

Getting Started: Configuring Your BrainStorm Platform

Welcome to the BrainStorm platform! Before diving in, follow this guide to setting up the platform to maximize your success with the BrainStorm platform.

When on your set-up call with your BrainStorm representative(s), you will need the following people from your organization on the call:

- Project team members.
- System administrator(s) with ability to:
 - Add Whitelisting
 - Add Trusted Sites
 - Authorize Microsoft Global Admin or Google Super Admin permissions
 - Configure SSO

Checklist

1. [Add Trusted Sites and Whitelist Required IP Addresses and URLs](#)
2. [Add and Authenticate Users in the BrainStorm Platform](#)
3. [Assign Administrator Roles](#)
4. [Create Groups](#)
5. [Give Content to Users](#)

System Requirements

Supported OS: Windows OS and Mac OS

Supported Browsers: Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari

Note: For security reasons and optimal operation of the BrainStorm platform, ensure browsers are up-to-date with the latest version and are at least within two of the most recent versions.

Add Trusted Sites and Whitelisting

IT Admins: Update the following settings in your environment to ensure users receive required communications and access to the platform.

Trusted Sites

Add the following as trusted sites:

- *.brainstorminc.com
- bsiprodamsmedincus-usno1.streaming.media.azure.net
- bsiprodmedigeneralincus.blob.core.windows.net

Whitelisting

To ensure users receive automated BrainStorm emails, whitelist the following:

IP Addresses

- 159.183.129.244
- 158.247.19.189

URL

- brainstorminc.com

Add and Authenticate Users in the BrainStorm Platform

As a best practice, BrainStorm recommends you [set up SSO](#) and use the [Google or Microsoft Graph integration](#) for adding users. This allows users to log in automatically with no passwords stored and allows access to be controlled by your users' corporate account status. See the [Setting Up SSO](#) article.

Users may be added to the BrainStorm platform via an integration, CSV, or manually. See the [Adding Users](#) article for full instructions.

[Assign Administrator Roles](#)

With users added onto the platform, give selected users access to manage different areas of the platform. See the [Managing Roles](#) article.

[Create Groups](#)

Organizing your users into groups allows you manage adding relevant content for users easier. See the [Creating Groups](#) article.

Give Content to Users

[Purchase Packs in the Marketplace](#) or if you have your own content you can begin [uploading or creating assets](#) and adding them to [Flows](#).

Setting Up Single Sign-On (SSO)

Single Sign-On (SSO) authentication allows for secure authentication against your current identity database, reducing the administrative overhead and the risks associated with maintaining an additional external database of users and passwords.

BrainStorm is compatible with most SSO platforms that support WS-Federation or SAML 2.0 standards. Download the appropriate metadata file from below:

[SAML Metadata](#)

[WS-Federation Metadata](#)

After configuring, you may use either an XML file or a URL to share metadata with the BrainStorm platform.

Checklist

1. [Configure SSO in your Identity Provider](#)
2. [Configure SSO in BrainStorm](#)

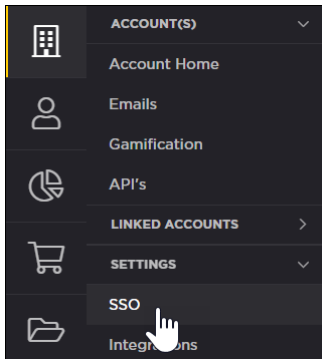
Identity Provider Configuration

WARNING: You will first need to configure your Identity Provider before completing configuration in the BrainStorm platform.

See the [SSO IdP Configuration Guide](#) **first** for complete instructions for configuring your Identity Provider.

Configure SSO in BrainStorm

1. From the left sidebar select **Accounts > Settings > SSO**.



2. Click the **Add ID Provider** button in the right corner.
3. **Name your SSO provider.** This name will appear in your SSO settings.
4. Select from the dropdown your SSO type, SAML or WS-Federation .

Note: For Azure AD select WS-Federation.

5. **Add SSO metadata.** You may add your SSO metadata one of two ways:
 - a. Attaching the XML file from your provider by clicking **Browse** in the **File** field.
 - b. Or, enter the metadata URL in the **URL** field. If you use a URL you have the option to automatically update your metadata. If selected, BrainStorm will check your SSO certificate nightly for changes. If an update or change is found it will be automatically imported into the BrainStorm platform. Click, next.
6. **Map SSO attributes to fields available in the BrainStorm platform.** First name, last name, and email address are required, but it is recommended to include job title and department.

Add ID Provider ✕

1 Configuration
Required
2 **Attribute Mapping**
Required

SSO Information	System Field Name
<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"/>	→ Email <small>* Required</small>
<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"/>	→ First Name <small>* Required</small>
<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"/>	→ Last Name <small>* Required</small>
<input type="text" value="JobTitle"/>	→ Title ✕
<input type="text" value="Department"/>	→ Department ✕
<input type="text" value="Value"/>	→ Value ▼
<input type="text" value="Value"/>	→ Value ▼

+ Add row

Update user info based on mapping ⓘ

Note: For Azure AD, use the following schemas:
 First Name: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname>
 Last Name: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname>

For Email, the schema may be:
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>
 OR
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

If you selected WSFederation as your SSO type in step 2, you'll click **Finish**.

