2021

Enterprise SSO

Overview and User Guide

ENTERPRISE SSO

Overview and User Guide

PURPOSE

The primary purpose of this document is show how to connect your Azure AD Environment to Pax8 for federated single sign on.

AUDIENCE

This document was designed for partners who use Azure AD as their primary identity provider. In future iterations, we will extend SSO capabilities to other IDPs and protocols.

LAST UPDATED

May 2021

ENTERPRISE SSO

Overview and User Guide

Summary

Federated Single-Sign On with Azure AD allows a partner to use their Microsoft identity to authenticate to the Pax8 Platform. This means they do not have to maintain two sets of credentials and a separate MFA token. Once the configuration is in place, app users will be redirected to authenticate with their Microsoft credentials after they put in their username at https://app.pax8.com/

Requirements

- An Azure Active Directory account
- A verified domain in Azure AD
- A Global Admin in the Azure AD account.
- A Primary Partner Admin in Pax8
- **UserPrincipalNames in Microsoft that match your Pax8 login username**

After the configuration is established, all Pax8 app users will be asked to sign in with their Microsoft credentials so it is best to send out communications internally of this change before you create the connection.

WARNING

Before you start this process, ensure that your UserPrincipalName in Microsoft matches your Pax8 login username. If you have a different username in Microsoft than your email address you may need to create new app users in Pax8 that match the UserPrincipalName in Microsoft. If you set up SSO and these values are different, then you will not be able login to the Pax8 Platform and would need to reach out to support. To avoid this issue, ensure that your login to Microsoft and the Pax8 Platform match. If they do not, you can create new app users in Pax8 with the appropriate username that matches Microsoft. You can do this by performing the following steps:

1. Go to Users>Create Users

2. Create all necessary app users with the correct username that matches Microsoft

3. Follow the steps to set up SSO

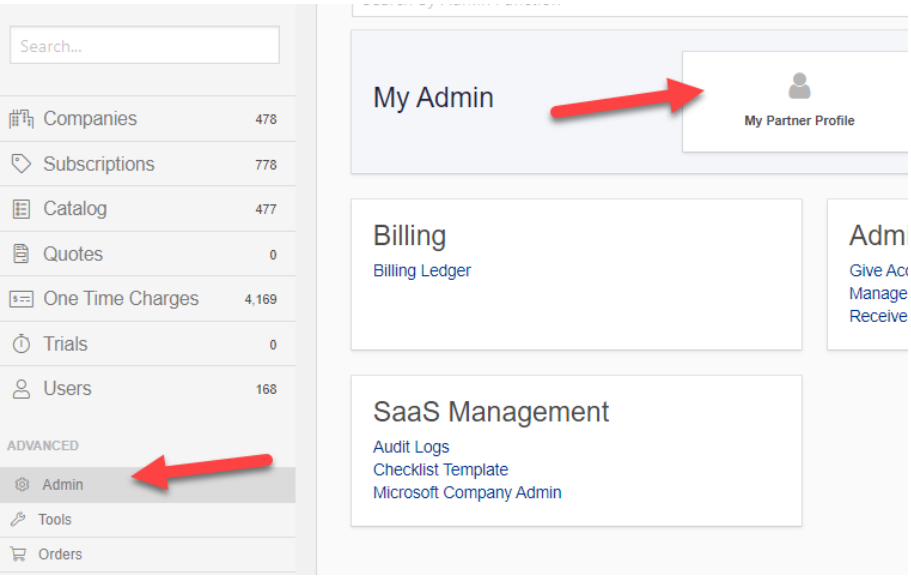
4. After you have signed back in you would be good to remove the duplicate app users.

