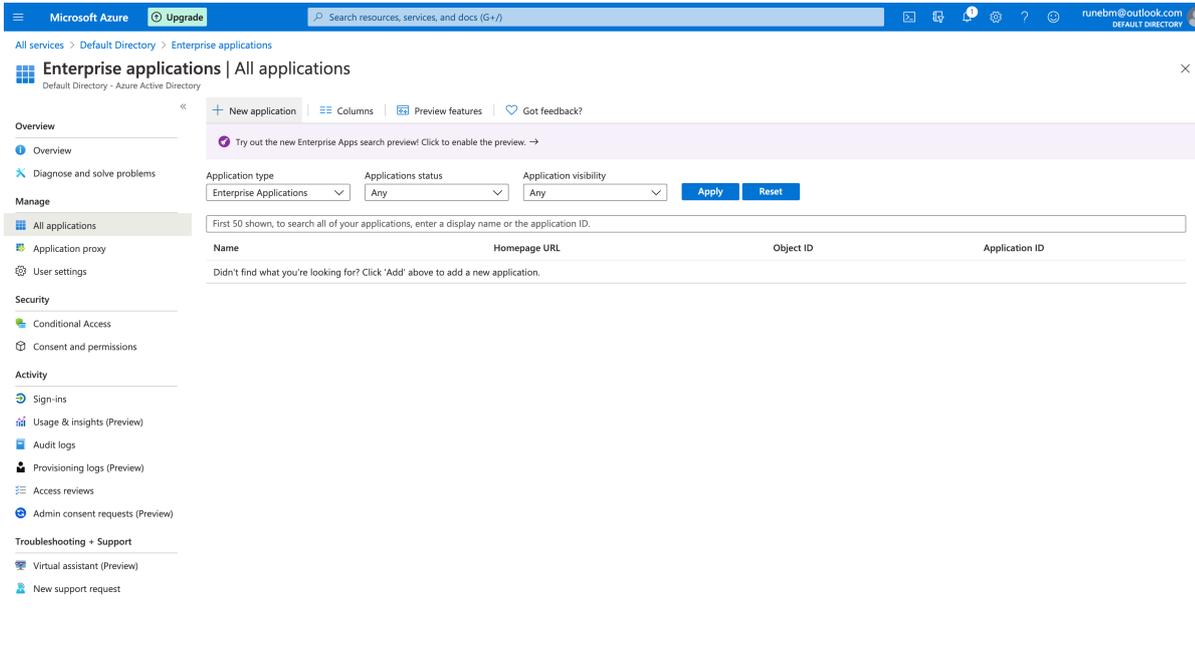
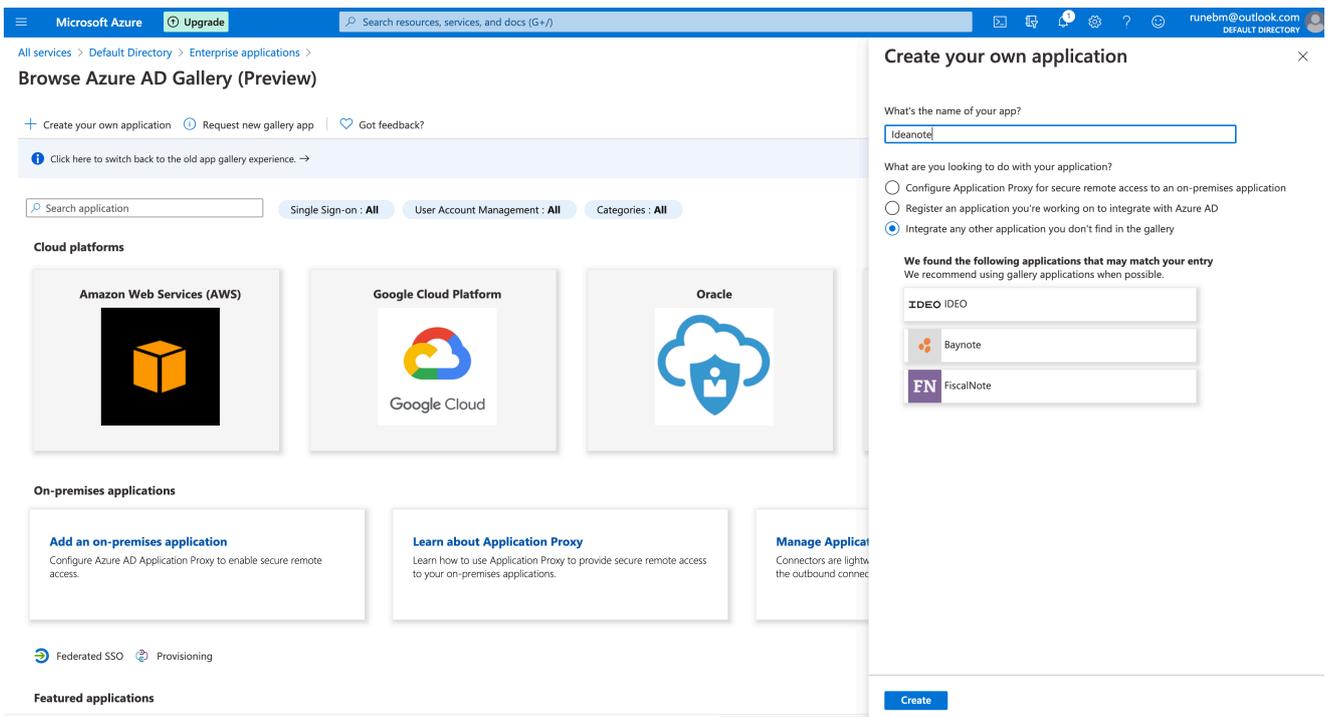


