madcap software

USER GUIDE

MADCAP FLARE ONLINE

License Management Guide

MadCap Software
1660 17th Street, Suite 201
Denver, Colorado 80202
858-320-0387
www.madcapsoftware.com

THIS PDF WAS CREATED USING MADCAP FLARE.

CONTENTS

CHAPTER 7

CHAPTER 8

CHAPTER 9

CHAPTER 10

APPENDIX

CHAPTER 3

Single Sign-On

MadCap Flare Online supports single sign-on (SSO), which is an authentication method that lets users log in to multiple software systems with just one set of credentials. This is particularly important for large enterprise organizations.

EXAMPLE You might set up MadCap Flare Online to use SSO with Microsoft Azure Active Directory, the same identity provider (IdP) that your company uses to log employees into Windows and various applications. Since your users are already part of that IdP, they can rely on the same credentials to log in to Flare Online.

NOTE SSO is an optional feature. If you do not wish to use SSO for your license, users can still gain access to Flare Online in the same way that's always been available, with a unique Flare Online password.

This chapter discusses the following:

General Information for Single Sign-On

There are various pieces of general information you should know if you plan to use this feature.

Benefits of Using Single Sign-On

Here are some of the main benefits of single sign-on (SSO).

- Fewer login credentials for users to remember and maintain
- Stronger authentication security
- Simplified admin tasks (identity provider manages users and access, instead of a manual process)
- Faster onboarding process for multiple users of a private site
- Easier to prevent access to the license when users leave the company

Supported Identity Providers for Single Sign-On

There are many identity providers (IdPs) on the market, which might use one or more protocols for authentication. Here are a few of the major IdPs that you can integrate with Flare Online, since they support the Security Assertion Markup Language (SAML) protocol. This is not an exhaustive list. As long as your IdP supports SAML 2.0, you can use it with your Flare Online license.

- AuthO
- Azure Active Directory
- Okta Identity Management
- More…

Claim Attributes and Formats for Single Sign-On

Depending on your identity provider (IdP), you (or your IT department) might need to use the following claim attributes and formats when configuring single sign-on (SSO) with Flare Online. See "Process for Single Sign-On" on page 28.

Claim Attributes

- email

  http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress or *User.email* or *mail*

- first name

  http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname or *first_name* or *User.FirstName* or *givenName*

- last name

  http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname or *last_name* or *User.LastName* or *sn*

- department

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

Formatting for Attributes

Other claim attributes are not yet in use. However, all attributes should be formatted as follows:

```
<AttributeStatement><Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"><AttributeValue>
Value Text<AttributeValue></AttributeStatement>
```

Onboarding Users With Single Sign-On

If you enable single sign-on (SSO) on your license, you have multiple options when it comes to onboarding new users.

Onboarding Viewers to Private Sites With SSO

If you have a private site in Flare Online and want to onboard users with the viewer status so they can simply view your output, you have a couple of options when SSO is enabled on the license.

- Option 1 If the users are already added to your identity provider (IdP) through your IT department, you can simply provide all of those users with a link to the private output. This automatically creates a viewer seat type for each person who is not already part of the Flare Online license, and it associates them with the default team(s) you choose. See " " on page 39.
- Option 2 You can use the traditional invitation method via the wizard in Flare Online. This can require more effort because you need to enter the information for each user or link to a CSV file that you've prepared in advance. When users click the link in the email they receive, they can log in using SSO.

Onboarding Authors or Subject Matter Experts With SSO

When onboarding authors or subject matter experts (SMEs) to a Flare Online license enabled with SSO, you also have a couple of options.

- Option 1 If you have private output and the users are already added to the IdP, you can provide them with a link to that output, just as you would for viewers (see " " on page 39). However, since this automatically creates a viewer (rather than author or SME) seat type for each person, you would then need to manually change the status to either author or SME for each user in Flare Online after the fact. This can be done by opening the Users page and clicking the Seat Type for each user and switching it to another. After this, you could also set permissions for users who are changed to authors.
- Option 2 You can use the invite user wizard in Flare Online, just as you can for viewers. When users click the link in the email they receive, they can log in using SSO. The advantage of using this option is that you can set permissions for authors at the same time that you invite them to the license.

The Login Experience for Single Sign-On

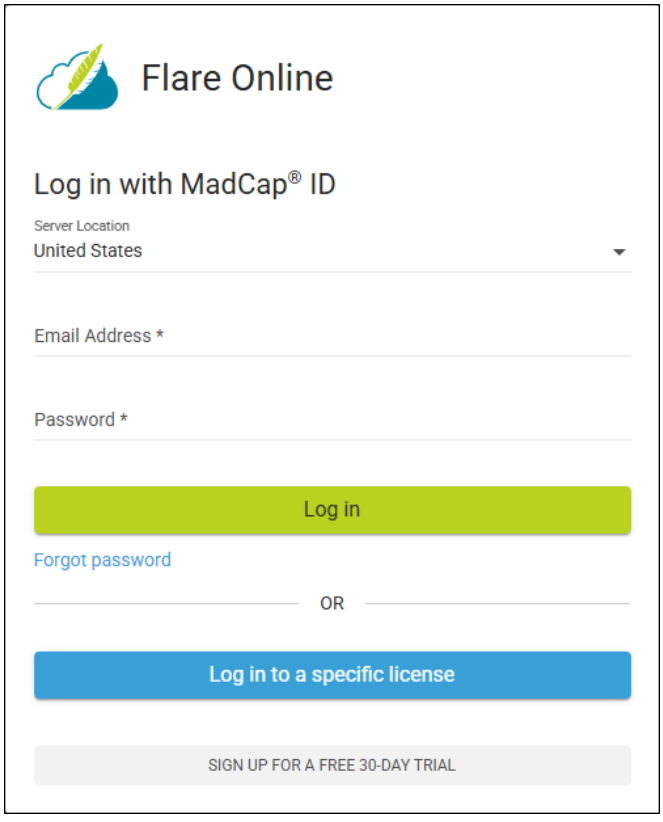
The single sign-on (SSO) login experience depends on different factors, such as whether it's the user's first time logging in, if there are multiple licenses, how the identity provider (IdP) is set up, etc.

First-Time SSO Login

The first time users try to access Flare Online, they might experience one of two scenarios.

Scenario 1

The following login window displays if the user tries *to access the Flare Online portal in general, as opposed to a specific license*.



EXAMPLE The user goes to https://madcapflare.com instead of https://**fictionsoftinc**.madcapflare.com), where "fictionsoftinc" is the vanity for the license.

In this case, the user needs to have an email and password already associated with Flare Online to log in. That's because it's possible for a person to be part of multiple licenses, some enabled with SSO and some not, and Flare Online doesn't know which you want to access.

NOTE The login window above would also display if the license is not yet enabled for SSO.

NOTE If you do not already have a Flare Online password, you can click **Forgot password** to set one up.

Scenario 2

A different login window displays if the user tries *to access a specific Flare Online license* that is enabled for SSO. It directs the user to log in with a third party.

EXAMPLE The user goes to:

```
https://fictionsoftinc.madcapflare.com
```

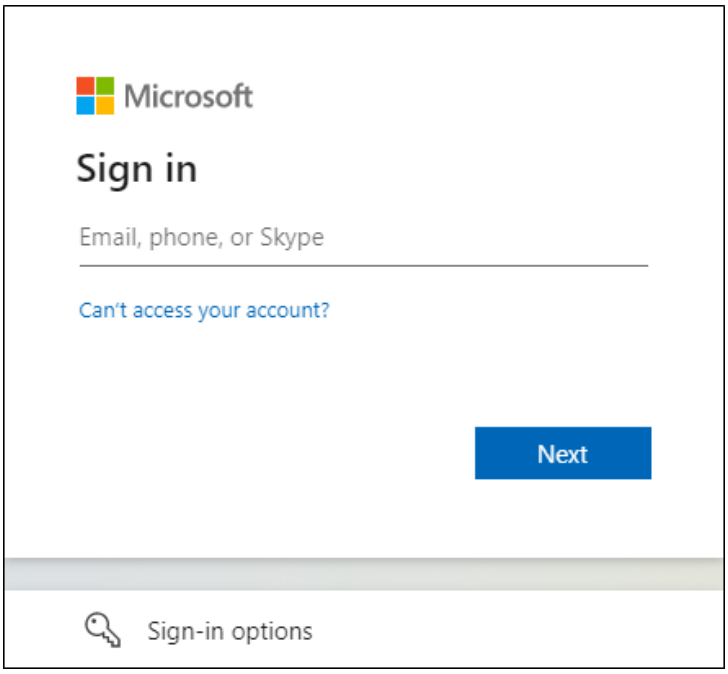
The vanity for the license is "fictionsoftinc."

NOTE The button label "Log in with third party" is the default text, but you can customize it to say something else (e.g., Microsoft Login, Okta SSO, AuthO Access).

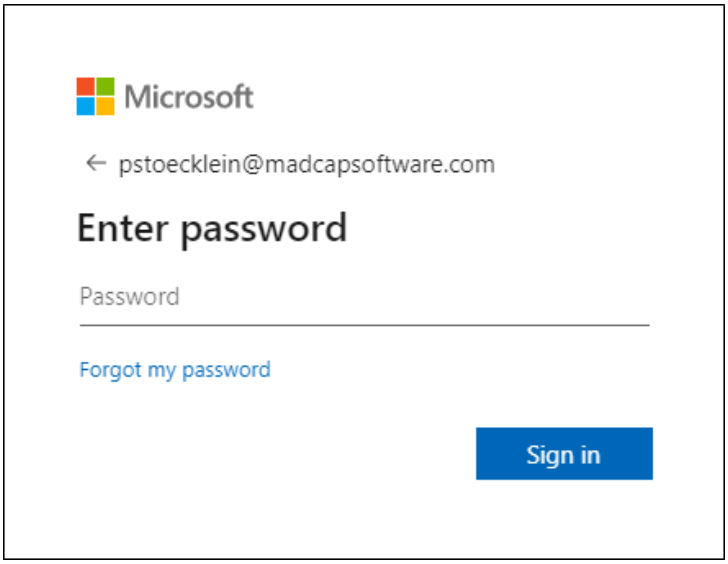
After you click the button to log in, additional windows open so you can enter credentials of some kind. The type of credentials depends on how your IT department sets up the IdP (e.g., password, verification code sent to email, two-factor authentication via smart phone).

☆ EXAMPLE — Password

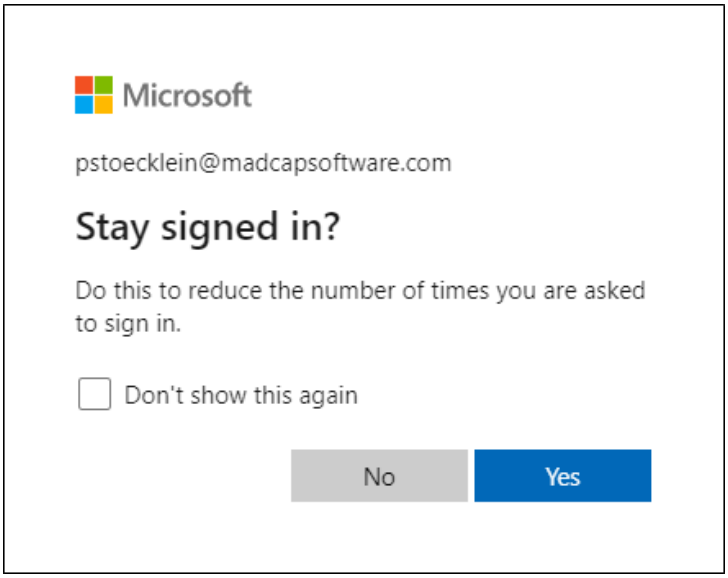
In this example, Microsoft Azure is the IdP, and it has been set up to first ask for your email, with the possibility to select other sign-in options (e.g., security key).



After this, Microsoft asks for your IdP password (i.e., the password you use to log in to Windows when you start your computer).



