

# Content Collaboration: Single Sign-On Configuration Guide

## G Suite for Business

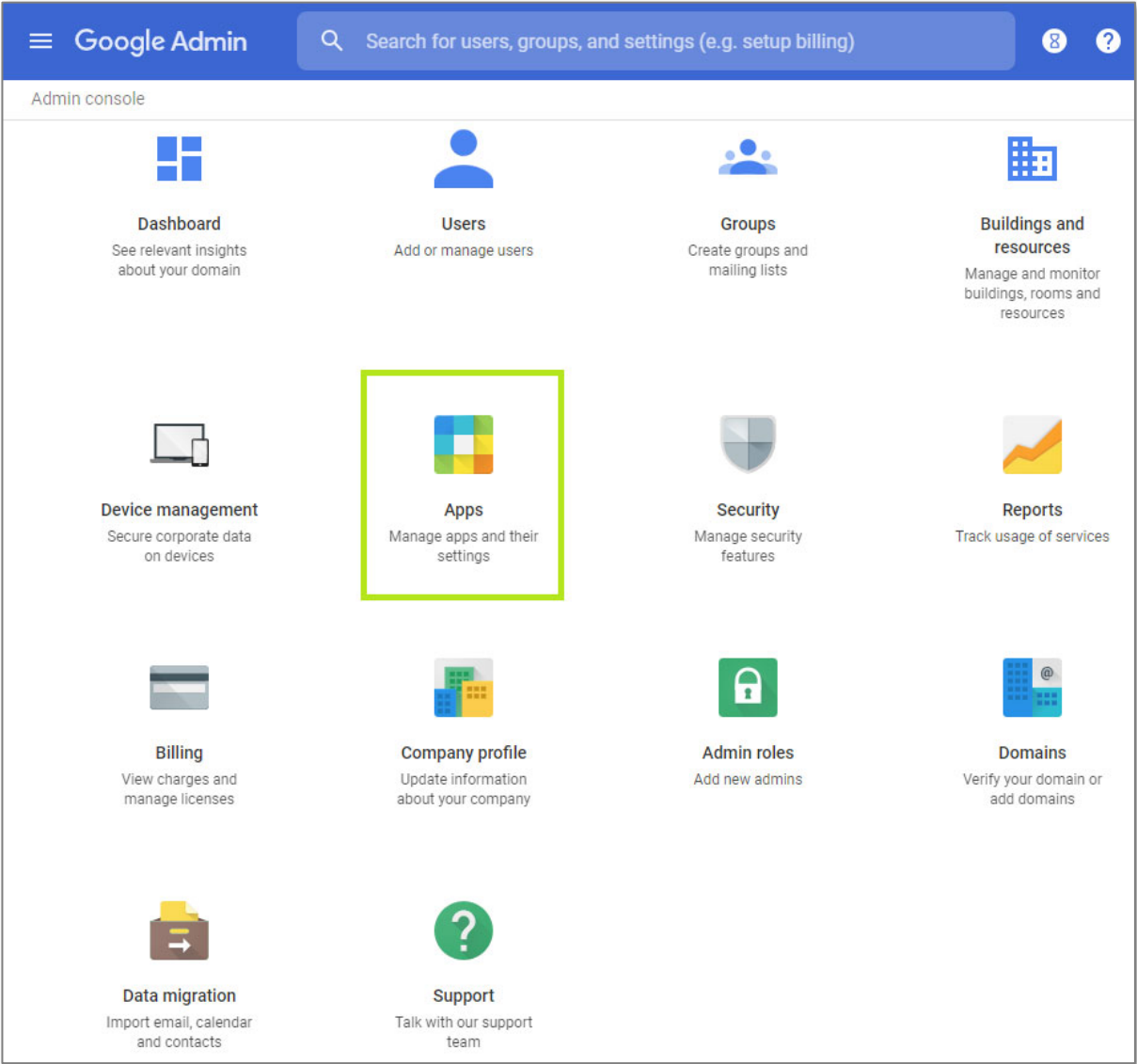


Last Revised: May 2019

## LEGAL NOTICE

This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc. This document and the software may be used and copied only as agreed upon by the Beta or Technical Preview Agreement.

