

 Security Awareness Training Partner Guide

— Federated Login or Native MFA Setup Microsoft 365, Okta and Google Activation and client integration



www.TrustTelesystem.com

Federated Login Setup

Table of Contents

General Informationpages 3 – 4

Native MFA Configurationpages 5 – 6

Azure Configurationpages 7 – 15

Okta Configuration pages 16 - 27

Google Configurationpages 28 – 29

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](#).

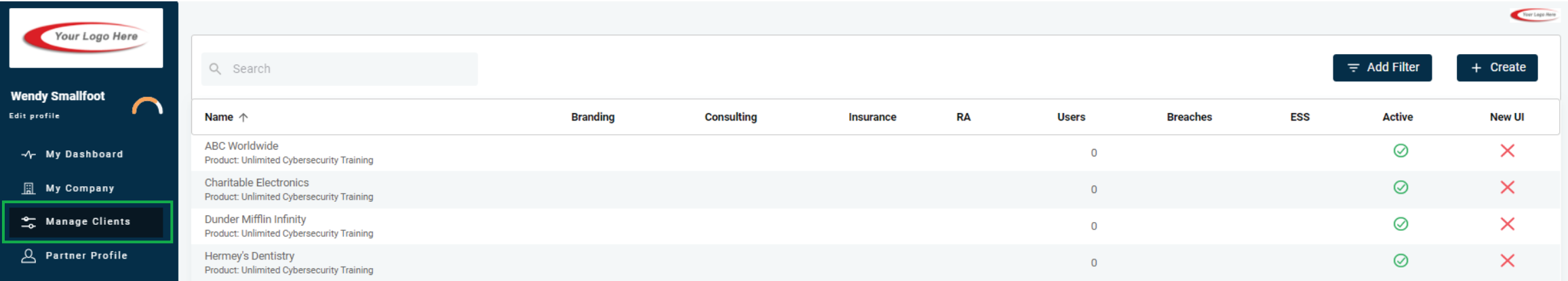
Okta: If the client is using Okta, please begin on [page 14](#).

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)

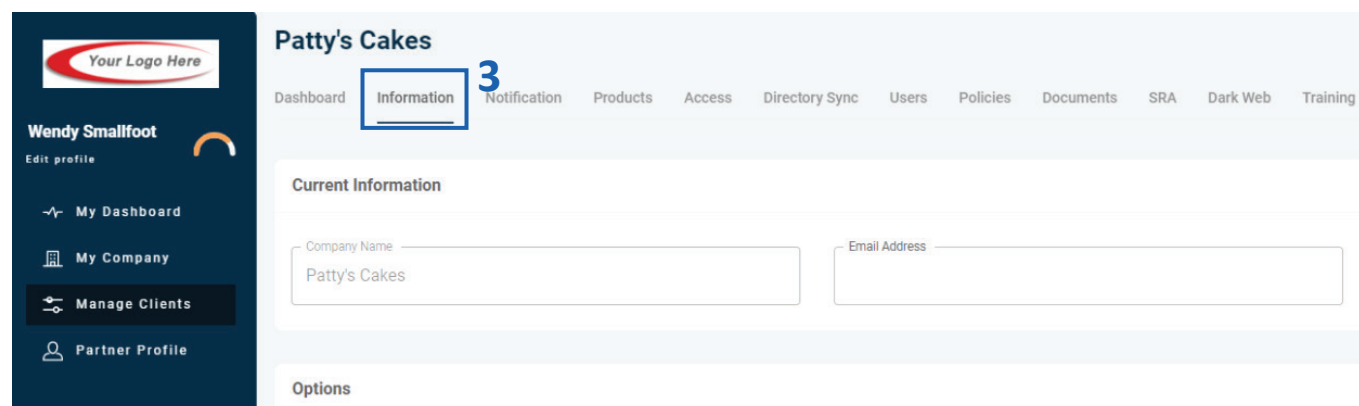
Navigating to the Information Screen

1



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



Patty's Cakes

Dashboard **Information** 3 Notification Products Access Directory Sync Users Policies Documents SRA Dark Web Training F

