



Breach Secure Now Partner Guide

— User Management

Azure AD Sync, On-Premise AD Sync, G-Suite Sync, and Bulk User Management

Questions, Concerns? Want a 1-on-1 on-boarding with our Operations team?

Email: Operations@breachsecurenow.com

Phone: (877) 275 – 4545



User Management

Table of Contents

Resources <i>marketing content, how-to guides, & additional info</i>	<u>page 3</u>
User Management Overview <i>methods to adding users & overview</i>	<u>page 4</u>
General User Management <i>basic manual user options</i>	<u>pages 5 – 10</u>
<i>Creating a New User</i>	<u>pages 5 – 6</u>
<i>Adding Tags</i>	<u>page 7</u>
<i>Editing an Existing User</i>	<u>pages 8 – 10</u>
Azure Active Directory Sync – Simple Setup <i>setup, notifications, and automated user management</i>	<u>pages 11 – 20</u>
<i>Setup in Microsoft 365 Admin Center</i>	<u>pages 11 – 14</u>
<i>Configurations Within the PII Protect Portal</i>	<u>pages 10 - 15</u>
Azure Active Directory Sync – Classic Setup <i>setup, notifications, and automated user management</i>	<u>pages 21 – 32</u>
<i>Setup in Microsoft 365 Admin Center</i>	<u>pages 21 – 26</u>
<i>Configurations Within the PII Protect Portal</i>	<u>pages 27 – 32</u>
On-Premise Active Directory Sync <i>Integration with on-premise AD</i>	<u>pages 33 – 42</u>
<i>Setup in On-Premise Active Directory</i>	<u>pages 33 – 37</u>
<i>Configurations within the PII Protect Portal</i>	<u>pages 38 – 40</u>
<i>Downloading the On-Premise Directory Sync Agent</i>	<u>page 41 – 42</u>
<i>Additional Information for On-Premise Directory Sync</i>	<u>page 43</u>
G-Suite Directory Sync <i>setup, notifications, and automated user management</i>	<u>pages 44 – 57</u>
<i>Setup in Google Console</i>	<u>pages 44 – 54</u>
<i>Configurations within the PII Protect Portal</i>	<u>pages 55 – 57</u>
Bulk User Management via CSV <i>setup, notifications, template modification</i>	<u>pages 58 – 61</u>
<i>Configuring Message & Notification Settings</i>	<u>pages 58 – 59</u>
<i>CSV Template Modification & Uploading</i>	<u>pages 60 – 61</u>

User Management

Resources

- [BSN Program Overview](#)
- [In-Portal Purchasing & Billing](#)
- Find product-specific how-to guides in the Partner Resources page!

User Management Overview

Adding, updating, deleting, and deactivating users in the PII/PHI Protect portal can be done manually, by .csv file, by Azure Active Directory (Azure AD), or with our On-Prem solution.

General User Management – page 5

A quick overview of the basic user options including ad-hoc user creation, editing a user, and creating Tags.

Azure Active Directory Synchronization – setup starts on page 10 or page 20 – see below

Azure AD allows you to simply manage your PII Protect users for your Azure clients. Choose between Classic setup and Simple Setup.

Simple Setup - *Recommended

This syncing feature will take away all your syncing pain points. Quickly access your client's directory, verify counts and groups, then sync users within minutes. No more long waiting for initial syncs, no more Powershells, no more headaches!

Requirement: You must have a Global Admin account in the tenant you are syncing. Begin on [Page 10](#)

Classic Azure AD Sync

For Partners without access to a Global Admin account within their client's tenant, Classic Azure AD Sync will be your best option. Powershell script options will be provided but initial syncs will take up to 4 hours. No instant verification of set up is available.

For this set up process, begin on [Page 20](#)

On-Premise Active Directory via our NEW Active Directory Monitor and Sync Agent – setup starts on page 32

If you have clients that are using On-Premise, you can utilize Active Directory along with our new Active Directory Monitor and Sync solution to sync with the Breach Secure Now portal and simplify user management for your clients!

G-Suite Directory Synchronization – setup starts on page 42

G-Suite Directory Sync allows you to simply manage your PII Protect users for your G-Suite clients.

Bulk User Management via CSV Upload – setup starts on page 56

If you'd prefer to manage users manually, we provide a .csv that is available for adding, updating, or deactivating users inside the PII/PHI portal.

If you have any questions, please feel free to contact us at operations@breachsecurenow.com

General User Management – Creating a New User

We've made it easy for Partners to quickly add users on-the-fly. Though setting up synchronization tools are more beneficial for automation, ad-hoc user creation can help for smaller clients or trialing users.

Adding a New User

The screenshot displays the PII Protect user management interface. The 'Users' tab is selected, and the '+ New User' button is highlighted. A modal form titled 'Create New User' is open, showing fields for Group Role, Personal Info, and Access Information. The 'Group Role' dropdown is highlighted with a blue box and the number 4.

1 To add a new user, within your desired client, click the “Users” tab

2 To add a new user, click the “New User” button

3 A modal will appear with options to create a new user.

4 Group Role: Select the user’s access level by role.

Employee: Basic access to interact with trainings and read-only document access

Manager: Full access to manage company account, employees, view reports, add/edit documents etc.

Manager Admin: Manager level access plus the ability to schedule and send phishing campaigns

Continued...

General User Management – Creating a New User

We've made it easy for Partners to quickly add users on-the-fly. Though setting up synchronization tools are more beneficial for automation, ad-hoc user creation can help for smaller clients or trialing users.

Adding a New User

The screenshot shows a 'Create New User' dialog box with the following fields and callouts:

- 5**: Tag (dropdown menu)
- 6**: First name * (text input)
- 6**: Last name * (text input)
- 7**: Phone number (text input with country code dropdown and '+1' indicator)
- 7**: Ext. (text input)
- 7**: Cell number (text input with country code dropdown and '+1' indicator)
- 8**: Email * (text input)
- 8**: Confirmed email (text input)
- 9**: Password * (text input)
- 9**: Verify password (text input with eye icon)
- 10**: Send welcome message (checkbox)
- 11**: Add User (green button with checkmark)

5. Tag: (optional) Select a pre-set tag for this user (for information on tag creation, see page 7)
6. First/Last name: required
7. Phone numbers: (optional) enter their work and/or cell phone numbers
8. Email: (required) this will be how the user accesses their account with. Must be a valid email.
9. Password: Password must be at least 6 characters in length. *Not required if "Send welcome message" is enabled (see below)
10. Send welcome message: If enabled, a welcome email will be sent to user's email once created. No password would be set upon creation screen, user would set their own password via the welcome message.
11. Click "Add User" button when ready

Note: If synchronization methods (Azure, On-Prem, Google) are enabled, creating users manually via this method will result in an error. The user should be set up via the appropriate sync method instructions.

General User Management – Adding Tags

Tags are an easy way to position users into groups to help with more accurate reporting and tracking. Tags can be set up within the “User” tab or can be created using any other synchronization method (Azure, On-Prem, Google, CSV)

Adding Tags

The screenshot shows the PII Protect user management interface. The 'Users' section is active, and the '+ New Tag' button is highlighted with a blue box and the number 1. A modal window titled 'Create Tag' is open, showing a text input field labeled 'Enter a tag...' with a blue box and the number 3, and an '+ Add Tag' button with a blue box and the number 4. Below the input field is a table of existing tags with columns for Name, Created, and Modified. The table contains three rows: Finance, Human Resources, and Product. A blue box and the number 5 highlight the table. The modal also shows pagination information: '1 - 3 of 3 Items', '25' items per page, and page '1'.

