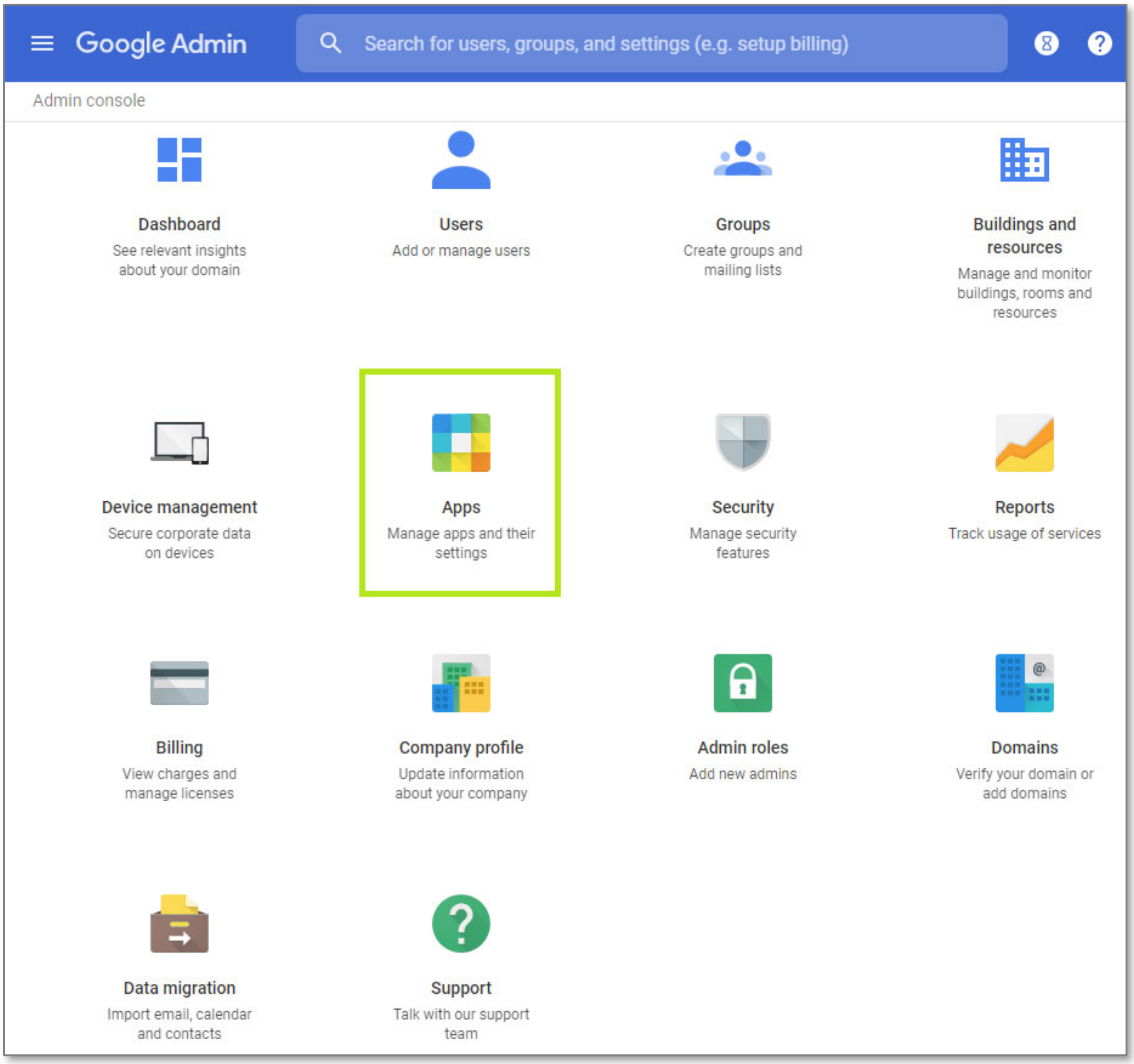
Content Collaboration: Single Sign-On Configuration Guide

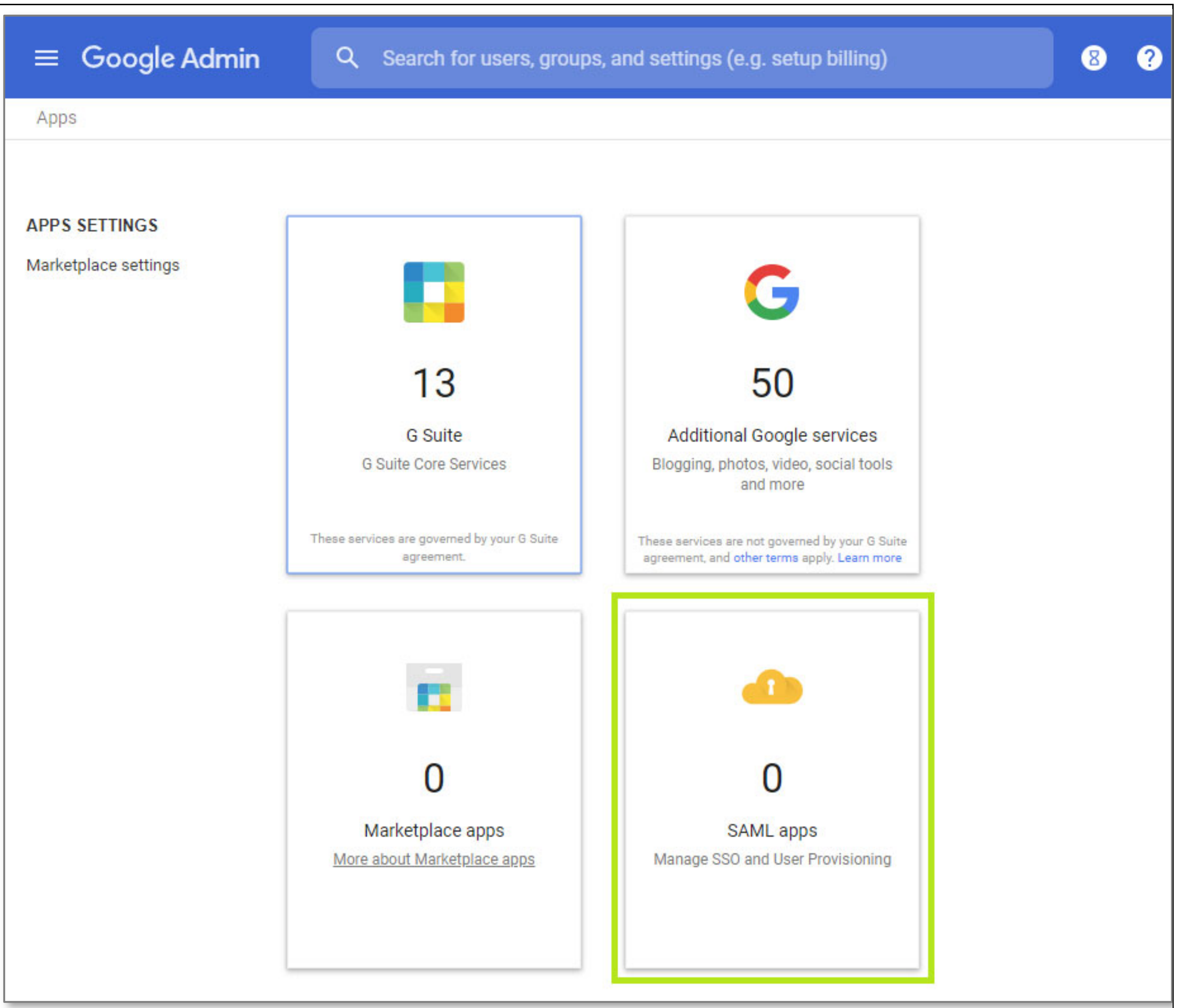
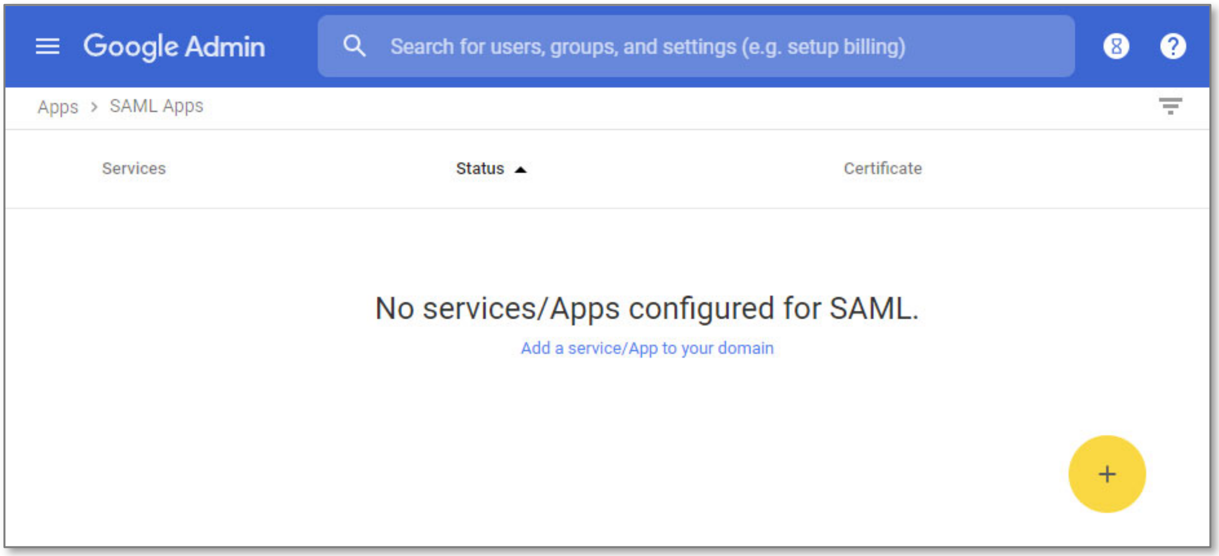
G Suite for Business

