QuickHelp™ Single Sign-On

BrainStorm

Contents

QuickHelp™ Single Sign-On

Overview

Enabling Single-Sign On (SSO) authentication for your organization 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 recommends SSO for **all** organizations.

QuickHelp is compatible with potentially any SSO platform that supports WS-Federation or SAML 2.0 standards.

You will need to configure not only your Identity Provider, but your organization's QuickHelp portal, as well, to enable SSO authentication.

In your Identity Provider, you will configure which end-user attributes will be sent to QuickHelp each time a user logs in. The following attribute fields are available in QuickHelp:

Attribute Label	Description
Email*	Email – required; can be email or UPN, if the user can receive emails to the UPN
First Name	Given Name
Last Name	Surname
Company	Company/Organization
Title	User Title
Department	User Department
Location	User Location – could be City, Office, Country, State, etc.
Group	Any attribute in your IdP to use as a QuickHelp Group identifier/creator
UserID	Employee ID
Platform	Workstation information – Mac, Windows, OS, etc.
Custom 1	Custom
Custom 2	Custom
Custom 3	Custom

The Email field is required. Including First Name, Last Name, Title, and Department is BrainStorm's best practice. The other fields are optional and can be used to send any desired attribute to QuickHelp for user classification and reporting, not just what the Attribute Label indicates.

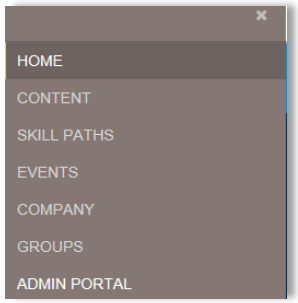
NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

Before You Begin

Before you begin SSO setup you should confirm:

- You have a login to your QuickHelp Web Portal (https://quickhelp.com/routeurl). You can create an account using your organizational e-mail address if you don't have an account.
- You (or another authorized user) have accepted the End-User License Agreement (EULA) on behalf of your organization. If this hasn't been accepted yet, you should be prompted after logging in.
- You have been granted "Administrator" privileges. To verify that you have this access, look for the "Admin Portal" option in the left-side menu.

Click Admin Portal.



Click Settings

Look for the Authentication Settings tab

AUTHENTICATION SETTINGS

Check with the your organizational QuickHelp Administrator or your BrainStorm Client Success Manager if any of these are not as described.

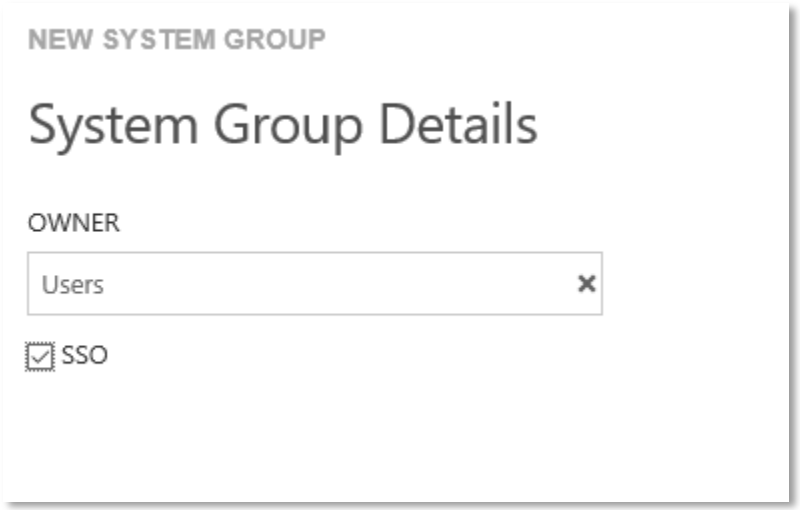
QuickHelp™ Single Sign-On

QuickHelp Groups

QuickHelp utilizes groups to organize users and assign relevant content, among other things. Single Sign-On can be used to automatically create and populate these groups. If there is a single- or multiple-value attribute in your IdP that can be used as a QuickHelp Group identifier, include it as the Group parameter.

The number of user-assigned values for the chosen attribute should be relatively small as a QuickHelp group will be created for each value. This group-creation process happens when users log in to QuickHelp.

However, before your users ever log in to QuickHelp, you can create System Groups in QuickHelp to match the values of the attribute you are sending. The names must match exactly. During the System Group Creation process, you will see an SSO checkbox:



Checking that box makes the manually created group behave as if it were created via SSO, meaning that users will be automatically added to and/or removed from the group based on their identity database profile. If the SSO checkbox is not checked, users will not be automatically added to the group based on their identity database profile.

QuickHelp™ Single Sign-On

BrainStorm

QuickHelp™ Single Sign-On

BrainStorm

ADFS

Compatibility

QuickHelp is compatible with ADFS 2.0, 3.0, or 4.0.
Please note that SSO will not be enabled until both the following ADFS server configuration and the QuickHelp Portal configuration have been completed.

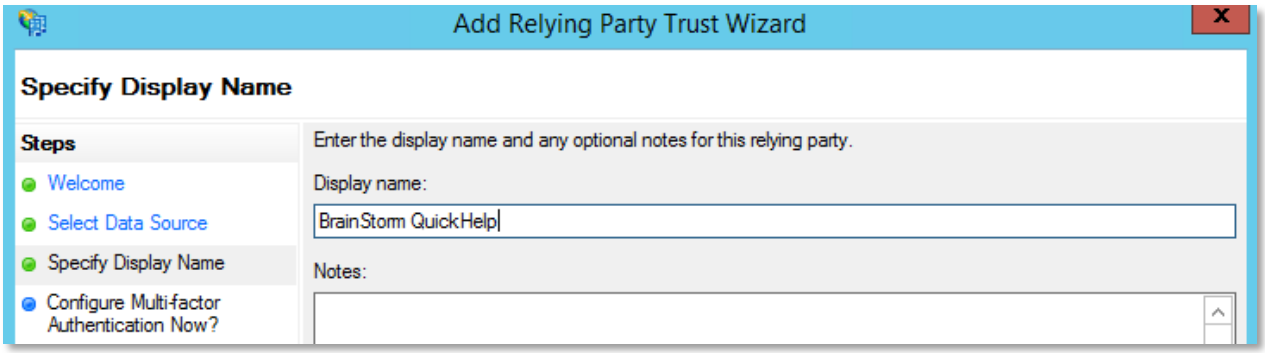
ADFS server configuration

While these instructions are written with ADFS 3.0 in mind, the steps should be nearly identical for ADFS 2.0 and 4.0. On your primary internal ADFS server you will need to **Add Relying Party Trust**.

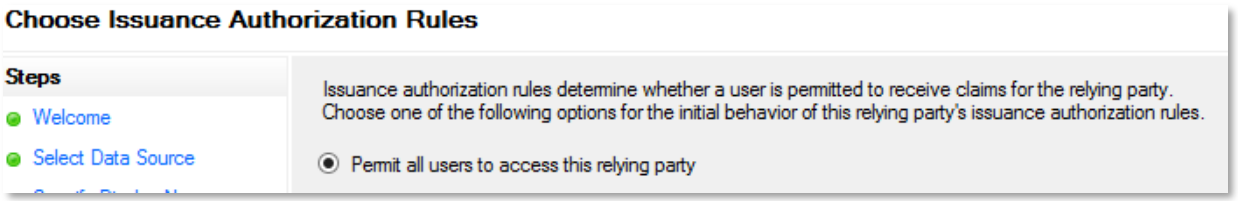
1. On the *Welcome to Add Relying Party Trust Wizard* screen click **Start**.
2. Paste the following into the URL field then click next.

https://quickhelp.blob.core.windows.net/metadata/QuickHelpWSFederationMetadata2024.xml

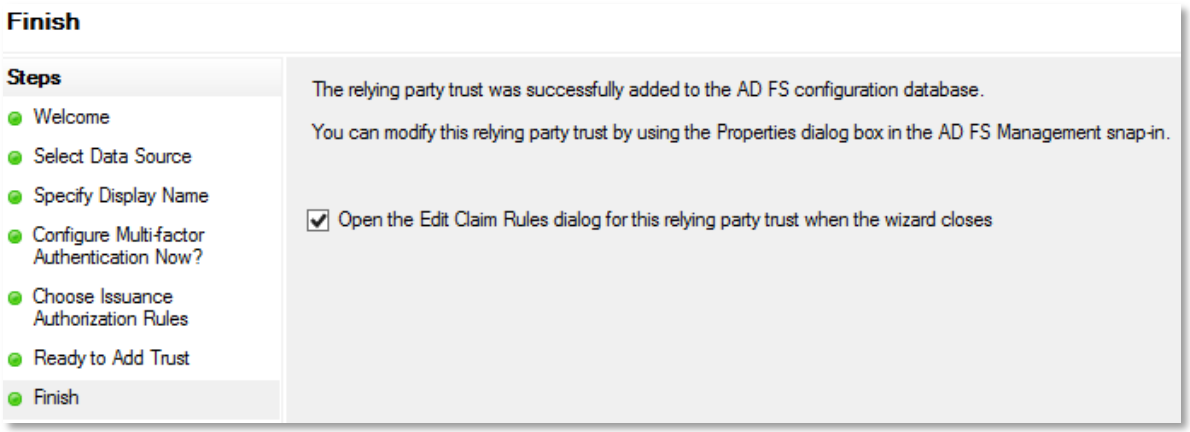
3. For the *Display name* you can accept the default or enter something more descriptive such as ***BrainStorm QuickHelp*** then click **Next**.



4. Accept the defaults on the *Multi-factor Authentication configuration* page and click **Next**.
5. For *Issuance Authorization Rules* select the default of permitting all users and click **Next**.

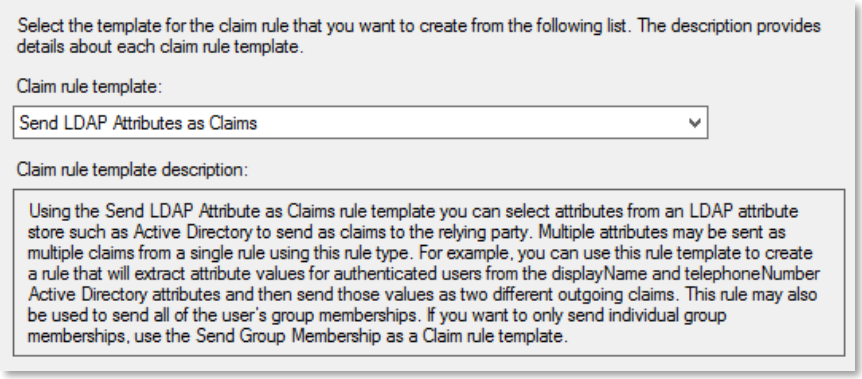


6. On the *Ready to Add Trust* page click **Next**.
7. On the *Finish* page leave the Open the Edit Claim Rules box checked and click **Close**.



8. Click **Add Rule**.

9. Select the default template of **Send LDAP Attributes as Claims** and click **Next**.

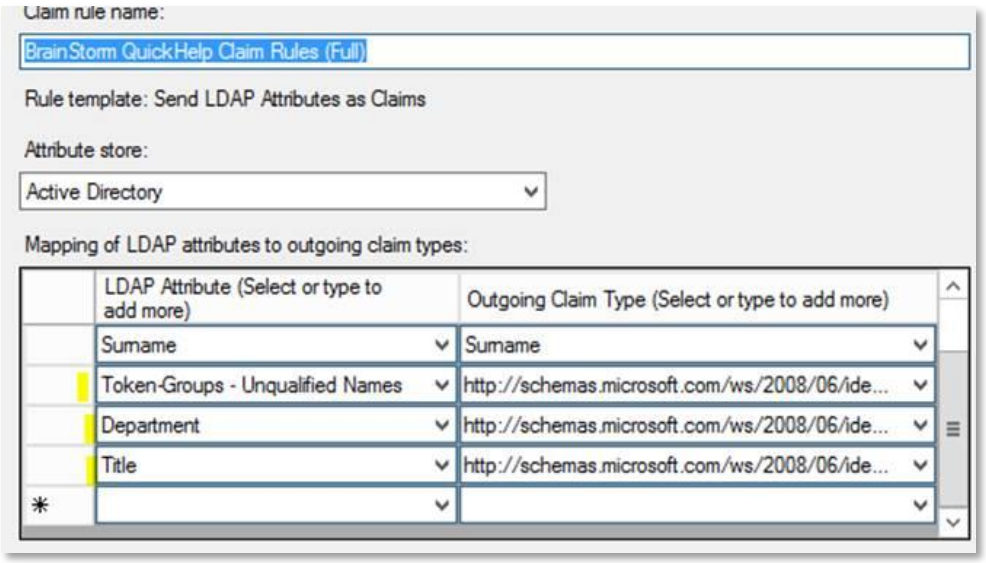


10. For the Claim Rules name, enter something descriptive such as ***BrainStorm QuickHelp Claim Rules***.
11. For the *Attribute store* select **Active Directory**.
12. For *Mapping of LDAP Attributes* the left column is the LDAP description of the field and the right side is the SAML type description. Use the table below as a guide.

	LDAP attribute	Outgoing Claim Type
1	E-Mail-Addresses	E-Mail Address
2	Given-Name	Given Name
3	Surname	Surname
4*	Token Groups - Unqualified Names	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
5	Department	http://schemas.microsoft.com/ws/2008/06/identity/claims/department
6	Title	http://schemas.microsoft.com/ws/2008/06/identity/claims/title

***If AD Token Groups are mapped to QuickHelp Groups, all AD groups to which each user belongs will automatically create corresponding groups in QuickHelp when the user logs in for the first time. Depending on the number of your AD groups, the number of QuickHelp groups has the potential of growing exponentially. If there is a different AD attribute that makes sense for QuickHelp groups (like Location), you won't need to create the Token Group attribute.**

Other attributes such as Company, Location, UserID, etc can be added, but will not yet be visible to end users and/or Admins.



13. Click **Finish**.
14. **To complete configuration, go to the Portal Configuration section of the document.**

Limiting access

Some organizations may choose to limit access to QuickHelp. To limit access to an ADFS relying party to only specific groups.

1. In the ADFS console, navigate to the relying party trusts. Select the trust for QuickHelp, click edit claim rules.
2. Navigate to Issuance Authorization Rules, select “Permit all Users” if it exists and click remove rule.
3. Click Add Rule. Select the “Permit or Deny Users Based on an Incoming Claim” template and click next.
4. Type a name for the rule such as “Allow QuickHelp Authorized”. Under Incoming Claim Type, select Group SID. Click Browse and select the security group you want to allow access, then select the “Permit” radio button and click finish.
5. Repeat for any additional groups you want to grant or deny access. There is an implicit deny all at the end of the list.

QuickHelp™ Single Sign-On

BrainStorm

QuickHelp™ Single Sign-On

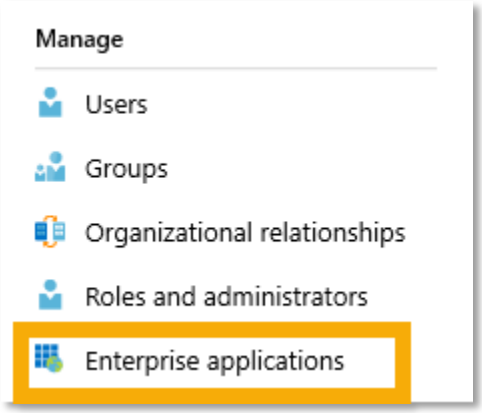
Azure Active Directory

Compatibility

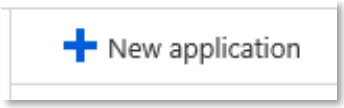
QuickHelp is compatible with Microsoft Azure Active Directory and requires O365 Administrator access.
Please note that SSO will not be enabled until both the following Azure Active Directory configuration and the QuickHelp Portal configuration have been completed.

Azure Active Directory configuration

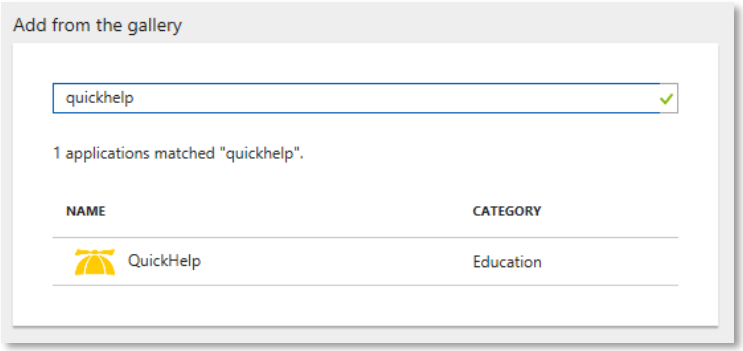
1. Log in to the Office 365 Admin center and select **Azure Active Directory** from the *Admin Centers*.
2. Choose to manage **Enterprise applications**.



3. From the top, click **New Application**.



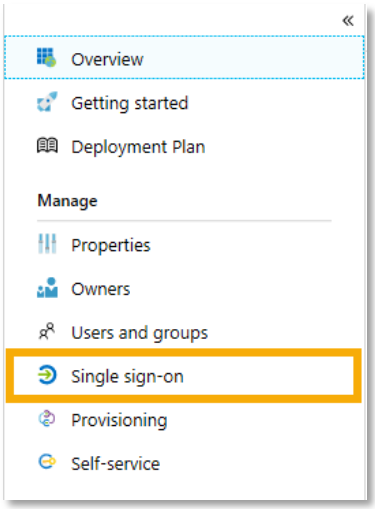
4. Type ***QuickHelp*** in the ***Add from gallery*** search field that appears.



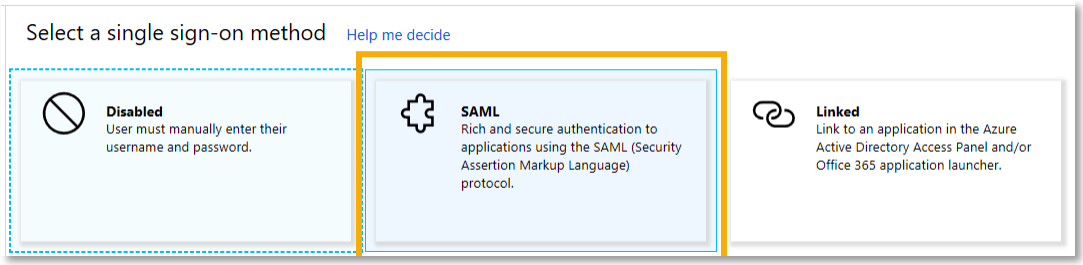
5. Select the **QuickHelp** app from the results.

Please ensure you are using the QuickHelp app and not the BrainStorm app.