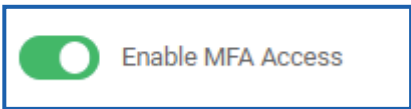
Current Information

Company Name
Patty's Cakes

Email Address

Options

4



Password

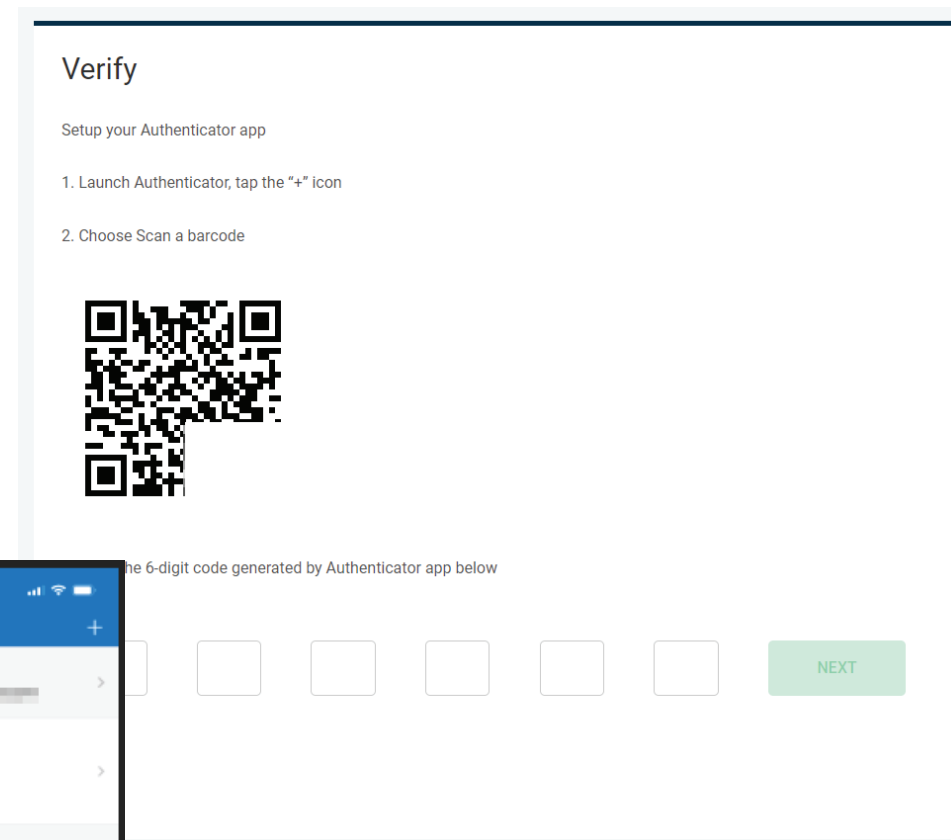
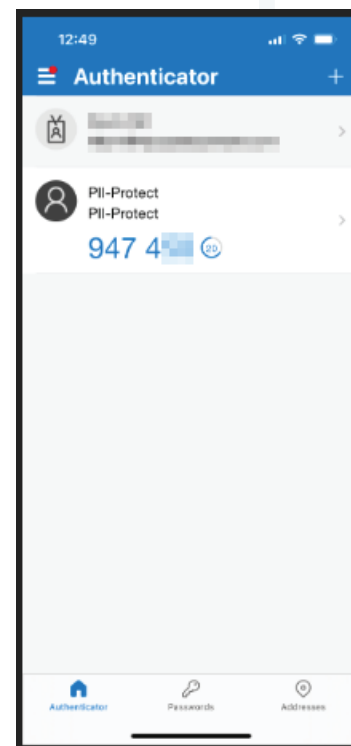
☒ Enable MFA Access

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.



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

1

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

3

Patty's Cakes

Dashboard **Information** Notification Products Access Directory Sync Users Policies Documents SRA Dark Web Training F

Current Information

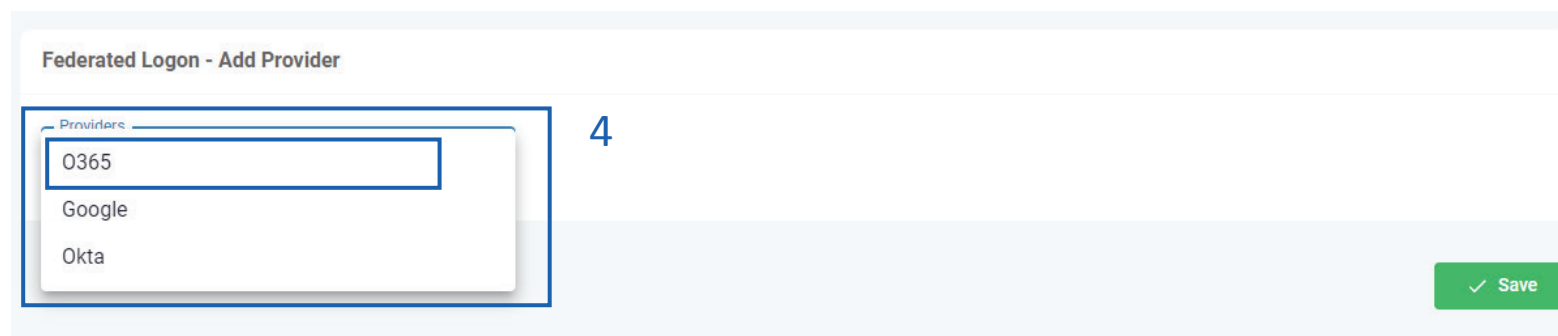
Company Name: Patty's Cakes

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

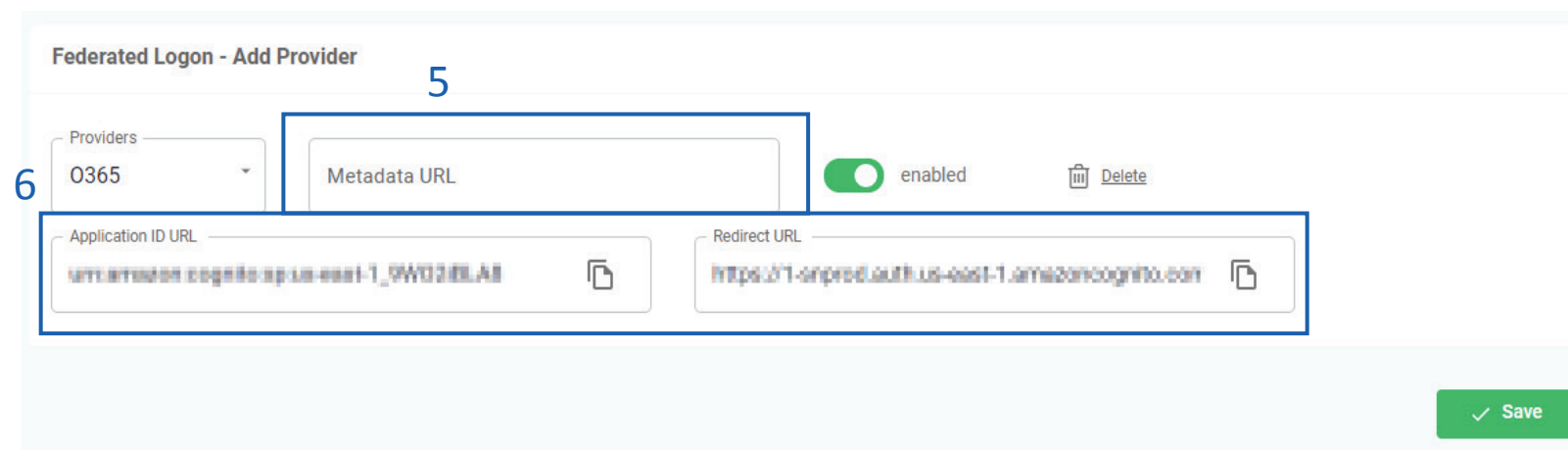
Save

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.