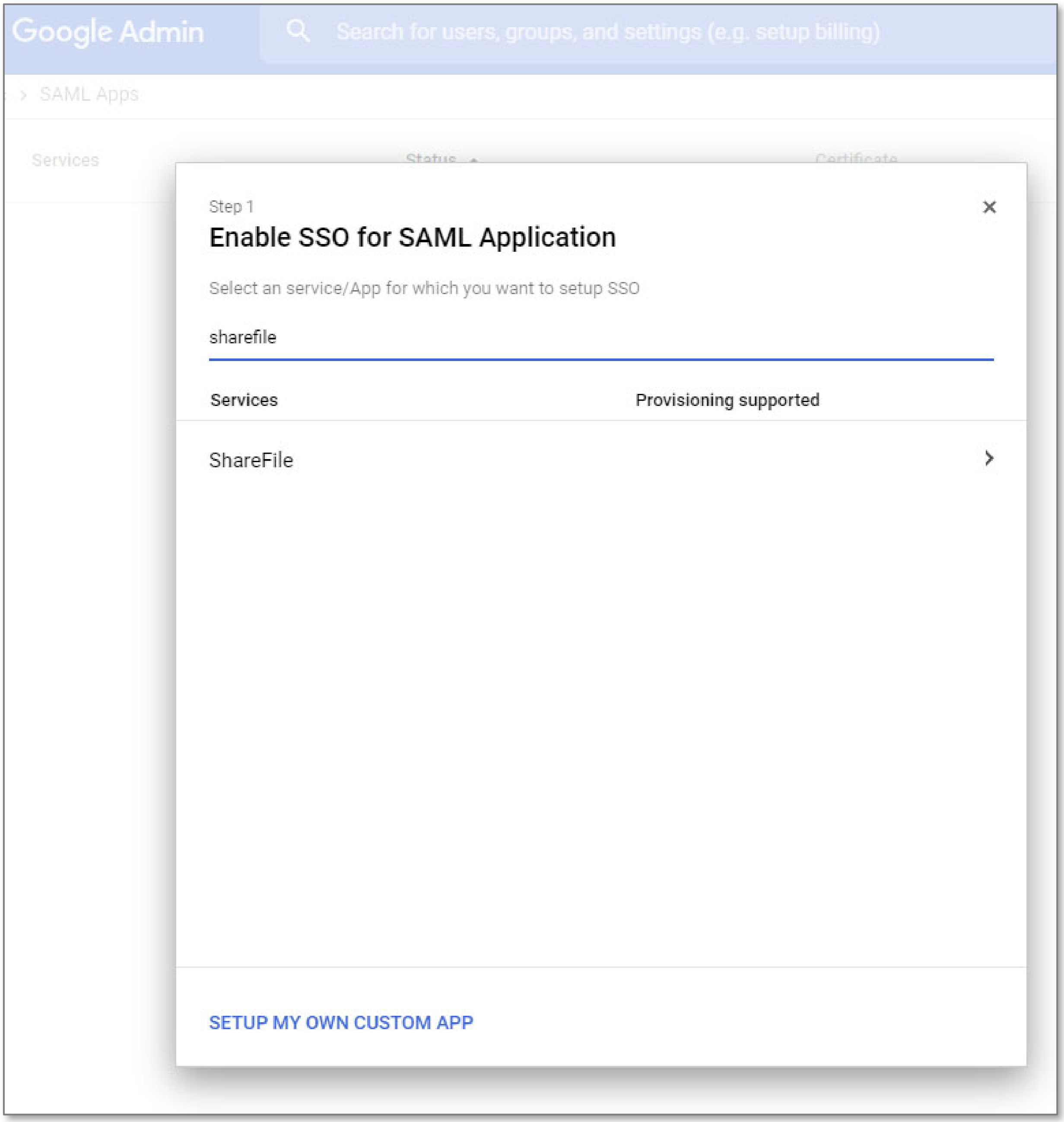
Last Revised: May 2019

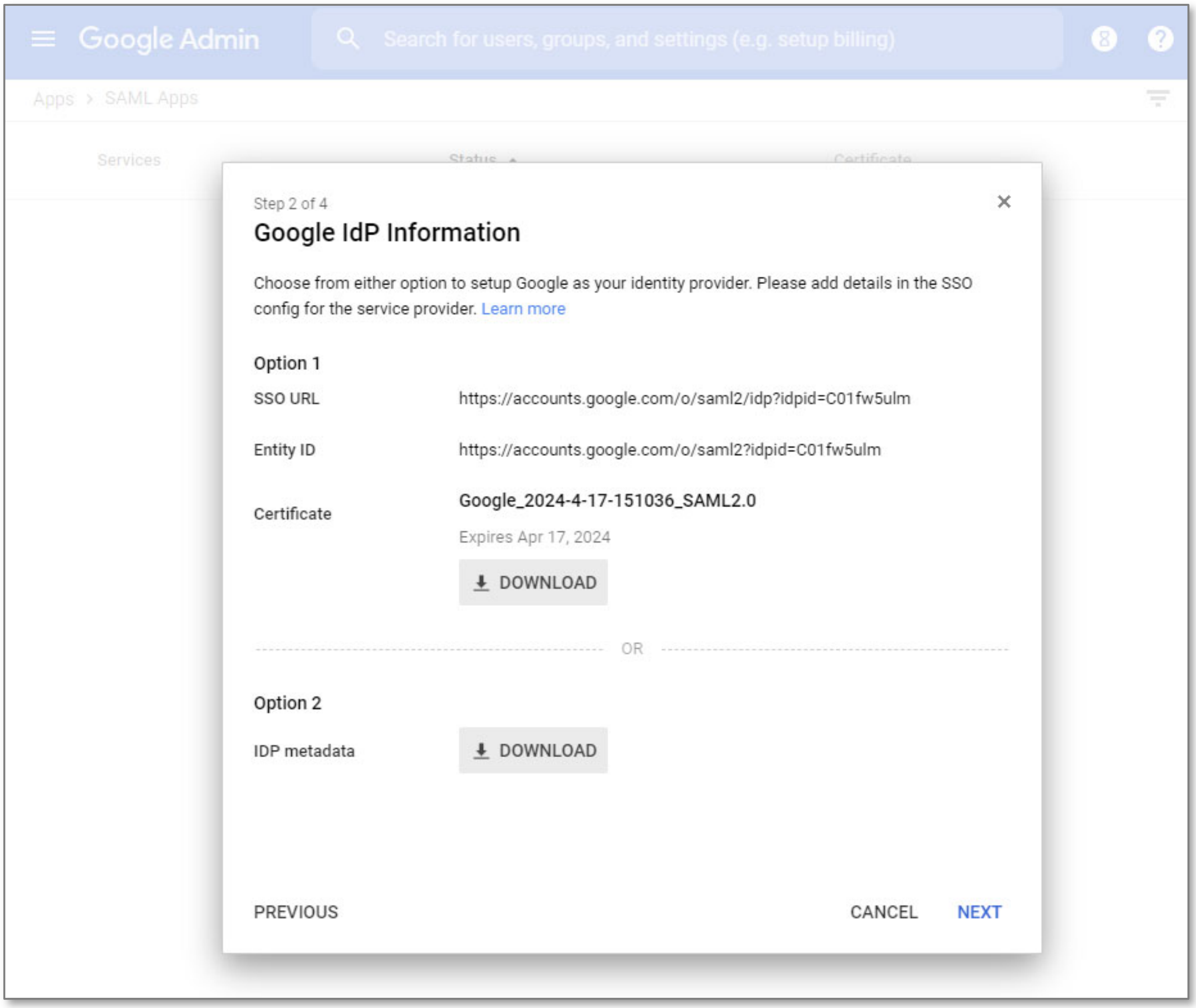
LEGAL NOTICE

