the certificate that is used for signing the SAML response message on the Identity Provider’s side. This step automatically populates the **Certificate thumbprint** field.

2.3.2 Edit a SAML Identity Provider

Once the SAML Identity Provider has been set up, it appears in the **Identity Providers** list on the **SAML** tab.

1. Click the name of the Identity Provider to open the pane **Details for Identity Provider**.



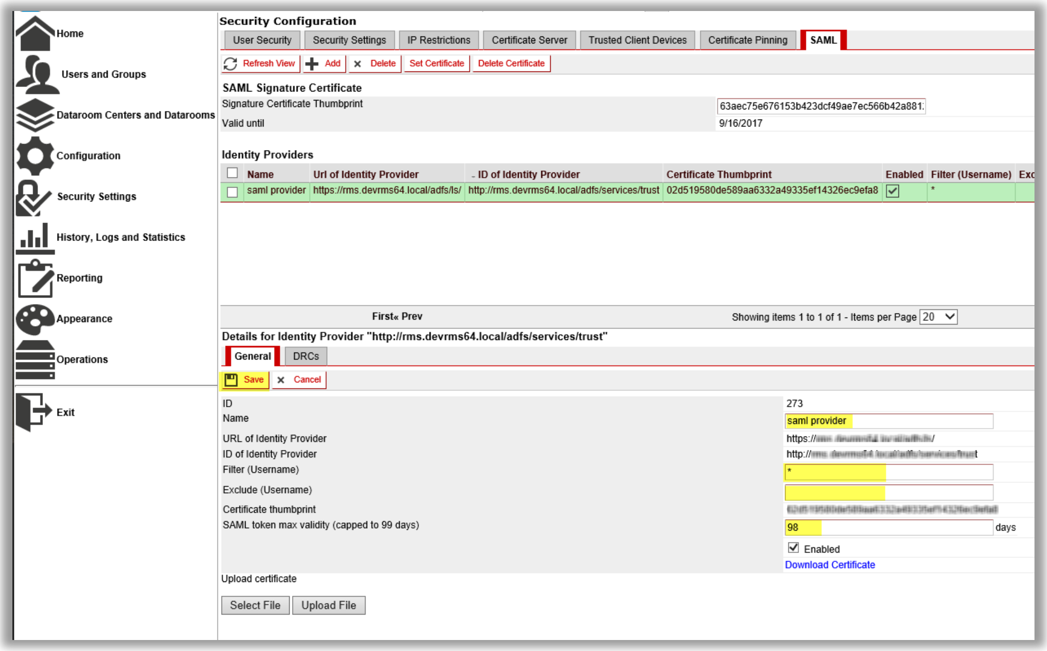
SAML Signature Certificate

Signature Certificate Thumbprint	63aec75e676153b423dcf49ae7ec566b42a881:
Valid until	9/16/2017

Identity Providers

□	Name	Url of Identity Provider	ID of Identity Provider	Certificate Thumbprint	Enabled	Filter (Username)	Ex
□	saml provider	https://[redacted]	http://[redacted]	[redacted]	☑	*	

2. On the **General** tab, click **Edit** to modify the settings. Modify the settings as needed and then click **Save**.



SAML Signature Certificate

Signature Certificate Thumbprint	63aec75e676153b423dcf49ae7ec566b42a881:
Valid until	9/16/2017

Identity Providers

□	Name	Url of Identity Provider	ID of Identity Provider	Certificate Thumbprint	Enabled	Filter (Username)	Exc
□	saml provider	https://rms.devrms64.local/adfs/ls/	http://rms.devrms64.local/adfs/services/trust	02d519580de589aa6332a49335ef14326ec9efa8	☑	*	

Showing items 1 to 1 of 1 - Items per Page 20

Details for Identity Provider "http://rms.devrms64.local/adfs/services/trust"

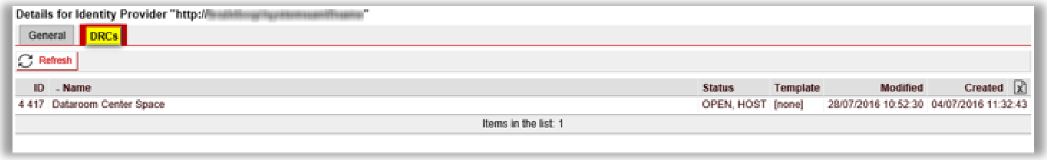
ID	273
Name	saml provider
URL of Identity Provider	https://[redacted]/
ID of Identity Provider	http://[redacted]t
Filter (Username)	*
Exclude (Username)	
Certificate thumbprint	[redacted]
SAML token max validity (capped to 99 days)	98 days
	☑ Enabled

Upload certificate

Note: The URL and the ID of the SAML Identity Provider cannot be edited. If any

of these fields need to be changed, it is necessary to delete the Identity Provider and to create a new one.

3. Click the **DRCs** tab to view a list of Dataroom Centers that are using the selected Identity Provider.



Details for Identity Provider "http://[redacted]"

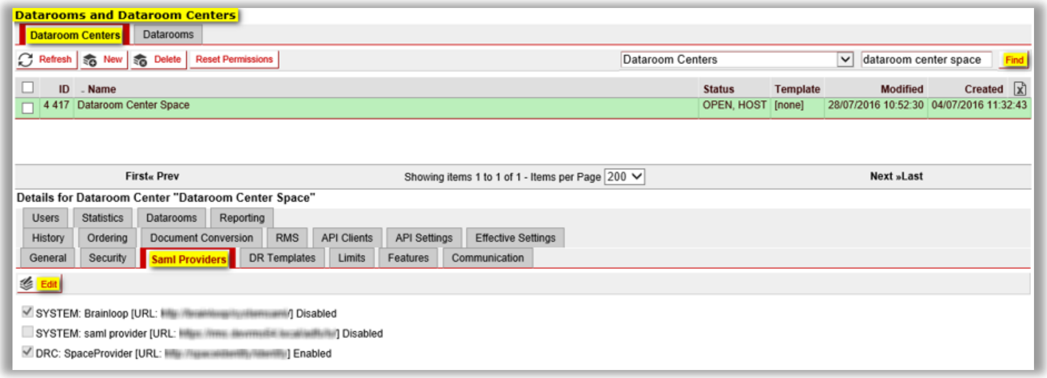
ID	Name	Status	Template	Modified	Created
4 417	Dataroom Center Space	OPEN, HOST	[none]	28/07/2016 10:52:30	04/07/2016 11:32:43

Items in the list: 1

2.3.3 Link a SAML Identity Provider to a Dataroom Center or to a DRC Template

A SAML Identity Provider can be linked to more than one Dataroom Center. Follow the steps below to make an existing Identity Provider available to additional Dataroom Centers.
In addition, SAML Identity Providers can be configured and linked to a Dataroom Center Template by Application Administrators. Dataroom Centers created from that template are automatically configured for these SAML Identity Providers.

1. Open the Application Administration.
2. Select Datarooms and Dataroom Centers. By default, the Dataroom Centers tab is shown.
3. Use the search field to find your Dataroom Center or Dataroom Center Template.
4. In the results pane, click the ID or name of the Dataroom Center or Dataroom Center template to open the **Details for Dataroom Center** pane.



