Security Awareness Training Partner Guide

Federated Login or Native MFA Setup

Microsoft 365, Okta and Google Activation and client integration

Telesystem
IT's About Trust

#HackersSuck

www.TrustTelesystem.com

Federated Login Setup

Table of Contents

General Information

Important information on Federated Login

What is Federated Login? – Federated Login enables your client's users to use a single authentication token to access their PII Protect portal synced with their Microsoft 365, Okta, or Google accounts.

Why Federated Login? – This feature will allow *you* to control client passwords and any additional authentication methods at the Microsoft 365, Okta, and Google level, making passwords more secure and easier to manage. Additional benefits include: One less password for employees to remember meaning fewer resets and lockouts, unified password policies, and ability to enforce Multi-Factor Authentication (MFA).

Which clients can use Federated Login? – Any client in any product can use Federated Login. The client would need to have either a Microsoft 365, Okta, or Google G-Suite account.

Important information on Native MFA

For clients that do not have the ability to turn on Federated Login, our native MFA features will help secure accounts. This feature is simple to activate, and the verification process is simple for users on their Authenticator application.

Federated Login Information

Let's Get Started!

The Federated Login setup process will differ based on Microsoft 365, Okta, or Google that the client is using.

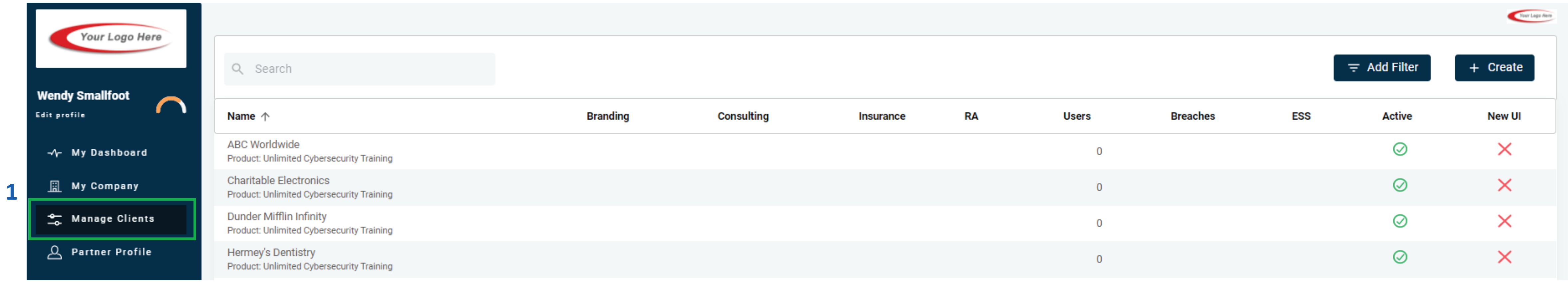
Microsoft 365: If the client you are configuring Federated Login for is using **Microsoft 365**, please begin on page 5.

Okta: If the client is using Okta, please begin on page 14.

Google: If the client you are configuring Federated Login for is using **Google**, there are no initial configuration steps. Please begin at page 26. Federated Login for Google can be quickly enabled for the client within the PII Protect portal, upon the user's next login to the PII Protect portal they will be prompted to enter their Google credentials via the Google interface.

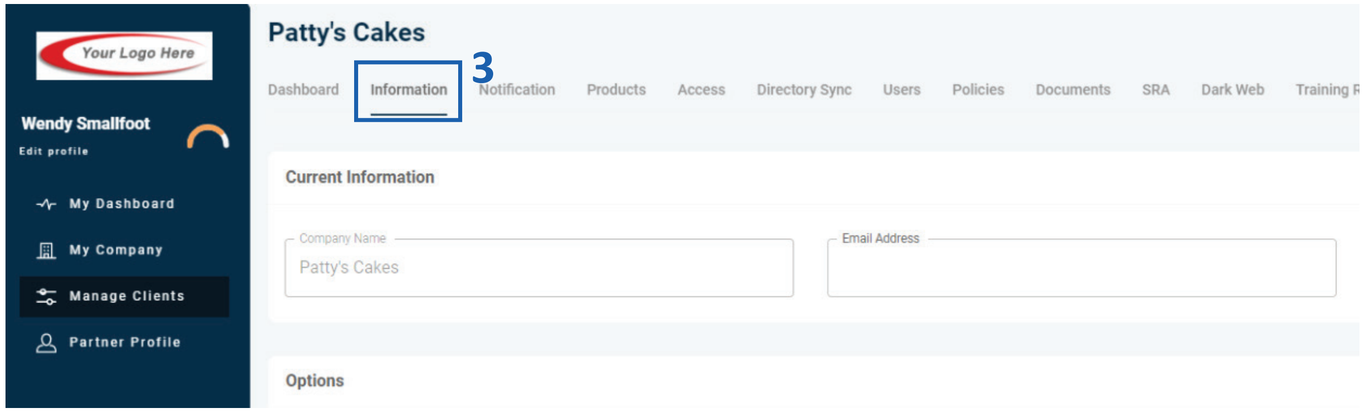
Enabling Native Multi-Factor Authentication (MFA)

Navigating to the Information Screen



Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			✓	✗

1. Login as a Partner Administrator to the PII-Protect portal here. Once logged in select "**Manage Clients**" to access your client list (above).
2. Select the client you want to enable Microsoft 365 Federated Login for.
3. Click on the "**Information**" tab at the top
4. In the "Password" section, click the slider to turn "green" to enable MFA access for this client

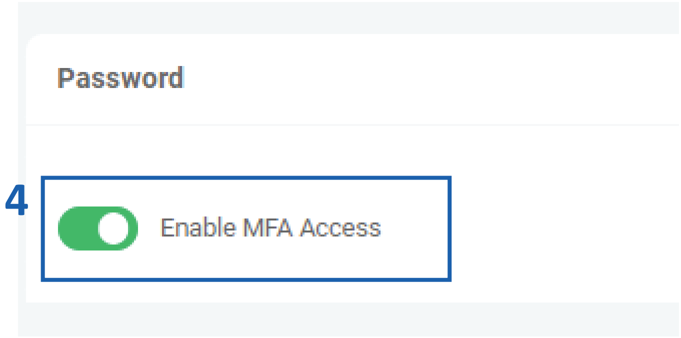


Current Information

Company Name: Patty's Cakes

Email Address:

Options



Password

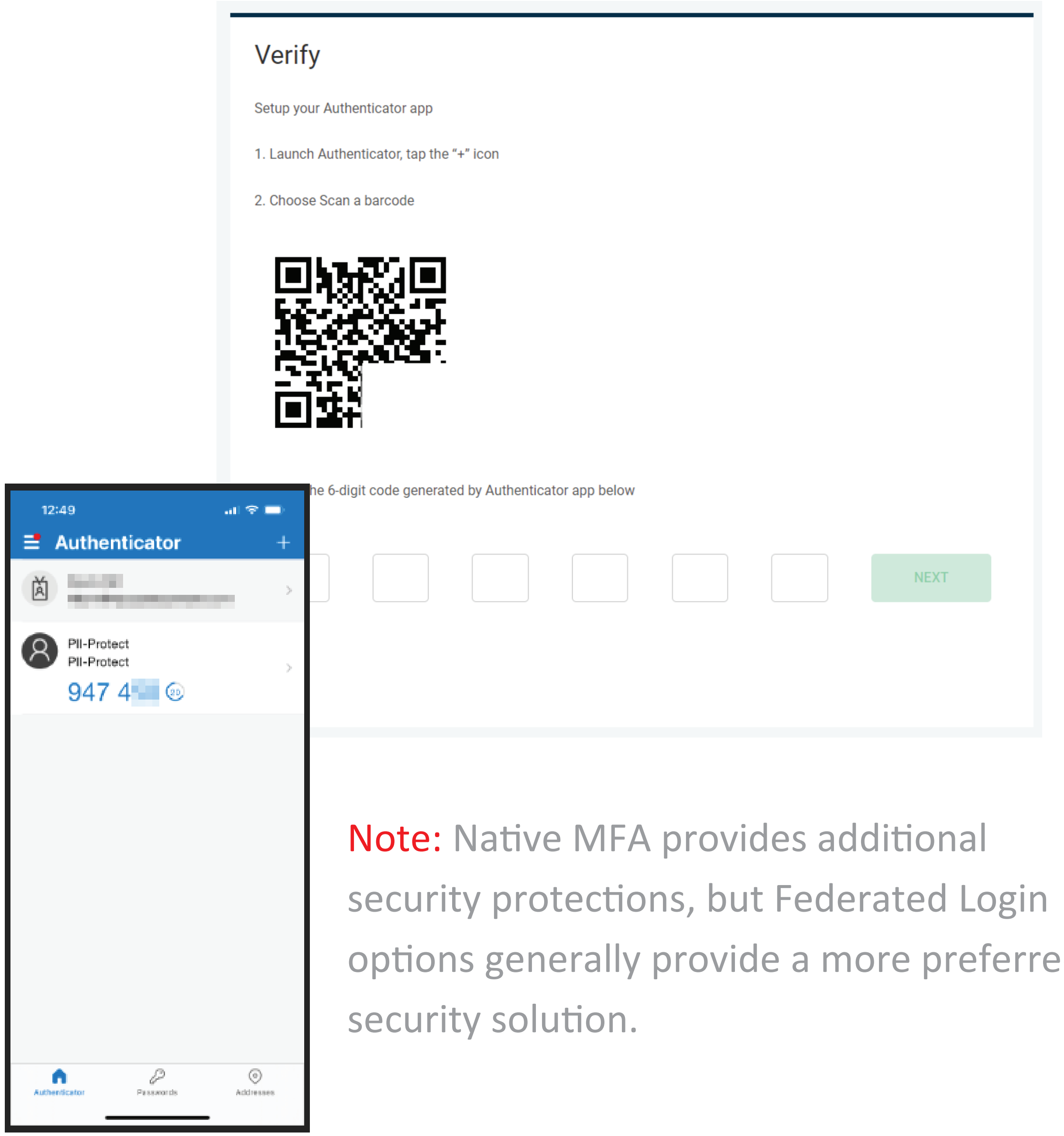
● Enable MFA Access

Enabling Native Multi-Factor Authentication (MFA)

Client Verification Process with MFA

Client MFA is now enabled! Upon the next login for users within this Client, a verification page will be shown. Users should open their Authenticator Application to add PII Protect as a new account. A scannable QR code will be presented and once scanned will provide a unique passcode to enter back on the PII Protect portal verification page.

For future login attempts, after entering their email address and password, users can retrieve their passcode within their Authenticator app.



Verify

Setup your Authenticator app

1. Launch Authenticator, tap the "+" icon

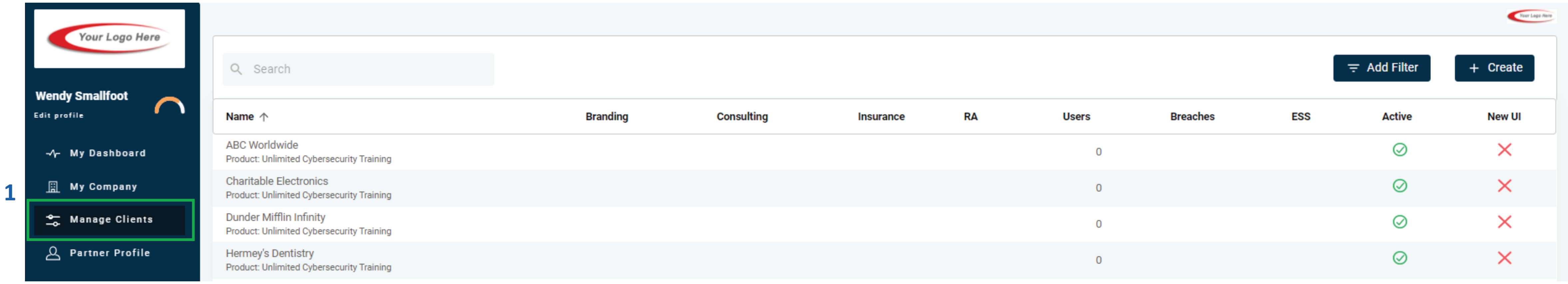
2. Choose Scan a barcode

he 6-digit code generated by Authenticator app below

Note: Native MFA provides additional security protections, but Federated Login options generally provide a more preferred security solution.