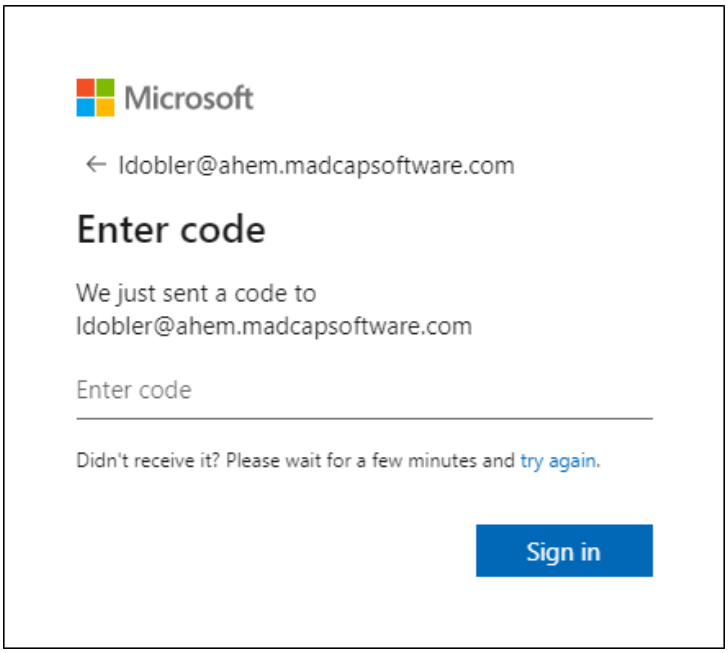
Then, it might ask if you want to stay signed in.



After this window, you are logged in to Flare Online.

EXAMPLE — Verification Code

This example is the same as the previous one, except that the IdP is set up to ask for a verification code instead of a password.



In this case, you receive an email, where the code is found.

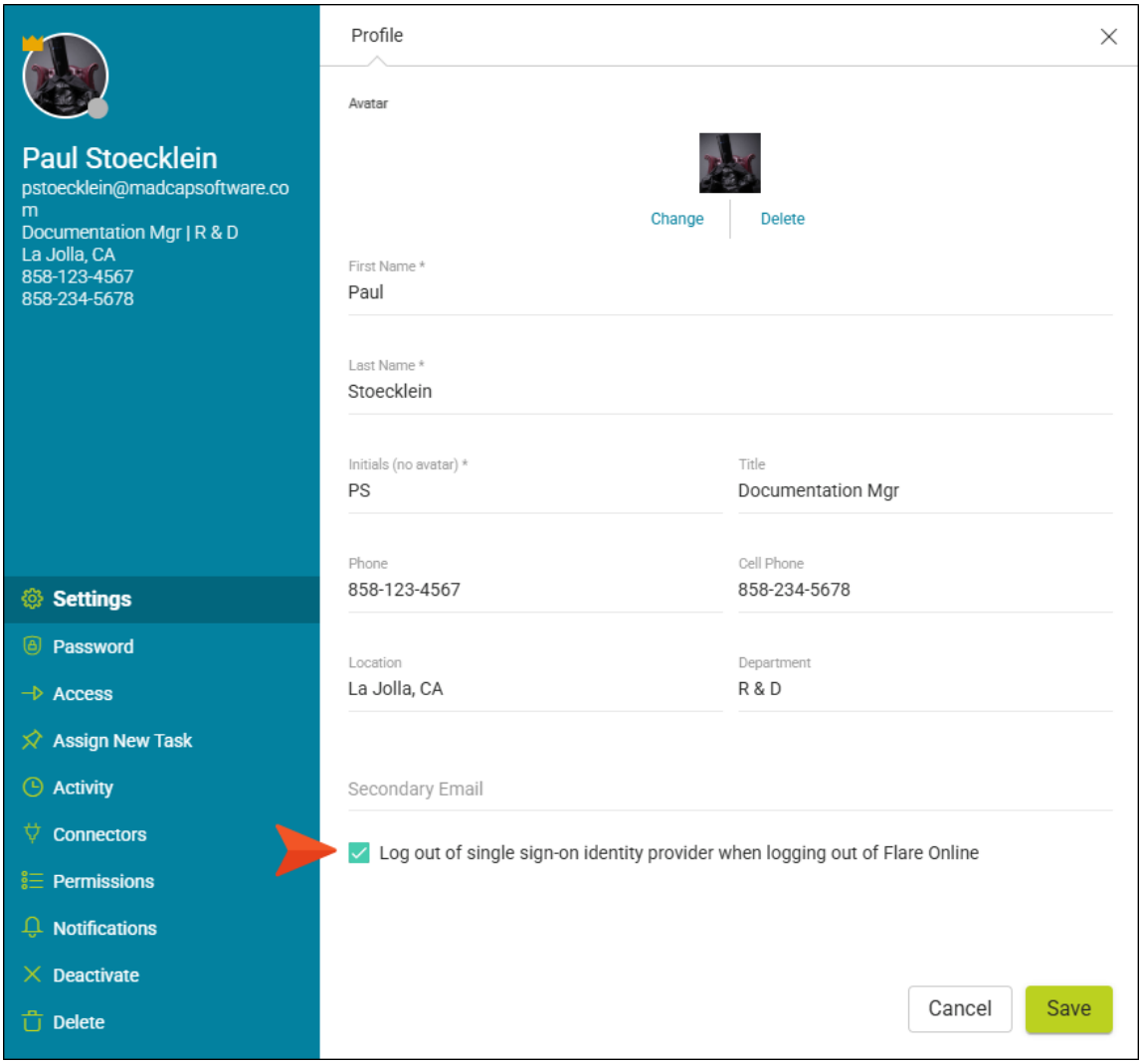
After pasting the code into the field and clicking **Sign in**, you are logged in to Flare Online.

After the First Login

For a license that is enabled with SSO, you need to enter credentials only the first time you log in. If you log out and then try to log back in, you will see the SSO login window once more.

When you click the button to log in again, you do not need to enter the IdP credentials a second time. Instead, you are simply logged in with them. This is different than a license that is not enabled for SSO, where you must enter your unique Flare Online password each time you log in.

NOTE The exception to this is if you have enabled this option in your user settings in Flare Online:



In that case, each time you log out of Flare Online, you are also logged out of your IdP and must re-enter your credentials whenever you log back in to Flare Online.

NOTE If you log out through the Flare Desktop interface (as opposed to a browser) and then log back in, it's possible you will need to enter the credentials once again.

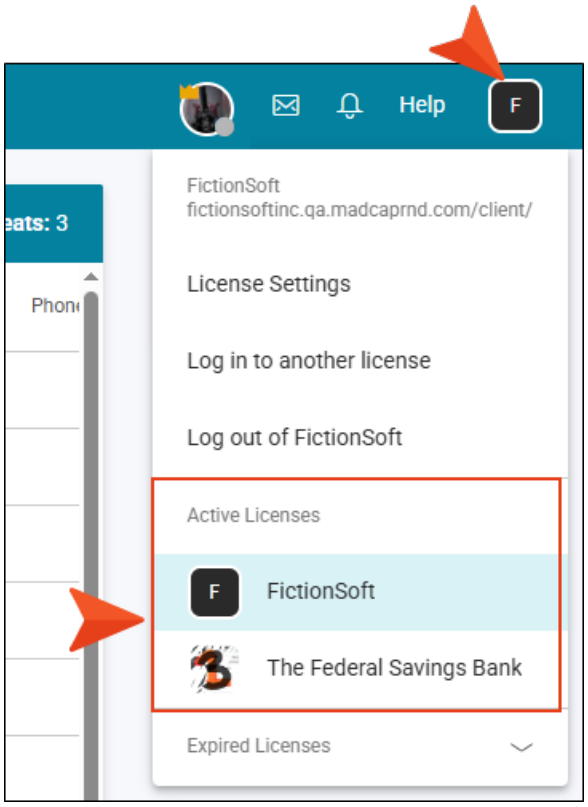
Multiple Licenses

Some Flare Online users might be part of multiple Flare Online licenses. Not only that, but some of those licenses might be enabled for SSO and some might not. Therefore, when logging in, you might encounter a license hub, where you select the license that you want to log in to.

In addition, there are multiple methods for switching to a different license.

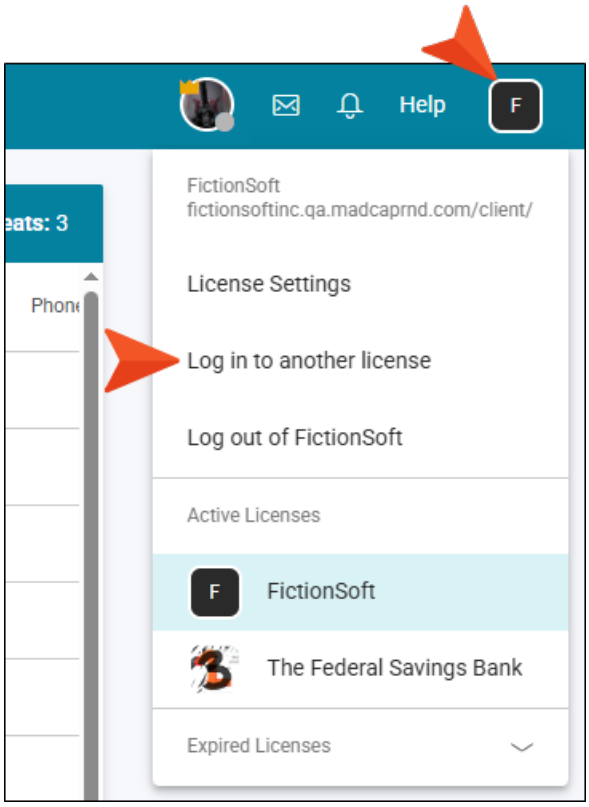
Method 1: Select License in Drop-Down

Once a user on multiple licenses is logged in to Flare Online, that person can click the license avatar (or initial) in the upper-right of Flare Online and select a different license.



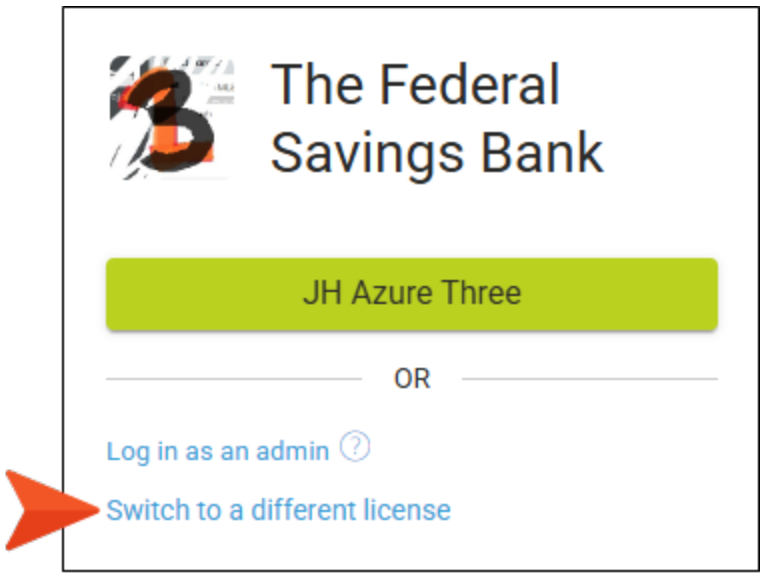
Method 2: Option in License Drop-Down

In the license drop-down in Flare Online, there is also an option named "Log in to another license."