Datarooms and Dataroom Centers

Dataroom Centers | dataroom center space

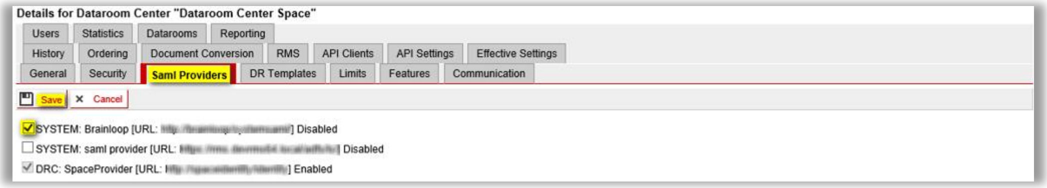
□	ID	Name	Status	Template	Modified	Created
□	4 417	Dataroom Center Space	OPEN, HOST	[none]	28/07/2016 10:52:30	04/07/2016 11:32:43

Showing items 1 to 1 of 1 - Items per Page 200

Details for Dataroom Center "Dataroom Center Space"

☑ SYSTEM: Brainloop [URL: [redacted]] Disabled
□ SYSTEM: saml provider [URL: [redacted]] Disabled
☑ DRC: SpaceProvider [URL: [redacted]] Enabled

5. In the **Dataroom Centers** pane, select the **SAML Providers** tab and click **Edit**.
6. Select SAML Identity Providers by enabling the corresponding options, and click **Save**.



Details for Dataroom Center "Dataroom Center Space"

☑ SYSTEM: Brainloop [URL: [redacted]] Disabled
☐ SYSTEM: saml provider [URL: [redacted]] Disabled
☑ DRC: SpaceProvider [URL: [redacted]] Enabled

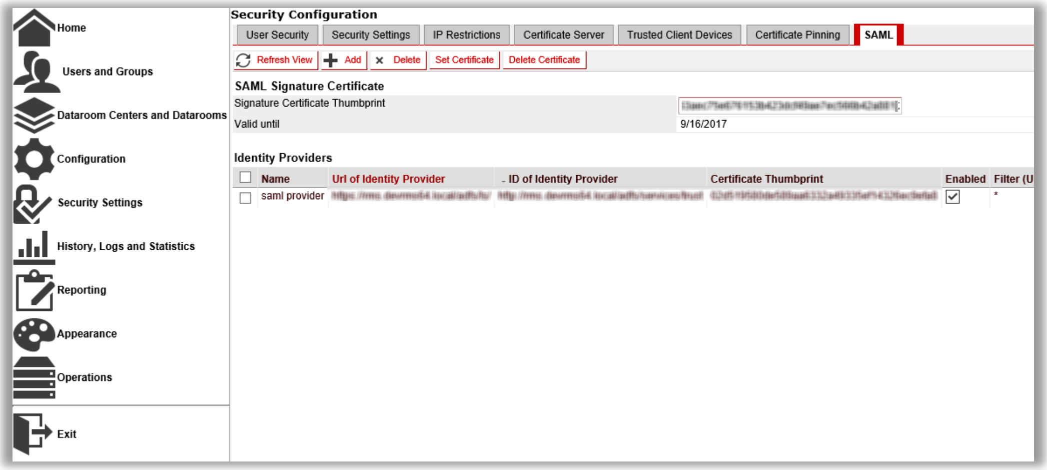
> **Note: SAML Identity Providers configured by the Dataroom Center Administrator are displayed in this list but cannot be edited.**

2.4 Configure SAML authentication reset for the platform

When logging off from Brainloop Secure Dataroom it is recommended, in particular for shared computers, to reset the SAML server authentication by enabling the corresponding option **Reset SAML server authentication** in the **Logout** dialog.

To make this option available to the users, it needs to be configured in the Application Administration:

1. Install a new SAML signature certificate (RSA SHA265 Certificate with Private Key) into the Local Computer Personal Certificate Store on each server farm member.
2. Add the certificate in the **Application Administration**:
   Application Administration > **Security Settings** > **SAML**.



Security Configuration

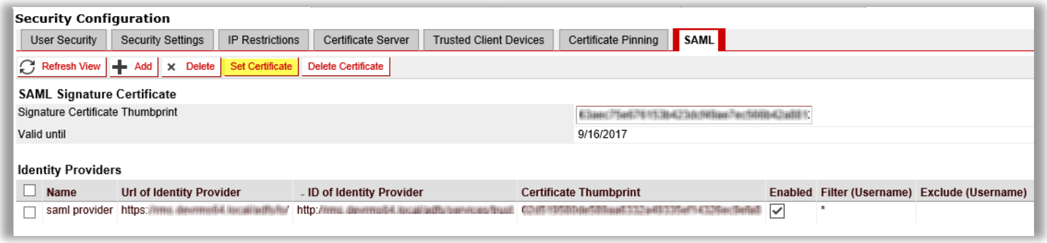
SAML Signature Certificate

Signature Certificate Thumbprint	[redacted]
Valid until	9/16/2017

Identity Providers

☐	Name	Url of Identity Provider	ID of Identity Provider	Certificate Thumbprint	Enabled	Filter (U
☐	saml provider	[redacted]	[redacted]	[redacted]	☑	*

3. Click the **Set Certificate** button in the **SAML Signature Certificate** section to add the certificate.



Security Configuration

SAML Signature Certificate

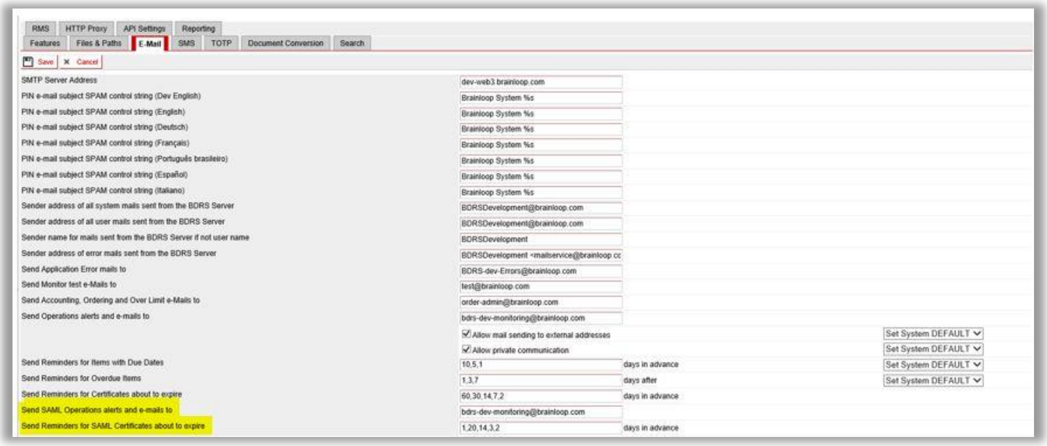
Signature Certificate Thumbprint	[redacted]
Valid until	9/16/2017

Identity Providers

☐	Name	Url of Identity Provider	ID of Identity Provider	Certificate Thumbprint	Enabled	Filter (Username)	Exclude (Username)
☐	saml provider	https://[redacted]	http://[redacted]	[redacted]	☑	*	

2.5 Schedule the SAML alerts and reminders

Brainloop Secure Dataroom Application Administrators and Dataroom Center Administrators are notified when a certificate used for SAML Login will soon expire. Under **Application Administration > Configuration > E-Mail**, you can set the notification cycle for different information items.