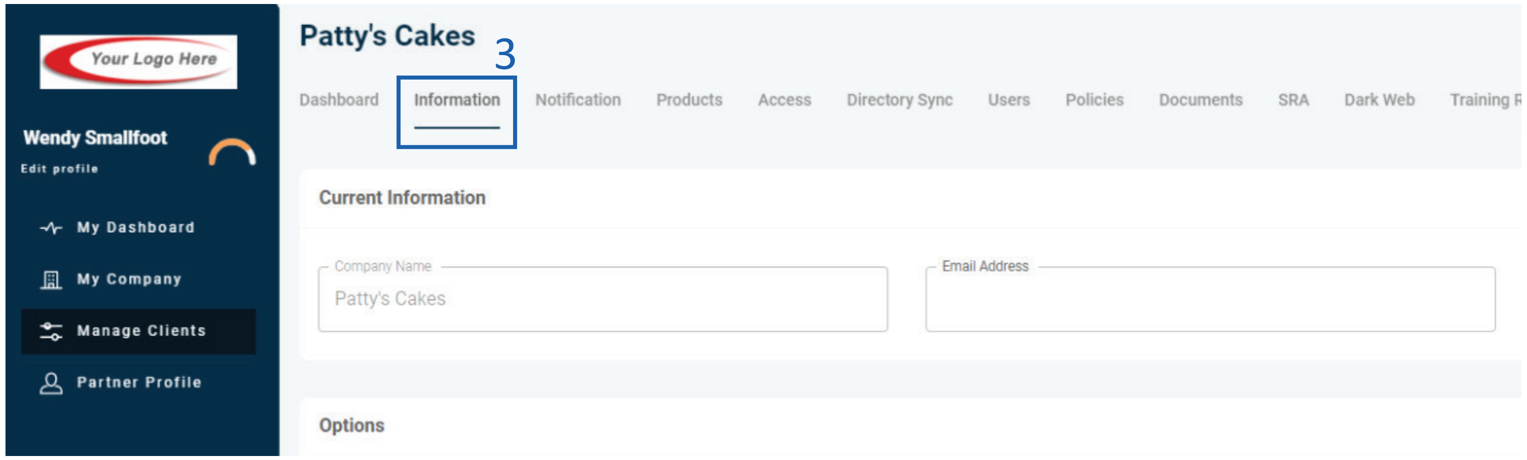
Configuring Federated Login Within the PII Protect Portal – Microsoft 365

Navigating to the Client View Screen



Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			✓	✗

1. Login as a Partner Administrator to the PII-Protect portal here. Once logged in select "**Manage Clients**" to access your client list (above).
2. Select the client you want to enable **Microsoft 365** Federated Login for.
3. Click on the "**Information**" tab at the top



Current Information

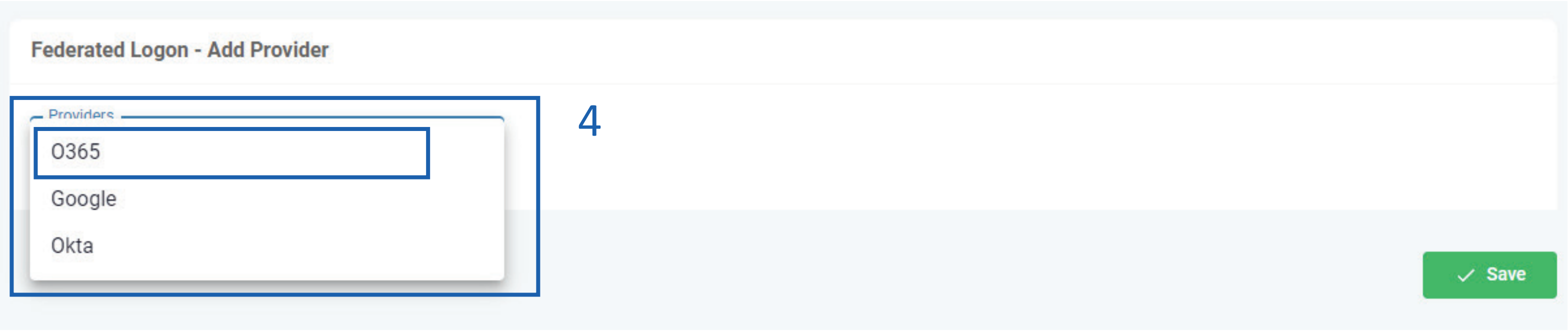
Company Name: Patty's Cakes

Email Address:

Options

Configuring Federated Login Within the PII Protect Portal – Microsoft 365

Configure Federated Login Settings



Federated Logon - Add Provider

Providers

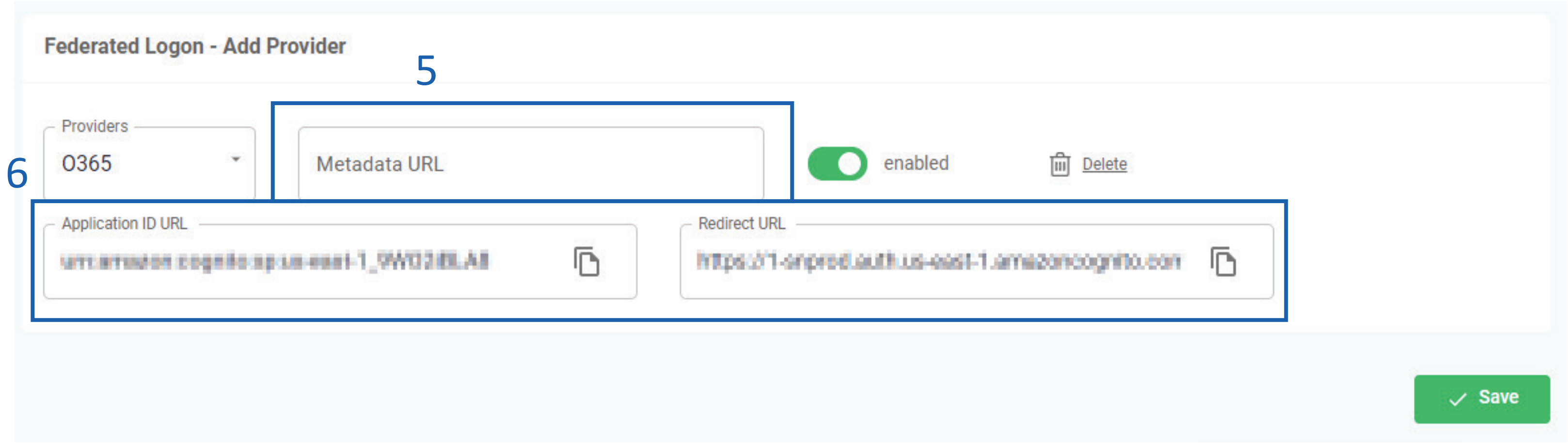
O365

Google

Okta

4. At the bottom of the screen for Federated Logon, select "**O365**"

5. You will need a **Metadata URL** that will become available when set up in the Azure Admin Center.



Federated Logon - Add Provider

Providers: O365

Metadata URL

enabled

Delete

Application ID URL: [redacted]

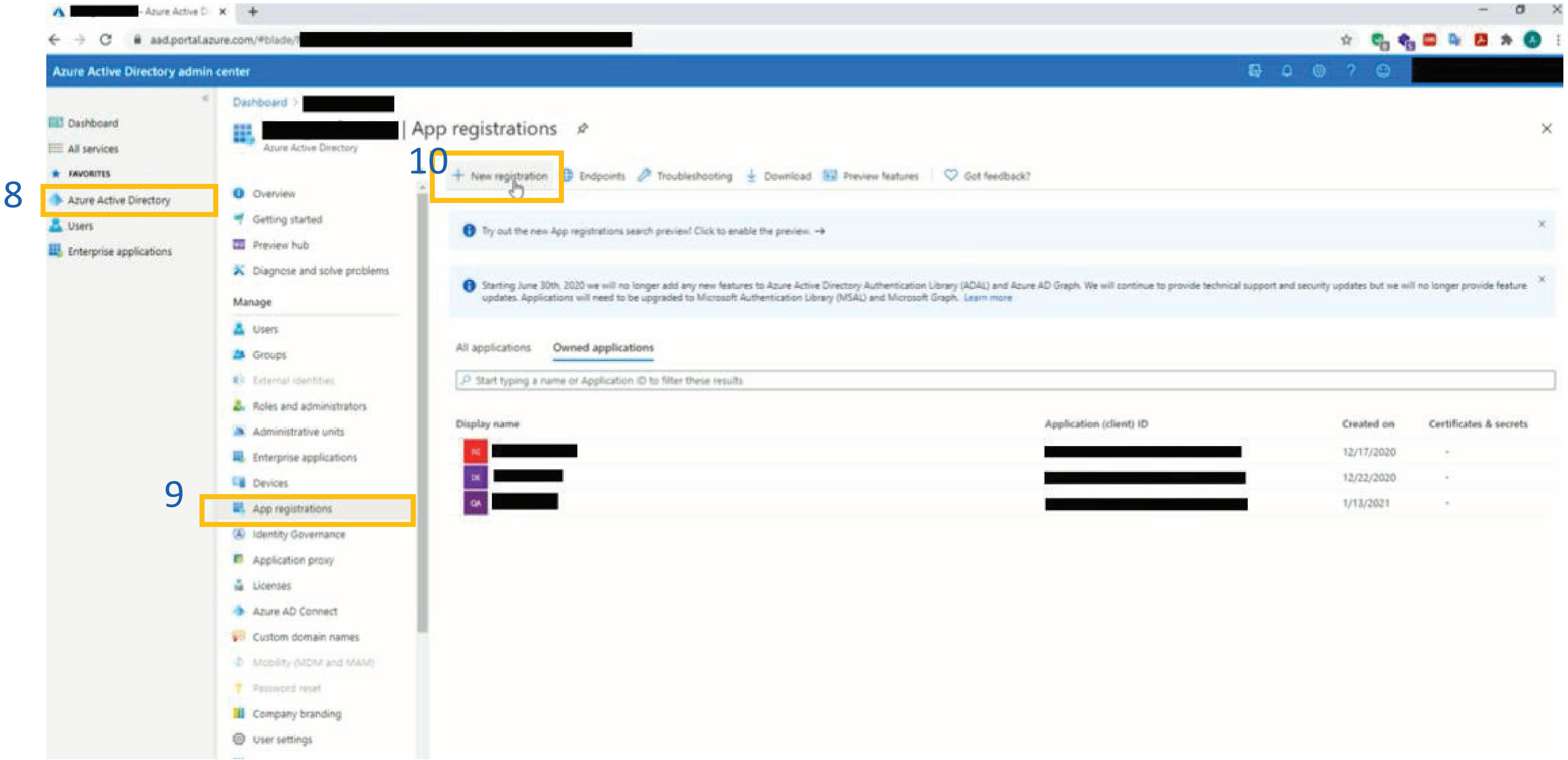
Redirect URL: [redacted]

6. Note that the "**Application ID URL**" and "**Redirect URL**" are filled in. You will be using these URLs in the next Azure steps so keep this page open.

7. Access the Azure Admin environment for this client account.

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center



Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Start typing a name or Application ID to filter these results

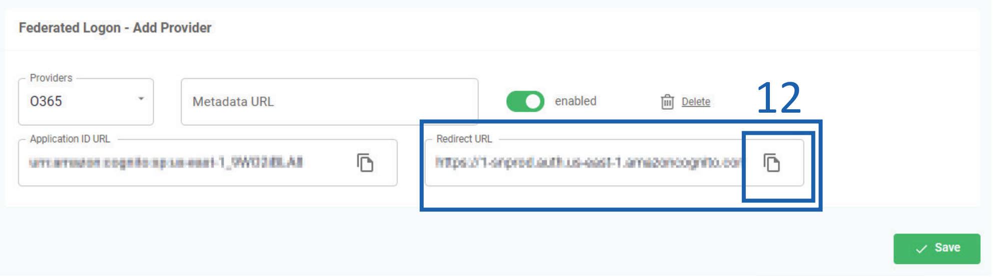
Display name	Application (client) ID	Created on	Certificates & secrets
[redacted]	[redacted]	12/17/2020	-
[redacted]	[redacted]	12/22/2020	-
[redacted]	[redacted]	1/13/2021	-

8. Select “**Azure Active Directory**”
9. Select “**App Registrations**”
10. Select “**New registration**”

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center

11. Enter name for application (example "prod-portal")
12. Return to your PII Protect portal page and locate the **Redirect URL**. Click the "Copy" button.
13. Return to the Azure Admin Center and paste this URL into the "Redirect URL" section.
14. Click "**Register**"



Federated Logon - Add Provider

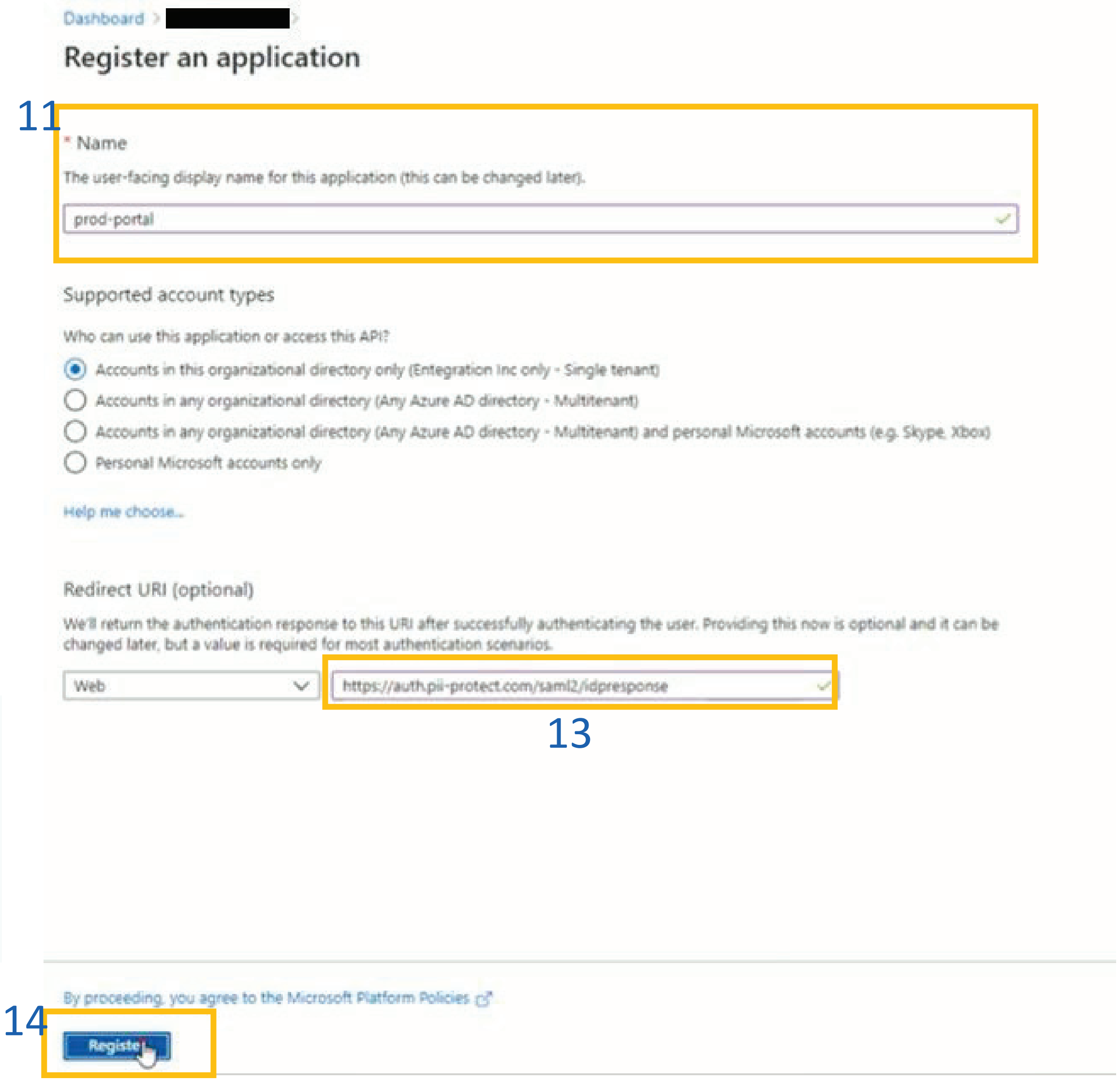
Providers: O365

Metadata URL

enabled

Application ID URL: [illegible]

