Azure AD SAML Support

This describes how you can set up SAML with Azure AD.

In Azure, you'll need to configure an Enterprise Application (Automox) and enable users for it. Please refer to the Azure docs for these steps as Microsoft's docs will be the most updated for Azure's process. But the basic outline is this:

Go to portal.azure.com

1. Create Enterprise Application (non-gallery app): https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-non-gallery-app
2. Create an organization (org) in the Automox console that you'll enable SAML on. In the console, go to **Settings > Security > Enable SAML**. (Settings can be found from the menu on the top right of the console.)
3. In Azure, configure single sign-on and select SAML. (The breadcrumbs to get here are **Enterprise Application > Automox > Single sign-on.**)
4. In Azure, on the "**Set up Single Sign-On with SAML**" page, edit the "**Basic SAML Configuration**" and change the URLs to point to staging and your org. The mapping is as follows:
    - From the Automox console, copy and paste into Azure -- and remember to modify the URL to point to staging:
        i. Automox Entity ID > Identifier (Entity ID)
        ii. Automox ACS URL > Reply URL (Assertion Consumer Service URL)
        iii. Automox Dashboard URL including org id > Relay State. For example: https://console.automox.com/dashboard?o=20171
    - In Automox, edit the SAML config. In Azure "SAML Signing Certificate" download the "Certificate (Base64)" and open it with a basic text editor (like Sublime or Text Edit) to get the x509 > paste into the x509 field in the Automox console.
    - From Azure, copy and paste from the "Set up Automox" section (where "Automox" is whatever you named your Enterprise Application in Azure)
        i. Login URL > Login URL
        ii. Azure AD Identifier > Entity ID
        iii. Logout URL
    - Save SAML config in AX
5. Set up Azure Active Directory
    - Create a tenant > Azure Active Directory
    - On Configuration > name it and set a domain name like "Automox" > Create
6. Create Azure AD users
    - In Azure Active Directory > Manage menu on left > Users
    - + New User
    - Create user option > set User Name and select the AD domain you created (this should be auto-filled)
    - Set the name, First Name, and Last Name fields

    - Create
7. Enable Automox (your test Enterprise App) to be seen in user's app launcher (from: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/access-panel-collections)
    - Azure Active Directory > Manage menu on left, click User Settings
    - "User feature previews" section > click Manage user feature preview settings
    - "Users can use preview features for My Apps" > choose "All"
8. Enable AD users to access Automox within Azure
    - Manage menu on left > Enterprise Applications > Automox (or whatever you called your test enterprise app) > In the Getting Started section, click "Assign users and groups"
    - + Add User > Users
    - Select the test user(s)
    - Click Assign (bottom left)

Notes about User Provisioning

The workflow to test user provisioning is as follows:

Follow all of the previously described steps. The test user exists in Azure AD but does not already exist in the AX org. To automatically provision a user, the "(Optional) Provision New Users" check box must be selected in the Automox SAML configuration modal. Then do as follows:

- The user must log in to https://myapplications.microsoft.com/
- If there is a banner that says "An updated My Applications experience is available " click "Try it"
- Automox should appear as a tile > Click it to launch Automox

If you do not want to go the User Provisioning route, you can invite the test user to your Azure org as normal. Accept the invitation as normal. On later logins, when the user enters their SAML-connected email in the login screen they should be redirected to the SAML auth workflow.