Help
F
FictionSoft
fictionsoftinc.qa.madcaprnd.com/client/
License Settings
Log in to another license
Log out of FictionSoft
Active Licenses
F
FictionSoft
The Federal Savings Bank
Expired Licenses

Method 3: SSO Login Window

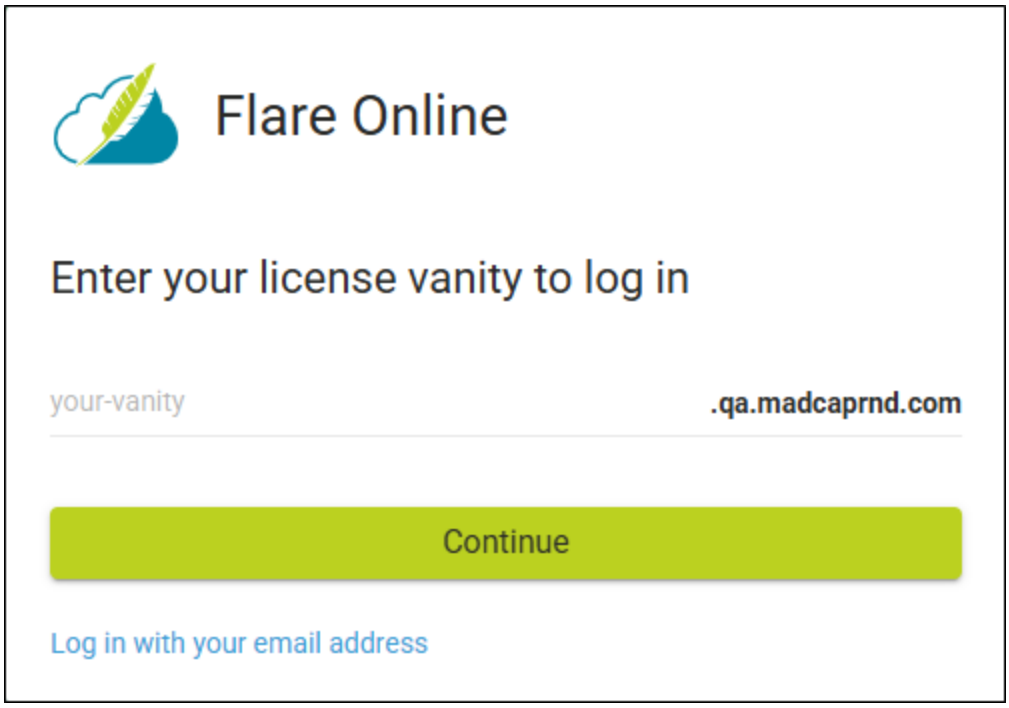
In the SSO login window, you will also see an option named "Switch to a different license."



Logging In Using Methods 2 or 3

If you use Method 2 or 3, the license hub opens, displaying all of your Flare Online licenses. You can then select the license you want to switch to.

Alternatively, in the main Flare Online login window you can click **Log in to a specific license**. This opens a different window where you can type the exact vanity of the license you want to log in to.



What Happens Next?

Regardless of the method you use, what happens next depends on whether the license is enabled for SSO.

If you select another license that *is enabled for SSO*, you can click the SSO login button to quickly sign in and load that license. Or the license might simply be loaded if you had previously logged in to it.

If you select another license that *is not enabled for SSO*, you must enter the email and Flare Online password to log in.

Log In Through Private Site

If your license is set up to create viewer users on demand, you can provide brand new users with a URL link to that output. That can be done in any number of ways (e.g., send an email with the link, put the link on an Intranet site, create a small online page with a hyperlinked image that links to the output).

After new users click the link, they see a page to log in.

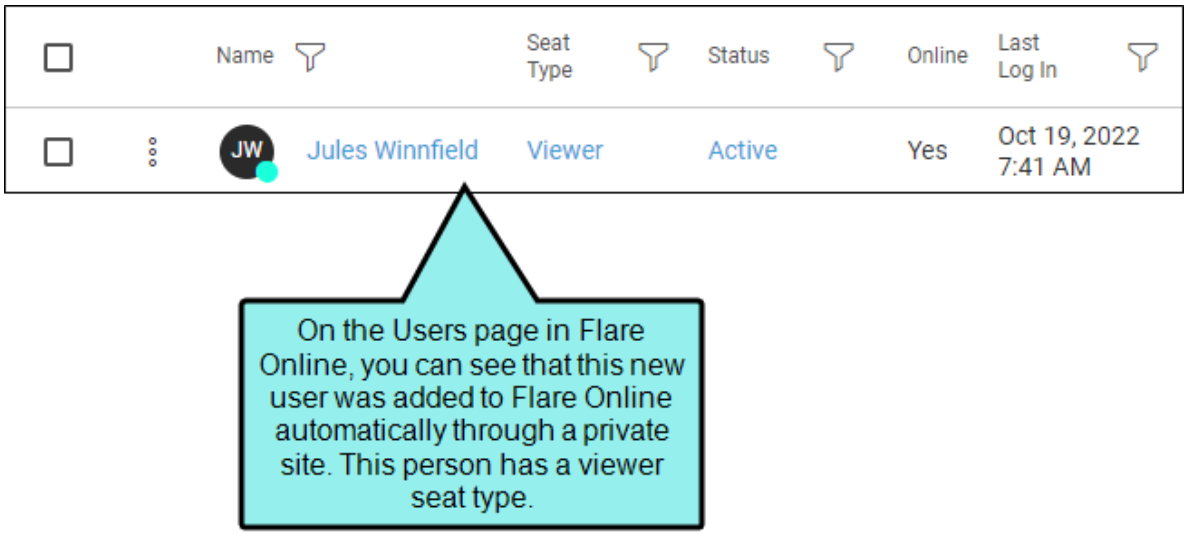
> NOTE You can change the look of the button by using a theme.

> NOTE The avatar and name above the button are coming from your license settings.

Clicking this login button takes them through the same process described above for first time logins. Once the person enters the initial credentials, a message displays.

In the email, the new user clicks the link to confirm the account.

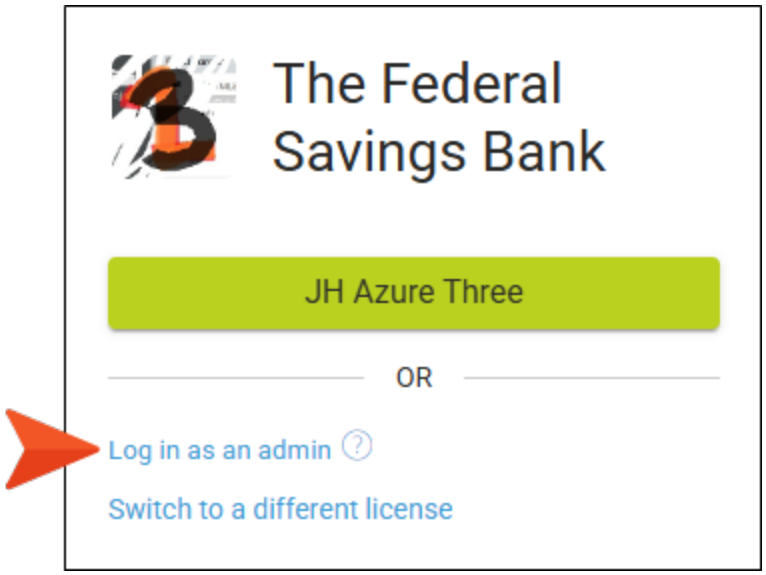
The output opens, and the new user is now automatically added to the license as a viewer.



> NOTE Keep in mind that these new users must have already been added to the application in your company's IdP in order for this process to work.

Log In as an Admin

In an SSO login window, you will see an option named "Log in as an admin."



This allows a person to enter an email address and password to log in. However, even if you are a Flare Online administrator, it doesn't mean you need to use this option. In most cases, you can use the initial button to log in via SSO (e.g., "Log in with third party"). You'll be logged in and will still have all of your administration permissions once you're in Flare Online.

The "Log in as an admin" option is really a back door in case there is an administrator who needs it.

☆ EXAMPLE A person might have been initially invited to an SSO-enabled Flare Online license by clicking on the link for a private site. This adds the person to the Flare Online license as a viewer, as opposed to an author or subject matter expert (SME). But because the user was automatically added to the license in this manner, that person never set up a Flare Online password, since the license was using SSO.

Later, somebody else (an administrator) might have then changed that first person to an author seat (instead of a viewer) and granted the individual administration permissions.

Over time, let's say all other administrators have left the license, leaving this one person. Since a Flare Online license always needs to have at least one administrator, and this particular person never set up a Flare Online password when onboarding, the back door option becomes necessary.

Frequently Asked Questions for Single Sign-On

Here are some questions that you might be wondering about when it comes to single sign-on (SSO).

How do I migrate existing Flare Online users to SSO?

You need to make sure those users are associated with your application on the IdP. Your IT department might have already done this, so there wouldn't be anything else you need to do. Those users will simply be directed to use the IdP login credentials when they sign in to Flare Online.

Can I create viewer users on demand for people outside my company?

New viewer users must be listed in your IdP, associated with your application, when they onboard themselves by trying to open the private output link. So this on demand feature via private output is probably limited to people in your company, since they're the ones who will be added to the IdP by your IT department.

What if a user already has a unique Flare Online password and you then decide to enable SSO on your license?

The user simply no longer needs to use the Flare Online password when logging on to an SSO-enabled license. If the user is part of multiple licenses, some of which aren't using SSO, the user will still use the Flare Online password to log in to those licenses. Also, if the user is directed to the Flare Online portal in general (instead of a specific license), it is still necessary to use the Flare Online password to see the license hub and choose the correct one.

Is it possible to "gate" new users on the Flare Online license through SSO (i.e., admit them to the license in separate groups so they have different access)?

Yes and no.

Currently, it is not possible to do this *automatically* when using the private output link option. When you set up the license to create viewer users on demand, you can select one or more teams to associate with those new users. However, you cannot direct some of the users to be on *this* team (which is, for example, associated with Private Output A), while other users should be on *that* team (which is, for example, associated with Private Output B). All users will be associated with any and all teams that you specify in your license settings, and therefore, they will all initially have access to any private outputs associated with those teams.

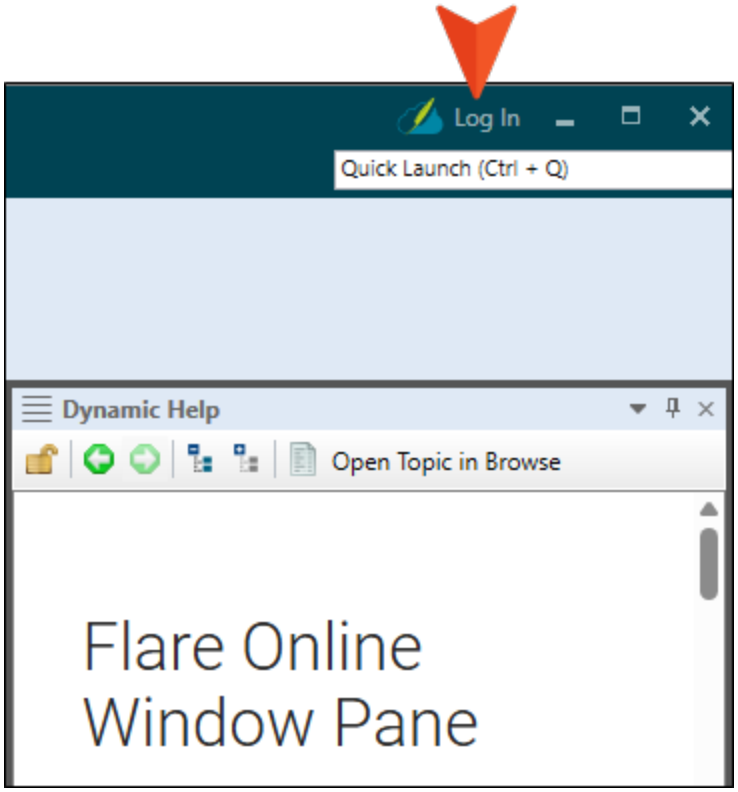
However, you can onboard users *manually* to an SSO-enabled license. You can add new users via the private output method, and once they are part of the license, an administrator can change a

user's seat type, team(s), and give specific permissions to those who have an author seat type. Also, if you use the original method of inviting users via the wizard, you can invite one group of users who will have the same seat type, team(s), permissions, etc. Then invite another group with a different seat type, team(s), etc.