Redirect URL: [illegible]



Register an application

* Name

The user-facing display name for this application (this can be changed later).

prod-portal

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (Entegration Inc only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

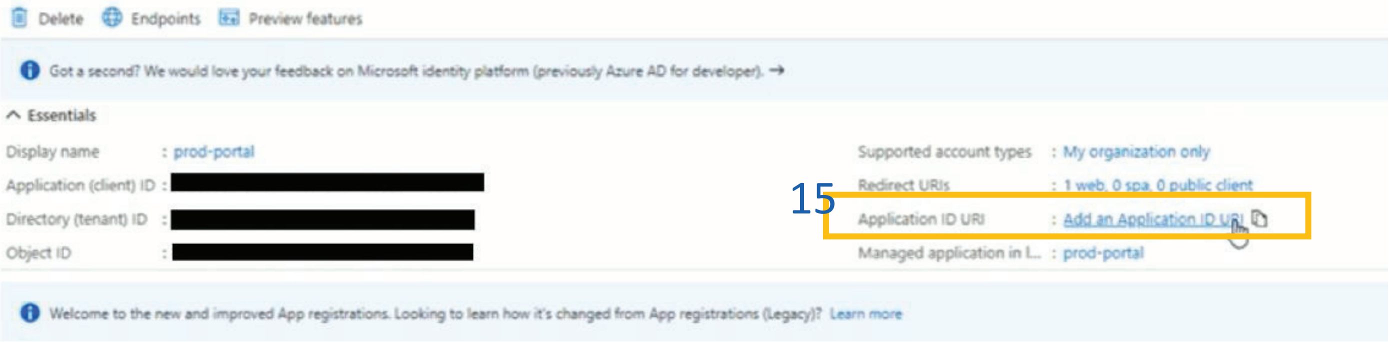
Web: https://auth.pii-protect.com/saml2/idpresponse

By proceeding, you agree to the Microsoft Platform Policies

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center

15. Click “**Add an Application ID URI**”
16. Click “**Set**”
17. Return to your PII Protect portal page and locate the Application ID URL. Click the “Copy” button.
18. Return to the Azure Admin Center and paste this URL into the “Set the App ID URL” section.
19. Click “**Save**”



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : prod-portal

Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

Object ID : [redacted]

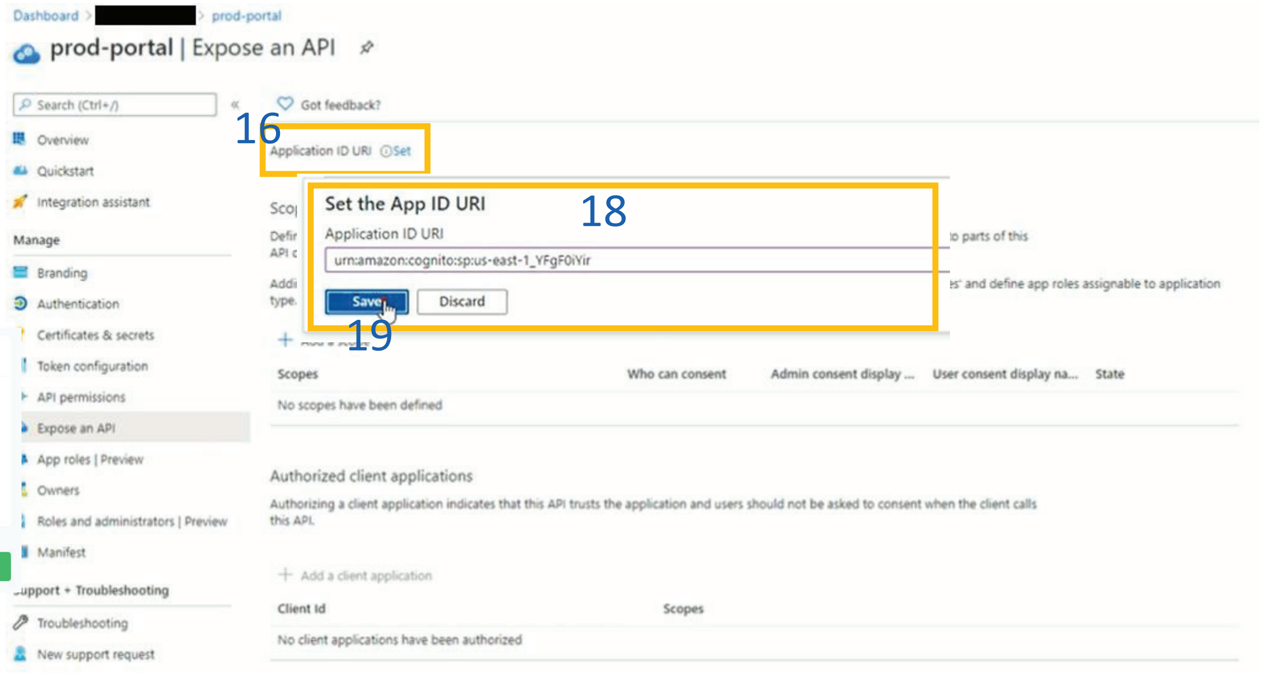
Supported account types : My organization only

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in l... : prod-portal

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more



Application ID URI ⓘ Set

Set the App ID URI

Application ID URI: urn:amazon:cognito:sp:us-east-1_YFgF0iYir

Scopes | Who can consent | Admin consent display ... | User consent display na... | State

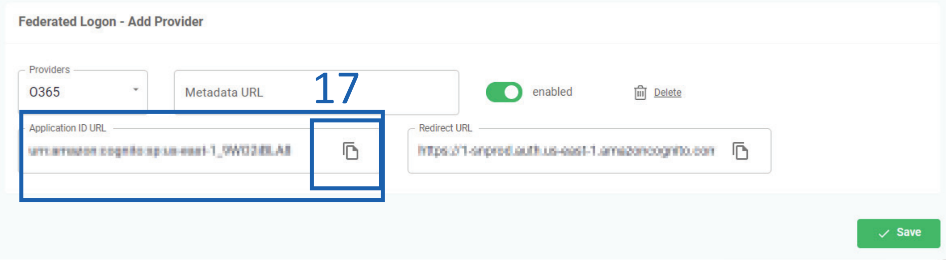
No scopes have been defined

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

Client Id | Scopes

No client applications have been authorized



Federated Logon - Add Provider

Providers: O365

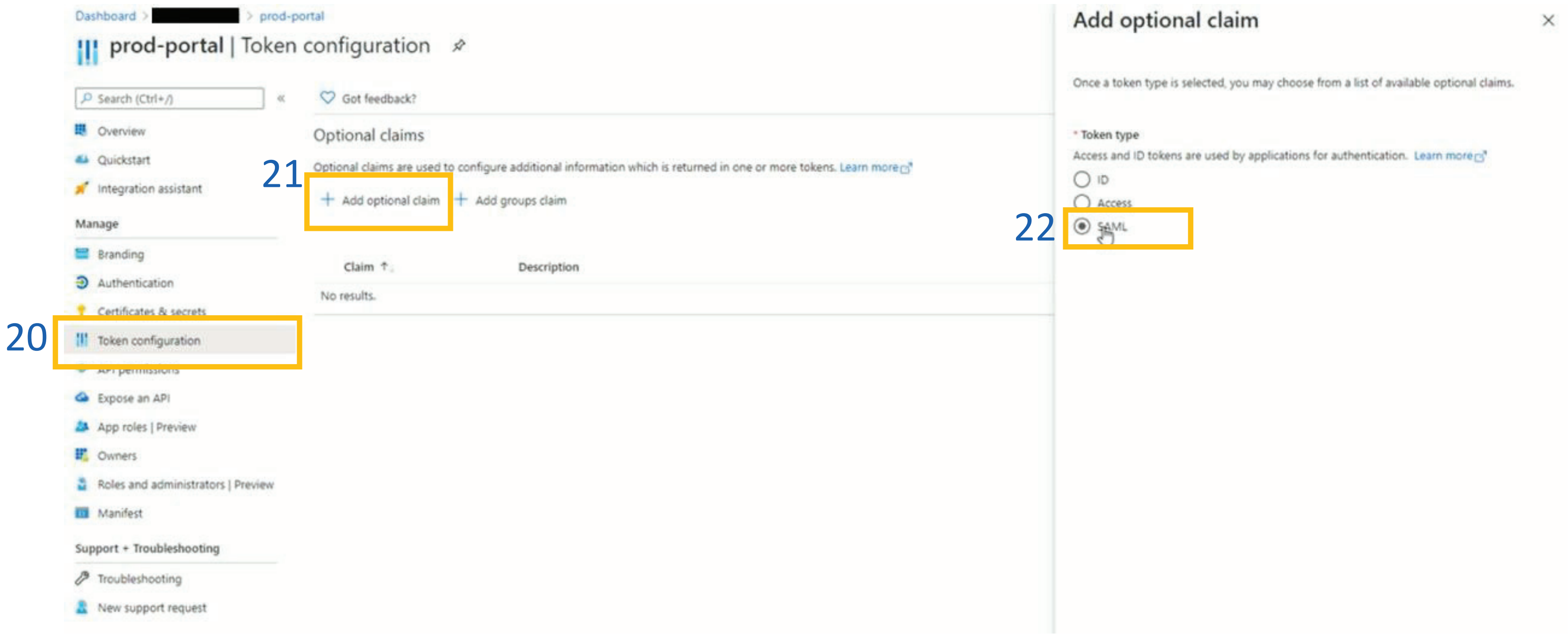
Metadata URL

Application ID URL: [redacted]

Redirect URL: [redacted]

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center



Dashboard > [redacted] > prod-portal

prod-portal | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. Learn more

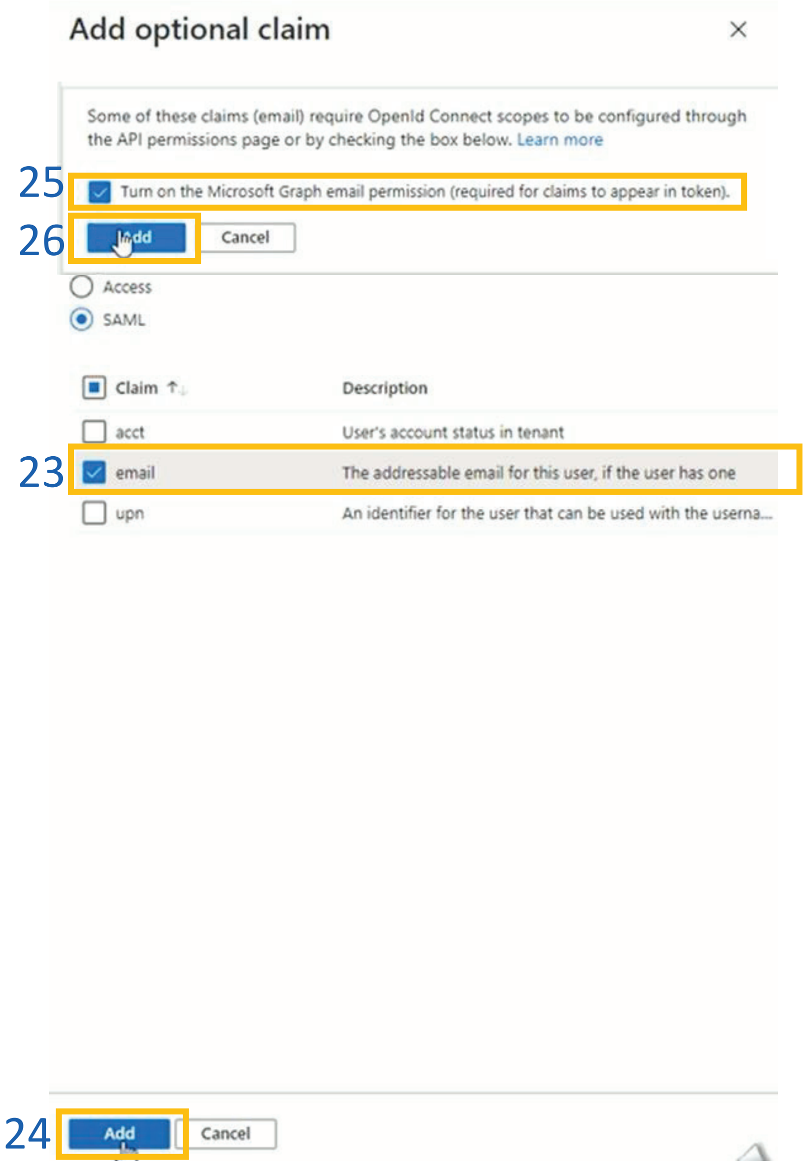
○ ID
○ Access
● SAML

20. Select “**Token configuration**”
21. Select “**Add optional claim**”
22. Select “**SAML**”

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center

23. Select “**email**”
24. Click “**Add**”
25. Select “**Turn on the Microsoft Graph email permission (required for claims to appear in token)**”
26. Click “**Add**”