ENTERPRISE SSO

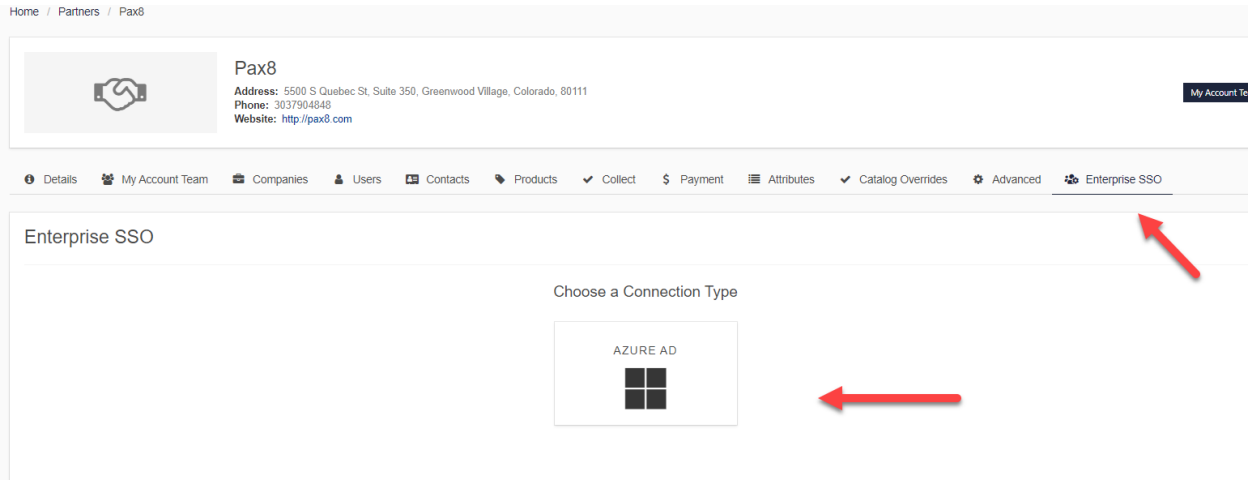
Overview and User Guide

Steps

1. As the primary partner admin, go to **Admin**>**My Partner Profile**

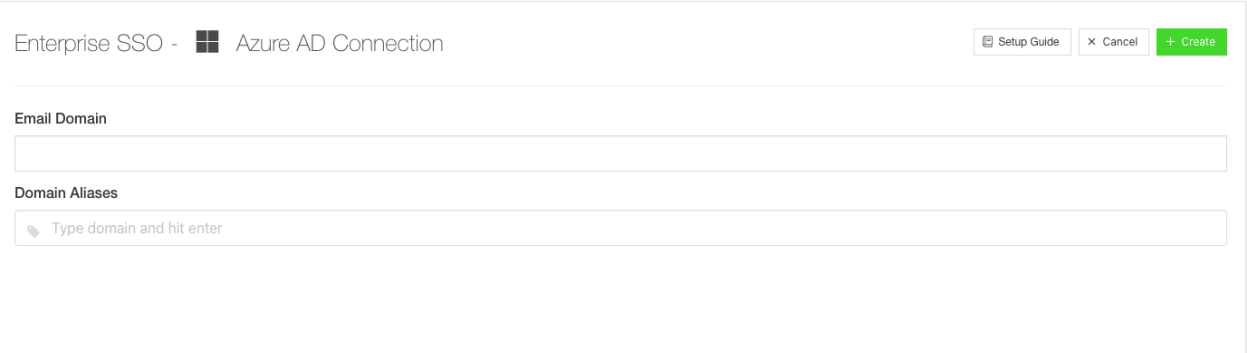


2. Here click **Enterprise SSO** > **Azure AD**



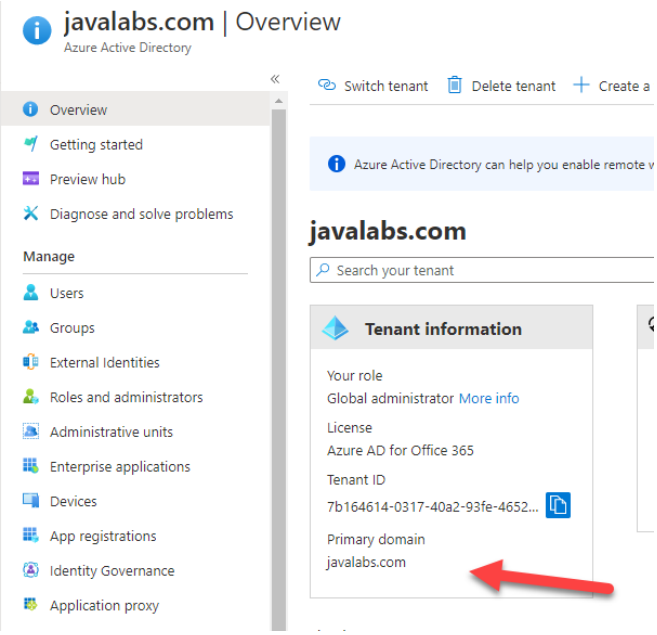
Overview and User Guide

3. Here you will fill out the following fields:



Email Domain: This is most likely your Azure Primary Domain

Click here as a Global Admin to verify what this is in your tenant. Ex.