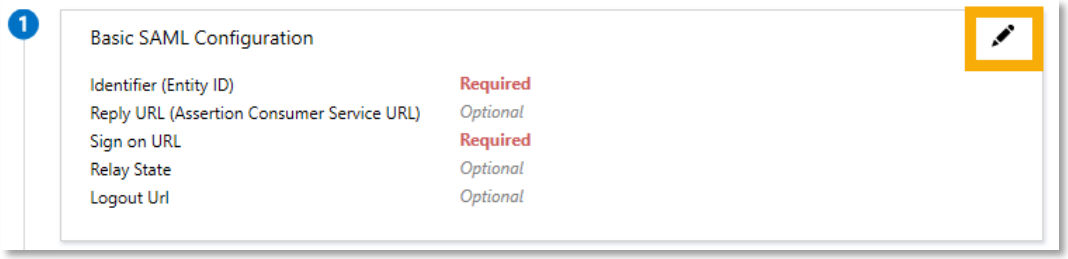
6. Click **Add** at the bottom of the window that pops up.
7. Once the app is added, a new *QuickHelp – Quick start* dialog appears. Click **Single sign-on** from the left.



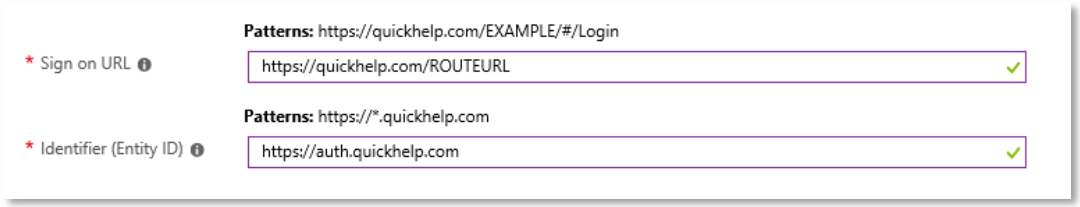
8. In the *Select a single sign-on method*, choose **SAML**.



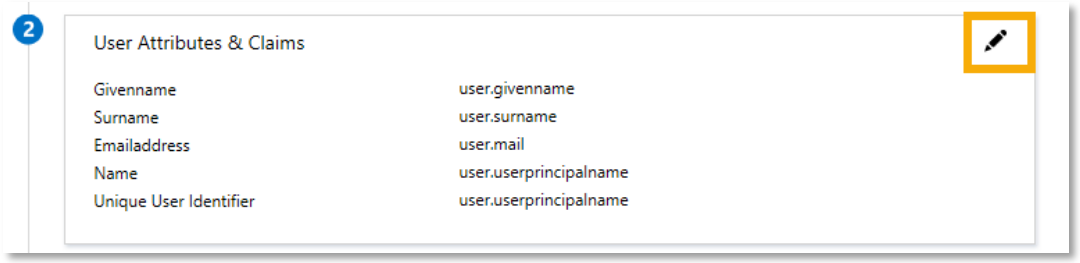
9. In **Basic SAML Configuration**, click Edit in the upper right-hand corner.



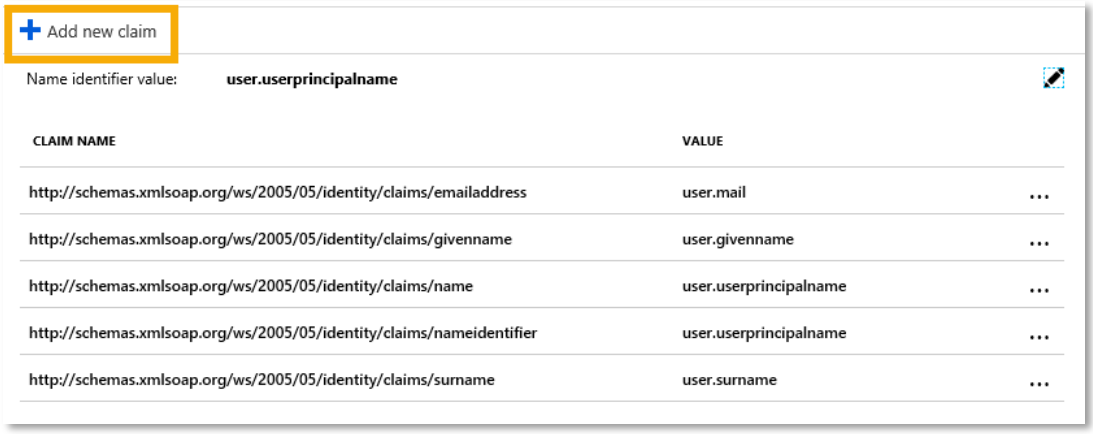
10. In the *Identifier (Entity ID)* field, enter https://auth.quickhelp.com.
11. In the *Reply URL* field, enter https://auth.quickhelp.com.
12. In the *Sign on URL* field, enter https://quickhelp.com/routeurl, where *routeurl* is the custom landing page designated for your organization. If you don't know your *routeurl*, please contact your organization's QuickHelp administrator or your BrainStorm Client Success Manager.



13. Click **Save**.
14. In **User Attributes and Claims**, click Edit in the upper right-hand corner.

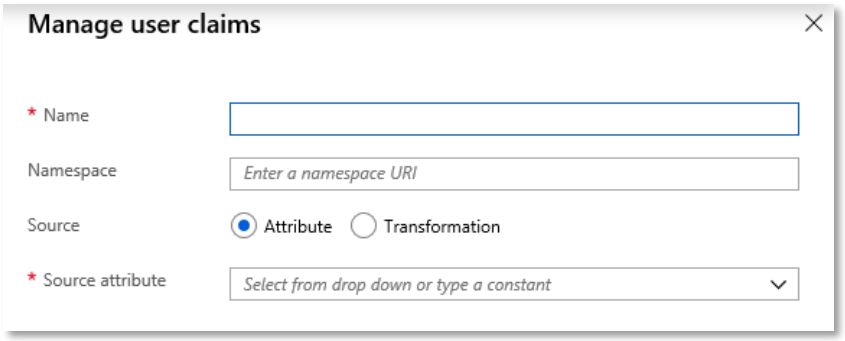


15. By default, you should see SAML Token Attributes for givenname, surname, emailaddress, and name (UPN). To add other attributes for Title, Department, UserID, Company, Platform, Location, or Custom Fields 1-3, click **Add new claim**.



NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

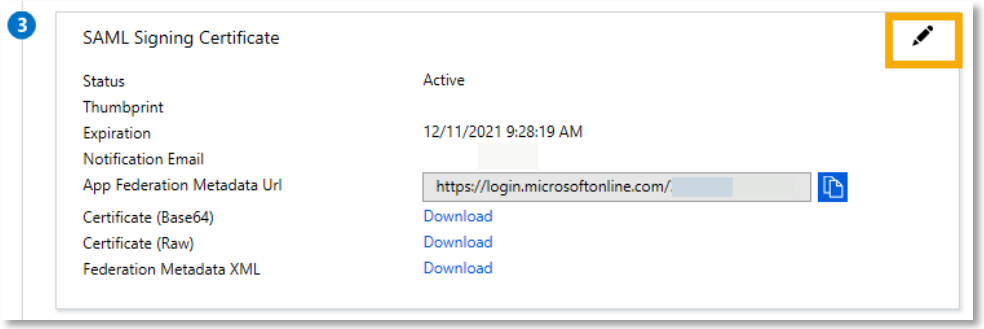
16. In the *Name* field, enter an appropriate name, e.g. Department. This is an open field but will be used in the Portal Configuration section of the document.
17. From the *Source Attribute* pulldown menu, select the corresponding AD attribute.



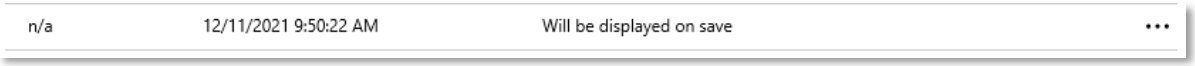
18. Click **Save** at the bottom of the *Manage user claims* dialog.
19. Repeat to add other attributes.

There is an additional QuickHelp attribute for Group. If there is a single- or multiple-value attribute in your IdP that can be used as a QuickHelp Group identifier, create it here. The number of user-assigned values for the chosen attribute should be relatively small as a QuickHelp group will be created for each value. This group-creation process happens as users log in to QuickHelp.

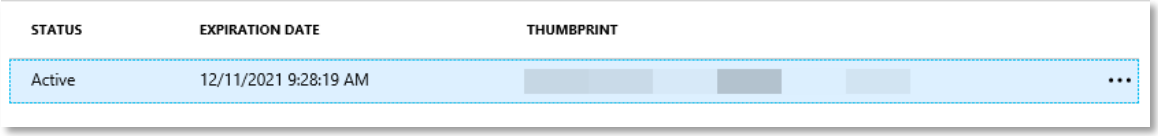
20. In **SAML Signing Certificate**, if there is not an active certificate, click Edit in the upper right-hand corner. **If an active certificate already exists, skip to step 26**.



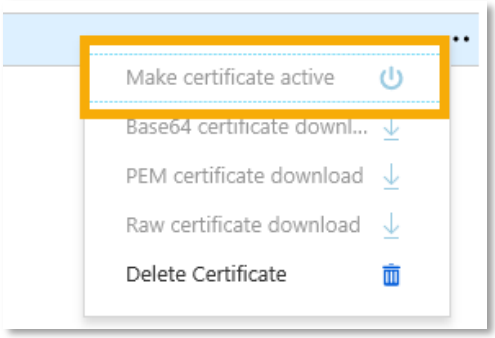
21. Click **New certificate**.
22. Choose an expiration date – you can select any date (up to three years from the current date).



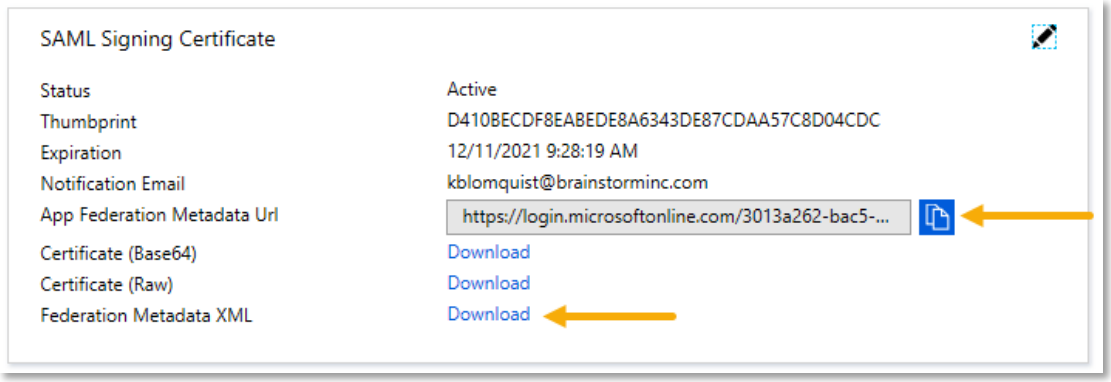
23. Click **Save**.
24. A row of information with an option to download Metadata XML is available.



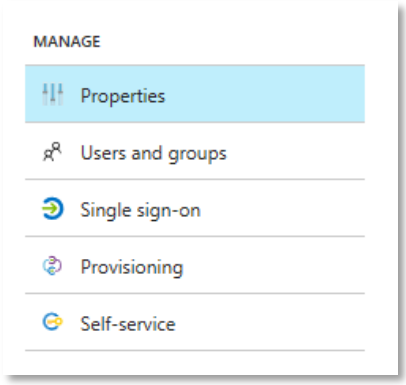
25. Verify that the **Status** of the certificate is *Active*. If not, click the three dots to the upper right of the certificate and select **Make certificate active**.



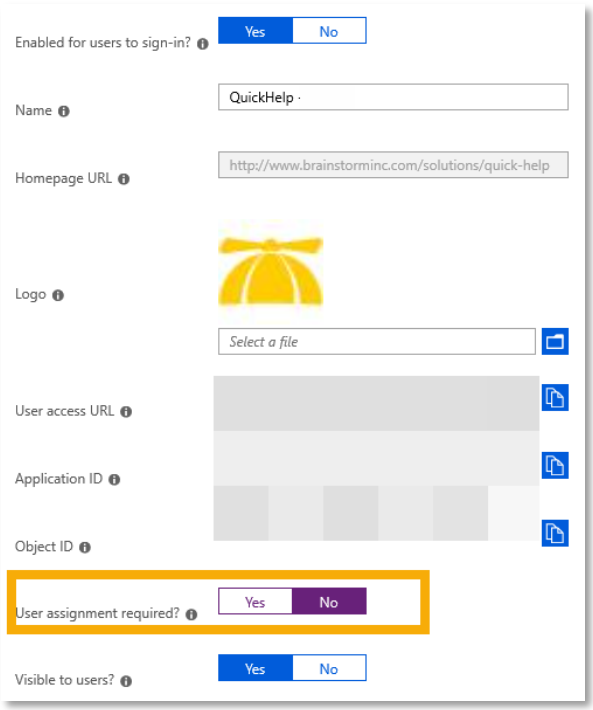
26. Click the Download link next to *Federation Metadata XML* and save the metadata file to a familiar location OR Copy the *App Federation Metadata Url*. This will be used later in the QuickHelp Portal Configuration.



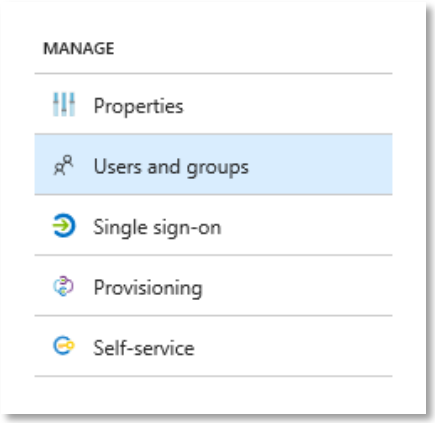
27. Save the Single Sign-On configuration.
28. Click **Properties** from the *Manage* list on the left.



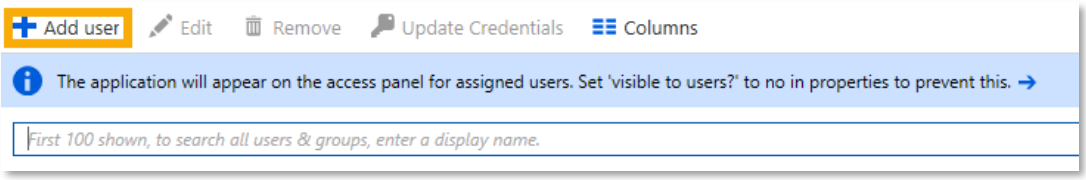
29. Set *User assignment required?* to either **Yes** or **No**.
    a. **Yes**: Users must be first assigned to the application before being able to access it for authentication.
    b. **No**: Any user in your Azure Active Directory can access it for authentication. If set to No, Save and skip to step 36.



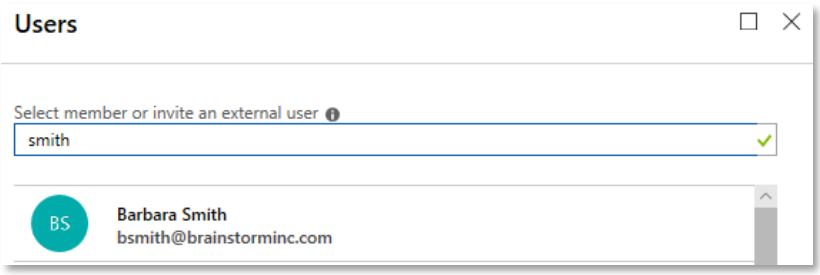
30. Click **Save**.
31. Click **Users and groups**.



32. Click **Add user** in the *User and groups* dialog that opens.



33. Click **Users** or **Groups** in the *Add Assignment* dialog. A dialog will open.
34. Within the respective dialog, search for the user/group to which QuickHelp should be assigned.



35. Select and Assign the user/group to be added. Repeat as needed.
36. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

BrainStorm

QuickHelp™ Single Sign-On

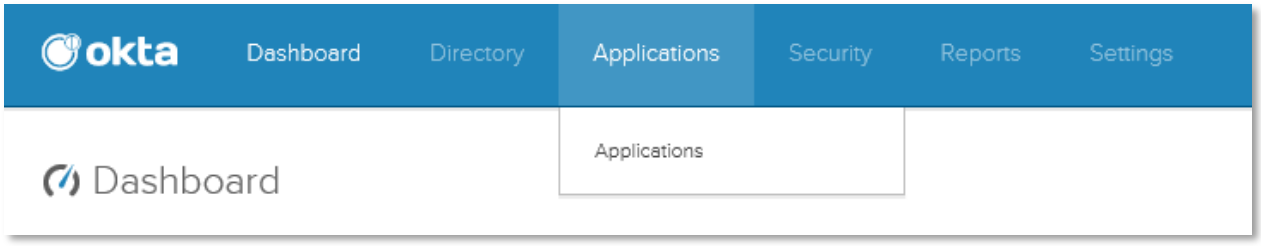
Okta

Compatibility

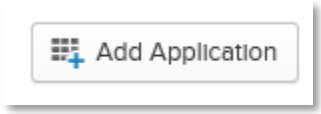
QuickHelp is part of the Okta Application Network (OAN), making it easy to enable Single Sign-On. Configuration requires an Okta administrator.
Please note that SSO will not be enabled until both the following Okta configuration and the QuickHelp Portal configuration has been completed.

Okta configuration

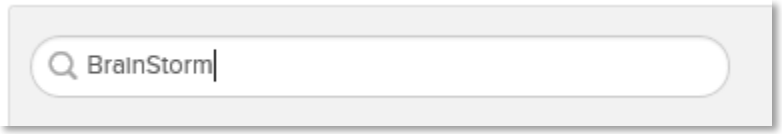
1. Log in to Okta as an administrator.
2. Navigate to the administration area.
3. From the options across the top, click on Applications > **Applications**.