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.



Federated Logon - Add Provider

Providers

O365

Metadata URL

enabled

Delete

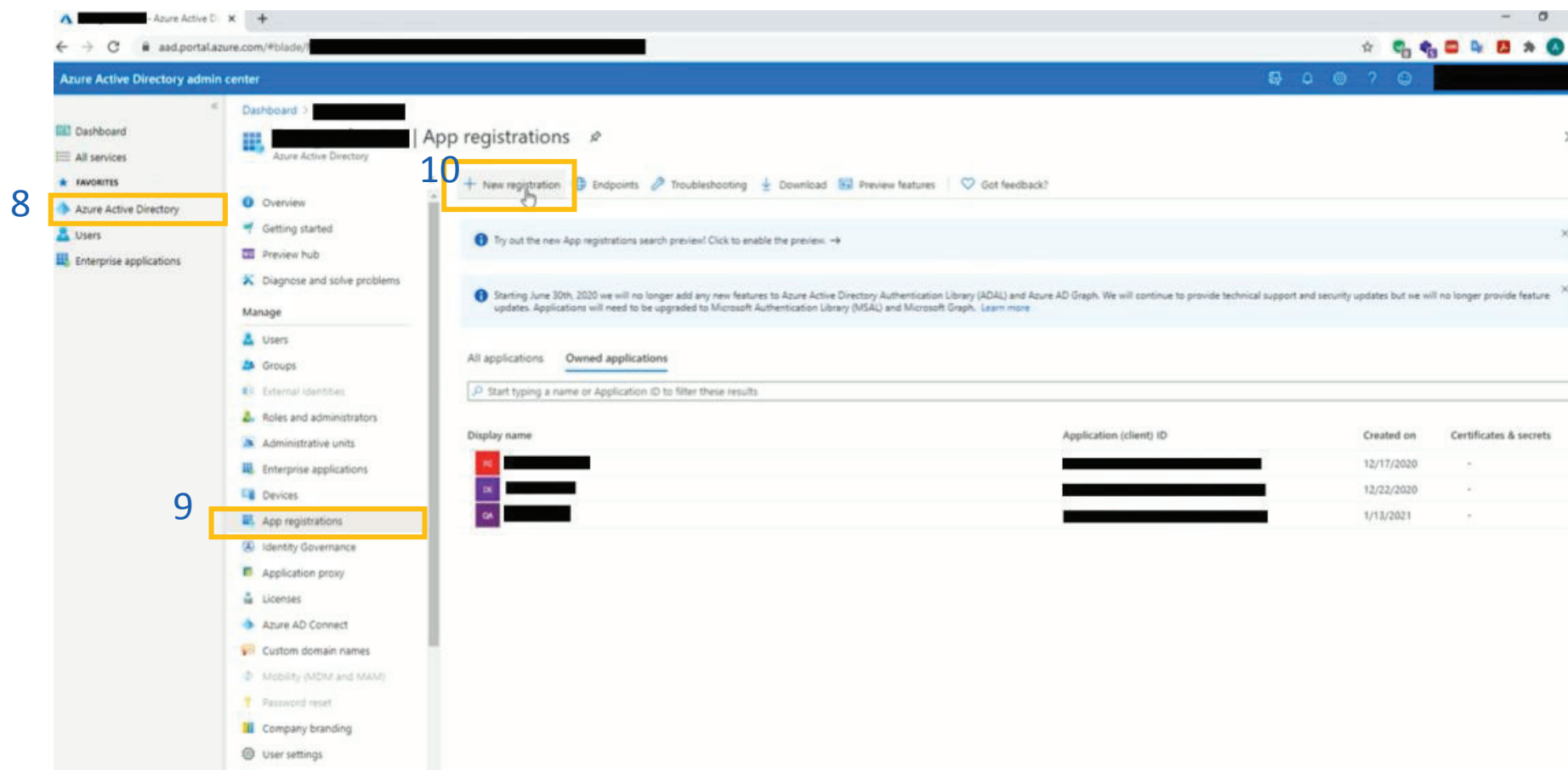
Application ID URL

Redirect URL

Save

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center



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**”