1. To create or manage tags, navigate to the “Users” section for the client, select “New Tag”.
2. A modal will appear where existing tags will appear, and new tags can be entered or managed.
3. To add a new tag, type your desired tag name in the “Enter a tag” textbox.
4. Click “Add Tag”.
5. The new tag should appear in the list below.
6. Users can be assigned tags when created individually or after creation by editing the user(s).

General User Management – Editing a User

After a user is created, their account details can be edited. Note: If certain directory sync or federated login options are enabled, some fields may not be editable within the PII Protect portal.

Editing an Existing User

	Name	Email	Group Role	Last Login	Tag	ESS	Data Breaches
<input type="checkbox"/>	Piere, Junior	Jane@gmail.com	1 MA	03/10/2022	350	0	
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							

1. To edit an employee, in the “Users” section, select/click the user you are editing.
2. A modal will appear with existing user data.
3. You can edit the Role, Tag, First/Last name, Email Address, Phone, and Password.
4. Acknowledge Policies: If slider is on (green) the user has acknowledged the provided policies and procedures. You may check or uncheck these here.
5. Messages: Here you can authorize this user (only for managers) for company positive opt-in for the weekly Micro Trainings. See [this guide](#) for reference.
6. Enable individual level access for weekly Micro Training emails to be sent to the user.

Edit User

3 Group Role * Manager Tag Empty TAG

First name * Junior Last name * Piere

Email Address * Jane@gmail.com Phone number +1

Extension Mobile Number +1

Password Verify password

4 Acknowledge Policies
 Security Other

5 Messages
 Authorized for Company Positive Opt-in for Micro-Training/Monthly Newsletter

6 Weekly Training and Monthly Newsletters
 Receive weekly training and monthly newsletter emails

Cancel Save

Note: Passwords must now meet certain complexity requirements. Passwords are measured compared to their overall crackability. If your password is rated as too risky, try adding an additional word or additional characters.

General User Management– Editing a User

After a user is created, their account details can be edited. Note: If certain directory sync or federated login options are enabled, some fields may not be editable within the PII Protect portal.

Editing an Existing User

7. Additional options may be available for users within YOUR MSP's tenant including;
 8. Billing – Enables user to access billing tab of portal
 9. Marketing Material – Enables user to access Partner Resource Kit
 10. Payment Information – Enables the user to edit payment information
 11. Tax Exempt – Enables user to access the Sales Tax Exemptions tab
 12. Click the “Save” button to save any edits made
- Note:** If synchronization methods (Azure, On-Prem, Google) are enabled, editing users manually via this method may result in an error for certain fields. The user should be edited via the appropriate sync method instructions.

The screenshot shows the 'Edit User' form with the following fields and sections:

- Group Role ***: Employee
- Tag**: [Tag icon]
- First name ***: [First name field]
- Last name ***: [Last name field]
- Email Address ***: [Email field]
- Phone number**: +1 (1) [Phone field]
- Extension**: [Extension field]
- Mobile Number**: +1 (1) [Mobile field]
- Additional Access**:
 - Billing: (8)
 - Marketing Material: (9)
 - Payment Information: (10)
 - Tax Exempt: (11)
- Acknowledge Policies**:
 - Security:
 - Other:
- Messages**:
 - Authorized for Company Positive Opt-in for Micro-Training/Monthly Newsletter:
- Weekly Training and Monthly Newsletters**:
 - Receive weekly training and monthly newsletter emails:
- Buttons**: Cancel, Save (12)

General User Management– Editing a User

After a user is created, their account details can be edited. Note: If certain directory sync or federated login options are enabled, some fields may not be editable within the PII Protect portal.

User Actions

1. Actions can be performed on any or multiple users. Use the checkbox options to select the user(s) you wish to perform the action on.

- Activating a User
- Inactivating a User
- Sending a Welcome Message
- Clearing a Bounced Email
- Resetting a Password
- Deleting a User
- And Resetting a Deleted User
- Resetting MFA*

Tip: Using the “select all” checkbox at the top of the table will only select all the users on the current page. Performing an action for all users would need to be done on a page-by-page basis.

Tip: If native MFA is enabled, and user has issues accessing the portal, use the “Reset MFA” action.

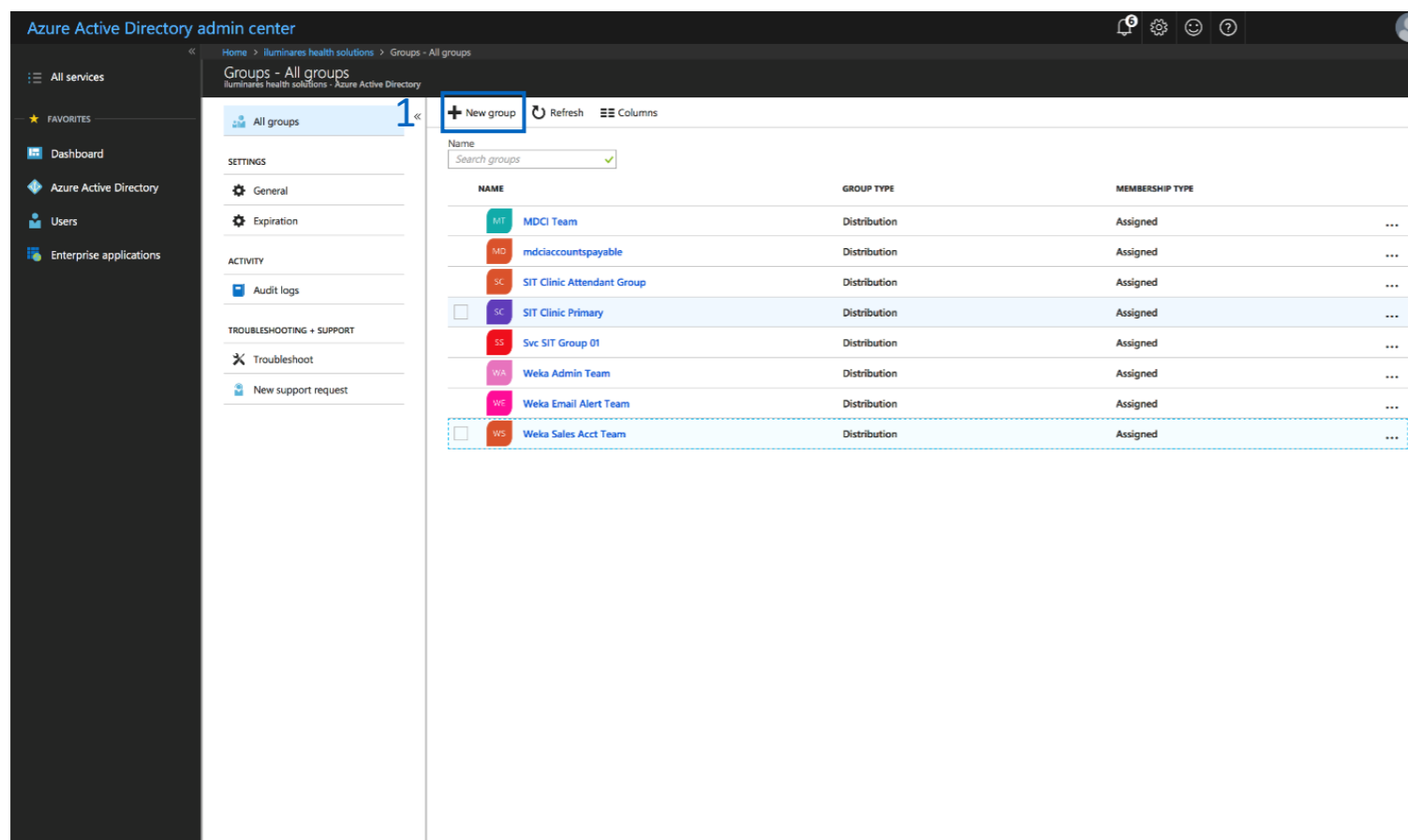
The screenshot displays the PII Protect user management interface for 'Bob's Burgers'. The interface includes a navigation bar with options like Information, Notification, Products, Access, Directory Sync, Users, Dark Web, and Training. Below the navigation bar is a search bar and buttons for 'Add Filter', '+ New User', '+ New Tag', and '+ Actions'. A table of users is shown with columns for 'Name' and 'Email'. The first row is selected. A dropdown menu is open over the 'Actions' column, listing various actions: Active, Inactive, Welcome Message, Clear Bounced Email, Reset Password, Delete, Reset Deleted User, and Reset MFA. The 'Reset MFA' option is highlighted with a green checkmark.