SMTP Server Address	dev-web3.brainloop.com		
PIN e-mail subject SPAM control string (Dev English)	Brainloop System %s		
PIN e-mail subject SPAM control string (English)	Brainloop System %s		
PIN e-mail subject SPAM control string (Deutsch)	Brainloop System %s		
PIN e-mail subject SPAM control string (Français)	Brainloop System %s		
PIN e-mail subject SPAM control string (Português brasileiro)	Brainloop System %s		
PIN e-mail subject SPAM control string (Español)	Brainloop System %s		
PIN e-mail subject SPAM control string (Italiano)	Brainloop System %s		
Sender address of all system mails sent from the BDRS Server	BDRSDevelopment@brainloop.com		
Sender address of all user mails sent from the BDRS Server	BDRSDevelopment@brainloop.com		
Sender name for mails sent from the BDRS Server if not user name	BDRSDevelopment		
Sender address of error mails sent from the BDRS Server	BDRSDevelopment <mailservice@brainloop.cc		
Send Application Error mails to	BDRS-dev-Errors@brainloop.com		
Send Monitor test e-Mails to	test@brainloop.com		
Send Accounting, Ordering and Over Limit e-Mails to	order-admin@brainloop.com		
Send Operations alerts and e-mails to	bdrs-dev-monitoring@brainloop.com		
	☑ Allow mail sending to external addresses		Set System DEFAULT
	☑ Allow private communication		Set System DEFAULT
Send Reminders for Items with Due Dates	10,5,1	days in advance	Set System DEFAULT
Send Reminders for Overdue Items	1,3,7	days after	Set System DEFAULT
Send Reminders for Certificates about to expire	60,30,14,7,2	days in advance	
Send SAML Operations alerts and e-mails to	bdrs-dev-monitoring@brainloop.com		
Send Reminders for SAML Certificates about to expire	1,20,14,3,2	days in advance	

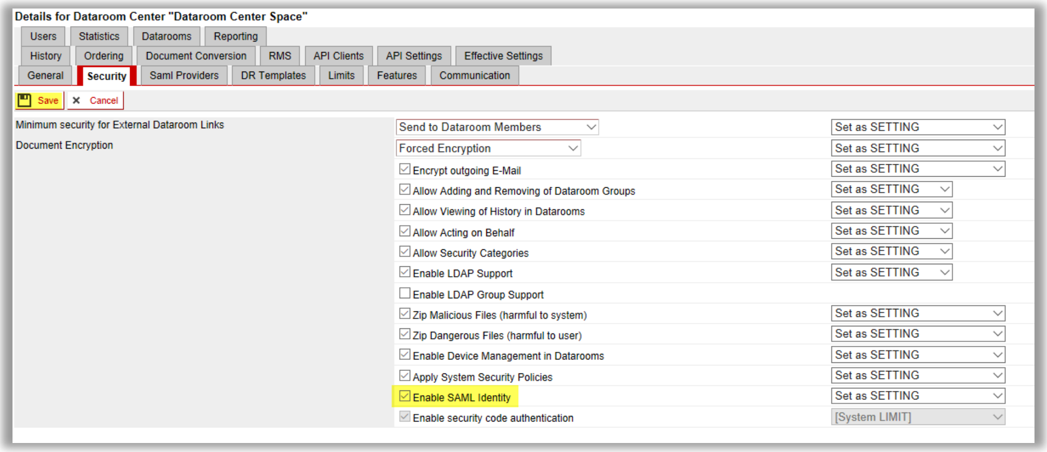
For SAML, set the following items:

- **Send SAML Operations alerts and e-mails to:** Enter the e-mail address to which SAML warnings and alerts should be sent.
- **Send reminders for SAML Certificates about to expire**: Enter the number of days beforehand that the Admins are informed that SAML Logins are about to expire. You can define several reminders at different intervals; for example, at 30, 20 and 10 days before the expiration date.

2.6 Enable SAML Identity Providers for a Dataroom Center

1. Open the **Application Administration**.
2. Use the search function to find the desired Dataroom Center.
3. In the results pane, enable the Dataroom Center or Dataroom Center template and click the ID or name to open the **Details for Dataroom Center** pane.
4. Select the **Security** tab and click **Edit**.

5. Enable the **Enable SAML Identity** option and click **Save**.



Details for Dataroom Center "Dataroom Center Space"

Minimum security for External Dataroom Links	Send to Dataroom Members	Set as SETTING
Document Encryption	Forced Encryption	Set as SETTING
	☑ Encrypt outgoing E-Mail	Set as SETTING
	☑ Allow Adding and Removing of Dataroom Groups	Set as SETTING
	☑ Allow Viewing of History in Datarooms	Set as SETTING
	☑ Allow Acting on Behalf	Set as SETTING
	☑ Allow Security Categories	Set as SETTING
	☑ Enable LDAP Support	Set as SETTING
	☐ Enable LDAP Group Support	
	☑ Zip Malicious Files (harmful to system)	Set as SETTING
	☑ Zip Dangerous Files (harmful to user)	Set as SETTING
	☑ Enable Device Management in Datarooms	Set as SETTING
	☑ Apply System Security Policies	Set as SETTING
	☑ Enable SAML Identity	Set as SETTING
	☑ Enable security code authentication	[System LIMIT]

2.7 Add and configure SAML Identity Providers in the Dataroom Center Administration

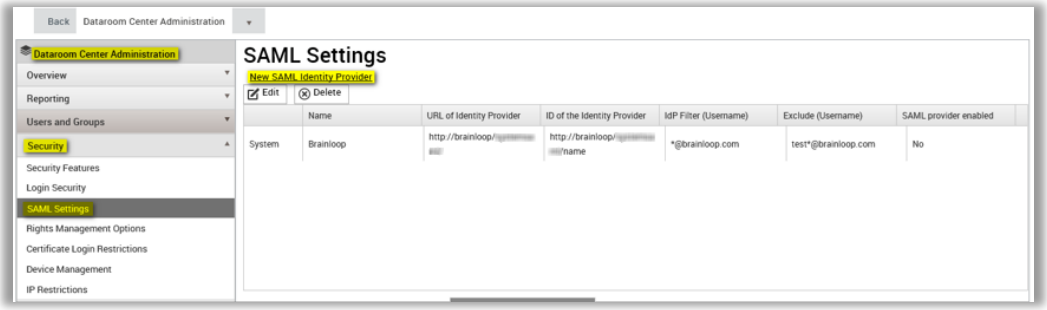
The individual settings for the SAML servers can be configured in the Dataroom Center Administration. These settings allow Dataroom Center Managers to connect to Dataroom Centers using different SAML servers.

> **!** **Caution: We highly recommend that every Dataroom Center has at least one non-SAML user as an administrator, in case the SAML configuration breaks.**

2.7.1 Add a SAML Identity Provider

Proceed as follows to register and manage SAML Identity Providers in the Dataroom Center Administration.