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center

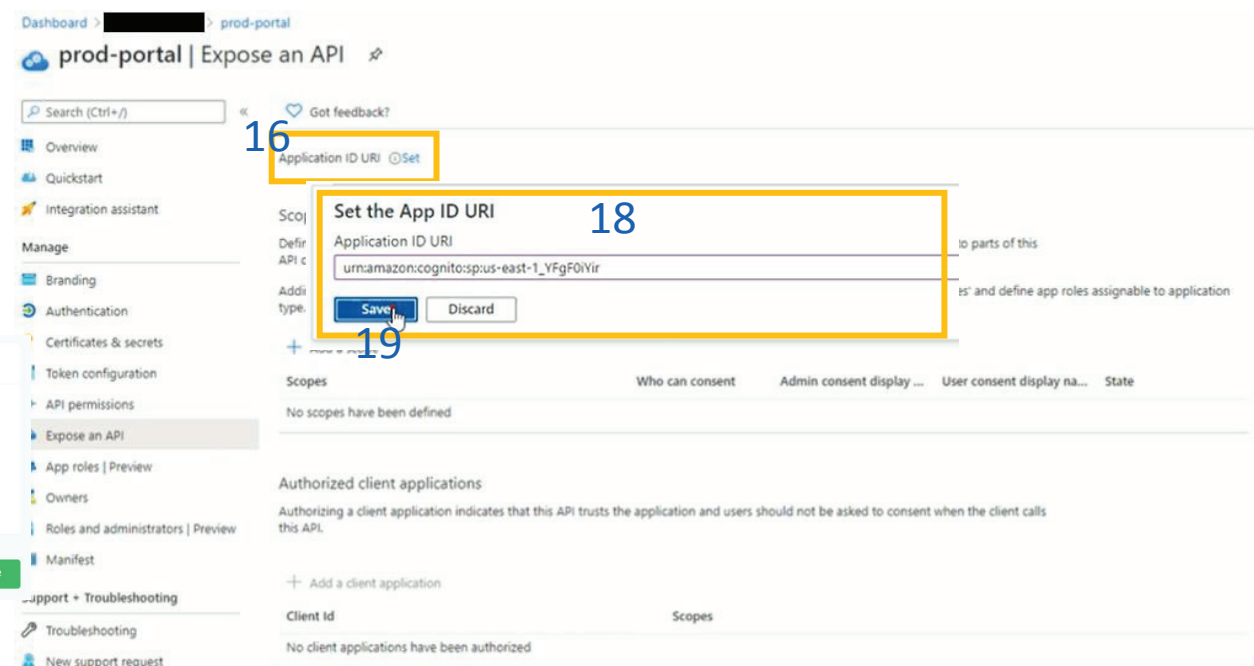
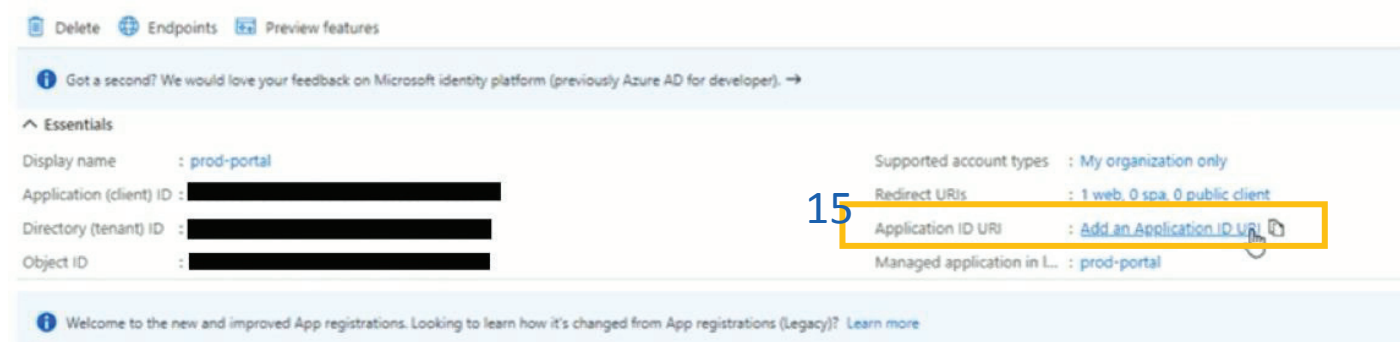
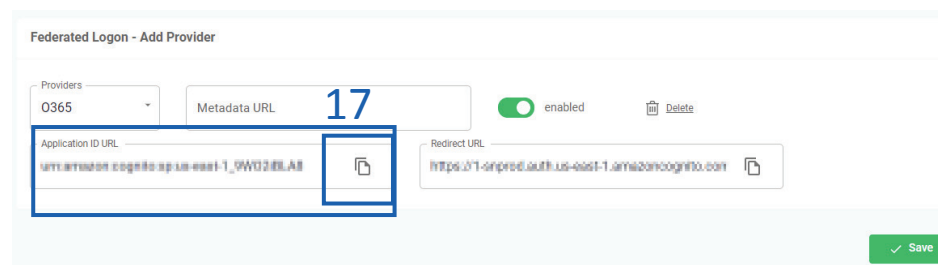
15. Click **“Add an Application ID URI”**

