Using Microsoft Active Directory Federation Services to sign in to the Workspace (SAML)

- Parallels Secure Workspace

Resolution

Configuring Microsoft Active Directory Federation Services (ADFS)

On an ADFS server:

1. Open **Server Manager**.
2. Navigate to **Tools > AD FS Management**.
3. In the left navigation pane, navigate to **AD FS > Relying Party Trusts**.
4. In the right **actions** pane, click **Add Relying Party Trust...** .
5. A wizard will start.
    1. Welcome: Pick **Claims aware** and press **[Start]**.
    2. Select Data Source: Pick "Enter data about the relying party manually". Click **[Next]**.
    3. Specify Display Name: Enter a name of your choice, e.g. Workspace. Click **[Next]**.
    4. Configure Certificate: Nothing to do. Click **[Next]**.
    5. Configure URL:
        1. Check "**Enable support for the SAML 2.0 WebSSO protocol**".
        2. For the "**Relying party SAML 2.0 SSO service URL**":
           Specify https://<*workspace_env*>/api/saml/ (Replace <*workspace_env*> with the FQDN of the Workspace).
    6. Configure Identifiers: Specify a name (keep this value in mind, it needs to be entered in Workspace later as "entity ID") for the "**Relying party trust identifier**" (e.g. Workspace) and click **[Add]**.
    7. Choose Access Control Policy: Nothing to do. Click **[Next]**.
    8. Ready to Add Trust: Nothing to do. Click **[Next]**.
    9. Keep "Configure claims issuance policy for this application" checked. Click **[Close]**.
6. The claims issuance policy window should be visible. Mind that this may be somewhere in the background.
   If it's not visible, select your Relying Party and in the **Actions** pane, click **Edit Claim Issuance Policy...** .
    1. Click **[Add Rule]**.
        1. Claim rule template: **Send LDAP Attributes as Claims**. Click **[Next]**.
        2. Configure:
            1. Claim rule name: UPN + Display Name.
            2. Attribute Store: Active Directory
            3. Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	UPN
Display-Name	Given Name

            4. Click **[Finish]**.
    2. Click **[Add Rule]**.
        1. Claim rule template: **Transform an Incoming Claim**. Click **[Next]**.
        2. Configure:
            1. Claim rule name: UPN.
            2. Incoming claim type: UPN.
            3. Outgoing claim type: Name ID.
            4. Outgoing name ID format: Email.

5. Select the "Pass through all claim values" radio button.
3. Click **[Finish]**.

Configuring Parallels Secure Workspace

In **System Settings**, after making sure the relevant domain is selected in the top left:

Navigate to **System Settings > Configure > User Connector.**

1. Under **Reverse Proxy,** verify the **default login host header** is set to the host header which end users will use to access this Workspace domain (e.g. workspace.somedomain.org).
2. Under **Federated Authentication:**
    1. Set the **Type** to **Pre-Authentication.** (Note: This article is limited to the instructions to set up Pre-Authentication, but these steps are the same when setting up Single Sign-On (SSO). SSO requires additional steps though.)
    2. Set the **Protocol** to **SAML.**
        ◊ Entity ID: Use the value used when configuring the Relying Party on the ADFS.
    3. Set the **Metadata Type** to **XML**. It's possible to point to the federation metadata XML. However, the SSL certificate needs to be trusted by Parallels Secure Workspace. In most scenarios when using ADFS, this is not the case. If opting to do so, make sure to allow untrusted certificates (**System Settings > Global > Domains > specific Workspace domain > Allow untrusted servers: Pre-Auth / SSO metadata**).
    4. Manually grab this by navigating to https://<*adfs_fqdn*>/federationmetadata/2007-06/federationmetadata.xml (Replace the <adfs_ffqdn> variable with the FQDN of the ADFS).
    Upload this file under **Metadata XML**.
    5. Choose the preferred option for **Single Logout**.
    6. Mind to change the **Username claim** to http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
    7. **Display Name Claim:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
    8. Workspace URL: This will be used to construct the ACS URL for the Authentication Provider. In most scenarios, this is the host header that end users will use to access this Workspace domain.
    9. Click **[Apply]**.

Note: the URLs will update each time the "Workspace URL" value has been saved.