4. Click **Add Application**.

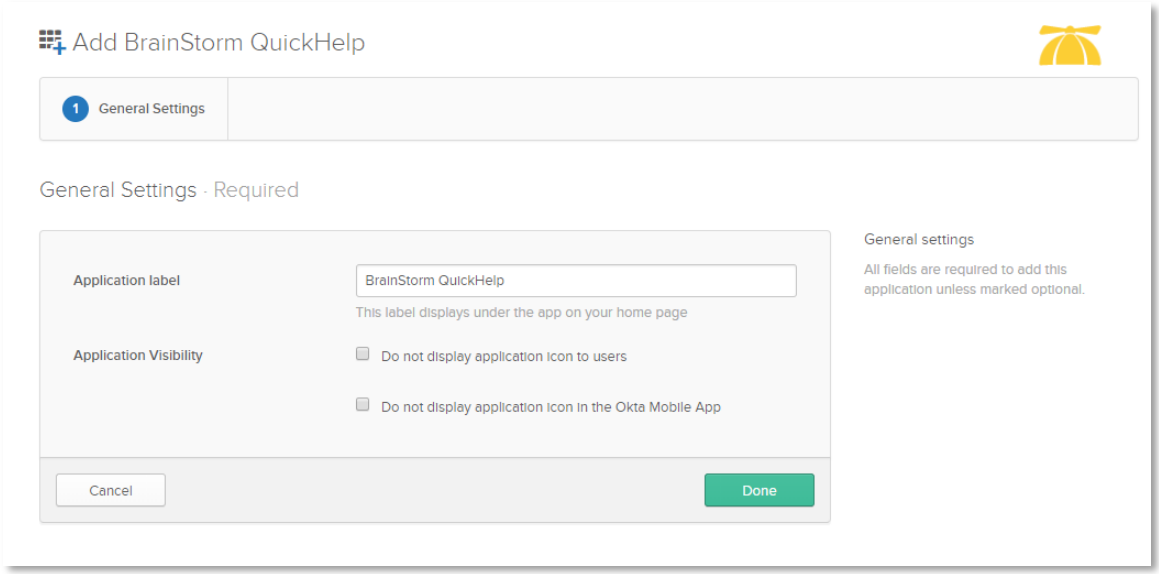


5. In the search field, search for *BrainStorm*.

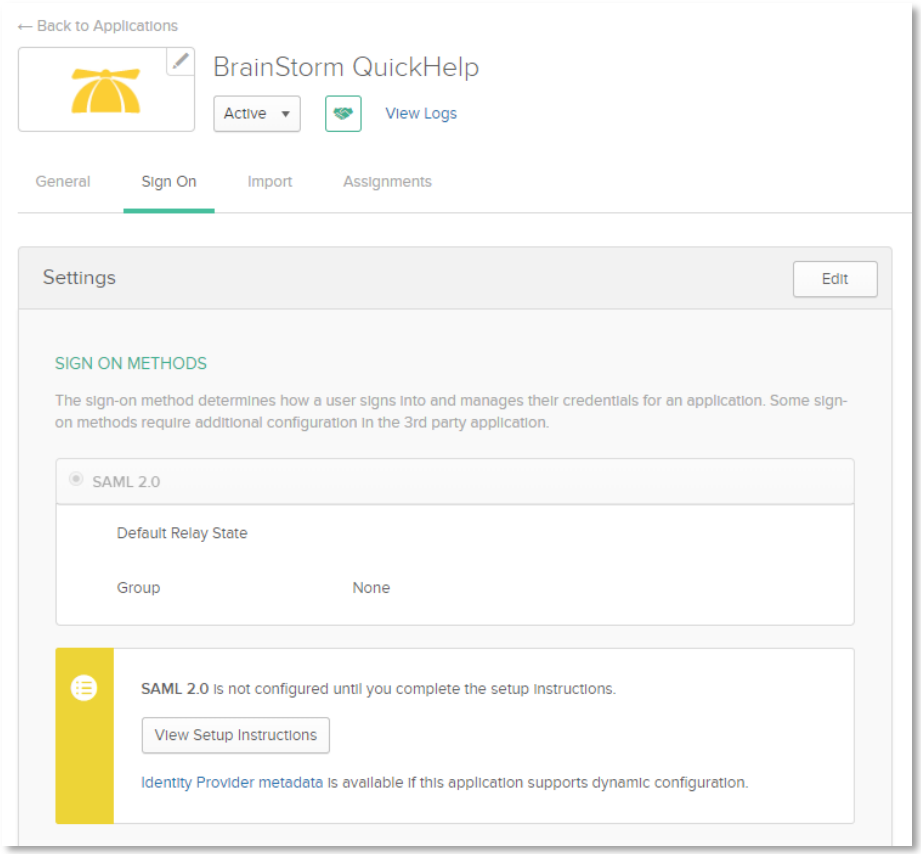


6. BrainStorm QuickHelp will pop up – click **Add**.

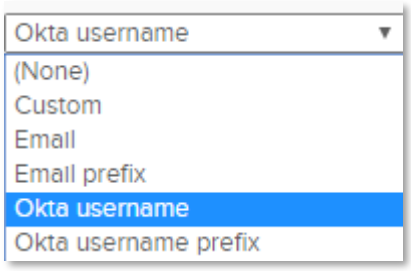
7. In the *General Settings* area, click **Done** (you can make changes if desired, but they are not needed).



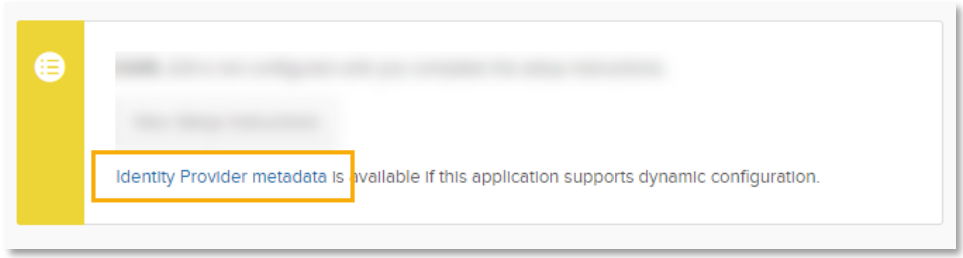
8. From the *Application attributes* area, click on **Sign On**.



9. If the **Application username format** value of *Okta username* is not the email you wish to send to QuickHelp, edit the *Settings* > *Credential Details* section and choose the desired value for the **Application username format**.



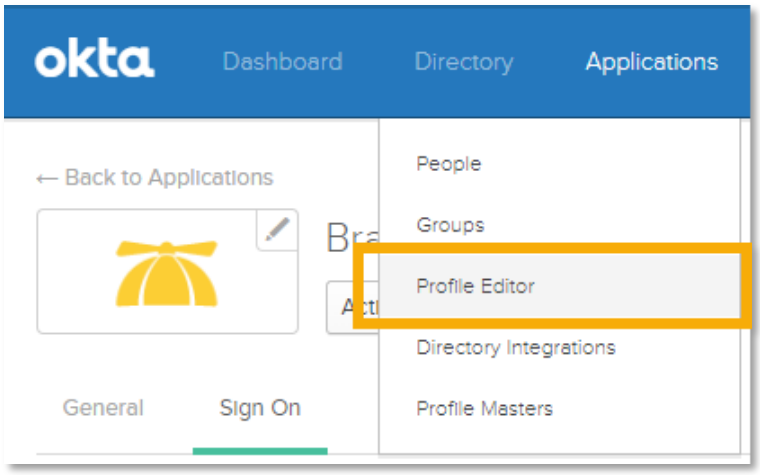
10. Click **Save**.
11. Click the **Identity Provider metadata** hyperlink.



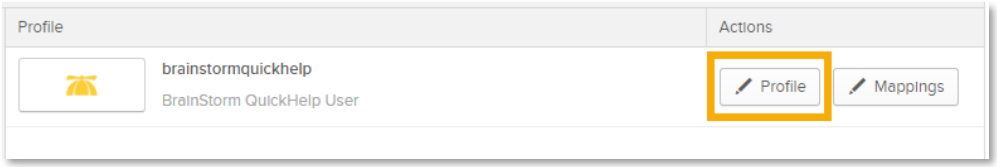
12. Save the metadata document to a familiar location.
13. By default, Okta sends email, First Name, Last Name, Title, and Department as attributes to QuickHelp. UserID, Company, Location, Platform, and three custom fields are optional fields, and must be configured to send the correct information. **If you are not configuring any other outgoing attributes, skip to step 15.**

NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

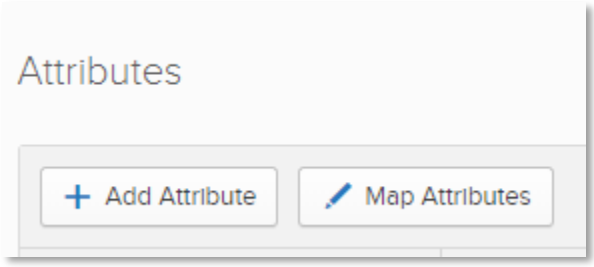
14. To configure all other optional attributes (UserID, Company, Location, Platform, Custom 1-3):
    a. From the options across the top, click on Directory > **Profile Editor**.



    b. In the search field, search for *BrainStorm*.
    c. To the right of the BrainStorm app, click **Profile**.

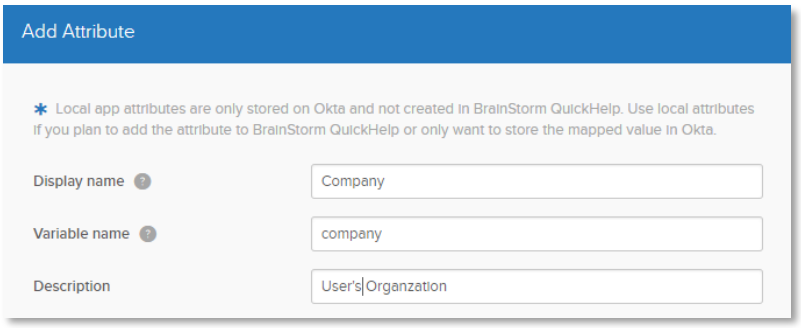


    d. In the *Attributes* area, click **Add Attribute**.



    e. Enter a *Display name* (determined by you).
    f. Enter the *Variable name* that relates to this attribute (please note, these are case sensitive): *userid, company, location, platform, custom1, custom2, custom3*.

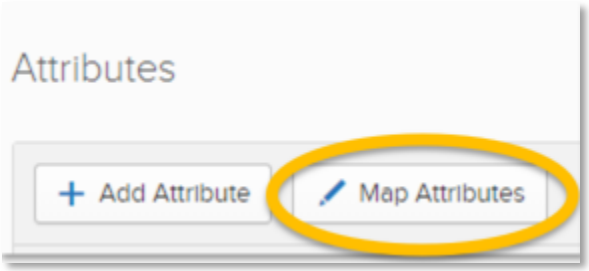
g. Enter a *Description*.



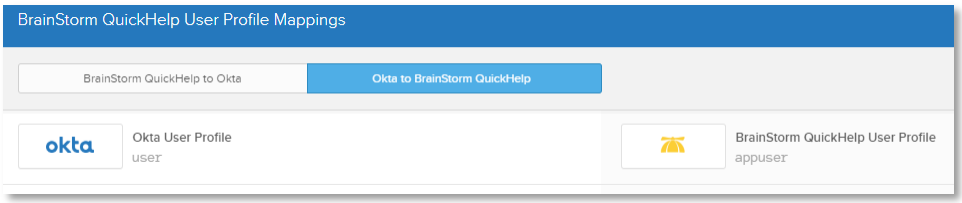
h. Click either **Save** or **Save and Add Another** (depending on whether or not you are adding more attributes).

i. Continue for all additional attributes.

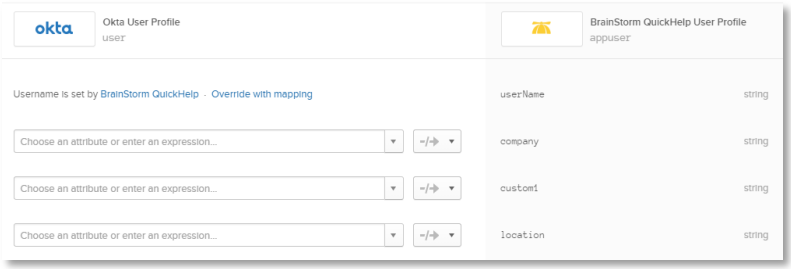
j. Once done adding the attributes, in the Attributes area, click Map Attributes.



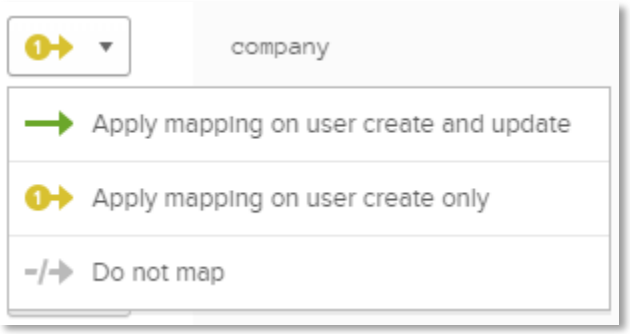
k. In the *BrainStorm QuickHelp User Profile Mappings* dialog, click **Okta to BrainStorm QuickHelp**.



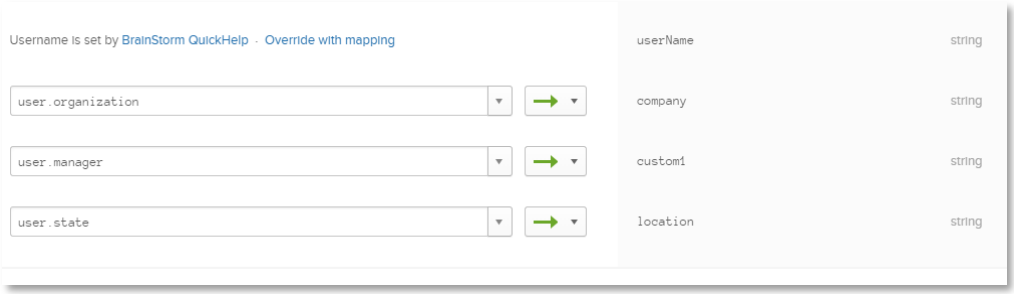
l. Below the Okta and BrainStorm logos, you will see a list of the attributes you added above. Since UserName is a preset attribute, it cannot be changed. To the left of the first added attribute, either click in the *Choose an attribute or enter an expression…* field or click the pulldown arrow to the right.



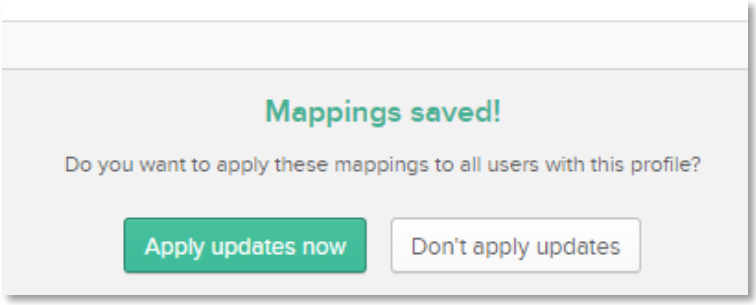
m. Choose the Okta attribute to map to the outgoing attribute. This can be any attribute that you want to use for user classification and reporting, not just what the Attribute Label indicates.
n. Click the pulldown menu to the right of the attribute field and choose *Apply mapping on user create and update*.



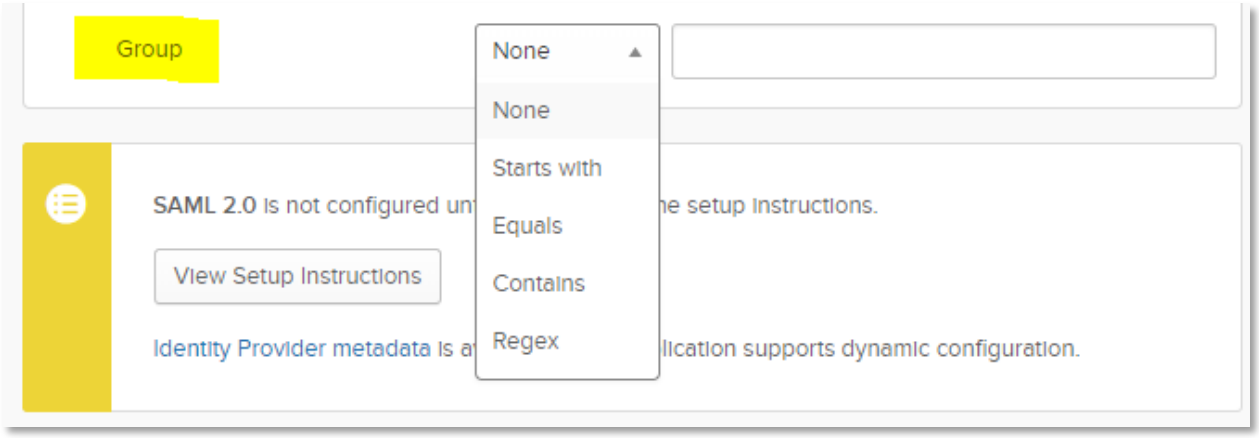
o. Repeat for all attributes.



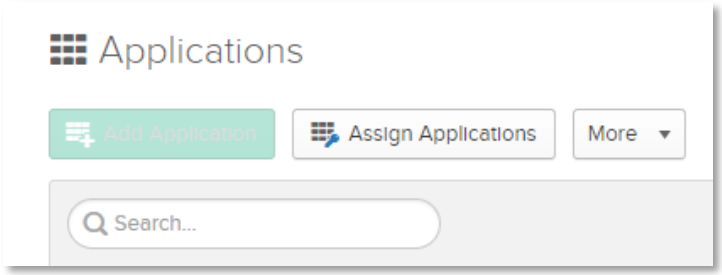
p. When done, click **Save Mappings**.
q. If QuickHelp has been assigned to users already, click Apply updates now in the Mappings Saved dialog at the bottom.



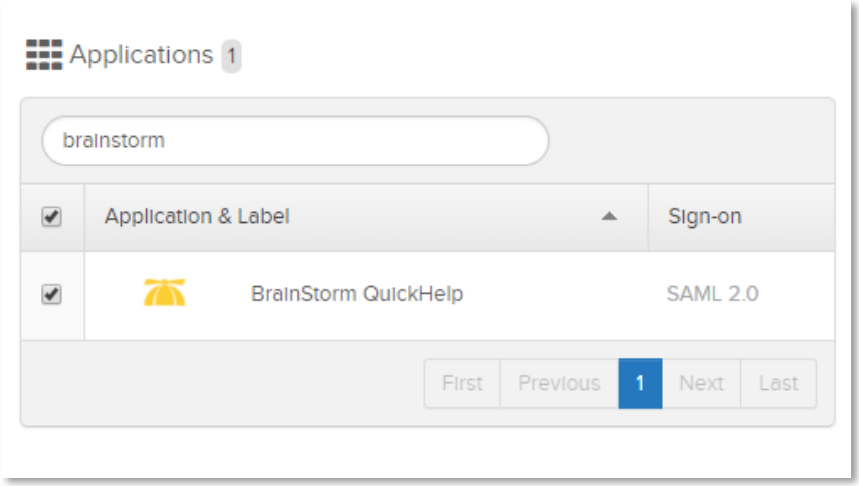
15. If you opt to send Groups as an attribute, edit the Sign-On section and click on the Filter pull-down menu by *Group*.



