How to setup G Suite for Single Sign-on Login from Office 365

Single sign-on is a mechanism where one system can make use of accounts on another system to allow users to log in. A user only has to log in once to the system where their account originates and then any time they need to log on to other systems that use single sign-on they will be automatically signed on.

In this video we'll be configuring G Suite to use accounts that have been created on Azure or O365. You can use this if you have set up both G Suite and Azure with your domain.

The first thing you need to do is add your domain to both Azure and G Suite. Once you've done that log into the Azure portal and choose Azure Active Directory. From there open "Enterprise applications" and add a new application.

We'll type in "G Suite" so we can find that and choose G Suite. Add that, and once that's added we're now going to add single sign-on. Choose "SAML" and now we'll edit the basic SAML configuration.

For the single sign-on URL you want to put in your domain so replace the "yourdomain.com" with whatever it is.

Now for the logout URL put in accounts.google.com/logout and save that.

Let's go back to the previous page. We'll test that ["Test single sign-on with G Suite"] later.

So now we need to download the base64 certificate. And copy the URLs from the setup G Suite section. Copy and save them. And you'll be using those in your G Suite configuration.

Next we're going to use a test user who we'll assign G Suite single sign-on to.

So let's go back to Azure Active Directory and from "Users" we'll create a new user. Make sure that their email address is in the new domain that we're using. Once you've created them we can go back into the G Suite Enterprise Application and assign single sign-on to that user you've just created. So choose that user. Select and assign them. And now that user will be able to log in to G Suite.

Now we're ready to set up G Suite. Go to the admin console and select security. Scroll down to "Set up single sign-on" and scroll down to "Setup SSO with third-party identity provider". Enable that and for the sign-in page URL you want to copy and paste in the login URL that you copied out of Azure. Then we paste in the logout URL and for the "Change password URL" you'll need to use this one:
https://account.activedirectory.windowsazure.com/ChangePassword.aspx

How to setup G Suite for Single Sign-on Login from Office 365

We need to upload a verification certificate so "choose file". Select the certificate you downloaded earlier and upload and then save.

Now you need to create the same user that you created in Azure. So go ahead and create a user using the same email address. Now you should be able to test out logging in as this user. So open up an incognito window and log in as that user. When you enter the email address it should redirect you to Microsoft to login. Enter the email address and password. We'll just click "Yes" for "Stay signed in" and you'll be logged in with Microsoft and then into Google.

So single sign-on is now working.

Now we have the ability to manually provision users from Azure to G Suite but this relies on you manually creating each user in G Suite and nobody has time for that! So we'll take advantage of automatic user provisioning in Azure which creates the G Suite accounts if they don't already exist.

Azure needs access in G Suite to be able to create accounts So we'll create an account for this purpose. I've created a user called "Azure" and given it Super Admin access. Microsoft recommends that you give it full API access and you can do that using a custom role. You'll see here that it has all the API privileges. But the process of authorizing it in Azure requires the user to log in and grant Azure access. Since we've already set up single sign-on in G Suite that user won't be able to log on unless it's a Super Admin user. Once it's been authorized in Azure you should come back and change the Super Admin access to the custom role.

To configure automatic user provisioning in Azure open up Azure Active Directory, "Enterprise applications", and select "G Suite". Under "Manage" → "Provisioning" change the mode from "Manual" to "Automatic".

We have to authorize the G Suite account. Login as the account. You'll need to put in the email and password the first time you do this. Allow Azure to access the account. If you test the connection it should verify that it is working. It's worth while entering an email address to receive notifications of errors. Now let's save this.

Rather than having to individually add each user to single sign-on we can use a group that we add the users to. I've created a group called G Suite of type Office 365 and added the users that need to be provisioned in G Suite.

Next we need to add a scoping filter that specifies what accounts are provisioned in G Suite. We want to filter the provisioned users whose email domain is our G Suite domain. Azure uses

How to setup G Suite for Single Sign-on Login from Office 365

"userPrincipalName" for the email address and we'll create a regular expression match to any user name at our domain. [Set Target Attribute to "userPrincipalName", Operator to "REGEX MATCH", and Value to ".*@yourdomain.com" where "yourdomain.com" is replaced with your domain]. The dot matches any character and the star matches any number of these characters.

Give it a name, add the clause, and save it. Let's enable provisioning and save it.

Now we'll assign users in our G Suite group to single sign-on. For the users begin typing the email address of the group and then choose the group and click "Select" and "Assign". To give a user access to G Suite simply add them to the group and as long as their email addresses is in the domain we added the scoping filter for their account will be automatically provisioned in G Suite and they will be able to log in using single sign on.

Let's create a new user and verify that it all works. Make sure we choose the correct domain. Copy the password and click "Create". The user has now been created. Add them to the G Suite Group and at the next provisioning the user will be created and will be able to login.

Let's force a sync and refresh. You can see that five users have been created.

From the G Suite admin console we can now find this user. Don't worry about it being automatically suspended - that's because I'm using a trial domain.

We can log in as the new user. We'll be redirected to Microsoft single sign-in. We can log in and then we'll end up being logged into G Suite.