


# SAML 2.0 CyberArk Identity Service Integration

Use this article to guide you in setting up CyberArk Workforce Identity (formerly Idaptive or Centrify Identity Service) with SAML single sign-on to manage access to a Agiloft knowledgebase. For more information on SAML configurations, see [SAML 2.0 SSO](#). Note that the steps in this topic might vary depending on the environment in which they are being implemented. Contact [Agiloft support](#) if you need more assistance.

## Prerequisites

To complete these steps, you need an Idaptive account with administrator access, and administrator-level login credentials for Agiloft. You can sign up for a [free trial account](#) to use for testing.

## Add SAML 2.0 to the Knowledgebase

 The full setup requires you to switch between Agiloft and Idaptive, so open each one in its own browser window so you can easily switch between them.

First, if you don't want users to be created automatically in Agiloft when they first log in with Idaptive SAML, create the users first and assign them to the appropriate Groups and Teams.

When you are ready to connect Idaptive:

1. Click the **Setup** gear in the top-right corner and go to **Access > Configure SAML 2.0 Single Sign-On**.
2. On the General tab of the SAML Configuration wizard:
  - a. Select **Enable SAML SSO**.
  - b. Select **Create SAML IdP Authenticated user in Agiloft**.
  - c. Select the last checkbox only if you want to synchronize the user attributes in Agiloft with those in the IdP every time a user logs in. If you leave this deselected, the user's attributes are synchronized only when the user is first created.

<input checked="" type="checkbox"/> <b>Enable SAML SSO</b>
<input checked="" type="checkbox"/> <b>Create SAML IdP Authenticated user in Agiloft</b>
<input checked="" type="checkbox"/> <b>Update User fields on subsequent logins by an existing user</b>
Add the user to / update the user record in the Table/Subtable shown below:
Employees ▼

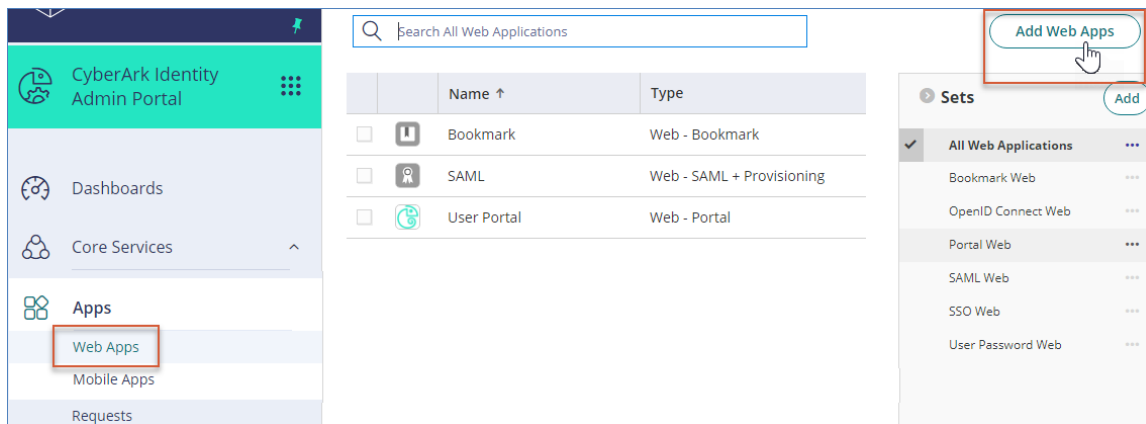
3. On the Service Provider Details tab:
  - a. Leave the first two fields as they are. They are used to fill in Idaptive fields below.
  - b. For the next fields, Keystore file path, Java KeyStore Password, and Alias to add the certificate to the Java KeyStore:

- If you are using Agiloft's hosted service, the fields are populated by Support.
  - If you are using an in-house server where Agiloft is installed, follow the steps in [SAML 2.0 SSO](#) under Generate a Keystore File and Configure the Identity Provider.
4. Click Finish.
  5. Click Download SAML 2.0 Service Provider Metadata and save it to an accessible location.
  6. Click Download X.509 Certificate and save it to an accessible location.