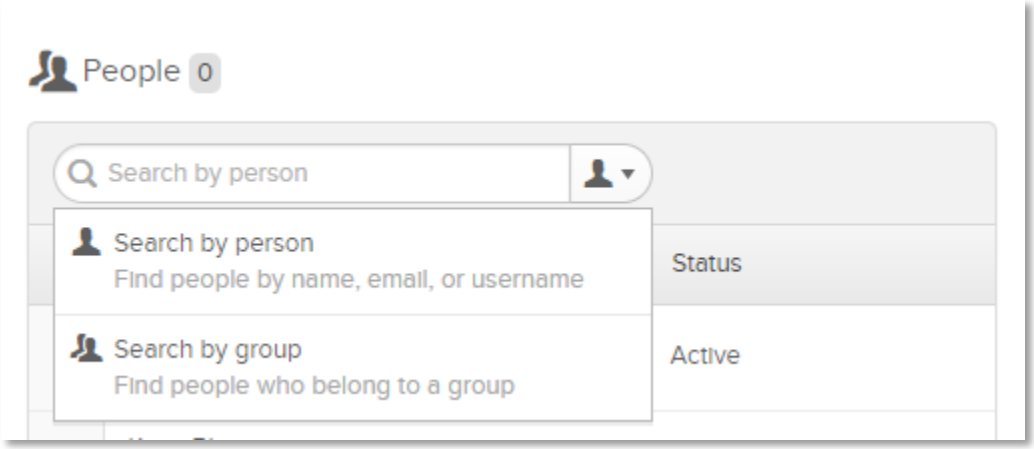
16. Use the filters to determine which Group names from within OKTA to send to QuickHelp.
    a. To not send any groups, leave as *None*.
    b. To send **all** groups, choose *Regex* as the filter type, and enter '**.***' as the value.
    c. To send specific groups only, use the filters as needed.
17. Click **Save**.
18. Return to Applications > **Applications**.
19. Click on **Assign Applications**.



20. From the *Applications* list on the left, find *BrainStorm QuickHelp* and check the box next to it.

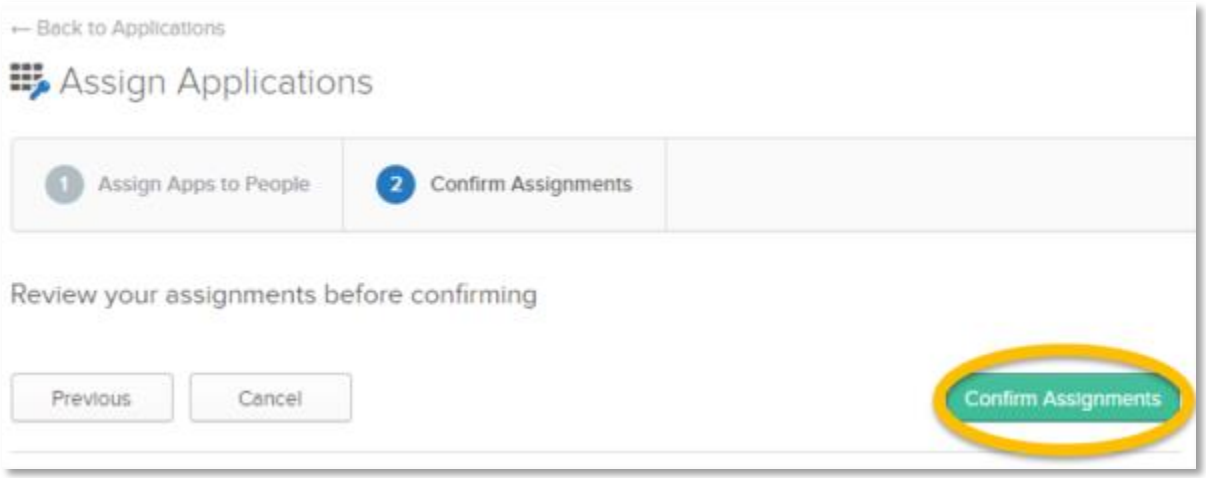


21. From the *People* list on the right, first click the person icon to the right of the search field and choose whether to search by person or group.



22. Check the box to the left of the people or groups to which QuickHelp should be assigned. Assign BrainStorm QuickHelp to enough people to perform adequate testing. After testing is complete, this app will need to be assigned to all necessary users.
23. Click **Next**.

24. Click **Confirm Assignments**.



25. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

BrainStorm

QuickHelp™ Single Sign-On

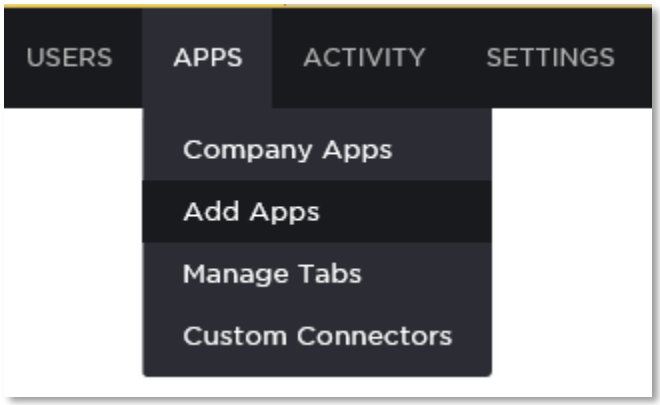
OneLogin

Compatibility

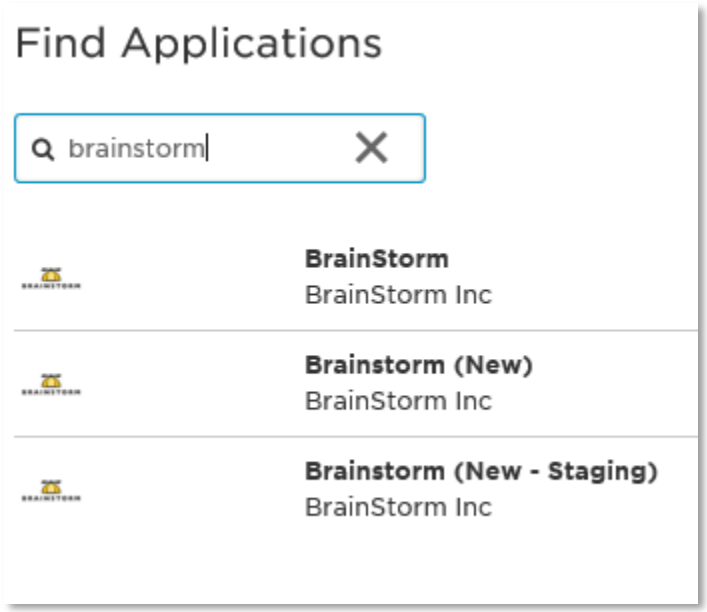
QuickHelp is part of OneLogin's catalog of pre-integrated applications, making it easy to enable single sign-on. Configuration requires a OneLogin administrator.
Please note that SSO will not be enabled until both the following OneLogin configuration and the QuickHelp Portal configuration have been completed.

OneLogin configuration

1. Log in to your OneLogin App Portal and select Apps > **Add Apps**.

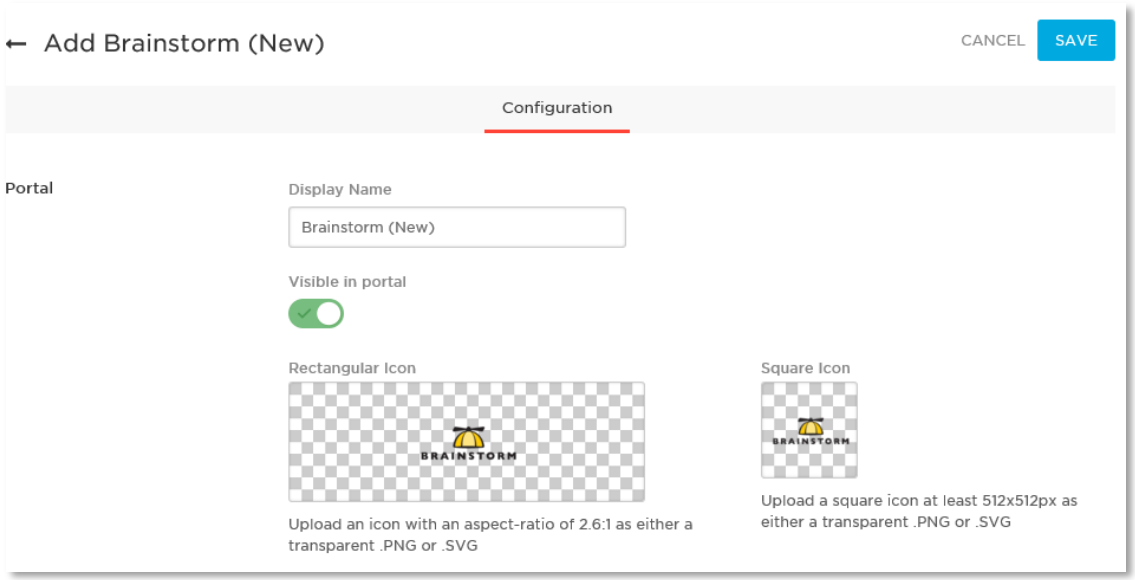


2. Search the catalog for ***BrainStorm***.

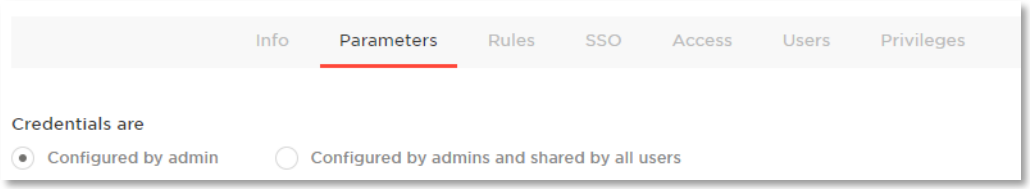


3. Click on **BrainStorm (New)**.
4. Change the Display Name as desired.

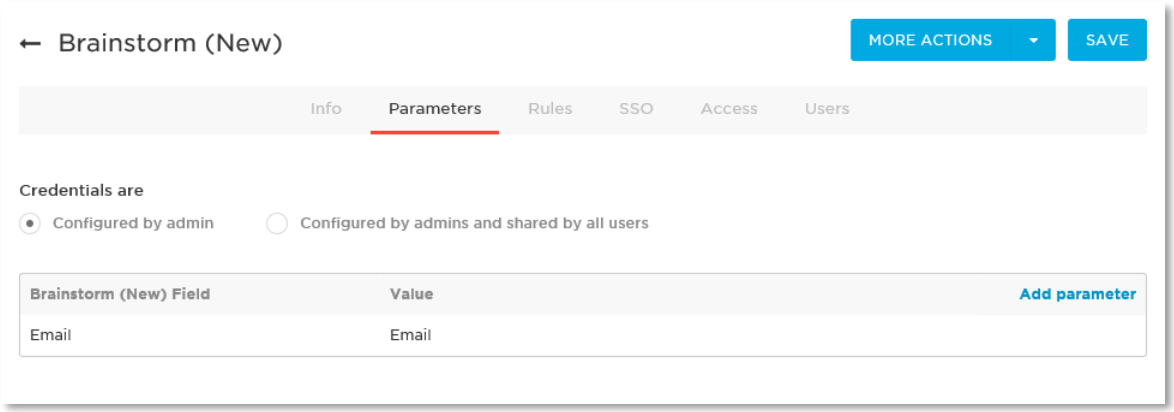
5. Click Save.



6. Once saved, click the **Parameters** tab.
7. Leave *Credentials are Configured by admin* selected.

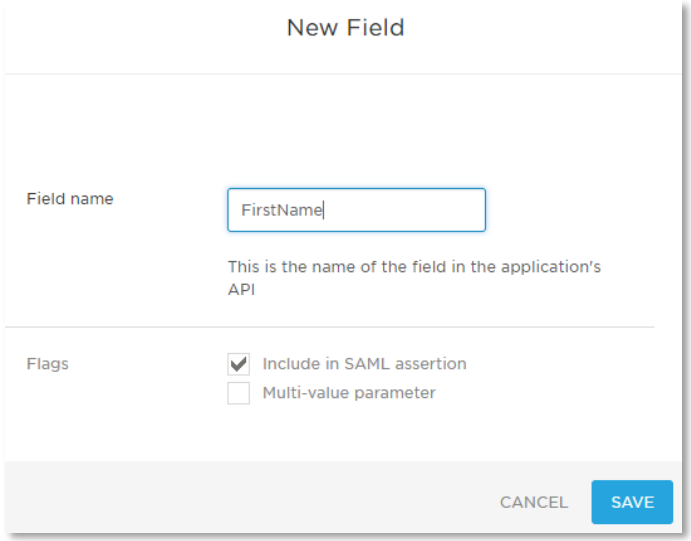


8. By default, OneLogin will send email as a parameter. First Name, Last Name, Title, Department, UserID, Company, Location, Platform, and three custom fields are optional parameters, and must be configured to send the correct information. The Email field is required. Including First Name, Last Name, Title, and Department is BrainStorm's best practice. The other fields are optional and can be used to send any desired attribute to QuickHelp for user classification and reporting, not just what the Attribute Label indicates.

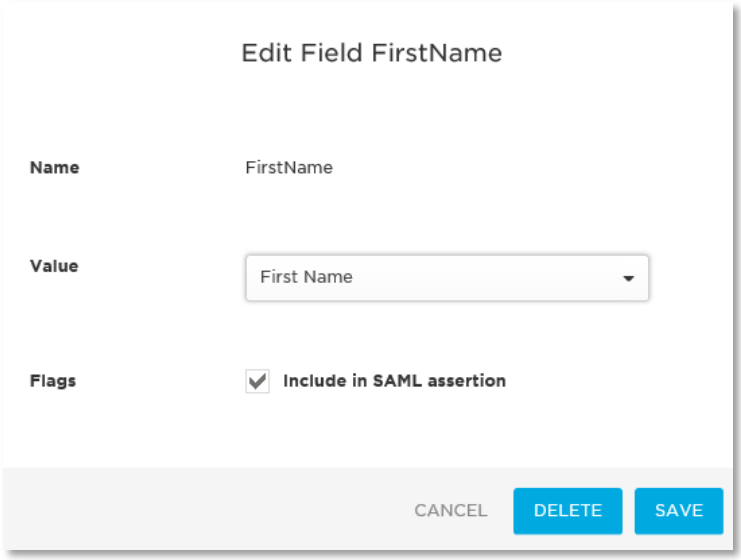


NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

9. To configure all other optional parameters:
    a. Click **Add parameter**.
    b. Enter a *Field Name*, e.g. FirstName – this is an open field but will be used in the Portal Configuration section of the document.
    c. Check the **Include in SAML Assertion** checkbox.



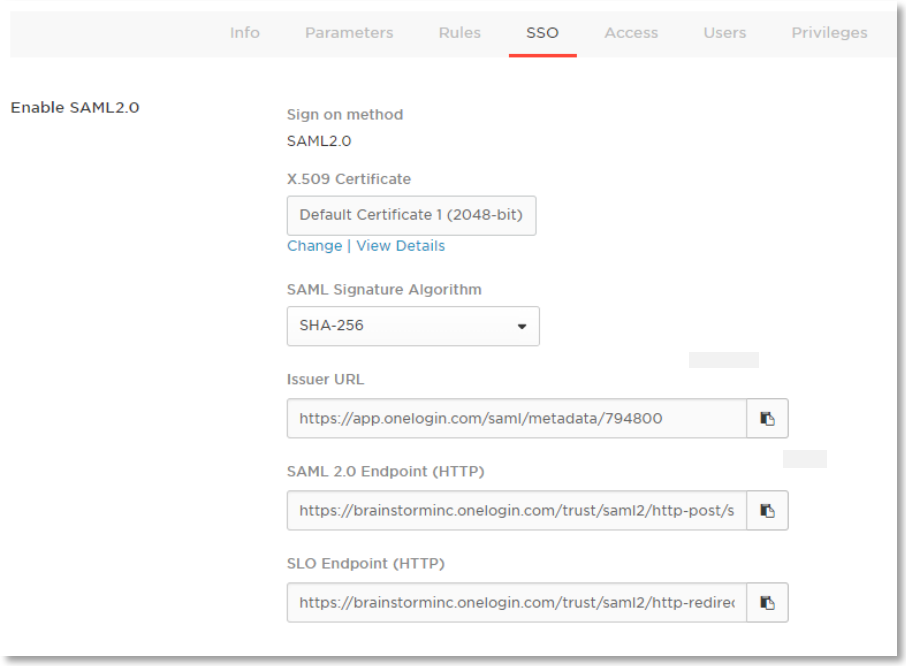
    d. Click **Save**.
    e. From the Value pull-down menu, select the corresponding OneLogin value.



    f. Click **Save**.
    g. Repeat for all added parameters.

There is an additional attribute for Group. If there is an attribute in OneLogin that makes sense to use for QuickHelp groups, add it here. However, whatever you use as the QuickHelp Group identifier should be fairly small in number as a QuickHelp group will be created for each user-assigned value of the attribute selected.

10. Click the **SSO** tab.
11. Change the *SAML Signature Algorithm* to **SHA-256**.
12. Copy and save the full URL for the Issuer URL.



13. Assign access to QuickHelp to the appropriate users.
    a. This can be done either on an individual user basis (**Users > All Users > Edit User > Applications tab > New**), or by using Roles and Mappings. For more information, consult OneLogin documentation.
14. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

BrainStorm

QuickHelp™ Single Sign-On

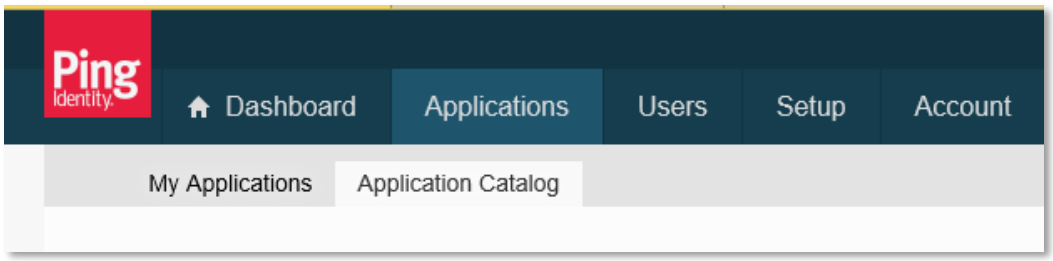
PingOne

Compatibility

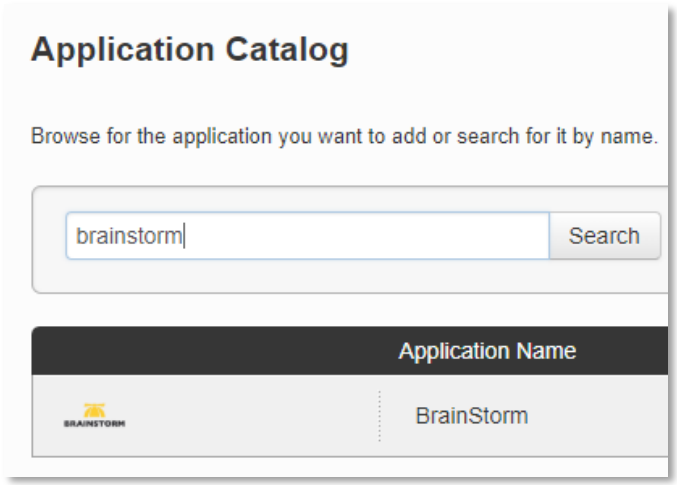
QuickHelp is part of PingOne's catalog of pre-integrated applications, making it easy to enable single sign-on. Configuration requires a PingOne administrator.
Please note that SSO will not be enabled until both the following PingOne configuration and the QuickHelp Portal configuration have been completed.

