Security Awareness Training Partner Guide

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



www.TrustTelesystem.com

CALENDAR

SAT

FRI

5

12

19

26

Federated Login Setup

Table of Contents

General Information	pages 3	3 – 4	
Native MFA Configuration	pages 5	5-6	
Azure Configuration	.pages 7	7 – 1	5
Okta Configuration	pages 2	16 - 2	27
Google Configuration	.pages 2	28 – 2	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.

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

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

Your Logo Here										Toer Lago Mere
	Q Search									+ Create
Wendy Smallfoot	Name 1	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
-∕γ- My Dashboard	ABC Worldwide Product: Unlimited Cybersecurity Training					0			\oslash	×
🚊 My Company	Charitable Electronics Product: Unlimited Cybersecurity Training					0			\oslash	×
📥 Manage Clients	Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			\oslash	×
A Partner Profile	Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			\oslash	×

- Login as a Partner Administrator to the PII-Protect portal <u>here</u>. Once logged in select "Manage Clients" to access your client list (above).
- 2. Select the client you want to enable <u>Microsoft 365</u> 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

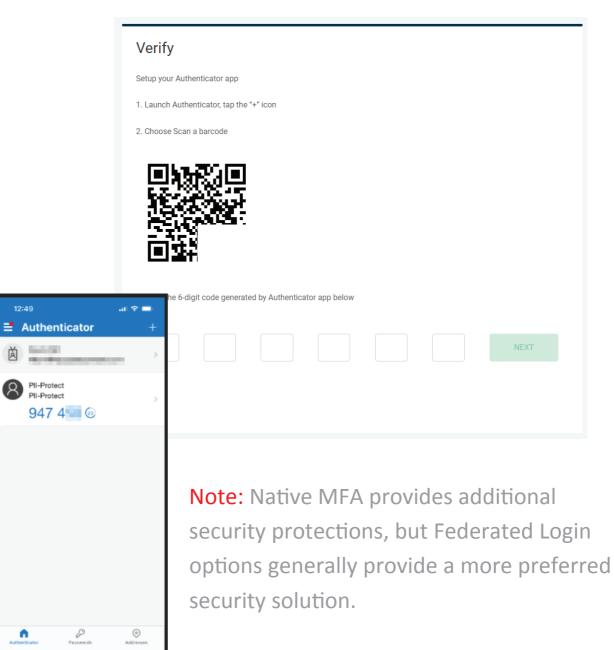
Your Logo Here	Patty's Cakes	Password
Wendy Smallfoot	Dashboard Information Products Access Directory Sync Users Policies Documents SRA Dark Web Training F	
-√ My Dashboard	Current Information	Enable MFA Access
Image Clients Image Clients	Patty's Cakes	
A Partner Profile		
	Options	

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.



Configuring Federated Login Within the PII Protect Portal – Microsoft 365

Navigating to the Client View Screen

Your Logo Here										Four Lage Man
	Q Search									+ Create
Wendy Smallfoot	Name 🛧	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
∧- My Dashboard	ABC Worldwide Product: Unlimited Cybersecurity Training					0			\oslash	×
🚊 My Company	Charitable Electronics Product: Unlimited Cybersecurity Training					0			\oslash	×
🔶 Manage Clients	Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			\oslash	×
A Partner Profile	Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			\oslash	×

- Login as a Partner Administrator to the PII-Protect portal <u>here</u>. 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

	Your Logo Here	Patty's	Cakes 3										
Wendy S		Dashboard	Information	Notification	Products	Access	Directory Sync	Users	Policies	Documents	SRA	Dark Web	Training F
	y Dashboard	Current In	nformation										
🚊 Му	y Company	Patty's					- Ema	il Address –					
🖆 Ma	anage Clients												
₽a	rtner Profile												
		Options											

Configuring Federated Login Within the PII Protect Portal – Microsoft 365

Configure Federated Login Settings

Federated Logon - Add Provider		
O365 Google	4	
Okta	✓ Save	1

	Federated Logon - Add	Provider 5			
6	O365 *	Metadata URL	enabled	m Delete	_
	Application ID URL	138-6881-1_9W028LA8	Redirect URL	mezancognito.com 🖸	
					🗸 Save