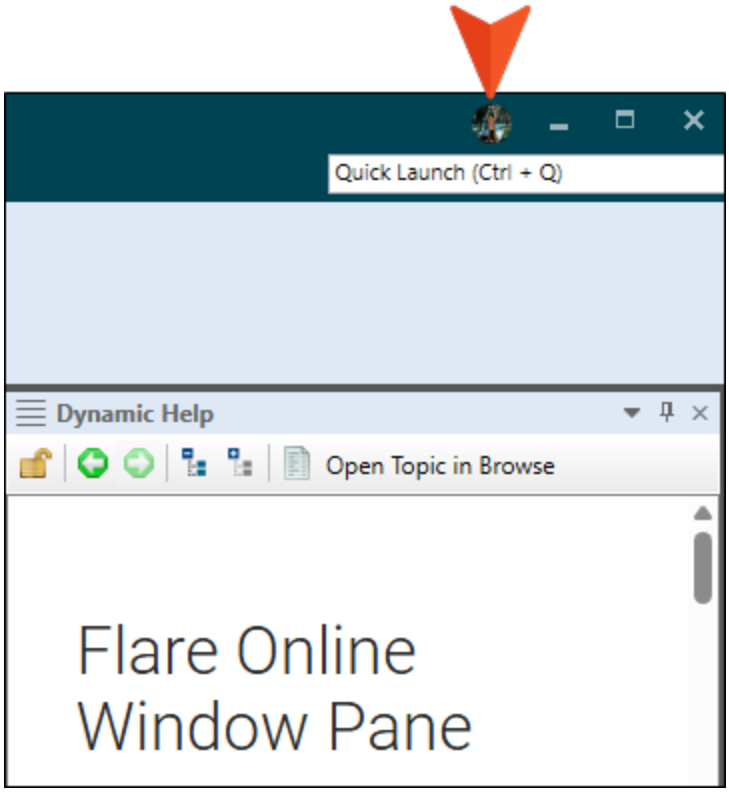
What happens on the Flare Desktop side for SSO?

MadCap Flare Desktop 2022 r2 (and later) is integrated with SSO, so if a user logs in to Flare Online from the Flare Desktop interface, the same process occurs.

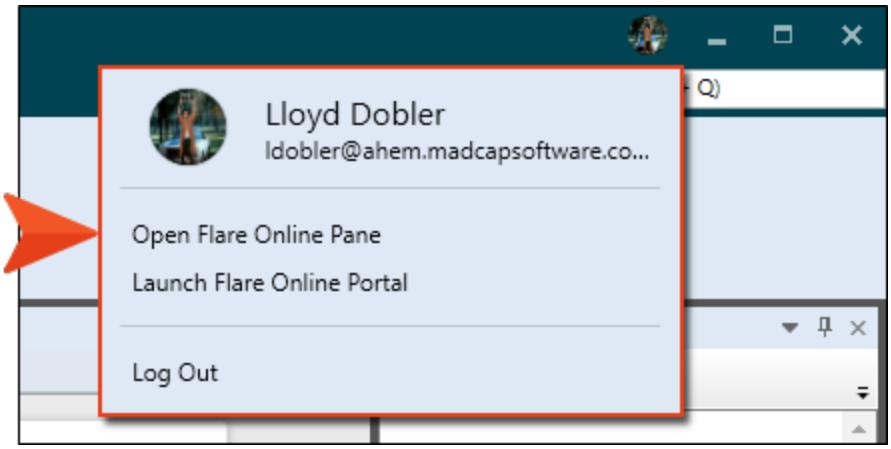
Also, there is a login option in the upper-right of Flare Desktop, which serves the same purpose as the login option in the Flare Online window pane.



Clicking the option opens a browser-based window to log in to Flare Online from Flare Desktop. Once logged in, the Log In button is replaced with your avatar (or your initials if you have not yet selected an avatar image).



You can click the avatar to open a drop-down menu. From here you can open the Flare Online window pane, launch the Flare Online portal in a browser, or log out.



For more information, see the Flare Desktop Help system.

> NOTE Older versions of Flare Desktop work the same as before with Flare Online, where individuals log in with a unique Flare Online password.

What happens if a Flare Online user is removed from the identity provider?

The user will no longer be able to log in to your Flare Online license. This can be a big benefit, because you don't need to worry about remembering to remove users' access from the Flare Online license if they leave the company. However, users who are removed from the identity provider (IdP) will still technically exist on your license until you remove them. So if you want to "clean up" the users on the license and free up a seat, you need to remove that person manually from Flare Online.

Process for Single Sign-On

Certain tasks must be completed in order when using this feature.

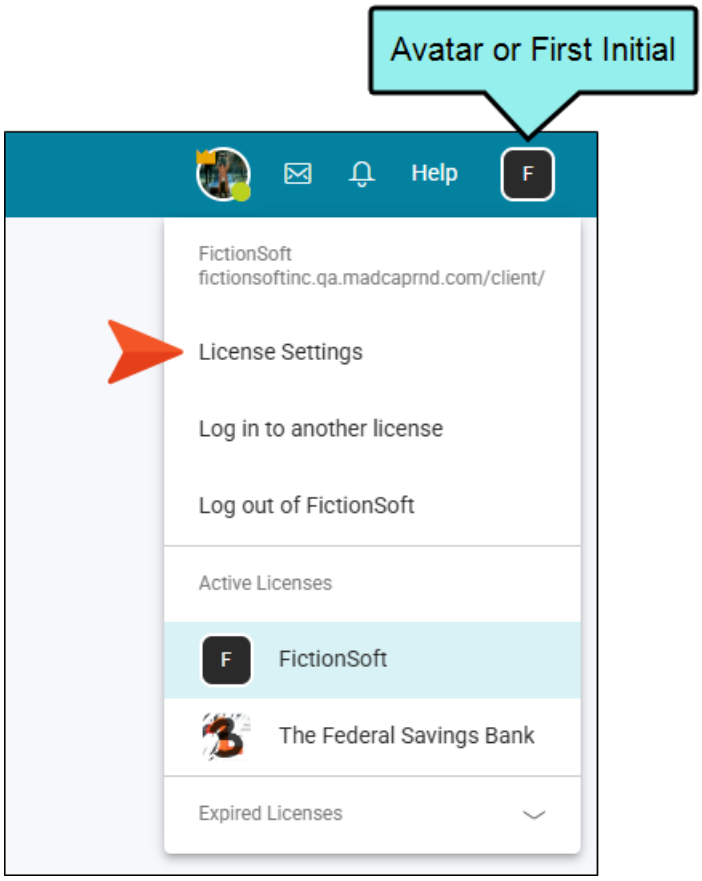
Providing and Obtaining Single Sign-On Information

Based on your Flare Online license settings, you need to provide some sign-on (SSO) information to your IT department, or whoever is in charge of your company's identity provider (IdP) settings. In turn, your IT department should then provide you with some SSO details, which you will then plug into Flare Online.

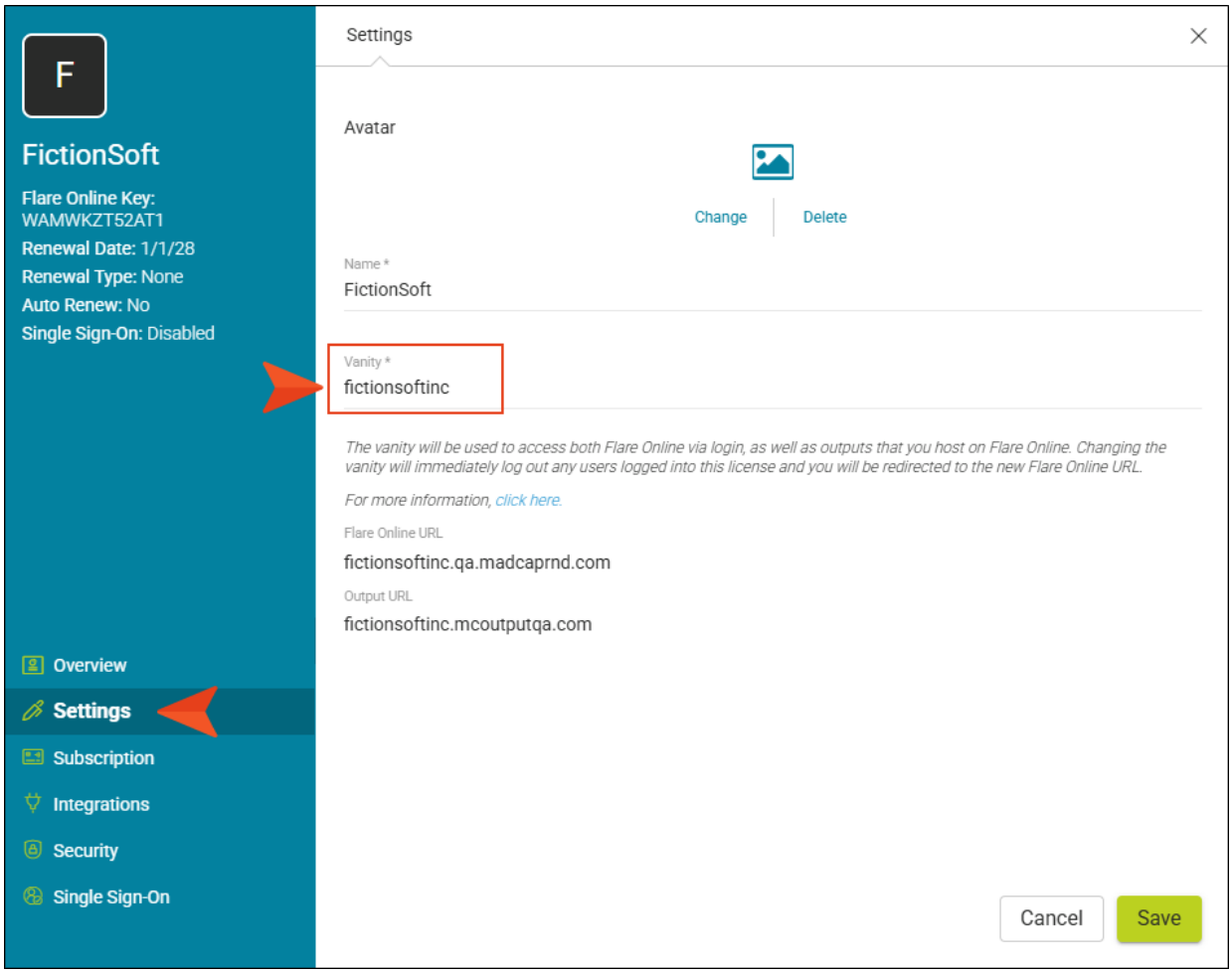
> NOTE Also, depending on your IdP, you (or your IT department) might need to use certain claim attributes and formats when configuring SSO with Flare Online. See "Claim Attributes and Formats for Single Sign-On" on page 7.

How to Provide and Obtain SSO Information

1. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select License Settings.



2. On the left side of the dialog, click **Settings**, and make note of your **Vanity**.



3. Provide your IT department with the following information, substituting the bracket text with your vanity (or host mapped domain in the final case). Ask IT to enter this information into the IdP and then in turn provide you with the appropriate information mentioned in the next set of steps (see "SAML Authentication Settings" on page 37).

   The IT department also needs to add an application in the IdP for your purposes, associating users with that application.

   > NOTE Use the following URLs *with your vanity*, even if you are mapping to a host domain (via CNAME) on the Sites page. The only case where you would include the *host mapped domain* is the SAML Endpoint URL for CNAME Sites.

   > NOTE Keep in mind that different terminology might be used by your company's IdP.