Integrating Ideanote with Azure AD

1. Go to "Enterprise applications" > "All applications" > "New application"



2. Press "Create your own application", name it and create it



3: Click "Set up single sign on"

The screenshot shows the Microsoft Azure portal interface for an application named 'Ideanote'. The top navigation bar includes 'Microsoft Azure', an 'Upgrade' button, a search bar, and the user's profile 'runebm@outlook.com'. The breadcrumb trail is 'All services > Default Directory > Enterprise applications > Browse Azure AD Gallery (Preview) > Ideanote | Overview'. The left sidebar contains a navigation menu with categories like 'Overview', 'Deployment Plan', 'Manage', 'Properties', 'Owners', 'Roles and administrators (Preview)', 'Users and groups', 'Single sign-on', 'Provisioning', 'Application proxy', 'Self-service', 'Security', and 'Activity'. The main content area is titled 'Properties' and includes fields for 'Name' (Ideanote), 'Application ID' (f4295c1a-6ee5-424a-89...), and 'Object ID' (12c818c7-59c0-4375-a3...). Below this is the 'Getting Started' section with five steps: 1. Assign users and groups, 2. Set up single sign on (highlighted with an orange border), 3. Provision User Accounts, 4. Conditional Access, and 5. Self service. A 'What's New' section at the bottom contains two items: 'Sign in charts have moved!' and 'Delete Application has moved to Properties'.

4: Click "Edit" on "Basic SAML Configuration" and enter the following:

Identifier: <https://api.ideanote.io/sso/saml/metadata.xml>

Reply URL: <https://api.ideanote.io/sso/saml/callback>

The screenshot shows the 'Basic SAML Configuration' page in the Azure portal. At the top left is a 'Save' button. The page contains several configuration fields: 'Identifier (Entity ID)' with a description 'The default identifier will be the audience of the SAML response for IDP-initiated SSO' and a value field containing 'https://api.ideanote.io/sso/saml/metadata.xml'; 'Reply URL (Assertion Consumer Service URL)' with a description 'The default reply URL will be the destination in the SAML response for IDP-initiated SSO' and a value field containing 'https://api.ideanote.io/sso/saml/callback'; 'Sign on URL' with a placeholder 'Enter a sign on URL'; 'Relay State' with a placeholder 'Enter a relay state'; and 'Logout Url' with a placeholder 'Enter a logout url'. Each value field has a green checkmark icon on the right, indicating the input is valid.

5: Download the Federation Metadata XML

3

SAML Signing Certificate Edit

Status	Active
Thumbprint	17E9B27BD037420AD722B75C232DD0A668A1DB6D
Expiration	1/21/2024, 12:22:58 PM
Notification Email	runebm@outlook.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/89c3ae41-c598-..."/>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

6: Assign users in Azure AD to the new application

7: Go to your Ideanote workspace settings and click "Advanced security" > "See or edit SSO settings" > "Upload IDP-metadata". Upload the Federation Metadata XML.

SSO Settings

SAML Single Sign On

[Download guide](#)

Upload IDP-metadata

[Upload IDP-metadata](#)

Certificate

MIIC8DCCA digAwIBAgIQYAYajTo3775HQUWany55hDANBgqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNybg

Entity ID

https://sts.windows.net/89c3ae41-c598-4880-a3cf-9e75aad3630a/

Login URL

https://login.microsoftonline.com/89c3ae41-c598-4880-a3cf-9e75aad3630a/saml2

Unauthorized Message

Sign request

Customize sign-in-button text

Azure AD

Customize sign-in-button icon

[Save](#)

Ideanote SAML service provider details

You'll need these to configure your Identity Provider to allow Ideanote access to your users.

8: Now SAML SSO has been set up successfully and can be tested by logging out of Ideanote. Be aware that IDP-initiated sign-on is not currently supported with Azure AD.

