



VOSS Automate Technote - Single Sign On (SSO) with Microsoft Entra

Nov 23, 2023

Copyright © 2023 VisionOSS Limited. All rights reserved.

Contents

Overview	2
One-time VOSS Automate Platform Setup	2
Microsoft Entra / VOSS Automate SSO Configuration	3

Overview

This technote article will take you step-by-step through one example of configuring VOSS Automate and Microsoft Entra for SSO.

Note: Microsoft has changed the name of Azure Active Directory to Microsoft Entra.

The VOSS Automate system supports Single Sign-on (SSO) via the SAML v2 protocol, acting as a service provider in the SAML authentication architecture with service provider-initiated user authentication against a SAMLv2 Identity Provider (IdP).

Although configuration information for every possible IdP is out of scope for VOSS Automate documentation, SSO integration with Microsoft Entra (formerly Azure Active Directory) is one common use case for which it may be worthwhile to provide some guidance.

Note: We've published the complete steps here as a technote to describe the setup in both VOSS Automate and Microsoft Entra, as at Automate v21.4-PB3. Since we cannot guarantee that these steps will remain the same on Microsoft Entra, please verify the steps for Microsoft Entra in the [Microsoft documentation](#).

To enable SSO integration for Microsoft Entra, you will need to complete the following tasks:

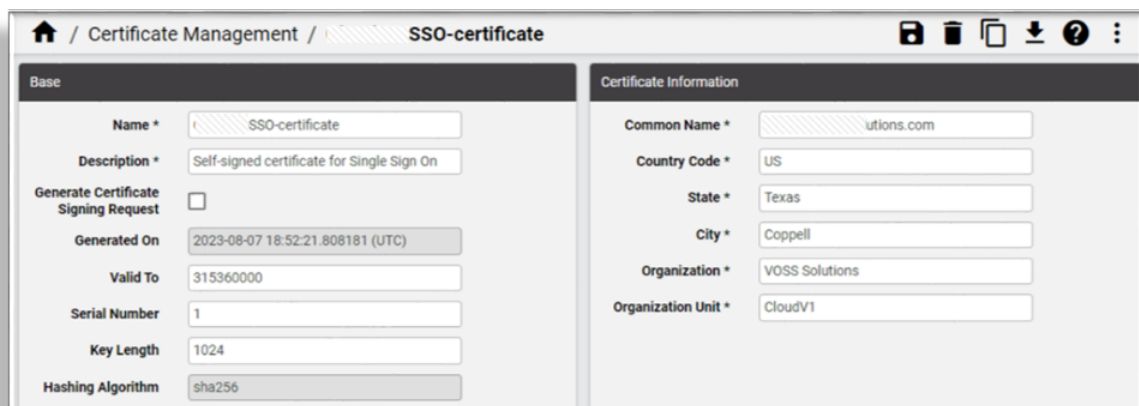
1. One-time VOSS Automate Platform Setup
2. Microsoft Entra / VOSS Automate SSO Configuration

One-time VOSS Automate Platform Setup

VOSS Automate can be configured for a single customer or as a multi-tenant (and multiple IdP) system. In either case there is a required one-time procedure for the VOSS Automate platform itself.

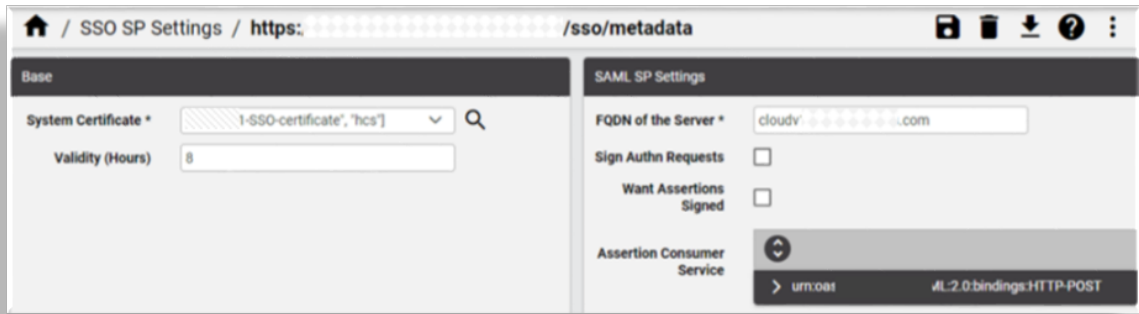
Note: You must perform this procedure as a user with the *HcsAdmin* role.

