



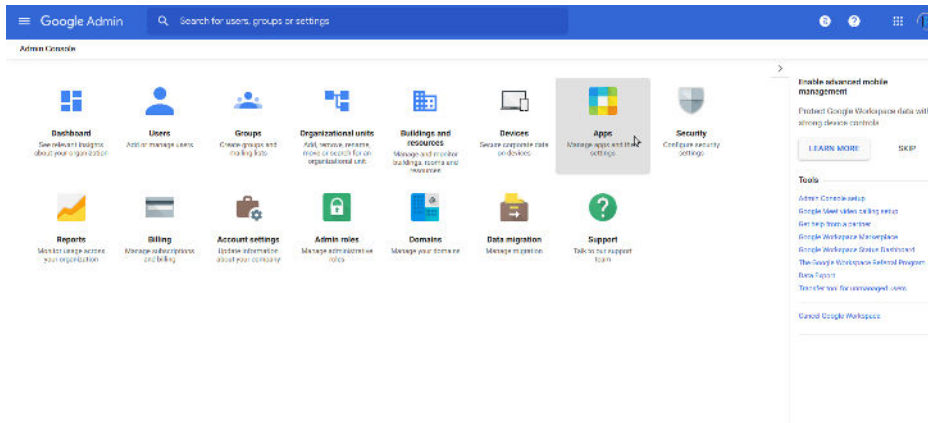
# SAML2 Integration

CPTeller

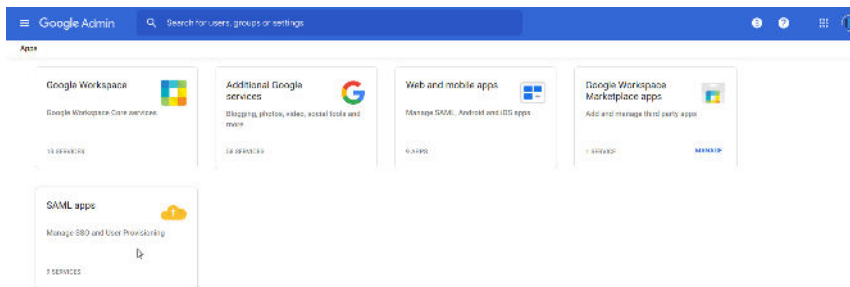
# Google Workspace Integration

To add your Google Workspace as an IdP for the IntelliPay CPTeller Portal:

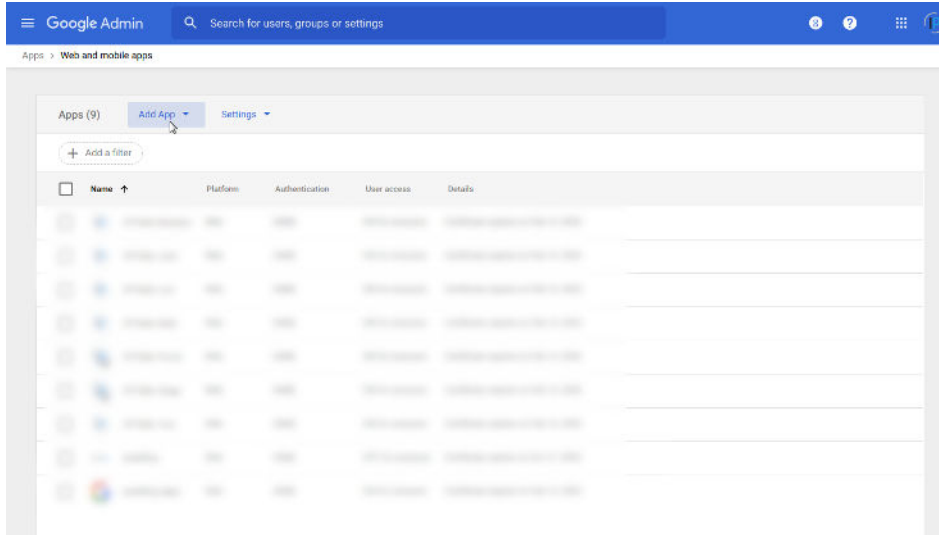
1. Sign in as an administrator to your Google Admin console.
2. Click on **Apps**.