## Create a Web App in Idaptive

Next, open Idaptive.

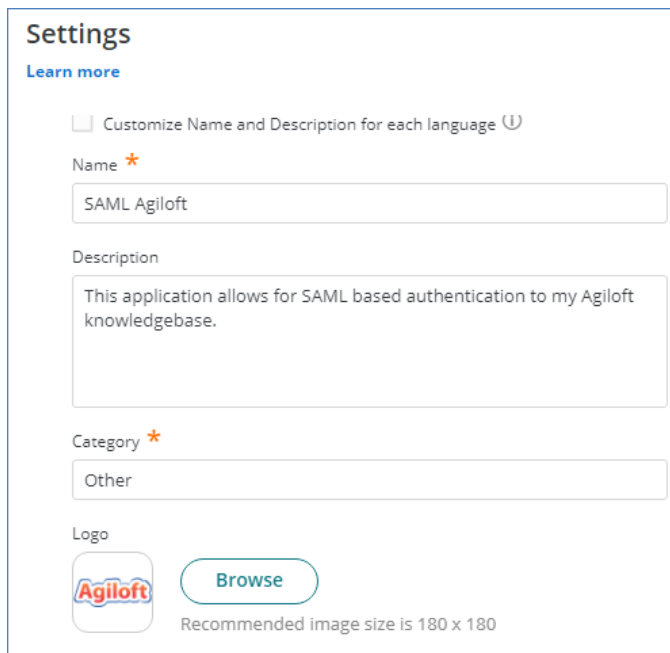
1. Log in to the CyberArk Identity Admin Portal using your administrator credentials; for example, <https://example0111.my.idaptive.app>.
2. Click Web Apps in the left pane, then click Add Web Apps.



Add Web Apps button

3. Go to the Custom tab, scroll down, and click Add SAML. Confirm your selection.
4. Close the dialog. You are automatically directed to the Application Settings window for the SAML application.
5. Click Settings.

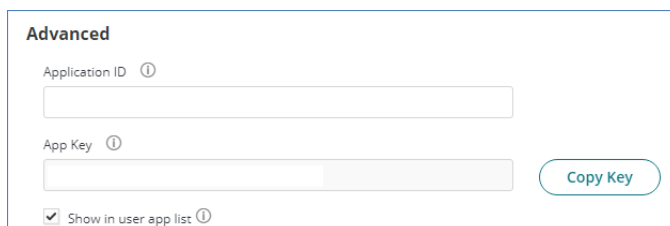
- a. Add a Name, Description, Category and Logo.



The screenshot shows the 'Settings' page in Idaptive. At the top, there's a 'Learn more' link. Below it is a checkbox labeled 'Customize Name and Description for each language' with a help icon. The 'Name' field is marked with an asterisk and contains 'SAML Agiloft'. The 'Description' field contains 'This application allows for SAML based authentication to my Agiloft knowledgebase.' The 'Category' field is marked with an asterisk and contains 'Other'. The 'Logo' section shows a preview of the Agiloft logo and a 'Browse' button. Below the logo preview, it says 'Recommended image size is 180 x 180'.

Settings page showing the information fields in Idaptive

- b. Scroll down to the Advanced section and select the "Show in user app list" checkbox. This enables you to log in directly from the Idaptive App list.



The screenshot shows the 'Advanced' section in Idaptive. It contains three input fields: 'Application ID', 'App Key', and 'Show in user app list'. The 'Application ID' and 'App Key' fields are empty. The 'App Key' field has a 'Copy Key' button next to it. The 'Show in user app list' checkbox is checked. Each field has a help icon.