Copyright © 2019 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Content Collaboration, and ShareFile are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Steps	Description
1.	<p>Log in to G Suite with Google Admin account.</p> <p>For example, login to <b>https://admin.google.com</b>.</p>
2.	<p>In Admin Console, click on <b>Apps</b>.</p>  <p>The screenshot shows the Google Admin console interface. At the top, there is a blue header with the 'Google Admin' logo, a search bar containing the text 'Search for users, groups, and settings (e.g. setup billing)', and user profile icons. Below the header, the main area is titled 'Admin console' and contains a grid of 14 icons representing different management functions: Dashboard, Users, Groups, Buildings and resources, Device management, Apps (highlighted with a green box), Security, Reports, Billing, Company profile, Admin roles, Domains, Data migration, and Support.</p>
3.	<p>In <b>App Settings</b>, click <b>SAML apps</b>.</p>

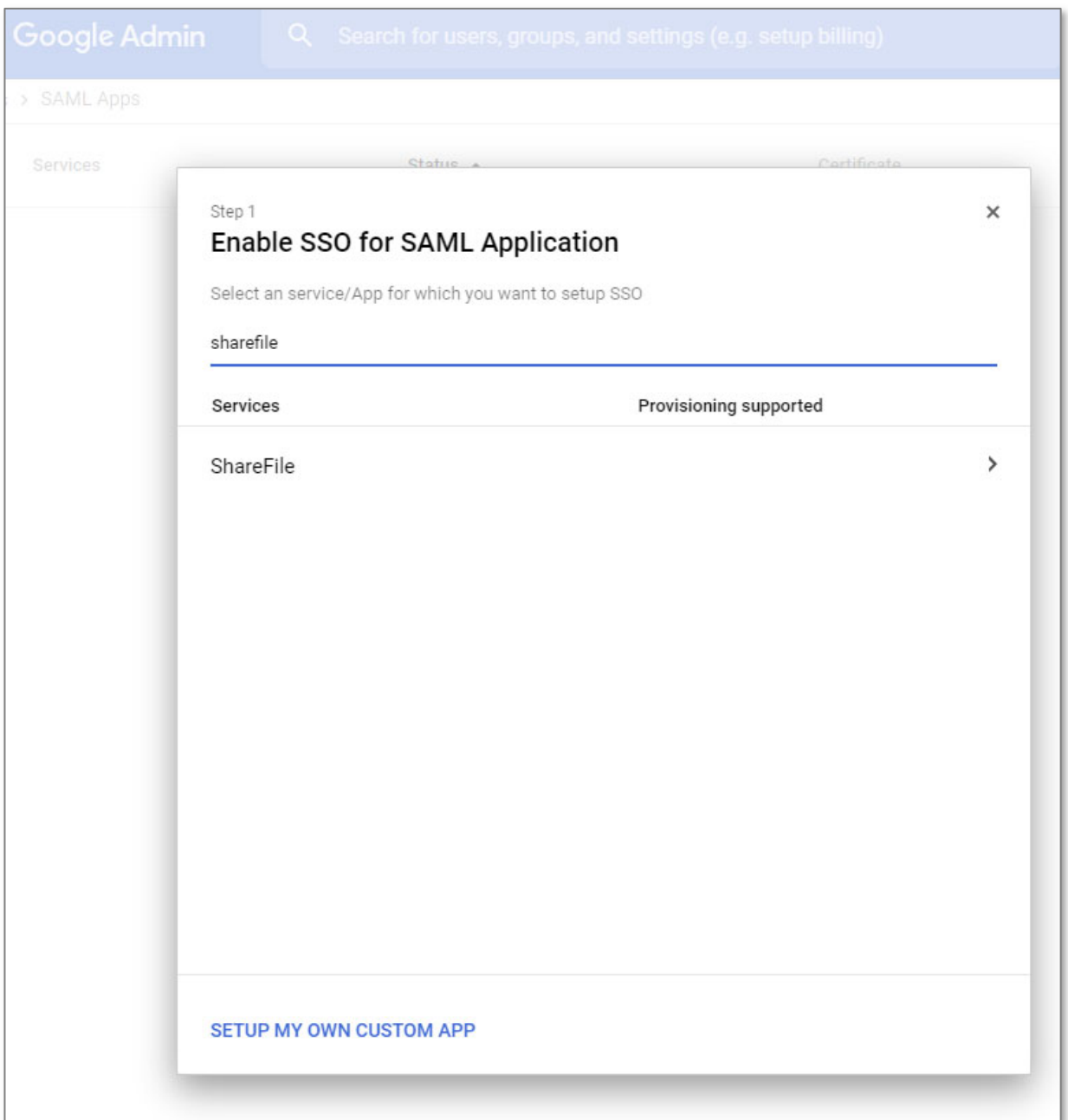
The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo, a search bar, and user information. Below the header, the page is titled "Apps". Under "APPS SETTINGS", there is a section for "Marketplace settings" with four cards:

- G Suite:** 13 G Suite Core Services. These services are governed by your G Suite agreement.
- Additional Google services:** 50 services including Blogging, photos, video, social tools and more. These services are not governed by your G Suite agreement, and other terms apply.
- Marketplace apps:** 0 apps. Includes a link for "More about Marketplace apps".
- SAML apps:** 0 apps. Includes a link for "Manage SSO and User Provisioning". This card is highlighted with a green border.

4. **Add a service/Apps to your domain** or click + symbol.

The screenshot shows the Google Admin console interface for SAML Apps. The breadcrumb trail is "Apps > SAML Apps". The page has a table with columns for "Services", "Status", and "Certificate". The table is empty, and the message "No services/Apps configured for SAML." is displayed. Below the message is a link "Add a service/App to your domain" and a yellow plus sign button in the bottom right corner.

5. Type "sharefile" to **Enable SSO for SAML Application.**



6. In **Google IdP Information**, Option 1, note your **SSO URL** and **Entity ID**.

Google Admin

Search for users, groups, and settings (e.g. setup billing)

Apps > SAML Apps

Services Status Certificate

Step 2 of 4

### Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

**Option 1**

SSO URL `https://accounts.google.com/o/saml2/idp?idpid=C01fw5ulm`

Entity ID `https://accounts.google.com/o/saml2?idpid=C01fw5ulm`

Certificate **Google\_2024-4-17-151036\_SAML2.0**  
Expires Apr 17, 2024

[↓ DOWNLOAD](#)