1. Create either a self-signed or a third-party-signed certificate, depending on your security requirements. For details, see [SSO Certificate Management](#).



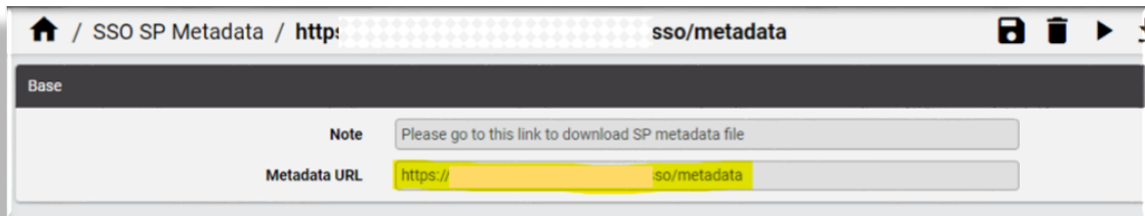
The screenshot displays the 'Certificate Management' interface for an 'SSO-certificate'. The interface is divided into two main sections: 'Base' and 'Certificate Information'. The 'Base' section includes fields for Name (SSO-certificate), Description (Self-signed certificate for Single Sign On), a checkbox for 'Generate Certificate Signing Request', 'Generated On' (2023-08-07 18:52:21.808181 (UTC)), 'Valid To' (315360000), 'Serial Number' (1), 'Key Length' (1024), and 'Hashing Algorithm' (sha256). The 'Certificate Information' section includes fields for 'Common Name' (utions.com), 'Country Code' (US), 'State' (Texas), 'City' (Coppell), 'Organization' (VOSS Solutions), and 'Organization Unit' (CloudV1).

2. Complete steps 1 - 6 of SSO Service Provider Configuration.



3. Choose **Single Sign On > SSO SP Metadata**

4. Copy the Metadata URL and paste it into your browser, then save the metadata.xml file to your computer. You will upload this file to each IdP that you configure with this VOSS Automate platform.



Microsoft Entra / VOSS Automate SSO Configuration

To configure SSO for Microsoft Entra and VOSS Automate, you will need to complete the following tasks, in either VOSS Automate, or in Microsoft Entra, as shown in the table.

The table describes the steps in this workflow:

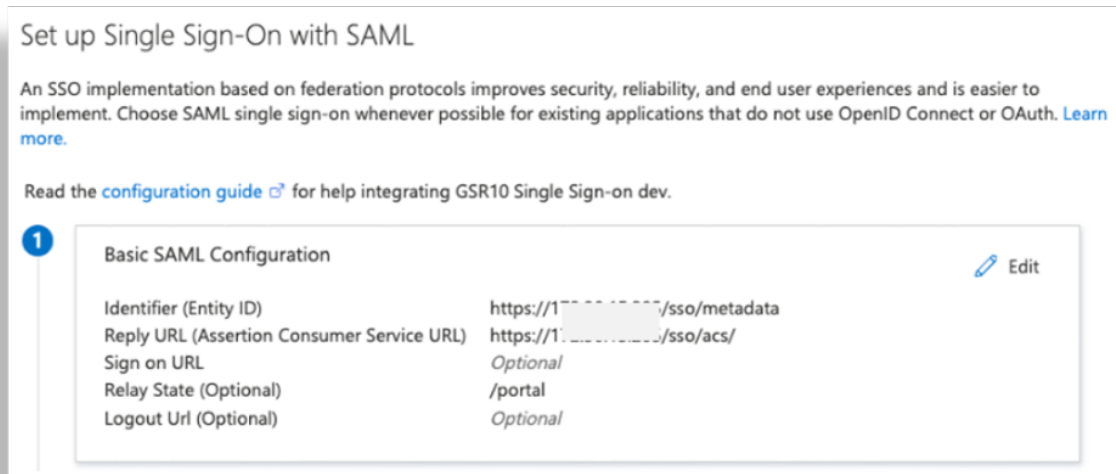
Perform this task in ...	Steps
Microsoft Entra	Step 1. Basic SAML configuration: Create Entra application and upload VOSS Automate metadata file. To configure SSO in Microsoft Entra you create an Enterprise Application in Entra corresponding to VOSS Automate. In this application, you will configure SSO for VOSS Automate.
Microsoft Entra	Step 2. Configure attributes and claims. VOSS Automate requires that the IdP release an attribute named <i>uid</i> . The value of the <i>uid</i> attribute must uniquely identify a single instance of the data/User model in VOSS Automate. For example, you could use a user's email address to uniquely identify that user. This task involves adding a new claim in Microsoft Entra, providing the <i>uid</i> as the claim name, then setting the name format as <i>attribute</i> , and choosing the source attribute, for example, <i>user.mail</i> .
Microsoft Entra	Step 3. Download metadata from Entra Enterprise Application. Download the Entra Enterprise Application metadata, and save the XML file to your local computer.
VOSS Automate	Step 4. Upload Entra Enterprise Application metadata and configure VOSS Automate SSO Identity Provider
Microsoft Entra	Step 5. Assign users to the Enterprise Application. For users to be able to use SSO to sign into VOSS Automate they must be assigned to the VOSS Automate Enterprise Application. You can assign individual users, one at a time, or you can assign MS-365 Groups to the application. This task involves adding users or MS-365 groups to the Enterprise Application you created. These users and groups will then be able to sign in to VOSS Automate using their Microsoft credentials.
VOSS Automate	Step 6. Assign VOSS Automate administrative roles