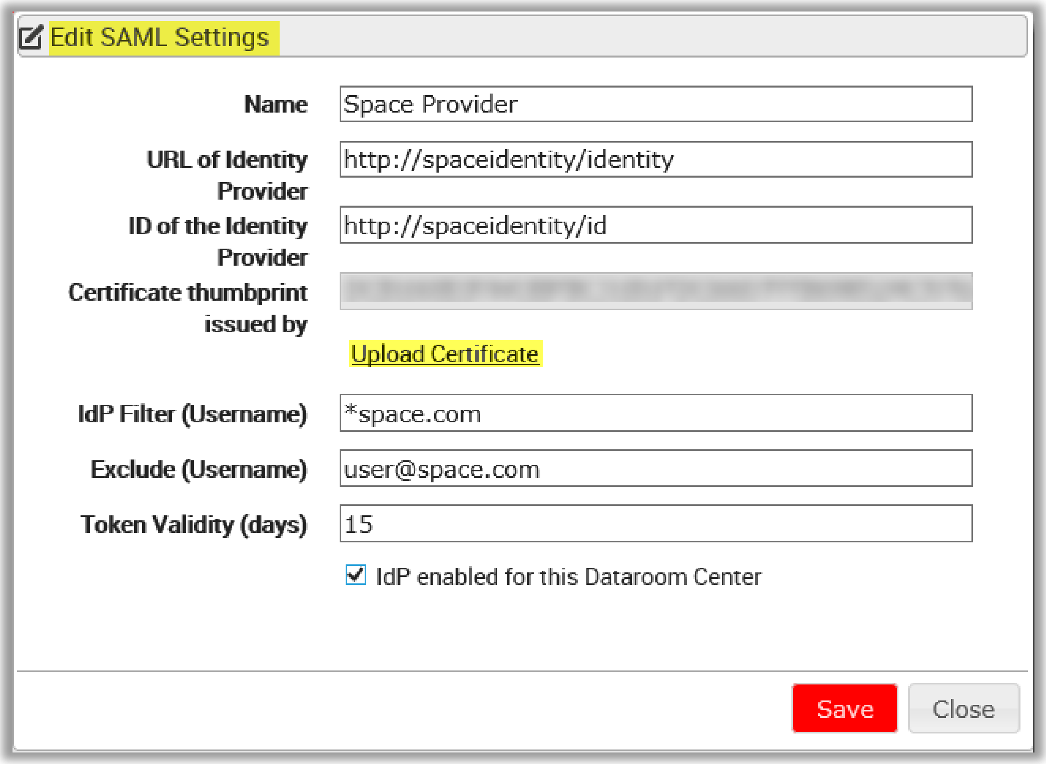
1. Open **Dataroom Center Administration.**
2. Select **Security > SAML Settings**.
3. Click **New SAML Identity Provider** to register a new SAML Identity Provider.


Back
Dataroom Center Administration
Dataroom Center Administration
Overview
Reporting
Users and Groups
Security
Security Features
Login Security
SAML Settings
Rights Management Options
Certificate Login Restrictions
Device Management
IP Restrictions
New SAML Identity Provider
Edit
Delete

SAML Settings

	Name	URL of Identity Provider	ID of the Identity Provider	IdP Filter (Username)	Exclude (Username)	SAML provider enabled
System	Brainloop	http://brainloop/[redacted]	http://brainloop/[redacted]/name	*@brainloop.com	test*@brainloop.com	No

The **Edit SAML Settings** dialog is displayed.



Edit SAML Settings

Name	Space Provider
URL of Identity Provider	http://spaceidentity/identity
ID of the Identity Provider	http://spaceidentity/id
Certificate thumbprint issued by	[redacted]
	Upload Certificate
IdP Filter (Username)	*space.com
Exclude (Username)	user@space.com
Token Validity (days)	15
	☑ IdP enabled for this Dataroom Center

- **Name**: Enter a friendly name.
- **URL of Identity Provider**: Enter the URL that the SAML request is sent to.
- **ID of Identity Provider**: Enter the ID of the SAML Identity Provider. This ID is available on the ADFS server.
- **Certificate thumbprint issued by:** This field is populated automatically when uploading a valid certificate.
- **Upload Certificate**: Upload the certificate that is used for signing the SAML response message on the Identity Provider's side. This step automatically populates the **Certificate thumbprint** field.
- **IdP Filter (Username):** Add usernames of users and user groups to enable them to use this SAML Identity Provider to log into the Dataroom Center. Semicolons are used as separators.
- **Exclude (Username):** Add usernames of individual users or sub-groups from the previously defined filter. This excludes these users from using this SAML Identity Provider to log into the Dataroom Center. This function is helpful, for example, when certain user groups need to use different SAML Identity Providers. It can also be used to ensure that only one specific Identity Provider is used for a particular user.
- **IdP enabled for this Dataroom Center:** Enable this option to enable the registered Identity Provider for this Dataroom Center.

New in 8.40.200:

- **Token validity (days):** Enter the number of days for which SAML authentication tokens are valid for the respective Brainloop Client per SAML Identity Provider.

4. Click **Save**.
   The list of configured Identity Providers for this Dataroom Center is displayed.

2.7.2 Edit a SAML Identity Provider

1. Open the **Dataroom Center Administration**.
2. Select **Security > SAML Settings**.
3. Select the desired SAML Identity Provider.
4. Click **Edit**.
   The **Edit SAML Settings** dialog is displayed.

i **Note: The URL and the ID of the SAML Identity Provider cannot be edited. If any of these fields need to be changed, it is necessary to delete the Identity Provider and to create a new one.**

5. Make the desired changes.

! **Caution: Make sure your changes are correct, otherwise you might not be able to log in again.**

6. Click **Save**.

2.7.3 Delete a SAML Identity Provider

! **Caution: Before deleting a SAML Identity Provider from Brainloop Secure Dataroom, make sure that you have another non-SAML user login for the respective Dataroom Center. You must have this additional user login to ensure that you do not lock yourself out of the Dataroom Center.**

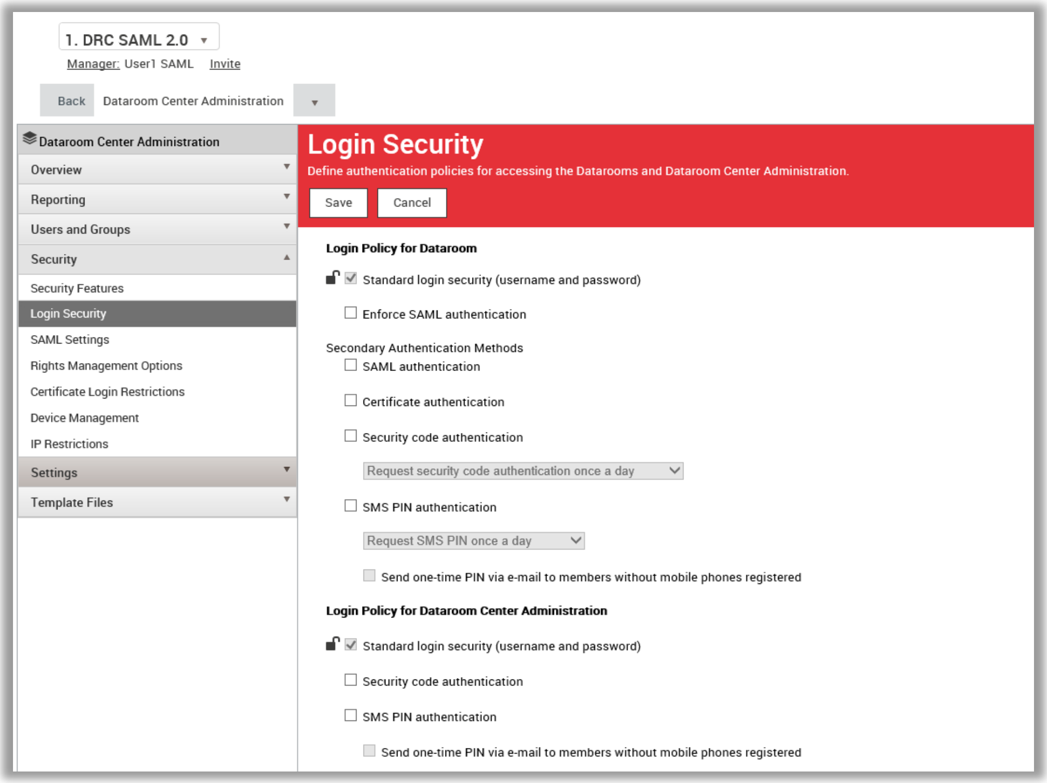
1. Open **Dataroom Center Administration**.
2. Select **Security** > **SAML Settings**.