Add optional claim

Some of these claims (email) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

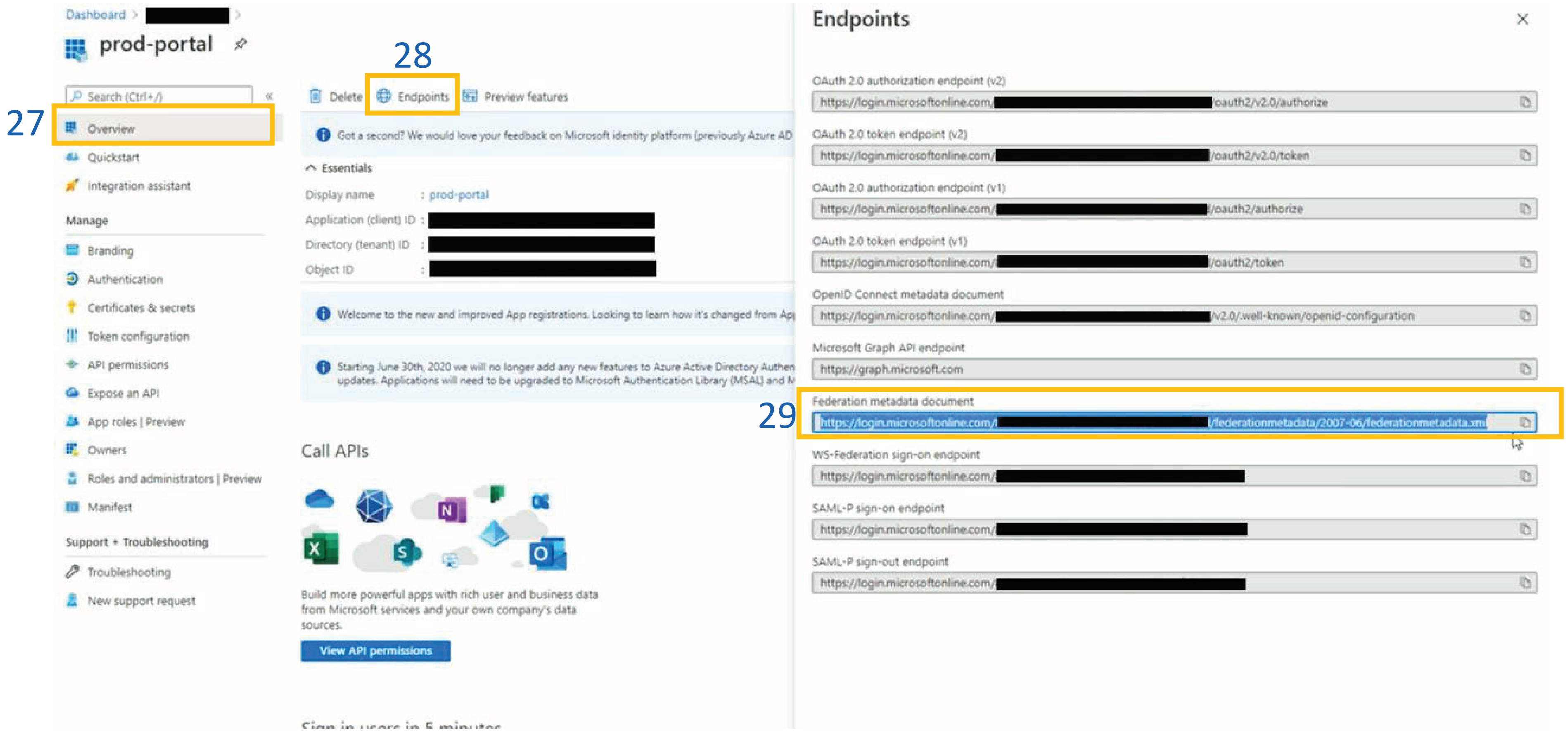
☑ Turn on the Microsoft Graph email permission (required for claims to appear in token).

○ Access
● SAML

Claim	Description
□ acct	User's account status in tenant
☑ email	The addressable email for this user, if the user has one
□ upn	An identifier for the user that can be used with the userna...

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD

Essentials

Display name : prod-portal

Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

Object ID : [redacted]

Welcome to the new and improved App registrations. Looking to learn how it's changed from Ap

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authen updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and M

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/[redacted]/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com

Federation metadata document
https://login.microsoftonline.com/[redacted]/federationmetadata/2007-06/federationmetadata.xml

WS-Federation sign-on endpoint
https://login.microsoftonline.com/[redacted]

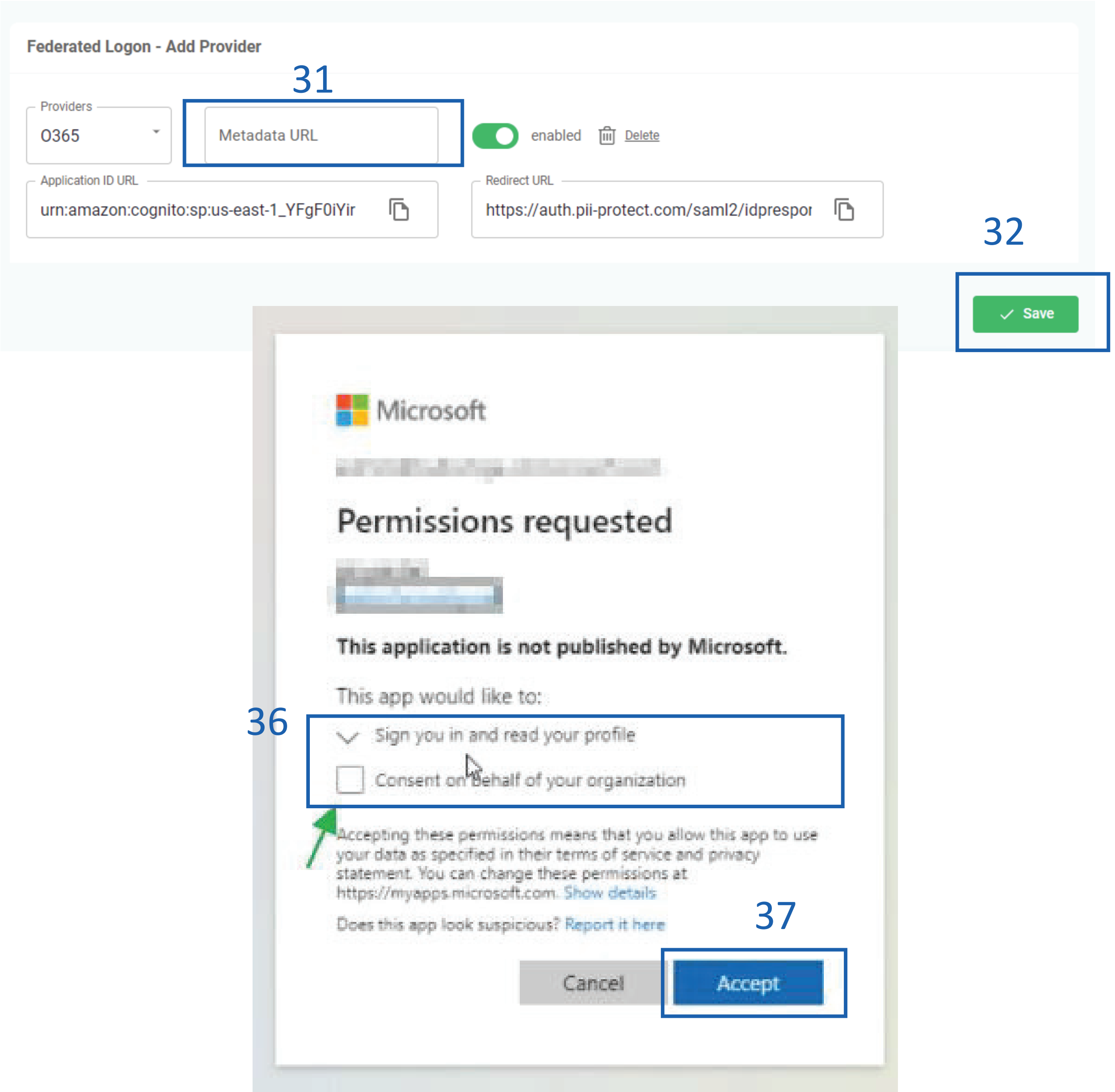
SAML-P sign-on endpoint
https://login.microsoftonline.com/[redacted]

SAML-P sign-out endpoint
https://login.microsoftonline.com/[redacted]

27. Select “**Overview**”
28. Select “**Endpoints**”
29. Copy link under “Federation metadata document”
30. Return to the PII Protect Portal for the final steps.

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings



Federated Logon - Add Provider

Providers: O365

Metadata URL

enabled Delete

Application ID URL: urn:amazon:cognito:sp:us-east-1_YFgF0iYir

Redirect URL: https://auth.pii-protect.com/saml2/idprespor

✓ Save

Microsoft

[redacted]

Permissions requested

[redacted]

This application is not published by Microsoft.

This app would like to:

Sign you in and read your profile

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel Accept

31. Paste in the “Metadata URL” you’ve copied from the Azure Admin Center.
32. Click the “**Save**” button

Important! If Using Microsoft 365, you need to provide consent for the Federated Login application to be enforced across the account

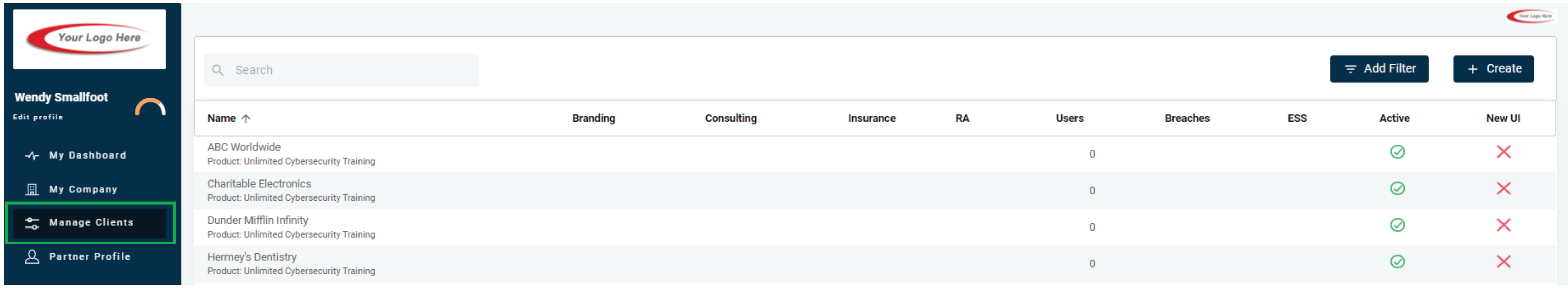
34. Log out of the Portal and log back into the Portal with a user account that is registered within the client that Federated Login was configured for

35. A “Permissions requested” notification should appear from Microsoft
36. Select/Check the option for “Consent on behalf of your organization”
37. Click the “**Accept**” button

You’re All Set!

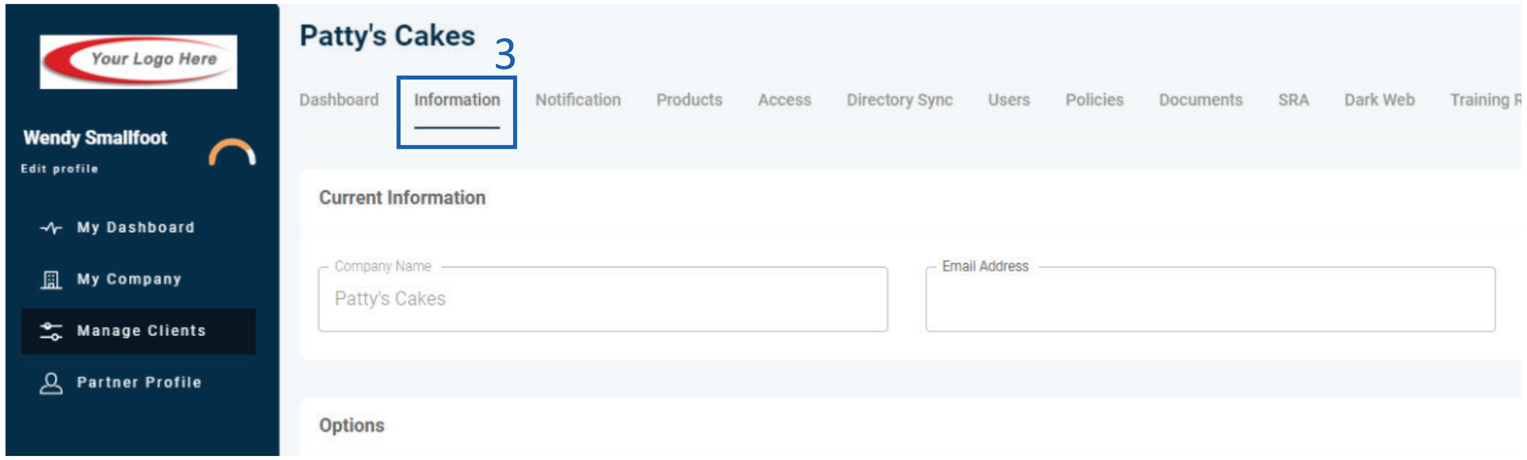
Configuring Federated Login Within the PII Protect Portal - Okta