PingOne configuration

1. Log in to the PingOne Admin Portal.
2. Click the Applications tab > **Application Catalog**

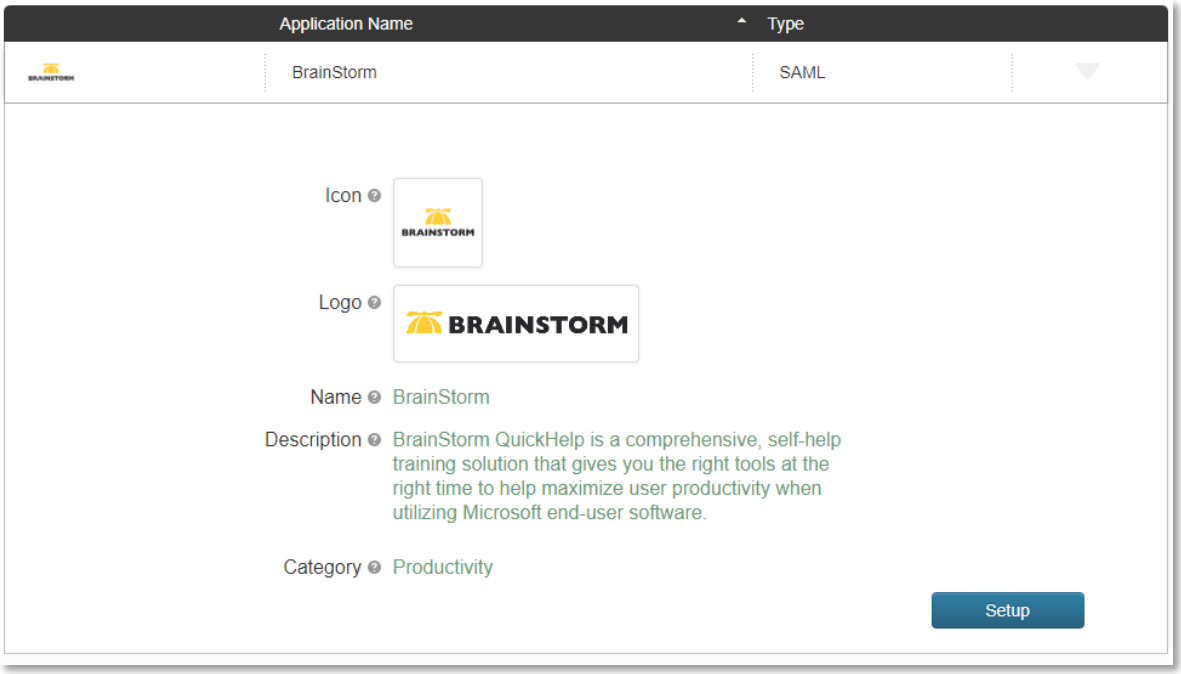


3. Search the catalog for ***BrainStorm***.



4. Click the Show Application Details button to the right of the Application Name.

5. Click **Setup**.

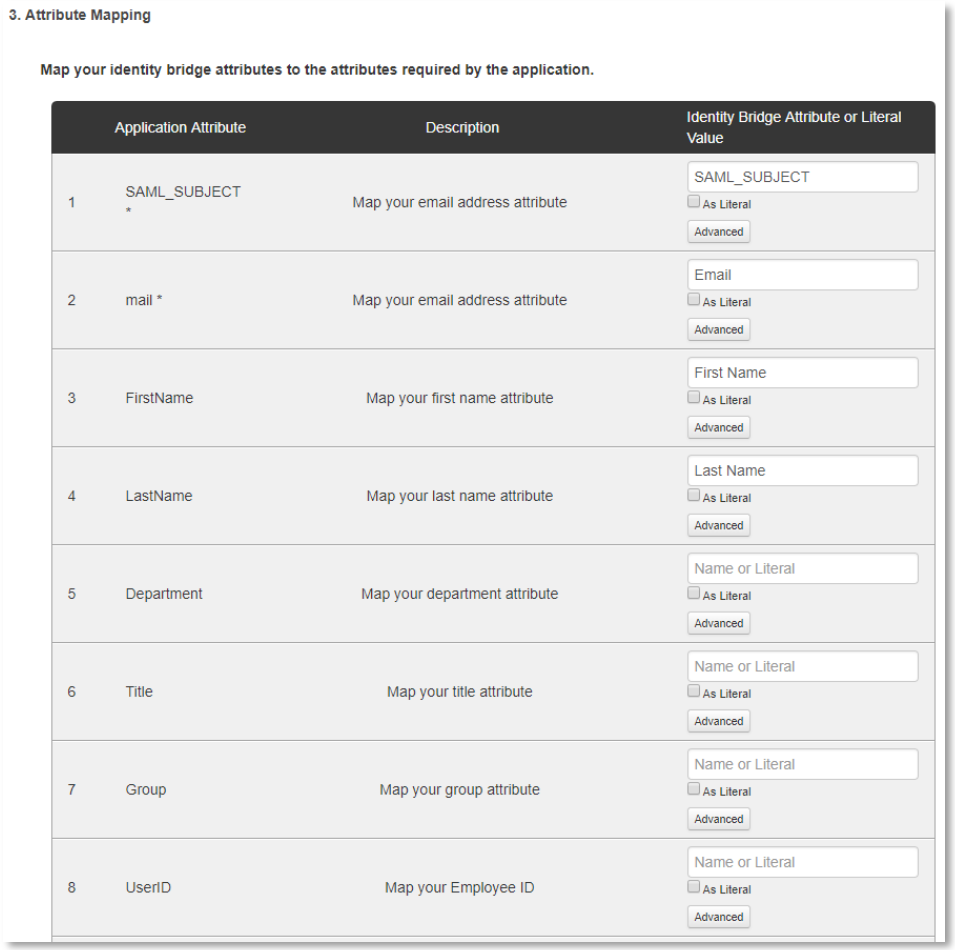


6. Leave SSO Instructions as the default and click **Continue to Next Step**.
7. Under Configure your connection > *Upload Metadata*, click **Or use URL**.
8. Put BrainStorm's metadata URL in the Upload Metadata field:
   https://quickhelp.blob.core.windows.net/metadata/QuickhelpSamlMetadata2024.xml

9. Once that is uploaded, click **Continue to Next Step**.
10. By default, PingOne will send attributes for Email (required), First Name, Last Name, Title, Department, UserID, Company, Location, Platform, and three custom fields. However, each attribute must be configured to send the desired information. The Email field is required. Including First Name, Last Name, Title, and Department is BrainStorm's best practice. The other fields are optional and can be used to send any desired attribute to QuickHelp for user classification and reporting, not just what the Attribute Label indicates.

NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

11. Click in the *Identity Bridge Attribute or Literal Value* field for **mail**.

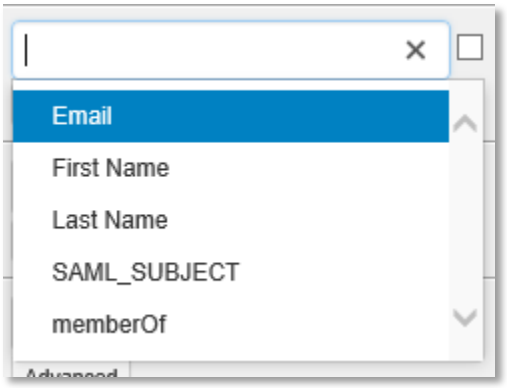


3. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	SAML_SUBJECT *	Map your email address attribute	SAML_SUBJECT As Literal Advanced
2	mail *	Map your email address attribute	Email As Literal Advanced
3	FirstName	Map your first name attribute	First Name As Literal Advanced
4	LastName	Map your last name attribute	Last Name As Literal Advanced
5	Department	Map your department attribute	Name or Literal As Literal Advanced
6	Title	Map your title attribute	Name or Literal As Literal Advanced
7	Group	Map your group attribute	Name or Literal As Literal Advanced
8	UserID	Map your Employee ID	Name or Literal As Literal Advanced

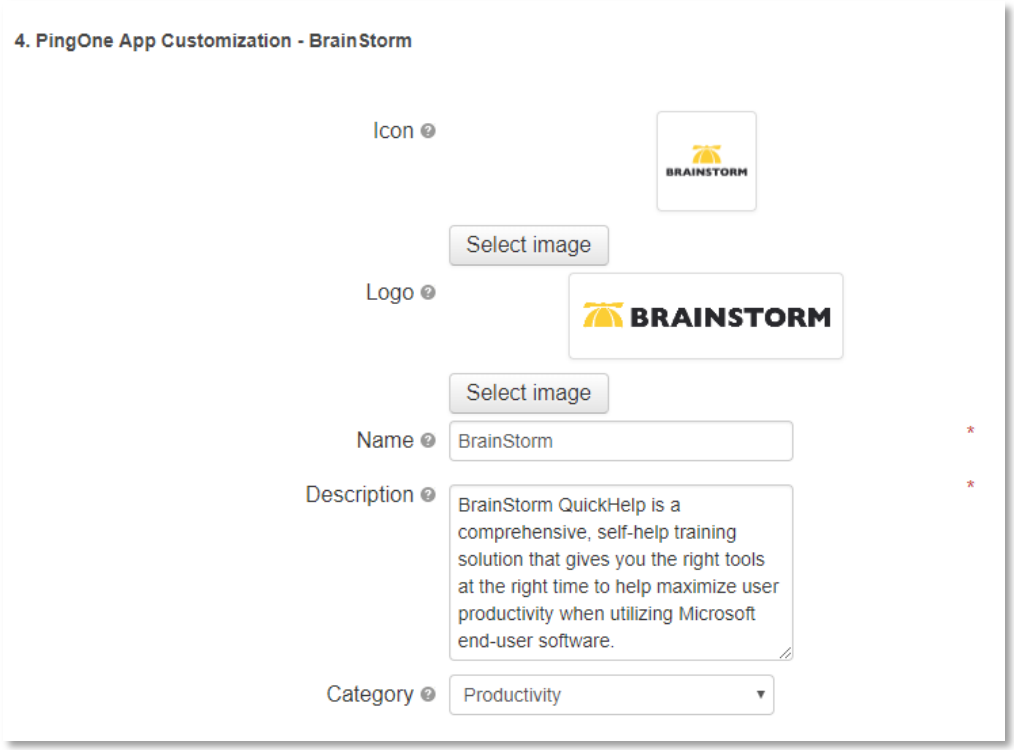
12. Choose **Email** from the pulldown menu.



13. Repeat for all other attributes, as needed.

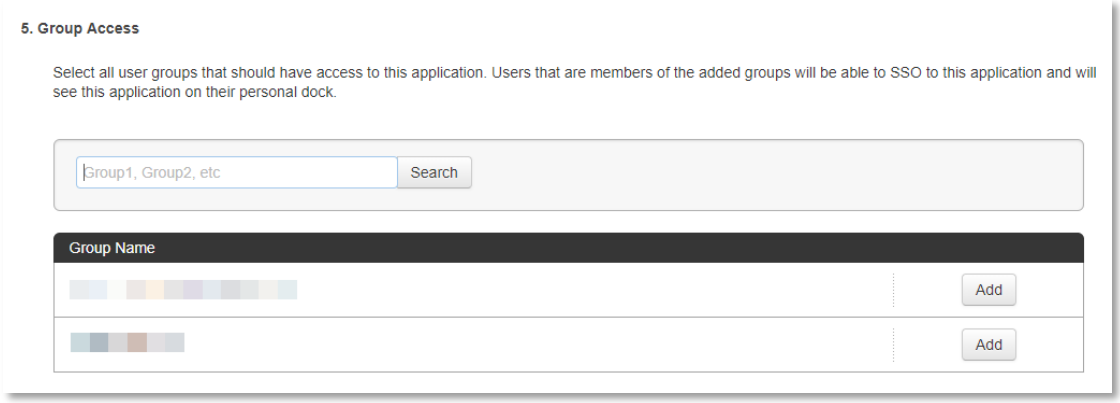
There is an attribute for Group. If there is an attribute in PingOne that makes sense to use for QuickHelp groups, map it here. However, whatever you use as the QuickHelp Group identifier should be fairly small in number as a QuickHelp group will be created for each user-assigned value of the attribute selected.

14. Click **Continue to Next Step**.
15. In *4. PingOne App Customization – BrainStorm*, change the Logo, Icon, or name, as desired. However, these fields can be left as they are.



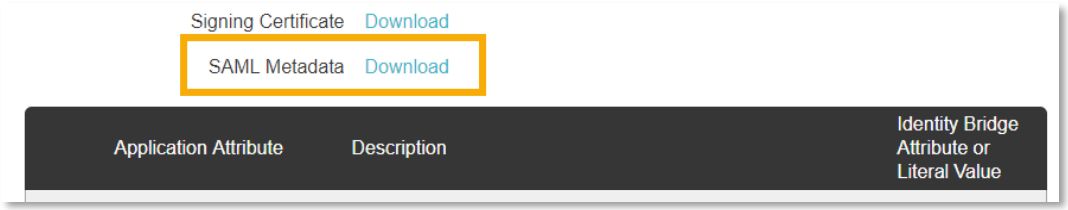
16. Click **Continue to Next Step**

17. Add the groups of users that should have access to QuickHelp



NOTE: If a user not belonging to the added group(s) attempts to access QuickHelp, that attempt will fail.

18. Click **Continue to Next Step**
19. Review the configuration setup
20. Click **Download** next to *SAML Metadata to download* and save the metadata file that will be used to finish configuration



21. Click **Finish**
22. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

BrainStorm

QuickHelp™ Single Sign-On

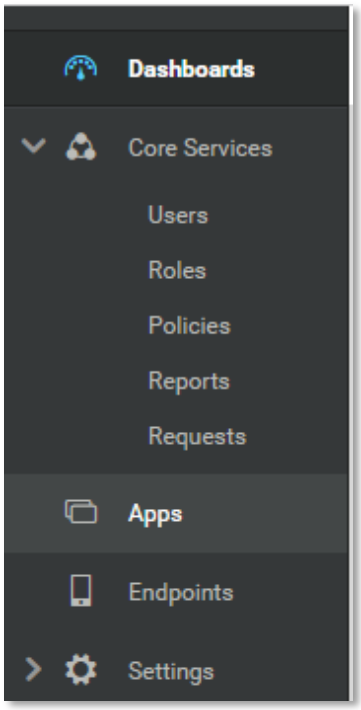
Centrify

Compatibility

QuickHelp is part of Centrify's catalog of pre-integrated applications, making it easy to enable single sign-on. Configuration requires a Centrify administrator.
Please note that SSO will not be enabled until both the following Centrify configuration and the QuickHelp Portal configuration have been completed.

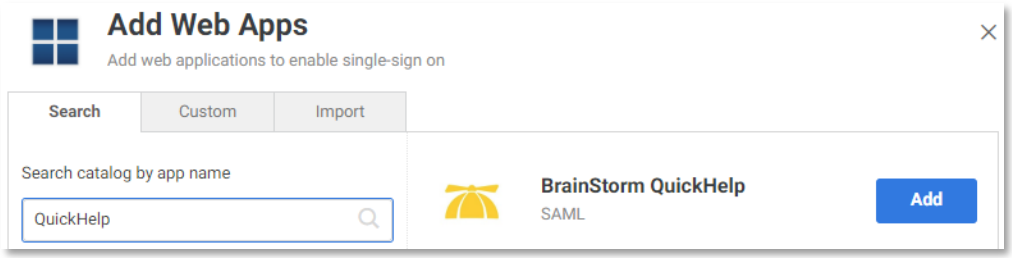
Centrify configuration

1. Log in to the Centrify Admin Portal.
2. Choose **Apps** from the left-hand menu.



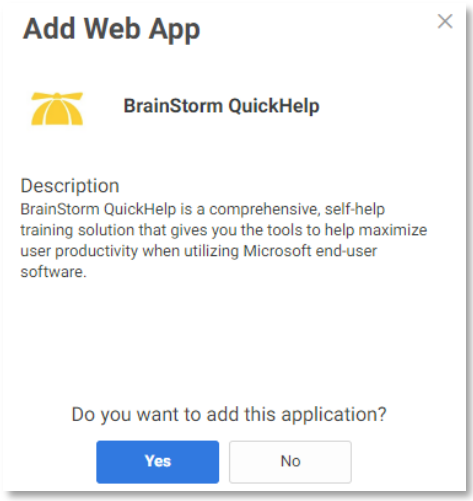
3. Click **Add Web Apps**.