<input type="checkbox"/>	Name	Email	Actions
<input checked="" type="checkbox"/>	Grace, William	[REDACTED]	<ul style="list-style-type: none"> ☑ Active ☑ Inactive ✉ Welcome Message 🗑️ Clear Bounced Email 🔄 Reset Password 🗑️ Delete 🔄 Reset Deleted User 👤 Reset MFA
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🔒
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️
<input type="checkbox"/>	[REDACTED]	[REDACTED]	🗑️

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



1. Create Azure AD Sync Security Groups to define the portal access for each employee. **The following two groups MUST be created:**

BSN-Employees: Defines the users that will be enrolled in the portal as standard employees under that client.

BSN-Managers: Defines users in the manager role, supersedes BSN-Employees.

- Managers get access to reporting and employee data inside the PII/PHI Protect portal.

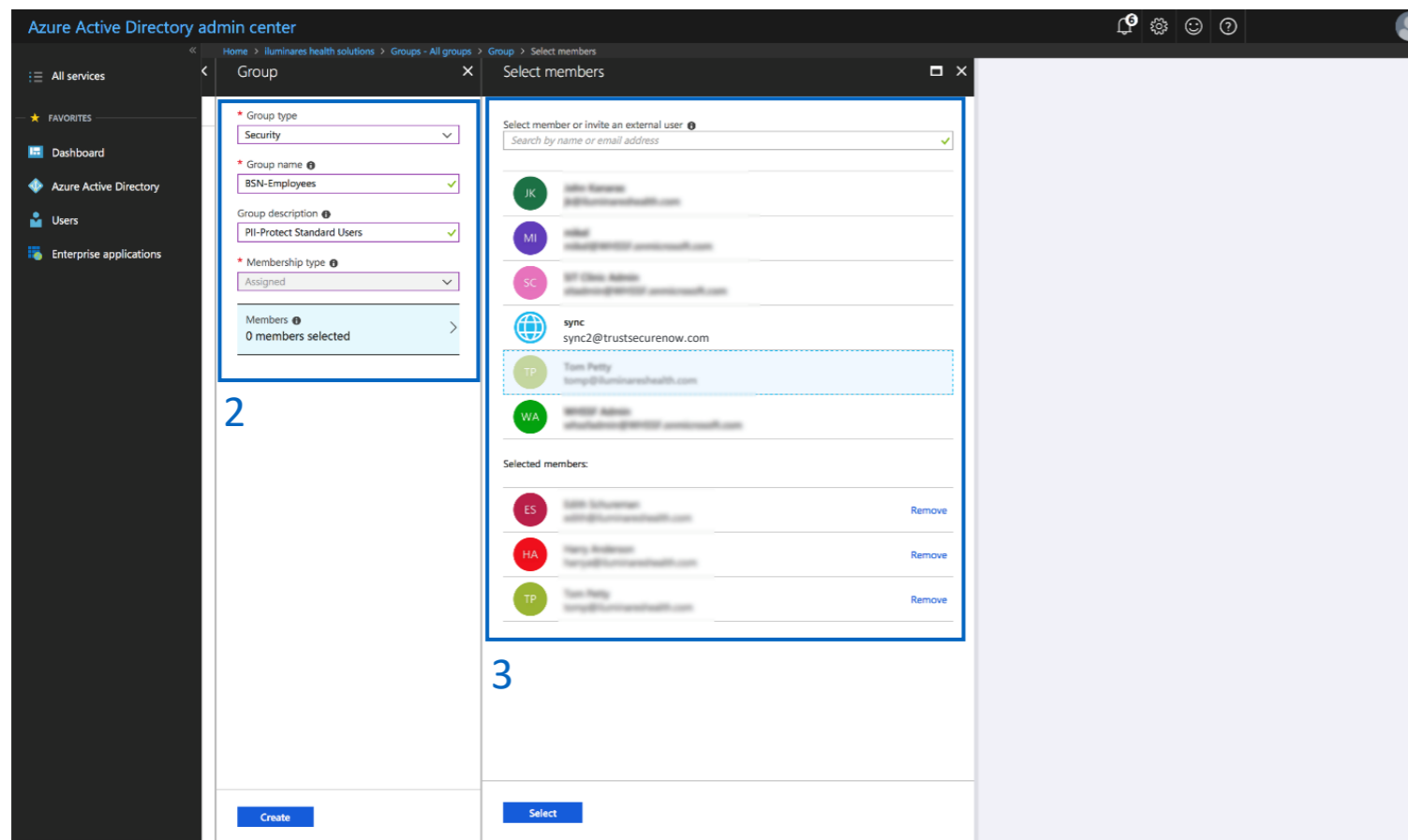
Note: When entering the above security groups, spaces are NOT permitted before, after, or within the string.

Important: If Azure AD Sync is enabled and these groups are NOT defined after the initial synchronization, there is a risk of users becoming deactivated in the portal and the users will be notified.