3.1 Basic SAML configuration: Create Entra application and upload VOSS Automate metadata file

To configure SSO in Microsoft Entra you create an *Enterprise Application* in Entra corresponding to VOSS Automate. In this application you will configure SSO for VOSS Automate.

1. Sign into <https://entra.microsoft.com> as an administrator with sufficient permissions to create an Enterprise Application.
2. Choose **Applications > Enterprise applications**.
3. Select **New application**, then **Create your own application**.
4. Give your application a name, for example *VOSS Automate Single Sign On*, then select the **Integrate any other application...** radio button. Select **Create**.
5. Under **Manage** select **Single sign-on**.
6. Under **Select a single sign-on method** select **SAML**.
7. On the SAML-based Sign-on blade select **Upload metadata file**. Upload the `metadata.xml` file you saved on your computer earlier.

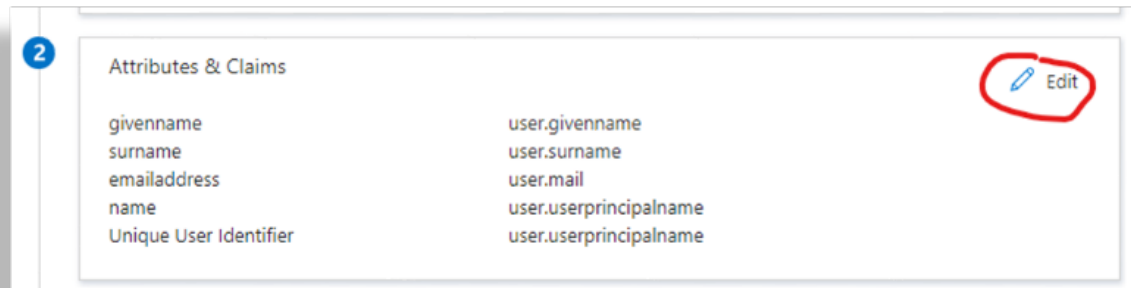
8. On the **Basic SAML Configuration** blade, select **Edit**, then set **Relay State (Optional)** to `/portal`, then select **Save**. All other parameters should be left with their default values.
9. At the **Test single sign-on with VOSS Automate Single Sign On** prompt select **No, I'll test later**.



3.2 Configure Attributes and claims

VOSS Automate requires that the IdP release an attribute named `uid`. The value of the `uid` attribute must uniquely identify a single instance of the `data/User` model in VOSS Automate. In this example we will use the user's email address to uniquely identify the user.

1. On the Entra **Set up Single Sign-On with SAML** blade select **Edit** under **Attributes & Claims**.



2. Select **Add new claim**

Attributes & Claims ...

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ***

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

Advanced settings

- At **Manage claim**, in the **Name** field, fill out the value, *uid*.

Note: This value must be lowercase. The field is case-sensitive.

- At **Choose name format** select the **Attribute** radio button and in the **Source attribute** field select **user.mail**.