3. Select the desired SAML Identity Provider.
4. Click **Delete** and confirm that you want to delete the Identity Provider.

2.8 Define the login behavior with SAML authentication

Once **SAML authentication** has been configured and enabled for Dataroom Centers or Datarooms the authentication policies must be defined by selecting the corresponding authentication methods. Depending on the configuration of the login behavior, authentication methods will be required for users, or made available to them, in order to be granted access Brainloop Datarooms.

1. Open the **Dataroom Center Administration** or **Dataroom Administration**.
2. Select **Security** > **Login Security**.
3. This pane displays all authentication options which are available or have been configured for the corresponding **Dataroom Center Administration** or **Dataroom Administration**.
4. Click **Edit**.



Login Security

Define authentication policies for accessing the Datarooms and Dataroom Center Administration.

Login Policy for Dataroom

☑ Standard login security (username and password)

□ Enforce SAML authentication

Secondary Authentication Methods

□ SAML authentication

□ Certificate authentication

□ Security code authentication

Request security code authentication once a day

□ SMS PIN authentication

Request SMS PIN once a day

□ Send one-time PIN via e-mail to members without mobile phones registered

Login Policy for Dataroom Center Administration

☑ Standard login security (username and password)

□ Security code authentication

□ SMS PIN authentication

□ Send one-time PIN via e-mail to members without mobile phones registered

5. Select the desired authentication methods.
   SAML authentication can be enforced for Datarooms. In this case, users without a SAML login will no longer be able to access the Dataroom. Alternatively, multiple authentication methods can be set up by using the section **Secondary Authentication Methods**.
   Under **Login Policy for Dataroom**, the basic authentication options can be specified for users:

- **Standard login security (username and password)**: Users log in using a username and password. This option is the default.
- **Enforce SAML authentication:** Users are forced to authenticate themselves via a SAML server if a SAML server has been configured for the Dataroom Center

! **Caution: If this option is selected, users without SAML login will no longer be able to access the respective Dataroom or Dataroom Center.**

Under **Secondary Authentication Methods**, you can configure additional login behavior options:

- **SAML authentication:** If SAML authentication has been enabled as a secondary method, and, for example, SMS PIN authentication is activated, SAML users can enter a Dataroom *without* having to provide an additional SMS PIN.

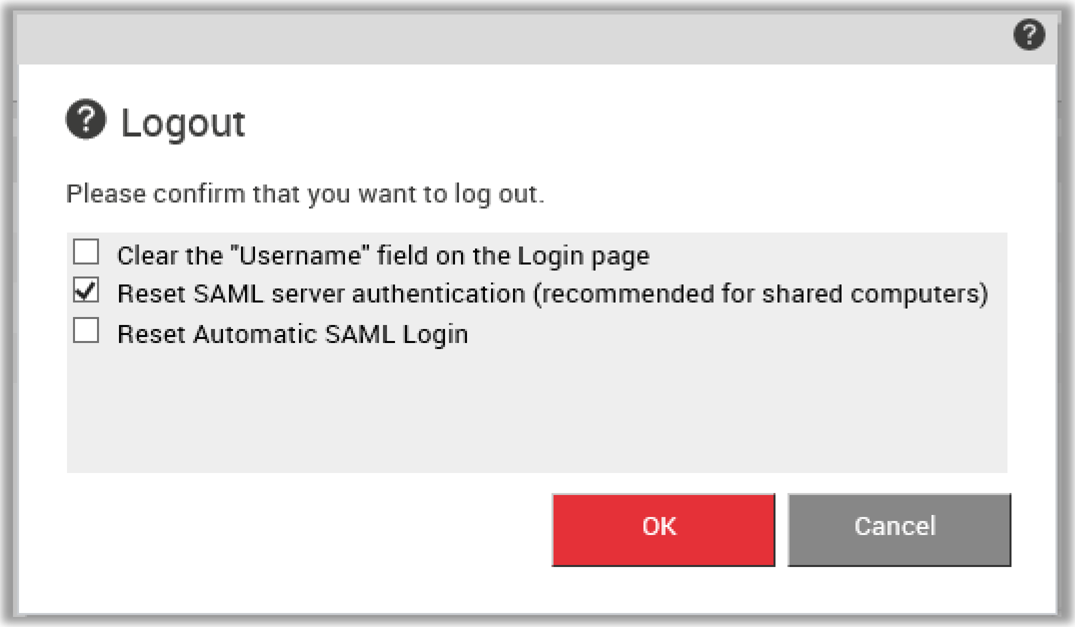
i **Note: This only applies if the user is logged in to the SAML server configured for this particular login authentication for this Dataroom Center. When using a different SAML server lacking this configuration to access this Dataroom Center, the SMS PIN must be entered.**

! **Caution: This option is only recommended for organizations with an established and secure two-factor SAML login process in place. Otherwise, your access security is weakened.**

- **Security code authentication**: When entering a Dataroom protected with a time-based, one-time password in the form of an automatically-generated security code, users are prompted to authenticate themselves by entering this security code.
- **Certificate authentication**: If certificate authentication and, for example, SMS PIN are enabled at the same time, SAML users with a valid certificate can log in without having to provide an additional SMS PIN.
- **SMS PIN authentication**: Users are prompted to authenticate with a PIN when entering a Dataroom. The PIN is sent to the user via SMS. You can also define the PIN prompt frequency here (once a day, once a week or once per session).
  Moreover, you can enable the permission to send the PIN via e-mail to members without a registered mobile phone.

2.9 Select logout behavior for SAML authentication

If SAML authentication has been enabled for your Datarooms and the SAML signature certificate has been configured in the Application Administration, we recommend that you use the new default option called **Reset SAML server authentication** for the **Logout** dialog.



Logout

Please confirm that you want to log out.

- ☐ Clear the "Username" field on the Login page
- ☑ Reset SAML server authentication (recommended for shared computers)
- ☐ Reset Automatic SAML Login

Functionality of the available logout options:

- **Clear the Username field on the Login page**: This removes the username information from the **Username** field in the **Login** dialog.
- **Reset SAML server authentication (recommended for shared computers)**: This is the recommended default option if you work with SAML authentication. With this option selected, when users log out of the Brainloop Secure Dataroom, they are automatically logged out of the SAML server as well. This enables the same user (or a different user) to then log in using a different Dataroom login having other user credentials by going back to the login screen.
- **Reset automatic SAML login**: With this option selected, the system reverts to the regular Brainloop Secure Dataroom login the next time the user logs in.