16. Click **“Set”**

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

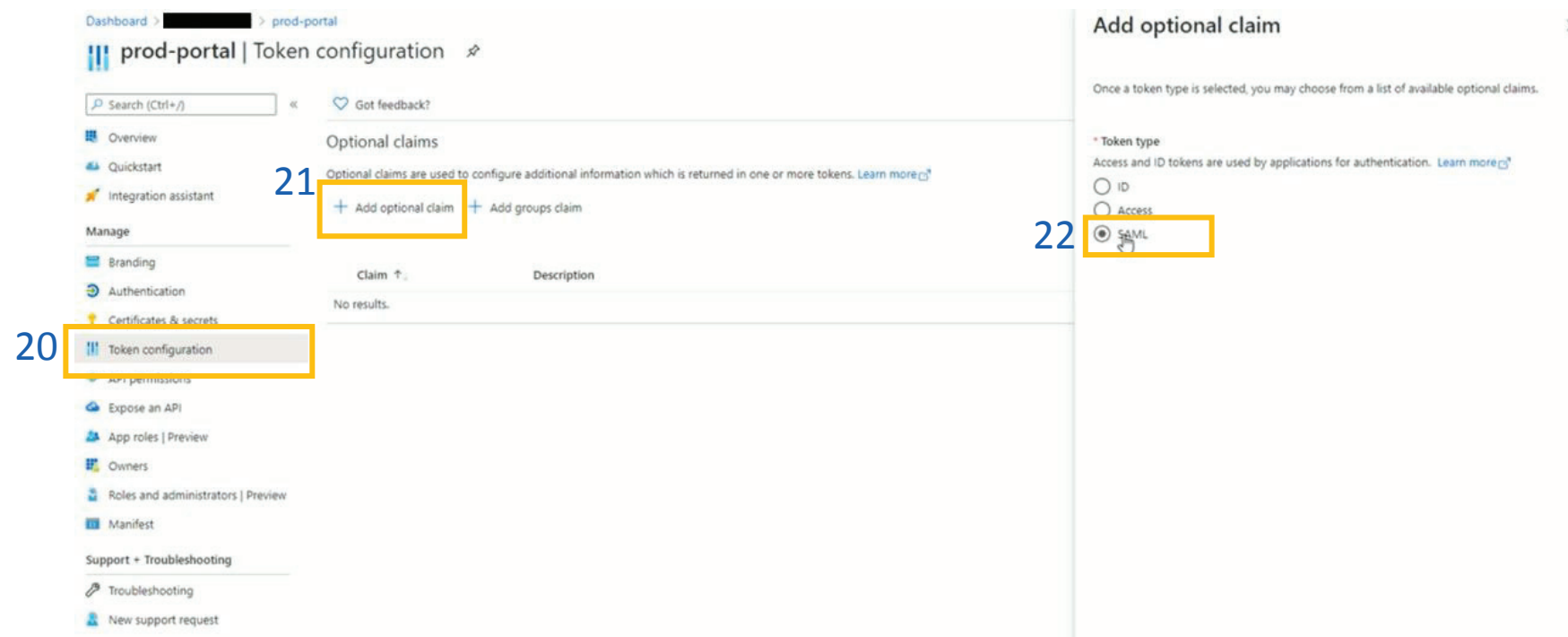
18. Return to the Azure Admin Center and paste this URL into the **“Set the App ID URL”** section.

19. Click **“Save”**



Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center



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 [X]

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](#)

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

26 **Add** Cancel

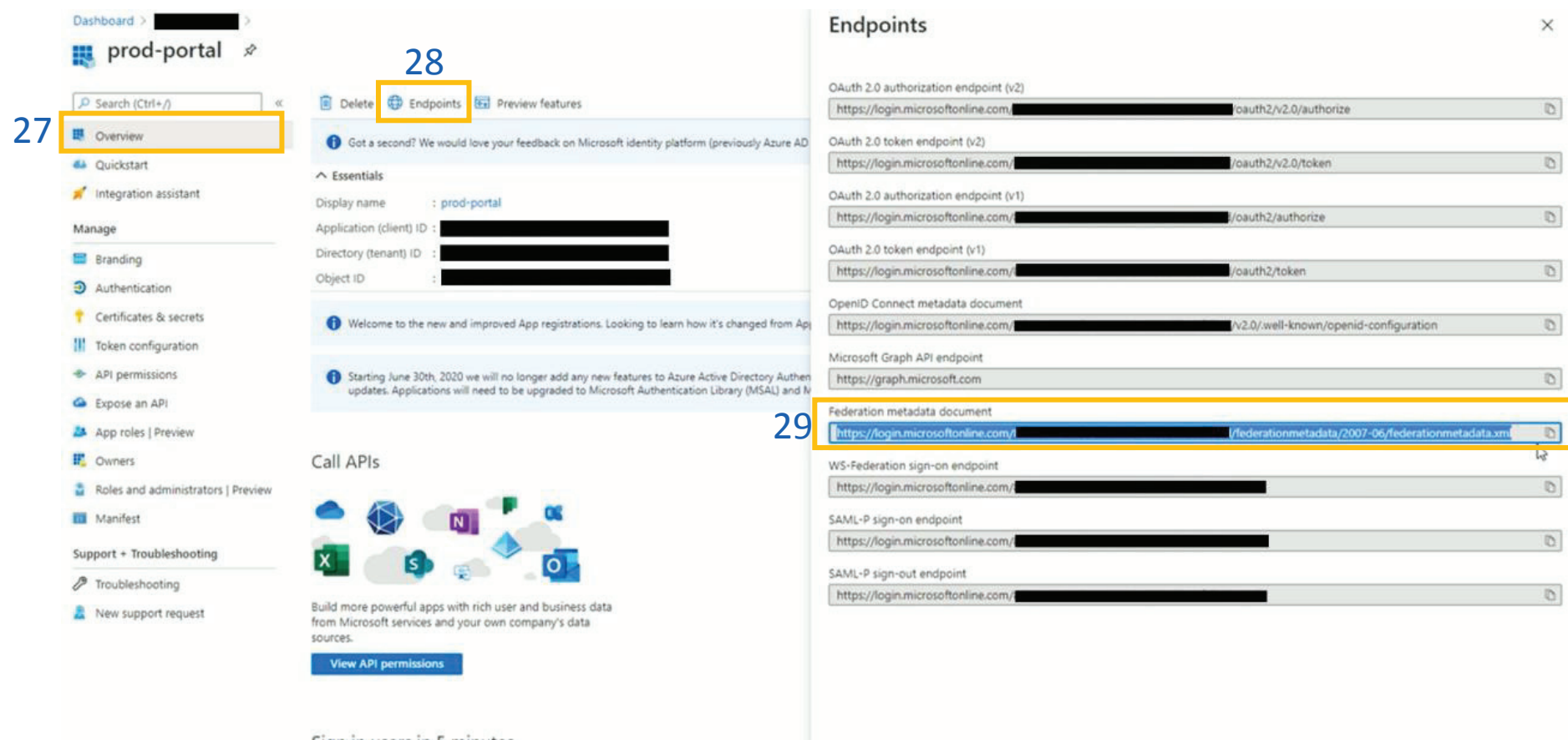
☐ Access
☒ SAML

Claim ↑↓	Description
<input type="checkbox"/> acct	User's account status in tenant
23 <input checked="" type="checkbox"/> email	The addressable email for this user, if the user has one
<input type="checkbox"/> upn	An identifier for the user that can be used with the usema...

