

MadCap Software Webinar Q&A

Webinar: How You Can Leverage SSO for Your User and Password Management

Date: November 16, 2022

Presenter: Jennifer Morse, MadCap Software

QUESTION	ANSWER
Is there a way to have a new user added to a particular team based on their email address domain?	Currently, that's not possible. Great question and feature suggestion. Ill add it to the list for V2
Where do you set the "license vanity"?	The license vanity is set on the License settings by selecting the license avatar > license settings. Note that changing the vanity will also change the subdomain.
Any way to see a report of the users who have added themselves in a particular time period?	Not currently. It will be something we are going to need to do at some point and other analytics. Great suggestion!
Can single sign on help users outside our organization access our password protected output?	Not unless they have an account with the IdP - the IdP is the gate keeper for access.
How can we test our SSO implementation in a QA environment rather than test it in our production environment?	You can create a new Trial license of Central and test it securely in that trial instance.
Looks like this is geared toward enabling the company who owns and uses Flare/Central for SSO. Is there any known method to using this feature for end-user authentication to private sites? Like, can we make it so only OUR customers can access our help output without creating and managing individual user accounts?	Yes, the SSO feature can be applied to private sites so long as your customers are on the IdP.
Is the viewer user a feasible solution for customer users? And does this make economic sense if users log in infrequently? I'm concerned that a	Viewers are free in Central. You can have as many viewers as you need to access the site at no additional cost.

user hits the Central hosted online help once, but they stay on our license (and bill) indefinitely?	
I might be jumping ahead, but will the same Flare login to Central feature eventually include other targets such as SharePoint Online? This would fulfill the Microsoft's Modern Authentication mandates.	Not currently, great feature request!
Prior to this SSO feature, our org chose not to use Central due to the user management overhead and instead is using SharePoint Online. With that issue resolved, converting to Central is very compelling. However, our staff are already used to using SharePoint Search to find documents published from Flare to SharePoint. Is there way we can covert to Central but still published something to SharePoint to maintain the search workflow our staff are now used to?	Flare can still publish articles to SharePoint without any changes, so you can continue to use SP as the hosting platform for the output. You can still configure SSO for accessing the Central portal, for source control, collaboration, staging content, reviews, analytics etc.
I see the SAML connector for mapping users to a default team. Is there a separate Azure AD connector to view all directory groups so we can leverage Azure AD groups for all team mapping? That would eliminate the manual work of changing users between teams when they change their job roles.	No, In Azure they will create an application for the connection to Central - that application controls the access and groups.
Can Central respond to SSO authentication from the calling application? Our users use Okta to sign into the app, and it would be GREAT if they didn't have to sign in to help.	They would still need to log in at least once. Access tokens must be shared for SSO to work.

Can you please go over what you mentioned about associating with teams?	When using private sites, you need to set up a team that will associate the SSO users to. That team can be applied to various sites. Here is a quick overview on how teams and sites work: https://www.madcapsoftware.com/videos/central/creating-sites/#content
Sounds like this is most beneficial if we are using Central for hosting output. If we host locally, then SSO is only beneficial for the authors (saving a step of logging into Central). Am I understanding this right?	Correct.
If I'm an admin in Central, can I set up SSO for all users (so all authors don't have to call IT)?	Yes. When you set up SSO, the IdP uses "Applications" that access the different sites like Central. Users assigned to that application in the Identity Provider would have access to Central via SSO.
If Viewer on Demand is disabled, how does that process look for new users?	This is a requirement for private sites with SSO.
What is the best method for our cyber security team to engage with you to determine security alignment for Central?	Sending an email to your sales agent can get that conversation started - they are happy to help!
Is the MadCap login screen presenting every time you access content in central?	Once you are logged in you should not be prompted with the log in screen until you sign out or the access tokens expire.
Can I define different teams the automatically created users get assigned to, e.g., depending on the private site they logged in for the first time?	All SSO users that log in for the first time are associated to the team(s) selected in the SSO settings. These teams can be associated to the different sites.
Can you clarify: did you say you would see all the users who logged on with SSO on the Central Users page, even if you had NOT previously added them to Central?	Correct. The users will be added as Viewers when that option is checked in the license settings.