OR

**Option 2**

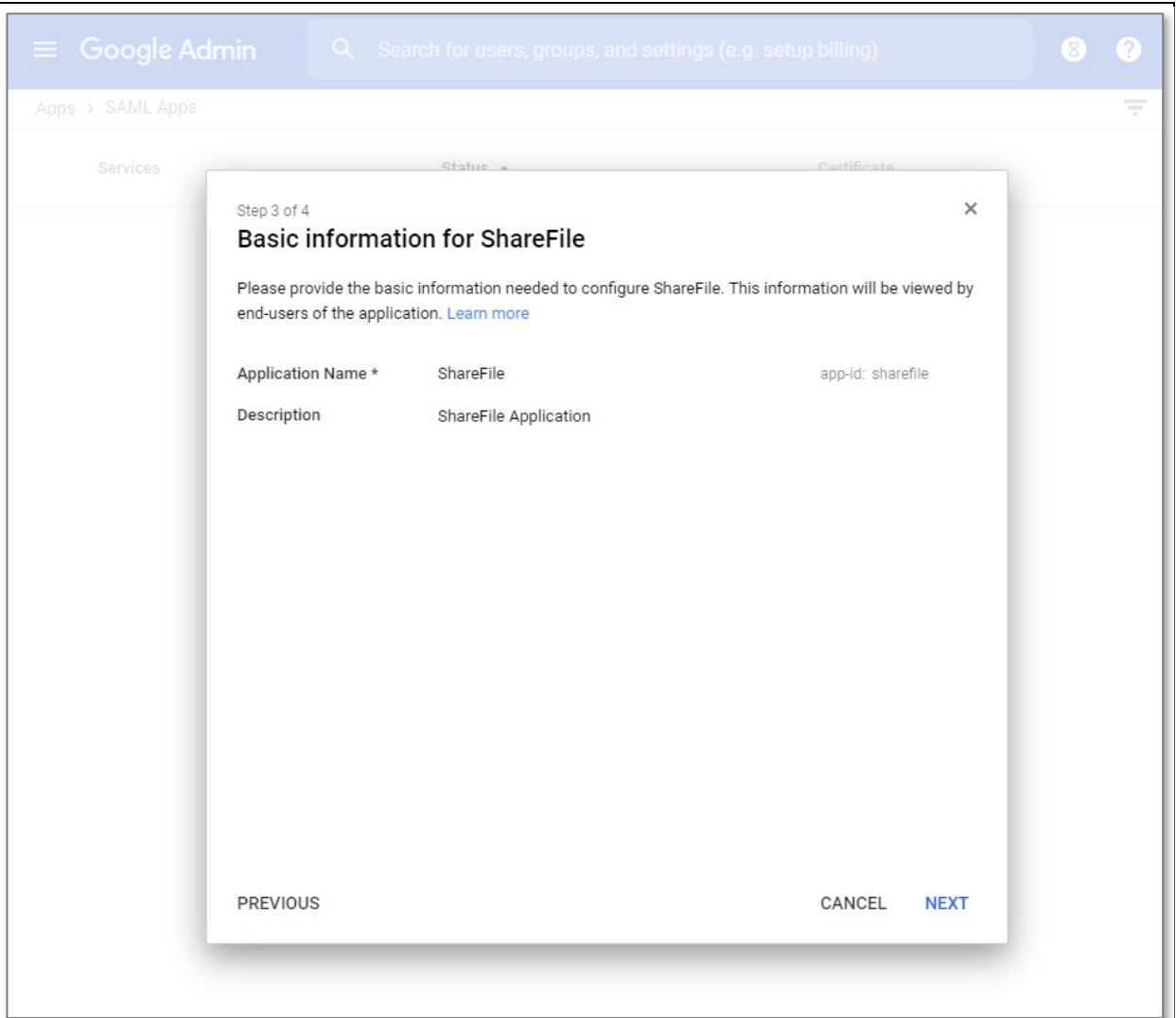
IDP metadata [↓ DOWNLOAD](#)

