

AzureAD: Setup SSO to G-Suite for free, and govern access! (Google Apps)



Matt Soseman (<https://social.technet.microsoft.com/profile/Matt+Soseman>) February 25, 2019

1 (<https://blogs.technet.microsoft.com/skypehybridguy/2019/02/25/azuread-setup-sso-to-g-suite-for-free-and-govern-access-google-apps/#comments>)

Did you know Azure Active Directory can provide Single Sign-On (SSO) to G-Suite (Google Apps)? In this blog, we will explore how to set this up from both the Azure AD side and also the G-Suite side.

Share 41 0 0

Once SSO is configured, consider creating policies for Conditional Access (<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>) to govern how G-Suite is accessed (e.g. only from a managed device, specific network, monitor for threats of the credentials such as for sale on the dark web, etc). For more information on G-Suite and Azure AD integration for SSO, see Tutorial: Azure Active Directory integration with G Suite (<https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/google-apps-tutorial>)

Note: SSO for up to 10 apps comes with the free version of AzureAD. For additional capability, P1 or P2 may be required. See Azure Active Directory pricing (<https://azure.microsoft.com/en-us/pricing/details/active-directory/>) for more information.

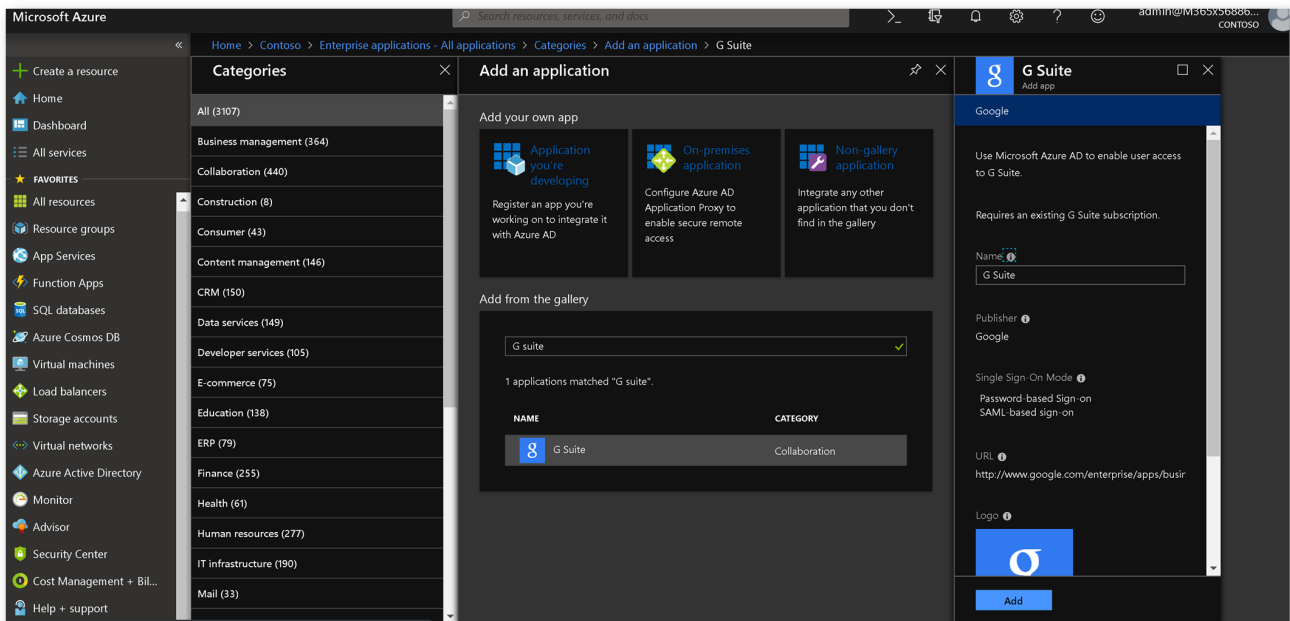
Important: Chromebooks can sign-in with Azure AD credentials, see this video (<https://youtu.be/qtVtTCr1Qcs>)! (and here (<https://support.google.com/chrome/a/answer/6060880>) for more information)

Also Important: Once SSO is enabled in G-Suite only Azure AD credentials will be authorized and all legacy credentials (i.e. G-Suite credentials) will not be authorized for sign-in. If the user is using a Windows 10 device that is AADJ, then they will not need to type in their password to access G-Suite, SSO from Win 10 will automatically be available.