4. In the Search bar, type ***QuickHelp***.

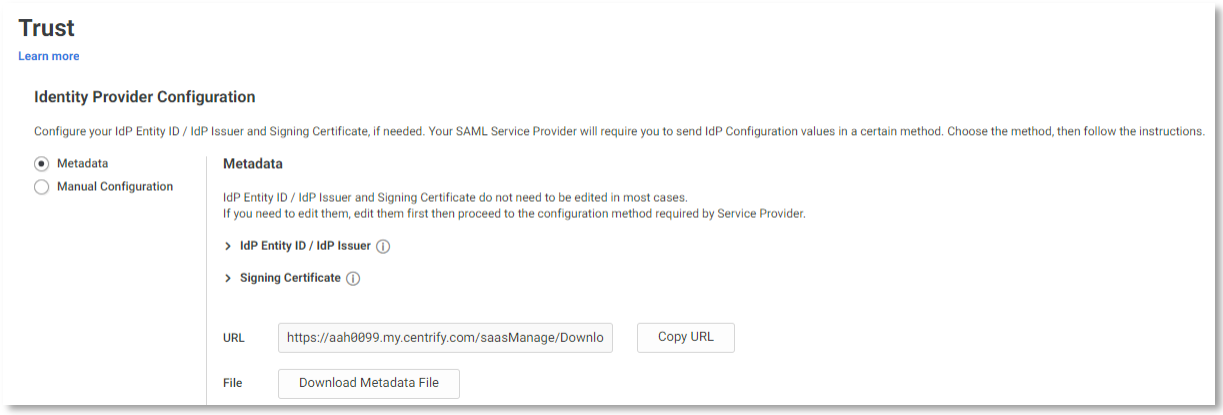


5. In the Results pane, click **Add** next to BrainStorm QuickHelp.

6. When asked if you want to add this application, click **Yes**.



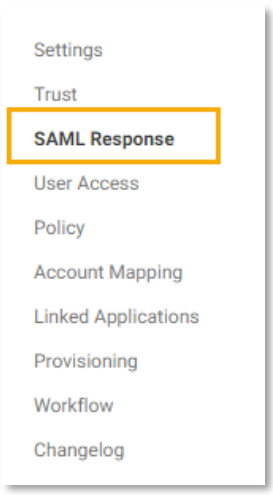
7. Close the *Add Web Apps* dialog window.
8. From the *Trust* configuration window, either copy and save the full URL for the **Metadata location URL** or Download the metadata file.



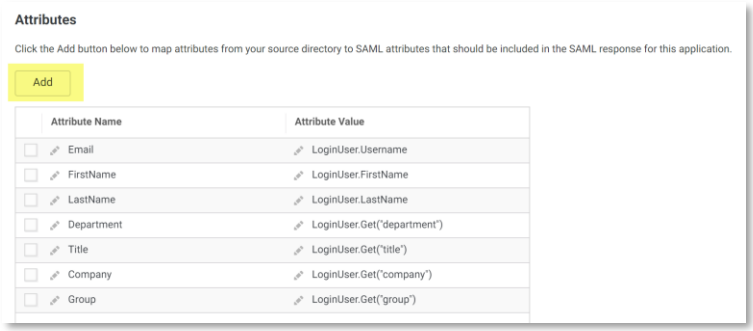
9. To assign QuickHelp to specific users, click **Permissions** on the left, and assign to the desired users, groups, or roles.
10. Click **Save**.
11. Centrify will send Email, First Name, Last Name, Title, Department, Company and Group as attributes to QuickHelp. UserID, Location, Platform, and three custom fields are optional parameters, and must be configured to send the correct information.

NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

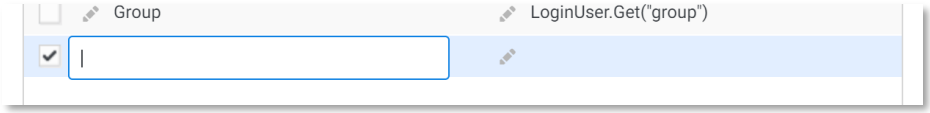
12. To configure optional attributes:
    a. Click on the **SAML Response** tab.



b. Click **Add**.



c. Enter an Attribute Name.
d. Choose the corresponding Attribute Value.



13. If you opt to send LoginUser.Get("group") as an attribute, use the Advanced script in the **SAML Response** dialog to determine which Group names from within Centrify to send to QuickHelp.
    a. To not send any groups, set *var sendgroups* = **false**.
    b. To send **all** groups, leave the *var criteria [ ]* as is.
    c. To send specific groups only, set *var criteria* using regular expressions to filter the group names.
14. Click Save.
15. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

Google

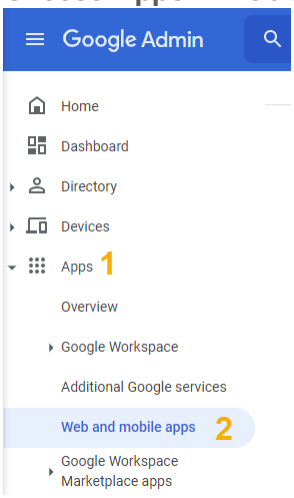
Compatibility

QuickHelp is compatible with Google as an Identity Provider, making it easy to enable single sign-on. Configuration requires a Google Super administrator.

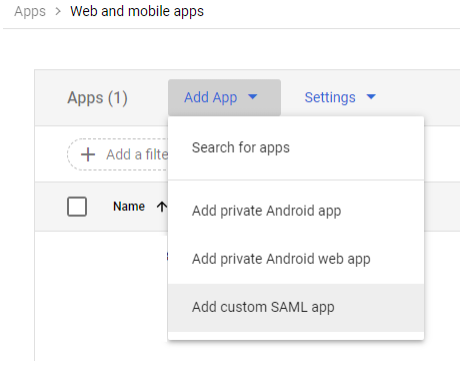
Please note that SSO will not be enabled until both the Google admin console configuration and the QuickHelp Portal configuration have been completed.

Google configuration

1. Log in to the Google Admin Console.
2. Choose **Apps > Web and mobile apps** from the left-hand menu.

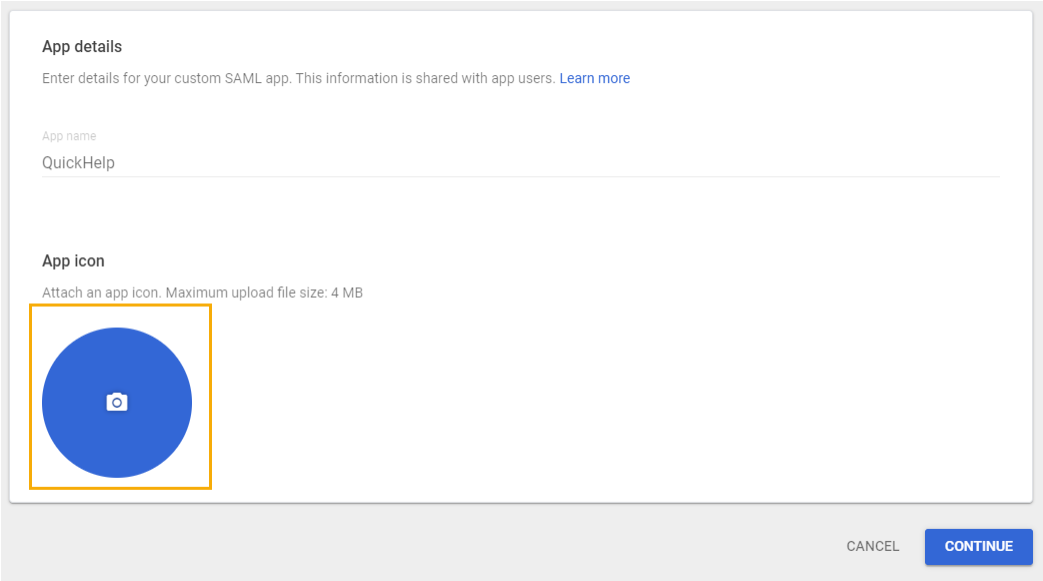


3. Choose **Add App > Add custom SAML app** from the top pulldown menu.

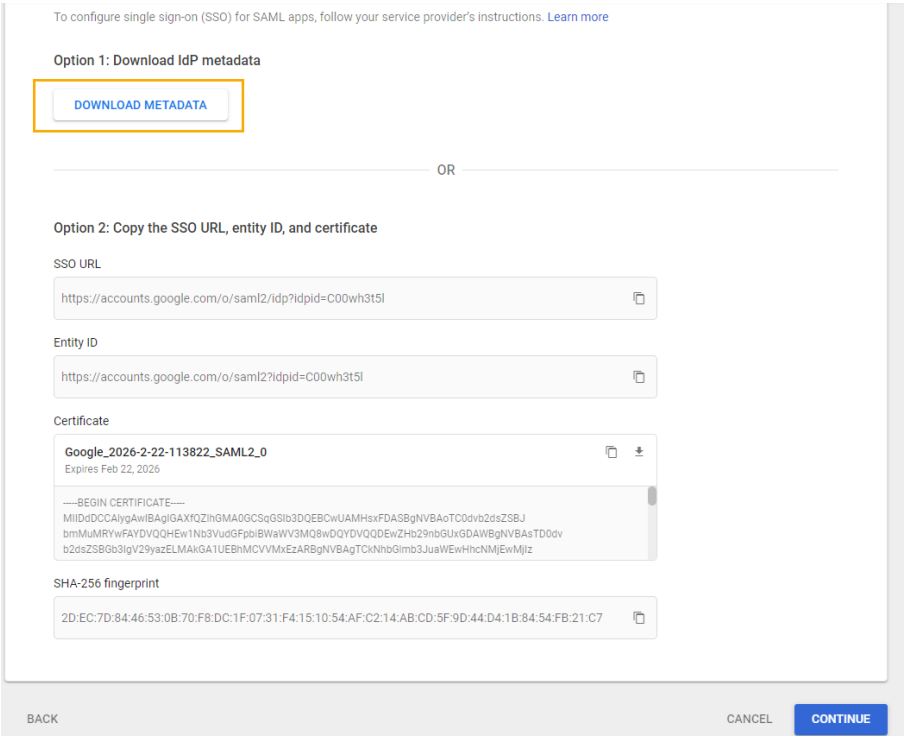


4. Download the BrainStorm logo here.
5. Enter a name in the *App Name* field.

6. Click the **camera** icon.

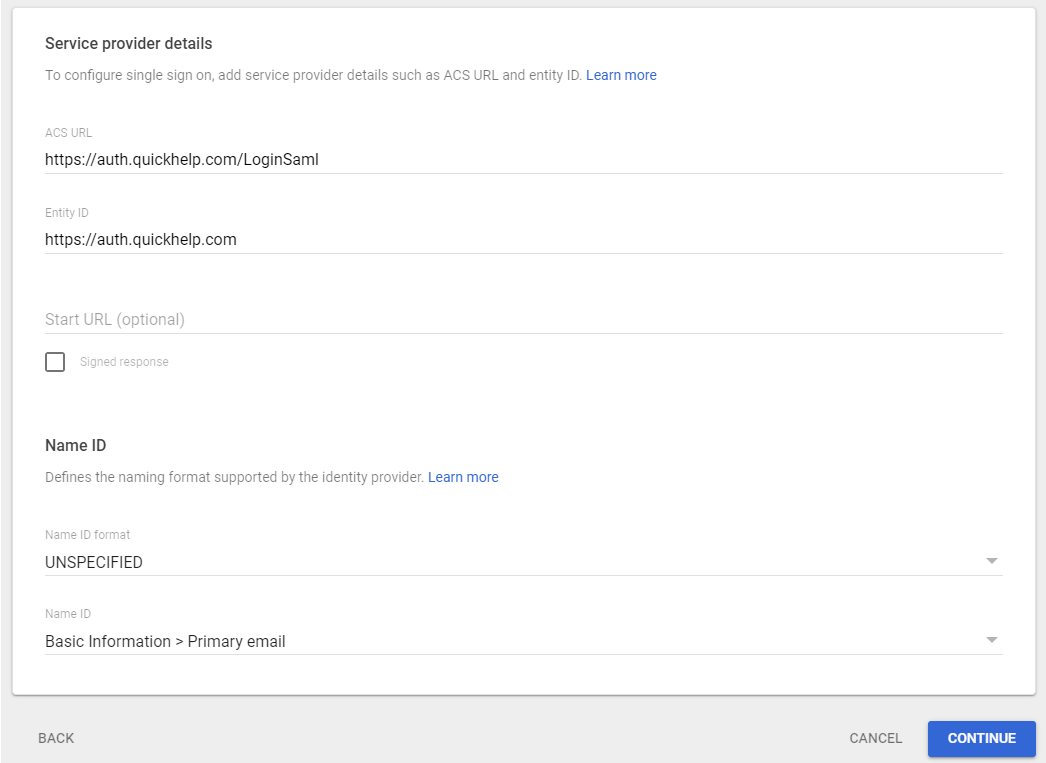


7. Navigate to and open the logo downloaded in step 4.
8. Click **Continue**.
9. Click **Download Metadata** – this will be used in the QuickHelp Admin Portal configuration section.
10. Click **Continue**.

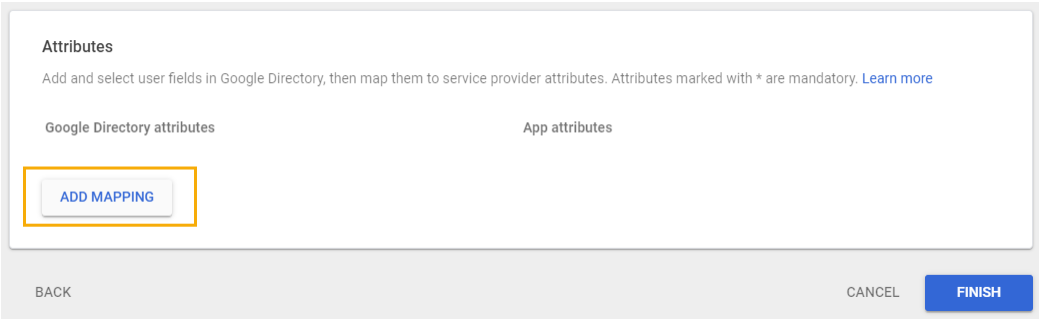


11. Enter https://auth.quickhelp.com/LoginSaml in the *ACS URL* field.

12. Enter https://auth.quickhelp.com in the *Entity ID* field.
    NOTE: These fields are case sensitive, so copy and paste these exact values.
13. Set the *Name ID format* field to **UNSPECIFIED**.
14. Set the *Name ID* field to **Basic Information > Primary email**.

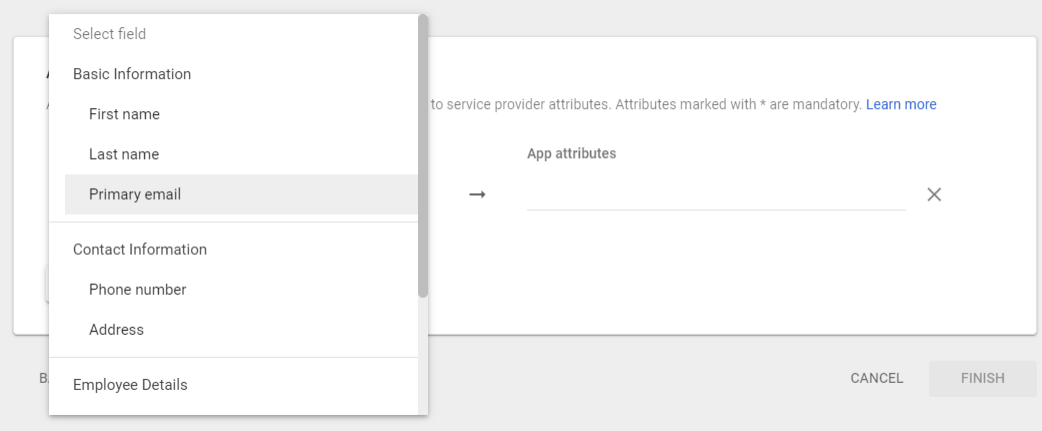


15. Click **Continue**.
16. Under *Attributes*, click **ADD MAPPING**.
    NOTE: The Email field is required. Including First Name, Last Name, Title, and Department is BrainStorm's best practice.

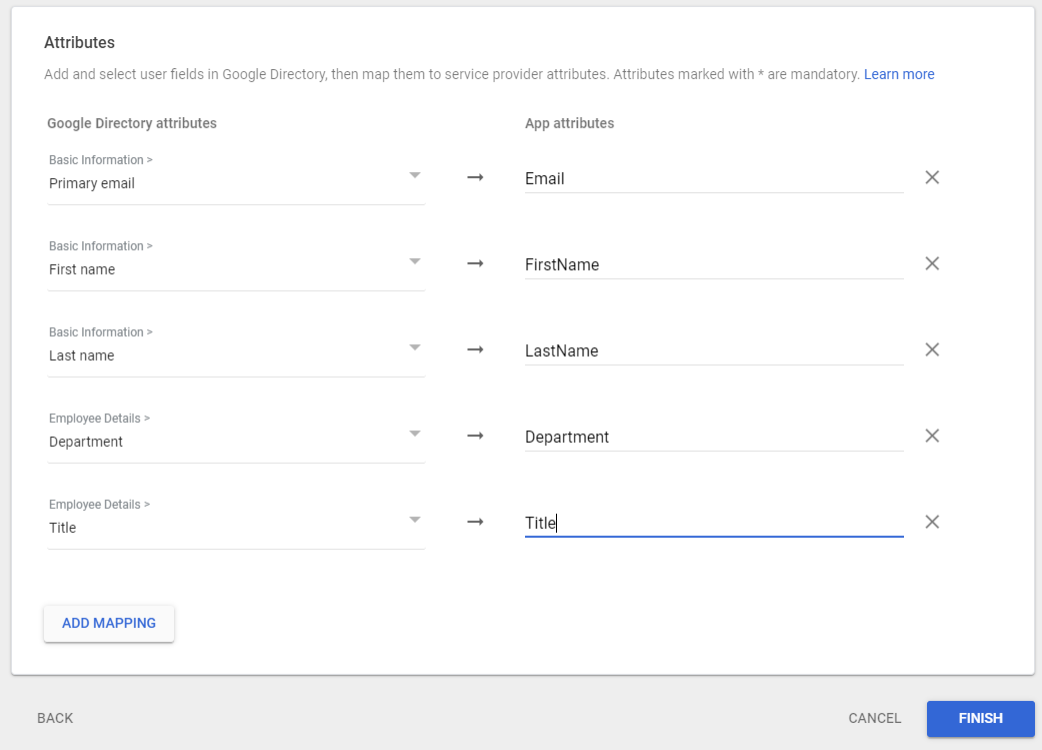


17. From the *Select field* pulldown under Google Directory Attributes, choose **Primary Email**.

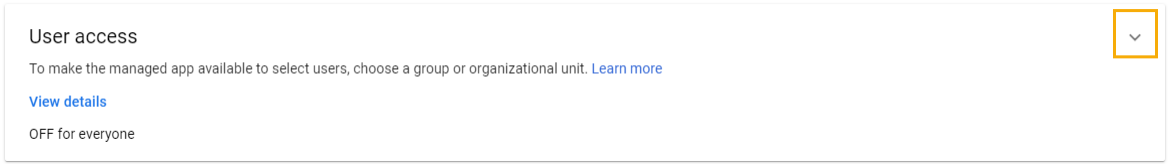
18. In the App Attributes field, give this attribute an **outgoing name**, e.g., Email.
    This is an open field but will be used in the Portal Configuration section of the document.