   - Login URL

     ```
     https://[vanity].madcapflare.com
     ```

     > EXAMPLE If your vanity is fictionsoftinc, the URL would be:
     >
     > ```
     > https://fictionsoftinc.madcapflare.com
     > ```

- SAML Endpoint for Portal

  United States server:

  ```
  https://[vanity].api.madcapcentral.com/api/users/SamlLoginSucceeded
  ```

  > ☆ EXAMPLE If your vanity is fictionsoftinc on the United States server, the URL would be:
  >
  > ```
  > https://fictionsoftinc.api.madcapcentral.com/api/users/SamlLoginSucceeded
  > ```

  European server:

  ```
  https://[vanity].api.eugwc.madcapcentral.com/api/users/SamlLoginSucceeded
  ```

- SAML Endpoint for Sites

  United States server:

  ```
  https://[vanity].mcoutput.com/api/users/SamlLoginSucceeded
  ```

  > ☆ EXAMPLE If your vanity is fictionsoftinc, the URL would be:
  >
  > ```
  > https://fictionsoftinc.mcoutput.com/api/users/SamlLoginSucceeded
  > ```

  European server:

  ```
  https://[vanity].mcoutputeu.com/api/users/SamlLoginSucceeded
  ```

- (Optional) Single Log Out (SLO)

  Use the same URL as your login, so that people are redirected to it when they log out.

  United States server:

  ```
  https://[vanity].api.madcapcentral.com/api/users/SamlLogoutSucceeded
  ```

  European server:

  ```
  https://[vanity].api.eugwc.madcapcentral.com/api/users/SamlLogoutSucceeded
  ```

> NOTE The SLO option is supported only by some IdPs, specifically those that only use the usernameID in the call to the endpoints. Check with your IT department to see if your IdP supports SLO.

> NOTE This setting also allows Flare Online users to enable an option to control how they log out (see "Providing and Obtaining Single Sign-On Information" on page 28). When logging out, it can mean that they are only signed out of the Flare Online license, or it can mean that they are also signed out of the IdP.

- (Optional) SAML Endpoint URL for CNAME Sites

```
https://[host mapped domain]/api/users/SamlLoginSucceeded
```

> ☆ EXAMPLE If your host mapped domain is help.fictionsoftinc.com, the URL would be:
>
> ```
> https://help.fictionsoftinc.com/api/users/SamlLoginSucceeded
> ```

> NOTE This information is optional. If you are not mapping to a host domain on the Sites page, you do not need to provide this information to your IT department.

What's Next?

After you obtain the necessary information from the IdP, you need to enable SSO and add the details into Flare Online. See "Setting Up Single Sign-On Authentication on a License" on the next page.

Setting Up Single Sign-On Authentication on a License

After receiving the necessary information back from your IT department, complete the following steps.

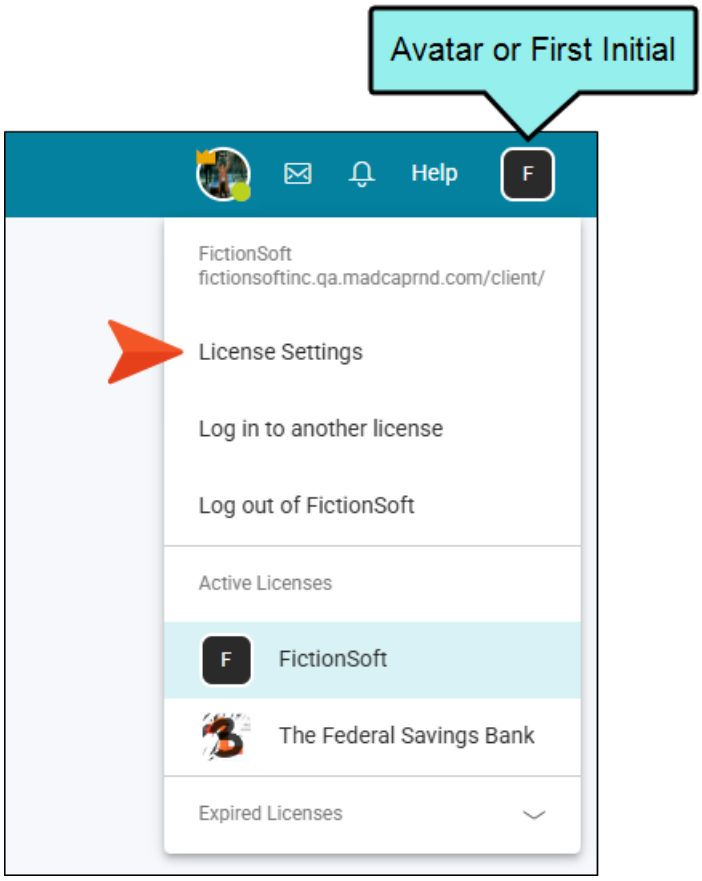
Permission Required?

For this activity, you must have the following permission setting:

For more information about permissions, see the Help system.

How to Set Up SSO Authentication on a License

1. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select License Settings.



2. On the left side of the dialog, click **Single Sign-On**, then click **Configure** or **Change Settings**.
3. Enter the SAML 2.0 settings that you obtain from your IT department.

   SAML Authentication Settings

   - **Enable SSO for Flare Online login** This integrates SSO with your license. If this is not selected, users cannot log in via SSO and must use the other process of entering a Flare Online password manually.
   - **SAML 2.0 Login Endpoint (HTTP)** This path is used when individuals log in.
   - **(Optional) SLO Logout Endpoint (HTTP)** Single log out (SLO) is a path used when individuals log out. You can leave this field blank if you don't intend to use it.

     > **NOTE** The SLO option is supported only by some IdPs, specifically those that only use the usernameID in the call to the endpoints. Check with your IT department to see if your IdP supports SLO.

     > **NOTE** This setting also allows Flare Online users to enable an option to control how they log out (see "Setting Up Single Sign-On Authentication on a License" on page 35). When logging out, it can mean that they are only signed out of the Flare Online license, or it can mean that they are also signed out of the IdP.

   - **Identity Provider Issuer** This is a unique string associated with your IdP.
   - **Public Certificate** Copy and paste the text from your certificate into this field.

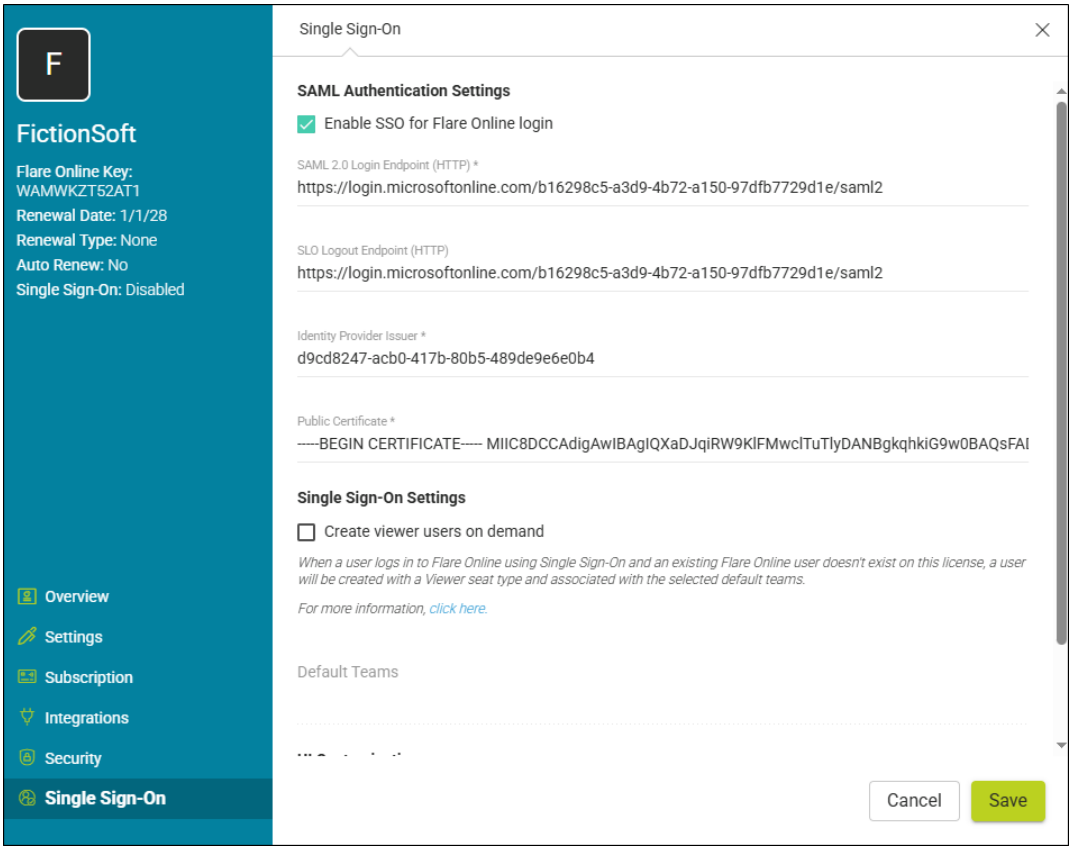
   Single Sign-On Settings

   > **NOTE** The fields "Create viewer users on demand" and "Default Teams" are covered in the next set of steps, which are optional. See " " on page 39.

UI Customization

- **Login Button Label** By default, the button label is "Log in with third party," but you can change it. For example, you might want it to be more specific to your SSO provider (e.g., Microsoft Login).

> ☆ **EXAMPLE** When finished, your settings might look something like this:



4. Click **Save**.

What's Next?

After enabling SSO and providing the configuration information, there isn't anything else you must do. However, you might decide you want to create viewer users on demand. In addition, individual Flare Online users might want to determine their own logout behavior. See "Other Activities for Single Sign-On" on the next page.

Other Activities for Single Sign-On

There are some additional tasks you might perform regarding this feature.

Creating Viewer Users On Demand

You can complete some optional settings if you intend to invite viewers on demand (i.e., by sending them a link to the private output). See "Onboarding Viewers to Private Sites With SSO" on page 8.

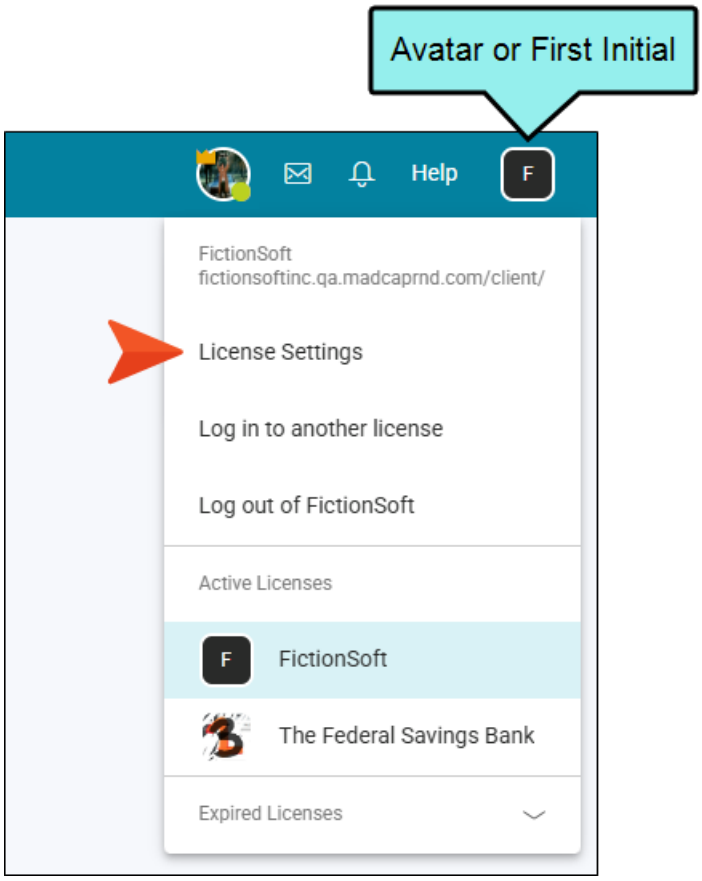
Permission Required?

For this activity, you must have the following permission setting:

For more information about permissions, see the Help system.