3 Log in to Brainloop Secure Dataroom using SAML authentication

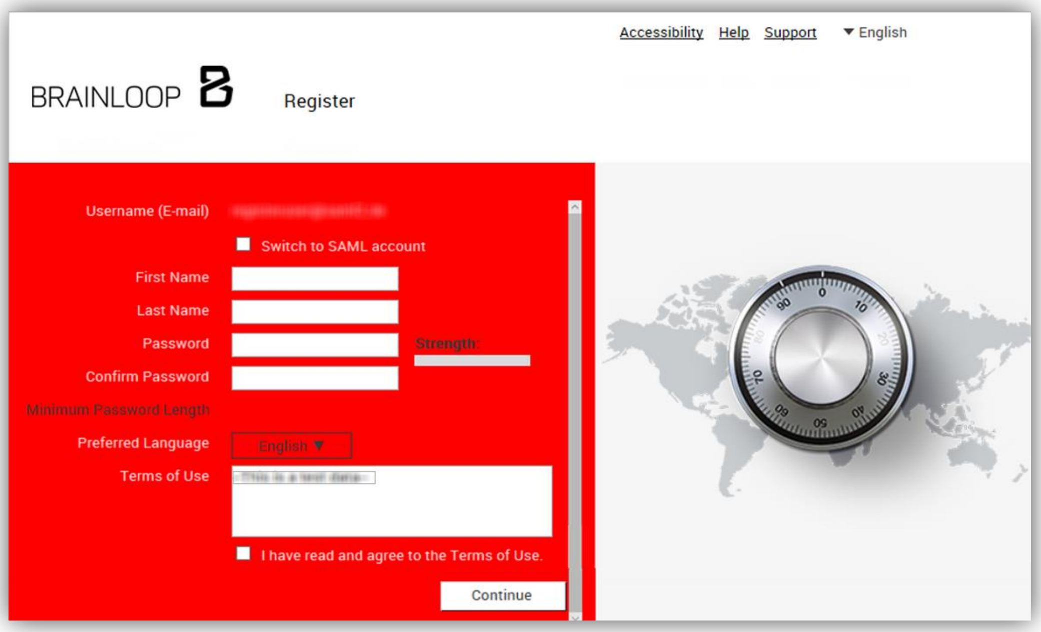
Once SAML authentication is configured in a Dataroom Center, users can log in to Brainloop Secure Dataroom via SAML authentication. Users who have access to this Dataroom Center and have a username that matches the configured login filter are shown the **Select SAML Authentication Server** dialog when they log in to Brainloop Secure Dataroom.

> **Note: Once a user has logged in via SAML authentication, this login method can only be reversed at the platform level (see chapter "Reset the SAML login for a user" on page 23ff).**

3.1 Unregistered users: Register and log in via SAML authentication

If you have not yet registered with Brainloop Secure Dataroom and want to log in to your Datarooms via SAML authentication, you can register and authenticate via your SAML server in one flow.

1. Open your Brainloop Secure Dataroom invitation e-mail and click the link it contains.
   The Brainloop Secure Dataroom registration page is displayed.



Username (E-mail)

☐ Switch to SAML account

First Name

Last Name

Password Strength

Confirm Password

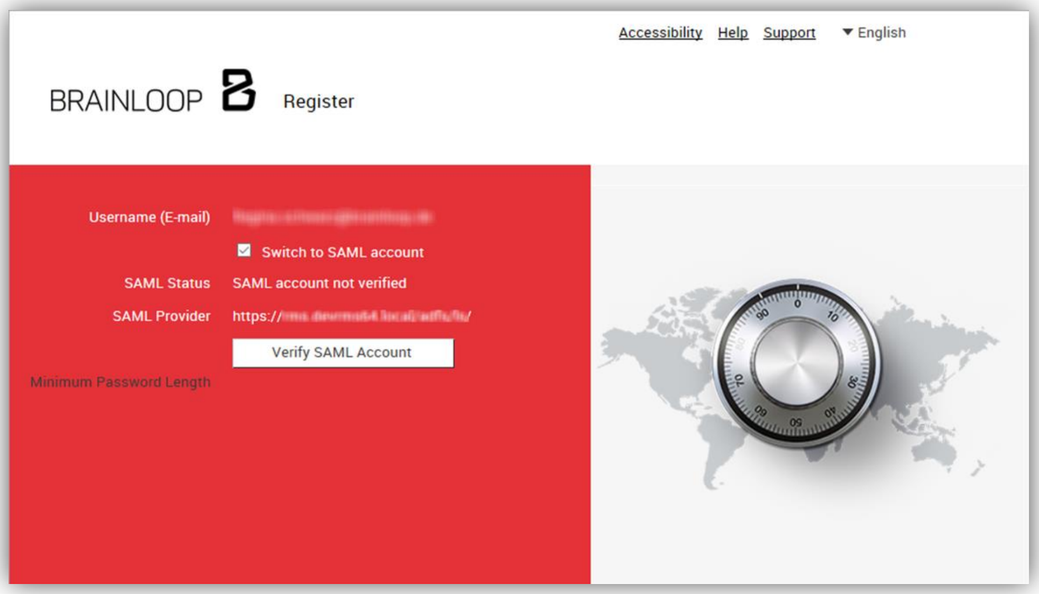
Minimum Password Length

Preferred Language English ▼

Terms of Use

☐ I have read and agree to the Terms of Use.

2. Enter the required information and enable the **Switch to SAML account** option. The next registration page appears. In it, the **Switch to SAML account** option is marked and below that line it says **SAML Status - SAML account not verified**.



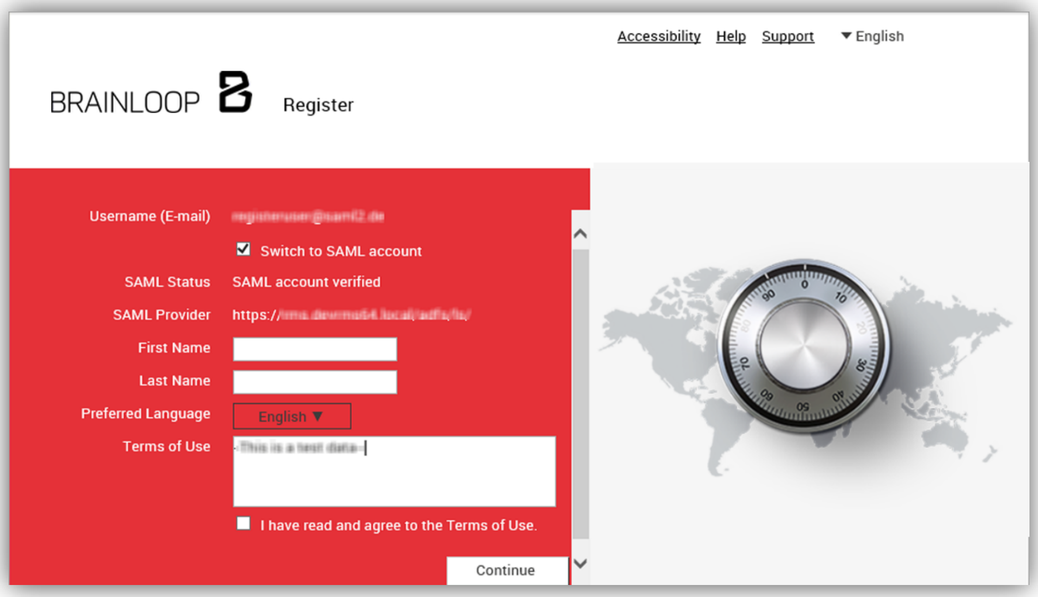
Username (E-mail) [redacted]

☑ Switch to SAML account

SAML Status SAML account not verified

SAML Provider https://[redacted]

3. Click **Verify SAML Account**. After logging on to the SAML server, the next registration page is displayed and the **SAML Status** now is **SAML account verified**.