Advanced options

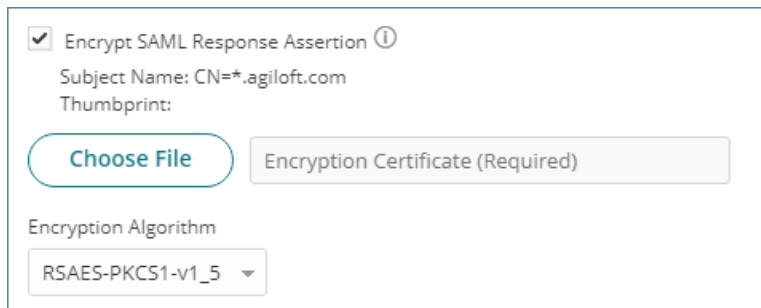
- c. Click Save.

## Establish the SAML Connection to Agiloft

With these configurations in place, you can establish the connection.

1. In Idaptive, click Trust.
2. Now, if possible, bring up the Agiloft window next to the Trust configuration in Idaptive, so you can go between them to fill in the values. In Agiloft, return to the Service Provider Details tab, if it isn't already open.
3. Complete the Idaptive fields as follows:
  - a. At the bottom, under Service Provider Configuration, click Choose File. Navigate to the metadata XML file you downloaded, select it, and click OK.
  - b. In the Service Provider Configuration section, select Manual Configuration.
  - c. In the Issuer field, paste the value from the Agiloft (SP) Entity ID field in Agiloft.

- d. In the Assertion Consumer Service URL field, paste the value from the SAML V2 Assertion Consumer Service (ACS) Endpoint field in Agiloft.
- e. For Sign Response or Assertion?, select Both.
- f. Select Encrypt Assertion.
- g. If Subject Name and Thumbprint don't have a value, click Browse and navigate to the X.509 certificate you downloaded earlier. When the file is uploaded, encryption assertion details appear.



The screenshot shows a form titled "Encryption Assertion Details". It contains a checked checkbox labeled "Encrypt SAML Response Assertion" with an information icon. Below this, there are fields for "Subject Name: CN=\*.agiloft.com" and "Thumbprint:". A "Choose File" button is next to a disabled "Encryption Certificate (Required)" button. At the bottom, there is a label "Encryption Algorithm" and a dropdown menu currently showing "RSAES-PKCS1-v1\_5".

Encryption Assertion Details

4. In Agiloft, go to the Identity Provider Details tab. In Idaptive, go to the Identify Provider Configuration section.
  - a. Select Manual Configuration and expand the IdP Entity ID and Signing Certificate drop-downs.
  - b. For IdP Entity ID/Issuer, copy the URL from Idaptive into the equivalent field in Agiloft.
  - c. For IdP Provided X.509 certificate contents, click Download under Signing Certificate and save the file to an accessible location. Open the .cer file in a text editor, copy the contents, and paste them into Agiloft.
  - d. For IdP Login URL, copy the Single Sign On URL field from Idaptive into Agiloft.
  - e. For IdP Logout URL, copy the Single Logout URL field from Idaptive into Agiloft.
5. In Agiloft, click Finish. In Idaptive, click Save.

At this point, the initial SAML configuration is complete. Next, create Idaptive and Agiloft users.

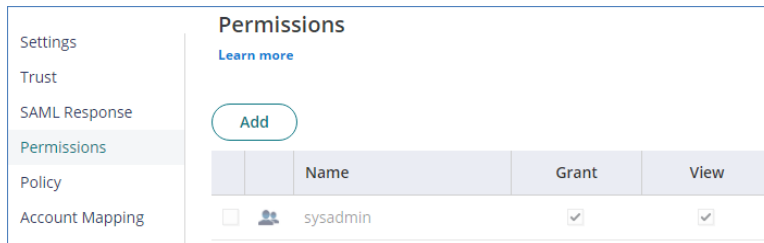
## Assign Idaptive Users to the Application

---

If you do not already have a list of users and roles in your organization's Idaptive account, begin by defining the roles you need. Then, in Idaptive, add, invite or import them, and then set up their roles. For more information on these processes, see the [CyberArk Documentation](#).