24 **Add** Cancel

Configuring Settings in the Azure Admin Center

Setup in Azure Active Directory Admin Center



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

The image shows two screenshots. The top screenshot is the 'Federated Logon - Add Provider' page. It has a 'Providers' dropdown set to '0365'. A blue box labeled '31' highlights the 'Metadata URL' field. Below it, the 'Application ID URL' is 'urn:amazon:cognito:sp:us-east-1_YFgF0IYir' and the 'Redirect URL' is 'https://auth.pii-protect.com/saml2/Idprespor'. A green 'Save' button is highlighted with a blue box labeled '32'. The bottom screenshot is a Microsoft 'Permissions requested' dialog. It states 'This application is not published by Microsoft.' and lists permissions: 'Sign you in and read your profile' (checked) and 'Consent on behalf of your organization' (unchecked). A blue box labeled '36' highlights the 'Consent on behalf of your organization' checkbox. A green arrow points to the 'Accept' button, which is highlighted with a blue box labeled '37'.

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

Your Logo Here

Wendy Smallfoot

Edit profile

My Dashboard

My Company

Manage Clients

Partner Profile

Search

Add Filter

Create

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.
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

Your Logo Here

Wendy Smallfoot

Edit profile

My Dashboard

My Company

Manage Clients

Partner Profile

Patty's Cakes

3

DashboardInformationNotificationProductsAccessDirectory SyncUsersPoliciesDocumentsSRADark WebTraining F

Current Information

Company Name

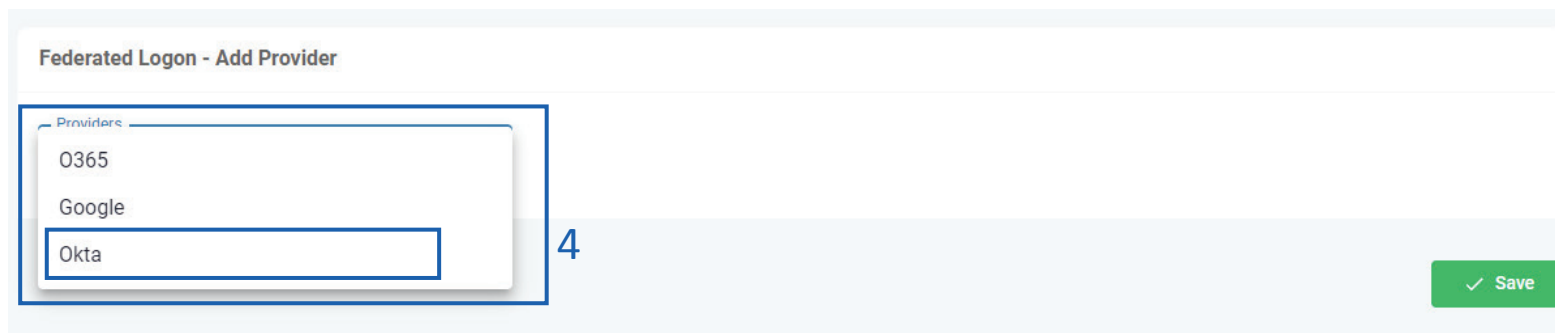
Patty's Cakes

Email Address

Options

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings



Federated Logon - Add Provider

Providers

0365

Google

Okta

4

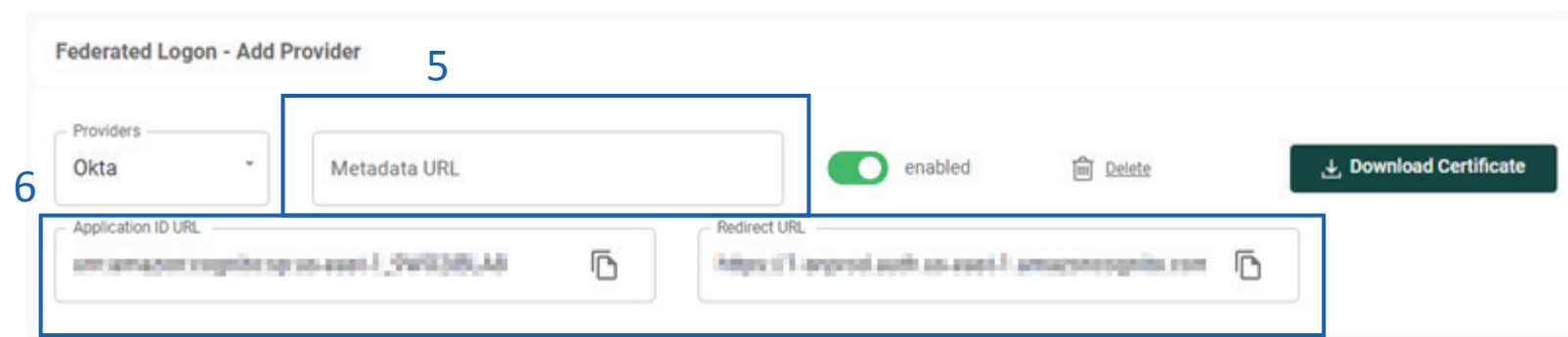
✓ Save

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.