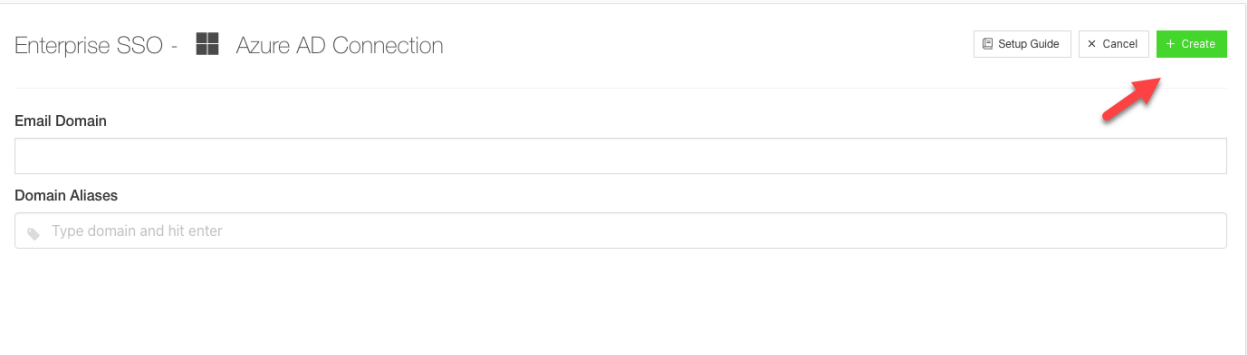


It is the primary SMTP address you have in your Azure AD tenant.

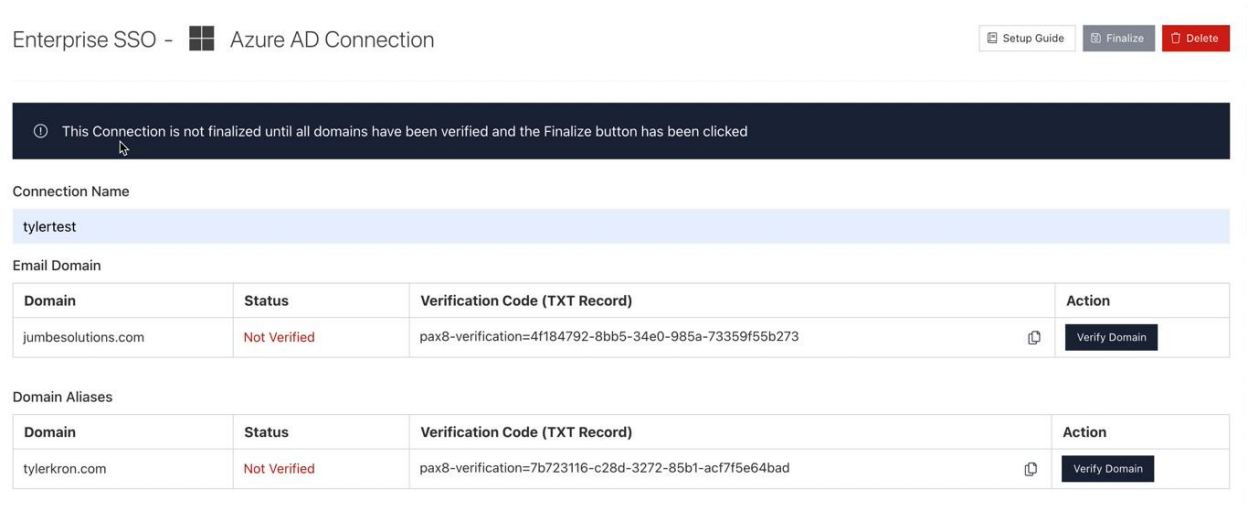
Domain Aliases: Optional field. Enter any other domain's in use within your Azure AD that users might have as their primary User Principal Name. Ex. Javalabs.biz, jlabsco.com. If you do not have any, you can leave this field blank.