1. Once the roles and users have been created, open Idaptive, select Web Apps, and open the SAML application.

2. Click Permissions and then click Add.



Name	Grant	View
sysadmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>


3. Select the roles and users you want to allow to access the Agiloft application via Idaptive.
4. Click Save.

At this point, the users who were assigned roles are now be able to access the Agiloft knowledgebase using this URL syntax: `https://[agiloftserver]/gui2/samlssologin.jsp?project=KB_NAME`

### Example

`https://server.agiloft.com/gui2/samlssologin.jsp?project=Idaptive`

In addition, a user can login to the Agiloft GUI from the Idaptive apps dashboard in the User Portal by clicking on the Agiloft SAML application icon.

 For more information on creating the Group and Team mappings in Agiloft, see [Configure Agiloft](#).

## Dynamic Group and Team Mapping

A standard configuration assigns a fixed Group and Team mapping to any new users created via Agiloft SAML SSO. However, it is also possible to allocate users to different Groups or Teams from within Idaptive.

To set up dynamic Group and Team mapping:

1. Create all of the Groups and Teams in Agiloft. If a new Group or Team is added to the Active Directory or repository used by Idaptive, then they should also be added to Agiloft.
2. In the CyberArk Identity Admin Portal:
  - a. Open the Web App you created for accessing Agiloft.
  - b. Click SAML Response to open the Attributes and Custom Logic screen.
  - c. Add the following line to the SAML Script Editor, which specifies that the Groups associated with a user are sent in an attribute called "Group" in the SAML authentication response:

```
setAttributeArray('Groups', LoginUser.GetGroupAttributeValues  
("userprincipalname"));
```

There are several alternate ways of sending the group information as SAML attributes in the SAML response. For example:

```
setAttributeArray('Groups', LoginUser.EffectiveGroupNames);
```

Or

```
setAttributeArray('Groups', LoginUser.GroupNames);
```

**Custom Logic**

Use the Script Editor below if you require more complex logic for attribute mappings for your SAML response. Press Ctrl+Space for script assistance.

[Reset Script](#) [Preview SAML Response](#)

**SAML Script Editor**

```
1 setAttributeArray('Groups', LoginUser.GetGroupAttributeValues("userprincipalname"));
```

Custom Logic example

- d. Do the same for the Team attributes, if needed.
  - e. Click Save. You can use the Test button to verify the SSO token values that will be sent at runtime to Agiloft.
3. In Agiloft:
- a. Log in as an admin user and go to **Setup > Access > Configure SAML**.
  - b. Go to the User Group Mapping tab.
  - c. Select Map the group(s) from this SAML attribute, and fill in the group name with the name of the SAML attribute name you specified in step 2c above.

☒ Map the group(s) from this SAML Attribute

Groups

Map the groups from this SAML Attribute

- d. Choose whether to update the user groups on subsequent logins.
- e. If needed, open the User Team Mapping tab and select the Set the User's teams from the IdP checkbox, and name the SAML Team attributes, similar to step 3c.
- f. Select the Service Provider Details tab and click Finish.

## Dynamic Field Mapping

It is also possible to define the user fields dynamically, using similar steps to the dynamic group and team mapping. The examples below show you how to map a user's First Name and Last Name between Agiloft and Idaptive. Other field attributes are done in the same way.

1. In Idaptive:
  - a. Open the Web App you created for accessing Agiloft.
  - b. Click SAML Response to open the Custom Logic screen.

- c. See the example below:

**Custom Logic**  
Use the Script Editor below if you require more complex logic for attribute mappings for your SAML response. Press Ctrl+Space for script assistance.

Reset Script

Preview SAML Response

**SAML Script Editor**

```
1 setAttributeArray('Groups', LoginUser.GetGroupAttributeValues("userprincipalname"));
2 /* Custom Additions */
3 setAttribute('FName', LoginUser.FirstName);
4 setAttribute('LName', LoginUser.LastName);
5 /* Attribute from Active Directory keys */
6 setAttribute('DEPT', LoginUser.Get('department'));
7 setAttribute('Phone', LoginUser.Get('phone'));
```

Custom Logic dynamic fields example

- d. In lines 3-4, the FName and LName attributes are used to send the user's First Name and Last Name to Agiloft.
- e. Lines 6-7 show some examples of additional values for Department and Phone Number, which can be mapped from an Active Directory or LDAP repository, which the Idaptive account is using to store user values. These examples assume that Active Directory or LDAP values of DEPT and PHONE exist.
2. In Agiloft:
- Log in as an admin user and go to **Setup > Access > Configure SAML**.
  - Go to the User Field(s) Mapping tab.
  - Enter the values that correspond to the SAML attributes in Idaptive.