Manage claim ...

Save Discard changes | Got feedback?

Name * uid

Namespace Enter a namespace URI

Choose name format

Source * Attribute Transformation Directory schema extension

Source attribute * user.mail

Claim conditions

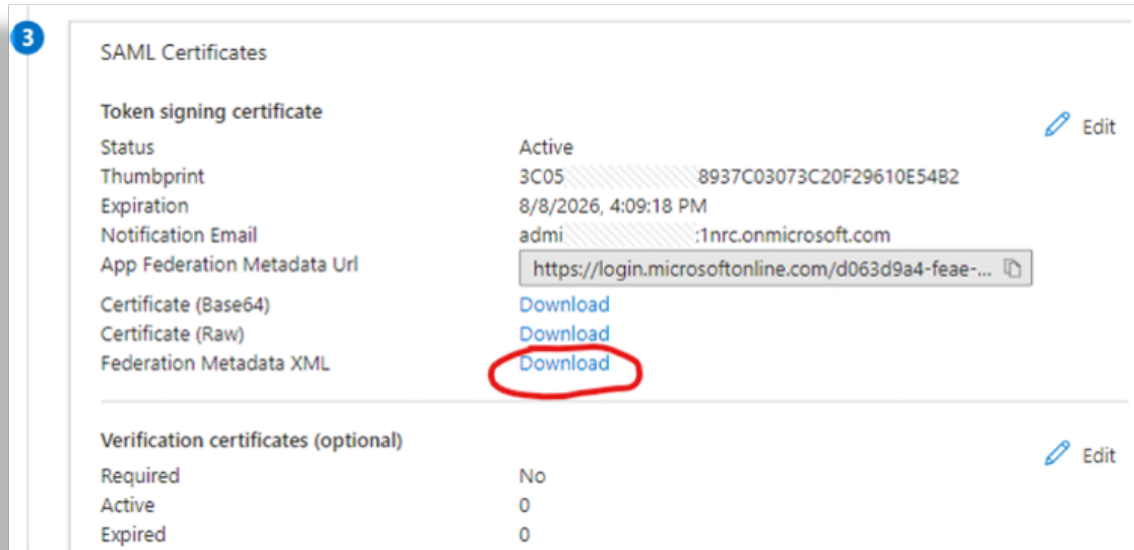
Advanced SAML claims options

- Click **Save**, then close out of the **Attributes & Claims** blade.

3.3 Download metadata from Entra Enterprise Application

We previously downloaded the metadata from VOSS Automate and uploaded it into the Single sign-on configuration for the Entra Enterprise Application. We will now do the reverse: download the Entra Enterprise Application metadata and, in the next step, upload that data into VOSS Automate.

1. On the **SAML-based Sign-on** configuration blade, under **SAML Certificates**, select the **Download** link next to **Federation Metadata XML**. Save the XML file to your computer.



3.4 Upload Entra Enterprise Application metadata and configure VOSS Automate SSO Identity Provider

In this step we'll provision VOSS Automate with the details of the IdP with which we're integrating.

VOSS Automate provides several possible configuration options, depending on how you want to implement SSO. You can associate an IdP with a particular hierarchy node, or with a particular hierarchy node and everything beneath that node. With this scheme, VOSS Automate can accommodate the following scenarios simultaneously:

- An IdP configured only at the provider level, providing Single Sign-On for provider administrators with authentication by the provider's IdP.
- An IdP configured at the customer level and below, providing Single Sign-On for customer administrators with authentication by each customer's own IdP.

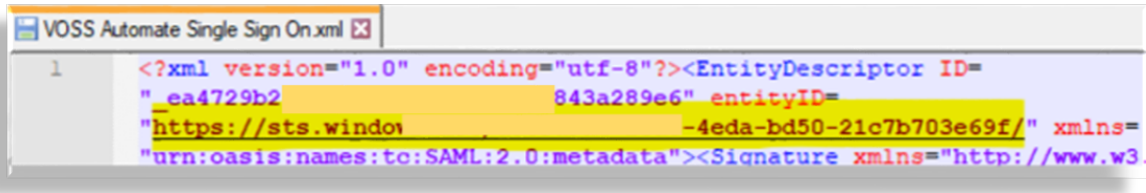
Note: Only one IdP can be configured for a specific hierarchy node.