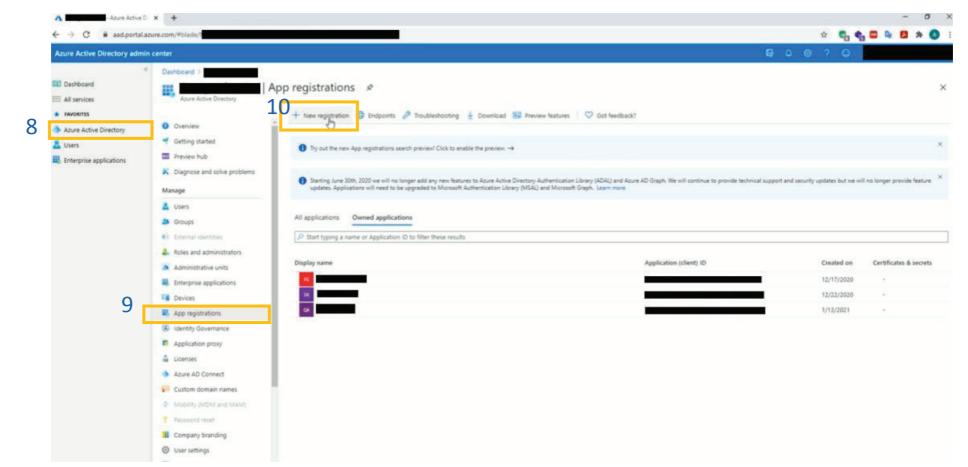
4. At the bottom of the screen for Federated Logon, select "**O365**"

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 <u>so keep this page open</u>.

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

Setup in Azure Active Directory Admin Center



- 8. Select "Azure Active Directory"
- 9. Select "App Registrations"
- 10. Select "New registration"

Setup in Azure Active Directory Admin Center

11. Enter name for application (example "prodportal")

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.

0365

14. Click "Register" 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. https://auth.pii-protect.com/saml2/idpresponse Web V Federated Logon - Add Provider 13 12 enabled Metadata URL Delete edirect UR Application ID URL ß 6 uncerneon cognito apue-east-1_9W0248LAB https://1-enpred.auth.us-east-1.amazoncognit By proceeding, you agree to the Microsoft Platform Policies 2 14

Dashboard > **Register an application**

Name

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

prod-portal

11

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) O Personal Microsoft accounts only

Help me choose..