Navigating to the Client View Screen



Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			✓	✗

1. Login as a Partner Administrator to the PII-Protect portal here. Once logged in select "**Manage Clients**" to access your client list (above).
2. Select the client you want to enable **Okta** Federated Login for.
3. Click on the "**Information**" tab at the top



Current Information

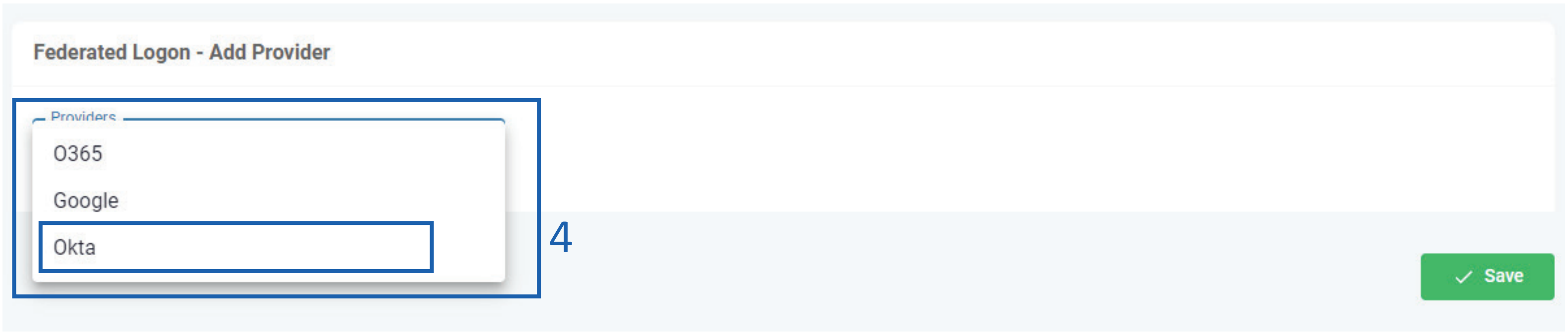
Company Name: Patty's Cakes

Email Address:

Options

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings



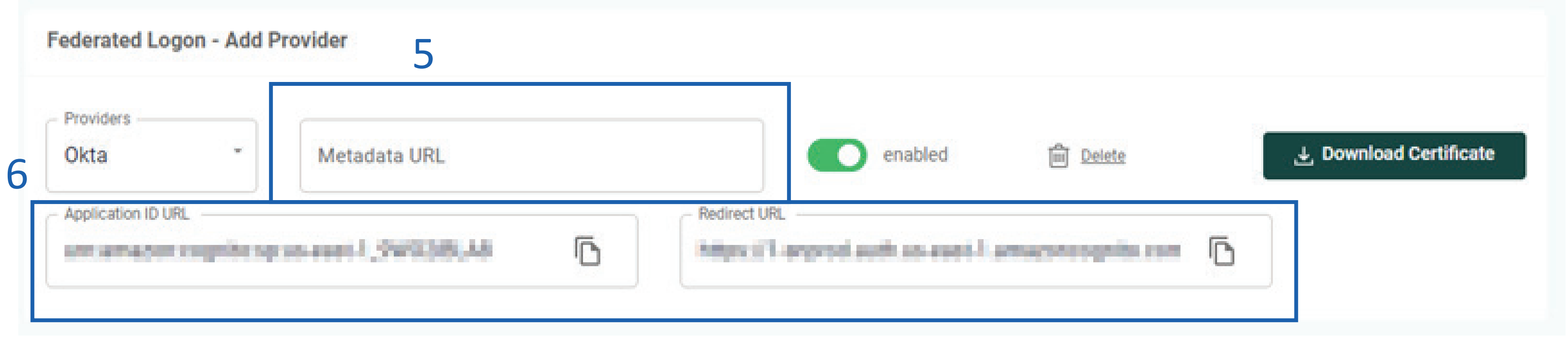
Federated Logon - Add Provider

Providers

O365

Google

Okta



Federated Logon - Add Provider

Providers: Okta

Metadata URL

enabled

Application ID URL: [redacted]

Redirect URL: [redacted]

4. At the bottom of the screen for Federated Logon, select “**Okta**”

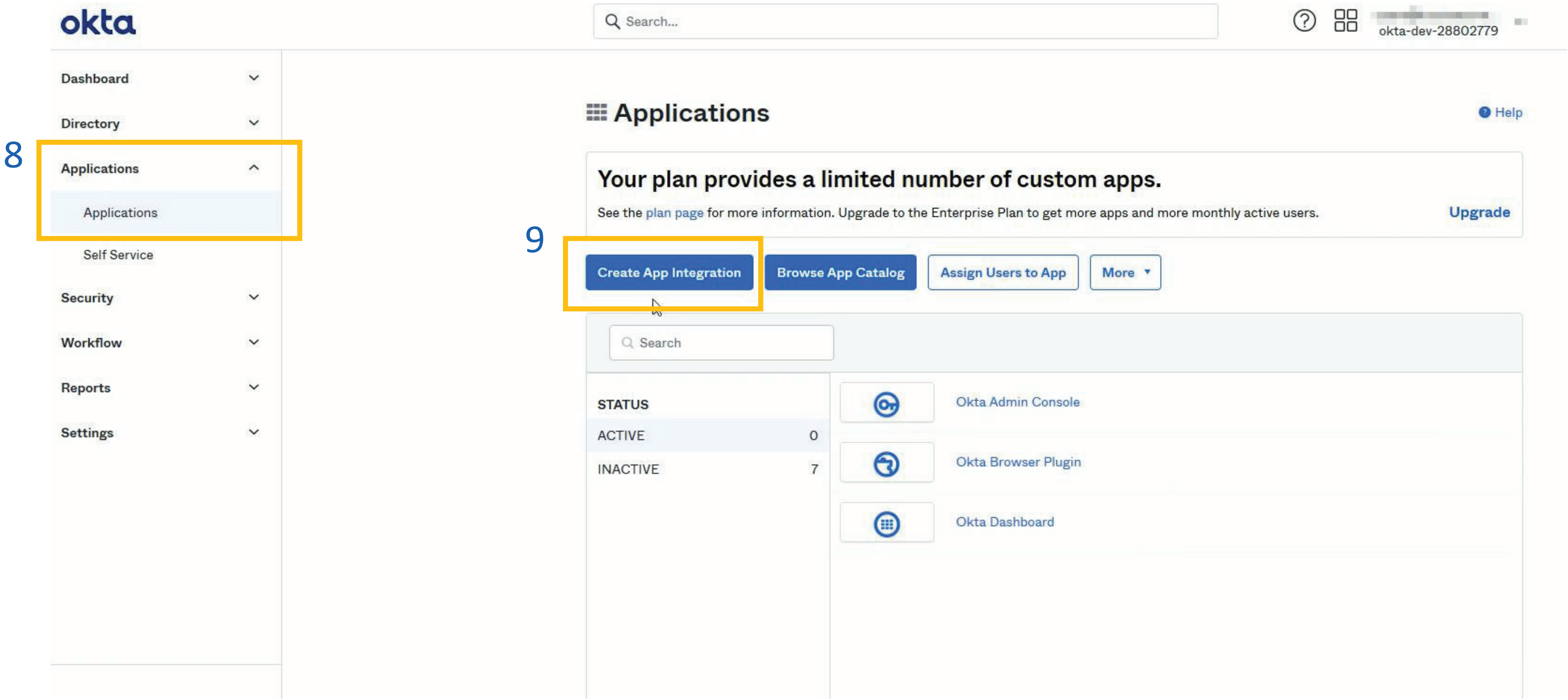
5. You will need a **Metadata URL** that will become available when set up in the Azure Admin Center.

6. Note that the “**Application ID URL**” and “**Redirect URL**” are filled in. You will be using these URLs in the next Azure steps so keep this page open.

7. Access the Azure Admin environment for this client account.

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



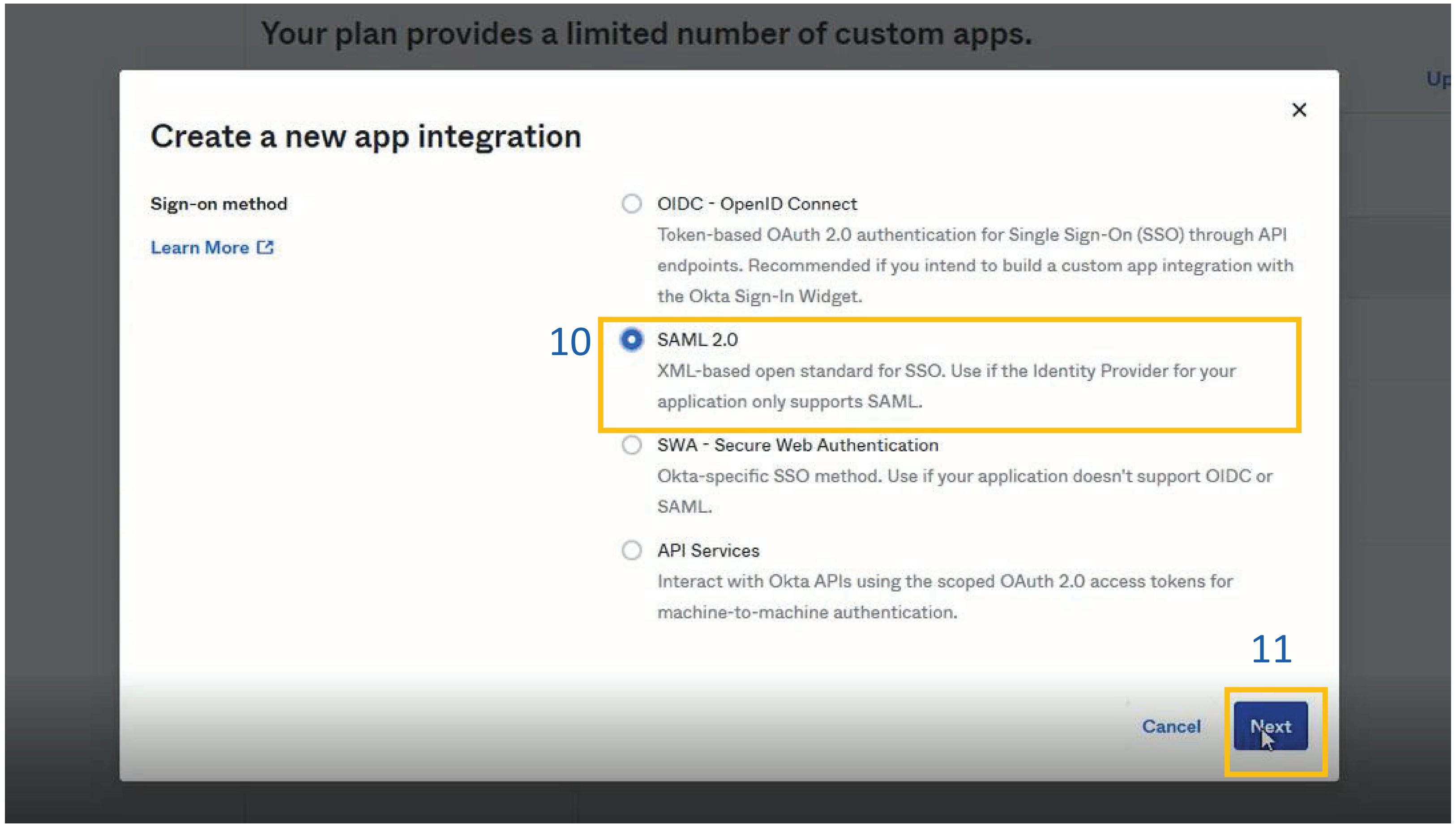
Your plan provides a limited number of custom apps.

See the plan page for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users. Upgrade

8. Within the Okta Admin view Select "**Applications**" from the left panel then "**Applications**"
9. Select "**Create App Integration**"

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Your plan provides a limited number of custom apps.