In this example we will provision VOSS Automate with the details of a customer's IdP, allowing that customer's administrators to be authenticated by their own IdP.

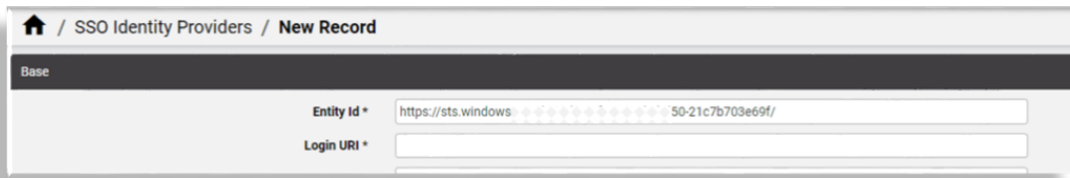
1. Log into VOSS Automate as a Provider administrator and set your hierarchy to the node where you want the IdP to be associated. In this example, we will set the hierarchy to the customer level.
2. Choose **Administration & Audit Tools > File Management**, then click **Add**.

3.4 Upload Entra Enterprise Application metadata and configure VOSS Automate SSO Identity Provider

3. Select the metadata XML file you downloaded from Microsoft Entra in the previous section, then click **Save**.
4. In a text editor, open this XML file. Near the top you will find an element named **entityID**. Copy that value (everything inside the quotes) to your clipboard.
5. Choose **Provider Configuration > SSO Identity Providers**, then click **Add**.
6. Paste the **entityID** value from your clipboard into the VOSS Automate **Entity ID** field.



```
1 <?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID=
"ea4729b2843a289e6" entityID=
"https://sts.windows-4eda-bd50-21c7b703e69f/" xmlns=
"urn:oasis:names:tc:SAML:2.0:metadata"><Signature xmlns="http://www.w3
```



SSO Identity Providers / New Record

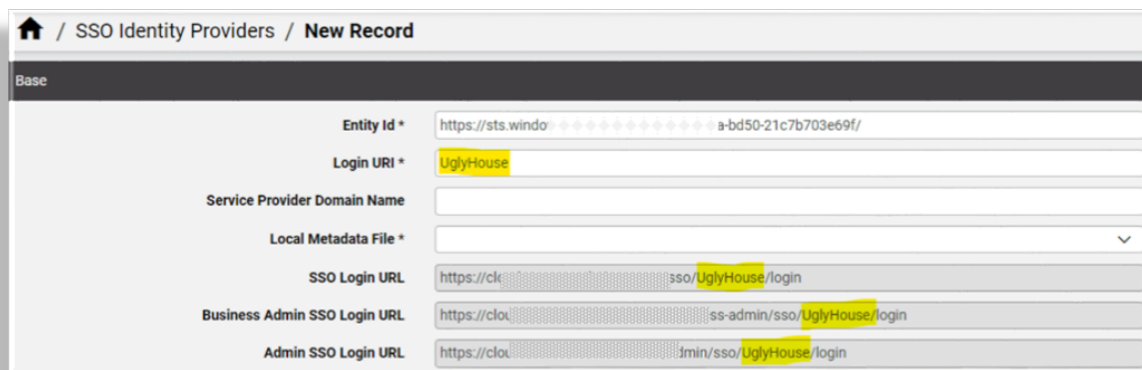
Base

Entity ID *

Login URI *

7. In the **Login URI** field, enter a name identifying, in this case, the customer.

Note: This is just a text string that will become part of the login URL for that customer's administrators, which makes the URL unique for that customer.



SSO Identity Providers / New Record

Base

Entity ID *

Login URI *

Service Provider Domain Name

Local Metadata File *

SSO Login URL

Business Admin SSO Login URL

Admin SSO Login URL

8. In the **Local Metadata File** field select the XML file you just uploaded.
9. In the **User lookup field** select **email** (which should uniquely map to the claim attribute **user.mail** that we set up earlier).
10. In this example, we'll set the **Authentication Scope** field to **Current hierarchy level and below**, meaning that any administrators at the current hierarchy or below will authenticate with this customer's IdP.