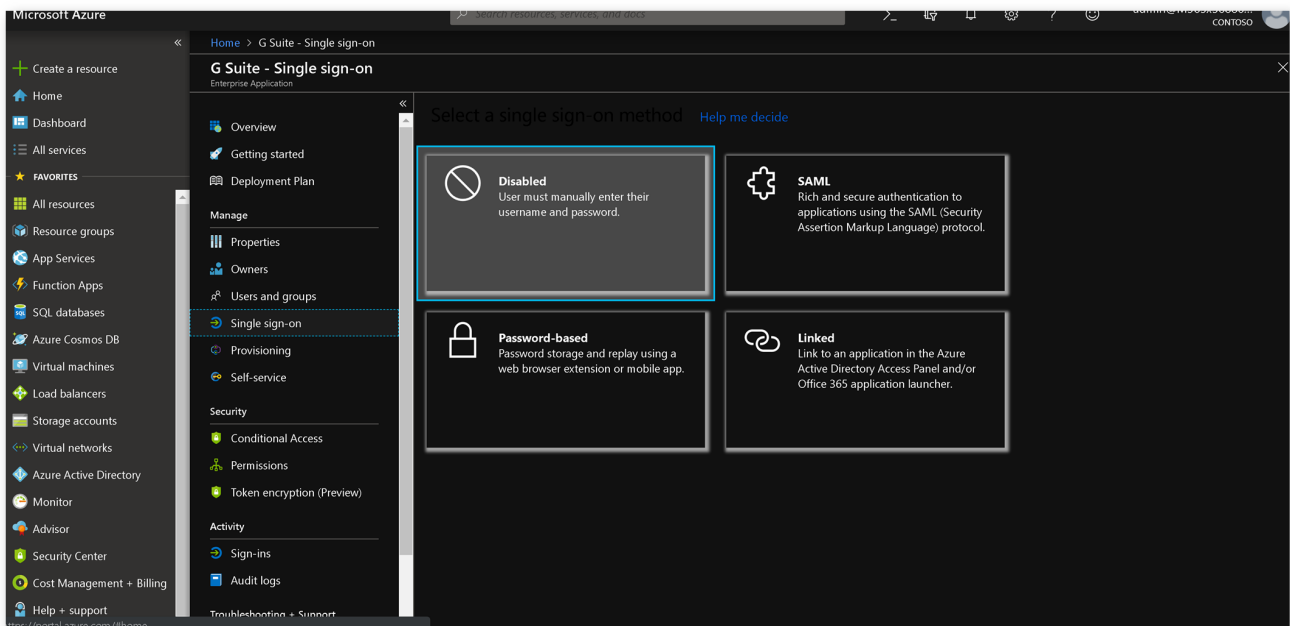
Let's begin!

Add G-Suite to Azure AD and configure it:

From within the Azure portal navigate to Azure Active Directory -> Enterprise Applications -> New Application and search for G Suite then click **Add**:



Once added, click *Single Sign-on* and click **SAML**



Edit the Basic SAML Configuration by clicking the pencil icon:

Home > G Suite - Single sign-on > SAML-based sign-on

G Suite - SAML-based sign-on

Enterprise Application

Change single sign-on mode Switch to the old experience Test this application

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating G Suite.

- Basic SAML Configuration**

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Optional
Sign on URL	Required
Relay State	Optional
Logout URL	Optional
- User Attributes & Claims**

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Signing Certificate**

Status	Active
Thumbprint	83F3D3D0D5CB0091B386AE7A01062D8A3A88F481
Expiration	2/24/2022, 2:56:44 PM

Configure using the following parameters:

Basic SAML Configuration

Save Upload metadata file

Identifier (Entity ID) (Required)

This value must be unique across all applications in your (Azure Active Directory) tenant. It should follow one of the patterns provided below the textbox.

google.com

google.com/a/soseman.org

Patterns: google.com, google.com/*, http://google.com, http://google.com/a/*

Reply URL (Assertion Consumer Service URL) (Optional)



The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML. It should follow one of the patterns provided below the textbox.

https://www.google.com/a/*

https://www.google.com

Patterns: https://www.google.com, https://www.google.com/a/*

Basic SAML Configuration

 Save  Upload metadata file

<https://www.google.com>

Patterns: <https://www.google.com>, https://www.google.com/a/*

Sign on URL (Required)

This URL contains the sign-in page for this application that will perform the service provider-initiated single sign-on. It should follow one of the patterns provided below the textbox.

<https://www.google.com/a/soseman.org/ServiceLogin?continue=https://mail.google.com> ✓

Patterns: <https://www.google.com/a/<your-domain>/ServiceLogin?continue=https://mail.google.com>,
<https://www.google.com/a/<your-domain>/ServiceLogin?continue=https://console.cloud.google.com>

Relay State (Optional)

Optionally, a SAML RelayState parameter can be provided. The RelayState instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout URL (Optional)

This URL is used to send the SAML Logout response back to the application.

✓

Click **Save**. For *User Attributes & Claims* click the pencil icon:

2

User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname



Add a new claim:

Manage user claims

* Name ✓

Namespace

Source ☒ Attribute ☐ Transformation

* Source attribute ▼

Go back to the main SAML SSO configuration page, and download the base64 certificate for **SAML Signing Certificate**:

SAML Signing Certificate

Status Active

Thumbprint [REDACTED]

Expiration [REDACTED], 2:56:44 PM

Notification Email [REDACTED]@onmicrosoft.com

App Federation Metadata Url

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Copy the following URLs to a scratch pad, we'll use these to configure G-Suite:

Set up G Suite

You'll need to configure the application to link with Azure AD.

Login URL

Azure AD Identifier

Logout URL

[View step-by-step instructions](#)

Setup G-Suite for SSO:

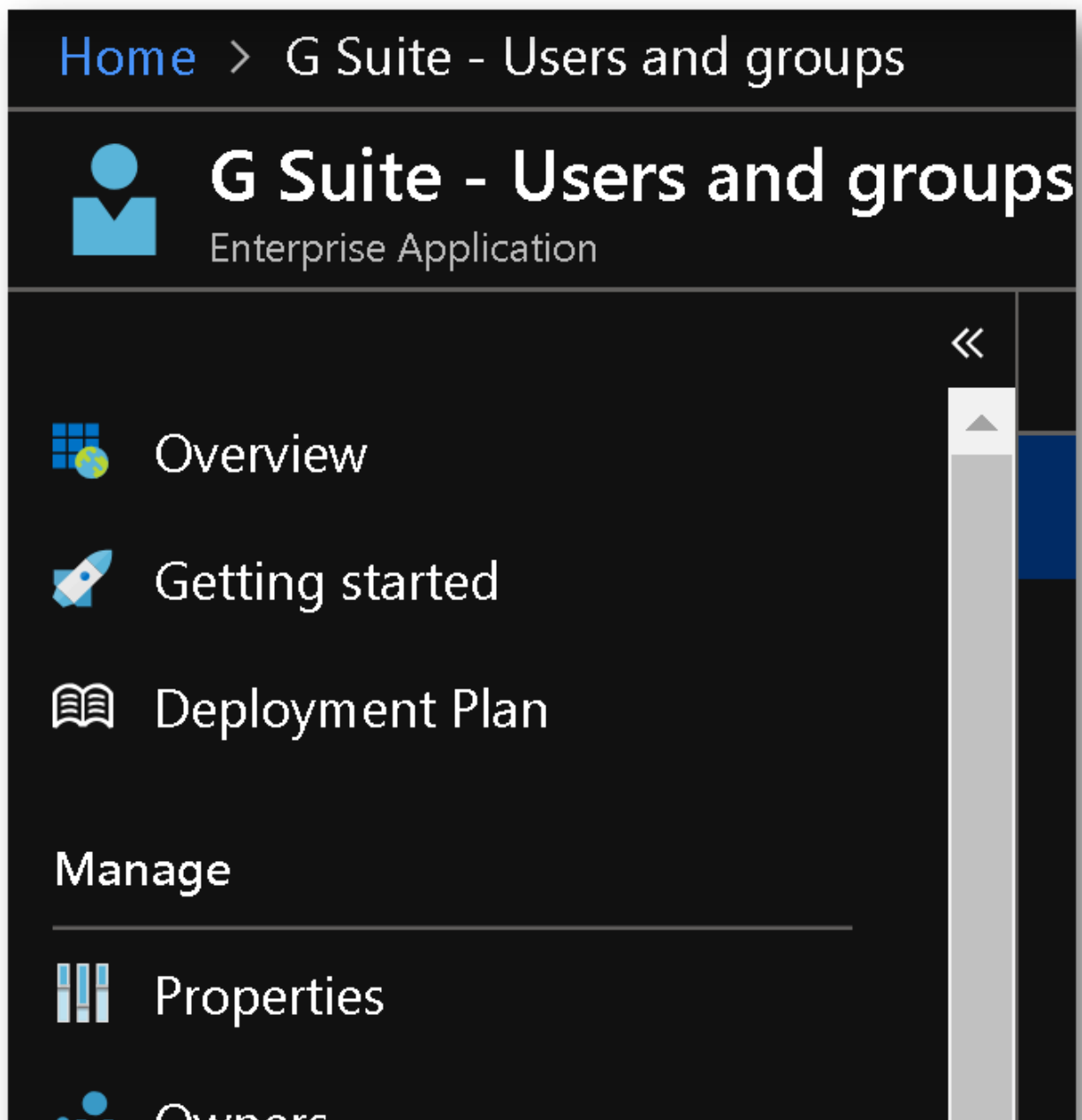
See this article (<https://support.google.com/a/answer/6087519?hl=en>) for more information on configuring G-Suite for SSO. From within G-Suite navigate to Admin → Security → Setup SSO. Paste the URLs you copied in the last step, into the SSO configuration, upload the

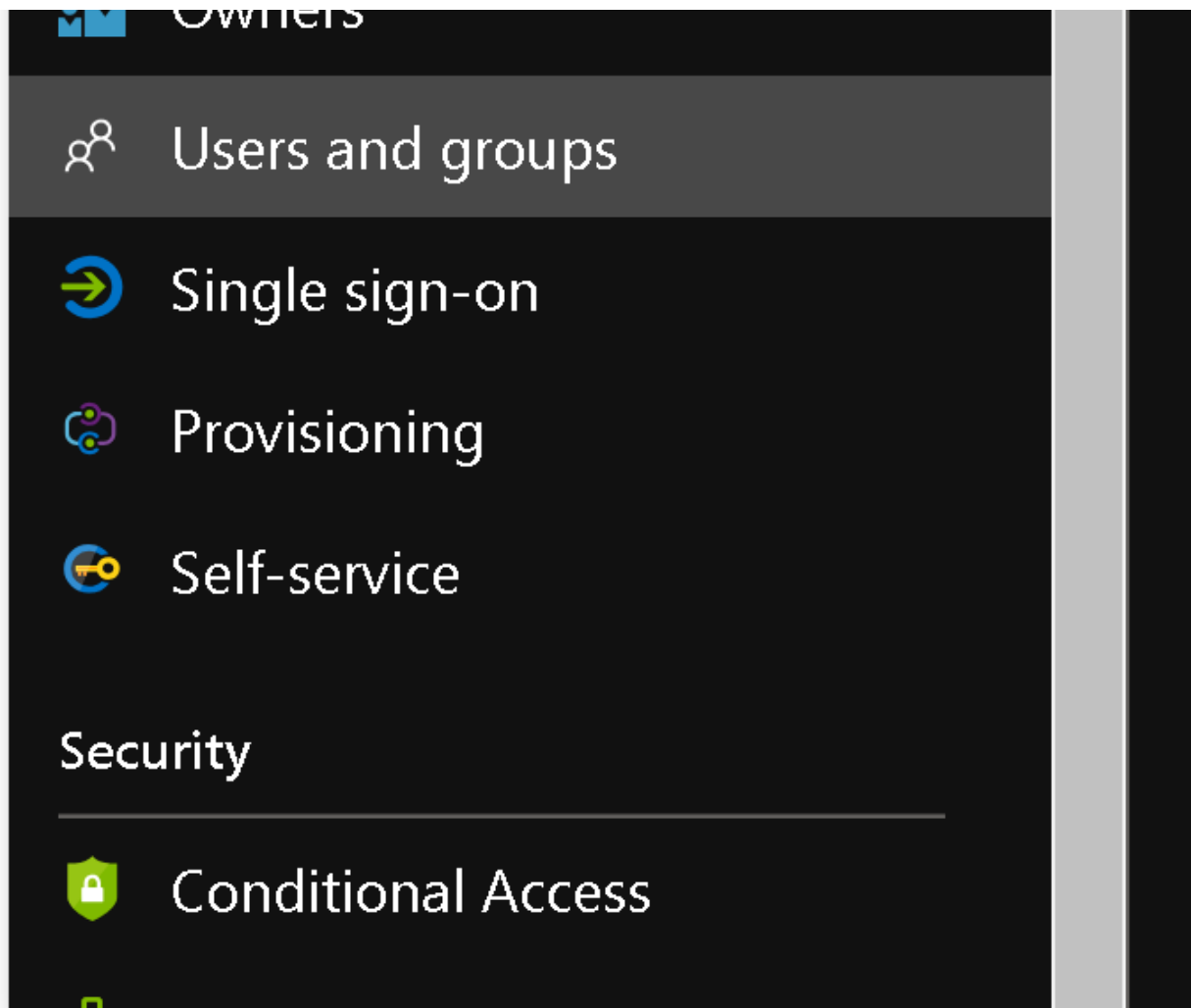
certificate you downloaded previously, check the box for **use a domain specific issuer** and then click **Save**:

The screenshot shows the Google Admin console interface. At the top, there's a blue header with the Google Admin logo and a search bar. Below the header, the 'Security' section is active. A message states: 'To setup third party as your identity provider, please provide the information below.' The form contains several fields: 'Sign-in page URL' with the value 'microsoftonline.com/796efce0-6cdd-4d4d-af31-d7b8500e31e0/saml2', 'Sign-out page URL' with the value '/login.microsoftonline.com/common/wsfederation?wa=wsignout1.0', 'Change password URL' with the value 'https://account.activedirectory.windowsazure.com/changepassword', and 'Verification certificate' with a note that a certificate file has been uploaded and a link to 'Replace certificate'. At the bottom, the checkbox 'Use a domain specific issuer' is checked.

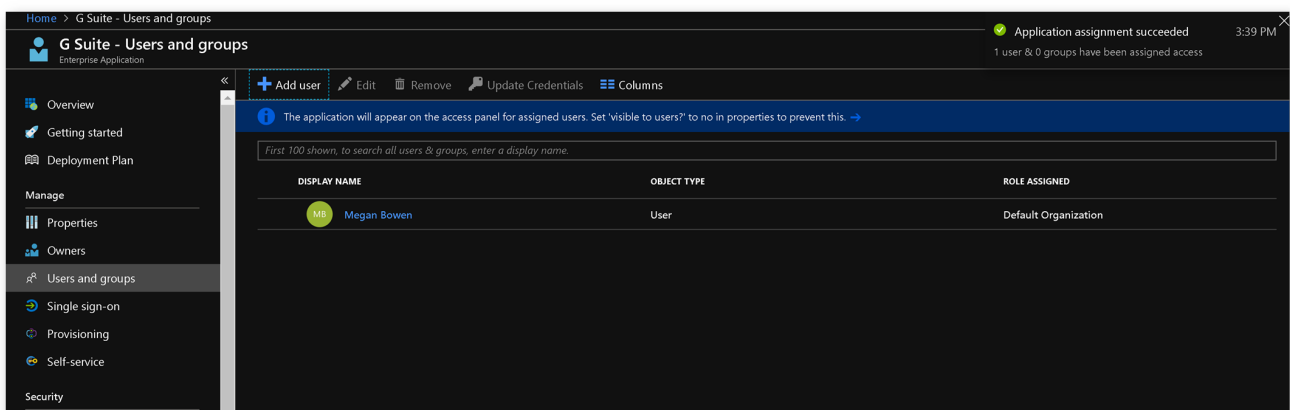
Assign the user to G Suite

Back in the Azure portal, click Users & Groups from within the G-Suite Enterprise Application:





Add a new user to G-Suite:



Turn on Provisioning:

Click on **Provisioning** and go through the steps on the blade. Starting with changing *Provisioning Mode* to Automatic.

Home > Contoso > Enterprise applications - All applications > G Suite - Provisioning

G Suite - Provisioning

Enterprise Application

Save Discard

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in G Suite based on user and group assignment.

Admin Credentials
Azure AD needs authorization to connect to G Suite's API and synchronize user data.

[Authorize](#)

[Test Connection](#)

Notification Email:

☐ Send an email notification when a failure occurs

Mappings
Mappings allow you to define how data should flow between applications.

NAME	ENABLED
Save your credentials to create mappings	

☐ Restore default mappings

Then click **Authorize** and type in your G-Suite credentials to go through the authorization process. Grant consent:

https://accounts.google.com/signin/oauth/consent?authuser=0&part=AJi8hAMddg51hgCZSh6tL0hyNgjR8WDIGiirxLiEZNGwuwSVn8n9qj0w_xhRV9SGeEmj88O72hYP

Azure Active Directory wants to access your Google Account

mattsoseman@soseman.org

This will allow **Azure Active Directory** to:

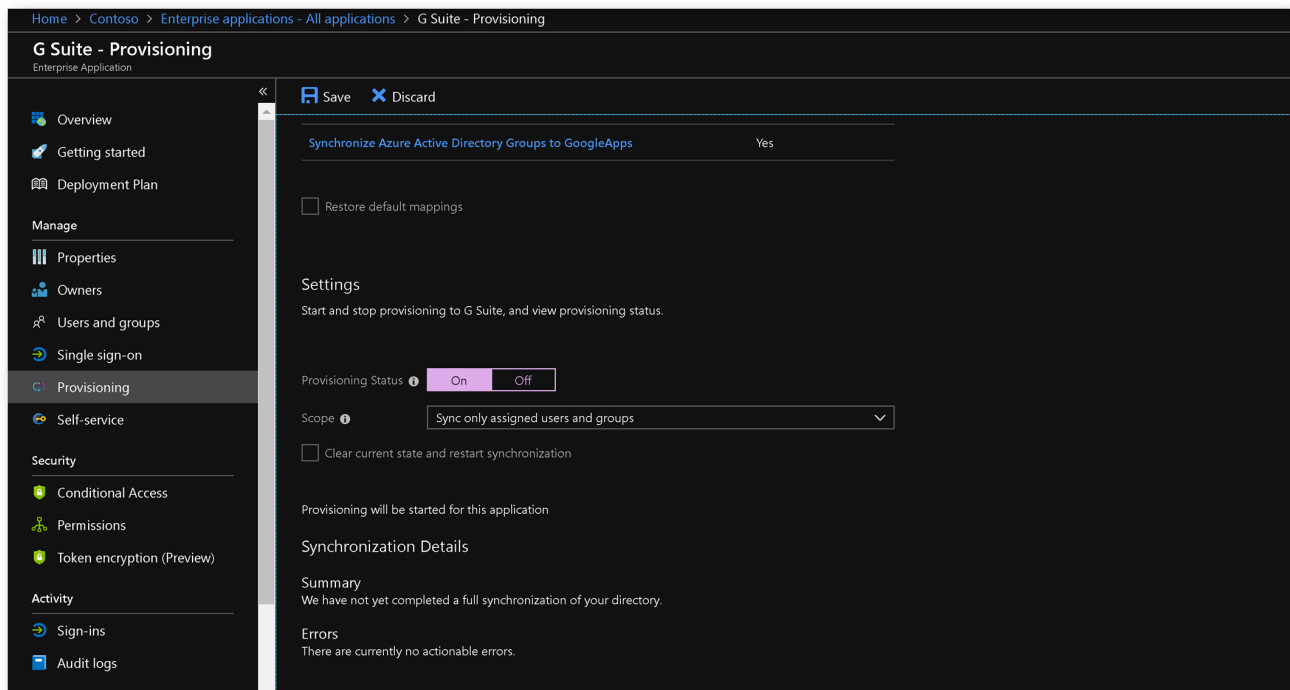
- View and manage the provisioning of groups on your domain
- View and manage the provisioning of users on your domain
- See, edit, download, and permanently delete your contacts

Make sure you trust Azure Active Directory
You may be sharing sensitive info with this site or app. Learn about how Azure Active Directory will handle your data by reviewing its [privacy policies](#). You can always see or remove access in your [Google Account](#).

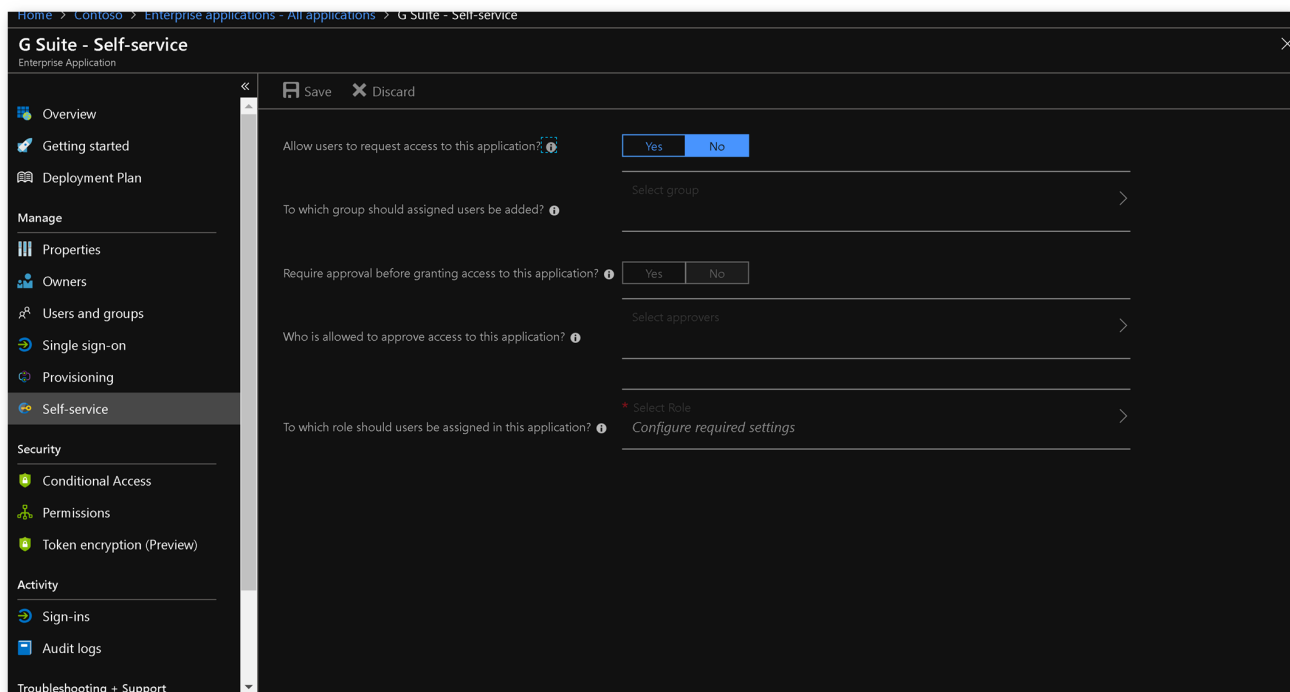
[Learn about the risks](#)