If you selected SAML, you will have an additional step of configuration, click **Next** to proceed to step six.

7. **Additional Configuration (For SAML IdPs only)** Verify the following SAML settings, and click **Finish**.

Omit Asser-	If turned on, BrainStorm will not verify the signature in your SAML
-------------	---

tion Sig- nature Check	response.
Use SiteMinder	If you are using SiteMinder as the IdP, turn this option on.
Sign Request	If turned on, BrainStorm will sign the request.
Signing Cer- tificate	BrainStorm's current certificate.
Signature Algorithm	Select the correct signature for your IdP between SHA1 or SHA256.
Force Auth	If turned on, BrainStorm will add a ForceAuthn attribute in the request from BrainStorm. However, whether this is used or not depends on your IdP. ForceAuthn is a standard SAML attribute.
Is Passive	If turned on, BrainStorm will add an <i>isPassive</i> attribute in the request from BrainStorm. As with Force Auth, whether this is used or not depends on your IdP. <i>isPassive</i> is a standard SAML attribute.
Response Encoding	Defaults to UTF-8 but may be changed as needed.
Certificate Validation	Defaults to <i>Selfsigned</i> certificate, but may be changed as needed.

Add ID Provider

- 1 Configuration Required 2 Attribute Mapping Required 3 **Miscellaneous**

Omit Assertion Signature Check

Use SiteMinder

Sign Request

Signing Certificate

auth.brainstorminc.com 2022

Signature Algorithm

SHA256

Force Auth

Is Passive

Response Encoding

UTF-8

Certificate Validation

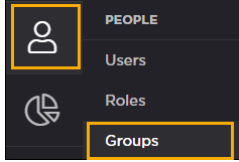
Selfsigned Certificate

Previous

Finish

Creating Groups

1. From the sidebar select the People icon > **Groups**. Click the **Create Group** button in the right corner.



2. Name your group and enter a description. You may also upload a thumbnail for your group that will be visible in the Groups page as well as the End User Portal (if group is visible to users, see step 2b).

Adjust your settings for your group and then click **Save and Continue**:

WARNING: Click **Save and Continue** once you have all of your settings on this page established. Clicking **Save and Continue** will progress you to the next step and **you will not be able** to return to this page to change settings.

- a. **Enrollment:** Enabling this setting allows you to set rules to automatically add users into your group. (See step 3.) If disabled, you will add users manually on the next step.
- b. **Aware:** Enabling this setting allows users to see they are a member of this group, receive group notifications, and interact with the group. Disabling this setting allows admins to manage the group without group member knowledge. If enabled, you will have the following setting options:
 - a. **Visibility:** Enabling this option makes the group visible to all users in the End User Portal and users may request to join this group. If disabled, only group members will see the group.

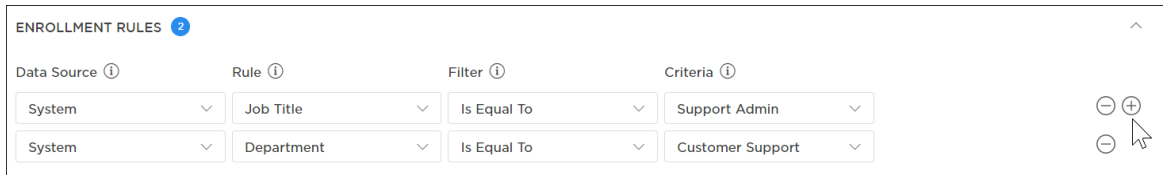
- b. **Access:** Enabling this option will require admin approval for users to join. Disabling this option allows anyone to join the group automatically if requested.
3. Next, you'll add users to groups. This step is dependent on if you enabled or disabled enrollment rules in step 2a.

Enabled Enrollment Rules

Set enrollment rules for your group in the following columns:

- a. **Source:** Select where you are pulling user data from for this group enrollment.
- b. **Rule:** From the rule dropdown, you can select.
- c. **Filter:** The filter dropdown will allow you to select relational operators to filter data by.
- d. **Criteria:** Enter criteria to filter by.

Use the plus or minus buttons to the right of each row to add or remove group enrollment rules.



The screenshot shows a table titled "ENROLLMENT RULES" with a blue notification bubble containing the number "2". The table has four columns: "Data Source", "Rule", "Filter", and "Criteria". There are two rows of rules. The first row has "System" for Data Source, "Job Title" for Rule, "Is Equal To" for Filter, and "Support Admin" for Criteria. The second row has "System" for Data Source, "Department" for Rule, "Is Equal To" for Filter, and "Customer Support" for Criteria. To the right of each row are minus and plus buttons. A mouse cursor is pointing at the plus button of the second row. There is also a plus button at the top right of the table area.