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



2. Create the **BSN-Employees** group with the following parameters:

Group Type: Security

Group Name: BSN-Employees

Group Description: PII/PHI Protect Standard Users

3. Assign users to the group.

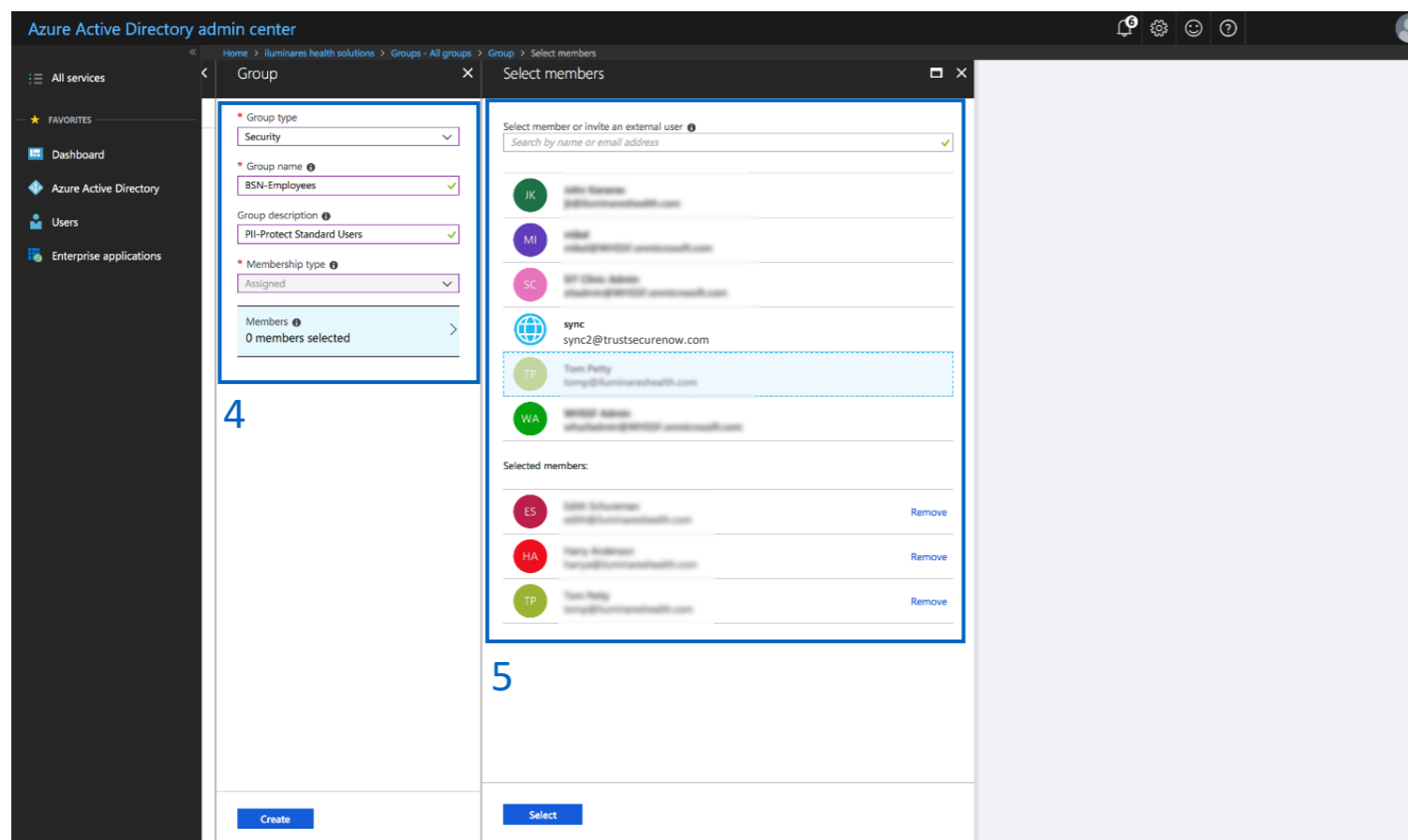
Note: Be sure not to assign non-user accounts to this group as portal accounts WILL be created for all users assigned to this group. If you assign users to this group and to the BSN-Manager group, the manager role will take precedence.

Important: For those using On-Premise along with Azure Sync to synchronize with the free tier or Azure AD: Nested group memberships are not supported for group-based assignment at this time.

Azure Active Directory Sync Setup – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



Optional Group: Add the **BSN-ManagerAdmins** group to give select managers the ability to manage phishing campaigns as well as the bulk manage user functionality. Standard manager accounts do NOT have this functionality. Follow steps 2 - 3 using **Group Name:** BSN-ManagerAdmins and **Group Description:** PII/PHI Protect Manager Admin Role

4. Create the **BSN-Managers** group with the following parameters:

Group Type: Security

Group Name: BSN-Managers

Group Description: PII/PHI Protect Manager Role

5. Assign users to the group. All managers will also have an employee account.

Optional Group: BSN-PartnerAdmins

Group Type: Security

Group Name: BSN-PartnerAdmins

Group Description: PII/PHI Protect Partner Administrator Role

- This user has the **highest** level of access and will have all administrative functions for all accounts within your portal. **This group is to ONLY be used for your company's internal Breach Prevention Platform (BPP) account**

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center

The screenshot shows the Azure Active Directory admin center interface. On the left, the navigation pane includes 'Dashboard', 'All services', 'Azure Active Directory', 'Users', and 'Enterprise applications'. The main content area is divided into two panels. The left panel, titled 'New Group', contains a form with the following fields: 'Group type' (Security), 'Group name' (BSN-TAG-Executive Team), 'Group description' (Executive Team Tag for BSN), and 'Membership type' (Assigned). Below these fields are sections for 'Owners' and 'Members'. A blue box highlights the form fields, and a blue '6' is placed below it. At the bottom of the panel is a blue 'Create' button, highlighted with a blue box and a blue '8'. The right panel, titled 'Add members', has a search bar and a list of services including 'AAD Request Verification Service - PROD', 'App Studio for Microsoft Teams', and 'Azure Media Service'. A blue box highlights the search bar and the list, with a blue '7' below it. At the bottom of the panel is a blue 'Select' button.

6. **Optional:** Create Tag Groups.

Tags are used for creating specific groups, typically to separate users by department, to create groups you'd like to send specific phishing emails to, or to simplify tracking in the portal.

Group Type: Security

Group Name: BSN-TAG-**tagname**

*tagname will be the tag you want the users associated with.

Example: BSN-TAG-Executive Team, BSN-TAG-Finance, etc.

Group Description: Optional field if you would like to add details on the tag you created.

7. Assign users to the group.

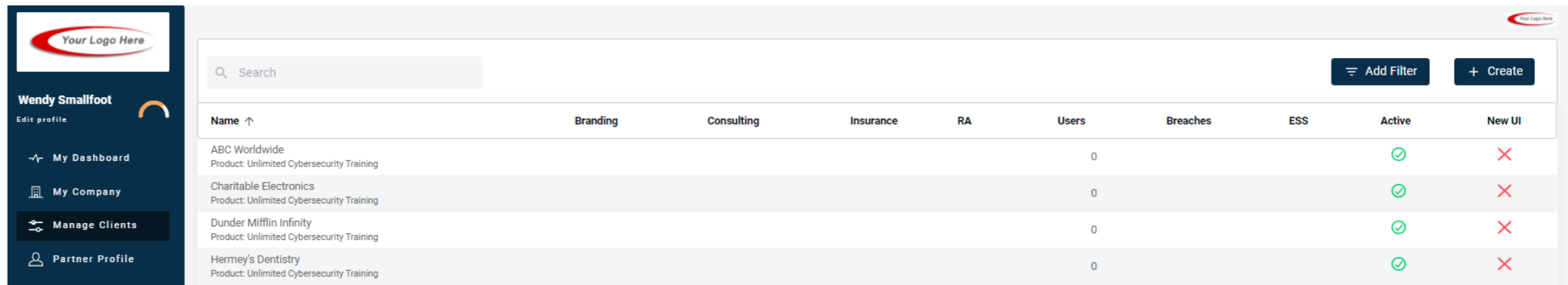
8. Click "**Create**".

Important: For those using On-Premise along with Azure Sync to synchronize with the free tier or Azure AD: Nested group memberships are not supported for group-based assignment at this time.

