Configuring G-Suite

Complete the following steps to configure G-Suite:

- **Step 1**: Ensure that you have the following G-Suite information:
 - Entity ID: google.com/a/<domain_name>
 - Assertion Consumer Service URL: https://www.google.com/a/<domain_name>/acs
- **Step 2**: Create a Federated Pair in Access
- Step 3: Update G-Suite with proxy metadata and extract the certificate

Step 1: Credentials for G-Suite

These credentials are available from your provider. Ensure that you have the domain name for G-Suite.

- Entity ID: google.com/a/<domain_name>
- Assertion Consumer Service URL: <u>https://www.google.com/a/<domain_name>/acs</u>

Step 2: Create a Federated Pair in Access

You must create a federated pair in Access with the appropriate provider. For more information, see Overview.

Step 3: Update G-Suite with proxy metadata and extract the certificate

- 1. Login to G-Suite with admin credentials.
- 2. On the Security tab, click Set up SSO with the third party IdP.

Google Admin	Q. Search for users, groups, and settings (e.g. add domain alias)
rity	
	Password monitoring Monitor the password strength by user.
	Login challenges Manage the information used during login to protect users.
	Set up single sign-on (SSO) for SAML applications Setup user authentication for web based applications (like Gmail or Calendar).
	Set up single sign-on (SSO) with a third party IdP Set up single sign-on for managed Google Accounts using a third-party identity provider.
	Manage EMM provider for Android Keep your company's devices secure with an enterprise mobility management provider.
	Advanced Protection Program Configure the strongest security settings for those who need it most

- 3. Click the application that you created.
- 4. Update ACS URL, Entity ID, and Start URL links.

Note: You can extract the Entity ID value from Access SP metadata (Upload to IdP) file and paste it for ACS URL, Entity ID, and Start URL.

- 5. (Optional) Enter the Change password URL.
- 6. Upload the IDP certificate file.

Note: G-Suite does not let you upload a metadata file. The information must be extracted from the IDP proxy metadata file. Extract the *Entity ID* from the IDP proxy metadata file.

- 1. Open the SP proxy metadata file that you downloaded when configuring Access for the federated pair.
- 2. Extract the certificate from the IDP proxy metadata file and save it in the .cer file.