Overview and User Guide

4. When you have filled out the necessary fields, Click **Create**

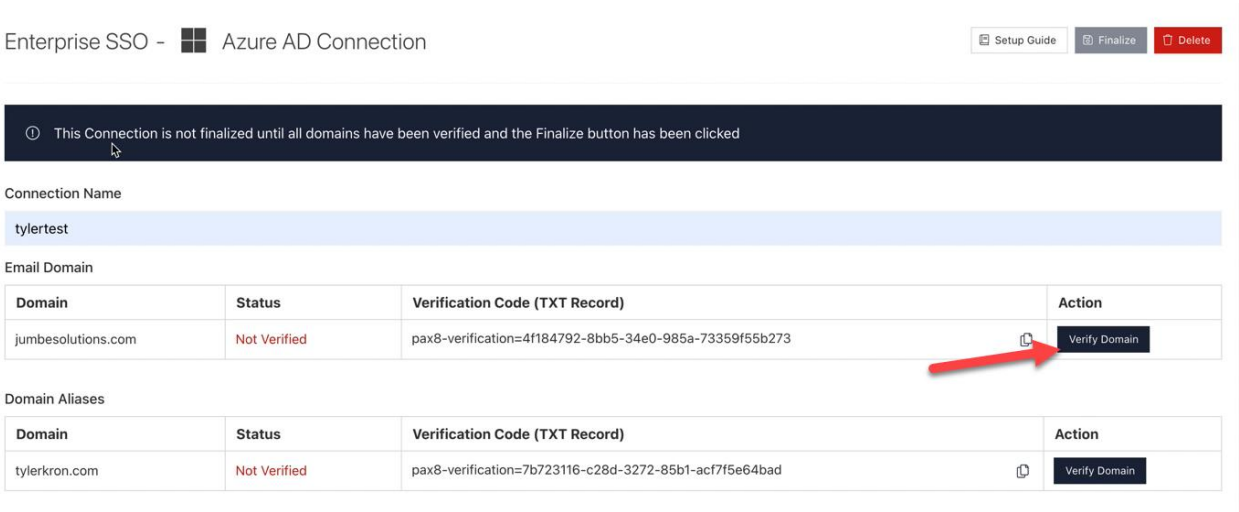


5. After you click create, the following page displays a text record(s) you will need to add with your DNS provider to your domain to prove that you own this domain. You can copy the Verification code and paste it into your DNS provider as a new TXT Record.

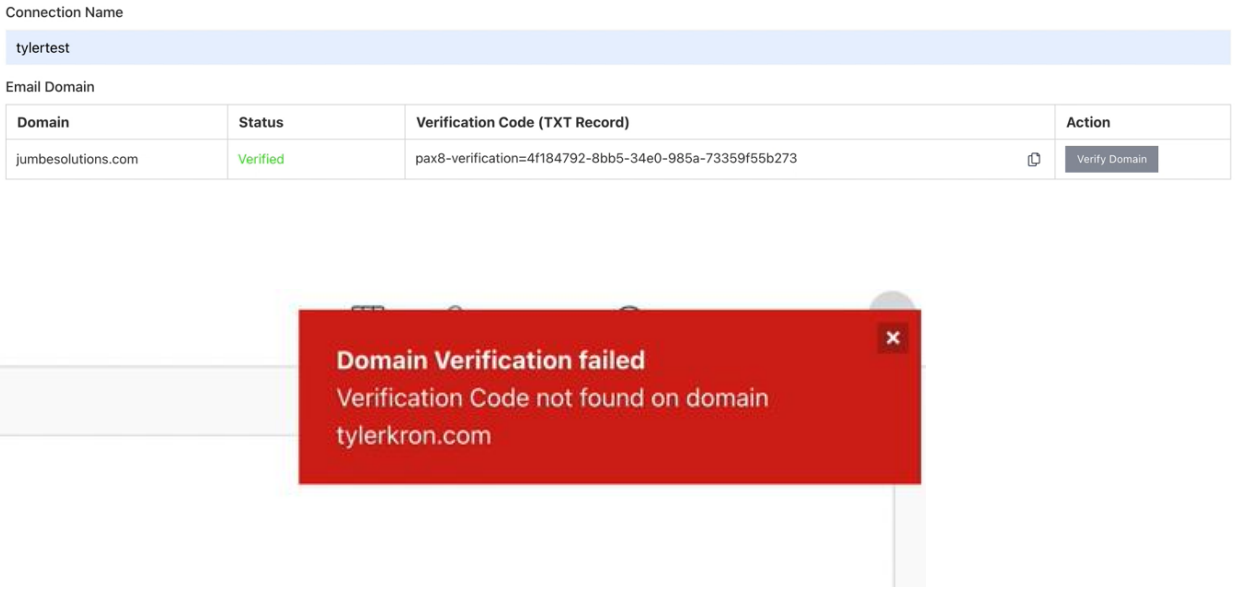


6. Depending on your DNS provider, propagation could take a few minutes or a few hours to successfully verify the domain. If you have a provider like GoDaddy, then it should only take a few minutes. After a few minutes have passed, click **Verify Domain**