PREVIOUS CANCEL NEXT

7. Download **Certificate** and note the **Expires** date is good for 5 years.

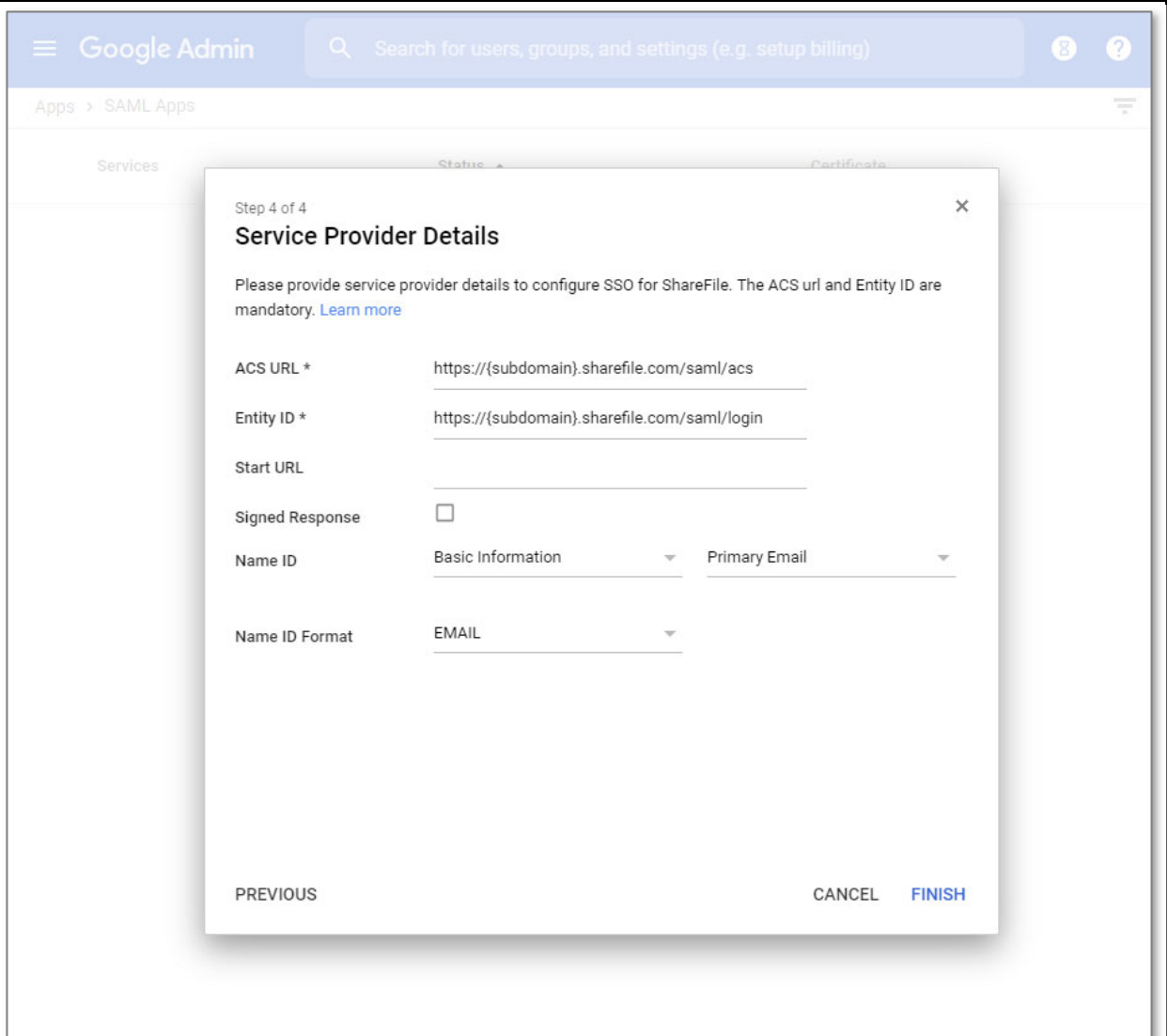
8. The certificate file is a **PEM file**. Open the file with **Notepad** or any text editor and save for later steps.



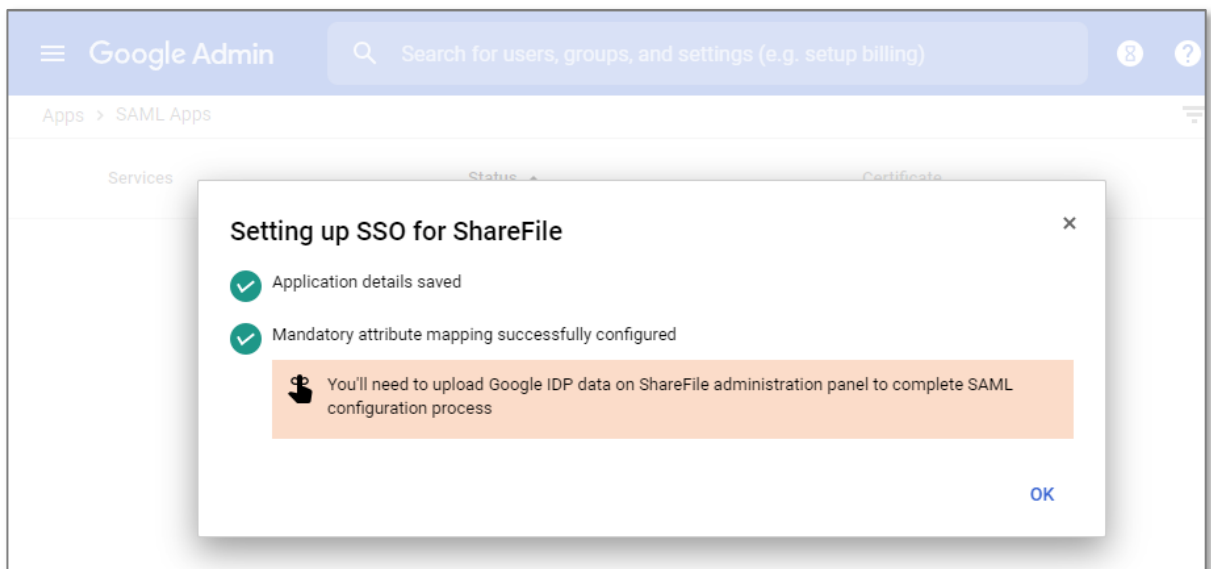


10. Enter **subdomain** information for your ShareFile account (the Service Provider). Leave **Email** and **Primary Email** in **Name ID** and **Name ID Format**. Click **Finish** when done.