11. For **User Sync Type**, we'll select **All users** in this example.

The screenshot shows the configuration page for an SSO Identity Provider in Microsoft Entra. The page is titled "Ugly House (Customer) VOSS Automate". The URL in the address bar is "https://sts.windows.net/d063d9a4-feae-4eda-bd50-21c7b703e69f/". The configuration fields are as follows:

- Entity ID ***: https://sts.wi...-bd50-21c7b703e69f/
- Login URI ***: UglyHouse
- Service Provider Domain Name**: (empty)
- Local Metadata File ***: ["VOSS Automate Single Sign-On"; Direct.Ugly House"]
- Note**: Navigate to https://...ss-solutions.com/sso/UglyHouse/metadata to download VOSS Automate metadata to be uploaded to the IDP.
- SSO Login URL**: https://clou...n/sso/UglyHouse/login
- Business Admin SSO Login URL**: https://clou...n/business-admin/sso/UglyHouse/login
- Admin SSO Login URL**: https://cl...o/UglyHouse/login (highlighted in yellow)
- User lookup field ***: email
- Authentication settings**:
 - Authentication Scope**: Current hierarchy level and below
 - User Sync Type**: All users

12. Click **Save**.

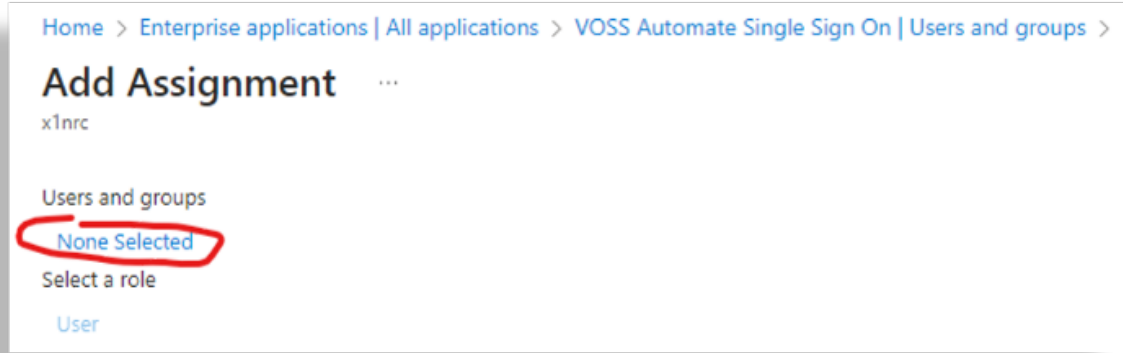
The two-way trust relationship between VOSS Automate and the Enterprise Application configured in Microsoft Entra is now established.

13. Copy the Admin SSO Login URL from this record. This is the URL you will publish to your SSO-enabled users, and the URL they will use to sign in to VOSS Automate.

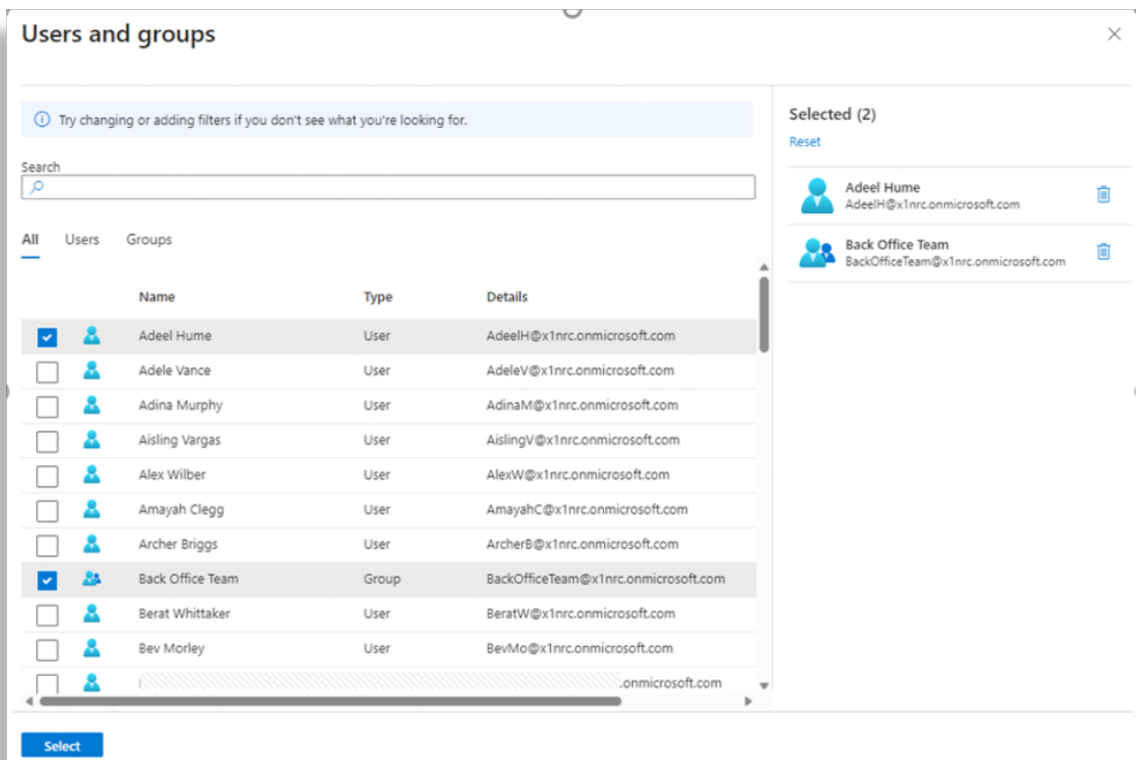
3.5 Assign users to the Enterprise Application