Overview and User Guide



7. After you click on verify, you will see the status go into a Verified state. If there has not been enough propagation time yet or if the record was incorrectly entered, you will see an error message:

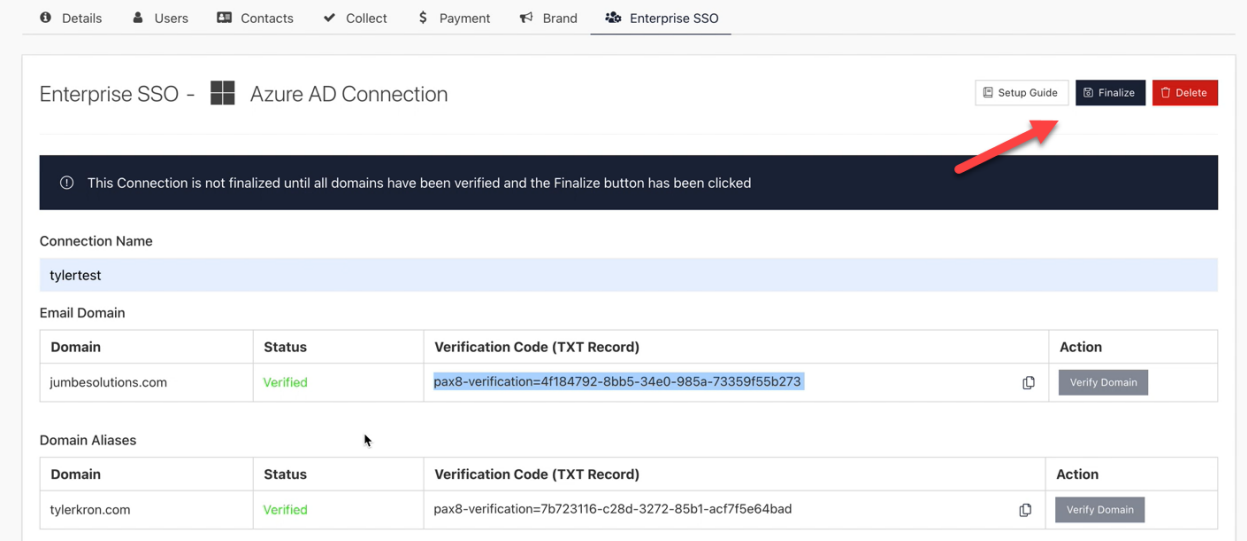


In most cases, you will just need to wait more time for the record to propagate to move past this error.

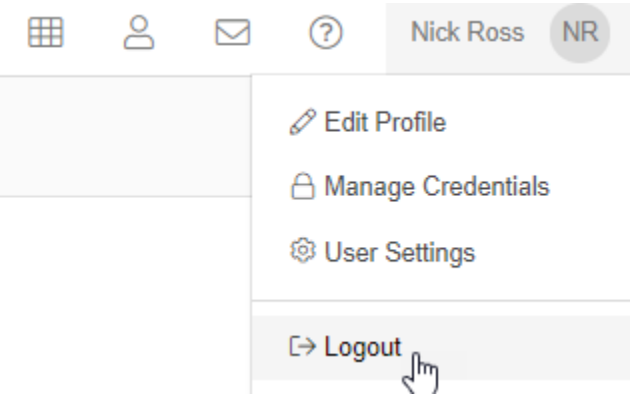
****NOTE** Before you move on to the next step, ensure that all of the app users within Pax8 are aware that they will be asked to sign in with Microsoft credentials upon their next log in to Pax8.**

Overview and User Guide

9. When you have successfully verified your domains, click **Finalize**

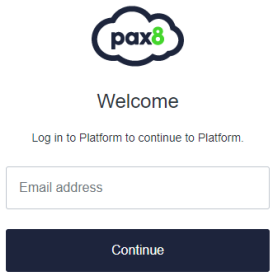


10. Now as soon as a user tries to login with a domain part of the configuration, that user will be redirected to authenticate with Microsoft. To try this out, Logout of Pax8.