Setup in Azure Active Directory Admin Center

15. Click "Add an Application ID URI"

16. Click "**Set**"

17. Return to your <u>PII Protect portal</u>page and locate the Application ID URLClick the "Copy" button.

18. Return to the Azure Admin Centerand paste this URL into the "Set the AppID URL" section.

Redirect URI

enabled

https://1-onpred.auth.us-east-1.amazoncognito.com

Delete

19. Click "Save"

Metadata URL

ercanozon cognito spise-east-1_9W02/BLAB

17

D

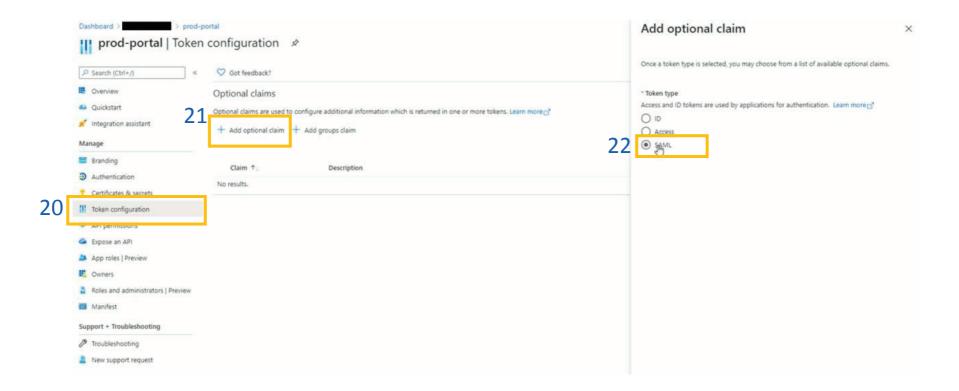
Federated Logon - Add Provider

0365

Application ID URI

Delete 🤀 Endpoints 🖬 Previ	iew features
Got a second? We would love your fe	feedback on Microsoft identity platform (previously Azure AD for developer). →
Essentials	
splay name : prod-portal	Supported account types : My organization only
oplication (client) ID :	1 Redirect URIs : 1 web, 0 spa, 0 public client
rectory (tenant) ID :	Application ID URI : Add an Application ID URI : Add an Application ID URI
bject ID :	Managed application in L. : prod-portal
🐴 Quickstart	Scol Set the App ID URI 18
1 Integration assistant	
Manage	Defir Application ID URI to parts of this urmamazon:cognito:sp:us-east-1_YFgF0iYir
	Defin Application ID URI to parts of this
Manage Branding	Defir Application ID URI to parts of this urn:amazon:cognito:sp:us-east-1_YFgF0iYir Addi
Manage Branding Authentication Certificates & secrets Token configuration	Defir Application ID URI to parts of this urn:amazon:cognito:sp:us-east-1_YFgF0iYir Addi
Manage Branding Authentication Certificates & secrets Token configuration API permissions	Defir Application ID URI to parts of this umamazon:cognito:sp:us-east-1_YFgF0iVir Addi type. Discard Discard to applicat
Manage Branding Authentication Certificates & secrets Token configuration	Defin Application ID URI to parts of this API c ummamazon:cognito:spus-east-1_YFgF0iVir Addi by: Stopes Discard Scopes Who can consent Admin consent display User consent display na State No scopes have been defined
Manage Branding Authentication Certificates & secrets Certificates & secrets Token configuration API permissions Expose an API	Defin Application ID URI to parts of this API c umamazon:cognito:spus-east-1_YFgF0iVir Addi biscard es' and define app roles assignable to applicat Scopes Who can consent Admin consent display User consent display na No scopes have been defined Admin consent display State
Manage Branding Certificates & secrets Certificates & secrets Token configuration API permissions Expose an API App roles Preview Owners Roles and administrators Preview	Defin Application ID URI to parts of this API c ummamazon:cognito:spus-east-1_YFgF0iVir Addi type. is and define app roles assignable to applicat Scopes Who can consent Admin consent display User consent display na Scopes have been defined
Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Preview Owners	Defin Application ID URI to parts of this API c umamazon:cognito:spus-east-1_YFgF0iVir Addi type. is and define app roles assignable to applicat Scopes Who can consent Admin consent display User consent display na Scopes Who can consent Admin consent display User consent display na No scopes have been defined
Manage Branding Certificates & secrets Certificates & secrets Configuration API permissions Expose an API App roles Preview Cowners Roles and administrators Preview Manifest	Defin Application ID URI to parts of this API c ummamazon:cognito:spus-east-1_YFgF0iVir Addi type. is and define app roles assignable to applicat Scopes Who can consent Admin consent display User consent display na Scopes have been defined

Setup in Azure Active Directory Admin Center



- 20. Select "Token configuration"
- 21. Select "Add optional claim"
- 22. Select "SAML"

Setup in Azure Active Directory Admin Center

25. Select "Turn on the Microsoft Graph email

permission (required for claims to appear in token)"

23. Select "email"

24. Click "Add"

26. Click "Add"

	email) require OpenId Connect scopes to be configured through ge or by checking the box below. Learn more
	oft Graph email permission (required for claims to appear in token).
26 Mode Cance	Ы
Access	
SAML	
Claim 🛧	Description
Claim 📬	Description
■ Claim ↑↓ □ acct マ email	Description User's account status in tenant The addressable email for this user, if the user has one