Federated Logon - Add Provider

5

Providers

Okta

Metadata URL

6

Application ID URL

Redirect URL

enabled

Delete

Download Certificate

Configuring Settings in the Okta Admin Center

Setup in Okta Admin Center

The screenshot displays the Okta Admin Center interface. On the left, a navigation sidebar lists various sections: Dashboard, Directory, Applications, Self Service, Security, Workflow, Reports, and Settings. The 'Applications' section is highlighted with a blue bar and a yellow border, and a blue number '8' is placed to its left. The main content area is titled 'Applications' and features a message: '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.' Below this message, there are four buttons: 'Create App Integration', 'Browse App Catalog', 'Assign Users to App', and 'More'. The 'Create App Integration' button is highlighted with a yellow border and a blue number '9' is placed to its left. Below the buttons, there is a search bar and a table with the following data:

STATUS	
ACTIVE	0
INACTIVE	7

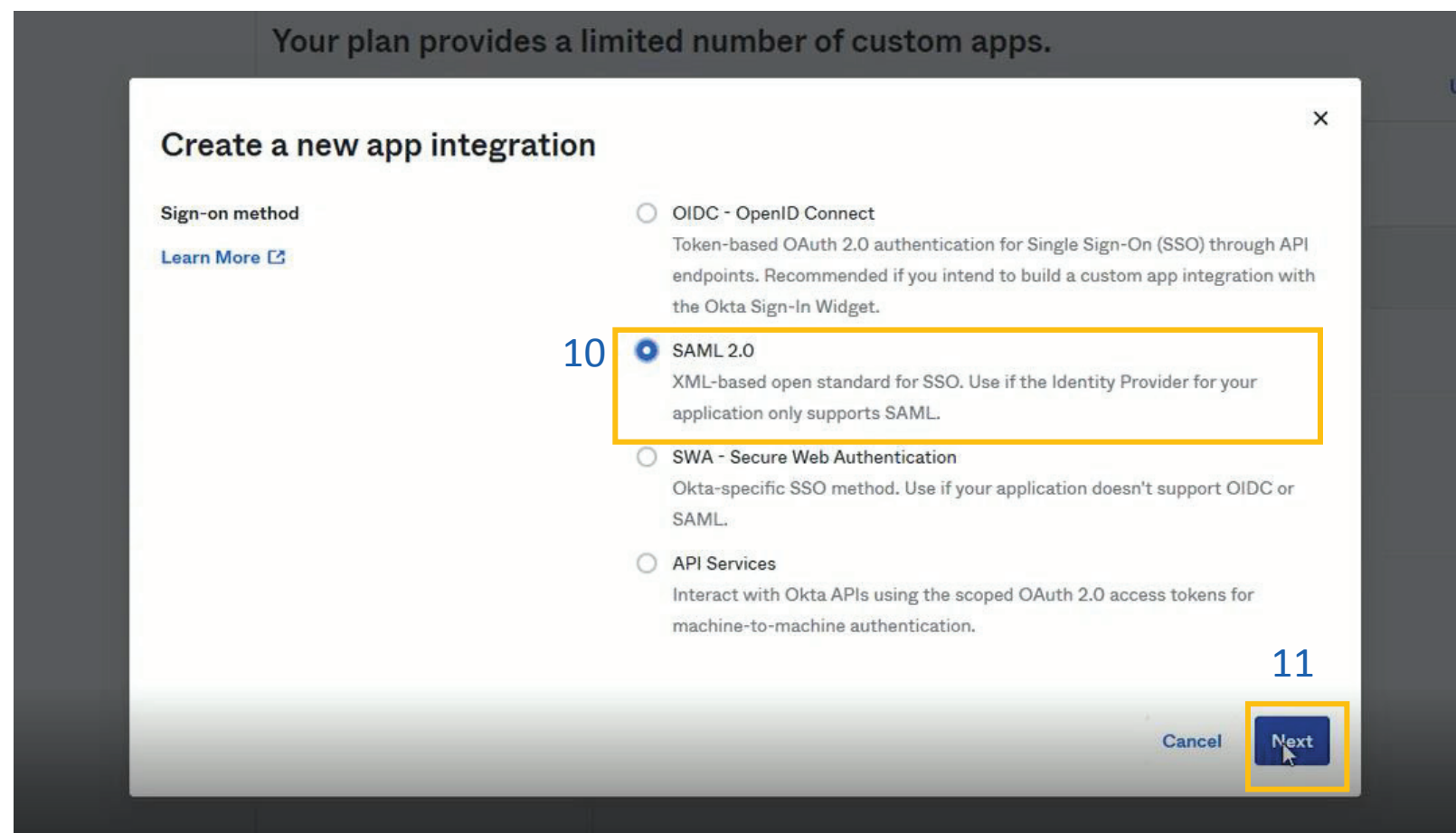
To the right of the table, there are three application cards: 'Okta Admin Console', 'Okta Browser Plugin', and 'Okta Dashboard'.