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal – Simple Setup



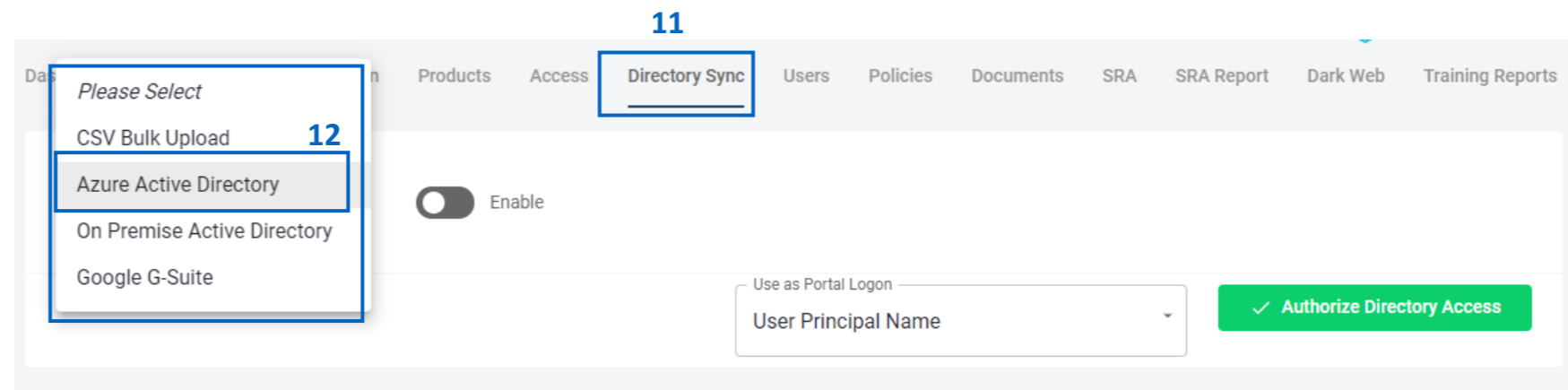
Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's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

9. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in select “Manage Clients” to access your client list (above).

10. Select the client you want to sync with Azure Active Directory.

11. Select the “**Directory Sync**” tab

12. Use the Sync Type drop-down selector to select “Azure Active Directory”



11

12

Products Access **Directory Sync** Users Policies Documents SRA SRA Report Dark Web Training Reports

Please Select

CSV Bulk Upload

Azure Active Directory

On Premise Active Directory

Google G-Suite

Enable

Use as Portal Logon

User Principal Name

✓ Authorize Directory Access

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal – Simple Setup

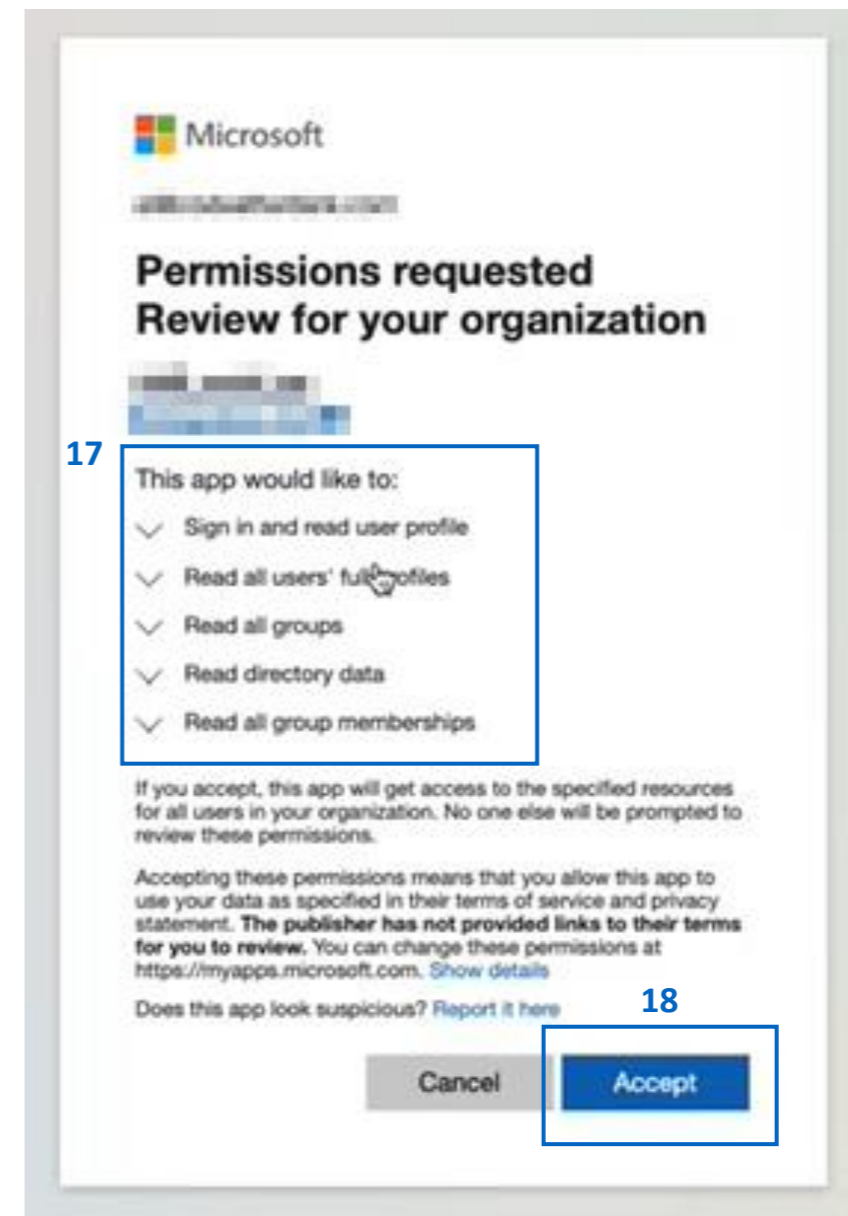
13. For Simple Setup, click the **“Enable”** button to begin (**not the “Enable Manual Setup” button**)
14. Select which option you would like to use as Portal Logon. **We highly recommend “Email”**
15. When ready, select the **“Authorize Directory Access”** button
16. You will be taken to the Microsoft sign on page. You **MUST** select/sign in with an account that is Global Admin within the client's tenant

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal – Simple Setup

17. After signing into your Global Admin account within the tenant, you will be requested to accept the permissions required for this sync
18. Review the permissions then click **“Accept”**
19. A verification process will occur quickly to ensure that your account has the required access



Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal – Simple Setup

20

21

20. If successful, a “Verified Successfully!” notification will appear below the Azure Active Directory sync type

21. Before Authorizing Directory Access, we recommend configuring your Welcome Message options. More information on this is available in the next page.

Azure Active Directory Sync – Simple Setup

Setup Application Authentication with Azure AD on the client Azure AD Sync Settings Page. You will be required to run a Powershell Script and access Azure AD for the client you'll be configuring Application Authentication for.

Configure Messaging & Notification

The screenshot displays the Azure AD Sync Settings page. At the top, the 'Sync Type' is set to 'AzureActiveDirectory' and is enabled. Below this, there are two main sections for configuring messages:

- 23:** A toggle for 'Send Welcome Messages'.
- 24:** A toggle for 'Use custom message'.
- 25:** Two buttons for 'Welcome Message' and 'Welcome Back Message'.

A 'Verify Setup' dialog box is open, showing the following options:

- 26:** A toggle for 'Defer sending of welcome message'.
- 26:** A dropdown for 'Welcome message' set to 'Hours'.
- 26:** A dropdown for 'How many hours?' set to '1'.
- 27:** A 'Send Test' button.

The dialog also shows a rich text editor for customizing the message content, with a 'Save Draft' button and 'Cancel'/'Publish' options at the bottom.

Welcome Message: Email sent to new users added to the platform

Welcome Back Message: Email sent to reactivated users

22. You can configure how these welcome messages are sent to users during the sync.
 23. **“Send Welcome Messages”** will send the welcome message to newly added employees during the sync.