[Cancel](#) [Allow](#)

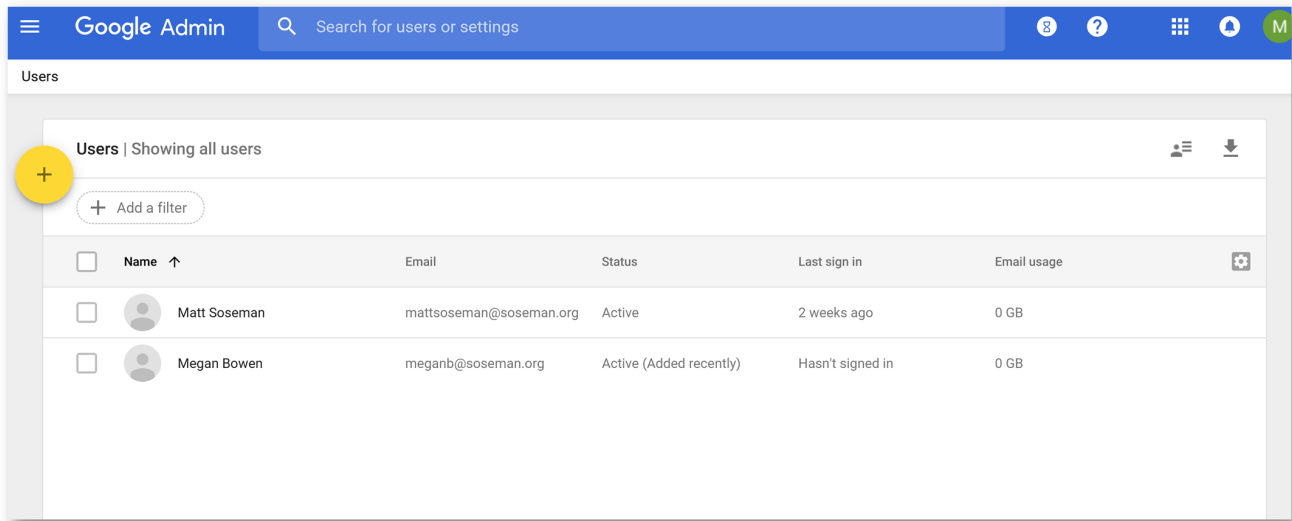
Back in the Azure portal, click **Save** to save your provisioning configuration. Once saved, you can opt to enable automatic synchronization of identities from Azure AD to G-Suite by clicking **On** for *Provisioning Status*:



Side bar, I *could* configure self service for end-users!

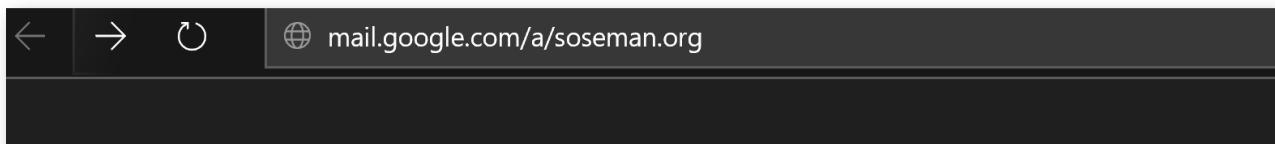


Back in G-Suite, you will notice the assigned users will start to sync:

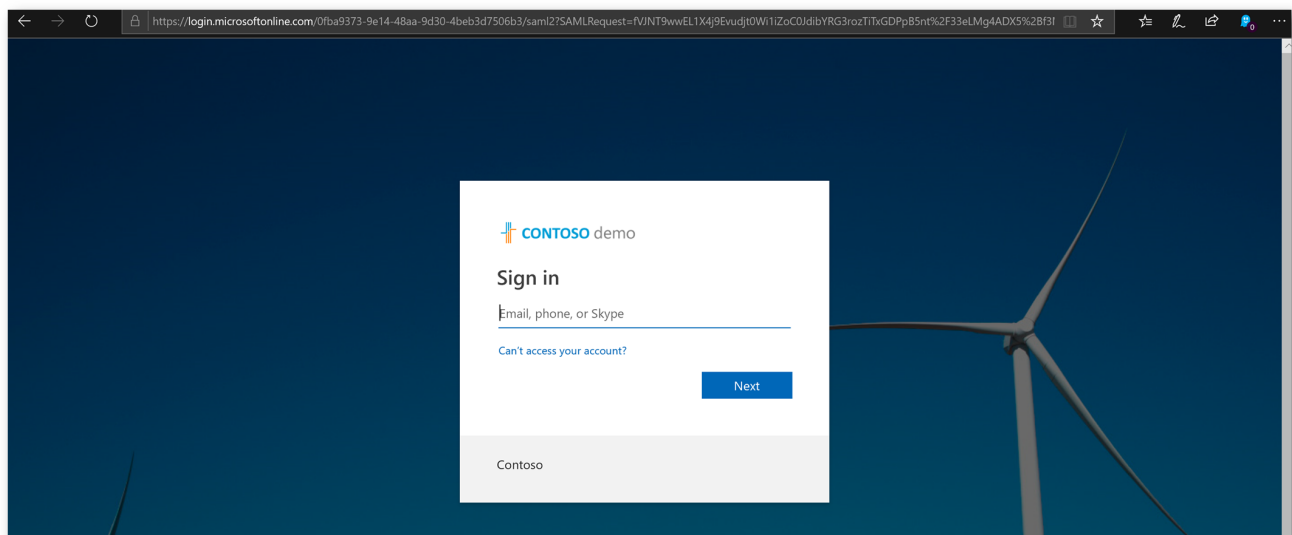


Time to test!