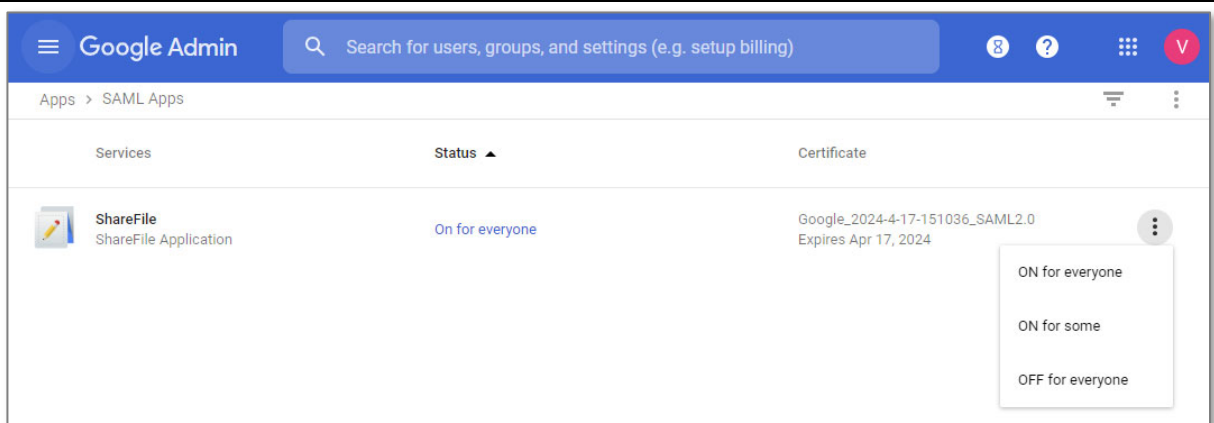




11. Confirm "OK" **ShareFile application details** are saved and **attribute mapping** are successful configured.



12. In Admin Console, click **Apps**, and then click **SAML Apps**. For the **ShareFile Application**, make sure the **Status is ON for Everyone** or **ON for some**.



13. Go to your ShareFile account: <https://subdomain.sharefile.com> > Login with Administrator account > **Settings** > **Admin Settings** > **Security** > **Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration**.

14. Use these settings to configure ShareFile:

### **Basic Settings**

- **Enable SAML:** Select **Yes**
- **ShareFile Issuer / Entity ID:** <https://subdomain.sharefile.com/saml/login>
- **Your Issuer / Entity ID:** LEAVE BLANK (Do not save text in this box; if text is saved, **see next step.**)
- **X.509 Certificate:** Click **Change**, then copy and paste the certificate from the PEM file opened in Notepad earlier.
- **Login URL:** Copy and paste from **SSO URL** provided earlier (i.e. <https://accounts.google.com/o/saml2/idp?idpid=C01fw5ulm>)
- **Logout URL:** Leave blank  
(When users log out of ShareFile, they will be redirected to ShareFile login page <https://subdomain.sharefile.com>.)

## Basic Settings

Enable SAML: (?)

Yes  No

ShareFile Issuer / Entity ID: (?)

Your IDP Issuer / Entity ID: (?)

X.509 Certificate: (?)

Saved [Change](#)

Login URL: (?)

Logout URL: (?)

15. **NOTE:** If a value is saved in the **Your IDP Issuer / Entity ID** box, please read the following:

The value of “**Your IDP Issuer / Entity ID**” in the ShareFile SSO settings is appended to the “**ShareFile ACS URL**” in the SAML Request like this:  
<https://subdomain.sharefile.com/saml/acs?idpentityid=youridpissuer>

At this time, clearing the box in ShareFile SSO settings will not clear the value ☹ in the ShareFile database. In order for the SAML request to be accepted by Google, the ACS URL values should match in both settings.