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



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 2 Configure SAML 3 Feedback

1 General Settings

12 App name

App logo (optional)   

App visibility ☐ Do not display application icon to users
☐ Do not display application icon in the Okta Mobile app

Cancel **Next** 13

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

Create SAML Integration

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 Login - Add Provider

Providers: Okta Metadata URL: **21** ☒ enabled [Hide Advanced Settings](#)

Application ID URL: **21**

Assertion Signature: Signed

Signature Algorithm: RSA-SHA256

Digest Algorithm: SHA256

Assertion Encryption: Unencrypted

19 Enable Single Logout: ☒ Allow application to initiate Single Logout

20 Single Logout URL:

22 SP Issuer:

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 23

Providers: Okta Metadata URL: ☒ enabled [Delete](#) [Download Certificate](#)

Application ID URL: Redirect URL:

Single Logout URL: [?](#)

SP Issuer: [?](#)

24 Signature Certificate: [Browse](#)

24 [Upload Certificate](#)

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) 27 [LEARN MORE](#)

25

Name
/claims/emailaddress

26

Name format
(optional)
Unspecified

Value
user.email

[Add Another](#)

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
	Unspecified	Starts with

[Add Another](#)

B Preview the SAML assertion generated from the information above

<> Preview the SAML Assertion

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

Previous

Cancel

Next

28

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

1 General Settings

2 Configure SAML

3 Feedback

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

Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

Previous

30Finish

Why are you asking me this?

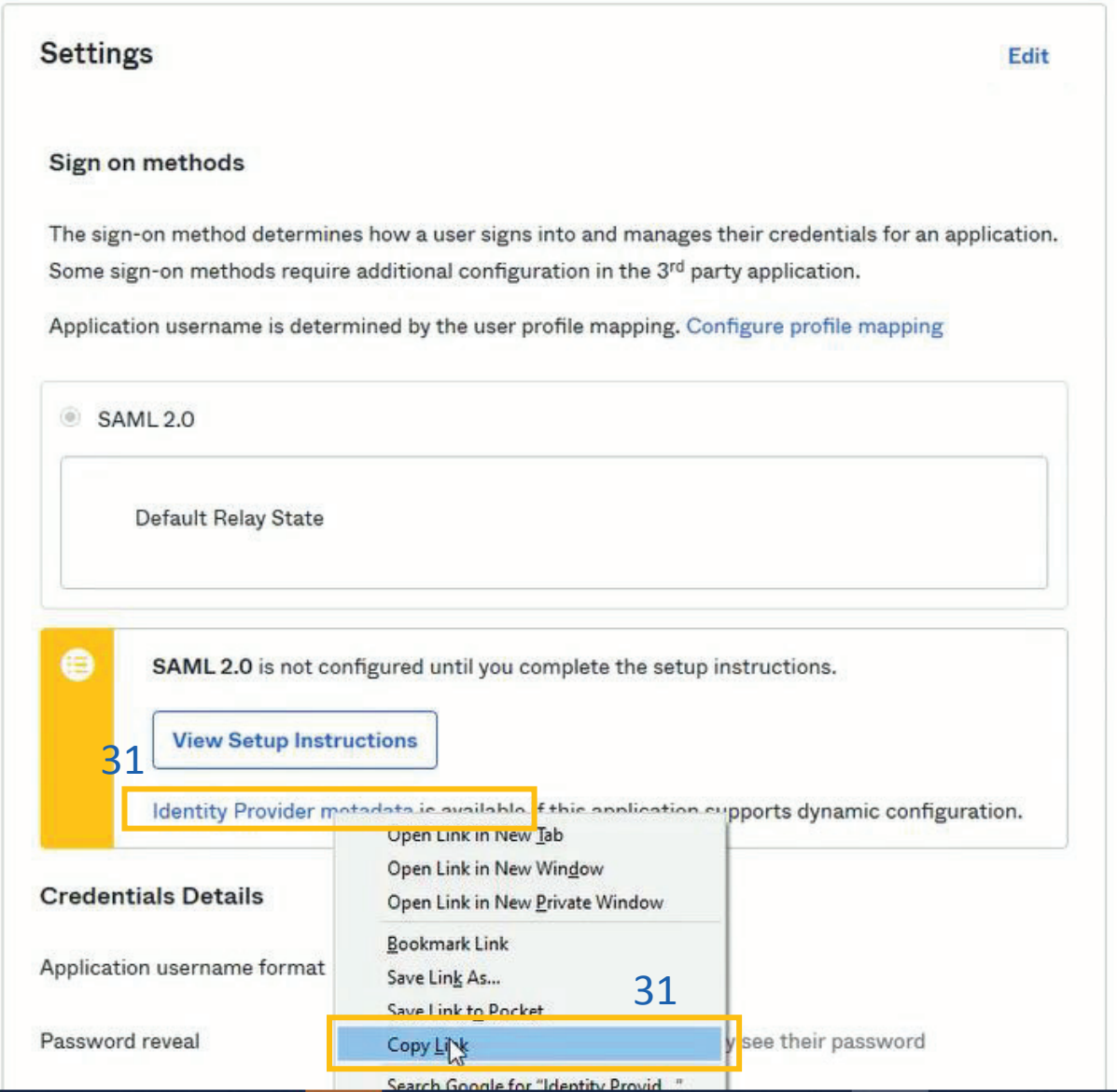
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

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



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 33

Providers: Okta

Metadata URL:

Application ID URL:

Redirect URL:

☒ enabled [Delete](#) [Download Certificate](#)

34

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

Your Logo Here

Wendy Smallfoot

Edit profile

My Dashboard

My Company

Manage Clients

Partner Profile

Search

Add Filter

Create

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

Your Logo Here

Wendy Smallfoot

Edit profile

My Dashboard

My Company

Manage Clients

Partner Profile

Patty's Cakes

Information

Notification

Products

Access

Directory Sync

Users

Policies

Documents

SRA

Dark Web

Training F

Current Information

Company Name

Patty's Cakes

Email Address

Options

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings

The screenshot shows a configuration interface titled "Federated Logon - Add Provider". It features a "Providers" dropdown menu with "Google" selected, a green toggle switch labeled "enabled", and a "Delete" link. A green "Save" button with a checkmark is located at the bottom right.

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