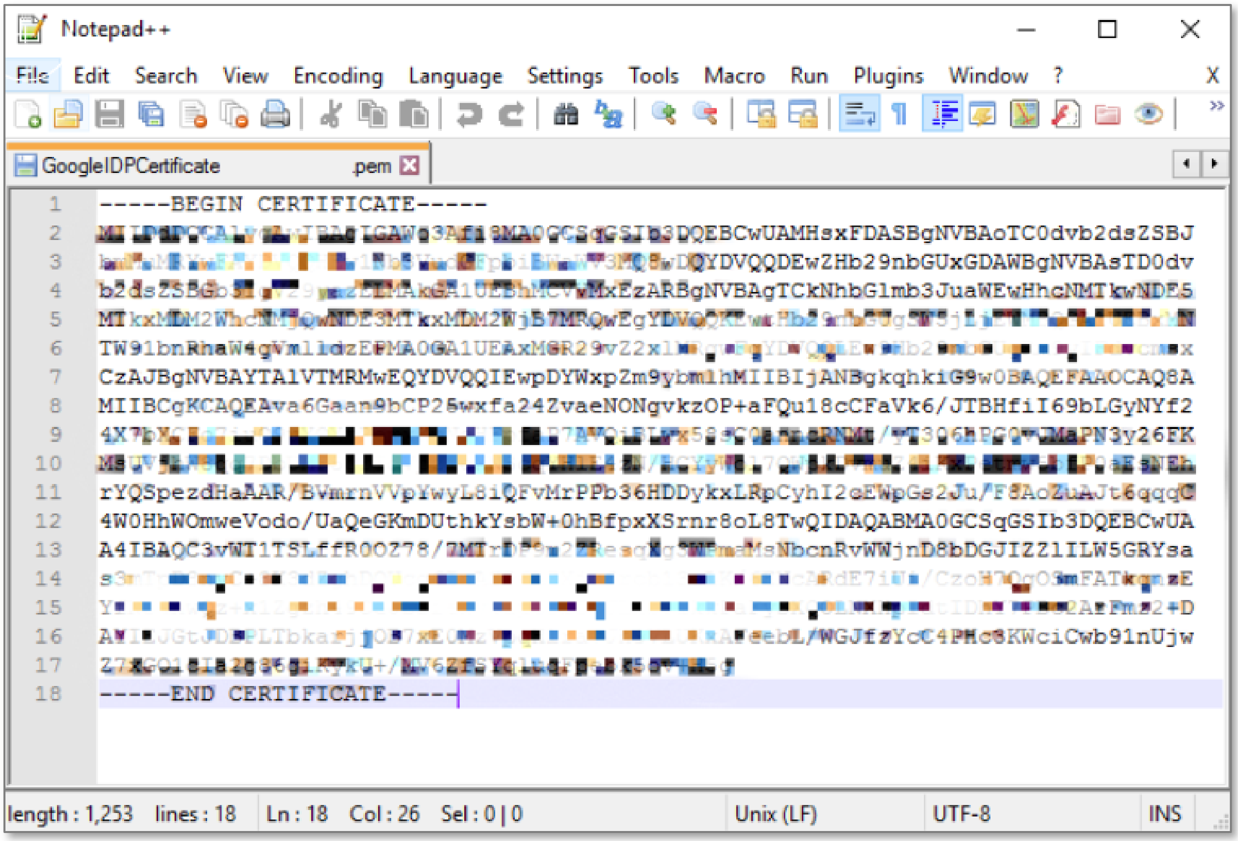
This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness 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.