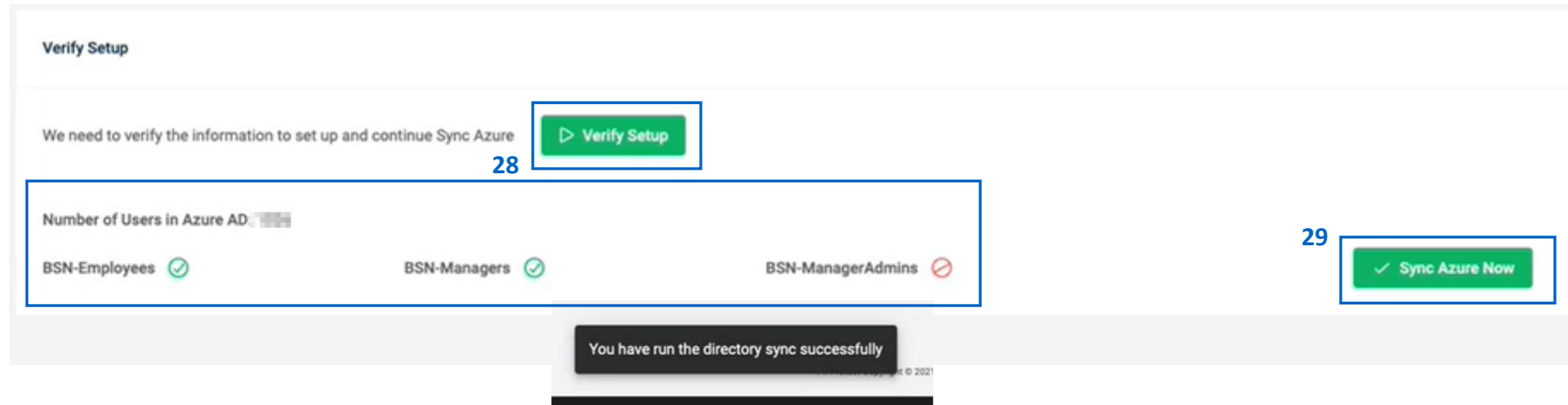
24. **“Use Custom Message”** will enable welcome messages to be customized. Without this option checked, the standard messages will be sent based off the Global Messages in the Partner Profile.
 25. Clicking **“Welcome Message”** or **“Welcome Back Message”** will allow you to adjust the message.

26. Messages can be deferred for a period of hours or days.
 27. The text within the message can be adjusted and a test message can be sent to preview.

Azure Active Directory Sync – Simple Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal – Simple Setup



28. After you've set up your Message configurations, click the “**Verify Setup**” button – this will return the number of users within the Azure tenant and will confirm the sync groups used within the tenant

29. When you are ready, click the “**Sync Azure Now**” button. You will receive a confirmation at the bottom of the page that the sync has been run successfully!

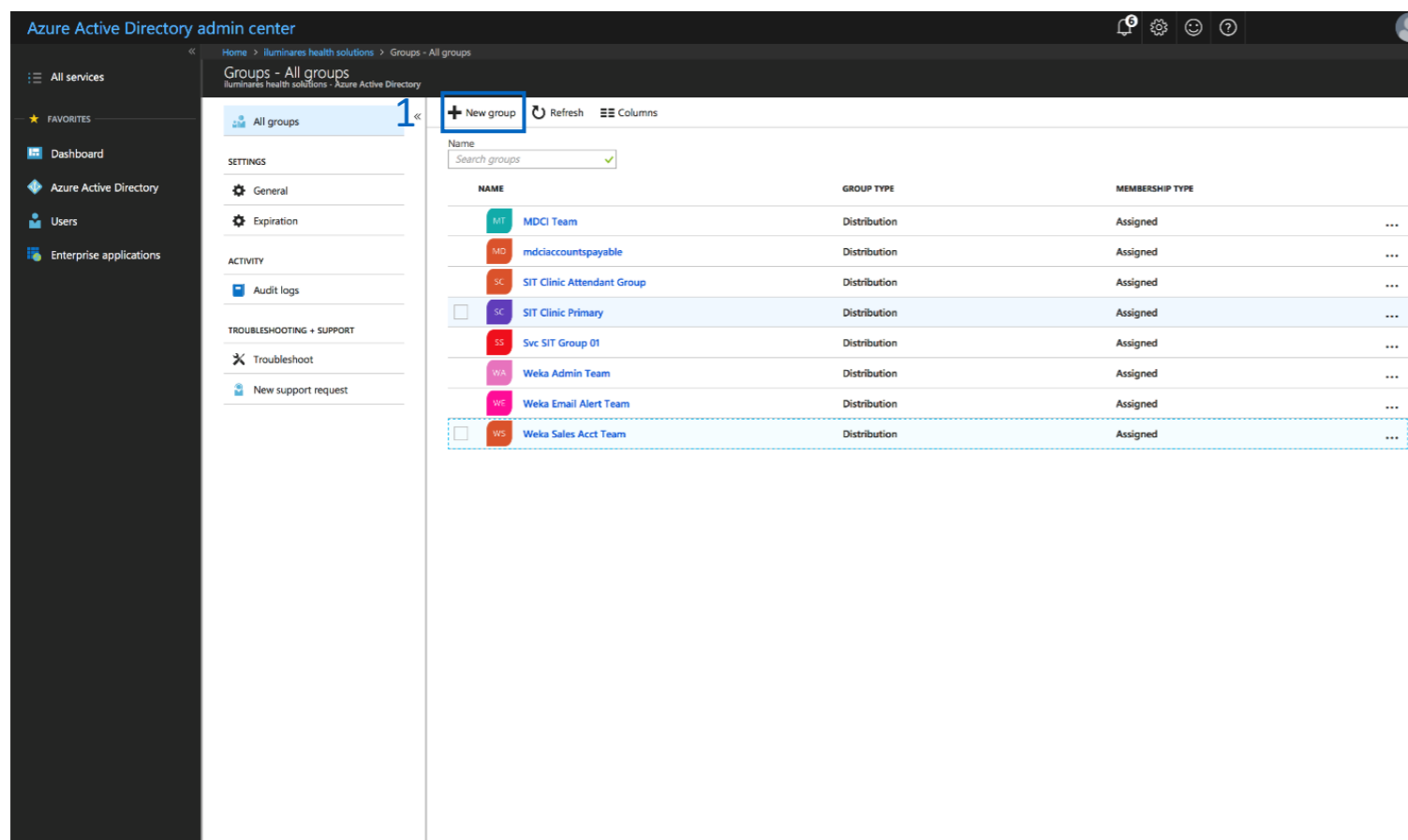
You're all set!

- Depending on the user count within the tenant, the users should begin appearing within the User tab within the portal in **less than 5 minutes!**
- If your sync is in progress, you can't queue up multiple syncs. Please wait 15 minutes then retry if no users appear

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



Important: If Azure AD Sync is enabled and these groups are NOT defined after the initial synchronization, there is a risk of users becoming deactivated in the portal and the users will be notified.

1. Create Azure AD Sync Security Groups to define the portal access for each employee. **The following two groups MUST be created:**

BSN-Employees: Defines the users that will be enrolled in the portal as standard employees under that client.

BSN-Managers: Defines users in the manager role, supersedes BSN-Employees.