Create a new app integration

Sign-on method

Learn More

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

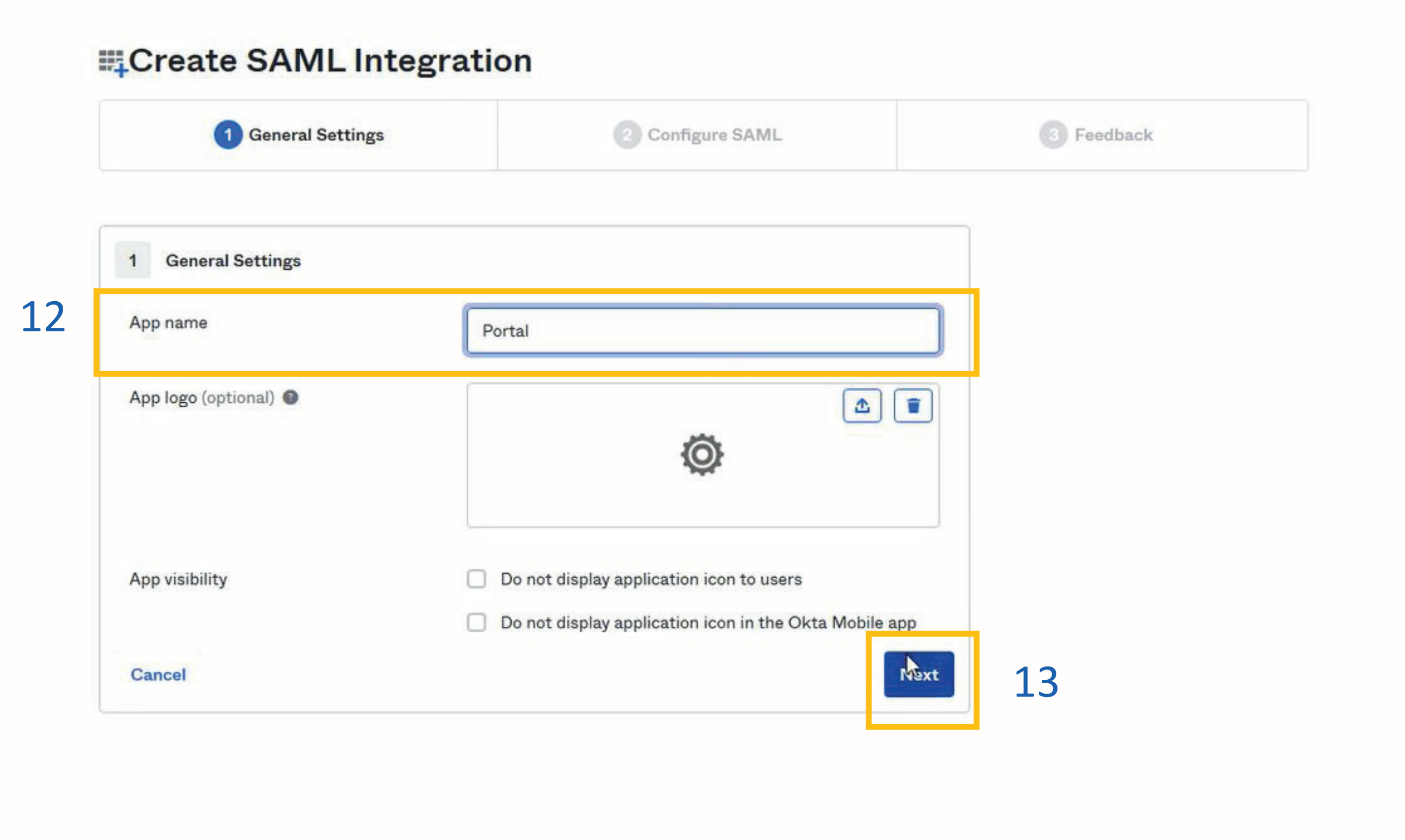
○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

10. Within the pop-up window, select "**SAML 2.0**"

11. Click the "**Next**" button

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Create SAML Integration

1 General Settings

App name: Portal

App logo (optional)

App visibility

□ Do not display application icon to users

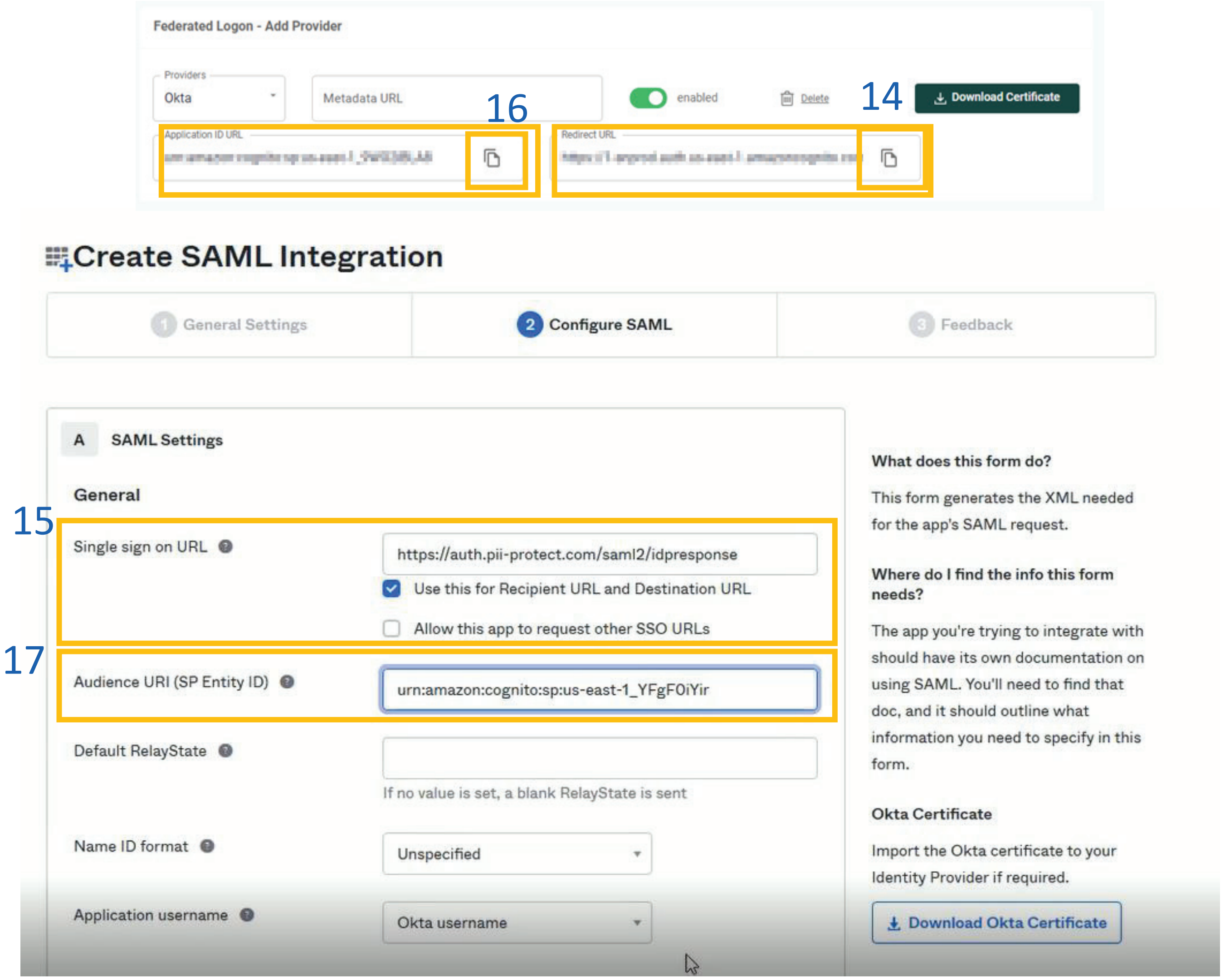
□ Do not display application icon in the Okta Mobile app

12. In the General Settings, for the "**App name**" type "Portal"

13. Click the "**Next**" button

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Federated Logon - Add Provider

Providers: Okta

Metadata URL

enabled

Application ID URL: [redacted]

Redirect URL: [redacted]

Create SAML Integration

1 General Settings — 2 Configure SAML — 3 Feedback

A SAML Settings

General

Single sign on URL: https://auth.pii-protect.com/saml2/idpresponse

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): urn:amazon:cognito:sp:us-east-1_YFgF0iYir

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

14. Return to your PII Protect portal page and locate the Redirect URL. Click the “**Copy**” button.

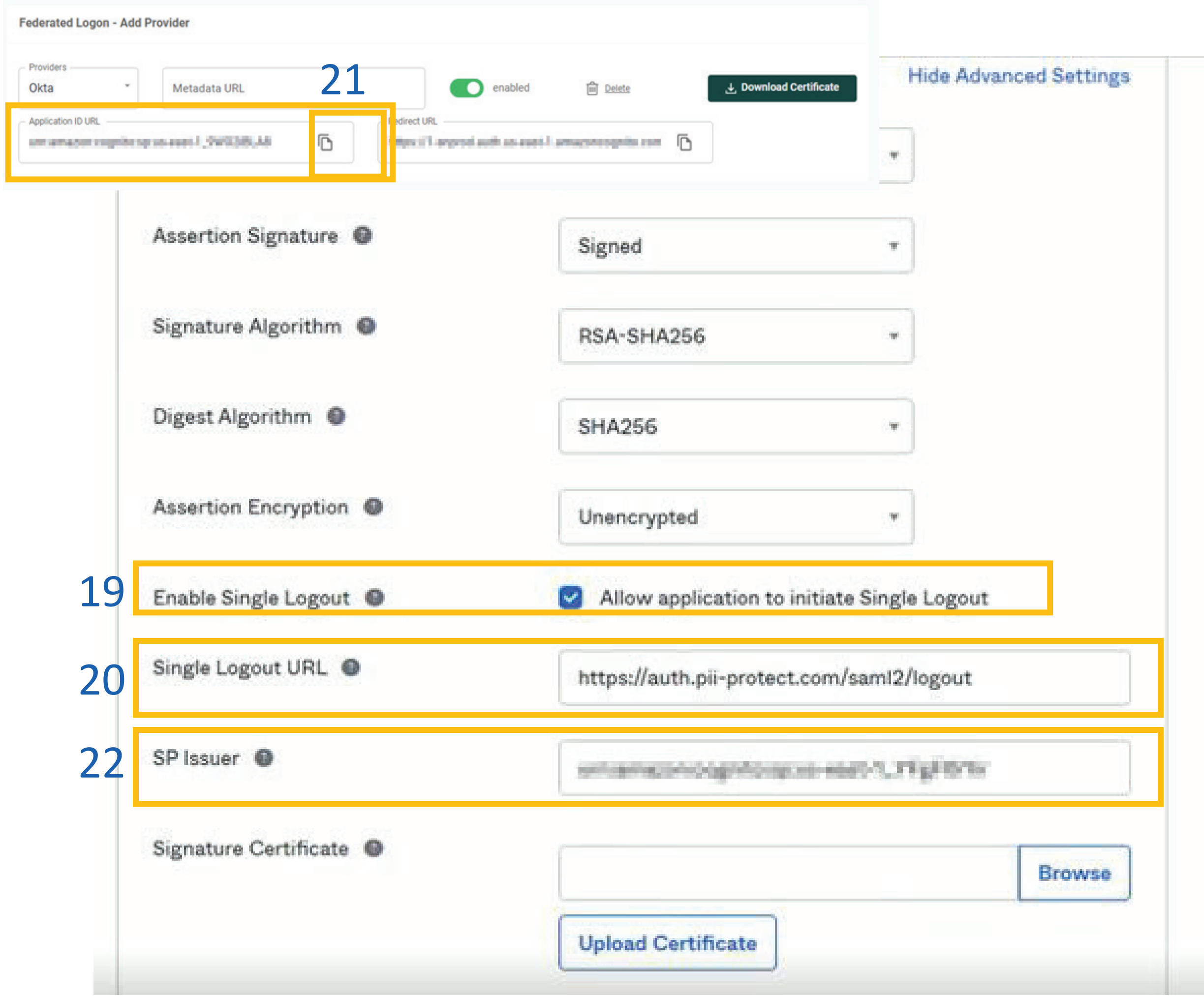
15. Back in your Okta Admin Center, in the Single sign on URL section, paste the Redirect URL you’ve copied.

16. Return to your PII Protect portal page and locate the Application ID URL. Click the “**Copy**” button.

17. Back in your Okta Admin Center, in the Audience URL section, past the Application ID URL you’ve copied.

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Federated Logon - Add Provider

Providers: Okta

Metadata URL

enabled

Application ID URL: [redacted]

Redirect URL: [redacted]

Assertion Signature: Signed

Signature Algorithm: RSA-SHA256

Digest Algorithm: SHA256

Assertion Encryption: Unencrypted

Enable Single Logout: ☑ Allow application to initiate Single Logout

Single Logout URL: https://auth.pii-protect.com/saml2/logout

SP Issuer: [redacted]

Signature Certificate

18. Click the "**Show Advanced Settings**"

19. In the Enable Single Logout, check the box to "Allow application to initiate Single Logout".

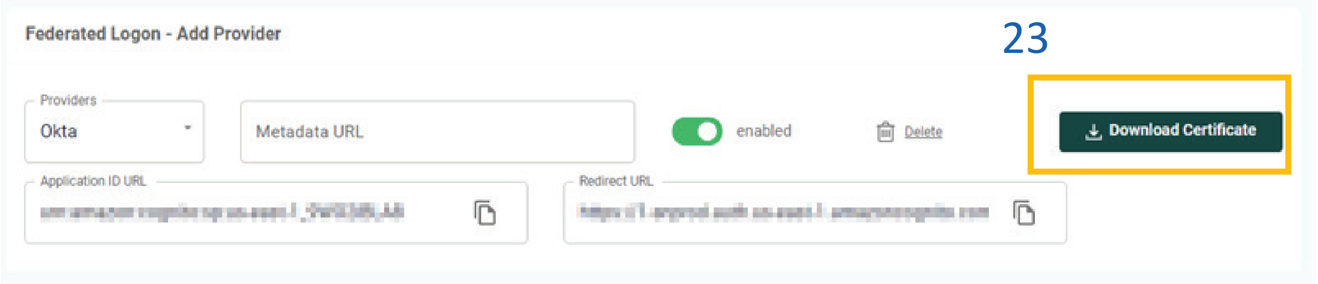
20. Copy and paste (or type out) this URL in the Single Logout URL: https://auth.pii-protect.com/saml2/logout