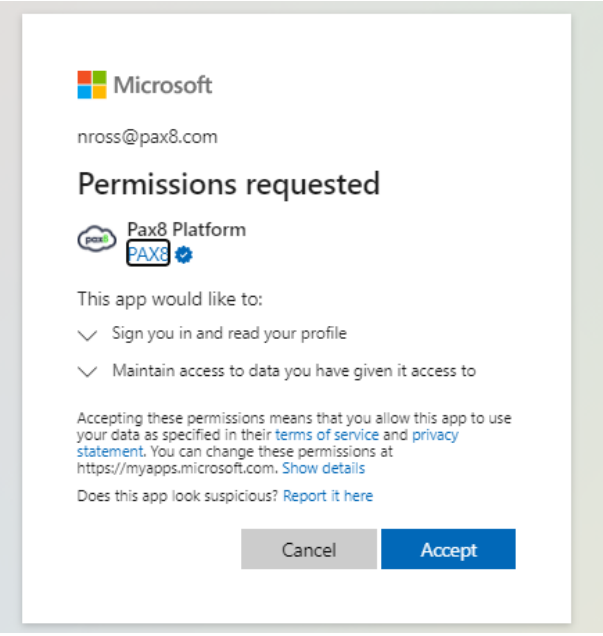


Overview and User Guide

11. Type in your username into the login screen. **You will need to be a Global Admin within your Azure AD to consent to our application for the first time. Subsequent users will then be able to sign in with their Microsoft Credentials as well.**



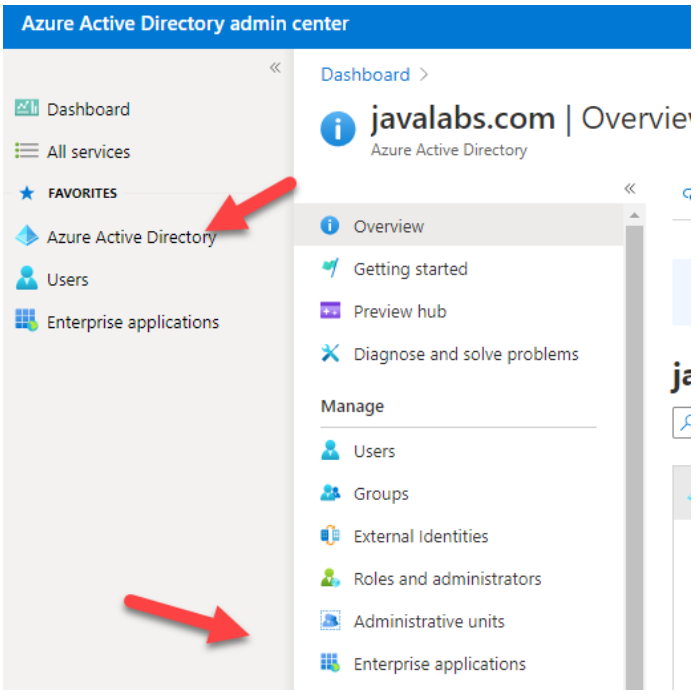
12. Now you will notice you are redirected to a Microsoft page that is asking for consent for Pax8 to read necessary information for this federated connection. If you are already logged into Microsoft you will be taken to the page you see below. If you are not logged in to Microsoft you will be asked to do so first. Click **Accept** on this page.