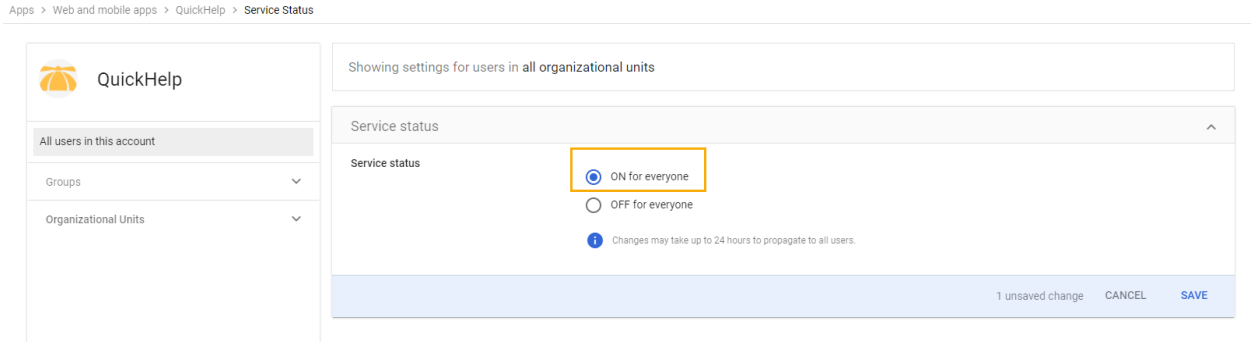
19. Repeat to add other attributes (First Name, Last Name, Department, Job Title).



20. Click **Finish**.
21. You are redirected to the Web and mobile apps configuration page for this new app – to turn on this SSO service for all users, click the **down arrow** in the **User Access** section.



22. Select the **ON for everyone** radio button.



23. Click **Save**.
    NOTE: To turn the service on by organization unit or access group, please refer to the **Turn on your SAML app** section in Google's Set up your own custom SAML application document.
24. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

BrainStorm

SAML 2.0

Compatibility

As mentioned in the introduction, QuickHelp is compatible with potentially any SSO platform that can support SAML 2.0 standards. While there are too many to list individually, two of note are Ping Federate and CA Single Sign-On (CA SiteMinder).

This section of configuration instructions will contain BrainStorm information only and should work with most SAML 2 Identity Providers (IdPs).

Please note that SSO will not be enabled until both the following SAML 2.0 configuration and the QuickHelp Portal configuration have been completed.

SAML 2.0 configuration

1. Log in to your SAML 2.0 Identity Provider.
2. BrainStorm's metadata can be found here: https://quickhelp.blob.core.windows.net/metadata/QuickhelpSamlMetadata2024.xml
3. Email must be an assertion attribute, not just the SAML Subject or NAME ID.
4. Add First name, Last name, Title, and Department as additional assertion attributes. UserID, Company, Location, Platform, and three custom fields are optional parameters, and must be configured to send the correct information.

NOTE: Currently, only Email, First Name, Last Name, Title, Department, and Group are visible to end users and/or Admins. The other fields are stored In QuickHelp but are not yet visible.

There is an additional attribute for Group. If there is an attribute in your Identity Provider that makes sense to use for QuickHelp groups, add it here. However, whatever you use as the QuickHelp Group identifier should be fairly small in number as a QuickHelp group will be created for each user-assigned value of the attribute selected.

5. Copy and save the IdP-generated metadata URL.
6. **To complete configuration, go to the Portal Configuration section of this document.**

QuickHelp™ Single Sign-On

BrainStorm

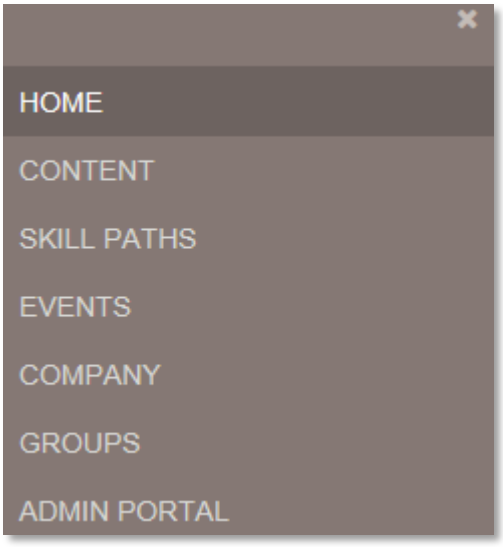
Portal configuration

Compatibility

The following steps require that you have access to the QuickHelp Admin Portal. If you don't have access, please contact your organization's QuickHelp Administrator, or your BrainStorm deployment team.

Configuration

1. Login to the QuickHelp portal using your QuickHelp administrator account and password.
2. Click the three-line menu at the top left and then choose **Admin Portal**.



3. Click **Settings**.

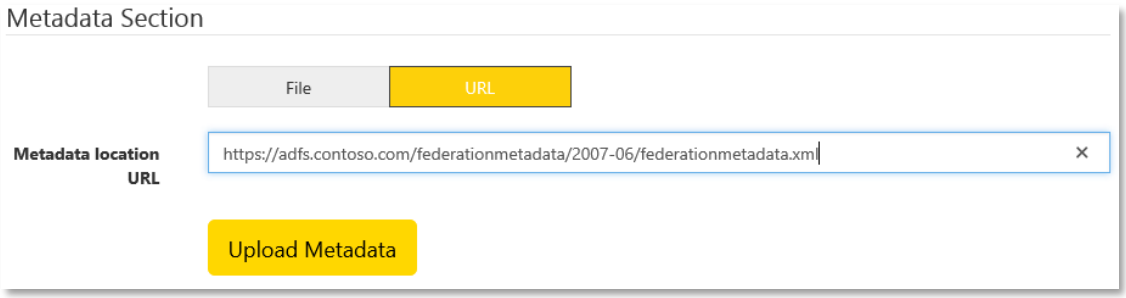
4. Click **Authentication Settings**.

5. Click **Add Provider** in the Action Bar at the bottom of the screen.

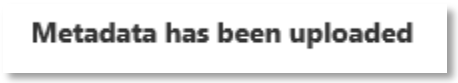
6. For SSO Type, choose the appropriate setting:
    a. ADFS = WSFederation
    b. Azure Active Directory = WSFederation
    c. Okta = SAML2
    d. OneLogin = SAML2
    e. PingOne = SAML2
    f. Centrify = SAML2
    g. SAML 2.0 = SAML2

7. If your metadata is accessible from the Internet, select **URL** under *Metadata* and enter the URL for your metadata.

ADFS like: https://adfs.contoso.com/federationmetadata/2007-06/federationmetadata.xml
Azure Active Directory like: https://login.microsoftonline.com/<alphanumeric-sequence/federationmetadata/2007-06/federationmetadata.xml?appid=<alphanumeric-sequence> or Azure downloads the file, so use the Direct File Upload.
OneLogin similar to: https://app.onelogin.com/saml/metadata/<6-digits>
OKTA: OKTA downloads the file, so use the Direct File Upload.
PingOne: PingOne downloads the file, so use the Direct File Upload.
Centrify: Centrify downloads the file, so use the Direct File Upload
SAML 2.0: may vary by Identity Provider



8. Click **Upload Metadata**. You should get this confirmation:



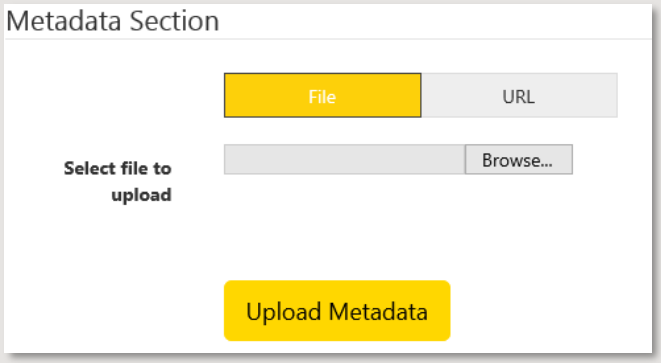
If you see an error, check your URL and inbound access by trying to access the same URL from outside your organizations firewall or use the Direct File upload instead.

Direct File Upload

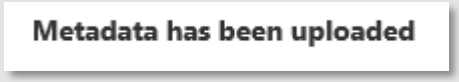
If the URL upload doesn't work (or if you only have a metadata file), you can upload your metadata file directly.

NOTE: To create a file from the metadata URL, open the URL from a web browser (in some cases, this may require that you be inside your firewall). You should see a well-formed XML file. If using Internet Explorer and it does not look like a well-formed XML file, try using another browser or enable compatibility mode (don't forget to turn it back off later if you don't need it). Tap the alt key to display the menu bar if hidden, select File > Save As and save it to a familiar location.

From the QuickHelp Admin Portal, select File, **Browse** to the file, and click Upload Metadata.

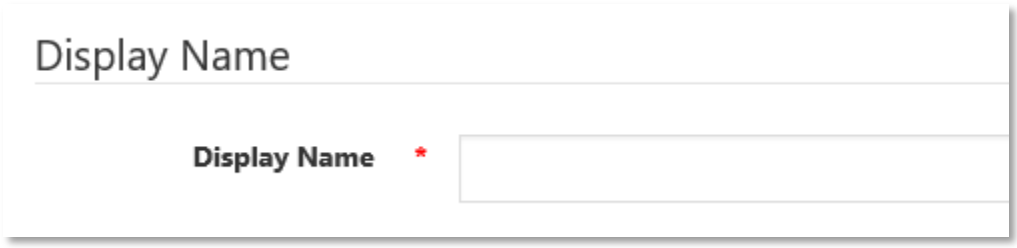


You should get this confirmation:

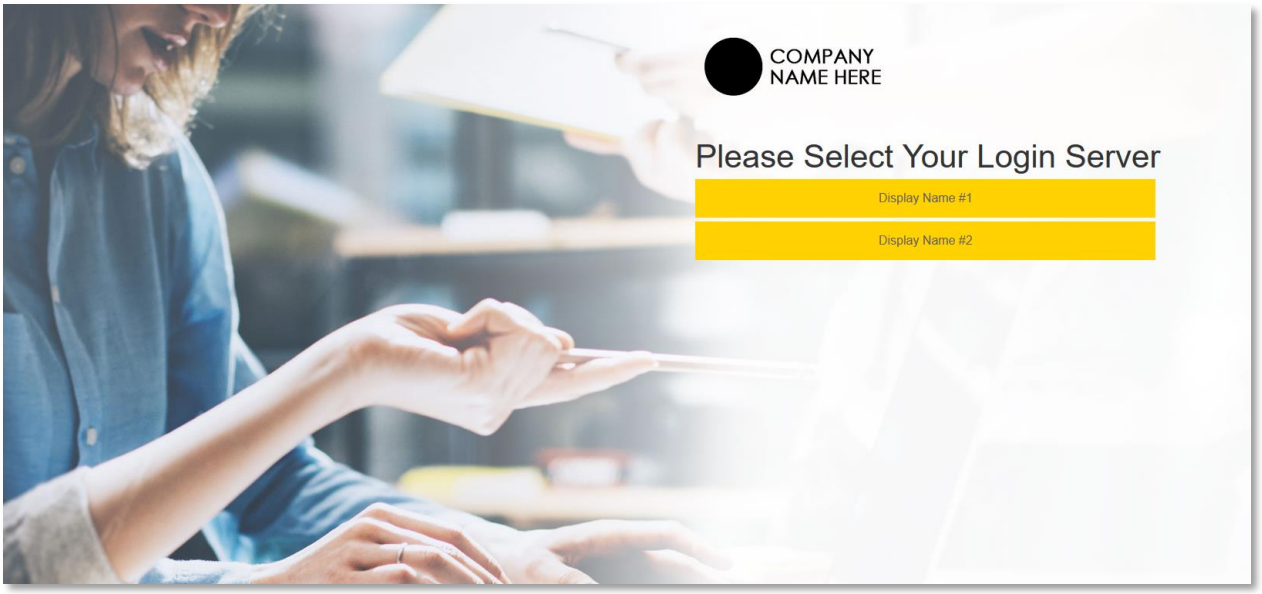


9. Enter a **Display Name** for this Provider

QuickHelp™ Single Sign-On



If your organization is configuring multiple Identity Providers, your end users will be asked to choose the appropriate Login Server before the authentication process can start (see screenshot below). Please choose a Display Name that will be familiar to your end users.



10. In the Attribute Mapping area, paste the correct mapping fields into the corresponding locations – these will vary based on your SSO method. Attributes for each IdP are listed below:

ADFS Mapping

Email: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

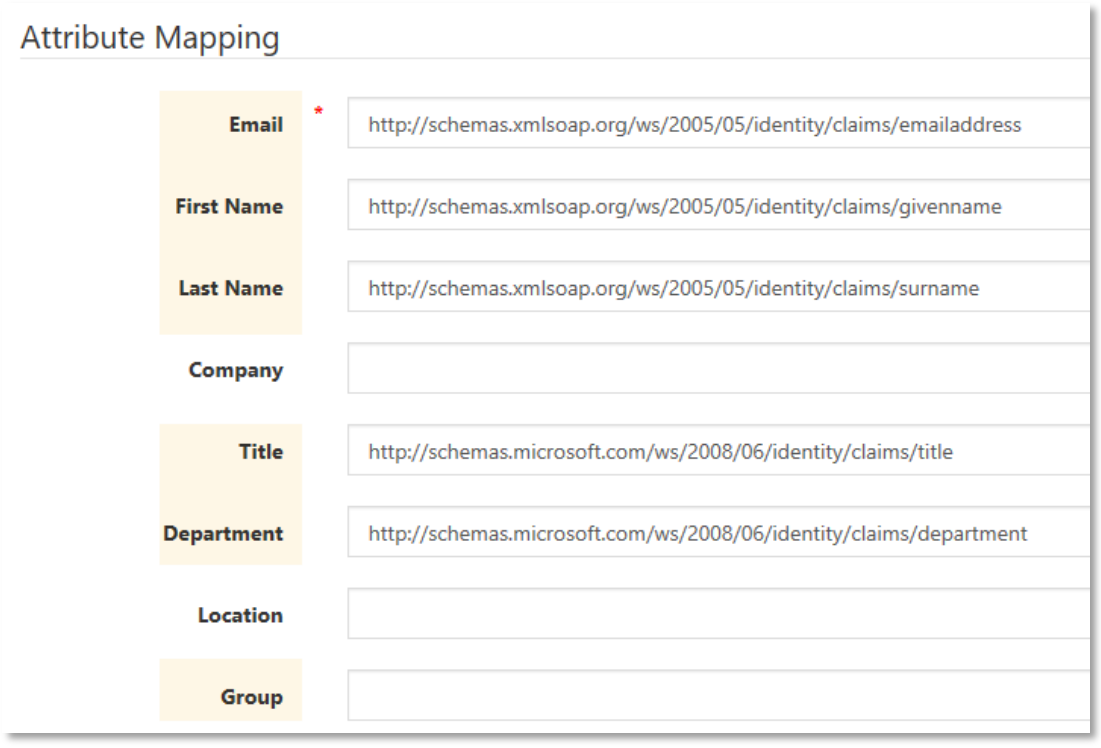
First Name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Last Name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Title: http://schemas.microsoft.com/ws/2008/06/identity/claims/title

Department: http://schemas.microsoft.com/ws/2008/06/identity/claims/department

Group: **If there is an attribute in your IdP that would make sense as a QuickHelp Group Identifier, include it as a Parameter. Whatever you use as the QuickHelp Group Identifier, however, should be fairly small in number as a QuickHelp group will be created for each user-assigned value of the attribute selected. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



QuickHelp™ Single Sign-On

Azure Active Directory Mapping
Email: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress (or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if using UPN)

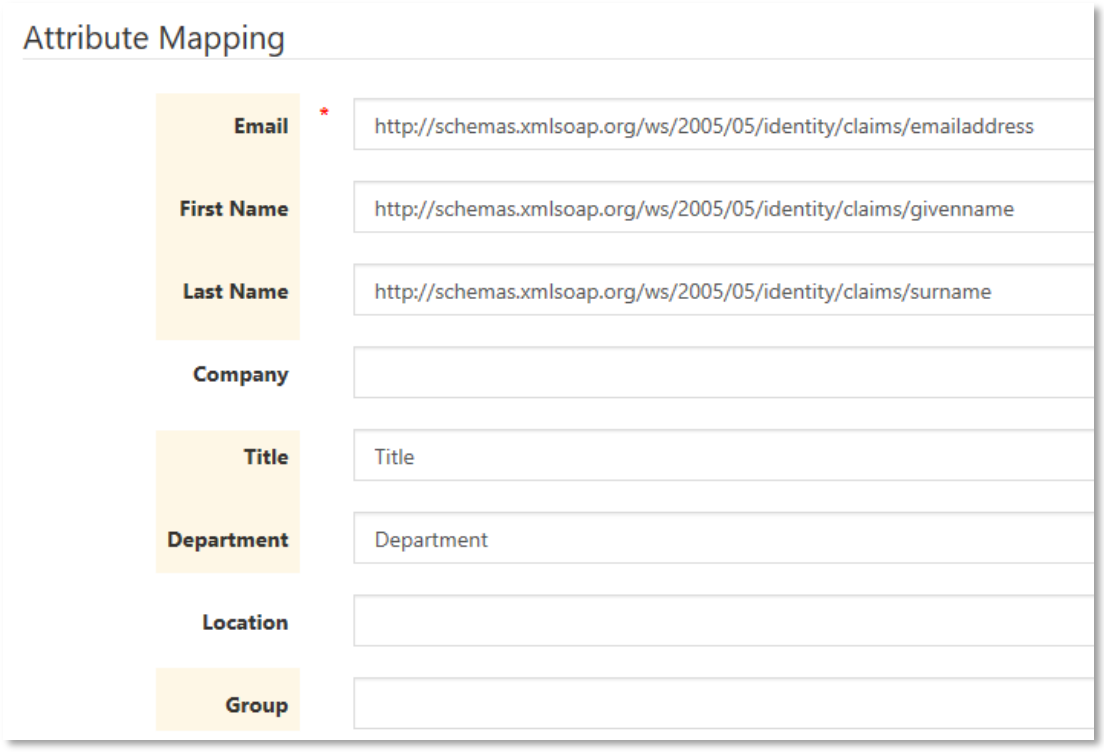
First Name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Last Name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Title: Title (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Department: Department (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Group: **If there is an attribute in your IdP that would make sense as a QuickHelp Group Identifier, include it as a Parameter. Whatever you use as the QuickHelp Group Identifier, however, should be fairly small in number as a QuickHelp group will be created for each user-assigned value of the attribute selected. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



