Recast

How to configure SSO with AD FS

Last Modified on 04.16.26

This article describes how to configure Active Directory Federation Services (AD FS) as an authentication source for Active Directory or Microsoft Entra ID (Azure AD), by delegating the authentication responsibility from the Application Workspace Server to the AD FS server.

Application Workspace supports OAuth2-based authentication in combination with an LDAP Active Directory or Microsoft Entra ID (Azure AD) identity source to achieve SSO with other applications. When activated, Application Workspace will no longer handle authentication using its login screen but will delegate authentication to the OAuth2 token service.

When multiple identity sources are visible to the user for login, Application Workspace will switch to the OAuth2 service after entering the username in the login screen.

For prerequisites, see Microsoft documentation.

Example

For this example, we will use the `workspace.recastsoftware.com` URL. This URL should be replaced by the FQDN of your Application Workspace.

PowerShell and Server Manager

1. On the AD FS server, open PowerShell with the AD FS module.

2. Execute the following command to define the Application Workspace endpoint:

```
Add-ADFSClient -Name "RecastSoftware" -ClientId "RecastSoftware" -RedirectUri "https://workspace.recastsoftware.com/api/auth/token/end" -LogoutUri "https://workspace.recastsoftware.com/logout.html"
```

For older AD FS versions, it might be required to skip the `-LogouUri` parameter.

3. Open Server Manager and navigate to **AD FS** > **Tools** > **AD FS Management** > **Relying Party Trusts**.
4. Start the Add Relying Party Trust wizard and configure the following:
   - At the **Welcome** step, choose **Claims aware**, and then click **Start**.
   - At the **Select Data Source** step, choose **Enter data about the relying party manually** and then click **Next**.
   - At the **Specify Display Name** step, enter a display name to identify the trust, for example *RecastSoftware* and then click **Next** until you reach the **Configure Identifiers** step.
   - At the **Configure Identifiers** step, in the **Relying party trust identifier** field, add "RecastSoftware".

5. Right-click on the newly created trust to open the context menu, and select **Edit Claim Issuance Policy**.

6. In the **Edit Claim Issuance Policy** dialog box that opens, in the **Issuance Transform Rules** tab click **Add Rule**.

7. In the **Add Transform Claim Rule Wizard** that opens, configure the following:
   - At the **Choose Rule Type** step, under **Claim rule template**, select *Send LDAP Attributes as Claims* and then click **Next**.
   - At the **Configure Claim Rule** step configure:
     - **Claim rule name** *UPN*

- **Attribute store** *Active Directory*
- Map the **LDAP attribute** *User-Principal-Name* to **Outgoing claim type** *upn*

8. Click **Finish**. In the **Edit Claim Rules** dialog box, click **OK** to save the new rule.
   For more information, see Microsoft documentation.

9. Execute the following command in PowerShell to associate the workspace OAuth2 client with the relying party trust that you just created at the previous steps:

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier "RecastSoftware" -ServerRoleIdentifier "RecastSoftware"
```

Application Workspace

1. Open Application Workspace, navigate to **Manage** > **Authentication** > **Identity Sources** and open the identity source that needs to use AD FS for authenticating.
2. Go to the **Authentication** screen, enable the *Federated* option by selecting its checkbox and then click **Edit**.
3. In the **Edit authentication** dialog box that opens, configure the following:
   - **Client ID** *RecastSoftware*
   - **Resource** *RecastSoftware*
   - **Redirect URI** `https://workspace.recastsoftware.com/api/auth/token/end`
   - **Token URI** `https://adfs.recastsoftware.com/adfs/oauth2/token`
   - **Authorization URI** `https://adfs.recastsoftware.com/adfs/oauth2/authorize`
   - **Logout URI** `https://adfs.recastsoftware.com/adfs/ls/?wa=wsignout1.0`

> AD FS 2019 – Content Security Policy
> AD FS 2019 (version 10) and later have a new security policy that restricts the type of content loading on the AD FS pages. A default configuration, will result in not loading the logout URLs that have been configured during an AD FS logout. For more information, see Microsoft documentation.