Authenticating using JumpCloud Single Sign-On (SAML)

- Parallels Secure Workspace

Resolution

In this guide, "the user's UPN" refers to the user principal name of a user on the LDAP server (e.g. Active Directory) specified in the settings of the domain in Parallels Secure Workspace.

The approach is to add a custom attribute (in this example "upn") to the user's information in JumpCloud to store the user's UPN. A custom SAML username claim will be used so JumpCloud can pass on the UPN to the Parallels Secure Workspace.

If the UPN matches the email address configured in JumpCloud, there's no need to work with a custom attribute. Instead, the NameID claim could be configured to return the email address.

Using a custom attribute to store the UPN:

When signed in to JumpCloud as an administrator, for each user:

- Click on a user name.
- A window pops up with the user's details.
- In the **Details** section, scroll to the bottom to **Custom Attributes**.
- Click **[add new custom attribute]**.
- Enter:
    - **Attribute Name:** upn
    - **Attribute Value:** this should be the userprincipalname of the user in the LDAP that is specified for the Workspace domain.
- At the bottom, click **[Save user]**.

Setting up the SSO in JumpCloud:

- In the left navigation panel, click **SSO.**
- Click **[+ Add New Application]**.
- At the bottom, click the **[Custom SAML App]** button.
- A new window opens with these tabs. There are more settings, only the relevant ones are listed here.
    - **General Info**
        - **Application Information**
            - **Display** Label: Workspace (or any other clear identification of the Workspace).
    - **SSO**
        - **IdP Entity ID:** Workspace
        - **SP Entity ID:** Workspace (Should be the same as Entity ID in Parallels Secure Workspace).
        - **ACS URL:** https://<workspace_env>/api/saml/
        - **Login URL:** https://<workspace_env>
        - **Attributes**
            - **User Attributes:**
                - Add a new line with:
                    - **Service Provider Attribute Name:** upn
                    - **JumpCloud Attribute Name:** upn (enter manually, it's not in the dropdown).
    - **User Groups**

◊ Add all relevant user groups (by default: All Users).

- Click **[Activate]** to create this custom SAML App.

In the SSO overview (accessed from the left navigation pane) on JumpCloud, the newly configured application should be visible.

- Click on the name to see the details and see similar tabs as above.
- Navigate to **SSO**.
- Click **[Export Metadata]**.

In Parallels Secure Workspace:

- Navigate to **System Settings > Configure > User Connector > Federated Authentication.**
  - **Type:** Pre-Authentication (or Single Sign-On, but this article does not explain the extra settings that are generic).
  - **Protocol:** SAML
  - **Entity Id:** Workspace (Should match SP Entity ID in JumpCloud)
  - **Metadata Type:** Mind that URL does not seem to work with JumpCloud. Instead, upload the federation XML metadata file that was downloaded from JumpCloud before.
  - **Single Logout:** As preferred.
  - **Username Claim:** upn
  - **Display Name Claim:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
  - **Workspace URL:** the FQDN (host header) of the Workspace domain.
  - Click **[Apply]**.