### ShareFile Settings

**Your IDP Issuer / Entity ID:** <https://subdomain.sharefile.com/saml/login>

### Google Settings

**ACS URL:**

<https://subdomain.sharefile.com/saml/acs?idpentityid=https://subdomain.sharefile.com/saml/login>

## Basic Settings

Enable SAML: (?)

Yes  No

ShareFile Issuer / Entity ID: (?)

Your IDP Issuer / Entity ID: (?)

X.509 Certificate: (?)

Saved [Change](#)

Login URL: (?)

Logout URL: (?)

## ^ Service Provider Details

Please provide service provider details to configure SSO for ShareFile. The ACS url and Entity ID are mandatory.

ACS URL \*

Entity ID \*

Start URL

Certificate  Expires Apr 17, 2024

[Manage certificates](#)

Signed Response

Name ID

Name ID Format

DISCARD

SAVE

Moreover, the **Your IDP Issuer Entity ID** can be of any value in ShareFile SSO settings; but in Google, the value of ACS URL you need to add:

**https://subdomain.sharefile.com/saml/acs + ?idpentityid= + Your IDP Issuer Entity ID value in ShareFile.**

Keep in mind changes in Google Admin Portal **may take 24 hours** to take effect.

\*\*Deleting and recreating the SAML app will propagate changes faster if you make a mistake in Google Admin site; however, do not forget to turn a new SAML app “**ON for everyone or some**” before testing.

16. Use these settings to continue to configure ShareFile:

### **Optional Settings**

- **Require SSO Login:** *Optional*  
After single-sign-on is successfully validated, checking **Yes** for this option will require all non-admin Employees to log in using Google.  
  
Admins will have the choice to login using Google (on the left) or their email address as the username and a native ShareFile password (on the right).
- **SSO IP Range:** *Optional*  
(Limit requiring non-admin Employees to login from a specific IP range. Employees outside of this specified range will not be required to use Okta to login.)
- **SP-initiated SSO Certificate:** Select **HTTP Redirect with no signature**
- **Enable Web Authentication:** **Yes** (Choose **No** when you do not want to allow logins via a web browser. This means Windows authentication will need to be available).
- **SP-initiated Auth Context:** Select **Username and Password.**
- **Active Profile Cookies:** Leave blank
- Click **Save**

### Optional Settings

Require SSO Login: ?

Yes  No

SSO IP Range: ?

SP-Initiated SSO certificate: ?

HTTP Redirect with no signature ▾

Enable Web Authentication: ?

Yes  No

SP-Initiated Auth Context: ?

User Name and Password ▾

Minimum ▾

Active Profile Cookies: ?

Save

Cancel

17. Test successful authentication by going to your ShareFile URL:

<https://subdomain.sharefile.com>

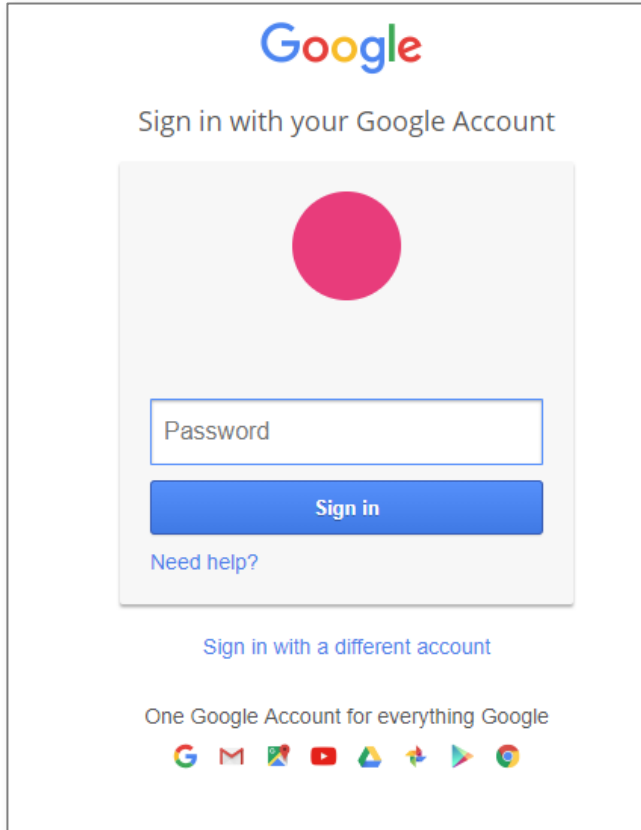
*\*\*Testing single-sign-on logins in private/incognito browser mode is best.*