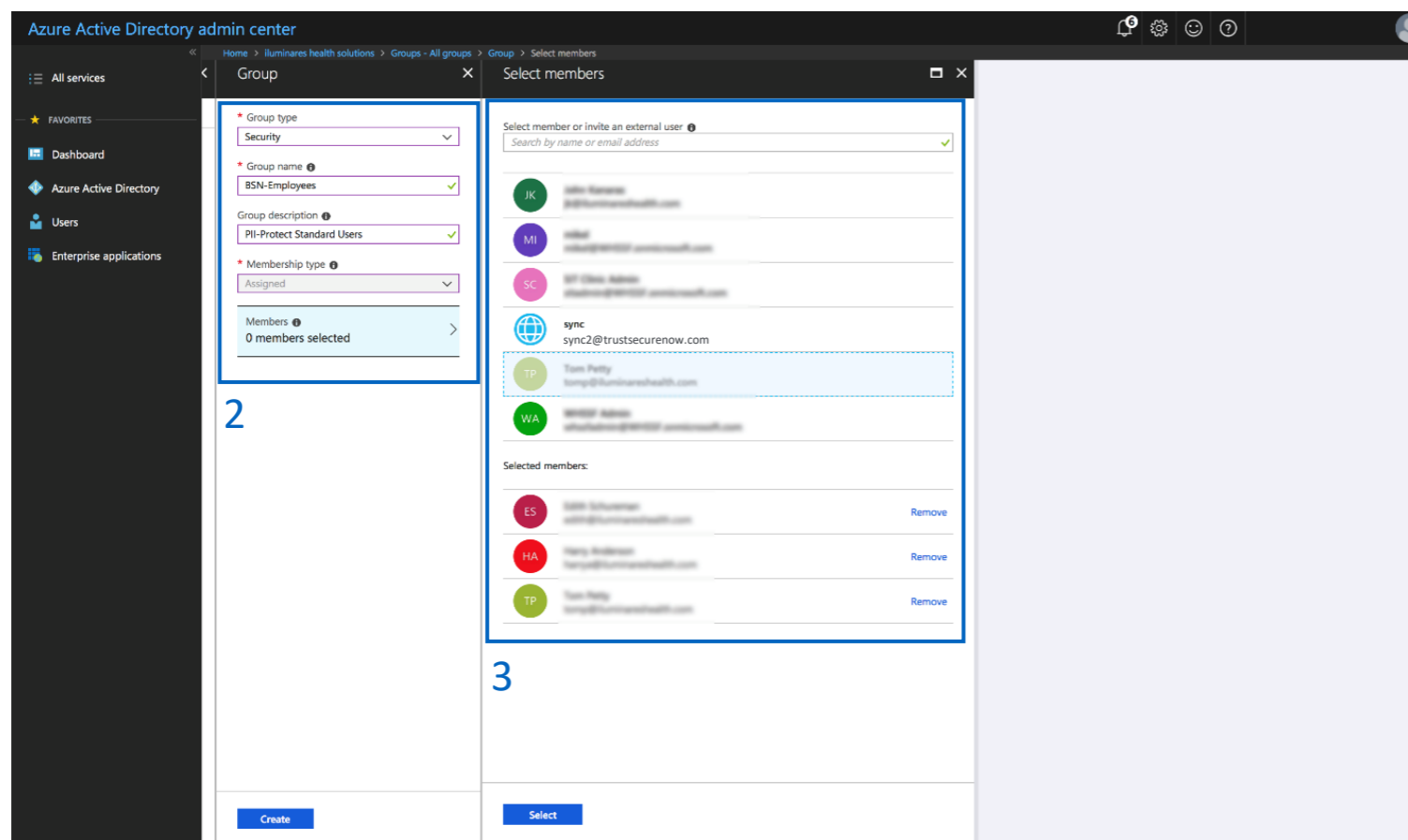
- Managers get access to reporting and employee data inside the PII/PHI Protect portal.

Note: When entering the above security groups, spaces are NOT permitted before, after, or within the string.

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



2. Create the **BSN-Employees** group with the following parameters:

Group Type: Security

Group Name: BSN-Employees

Group Description: PII/PHI Protect Standard Users

3. Assign users to the group.

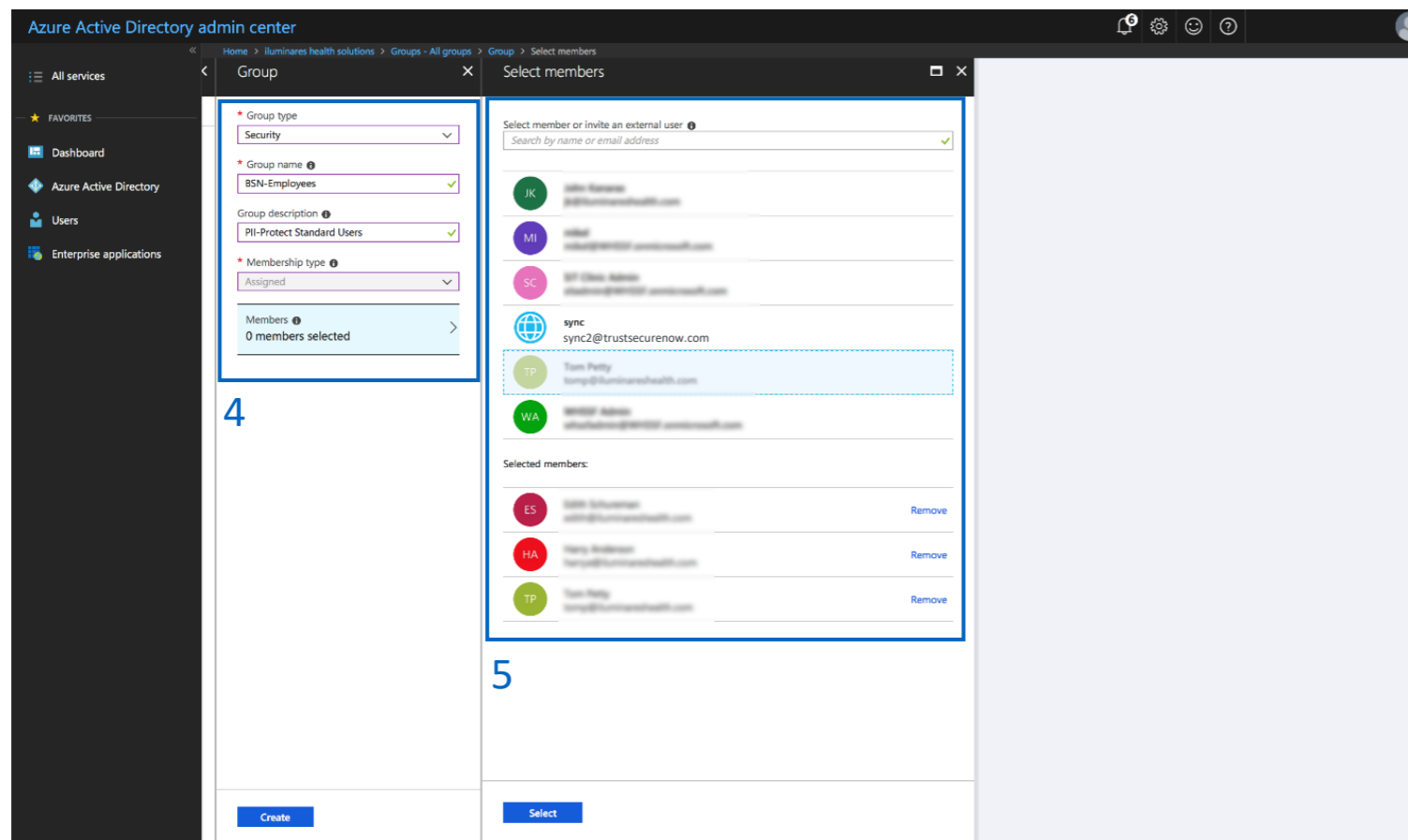
Note: Be sure not to assign non-user accounts to this group as portal accounts WILL be created for all users assigned to this group. If you assign users to this group and to the BSN-Manager group, the manager role will take precedence.