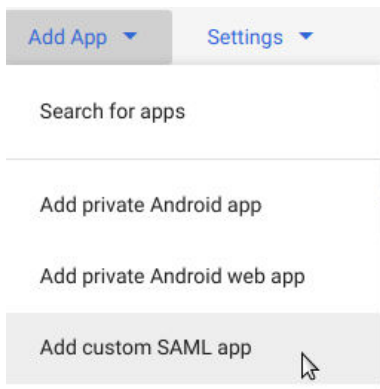
3. Click on **SAML Apps (Or Web and mobile apps, if not showing)**.



4. Click on the **Add App** dropdown.



5. From the Add App dropdown select **Add custom SAML App**.



6. Enter the **App name** and upload an **App icon** you prefer to use to identify the IntelliPay CPTeller portal and select **CONTINUE**.

**App details**


Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)

App name

App name is required

**App icon**

Attach an app icon. Maximum upload file size: 4 MB



CANCEL CONTINUE



8. Enter the **ACS URL** supplied to you by the support team. The **Entity ID** will be <https://secure.cpteller.com/login> , as shown. Select **EMAIL** for the **Name ID format**. Basic Information > Primary email should appear in the **Name ID** section. Click on **CONTINUE**.

**Service provider details**

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL

Entity ID

Start URL (optional)

Signed response

**Name ID**

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format

Name ID

BACK CANCEL

9. In the Attributes dialog click ADD MAPPING and add mappings for “department”, “firstname”, “lastname”, and “phone”, as shown. If desired you can have a user directed into the OneLink terminal by specifying a “dest” attribute of “onelink”. You can configure additional user attributes in the Google Workspace Users Directory in the **More** dropdown, but the mapping must be added here.

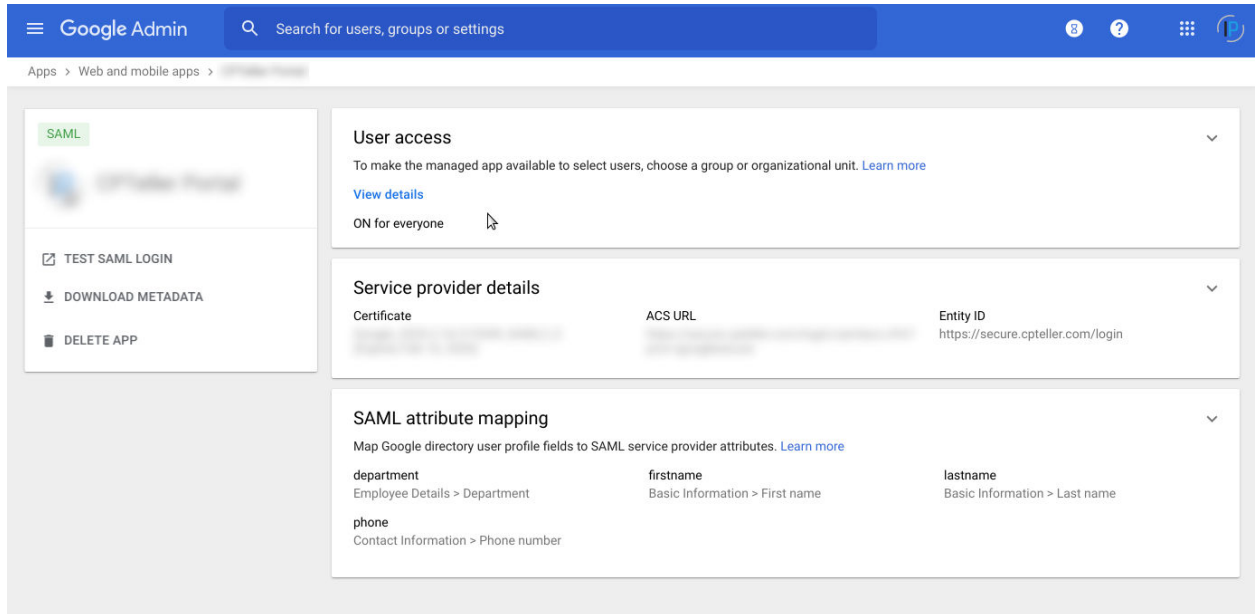
The screenshot shows a dialog titled "Attributes" with a subtitle: "Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with \* are mandatory. [Learn more](#)".