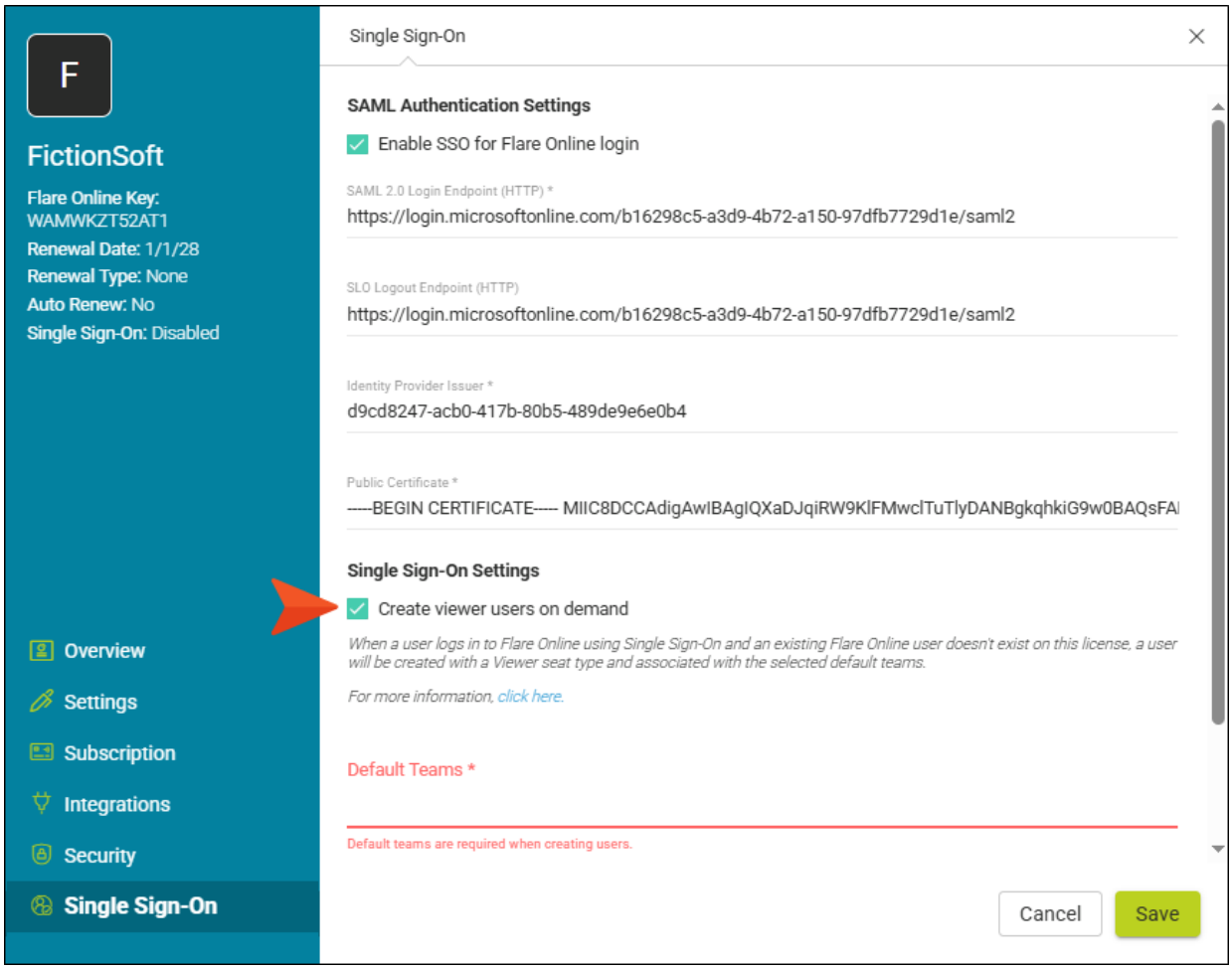
How to Create Viewer Users On Demand

1. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select License Settings.

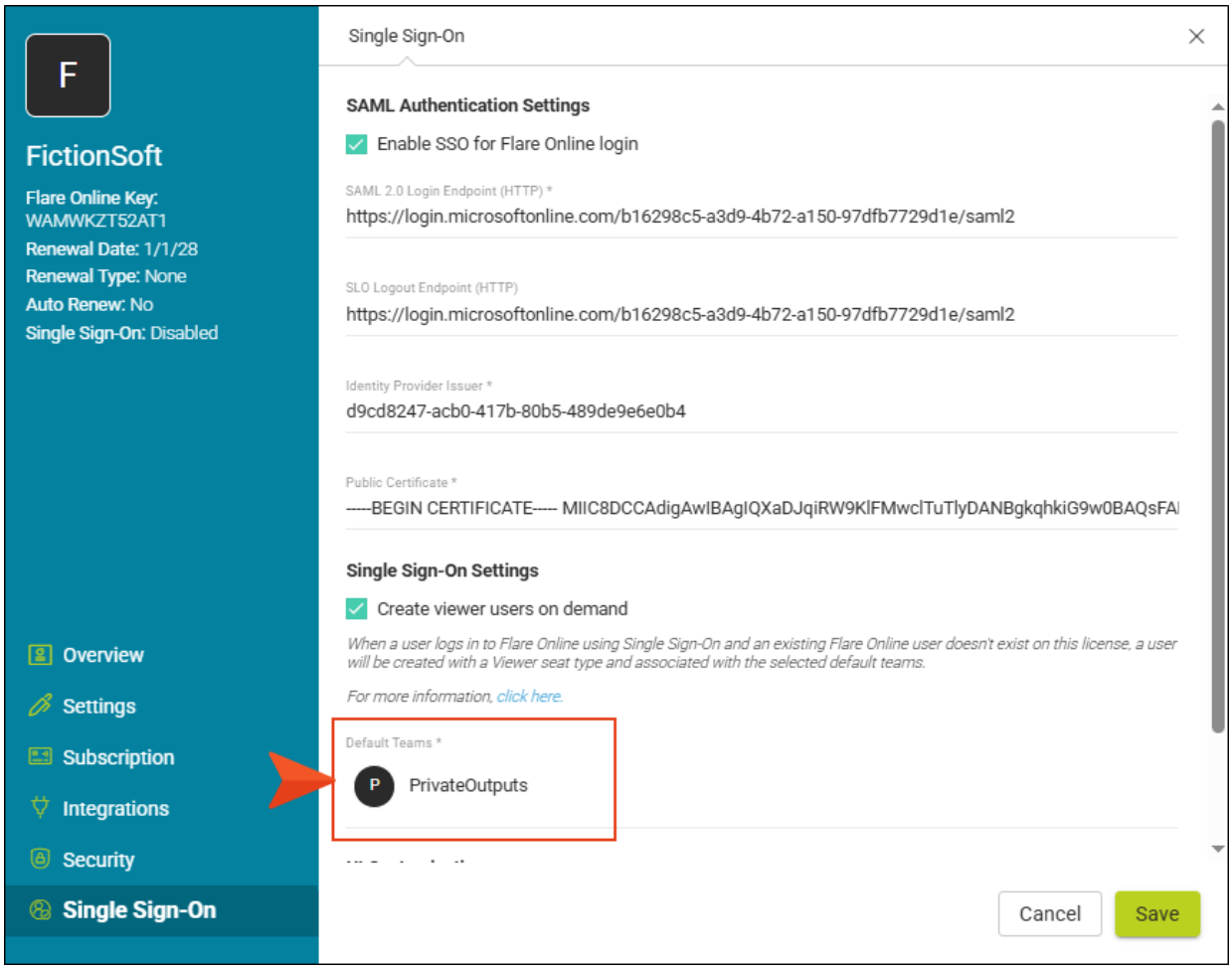


2. On the left side of the dialog, click Single Sign-On, and make sure you have completed the previous set of steps to set up and enable SSO authentication.
3. Click Change Settings.

4. Under **Single Sign-On Settings**, enable **Create viewer users on demand**.



5. Click in the **Default Teams** field, and select one or more teams that you have already set up. Newly onboarded viewers will automatically be added to the team(s) you select from this field. Also remember, viewers must be associated with a team that is tied to the private site you want them to access.



6. Click **Save**.
7. Provide your end users with a link to the private output.

Setting the Logout Behavior for Single Sign-On

If the optional single log out (SLO) endpoint is configured for single sign-on (SSO), Flare Online users can choose what happens when they log out of Flare Online. See "Setting Up Single Sign-On Authentication on a License" on page 35.

> NOTE The SLO option is supported only by some IdPs, specifically those that only use the usernameID in the call to the endpoints. Check with your IT department to see if your IdP supports SLO.

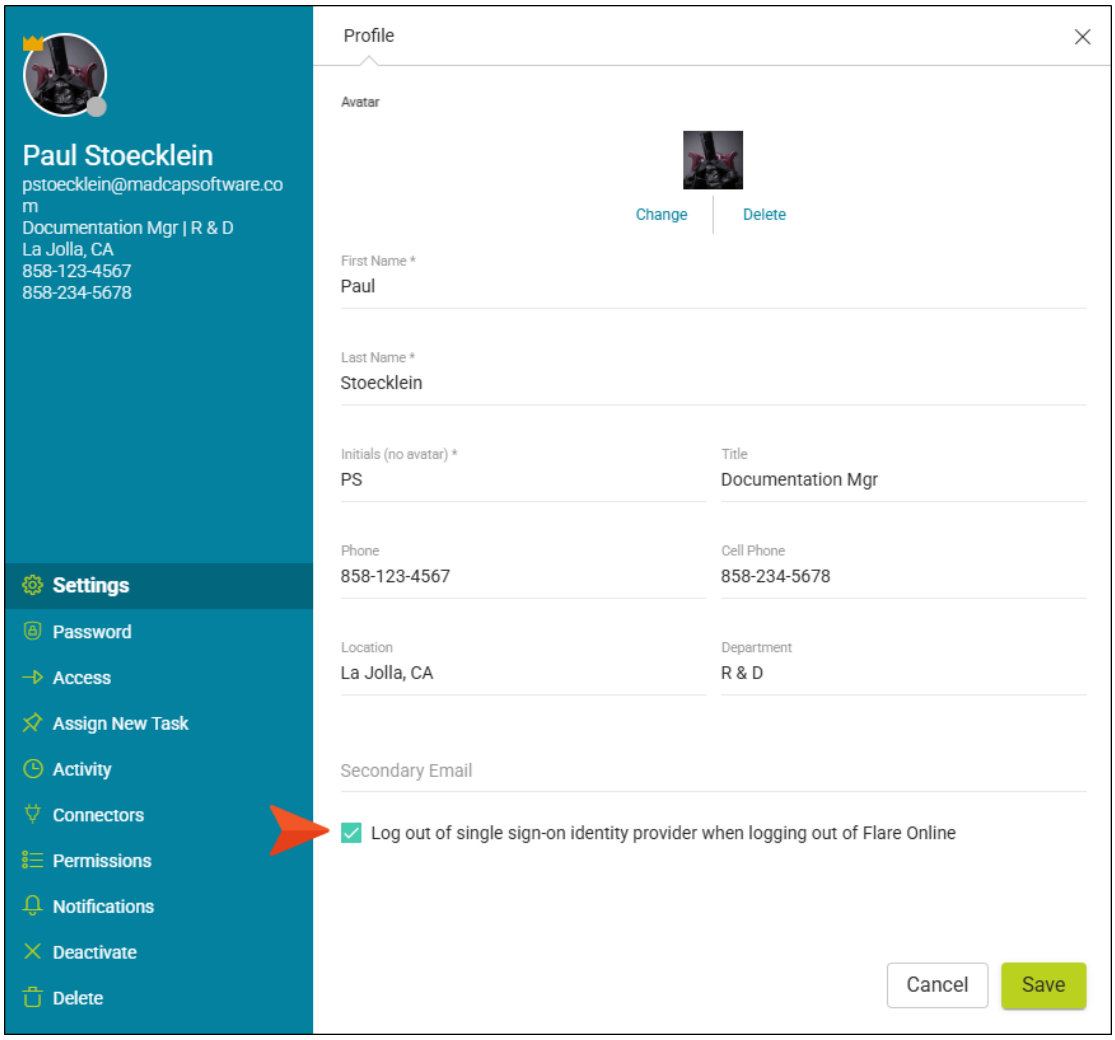
Permission Required?