Steps	Description
1.	Log in to G Suite with Google Admin account. For example, login to **https://admin.google.com**.
2.	In Admin Console, click on **Apps.**  Google Admin Search for users, groups, and settings (e.g. setup billing) Admin console Dashboard See relevant insights about your domain Users Add or manage users Groups Create groups and mailing lists Buildings and resources Manage and monitor buildings, rooms and resources Device management Secure corporate data on devices Apps Manage apps and their settings Security Manage security features Reports Track usage of services Billing View charges and manage licenses Company profile Update information about your company Admin roles Add new admins Domains Verify your domain or add domains Data migration Import email, calendar and contacts Support Talk with our support team
3.	In **App Settings**, click **SAML apps**.

	 Google Admin Search for users, groups, and settings (e.g. setup billing) Apps APPS SETTINGS Marketplace settings 13 G Suite G Suite Core Services These services are governed by your G Suite agreement. 50 Additional Google services Blogging, photos, video, social tools and more These services are not governed by your G Suite agreement, and other terms apply. Learn more 0 Marketplace apps More about Marketplace apps 0 SAML apps Manage SSO and User Provisioning
4.	**Add a service/Apps to your domain** or click **+** symbol.  Google Admin Search for users, groups, and settings (e.g. setup billing) Apps > SAML Apps Services Status ▲ Certificate No services/Apps configured for SAML. Add a service/App to your domain +
5.	Type “sharefile” to **Enable SSO for SAML Application**.

	 Google Admin Search for users, groups, and settings (e.g. setup billing) SAML Apps Services Status Certificate Step 1 Enable SSO for SAML Application Select an service/App for which you want to setup SSO sharefile Services / Provisioning supported ShareFile
6.	In **Google IdP Information**, Option 1, note your **SSO URL** and **Entity ID.**

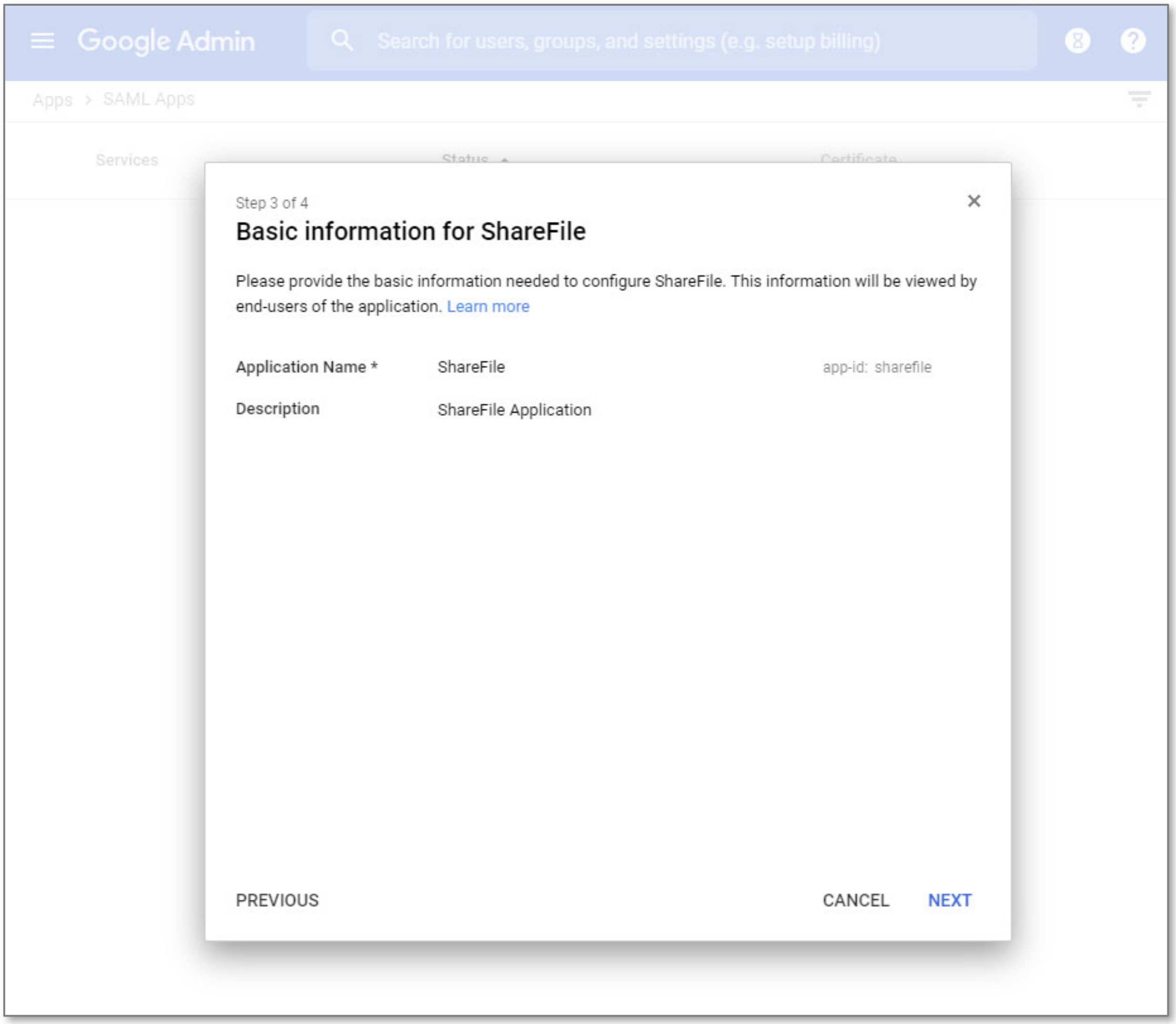
	 Google Admin Search for users, groups, and settings (e.g. setup billing) Apps > SAML Apps Services Status Certificate DOWNLOAD OR DOWNLOAD PREVIOUS CANCEL NEXT Step 2 of 4 Google IdP Information Choose from either option to setup Google as your identity provider. Please add details in the SSO config 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 Option 2 IDP metadata
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.

Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
GoogleIDPCertificate .pem
length : 1,253 lines : 18 Ln : 18 Col : 26 Sel : 0 | 0 Unix (LF) UTF-8 INS

```
-----BEGIN CERTIFICATE-----
[redacted]DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSBJ
[redacted]QYDVQQDEwZHb29nbGUxGDAWBgNVBAsTD0dv
b2dsZS[redacted]MxEzARBgNVBAgTCkNhbGlmb3JuaWEwHhcNMT[redacted]
MT[redacted]
TW91bnRhaW4gVmlldzEPMA0GA1UEAxMGR29vZ2xl[redacted]x
CzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAva6Gaan9bCP25wxfa24ZvaeNONgvkzOP+aFQu18cCFaVk6/JTBHfiI69bLGyNYf2
4X[redacted]/[redacted]PN3y26FK
[redacted]
rYQSpezdHaAAR/BVmrnVVpYwyL8iQFvMrPPb36HDDykxLRpCyhI2cEWpGs2Ju/F8AoZuAJt6qqqC
4W0HhWOmweVodo/UaQeGKmDUthkYsbW+0hBfpxXSrnr8oL8TwQIDAQABMA0GCSqGSIb3DQEBCwUA
A4IBAQC3vWT1TSLffR0OZ78/[redacted]sNbcnRvWWjnD8bDGJIZZ1ILW5GRYsa
[redacted]mFAT[redacted]E
[redacted]+D
A[redacted]L/WGJfzYcC4PHc8KWciCwb91nUjw
[redacted]
-----END CERTIFICATE-----
```