The dialog is divided into two columns: "Google Directory attributes" and "App attributes".

Google Directory attributes	App attributes
Employee Details > Department	department
Basic Information > First name	firstname
Basic Information > Last name	lastname
Contact Information > Phone number	phone

At the bottom of the dialog, there is an "ADD MAPPING" button. Below the dialog, there are three buttons: "BACK", "CANCEL", and "FINISH".

10. Click on **FINISH**. The application should now show in the list. Select the application and enable which users you'd like to have access to the IntelliPay CPTeller portal.



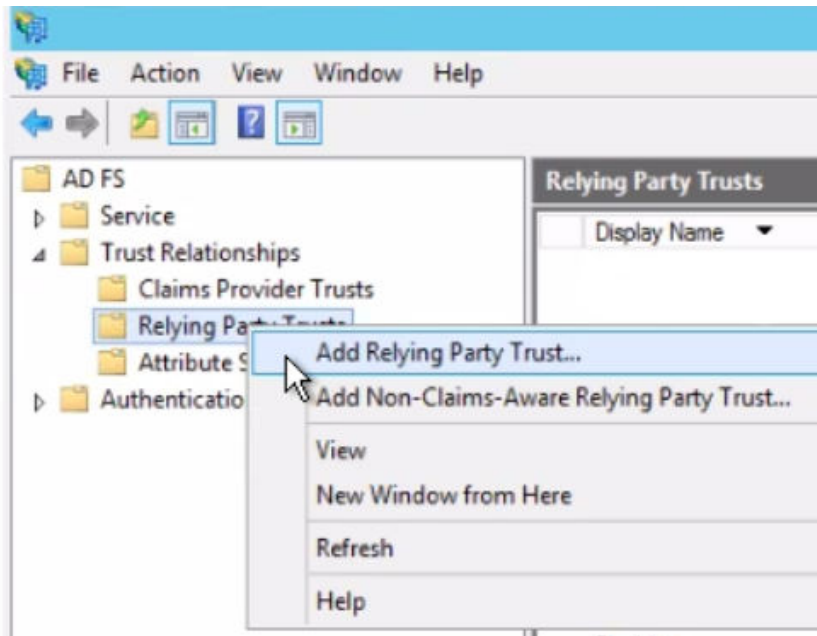
11. You should be able to use SAML authentication with the IntelliPay CPTeller portal.



## Microsoft ADFS Integration

To setup Microsoft AD FS as an IdP for the IntelliPay CPTeller Portal see <https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/configure-saml-2-settings> and follow these steps.

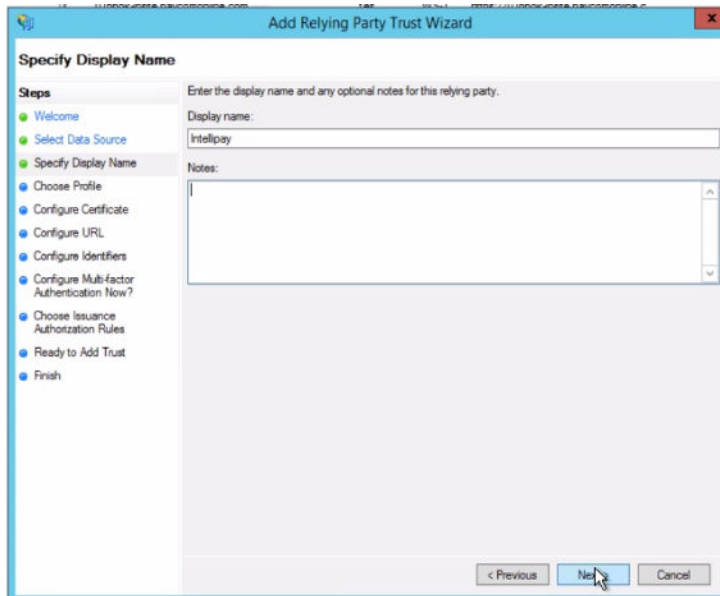
1. Using the AD FS Management tool, select Trust Relationships >Relying Party Trusts then select **Add Relying Party Trust**.