1

24 Add Cancel

Setup in Azure Active Directory Admin Center

Dashboard >		Endpoints	×
🔣 prod-portal 🖉	28		
		OAuth 2.0 authorization endpoint (v2)	
P Search (Ctrl+/) «	Delete Deletee Deletee Deletee Deletee Deletee Deletee Deletee Deletee Deletee Deleteee Delete	https://login.microsoftonline.com/ /oauth2/v2.0/authorize	D
2/ B Overview	Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD	OAuth 2.0 token endpoint (v2)	
duickstart	∧ Essentials	https://login.microsoftonline.com/	0
💉 Integration assistant	Display name : prod-portal	OAuth 2.0 authorization endpoint (v1)	
Manage	Application (client) ID :	https://login.microsoftonline.com/	D
	Directory (tenant) ID :	OAuth 2.0 token endpoint (v1)	
Branding	Object ID :	https://login.microsoftonline.com/l	D
Authentication		OpeniD Connect metadata document	
Certificates & secrets	Welcome to the new and improved App registrations. Looking to learn how it's changed from Apple of the second s	https://login.microsoftonline.com/	0
Token configuration		Microsoft Graph API endpoint	
API permissions	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authen	https://graph.microsoft.com	0
Expose an API	updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and N	Enderstein metedets das um ent	
🚨 App roles Preview	29	https://login.microsoftonline.com/i	D
Cowners	Call APIs	WS-Federation sign-on endpoint	63
Boles and administrators Preview		https://login.microsoftonline.com/	D
Manifest	🛎 🎊 👘 🏴 ĸ	SAML-P sign-on endpoint	
		https://login.microsoftonline.com/	D
Support + Troubleshooting	X 🗊 👝 🚺 💽	SAML-P sign-out endpoint	
Troubleshooting		https://login.microsoftonline.com/	D
New support request	Build more powerful apps with rich user and business data from Microsoft services and your own company's data		
	sources.		
	View API permissions		

27. Select "Overview"

- 28. Select "Endpoints"
- 29. Copy link under "Federation metadata document"

Cign in upper in 5 min

30. Return to the <u>PII Protect Portal</u> for the final steps.

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings

O365 Metadata UF	RL enabled 🛍 <u>Delete</u>	
- Application ID URL	gF0iYir	32
	Microsoft	
	Permissions requested	
	Permissions requested	
	This application is not published by Microsoft.	
36	This app would like to:	
	Consent on Behalf of your organization	
10	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 37	

31. Paste in the "Metadata URL" you've copied from the AzureAdmin 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 <u>log back into the Portal with a user</u> 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										Your Lago Her
	Q Search								╤ Add Filter	+ Create
Wendy Smallfoot	Name 1	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
-∕γ- My Dashboard	ABC Worldwide Product: Unlimited Cybersecurity Training					0			\oslash	×
🚊 My Company	Charitable Electronics Product: Unlimited Cybersecurity Training					0			\oslash	×
🚖 Manage Clients	Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			\oslash	×
2 Partner Profile	Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			\oslash	×

- Login as a Partner Administrator to the PII-Protect portal <u>here</u>. 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	's Cakes 3
Dashboa Wendy Smallfoot	rd Information Notification Products Access Directory Sync Users Policies Documents SRA Dark Web Trainin
	nt Information
My Company	Notification Products Access Directory Sync Users Policies Documents SRA Dark Web Training F mation
♣ Manage Clients	
A Partner Profile	
Optio	ns

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings

Federated Logon - Add Provider	
O365 Google	
Okta Z	✓ Save

	Federated Logon - Add F	Provider 5						
5	Okta *	Metadata URL			enabled	Delete		
	- Application ID URL	con-exect1_99/8386,A8	ē	Redirect URL	prolauthan aunt la	muconcognits con	6]

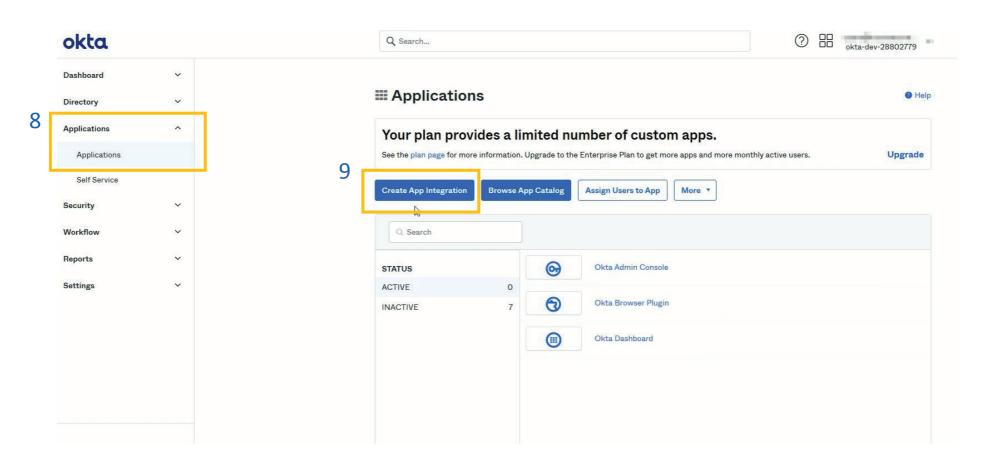
4. At the bottom of the screen forFederated Logon, select "Okta"