QuickHelp™ Single Sign-On

Okta Mapping

Email: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

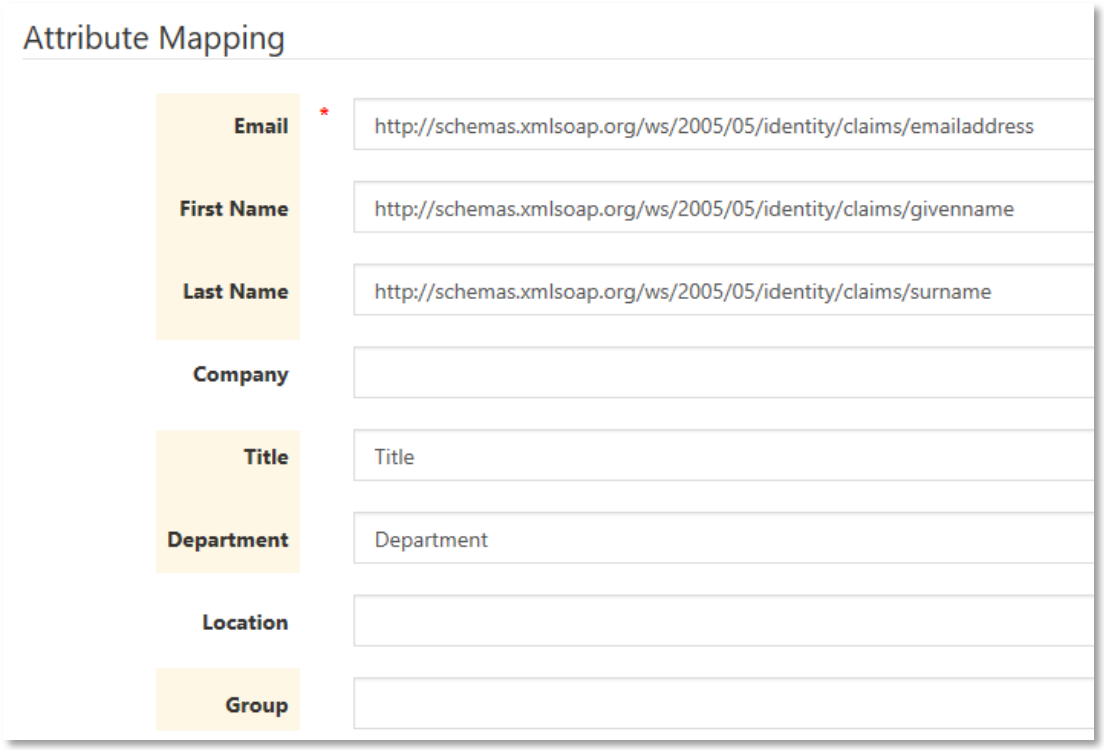
First Name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Last Name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Title: Title

Department: Department

Group: Group **Your OKTA configuration determines which group values will be sent to QuickHelp. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



OneLogin Mapping
Email: email

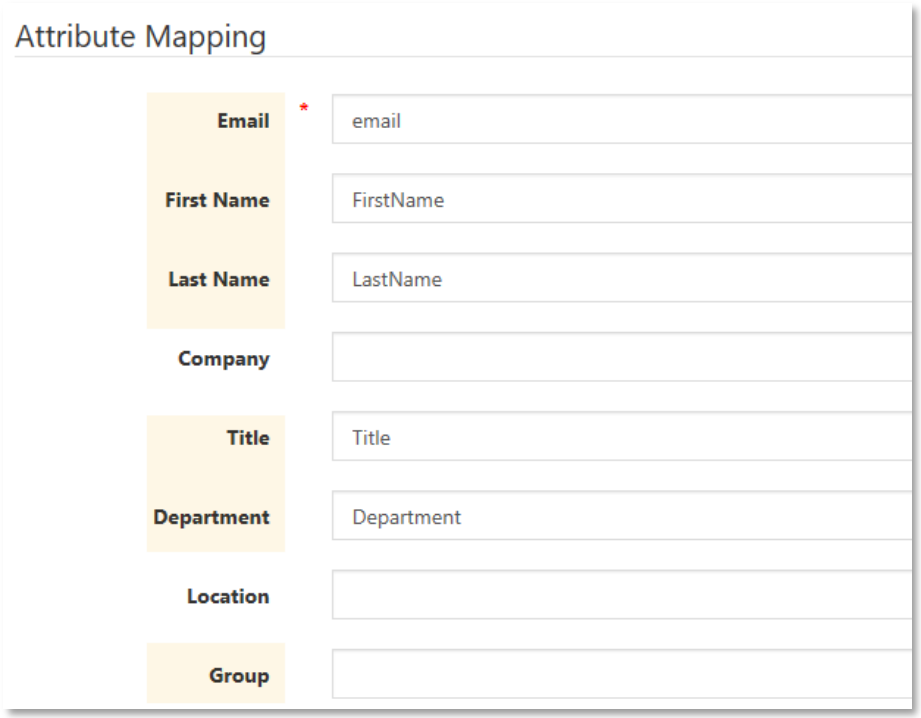
First Name: FirstName (NOTE: This entry depends on what you named the parameter when configuring OneLogin)

Last Name: LastName (NOTE: This entry depends on what you named the parameter when configuring OneLogin)

Title: Title (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Department: Department (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Group: Group (NOTE: This entry depends on what you named the parameter when configuring OneLogin) **Your OneLogin configuration determines which attribute will be sent to QuickHelp. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



QuickHelp™ Single Sign-On

PingOne
Email: mail

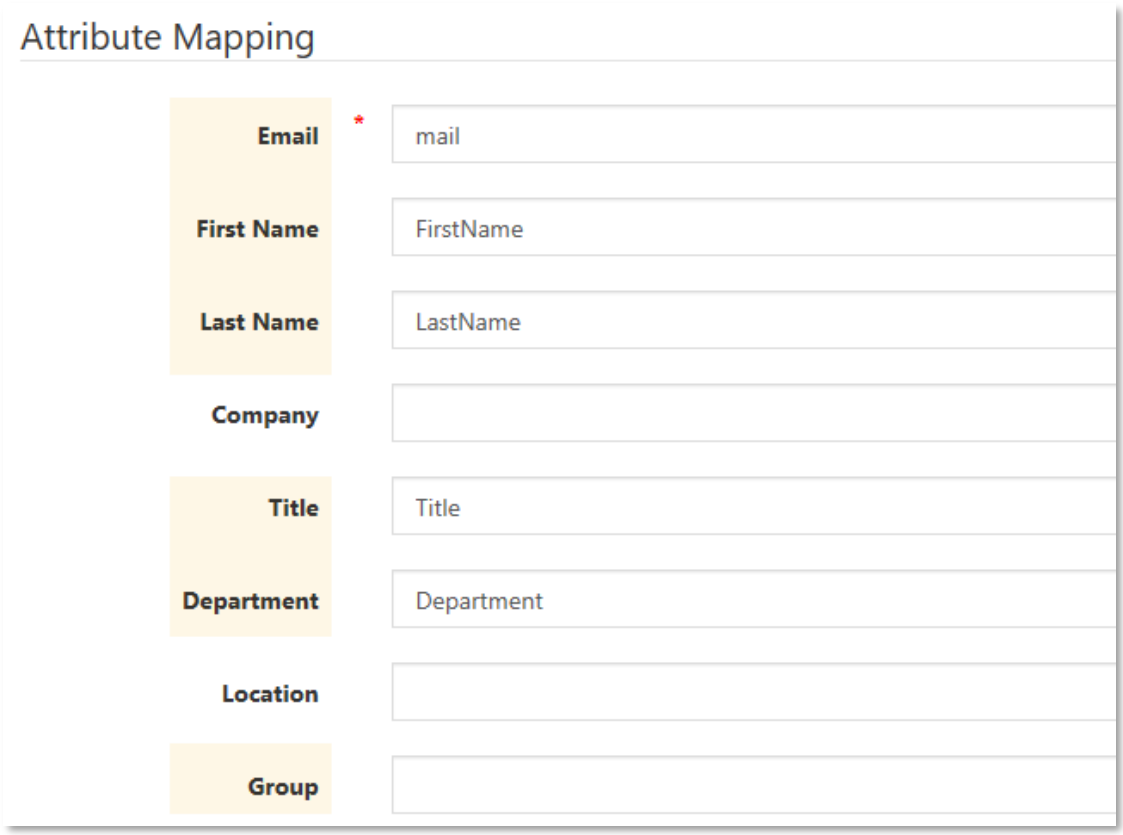
First Name: FirstName

Last Name: LastName

Title: Title

Department: Department

Group: Group **Your PingOne configuration determines which attribute will be sent to QuickHelp. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



QuickHelp™ Single Sign-On

Centrify
Email: Email

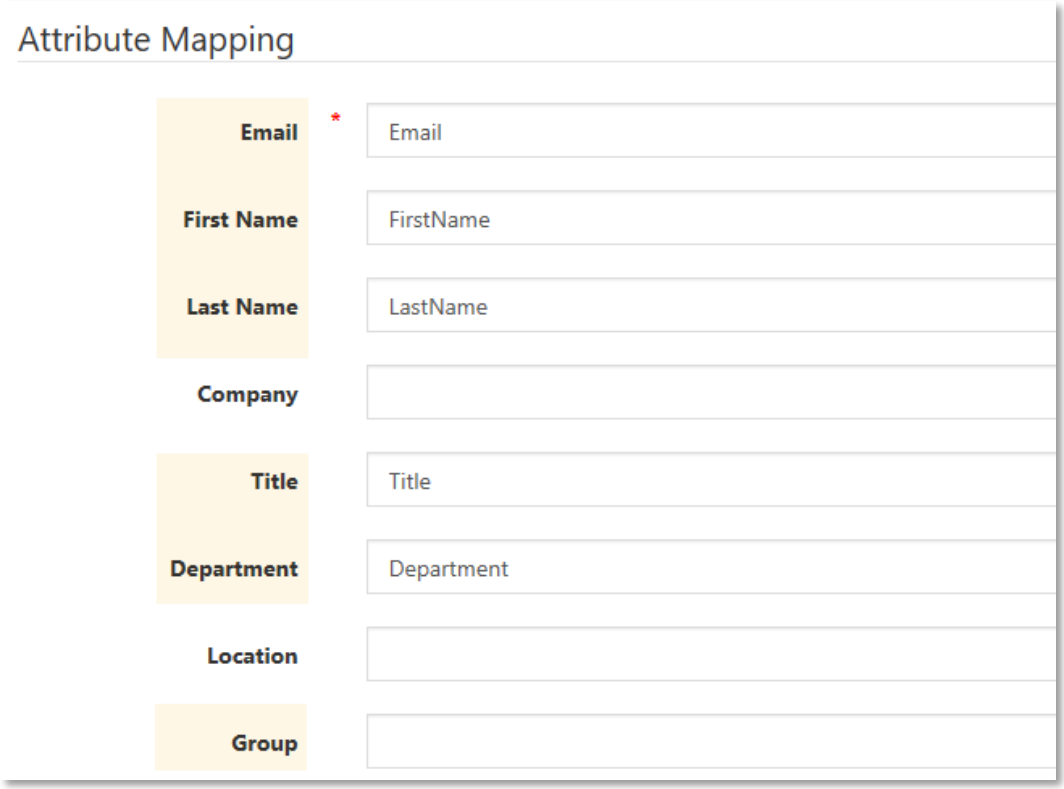
First Name: FirstName

Last Name: LastName

Title: Title

Department: Department

Group: Group **Your Centrify configuration will determine which group values will be sent to QuickHelp. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



SAML 2.0 Mapping

Email: email (NOTE: This entry depends on what you named the parameter when configuring the IdP)

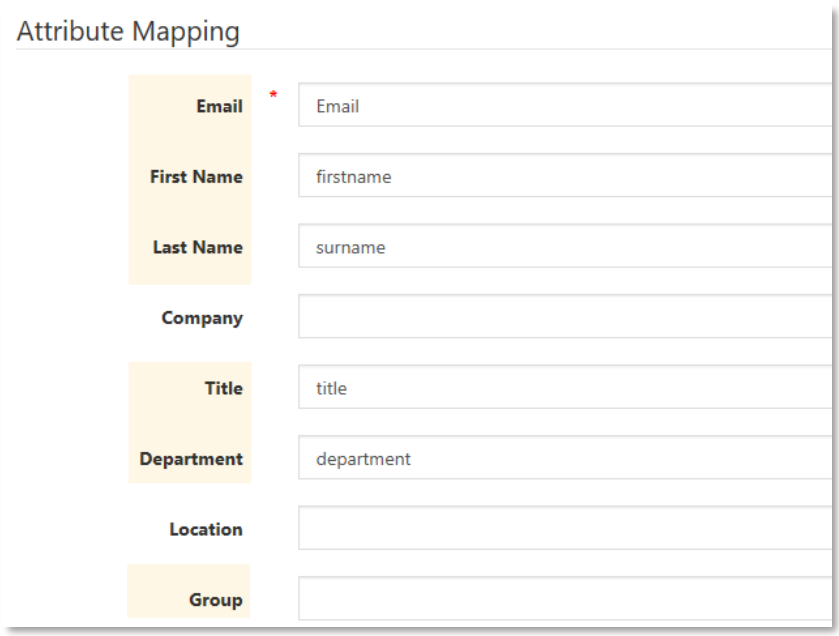
First Name: firstname (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Last Name: surname (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Title: title (NOTE: This entry depends on what you named the parameter when configuring the IdP)

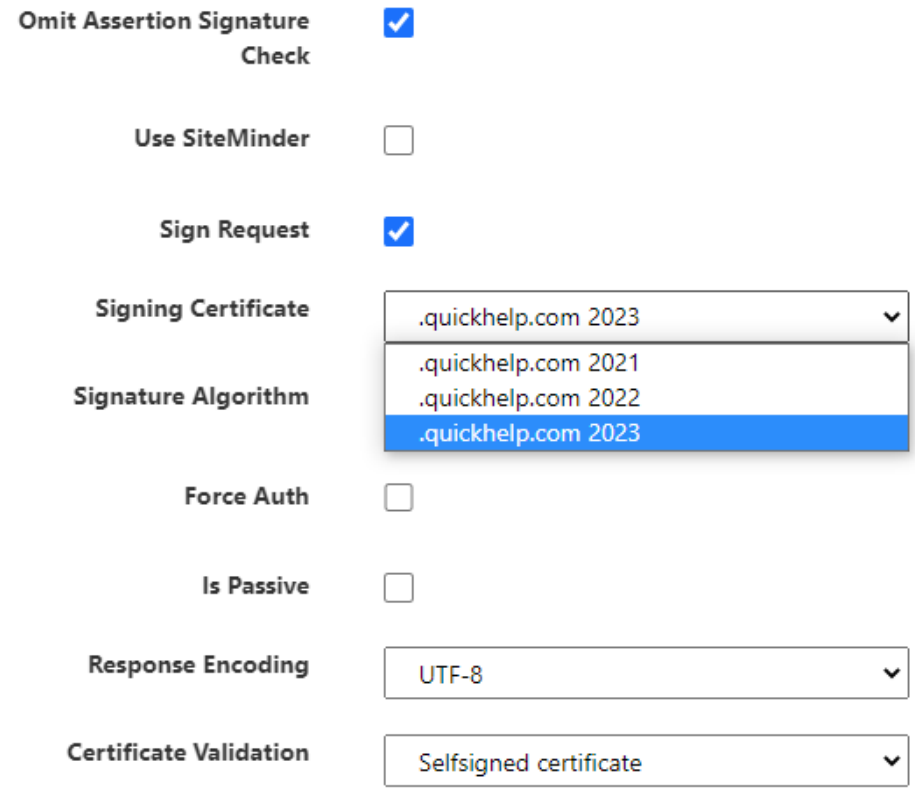
Department: department (NOTE: This entry depends on what you named the parameter when configuring the IdP)

Group: group (NOTE: This entry depends on what you named the parameter when configuring the IdP) **If there is an attribute in your IdP that would make sense as a QuickHelp Group Identifier, include it as a Parameter. Whatever you use as the QuickHelp Group Identifier, however, should be fairly small in number as a QuickHelp group will be created for each user-assigned value of the attribute selected. If you are using Department or Title as the Group Identifier, use the same name in each respective field.**



SAML 2.0 Settings

If you chose SAML2 as the SSO Type in step 6, you will be presented with the following settings. You will not see these settings with ADFS or Azure AD. Configure each setting as required by your IdP.



Omit Assertion Signature Check: If checked, QuickHelp will not verify the signature in your SAML response. In effect, the signature in the SAML response is ignored.

Use SiteMinder: If using SiteMinder as the IdP, check this box.

Sign Request: If checked, QuickHelp will sign the SAML request.

Signing Certificate: Ensure that this is set to *.quickhelp.com 2020*

Signature Algorithm: QuickHelp's default Signature Algorithm is SHA1. If your IdP requires SHA256, choose SHA256 from this pulldown menu.

Force Auth: If checked, QuickHelp will add a *ForceAuthn* attribute in the request from QuickHelp. However, whether this is used or not depends on your IdP. *ForceAuthn* is a standard SAML attribute.

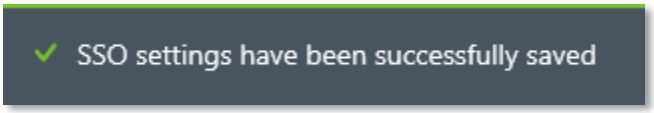
Is Passive: If checked, QuickHelp will add an *isPassive* attribute in the request from QuickHelp. As with Force Auth, whether this is used or not depends on your IdP. *isPassive* is a standard SAML attribute.

Response Encoding: Defaults to UTF-8 – change as needed

Certificate Validation: Defaults to Selfsigned certificate – changes as needed

11. If your metadata file was accepted and you have a valid entry for the Email field, you will see a Save Changes icon in the Action Bar, click Save Changes.

12. When you should see the following confirmation, your QuickHelp portal is now SSO-enabled.



13. To test, leave your existing QuickHelp portal connection open and conduct the testing from another computer (or InPrivate browser window) so that you can remove the SSO configuration if needed. See *Testing access using SSO* below.
14. If you find yourself unable to authenticate after configuring SSO, in the Admin Portal, navigate back to the main Authentication Settings page. Check the box next to your IdP configuration and click **Delete** from the Action Bar.

Testing access using SSO

1. From another computer, try accessing the QuickHelp portal at http://quickhelp.com/routeurl where ‘routeurl’ is the custom ‘landing page’ designated for your organization. If you don’t know your ‘routeurl’ you can initiate SSO by accessing the main site at http://quickhelp.com and entering your organizational e-mail address. It should redirect you to your SSO provider where you will authenticate and then login to QuickHelp.
2. If you are unable to automatically authenticate, and instead are presented with an incident or error ID, please provide that ID to the QuickHelp Support desk (support@quickhelp.com).