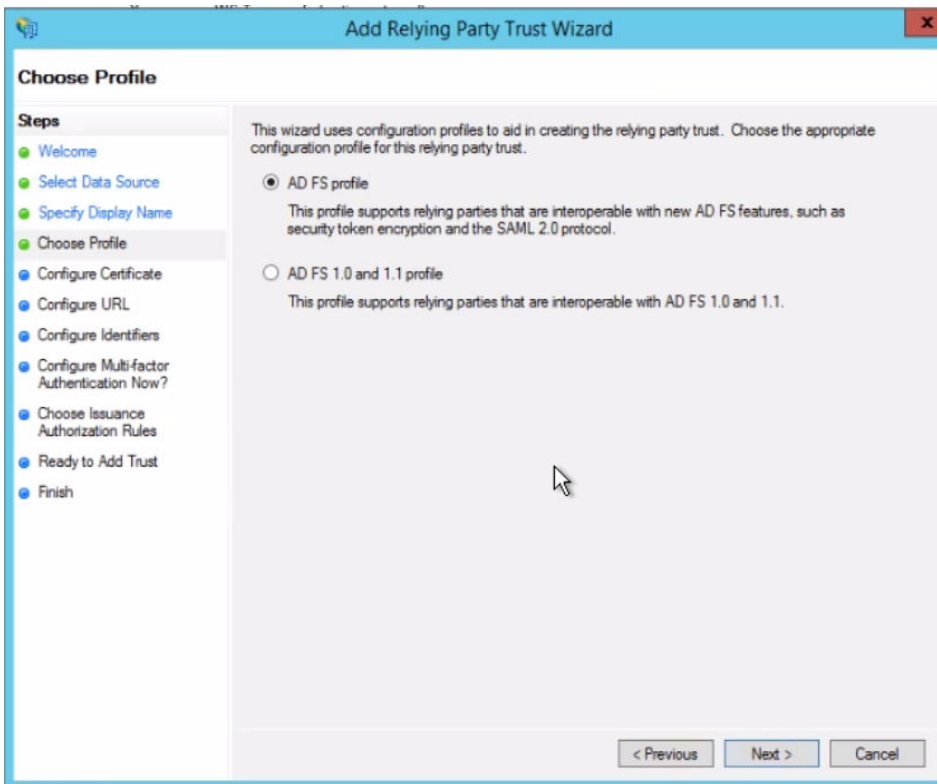
2. In *Welcome*: select **Start**. Then in *Select Data Source*: Select **Enter data about the relying party manually**, and then select **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main window has a light blue header and a white background. On the left, there is a 'Steps' pane with a list of steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Select Data Source' and contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network'. Below this is a text box for 'Federation metadata address (host name or URL):' with an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Below this is a text box for 'Federation metadata file location:' and a 'Browse...' button. 3. 'Enter data about the relying party manually'. Below this is the text: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right, there are three buttons: '< Previous', 'Next >' (with a mouse cursor over it), and 'Cancel'.

3. *Specify Display Name*: Enter a name, and then select **Next**. Example: “IntelliPay”