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 <u>so keep this page open</u>.

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

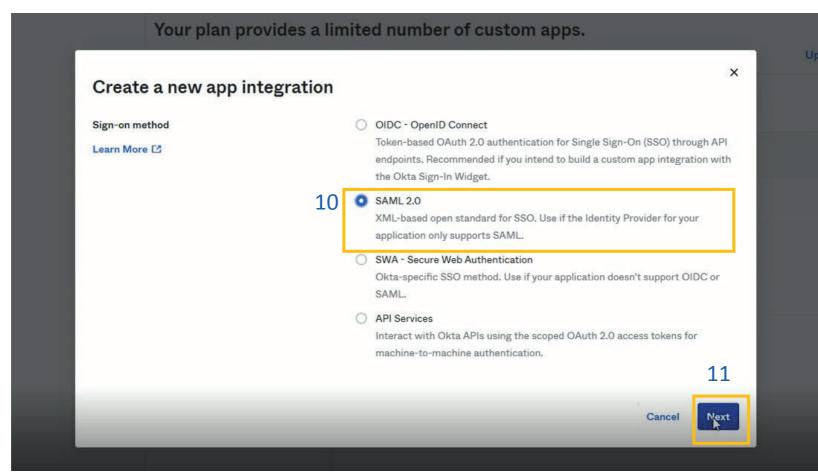
Setup in Okta Admin Center



8. Within the Okta Admin view Select "Applications" from the left panel then "Applications"

9. Select "Create App Integration"

Setup in Okta Admin Center

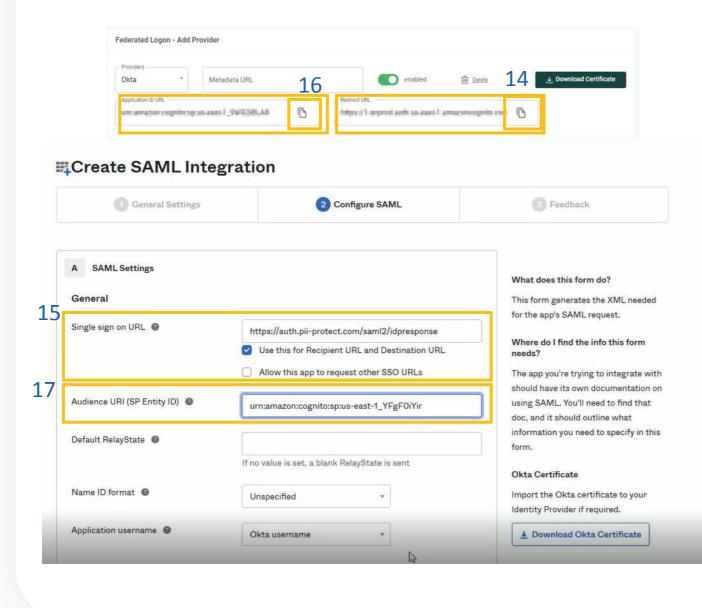


10. Within the pop-up window, select "SAML 2.0"

11. Click the "Next" button

	1 General Settings	Configure SAML	3 Feedback	
	1 General Settings			
2	App name	Portal		
	App logo (optional) 🜑			
	App visibility	 Do not display application icon to users Do not display application icon in the Okta Mobile application 	p	
	Cancel	1	13 J3	
		App name" type "Portal"	13	

Setup in Okta Admin Center



14. Return to your <u>PII Protect portal page</u> 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 <u>PII Protect portal page</u> and locate the Application ID URL. Click the "**Copy**" button.