Overview and User Guide

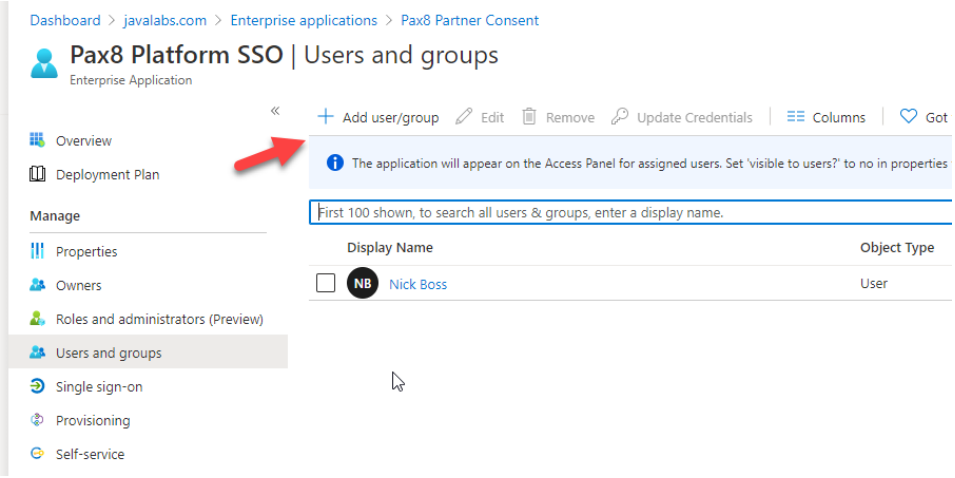
13. You will now be logged into Pax8. Every other app user will be asked to sign in with their Microsoft credentials. **Users must be created as an app user in Pax8 and have a user in Azure AD to be able to log into the platform.** After you establish the connection, new users who are created will not be asked to establish MFA with Pax8. They will need to have this set up within Microsoft. This meets Microsoft's secure application model for partner center as well.

14. By default, all users in Azure AD will have access to the platform if they are also an app user within Pax8. If you want to scope the group of users who have access even further, you can do so in Azure AD. Go to Aad.portal.azure.com >Azure Active Directory>Enterprise Applications



Overview and User Guide

10. Here you will find Pax8's App in the list provided. Clicking on this app allows you to scope the permissions to users or groups for access rights.



ENTERPRISE SSO

Overview and User Guide

FAQs

Q: I cannot see the Enterprise SSO icon under My Partner Profile

A: This tab is only viewable to Primary Partner Admins. Ensure you have the role of primary partner admin.

Q: I am logging in with the URL of <mydomain>.mycommandconsole.com and I am not prompted with SSO. Why is that?

A: This URL is currently unsupported with our existing configuration of SSO. Users will need to go to https://app.pax8.com to utilize the federation after it is in place. We will provide support for this custom URL in the future. We do not have ETAs at this time.

Q: New users I create in Azure AD are unable to login to Pax8. Why is that?

A: Users must be created in both Azure AD AND within Pax8 first before they are able to sign in with their Microsoft credentials.

Q: Do new users I set up after the federation is in place have to set up MFA with Pax8?

A: No, users only need to establish MFA with Microsoft

Q: Can my self-service customers take advantage of SSO?

A: Not at this time. We are planning to release this to them later this year.

Q: Is Microsoft the only provider Pax8 integrates with?

A: At this time, yes. We plan to extend this to other providers like Okta, Google, etc. later this year.

Q: What happens if I delete the connection for SSO later?

A: All users will be logged out of the platform and asked to sign back in with Pax8 credentials. If users have been created since the federation was in place they will also be asked to establish MFA with Pax8.

Overview and User Guide

Q: Is there a way to bypass SSO if I have a subset of users that don't have an identity in AzureAD?

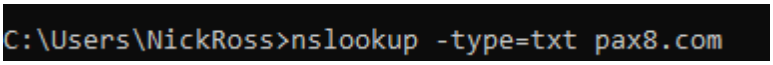
A: No, there is no way to bypass certain users after the federation is set up. They would have to have a domain that falls outside the scope of what was entered during the connection setup.

Q: Is Pax8 working towards provisioning and deprovisioning users automatically from Microsoft?

A: Yes, we are working our way towards a better model of access controls through an API that relies on the IDP for self-service user creation/deletion. Timelines for this are still being determined.

Q: My text record is not validating for my domain in Pax8. How can I check to see if it has propagated other than looking in my DNS provider?

A:

1. Open Command prompt (Start > Run > cmd)
2. Type "nslookup -type=txt" a space, and then the domain/host name. e.g. "nslookup -type=txt pax8.com" ex. 

3. Here you will be able to see TXT records that are published to you domain publically.

Q: I currently am integrated with a PSA tool like ConnectWise and Syncro. When I try to utilize the embedded iframe, I cannot sign in after I set up SSO. How can I resolve this issue?

A: Pax8 is currently working to support this functionality. For the time being you would still have to navigate to Pax8 in another window in the browser.