Would their emails be filled in?	This would depend on the end users set up, if they have cached user emails and passwords.
I do not see the new features in Central: The Avatar and first initial of license, and the Single sign-on option in the license settings.	I would recommend clearing your cache, if that doesn't work, give us a call, we will take a look with you.
Are there plans to add reviewing features in Central? The biggest reason I can see enabling SSO would be to allow internal reviewers to add comments to content without having to download a piece of software.	One of the other benefits of Central, is a web-based review workflow, where SMEs do not have to install anything. They can log into a simple lightweight web editor to review topics you send to them to review. Here is a quick overview on how that works: https://www.madcapsoftware.com/videos/central/reviews-author-perspective/#content
If you open/launch additional instances of Central from Flare now using the classic login, do you need to log in separately for each instance of Central in a browser? We like to have several instances Central open in multiple tabs.	You shouldn't need to log in each time. We will need to test this to be sure.
What about scenarios where we do not manage user accounts in our own IDP? Our customers access our product through their own solutions (some are Google, some are Azure AD, etc.). Will we be able to use the SSO solution still?	Not at this time. We will add this as a feature suggestion.
Do you associate teams to sites in Central? and is this process of associating teams to sites only available if you use SSO?	Yes, after you create the team, you associate those teams to sites in Central to grant access to a group of users. Associating teams is a requirement for privatized outputs in Central as well.
If you have more than one private site and each is assigned to a different team, is there a way to permission auto-added users via SSO to only a specific team?	In the first version of SSO, it will only support a 1 to 1 relationship with the entire Central license. That single configured SSO would be applied to all sites. This is a great feature suggestion!

If you're already logged into your IdP on your system, will Central still prompt you the first time to login, or will it recognize that you're already logged in?	You will need to log in via your IdP that first time so the access tokens can be applied.
If you enable SSO and still have users defined directly in Central, if they're removed from the IdP, will they still be able to provide their Central license to get in?	The removed user will not be able to access Central or any private sites at all – which is nice because you don't need to worry about remembering to remove users' access from the Central license if they leave the company. However, users who are removed from the IdP will still technically exist on your license until you remove them. So, if you want to "clean up" the users on the license, or free up an author or SME seat you need to remove that person manually from Central
I don't see that blue icon yet. I might've missed something. Is it going to show up soon?	That icon is an image on the presenter's screen, but it will be a letter on your end in Central if you haven't added an avatar for your license. Here are the instructions for changing that letter to an avatar: https://documentation.madcapsoftware.com/central/Content/Central/License/Setting-License-Avatar.htm
Hello, is this about using SSO for the users who log in to my website (that I created with Flare) or about the new SSO feature when logging in to Central?	Hello! It is a bit of both. I will review what enabling SSO on central means in terms of accessing the central portal, and private sites on Central
Where does one change the look and feel of the SSO login screen / button?	The text in the log in button is managed in the same page where you configure SSO. To change the colors of the button and fonts, you can create a Theme and associate it to the site. Click on Sites, then in the toolbar click on Themes, and you will come to the theme designer. The image you saw came from the license avatar set in the license settings.

Can I authenticate via two separate IDPs? (Say, one for internal employees using the company IDP, and one for customers who also need to access linked sites hosted externally (and using the external IDP?))	Not as this time. Central currently only supports one IDP. This is something that we are researching for future versions.
Is there a way to enable SSO for output without Enabling SSO for Central Login?	Not currently. Authors and SMEs still have the option to use the link in the login screen, and if SSO is enabled on the license, they will be directed to log in using SSO.
How does this work with Multifactor authentication if the user has a Yubikey vs. a number sent to a cell? We've had huge issues.	All this is set up in the IdP - So depending on those settings, the SSO users might have to use 2FA to get logged in.