21. Return to your PII Protect portal page and locate the Application ID URL. Click the "Copy" button.

22. Back in your Okta Admin Center, in the SP Issuer section, paste the copied URL

Configuring Settings in the Okta Admin Center

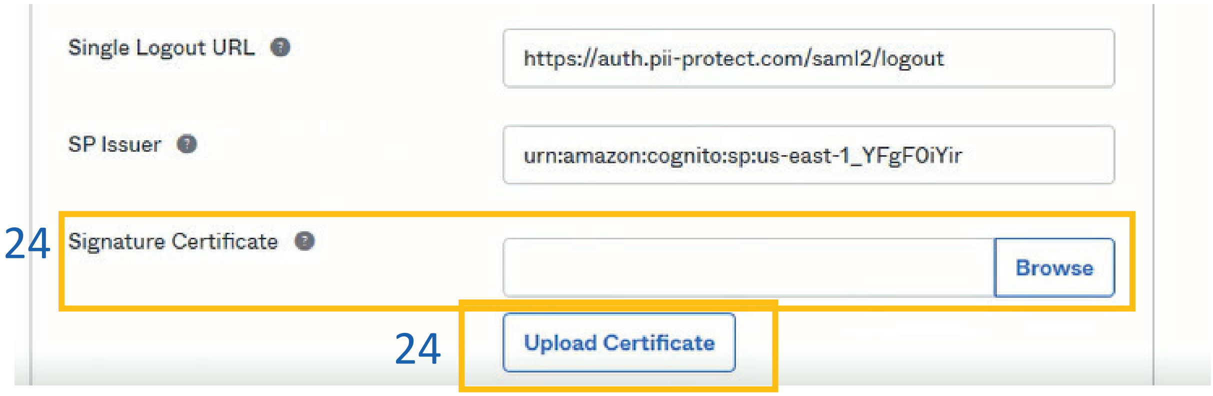
Setup in Okta Admin Center


Federated Logon - Add Provider

Providers: Okta

Application ID URL: [redacted]

Redirect URL: [redacted]


Single Logout URL: https://auth.pii-protect.com/saml2/logout

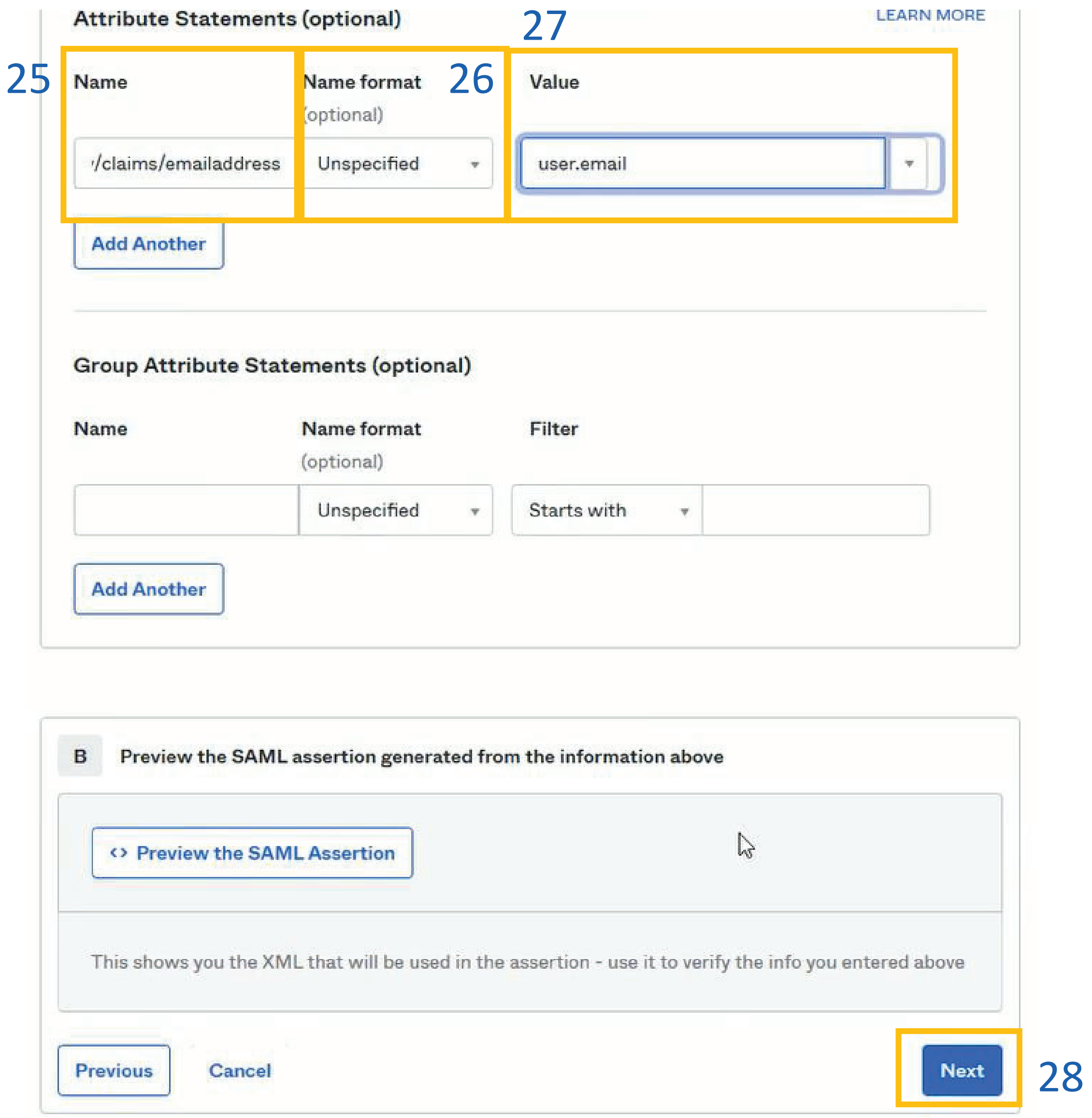
SP Issuer: urn:amazon:cognito:sp:us-east-1_YFgF0iYir

23. In your PII Protect Portal, locate the "Download Certificate" button. Download and save this file on your device

24. In the Signature Certificate section, click "Browse" to upload your Cognito certificate you just downloaded and saved. Click the "Upload Certificate" button

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Attribute Statements (optional)

Name	Name format (optional)	Value
/claims/emailaddress	Unspecified	user.email

Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
	Unspecified	Starts with	

B Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

25. In the Attribute Statements section, copy and paste (or type out) this URL in the Name section:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

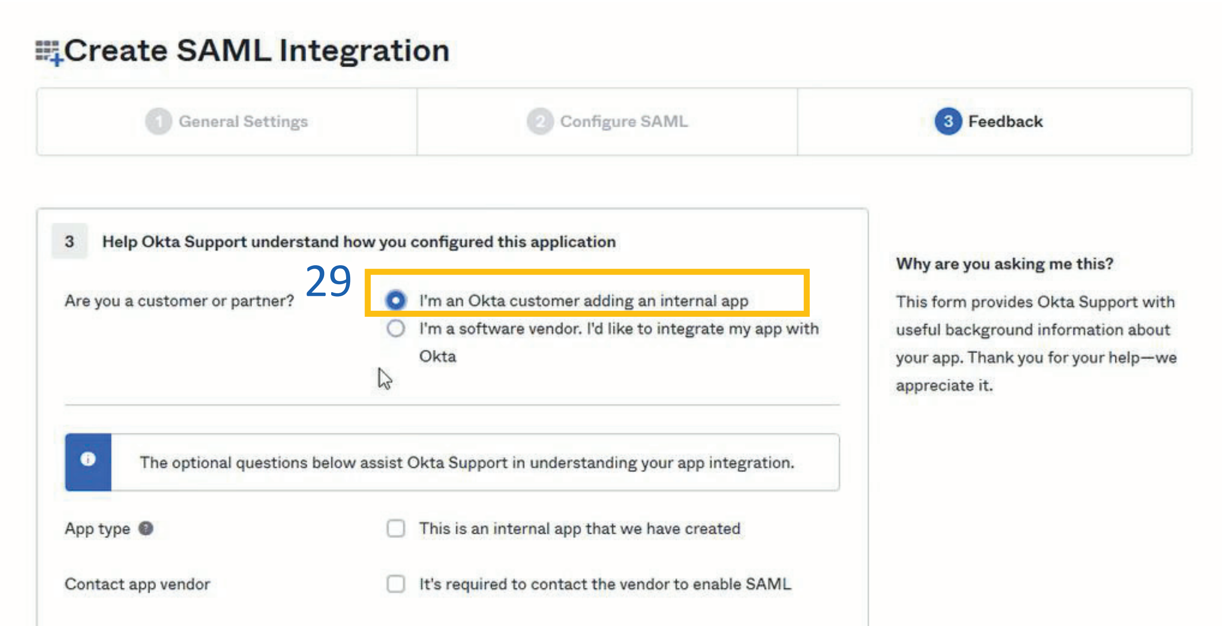
26. Keep the Name Format as Unspecified.

27. In the Value section, copy and paste (or type out) this:
user.email

28. Scroll down and click the “Next” button.

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Create SAML Integration

3 Help Okta Support understand how you configured this application

Are you a customer or partner? 29 ● I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

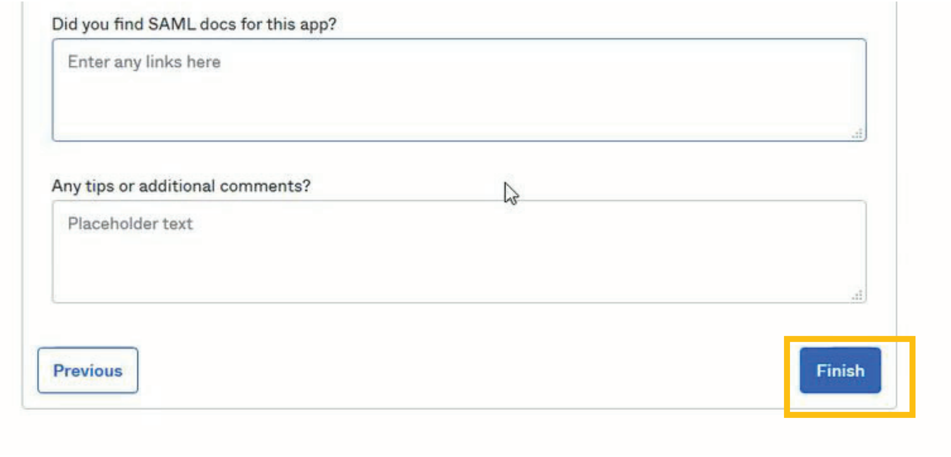
The optional questions below assist Okta Support in understanding your app integration.

App type □ This is an internal app that we have created

Contact app vendor □ It's required to contact the vendor to enable SAML

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.



Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

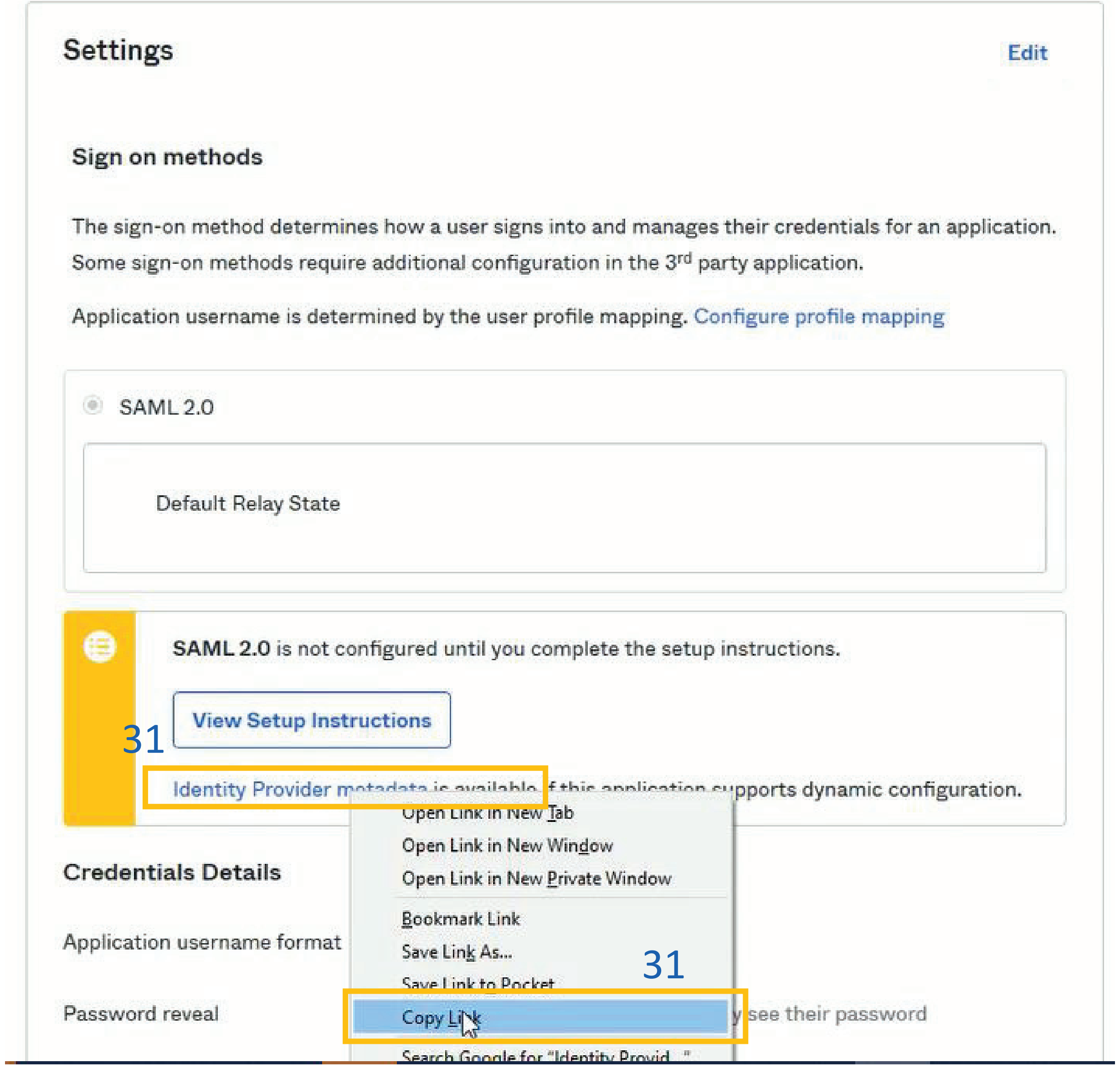
30

29. When asked if you are a customer or partner, select "I'm an Okta customer adding an internal app

30. Scroll down and click the "Finish" button.

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center



Settings

Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

Credentials Details

Application username format

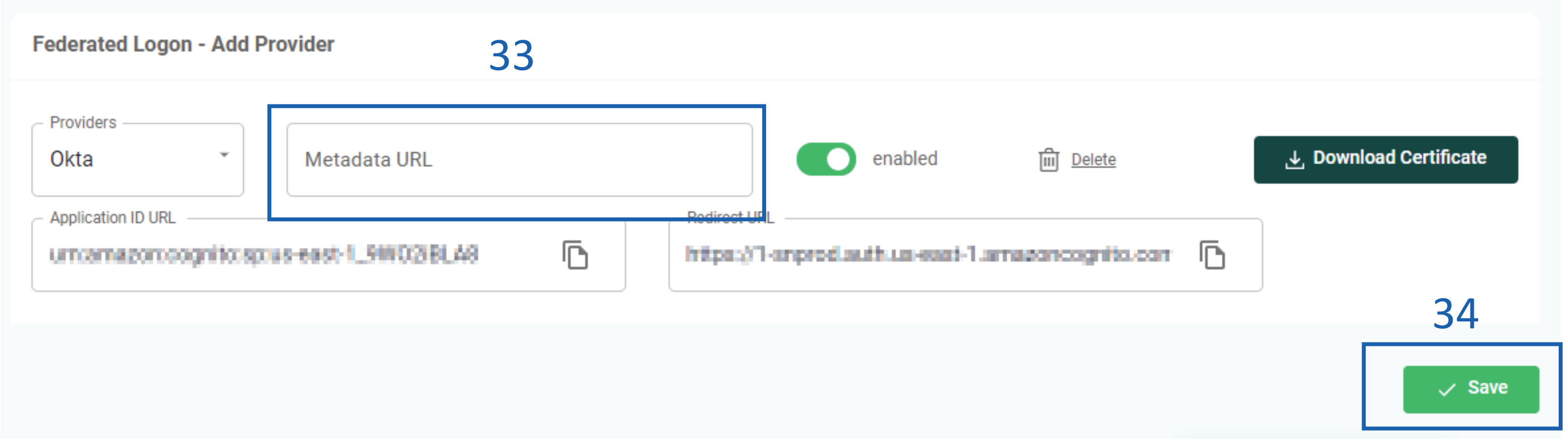
Password reveal

31. In Settings, right-click on the "**Identity Provider metadata**" and select "**Copy Link**".

32. Continue to the next page for the final steps of configuration within the PII Protect Portal.

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings



Federated Logon - Add Provider

Providers: Okta

Metadata URL

enabled

Application ID URL: urn:amazon:cognito:sp:us-east-1_9W03BLA8

Redirect URL: https://1-snprod.auth.us-east-1.amazoncognito.com

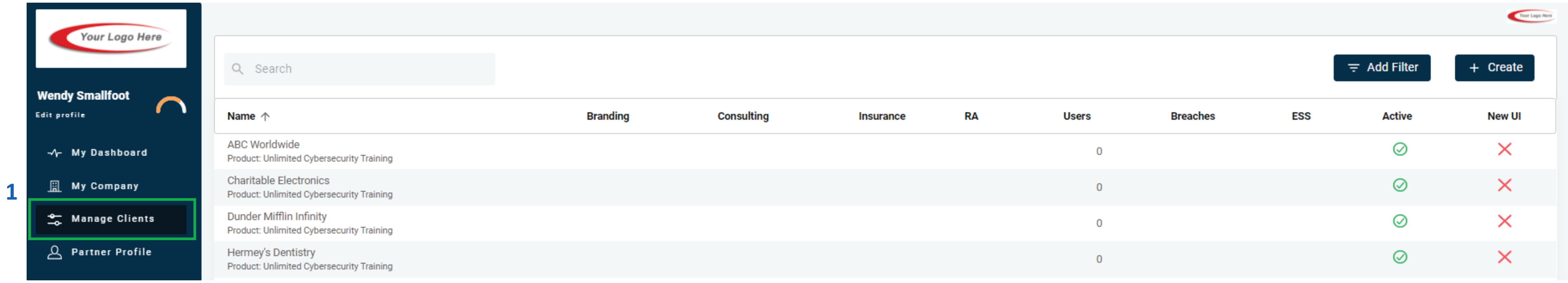
33. Return to your PII Protect portal page, paste in the “Metadata URL” you’ve copied from the Azure Admin Center.

34. Click the “**Save**” button

You’re All Set!

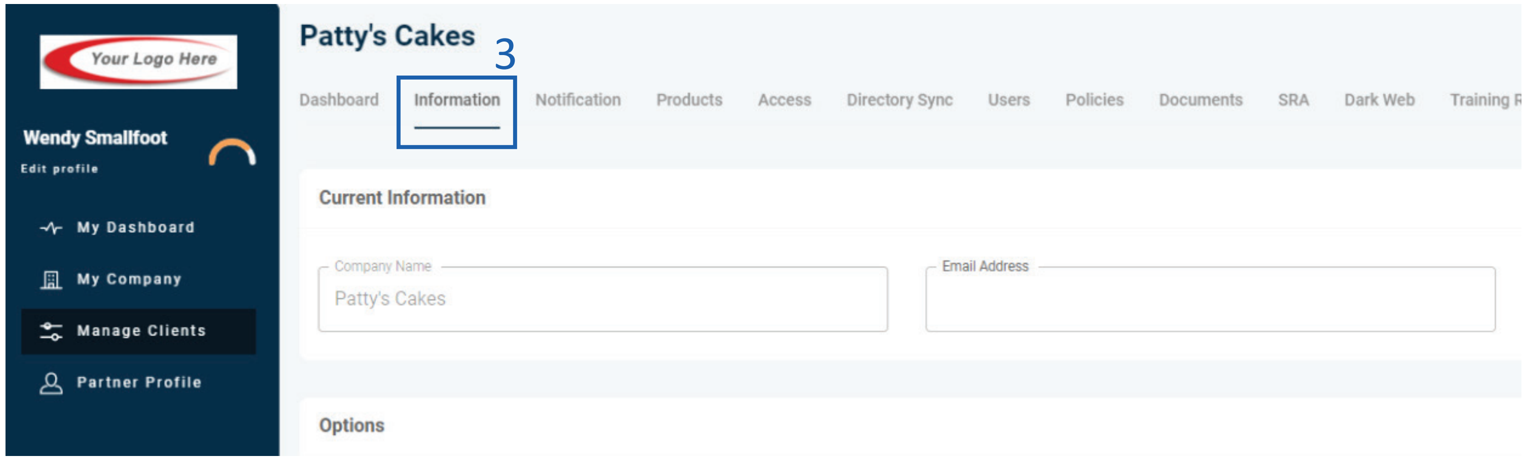
Configuring Federated Login Within the PII Protect Portal - Google

Navigating to the Client View Screen



Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			✓	✗

1. Login as a Partner Administrator to the PII-Protect portal here. Once logged in select “**Manage Clients**” to access your client list (above).
2. Select the client you want to enable Google Federated Login for.
3. Click on the “**Information**” tab at the top



Patty's Cakes

Current Information

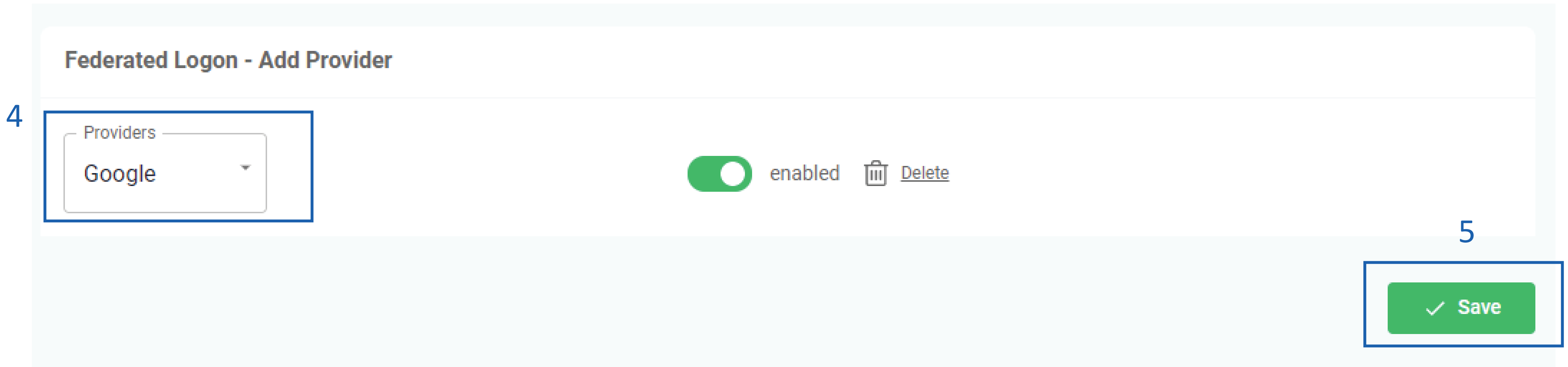
Company Name: Patty's Cakes

Email Address:

Options

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings



Federated Logon - Add Provider

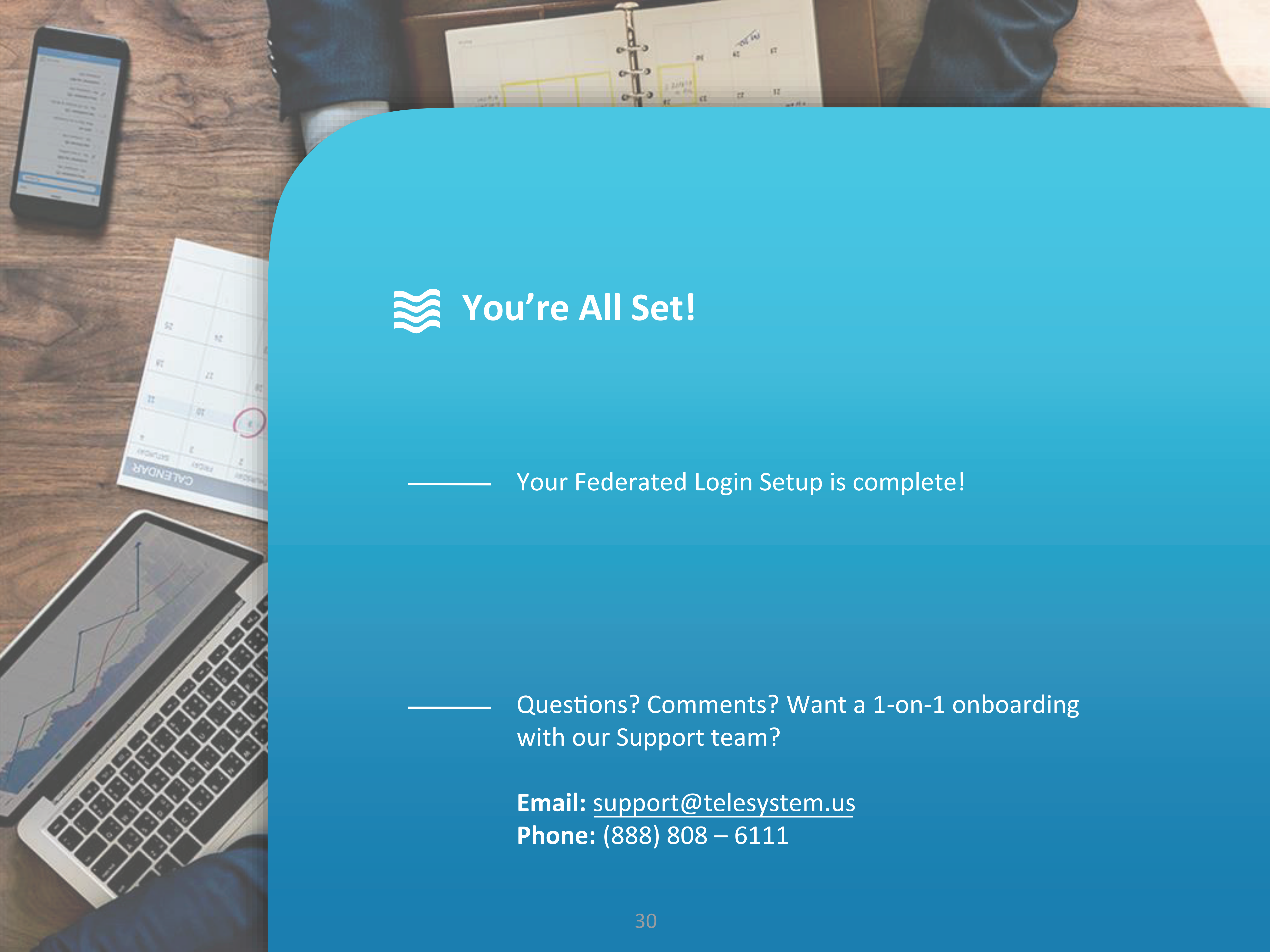
Providers: Google

enabled

4. At the bottom of the “Information” tab, in the “Federated Logon” section, select “Google”. Ensure that the “enabled” flag is turned on.

5. Click the “**Save**” button

You’re All Set!
Upon the user’s next login to the PII Protect portal they will be prompted to enter their Google credentials via the Google interface.



You’re All Set!

Your Federated Login Setup is complete!

Questions? Comments? Want a 1-on-1 onboarding with our Support team?

Email: support@telesystem.us
Phone: (888) 808 – 6111