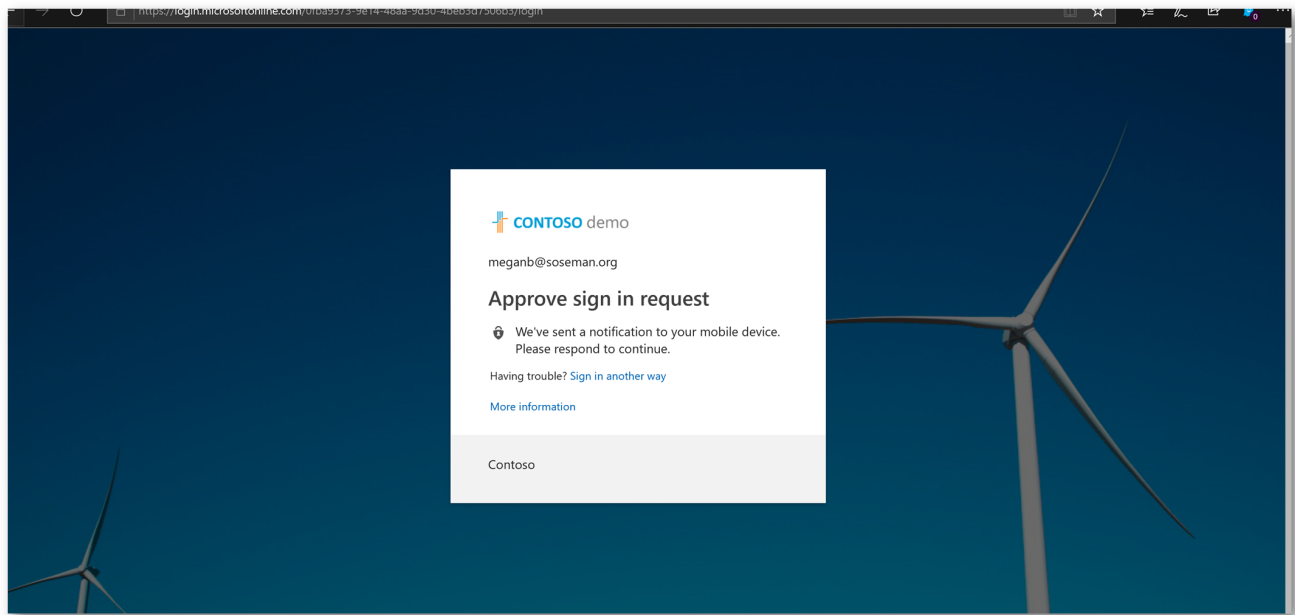
I'm going to navigate to <http://mail.google.com/a/soseman.org> (<http://mail.google.com/a/soseman.org>):



Notice this will redirect to Azure Active Directory:



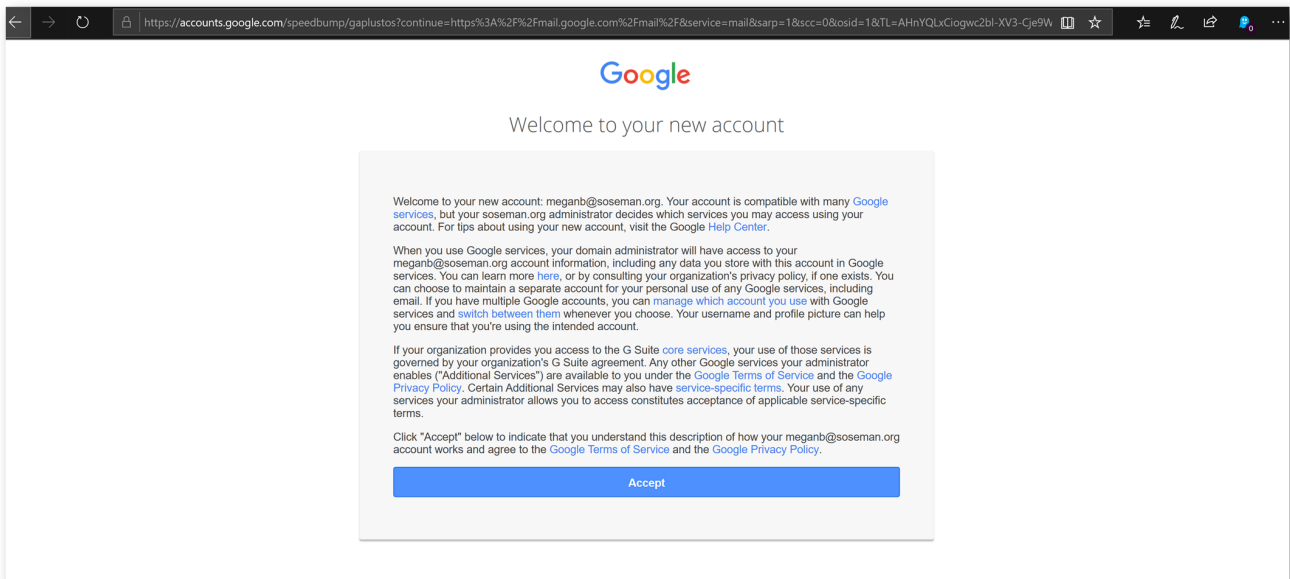
Notice it challenges me for multi-factor authentication!