9.	Click Next, and confirm **Basic information for ShareFile**.



Step 3 of 4

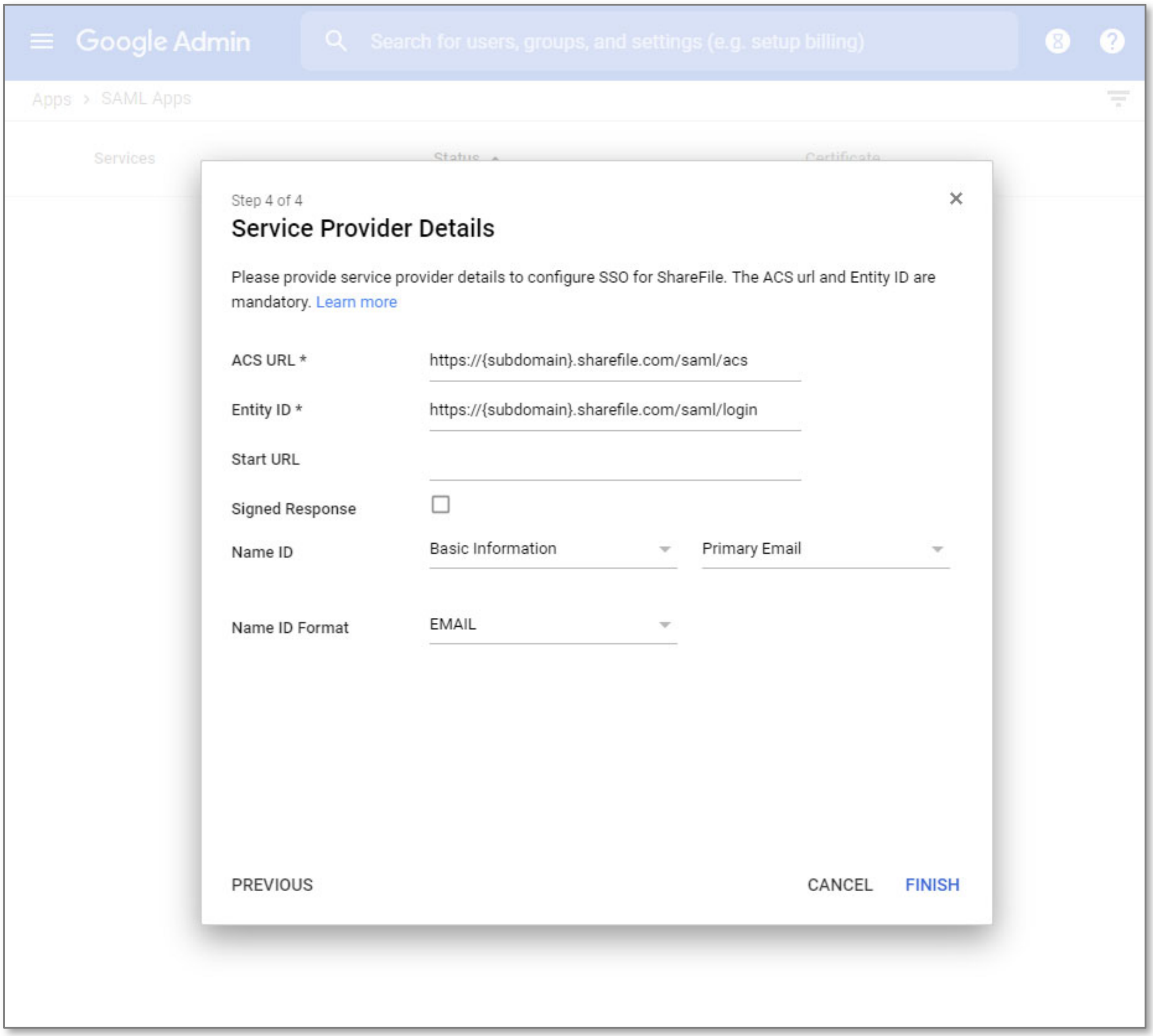
Basic information for ShareFile

Please provide the basic information needed to configure ShareFile. This information will be viewed by end-users of the application. Learn more

Application Name * ShareFile app-id: sharefile

Description ShareFile Application

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.