Username (E-mail) [redacted]

☑ Switch to SAML account

SAML Status SAML account verified

SAML Provider https://[redacted]

First Name

Last Name

Preferred Language English ▼

Terms of Use [redacted]

☐ I have read and agree to the Terms of Use.

4. Enter the first name and last name, and confirm that you have read and agree to the Terms of Use.
5. Click **Continue**.
6. If necessary, enter your credentials (i.e. username and password) for the configured SAML server and confirm them.

   You are now registered and logged in to Brainloop Secure Dataroom.

3.2 Registered users: Log in via SAML authentication

If you have already registered with Brainloop Secure Dataroom and want to log in to your Datarooms via SAML authentication for the first time, proceed as follows:

1. Open the login page of Brainloop Secure Dataroom in your browser.
2. Enter your username and click the ♻ icon.
3. If required, select the required SAML authentication server and click **OK**.
   Note that this step is only available if you can connect via several SAML providers.
4. Enter your credentials (i.e. username and password) for the configured SAML server.
5. In the e-mail you receive, click the link to confirm your SAML server.
6. Click **OK** to confirm the SAML server.
   The Brainloop Secure Dataroom login page is displayed.
7. Enter your username (e-mail address) and click **Login**.
   Note that you do not have to enter a password since it is no longer valid.
8. If required, enter your credentials (i.e. username and password) for the configured SAML server and confirm them. You are logged in to Brainloop Secure Dataroom.

3.3 Log in to Brainloop Secure Dataroom using SAML authentication

If you have already registered with Brainloop Secure Dataroom and have confirmed your SAML provider:

1. Open Brainloop Secure Dataroom in your browser.
2. Enter your username (e-mail address) and click **Login**.
3. If required, enter your credentials (i.e. username and password) for the configured SAML server and confirm them.
   You are logged in to Brainloop Secure Dataroom.

3.4 Log in via different SAML servers

If you are a member of multiple Dataroom Centers and have to use different SAML servers to log in, you can use the ♻ icon on the login page to select the correct SAML server.

1. Open Brainloop Secure Dataroom in your browser.
2. Enter your username (e-mail address).
3. Click the ♻ icon next to the **Login** button.
   The **Select SAML Authentication Server** dialog is displayed.
4. Select the required SAML authentication server and click **OK**.
5. If you have not yet confirmed the server, you have to do this first (see "Unregistered users: Register and log in via SAML authentication" for instructions).

6. Enter your credentials (i.e. username and password) for the configured SAML server and confirm these.
   You are logged in to Brainloop Secure Dataroom.

4 Single sign-on (SSO) from a portal

Brainloop Secure Dataroom supports SAML single sign-on. In this scenario, the partner portal generates and sends a SAML response to Brainloop Secure Dataroom that contains the authenticated user's login name (e-mail address). In accordance with the SAML 2.0 specification, this response is digitally signed with the partner's certificate. If Brainloop Secure Dataroom can verify the SAML response successfully, the user is logged in to Brainloop Secure Dataroom. In this case, the user does not have to select the SAML server. The first successful SSO login sets the SAML authentication method as the default login method for the user.

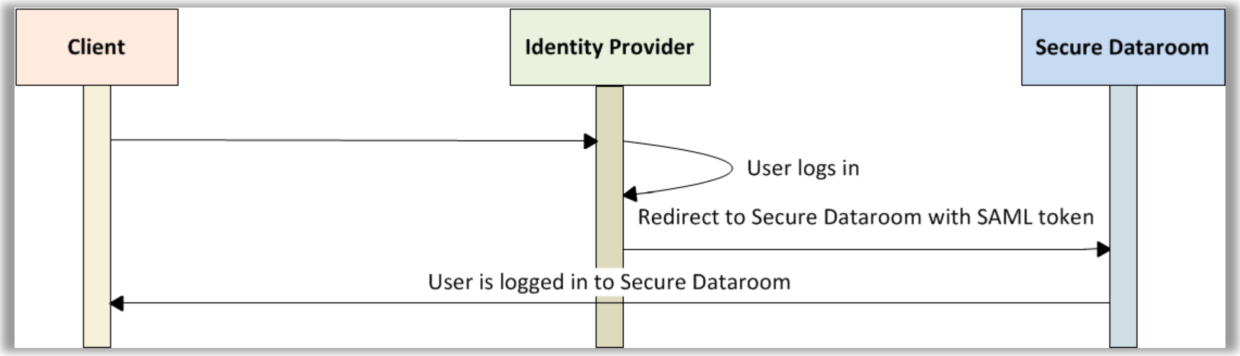

Client
Identity Provider
Secure Dataroom
User logs in
Redirect to Secure Dataroom with SAML token
User is logged in to Secure Dataroom

Figure 2: IdP (Identity Provider)-initiated scenario

5 Login via Brainloop Secure Client apps

Currently, SAML authentication is only implemented in the Brainloop Secure Client for iOS app and the Brainloop Secure Connector. As of Brainloop Secure Dataroom version 8.30.800, the Brainloop Secure Client for iOS app version 1.6 and newer is required.

When SAML users log in to the Dataroom server from within the app, a SAML login page is displayed where they have to enter their credentials once. Once the credentials are confirmed, the API token is generated and saved into a cookie. Client apps use this cookie to authenticate with Brainloop Secure Dataroom.

We recommend that you register with Brainloop Secure Dataroom and log in the first time using SAML in your web browser (see “Unregistered users: Register and log in via SAML authentication” and “Registered users: Log in via SAML authentication”.

To add a server in the Brainloop Secure Client for iOS app:

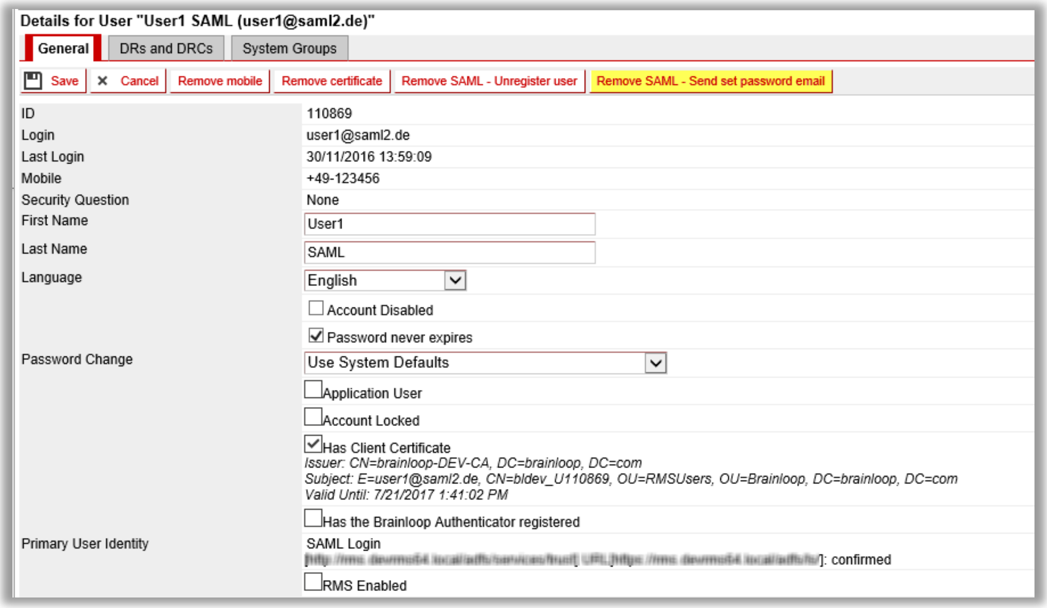
1. Log in to your app.
2. Select **Settings** > **Servers and Datarooms** > **Add Dataroom Server**.
3. Enter the name of your server (e.g. https://my.brainloop.net).
4. Enter your username (e-mail address).
5. Click **Login**.
6. If required, enter your credentials (username and password) for the configured SAML server and confirm them.