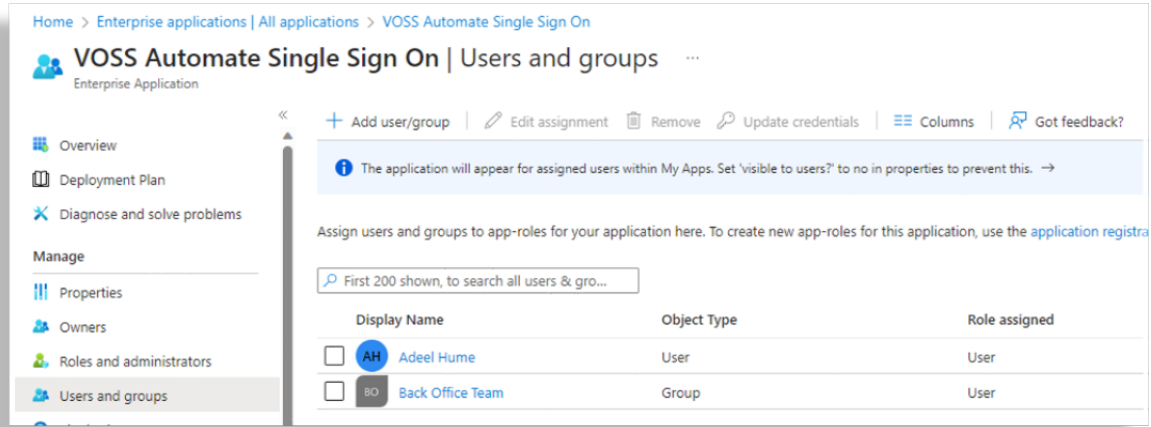
For users to be able to use SSO to sign into VOSS Automate they must be assigned to the VOSS Automate Enterprise Application. You can assign individual users, one at a time, or you can assign MS-365 Groups to the application.

1. In Microsoft Entra navigate to **Applications > Enterprise Applications**, then select the application you created previously.
2. Under **Manage**, select **Users and groups**.
3. Select **Add user/group**.
4. On the **Add Assignment**, blade select the link under **Users and groups**.



5. On the **Users and groups** blade, select the checkboxes beside one or more users or MS-365 groups. Click **Select**, then **Assign**.





6. In the example above, Adeel Hume and any direct members of the Back Office Team will be able to sign into VOSS Automate using their Microsoft credentials.

3.6 Assign VOSS Automate administrative roles

The users you assigned to the Enterprise Application in the previous section must be added to VOSS Automate with an administrative role.

- If the users already exist by virtue of a device/msgraph/MsolUser data sync, go to **Subscriber Management > Users** to confirm.
- If the users do not yet exist, you can add them manually.

To add users manually:

- Go to **Role Management > Admins**, then click **Add**.

Ensure that the field you're using to uniquely identify the user (email address, in this example) is provisioned correctly.

- Assign an appropriate administrative role to the user.

The user should now be able to sign into VOSS Automate and authenticate with their own IdP.