Step 4 of 4

Service Provider Details

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

ACS URL * https://{subdomain}.sharefile.com/saml/acs

Entity ID * https://{subdomain}.sharefile.com/saml/login

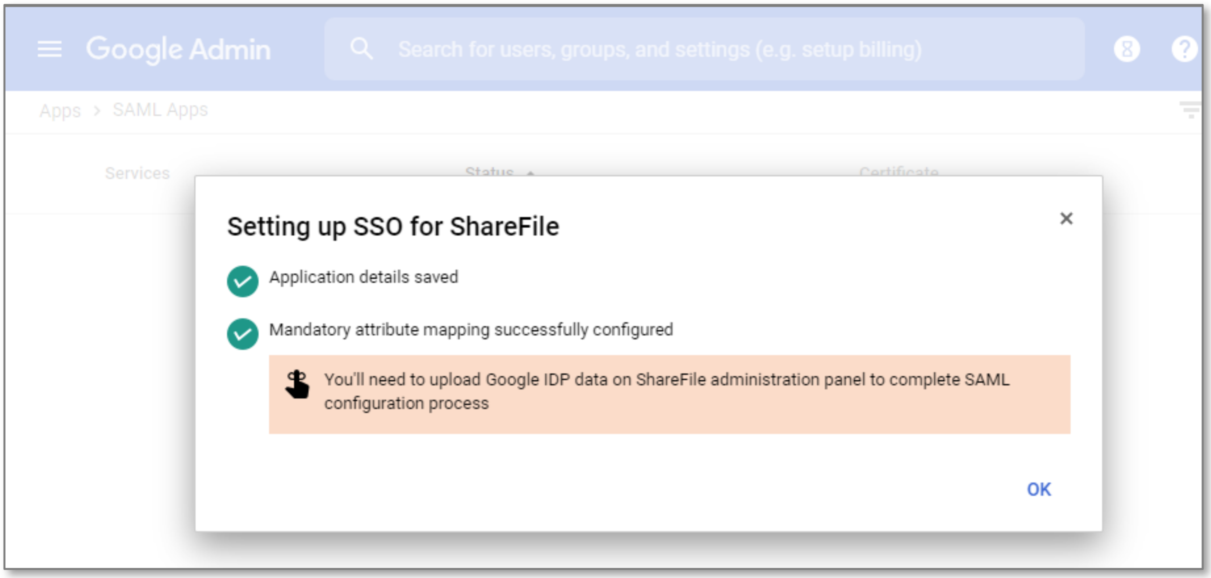
Start URL

Signed Response □

Name ID Basic Information Primary Email

Name ID Format EMAIL

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



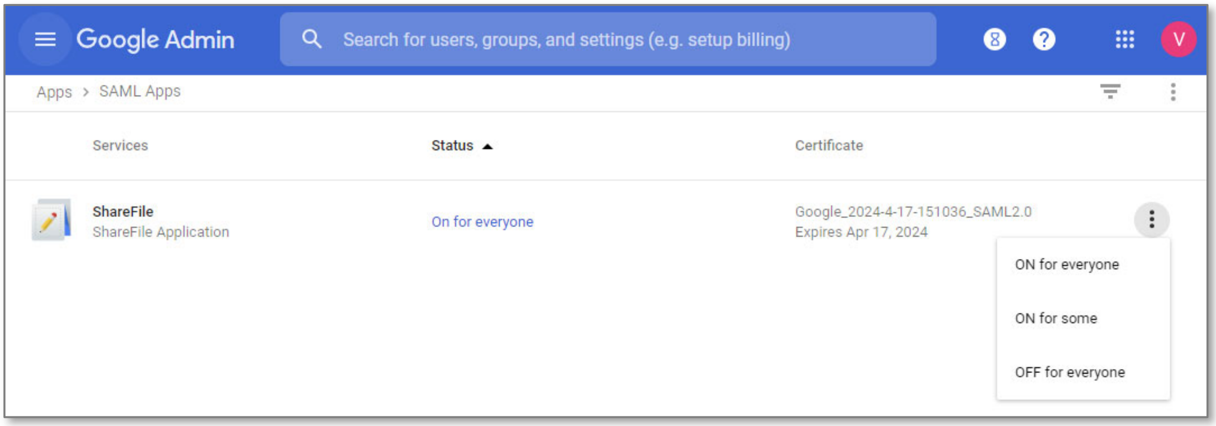
Setting up SSO for ShareFile

✓ Application details saved

✓ Mandatory attribute mapping successfully configured

You'll need to upload Google IDP data on ShareFile administration panel to complete SAML configuration process

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**.



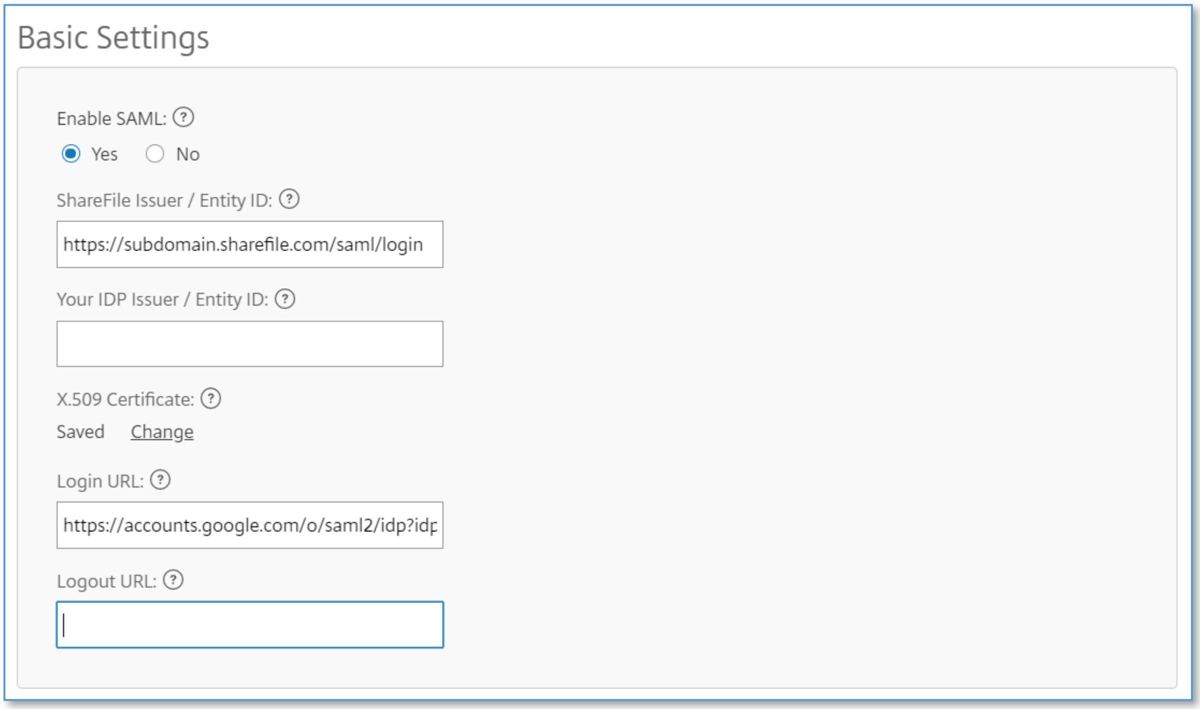
Services	Status	Certificate
ShareFile ShareFile Application	On for everyone	Google_2024-4-17-151036_SAML2.0 Expires Apr 17, 2024

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: https://subdomain.sharefile.com/saml/login

Your IDP Issuer / Entity ID:

X.509 Certificate: Saved Change

Login URL: https://accounts.google.com/o/saml2/idp?idp

Logout URL:

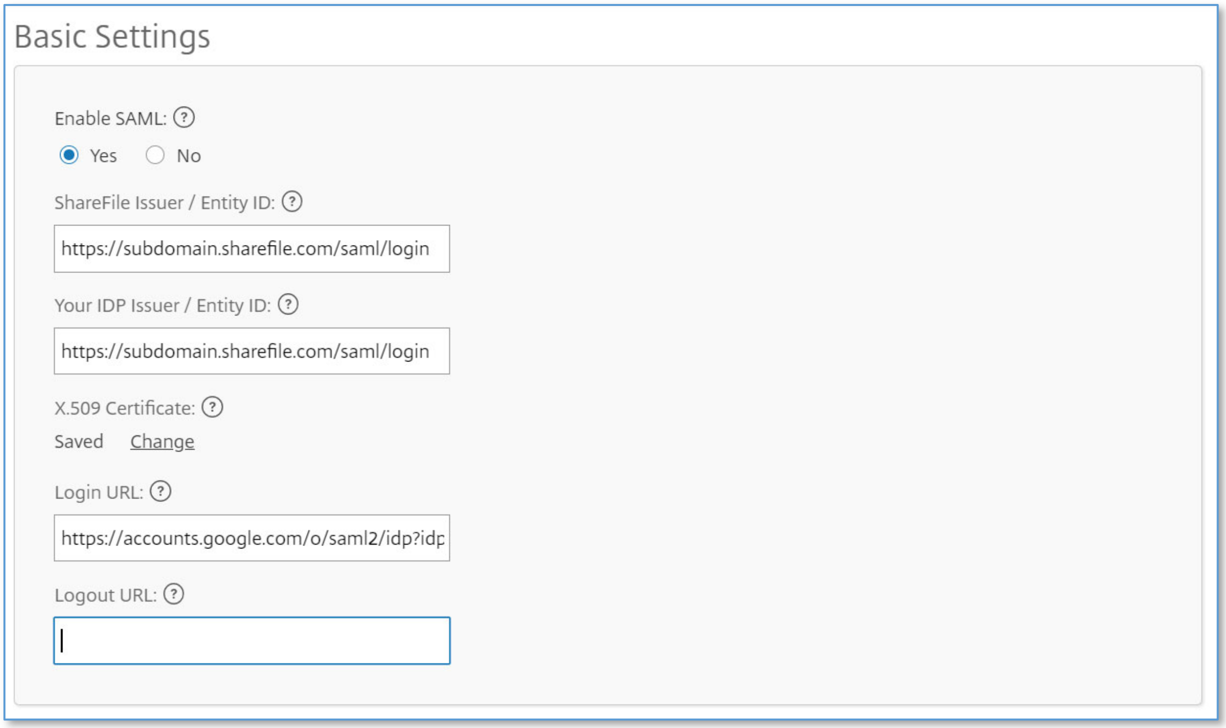
15. **NOTE**: If a value is saved in the **Your IDP Issuer / Entity ID** box, please read the following:

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: ?

https://subdomain.sharefile.com/saml/login

Your IDP Issuer / Entity ID: ?

https://subdomain.sharefile.com/saml/login

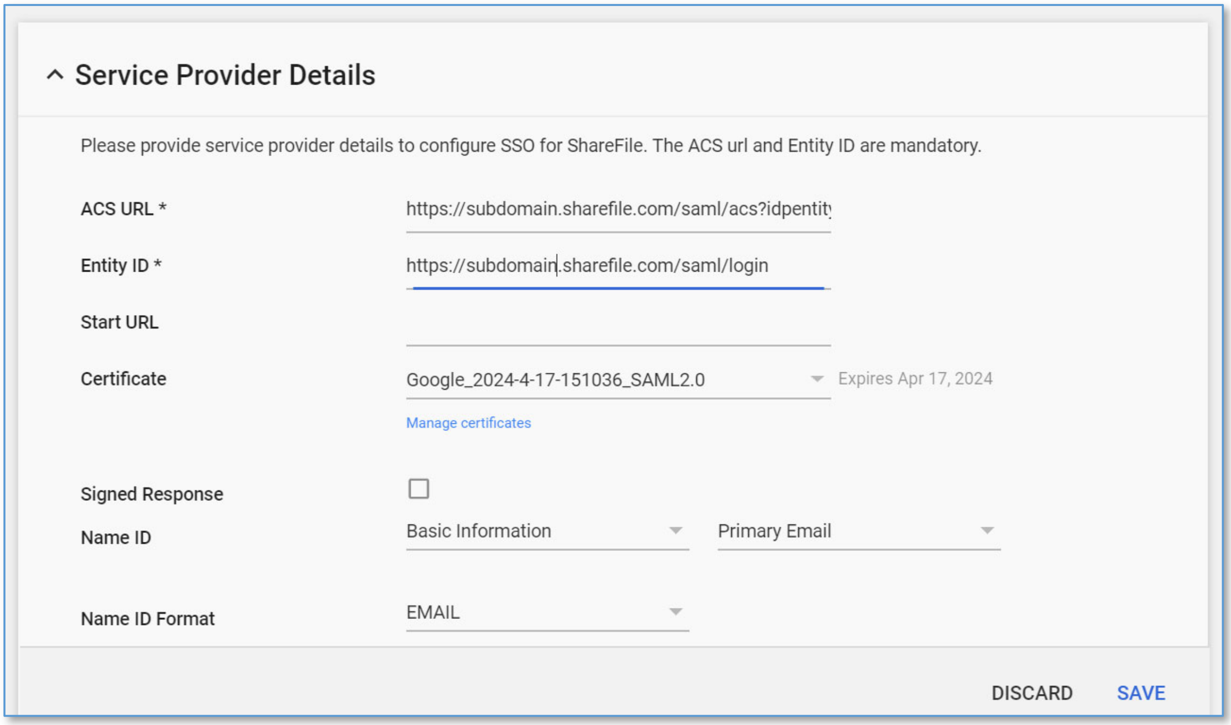
X.509 Certificate: ?

Saved Change

Login URL: ?

https://accounts.google.com/o/saml2/idp?idp

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 *	https://subdomain.sharefile.com/saml/acs?idpentit	
Entity ID *	https://subdomain.sharefile.com/saml/login	
Start URL		
Certificate	Google_2024-4-17-151036_SAML2.0 Manage certificates	Expires Apr 17, 2024
Signed Response	□	
Name ID	Basic Information	Primary Email
Name ID Format	EMAIL	

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.)

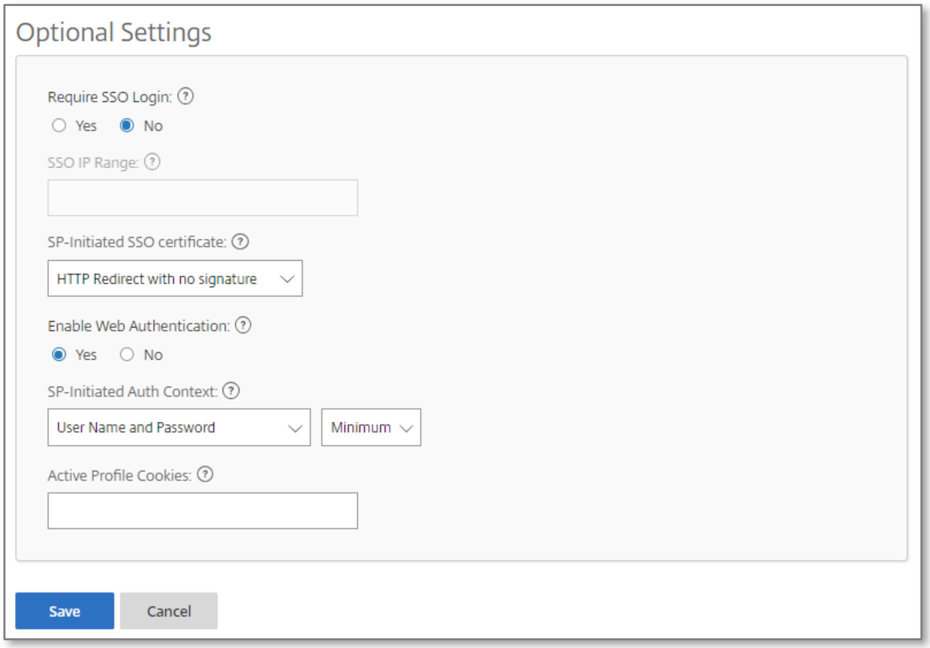
- **SP-initiated SSO Certificate**: Select **HTTP Redirect with no signature**