Data Source ⓘ	Rule ⓘ	Filter ⓘ	Criteria ⓘ	
System	Job Title	Is Equal To	Support Admin	⊖ ⊕
System	Department	Is Equal To	Customer Support	⊖ ⊕

Disabled Enrollment Rules

Click the box next to user names to select them to add to the group. You may also use the search bar and filters to narrow your results to find specific users. Click **Continue** once you have selected all users you would like to add to this group.

- Select group owners who will have the ability to add or remove users from this group. Click **Continue**.

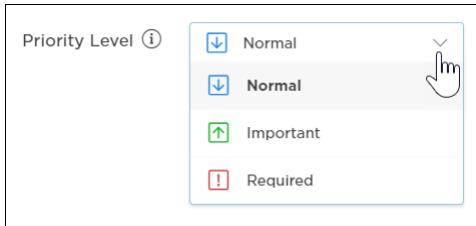
The screenshot shows the 'Customer Support' group configuration page. At the top, there are tabs for 'Configure', 'Members', 'Owners', and 'Content'. The 'Owners' tab is active. A search bar and a 'Filters' button are visible. The main area displays a table of group owners with columns for 'NAME', 'DEPARTMENT', 'JOB TITLE', and 'ADDED'. There are four rows, each with a checkbox in the left corner and a green 'OWNER' tag. The first and third rows have their checkboxes checked.

<input type="checkbox"/>	NAME	DEPARTMENT	JOB TITLE	ADDED
<input checked="" type="checkbox"/>	[Name]			05/31/2021
<input type="checkbox"/>	[Name]	QA Dept	QA Manager	07/27/2021
<input checked="" type="checkbox"/>	[Name]	QA Dept	QA Manager	07/28/2021
<input type="checkbox"/>	[Name]	QA Manager	Developer	08/10/2021

- Select content by checking the box in the left corner. You can filter your available content by type (Flows, assets, events) by using the drop down in the left corner. You may also filter using the **Filters** section. After selecting content, click the **Add** button in the right corner.

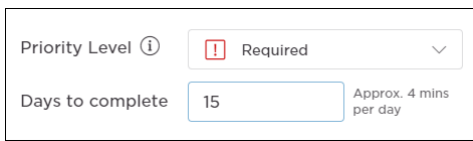
The screenshot shows the 'Add Content' dialog box. At the top, there is a search bar and a 'Sort by' dropdown set to 'Most Recent'. The main area displays a grid of content items, each with a checkbox in the top-left corner and a 'PUBLISHED' status. The third item in the first row has its checkbox checked. A 'Filters' sidebar is visible on the right, with sections for 'Date Added', 'Last Modified', 'Publisher', 'Packs', and 'Software Applications'. At the bottom, there are 'Cancel' and 'Add' buttons.

Click **Next**. Before the selected content is given to the group, you will need to assign a priority level to each content given.



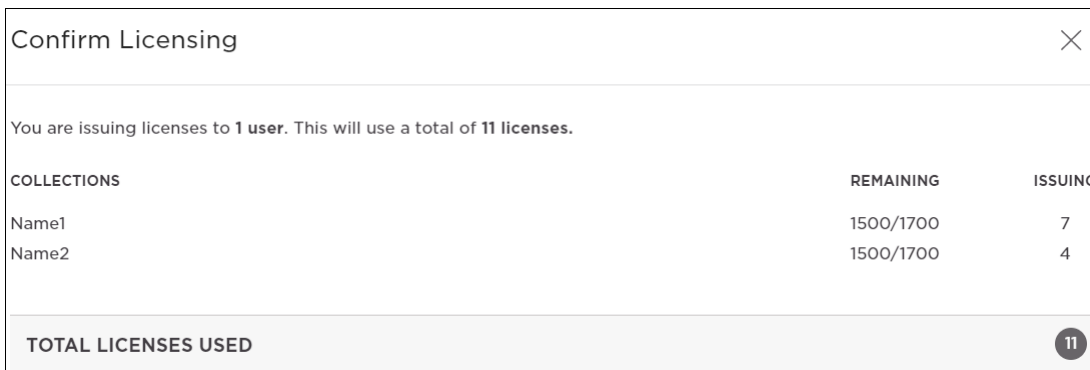
A screenshot of a 'Priority Level' dropdown menu. The menu is open, showing four options: 'Normal' (selected), 'Normal', 'Important', and 'Required'. A hand cursor is pointing at the second 'Normal' option.

If **Required** is selected, set the number of days the content must be viewed/completed within. Click next to confirm your selection and make the content visible to users.



A screenshot of the 'Priority Level' and 'Days to complete' fields. The 'Priority Level' dropdown is set to 'Required'. The 'Days to complete' field is set to '15', with a note that says 'Approx. 4 mins per day'.

If applicable, you will confirm the added licenses. Click **Confirm**.



A screenshot of the 'Confirm Licensing' dialog box. It shows a summary of license usage for two collections. The dialog includes a close button (X) in the top right corner.

COLLECTIONS	REMAINING	ISSUING
Name1	1500/1700	7
Name2	1500/1700	4
TOTAL LICENSES USED		11

6. *Optional*. You may select to notify group members of the group creation. A default email is available, but you may use the email editor to further customize your email. See the [Customizing Emails](#) article for details on email options and settings.