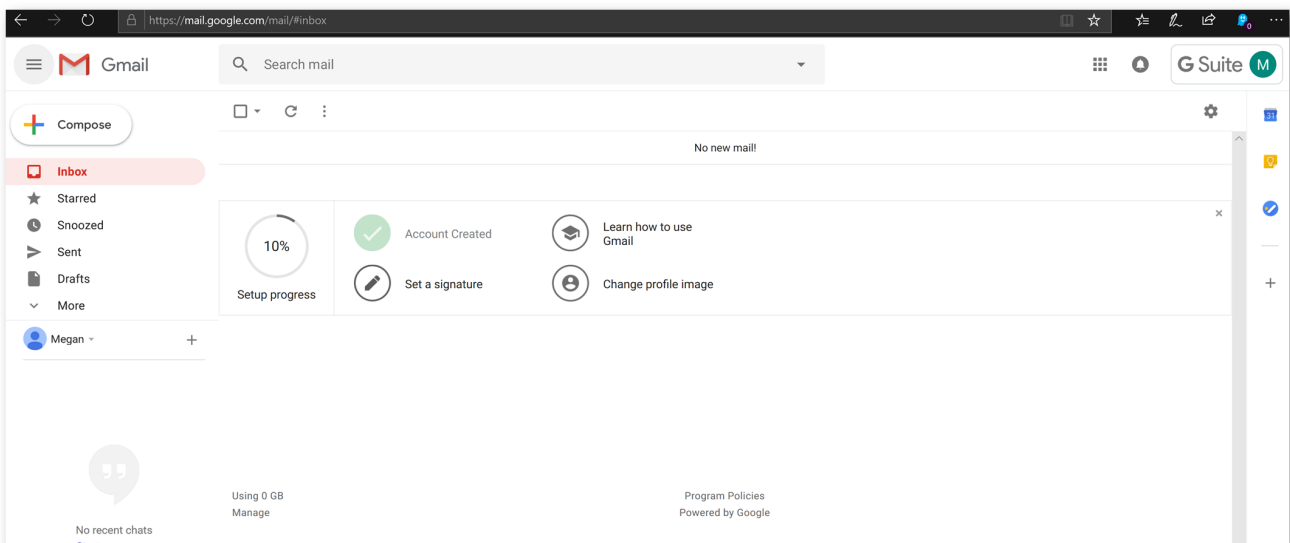
And I respond to the challenge using my Apple Watch 😊



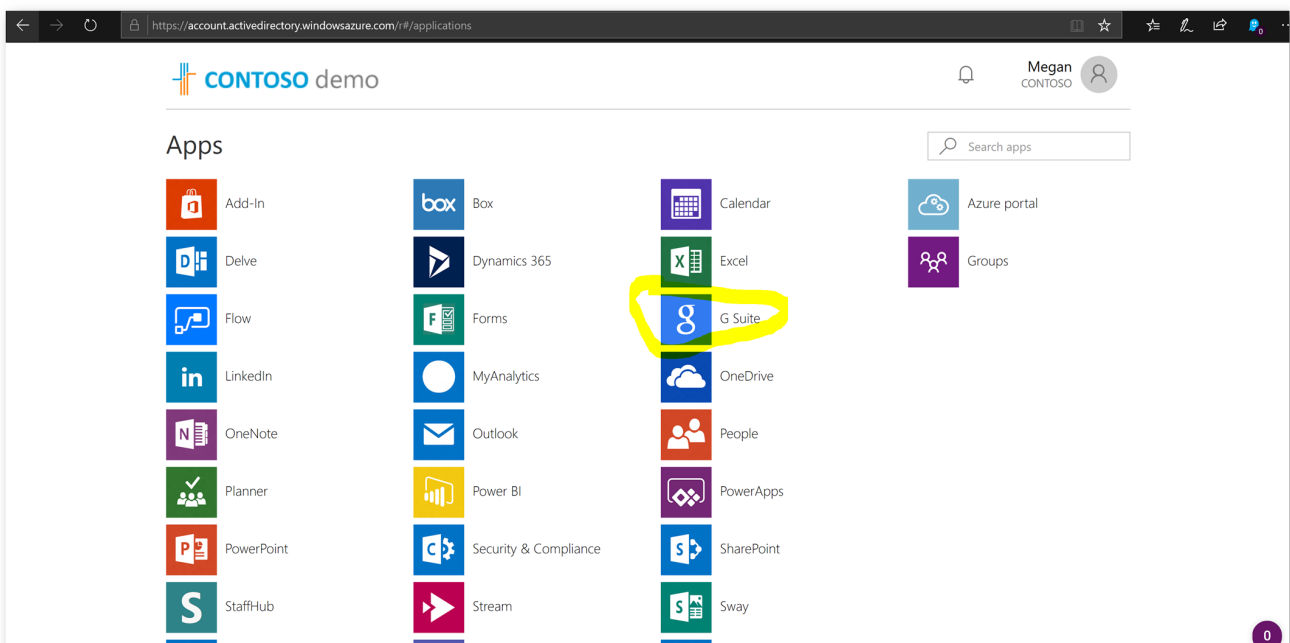
Once authenticated, accept the terms and conditions:



Now, I'm logged in and ready to use G-Suite!



Browsing to myapps.microsoft.com – G-Suite is added to the launcher!



Conclusion:

As you can see, configuring Single Sign On for G-Suite using Azure Active Directory is a rather easy and simple process – and probably can be completed within 15 minutes or less. Once configured, don't forget using Azure AD Conditional Access to govern how G-Suite is accessed, such as requiring a managed device (mobile or PC), monitoring the credentials for being compromised (impossible travel, up for sale on dark web, coming from atypical locations, etc), requiring MFA, and more!

Privacy (<https://privacy.microsoft.com>) Terms of Use (<https://msdn.microsoft.com/cc300389>)

Trademarks (<https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/EN-US.aspx>)

© 2019 Microsoft