- **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

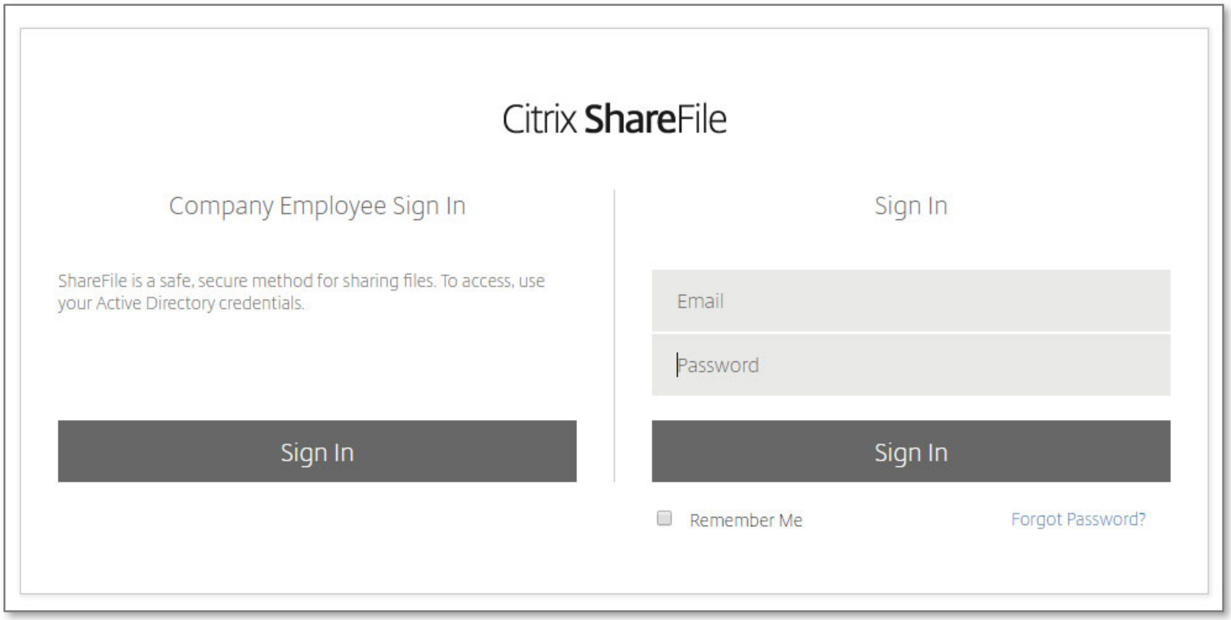
SP-Initiated Auth Context: ?
User Name and Password | Minimum

Active Profile Cookies: ?

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**



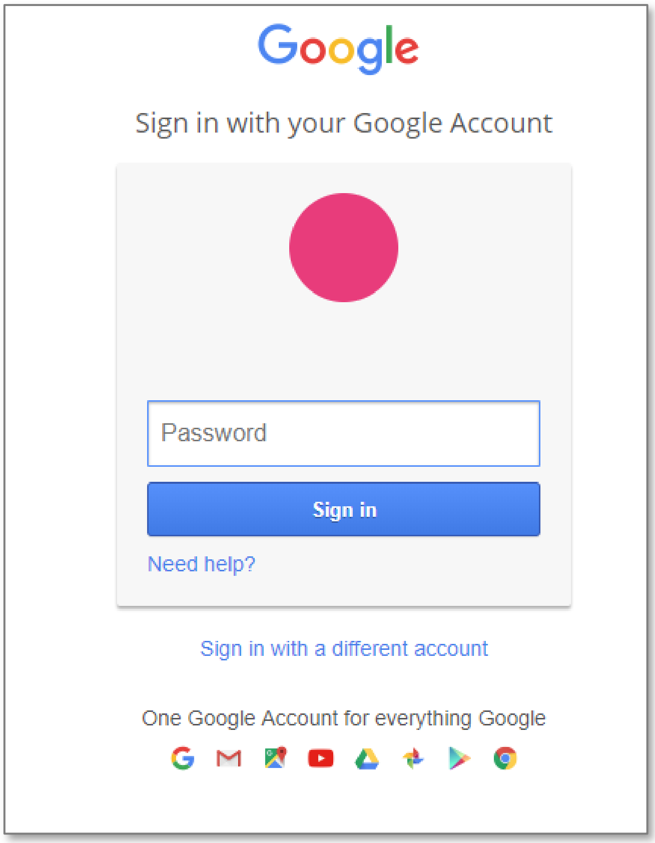
Citrix ShareFile

Company Employee Sign In

ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.

****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.**

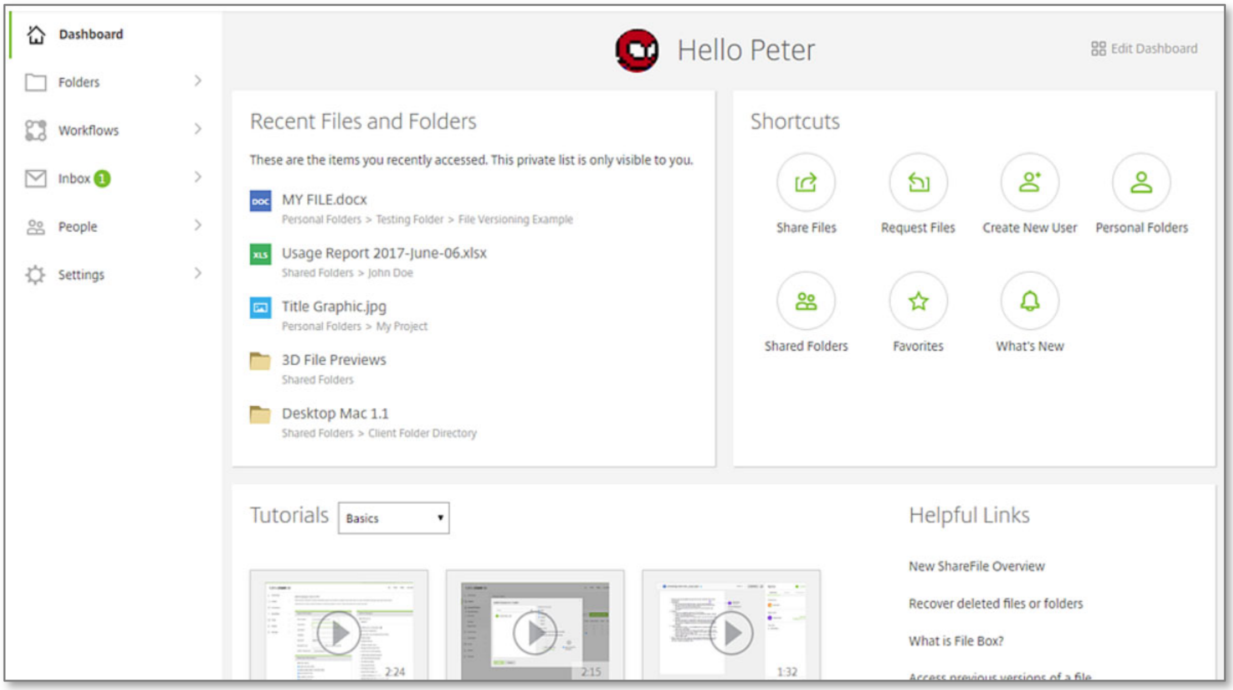
Sign in will redirect you to Google for sign in:



Sign in with your Google Account

One Google Account for everything Google

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



Hello Peter

Recent Files and Folders

These are the items you recently accessed. This private list is only visible to you.

MY FILE.docx
Personal Folders > Testing Folder > File Versioning Example

Usage Report 2017-June-06.xlsx
Shared Folders > John Doe

Title Graphic.jpg
Personal Folders > My Project

3D File Previews
Shared Folders

Desktop Mac 1.1
Shared Folders > Client Folder Directory

19. Done!