Field names of Employees table in Agiloft	Mapping SAML attribute names
Title	<input type="text"/>
First Name	<input type="text" value="FName"/>
Last Name	<input type="text" value="LName"/>
Email	<input type="text"/>
Direct Phone	<input type="text" value="PHONE"/>
Cell Phone	<input type="text"/>
Company	<input type="text"/>
Company Phone	<input type="text"/>
Employment Status	<input type="text"/>
Department	<input type="text" value="DEPT"/>

SAML attribute mapping

- d. Select the Service Provider Details tab and click Finish to save the settings.

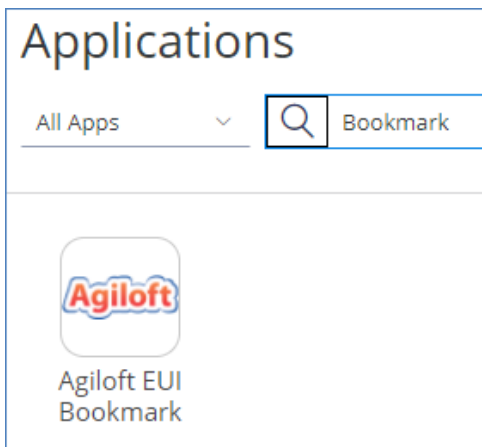
# Custom SSO URLs

---

By default, the Agiloft SSO login through the App List logs in as if using this URL structure with no parameters:  
`https://[agiloftserver]/gui2/samlssologin.jsp?project=KB_NAME`

If you need customized URLs with parameters, you can construct them based on [Hyperlink Syntax and Examples](#) and then set them up as Web Apps in Idaptive:

1. Select Web Apps and click Add Web Apps.
2. Select Custom Tab and click Add a Bookmark.
3. Confirm and close the Add Web Apps dialogue.
4. Open the new Bookmark app.
5. Set the URL to your custom SSO URL. For example, if you wanted all users accessing the App to be sent to the End User Interface, you might use a URL like this with your server and KB name: `https://[agiloftserver]/gui2/samlssologin.jsp?project=KB_NAME&State=Main&euiurl=/eui2template/main.php`
6. Click Save.
7. In the User Portal, test logging in from the App List.



Agiloft EUI Bookmark shown as example  
app

# Force SSO Login

---

Finally, to make sure users log in with SSO after the transition, manually set new passwords for users who should use SSO instead. To do so:

1. Go to the People table and select every user who should use SSO from this point on.





Don't select every single user in your system. It's best to leave at least one administrator unchanged, if not the whole admin team, in case you encounter SSO issues in the future that prevent users from logging in with SSO.

2. Click Mass Edit, or Edit Fields, in the action bar.
3. Select the Password field, then click Next to proceed to the Update tab.
4. Select the formula option and enter `random_password(15)`. This will call the `random_password(15)` function to randomly generate a new 15-character password for everyone you selected.
5. Click Next, then Finish.
6. Now, go to Setup Employees and go to the Layout tab. If you will use SSO for every user in the system, including external users, go to Setup People instead.
7. Remove the Password field from the layout. This prevents users from manually setting a new password and potentially using it to log in instead of SSO.

Next, go to **Setup > System > Manage Global Variables** and check the Customized Variables tab for the Hotlink Type variable. If it has been customized, edit it and reset it to the default value of STANDARD.

You might also notice a setting in the People table called SSO Authentication Method. This field is set automatically by the system when you enable SSO, and should not be modified.