17. Back in your Okta Admin Center, in theAudience URL section, past theApplication ID URL you've copied.

Setup in Okta Admin Center

tion ID URL	Metadata URL 21	enabled 🚔 Detecte	Certificate Hide Adv	anced Settings
		auth an auto 1 amagneografie con		
	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	https://auth.pii-protec	t.com/saml2/logout]
22	SP Issuer	whankonogritosy	constructing Parts	
	Signature Certificate			Browse
		Upload Certificate		

18. Click the "Show Advanced Settings"

19. In the Enable Single Logout, check the boxto "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

Setup in Okta Admin Center

a	Metadata URL		enabled 🛍 Delete	↓, Download Certif
cation ID	URL		C Redirect URL	
ener	e regelte spiso-aust 1,5W2385,A8	G	Adject (1-argent auth as and 1-amagneophic con	
	Single Logout URL		https://auth.pii-protect.com/saml2/logout	
	SP Issuer		urn:amazon:cognito:sp:us-east-1_YFgF0iYir	
	Signature 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

Name	Name format 26 (optional)	Value	
·/claims/emailaddress	Unspecified 🔻	user.email	_
Add Another			
Group Attribute Stat	ements (optional)		
Name	Name format (optional)	Filter	
	Unspecified *	Starts with 🔹	
Add Another			
B Preview the SAML	assertion generated fro	m the information above	
• Preview the SAM	IL Assertion	ß	

Setup in Okta Admin Center

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/ide ntity/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.

Setup in Okta Admin Center

General Settings	2 Configure SAML	3 Feedback
3 Help Okta Support understand ho	w you configured this application	Why are you asking me this?
Are you a customer or partner? 29	I'm an Okta customer adding an internal app	This form provides Okta Support with
	 I'm a software vendor. I'd like to integrate my app with Okta 	useful background information about your app. Thank you for your help—w appreciate it.
• 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	

Enter any links here		
Any tips or additional comments?	ß	<u></u>
Placeholder text		
£		

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.

Setup in Okta Admin Center

Sign on methods		
The sign-on method determine	s how a user signs into and manages their creder	ntials for an application
Some sign-on methods require	additional configuration in the 3 rd party applicat	ion.
Application username is determ	nined by the user profile mapping. Configure prof	ïle mapping
SAML 2.0		
Default Relay State		
31 View Setup Instru	figured until you complete the setup instructions ctions	
31 View Setup Instru Identity Provider mod	ctions	
31 View Setup Instru	<mark>ctions</mark> tadata is available, <mark>f this application supports dyr</mark> Open Link in New <u>I</u> ab Open Link in New Win <u>d</u> ow	

.

31. In Settings, right-click on the "IdentityProvider 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 F	Provider 33	3	
Providers Okta *	Metadata URL		enabled In Delete Jownload Certificate
Application ID URL	us-east-1_9W02BL48	ß	https://l-anproduauthus-east-1.amazoncognito.com
			34
			✓ Save

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										Your Lago Me
	Q Search								∓ Add Filter	+ Create
Wendy Smallfoot	Name 1	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
-∧,- My Dashboard	ABC Worldwide Product: Unlimited Cybersecurity Training					0			\oslash	×
🚊 My Company	Charitable Electronics Product: Unlimited Cybersecurity Training					0			\oslash	×
🔶 Manage Clients	Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			\oslash	×
A Partner Profile	Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			\oslash	×

- Login as a Partner Administrator to the PII-Protect portal <u>here</u>. 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

Wendy Smallfoot Information Notification Products Access Directory Sync Users Policies I Edit profile Formation Edit profile Edit profile Edit profile Edit profile	uments SRA	Dark Web Trair	ning F		
Current Information					
-√γ∽ My Dashboard					
Image: My Company Company Name Email Address Patty's Cakes Email Address					
Section 1 Sectio	e Clients				
2 Partner Profile					
Options					

Configuring Federated Login Within the PII Protect Portal

Configure Federated Login Settings

Fed	erated Logon - Add Provider	
	oviders	enabled ៣ <u>Delete</u>
		S Save

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.



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