6 Reset the SAML login for a user

6.1 Remove a user’s authentication via SAML by resetting the password

The **Remove SAML – Send set password e-mail** option is helpful if you don’t want users to use SAML authentication, but want these users to stay registered with Brainloop Secure Dataroom. In this case, these users receive a reset password e-mail so that they have to specify a new password to be able to log in to their Datarooms or Dataroom Centers again.

1. Open **Application Administration**.
2. Select **User and Groups**.
3. Use the search field to find the user.
4. Click the user’s ID or Login to select the user.
5. The **General** tab is selected by default. Click **Edit** to display the following dialog:



Details for User "User1 SAML (user1@saml2.de)"

ID	110869
Login	user1@saml2.de
Last Login	30/11/2016 13:59:09
Mobile	+49-123456
Security Question	None
First Name	User1
Last Name	SAML
Language	English
	☐ Account Disabled
	☑ Password never expires
Password Change	Use System Defaults
	☐ Application User
	☐ Account Locked
	☑ Has Client Certificate *Issuer: CN=brainloop-DEV-CA, DC=brainloop, DC=com* *Subject: E=user1@saml2.de, CN=bldev_U110869, OU=RMSUsers, OU=Brainloop, DC=brainloop, DC=com* *Valid Until: 7/21/2017 1:41:02 PM*
	☐ Has the Brainloop Authenticator registered
Primary User Identity	SAML Login [redacted]: confirmed
	☐ RMS Enabled

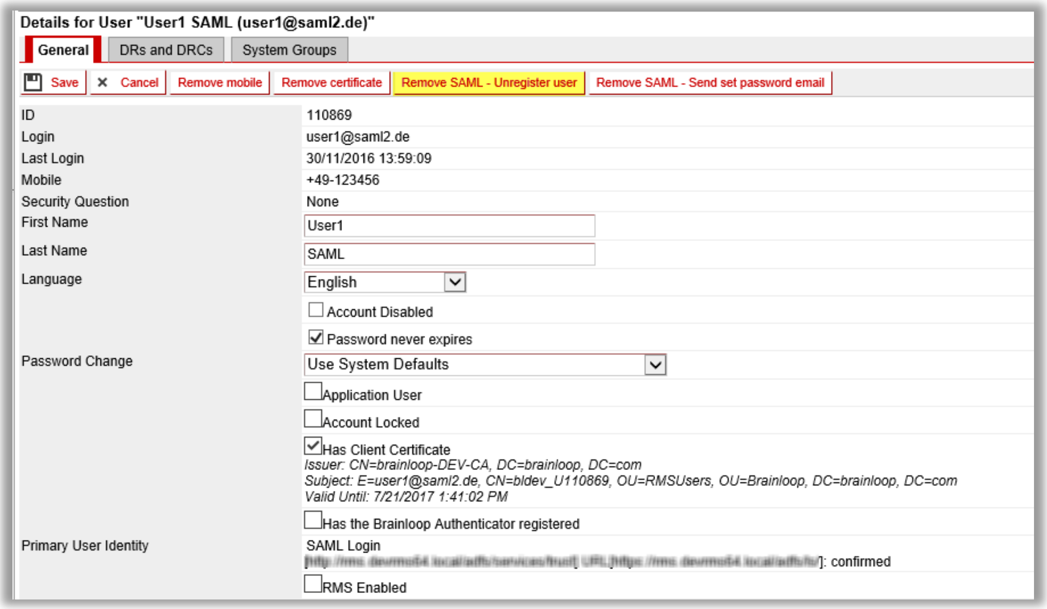
6. Click **Remove SAML – Send set password e-mail**.

   The user receives an e-mail containing a link to reset the password.

6.2 Remove a user’s authentication via SAML by unregistering the user

Use the **Remove SAML – Unregister user** option if you don’t want users to use the SAML authentication, and you want to require them to re-register before being able to log in to their Datarooms or Dataroom Centers again. These users must then be re-invited to be able to register and set a new password again.
Note: The users’ Datarooms, Dataroom Centers, and data are not affected by this process.

1. Open the **Application Administration**.
2. Select **User and Groups**.
3. In the **Search Users** field, search for the user and select this user.
4. Click **Edit**:



Details for User "User1 SAML (user1@saml2.de)"

ID	110869
Login	user1@saml2.de
Last Login	30/11/2016 13:59:09
Mobile	+49-123456
Security Question	None
First Name	User1
Last Name	SAML
Language	English
	☐ Account Disabled
	☑ Password never expires
Password Change	Use System Defaults
	☐ Application User
	☐ Account Locked
	☑ Has Client Certificate *Issuer: CN=brainloop-DEV-CA, DC=brainloop, DC=com* *Subject: E=user1@saml2.de, CN=bldev_U110869, OU=RMSUsers, OU=Brainloop, DC=brainloop, DC=com* *Valid Until: 7/21/2017 1:41:02 PM*
	☐ Has the Brainloop Authenticator registered
Primary User Identity	SAML Login [redacted]: confirmed
	☐ RMS Enabled

5. Click **Remove SAML – Unregister user**.
   This user no longer has access to their Datarooms or Dataroom Centers.

7 Configuration on the Identity Provider’s side

The following links are required for the configuration on the Identity provider’s side:

- SAML Assertion Consumer URL: https://<bdrs_server>/newlogin/saml.aspx
- SAML Logout URL: https://<bdrs_server>/newlogin/SamlSingleSignOut.aspx
- Identifier: https://<bdrs_server>/

7.1 Configure the Active Directory Federation Services (AD FS)

The configuration of AD FS is described in a separate setup guide.

8 Known restrictions

SAML login is currently not supported for **Brainloop Mobile** and for the **Accessibility** version of Brainloop Secure Dataroom.

9 Additional information

Please note that LDAP users can now also authenticate via SAML.

10 Appendix: Document revision history

Version	Date of change	Revision
1.0	17 August 2015	First release of the document
1.1	16 November 2015	Complete revision of the setup guide to match the changed setup and flow as of Brainloop Secure Dataroom version 8.30.800. Updated the following chapters, including subchapters: • “Configure the SAML settings in the Dataroom Center Administration”, pages 5ff • “Log in using SAML authentication”, pages 18ff • “Reset the SAML login for a user”, pages 24ff • “Login via Brainloop Secure Client apps”, page 23 Added the following chapter: • “Known restrictions”, page 26
1.2	August 2016	Added description of new functionalities released in Brainloop Secure Dataroom version 8.40.100. Added content and updated the following chapters, including subchapters: • “Configure SAML authentication in Brainloop Secure Dataroom”
1.3	December 2016	Added description of new functionalities released in Brainloop Secure Dataroom version 8.40.200. Updated screenshots throughout the document.