Click **Sign in** under **Company Employee Sign In**

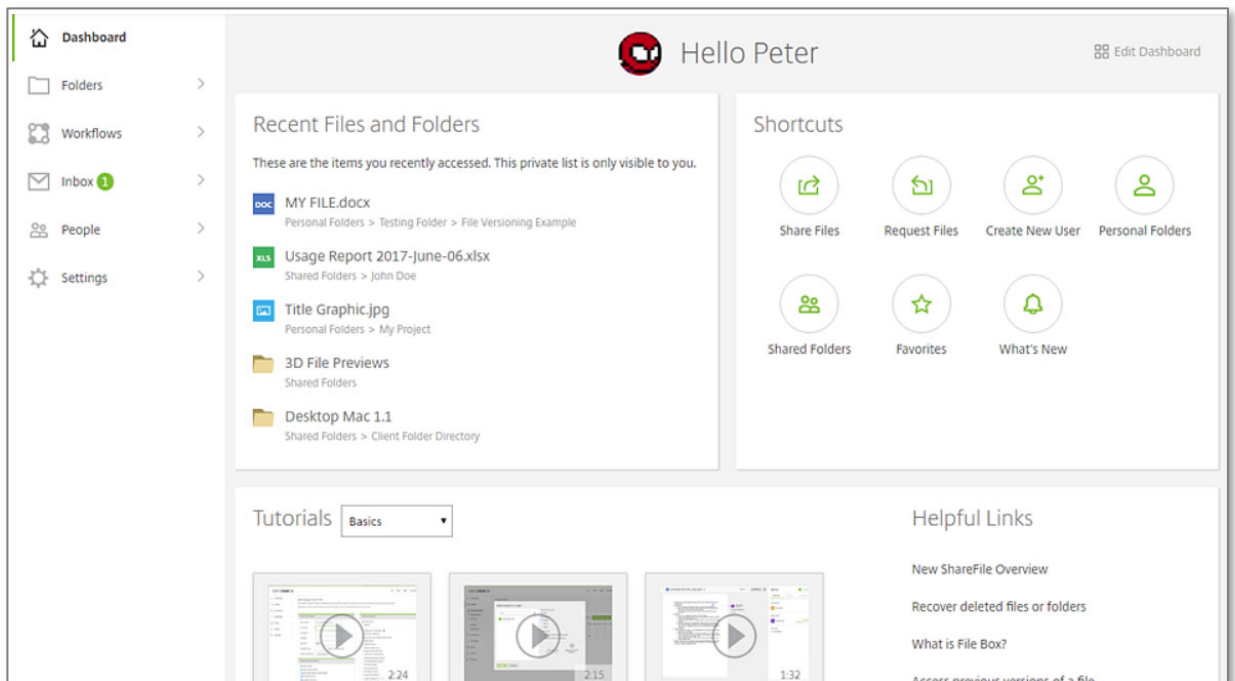
The screenshot shows the Citrix ShareFile login interface. On the left, under 'Company Employee Sign In', there is a message: 'ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.' Below this is a 'Sign In' button. On the right, under 'Sign In', there are input fields for 'Email' and 'Password', followed by a 'Sign In' button. At the bottom right, there are links for 'Remember Me' and 'Forgot Password?'.

**\*\*Make sure the user logging in with single sign-on has an Active Directory or Identity Provider email address that matches their email address in their ShareFile account.**

Sign in will redirect you to Google for sign in:



18. Successful logins will authenticate users into their ShareFile account **Dashboard**.



19. Done!