There is no special permission needed for this, except that the license must be enabled for SSO.

How to Set the Logout Behavior

1. At the top of Flare Online, click your avatar or name.
2. On the left side of the profile, make sure **Settings** is selected.

3. At the bottom, enable or disable **Log out of single sign-on identity provider when logging out of Flare Online**.



If the option is enabled, the user will be logged out not only from Flare Online, but also logged out of the IdP.

If the option is disabled, the user will be logged out of Flare Online, but will remain logged into the IdP.

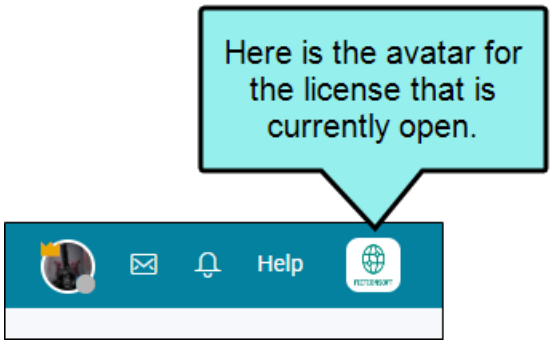
> NOTE This option displays only if SSO is enabled for the license.

4. Click **Save**.

CHAPTER 4

Setting a License Avatar

You can select an avatar image to represent your license. If you do not choose an image for the avatar, Flare Online will use the first initial of the license.



This chapter discusses the following:

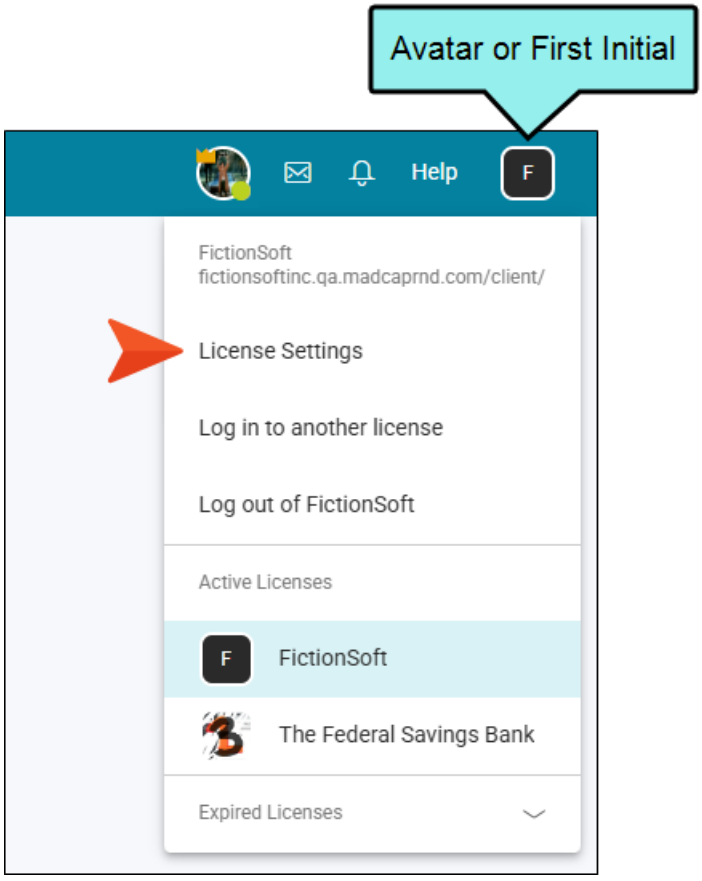
Permission Required?

For this activity, you must have the following permission setting:

For more information about permissions, see the Help system.

How to Set a License Avatar

1. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select **License Settings**.



2. On the left, select **Settings**.
3. In the **Avatar** section, click **Change**, select an image, and click **Open**.

> NOTE When used on a login screen, the avatar is displayed as a square 62 x 62 pixels. For high-DPI screens, you might want to use an image that is twice that size (124 x 124 pixels).

4. Click **Save**.

CHAPTER 5

Changing the License Key Label

The license key label is used internally to identify your MadCap Flare Online license. If you belong to multiple MadCap Flare Online licenses, a unique label ensures that you can distinguish between them in Flare Online. In addition, the first initial of the license, or a custom avatar, can be helpful to quickly find it (see "Setting a License Avatar" on page 45).

This chapter discusses the following:

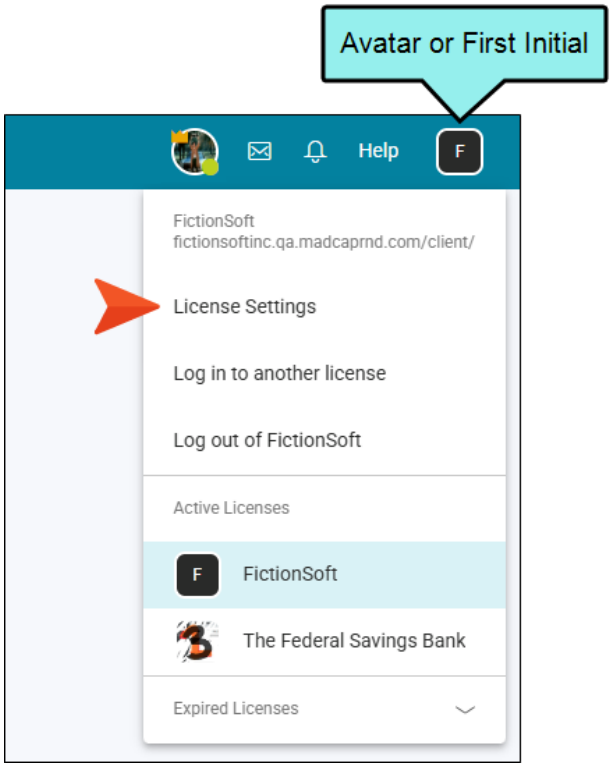
Permission Required?

For this activity, you must have the following permission setting:

For more information about permissions, see the Help system.

How to Change the License Key Label

1. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select **License Settings**.



2. On the left, select **Settings**.
3. Edit the **Name** field.
4. Click **Save**. Your license key label is updated throughout MadCap Flare Online.

NOTE The original license key label is based on the company name when a Flare Online license is purchased. The same is true for the license vanity (subdomain). If your company name has a space in it, that space is automatically removed. You can add the space back when you change your license key label. However, you cannot add a space when changing the license vanity.

NOTE Changing the license key label changes it for all users.

CHAPTER 6

Setting the License Vanity

When you first subscribe to Flare Online, a license vanity is provided for you based on your license (e.g., company) name. This vanity is the prefix (or subdomain) of the default Flare Online domain that is used for your outputs (e.g., **fictionsoft**.mcoutput.com). You can change this license vanity if you would like to use something else, although you cannot change the root Flare Online domain (i.e., the last part, which is "mcoutput.com").

> WARNING Use caution when changing the license vanity. It is generally best to do this when your Flare Online license is new and before you have set sites to “live.” If you have already published outputs and then decide to change the license vanity, any links to the older URL will be broken.

> IMPORTANT When changing your license vanity, keep in mind that MadCap Software is not responsible for other companies claiming a particular name before you are able to.

This chapter discusses the following:

Permission Required?

For this activity, you must have the following permission setting:

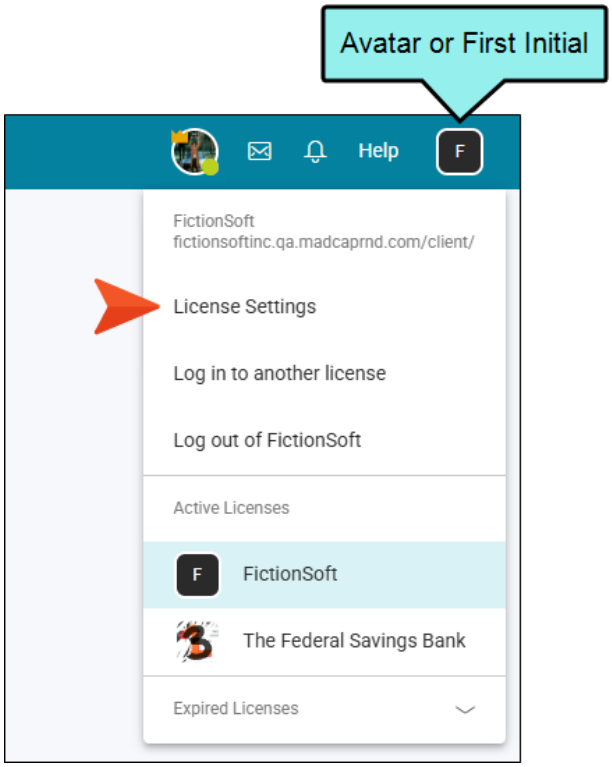
For more information about permissions, see the Help system.

How to Set the License Vanity

1. If your license is enabled for single sign-on (SSO), you will need to have your IT department update the application within your identity provider (IdP) to the changed vanity. Otherwise, you will not be able to log in to the license again after you change the vanity.

   If you are not using SSO, you do not need to bother with this step.

2. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select **License Settings**.



3. On the left, select **Settings**.
4. In the **Vanity** field, enter the subdomain you want to use for your license URL (only alpha characters and numbers are allowed).
5. Click **Save**.

NOTE The original license key label is based on the company name when a Flare Online license is purchased. The same is true for the license vanity (subdomain). If your company name has a space in it, that space is automatically removed. You can add the space back when you change your license key label. However, you cannot add a space when changing the license vanity.

NOTE If you prefer end users to see your company's domain instead of Flare Online's ("mcoutput.com"), you can create a CNAME (Canonical Name) to map to your own host domains.

CHAPTER 7

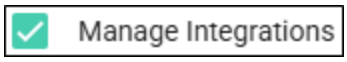
Connectors Integration

The publications feature gives you the option to publish output to Syndicate (i.e., MadCap's Enterprise Content Delivery Platform) or to a remote server via SFTP. A connector is the most important concept in the publishing process, because without it you cannot connect to an external location. A new connector basically requires credentials to access the outside server you are connecting to, such as login, authentication, and connector URL (host name).

This chapter discusses the following:

Permission Required?

For this activity, you must have the following permission to control and allow access to external servers:



A user with Administrator rights is expected to have the Manage Integrations permission to integrate a connector with a Flare Online license.

For this activity, you must have the following permission:

Users associated with a project only need the Publish Builds permission for publishing output.

For more information about permissions, see the Help system.

Connector Set Up

For Flare Online to push data to other systems, there are some considerations in order to establish outside connections. Your organization's administrator can help you with this set up.

Syndicate

You need to have Syndicate (which includes Elevate) with a Platform Login that gives you access to both applications.

A user (i.e., API user or standard user) needs to be part of the "Syndicate" role. Then in Elevate, the appropriate permissions need to be given for users to access Syndicate groups and folders, and to generate the Client ID and API key that is needed for the publications feature. Note that a standard user with Administrator privileges can generate API keys in the user profile settings in Elevate.

The URLs and credentials generated are all necessary to enter into the Flare Online connector for Syndicate authentication.

> NOTE Syndicate and Elevate are part of the MadCap Software family of products. This documentation assumes you have a Syndicate account and a working knowledge of the portal. For more information refer to Syndicate documentation.

SFTP

Your administrator can provide you with details pertaining to the remote server or the computer where you want to publish output.

How to Create a Connector

When you create a connecter at the license level, you are setting up a connection where all users on your license can use it.

1. In the upper-right of Flare Online, click your license avatar (or the first letter of your license if you haven't yet chosen an avatar image) and select **License Settings**.
2. On the left, select **Integrations**.
3. Select the **Connectors** tab (if it does not have focus).
4. Click **New Connector**.
5. From **Type**, select **Syndicate** or **SFTP**. Depending on the connector type, the fields you see vary.