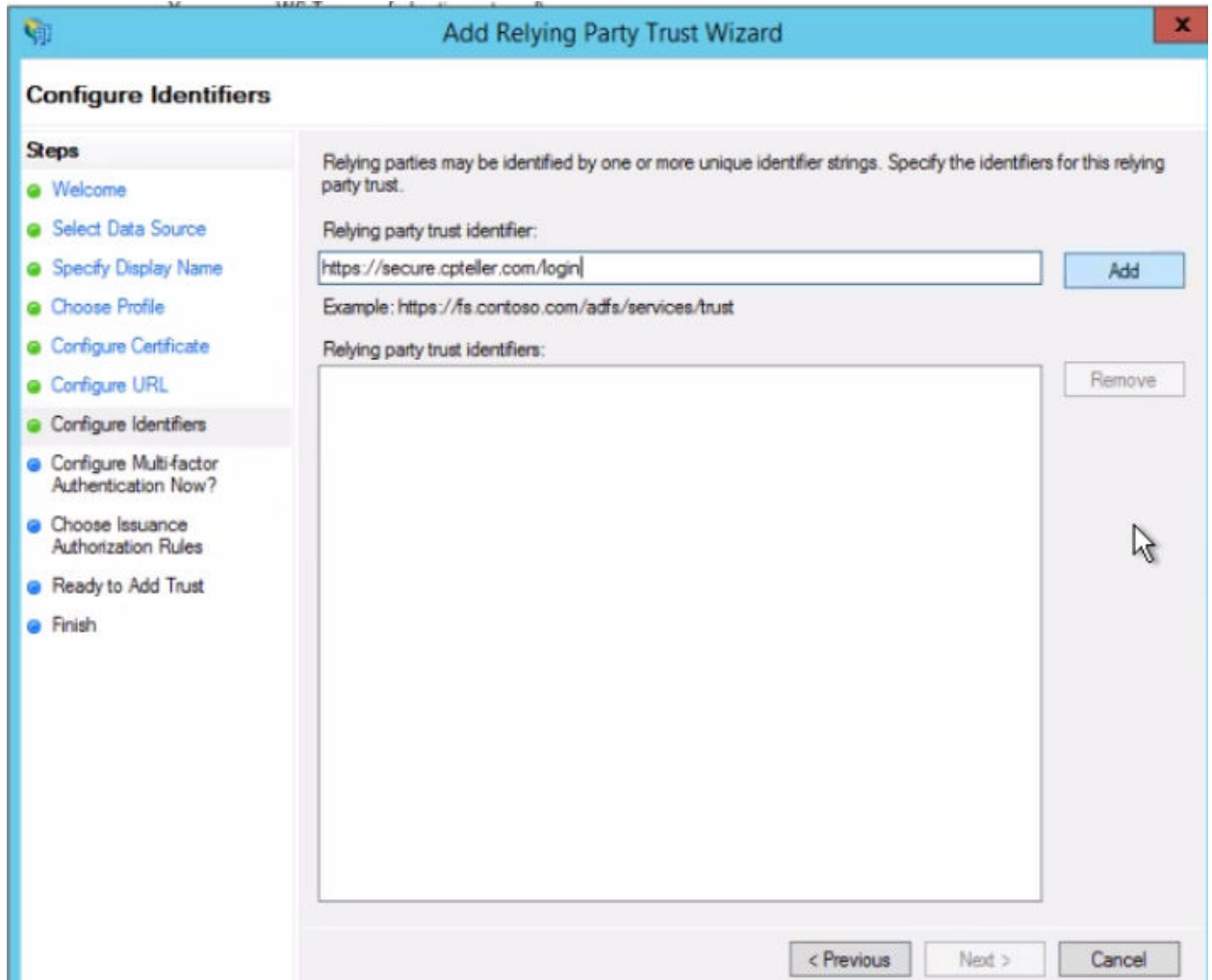
4. *Choose Profile*: Select **AD FS (2.0) profile**, and then select **Next**.



5. Configure Certificate: Select **Next**. Configure URL: Select the **Enable support for the SAML 2.0 WebSSO protocol** check box. In **Relying party SAML 2.0 SSO service URL** enter the ACS url provided to you by the IntelliPay support team.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure URL' step. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL (highlighted), Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.' There are two options: 'Enable support for the WS-Federation Passive protocol' (unchecked) and 'Enable support for the SAML 2.0 WebSSO protocol' (checked). Below the first option is a text box for 'Relying party WS-Federation Passive protocol URL:' with an example: 'https://fs.contoso.com/adfs/ls/'. Below the second option is a text box for 'Relying party SAML 2.0 SSO service URL:' with an example: 'https://www.contoso.com/adfs/ls/'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

6. Configure Identities: In **Relying party trust identifier** enter <https://secure.cpteller.com/login> , select **Add**, and then select **Next**. If applicable, you can add more identities for each additional relying party portal. Users can authenticate across any or all available identities.



7. Choose Issuance Authorization Rules: Select **Permit all users to access this relying party** (Or configure as needed), and then select **Next**. Ready to Add Trust: Select **Next**. Select **Close**.

- To edit the Claim Rules, select the **Relying Party Trusts** folder from **AD FS Management**, and choose **Edit Claim Rules** from the **Actions** sidebar. Configure as shown below. If desired you can have a user directed into the OneLink terminal by specifying a “dest” attribute of “onelink”.

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	Name ID
	Department	Department
	Given-Name	firstname
	Surname	lastname
*		

- Click **OK**. You should be able to use SAML authentication with the IntelliPay CPTeller portal.