   ### SYNDICATE

   a. In the **Settings** area, do the following:

      i. **Name** Enter a name for the connector. It can be anything.

      ii. **Elevate URL** Enter the Elevate URL (e.g., studio-[customer].xyleme.com)

      iii. **Syndicate URL** Enter the Syndicate URL host name (e.g., https://core-[customer].bravais.com)

      > NOTE It is the Delivery (CORe) API that is used to publish content to Syndicate. The base URL for the API call is https://core-[domain].bravais.com, where [domain] is the user's domain name. CORe stands for Core Object Repository, and bravais is the legacy name for Syndicate.

   b. In the **Authentication** area, enter the following:

      i. **Client ID** Enter the Elevate-generated Client ID.

      ii. **API Key** Enter the Elevate-generated API Key.

SFTP

a. In the Settings area, enter the following:
    i. Name Enter a name for the connector. It can be anything.
    ii. URL Enter the host name of the remote server or the computer where you want to publish the output files.
b. In the Validation area, from Type select:
    - None Select this if there is no validation of the SFTP server.
    - Public Key Select this to validate the server against a public key.
c. In the Authentication area, from Type select:
    - Password Select this if the server connection is authenticated by the user name and password.
    - Private Key Select this if the server connection is validated against a public or private key pair match. You need to supply the private key and password for the server.

6. Click Save.

CHAPTER 8

AI Assist Integration

Before you use AI Assist in Flare Online, you need to connect your ChatGPT account to AI Assist (via an API key) in the license settings in Flare Online.

This chapter discusses the following:

Permission Required?

Editing content and project files is an activity available to users with the Author status. By default, users with Author status have the following permissions set:

- 

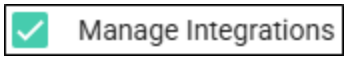
  If this is deselected, then viewing files in a read-only mode is allowed. On the left side of the page, the Files vertical three-dot menu is not available.

- 

  If this is deselected, the XHTML in the Code view is read-only.

  Editing code is regarded as a capability for an advanced user. If not done properly, the code can become malformed quickly. Administrators can prevent users from editing the code by deselecting the Edit Code permission.

In addition, AI Assist involves the following permissions:

- 

  This is required to integrate a ChatGPT account with a Flare Online license in the license settings.

- 

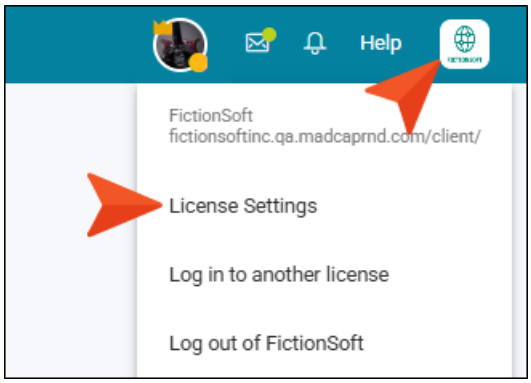
  This is required to use AI Assist (and therefore ChatGPT) when modifying topics and snippets.

  > NOTE Even if this permission is enabled, ChatGPT does not scan anything on your computer. The only information ChatGPT can acquire from you is what you enter manually into the prompt when using AI Assist. If your company has strict policies against AI or ChatGPT, simply do not use it.

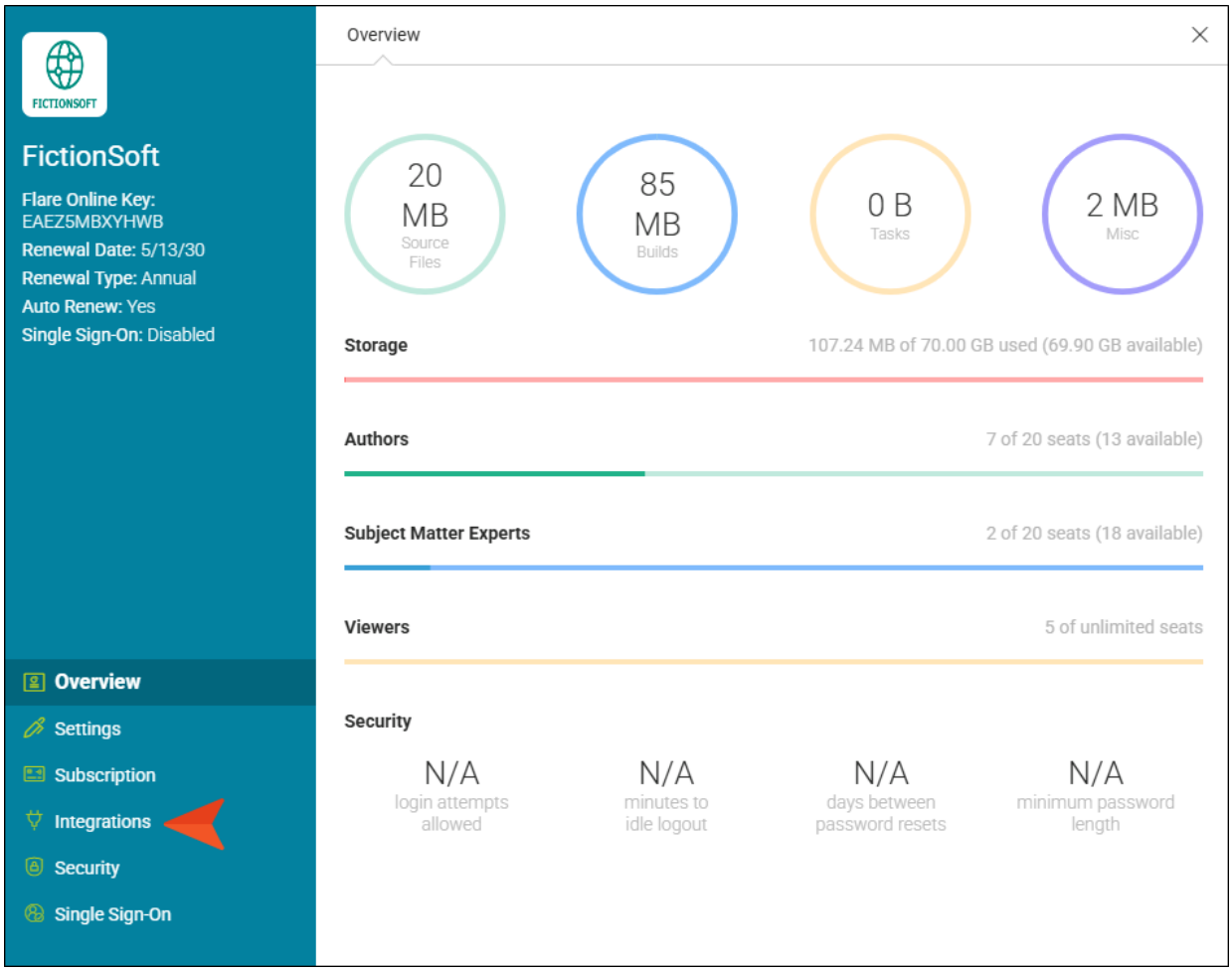
For more information about permissions, see the Help system.

How to Connect a ChatGPT Account to AI Assist in Flare Online

1. Go to openai.com/chatgpt, log in, and create an API key (or obtain one from your IT department). Refer to the OpenAI Help for steps to create an API key.
2. In the upper-right of Flare Online, click the license drop-down and select **License Settings**.



3. On the left, select **Integrations**, and then the **AI Assist** tab.



4. Paste your **API Key**.
5. In the **Version** field, select a ChatGPT model.
6. Click **Save**.

CHAPTER 9

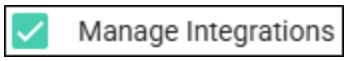
Slack Integration

If you have a Slack account, you can integrate it with Flare Online's notification system. By doing this, all types of activity alerts (e.g., builds completed, tasks edited or moved, projects deleted) can be fed directly to your Slack channels, making it easier for you to remain informed and communicate with others when certain events take place in Flare Online. Most of the steps for this integration take place in Flare Online.

This chapter discusses the following:

Permission Required?

For this activity, you must have the following permission setting:



For more information about permissions, see the Help system.

How to Set Up Slack Integration

1. In Slack, make sure you have set up a Slack account and created channels that you want to integrate with Flare Online.
2. At the top of Flare Online, click the license drop-down and select **License Settings**.
3. On the left side of the dialog, select **Integrations**, and then the **Slack** tab.
4. In the **Channels** section, click **Connect a Channel**.
5. Complete the Slack instructions in the browser.

   Slack sends an approval message to the workspace owner. After that person approves the request, you can continue with the next steps.
6. Choose your Slack team and then select a channel that you want to integrate.
7. Click **Allow**.
8. Back in Flare Online, a message indicates that the addition was successful.
9. Repeat the steps above if you want to add more of your Slack channels to the grid.
10. With your channel added, you're ready to connect it to any of Flare Online's notifications. Click **Add Notification**.
11. In the **Name** field, provide a name for the channel notification. It can be the same name as the Slack channel you want to hook it to, but this isn't necessary.
12. From the **Channel** field, select the Slack channel that you want to associate with the notifications.
13. From the **Activity Type** field, select one of the alert categories (i.e., Builds, Checklists, Projects, Sites, Tasks, Teams, Users). Notice these same groups are available when setting up notifications in your user settings.
14. Depending on the activity type you choose, additional fields are displayed in the area below. Complete the fields as necessary to choose the type of notifications you want to be associated with the Slack channel.
15. Click **Add**. A row is added for the new channel notification.

16. (Optional) You can perform an action in Flare Online that you have integrated with the Slack channel (e.g., set a target to "live"). You should see the notification added to your Slack channel.

NOTE Keep in mind that the notification UI in Flare Online is unique to each user. On the other hand, when you set up Slack integration, it is created for the entire license; therefore, other users can tap in to that channel notification to receive the same alerts via Slack.

NOTE If you encounter problems or need help with your Slack integration, please contact support. See the following:

http://www.madcapsoftware.com/support/contactoptions.aspx

CHAPTER 10

Setting Security Options

On your license, you can set the maximum login attempts, automatic logout settings when the system is idle, as well as password change and minimum requirements.

This chapter discusses the following:

Permission Required?

For this activity, you must have the following permission setting:

For more information about permissions, see the Help system.

How to Set Security Options

1. At the top of Flare Online, click your user name, then click License Settings.
2. On the left side of the dialog, click Security.
3. Select any of the check boxes and choose values for each. If you do not select a check box next to an item, it will not be enabled. These settings will affect all users on your license.
    - Login attempts allowed If a user exceeds the maximum number of login attempts, that person will be locked out for five minutes. After that, the user can try again, or click Forgot password.
    - Require password change after Starting two days before the expiration, users will see a reminder that their password will expire, prompting them to set a new password. Users can skip this prompt and continue with the old password until the final day, at which time they must set a new password.
    - Password minimum You can specify that a user must create a password with a certain number of characters. All passwords must have at least 12 characters.

      ☆ EXAMPLE If you select 15 in this field, the must create a new password that has at least 15 characters.

    - Logout after idle for If there is a lack of activity in Flare Online, a user will see a warning message when one minute is left. After the time expires, the user will be logged out. You can set the number of minutes of inactivity when this occurs.

NOTE This option is supported for both regular Flare Online logins and single sign-on (SSO).

4. Click **Save**.

NOTE If a user belongs to more than one Flare Online license, that person is bound to the most restrictive setting across all licenses. For example, License A might specify that three login attempts are allowed, while License B specifies five login attempts, and License C specifies seven login attempts. If the user is working on any of the licenses, that person will be limited to three login attempts.

PDFs

The following PDFs are available for download from the Help system.

AI Assist Guide

Analytics Guide

Authoring Guide

Branding Guide

Building Output Guide

Checklists Guide

Conditions Guide

Getting Started Guide

Images and Multimedia Guide

License Management Guide

Links Guide

Projects Guide

Reports Guide

Reviews Guide

Security Whitepaper

Sites Guide

Snippets Guide

Source Control Guide

Styles Guide

Targets Guide

Tasks Guide

TOC Guide

Topics Guide

Translation Guide

Users and Teams Guide

Variables Guide

What's New Guide

Widgets Guide