Important: For those using On-Premise along with Azure Sync to synchronize with the free tier or Azure AD: Nested group memberships are not supported for group-based assignment at this time.

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



Optional Group: Add the **BSN-ManagerAdmins** group to give select managers the ability to manage phishing campaigns as well as the bulk manage user functionality. Standard manager accounts do NOT have this functionality. Follow steps 2 - 3 using **Group Name:** BSN-ManagerAdmins and **Group Description:** PII/PHI Protect Manager Admin Role

4. Create the **BSN-Managers** group with the following parameters:

Group Type: Security

Group Name: BSN-Managers

Group Description: PII/PHI Protect Manager Role

5. Assign users to the group. All managers will also have an employee account.

Optional Group: BSN-PartnerAdmins

Group Type: Security

Group Name: BSN-PartnerAdmins

Group Description: PII/PHI Protect Partner Administrator Role

- This user has the **highest** level of access and will have all administrative functions for all accounts within your portal. **This group is to ONLY be used for your company's internal Breach Prevention Platform (BPP) account**

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center

The screenshot shows the Azure Active Directory admin center interface. On the left, there is a navigation pane with 'All services', 'FAVORITES', 'Azure Active Directory', 'Users', and 'Enterprise applications'. The main area is divided into two panels. The left panel, titled 'New Group', contains fields for 'Group type' (Security), 'Group name' (BSN-TAG-Executive Team), 'Group description' (Executive Team Tag for BSN), and 'Membership type' (Assigned). Below these are 'Owners' and 'Members' sections. A blue box highlights this entire panel, with the number '6' below it. The right panel, titled 'Add members', has a search bar and a list of users. A blue box highlights this panel, with the number '7' below it. At the bottom of the 'New Group' panel, a 'Create' button is highlighted with a blue box, with the number '8' below it.

6. **Optional:** Create Tag Groups. Tags are used for creating specific groups, typically to separate users by department, to create groups you'd like to send specific phishing emails to, or to simplify tracking in the portal.

Group Type: Security

Group Name: BSN-TAG-**tagname**

*tagname will be the tag you want the users associated with.

Example: BSN-TAG-Executive Team, BSN-TAG-Finance, etc.

Group Description: Optional field if you would like to add details on the tag you created.

7. Assign users to the group.

8. Click "**Create**".

Important: For those using On-Premise along with Azure Sync to synchronize with the free tier or Azure AD: Nested group memberships are not supported for group-based assignment at this time.

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options like Dashboard, Azure Active Directory, Users, and Enterprise applications. The main content area displays the 'Properties' tab for an Azure AD instance named 'iluminare health solutions'. The 'Directory ID' field is highlighted with a blue box and labeled '9'. The 'Properties' tab in the left sidebar is also highlighted with a blue box and labeled '10'.

Sharing the Directory ID

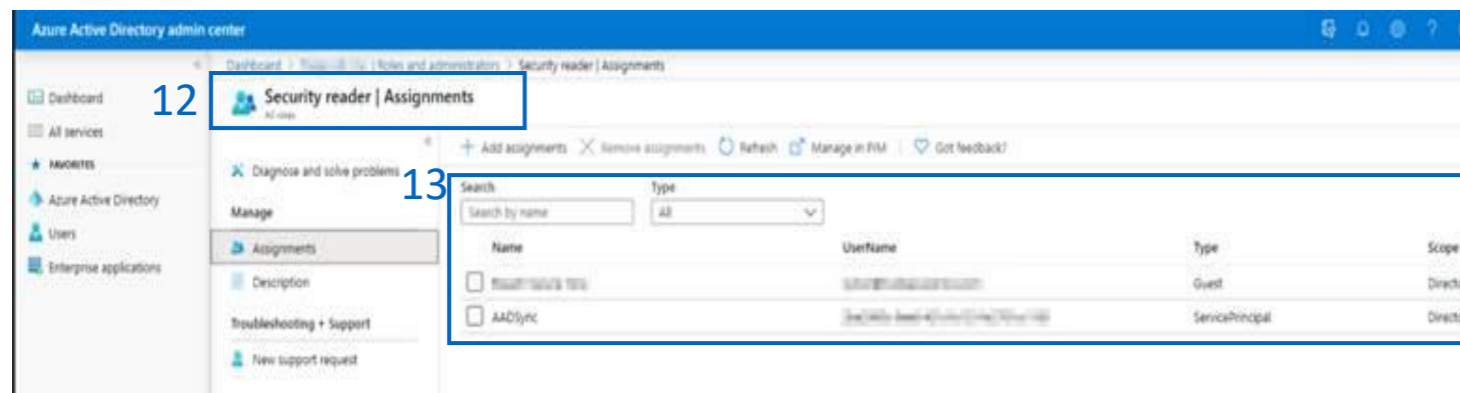
9. Select the “**Properties**” tab.
10. Locate the “**Directory ID**” field and press the Copy button – The Directory ID information will identify this Azure Active Directory to the AAD Sync process. This value will be important in step 25 on [page 23](#).

Important: Confirm that the email addresses of any current users in the portal (userID) are the same as their email address (userID) in Azure AD or else duplicate users will be created.

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Microsoft 365 Admin Center



Assigning the Security Reader Role

11. Navigate to Roles
12. Search for the Security Reader Role and click on Assignments
13. Assign the role to a user that has global admin privileges

Important: The Security Reader Role must be assigned to at least one user otherwise step 31 will produce errors

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal

14. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in select “Manage Clients” to access your client list and select the client you want to sync with Azure Active Directory.

15. Select the “**Directory Sync**” tab

16. Use the Sync Type drop-down selector to select “Azure Active Directory”

17. Click the “**Enable Manual Setup**” button then click the “**Enable**” button

18. Click the “**Create Powershell**” button

The image contains three screenshots of the PII Protect portal interface, illustrating the configuration steps for Azure Active Directory Sync:

- Top Screenshot:** Shows the 'Directory Sync' tab selected in the navigation menu. A dropdown menu is open, showing options: 'Please Select', 'CSV Bulk Upload', 'Azure Active Directory' (highlighted with a blue box and labeled '16'), 'On Premise Active Directory', and 'Google G-Suite'. Below the dropdown is an 'Enable' toggle switch (labeled '15') and a green 'Authorize Directory Access' button.
- Middle Screenshot:** Shows the 'Sync Type' dropdown set to 'AzureActiveDirectory' (labeled '16'). Below it is an 'Enable Manual Setup' button (labeled '17') and an 'Enable' toggle switch (labeled '17').
- Bottom Screenshot:** Shows the 'Sync Type' dropdown set to 'AzureActiveDirectory' (labeled '16'). Below it is a 'Disable Manual Setup' button and an 'Enable' toggle switch (labeled '18'). A green 'Create Powershell' button is highlighted with a blue box and labeled '18'.

Important: These instructions are for Classic Azure setup. For Simple Setup, navigate to page 6.

Azure Active Directory Sync – Classic Setup

Setup Application Authentication with Azure AD on the client Azure AD Sync Settings Page. You will be required to run a Powershell Script and access Azure AD for the client you'll be configuring Application Authentication for.

Configure Messaging & Notification - Azure AD Sync Settings Page

The screenshot displays the 'Configure Messaging & Notification' section of the Azure AD Sync Settings Page. Key elements include:

- 20:** A toggle switch labeled 'Send automated welcome' which is currently turned on.
- 21:** A toggle switch labeled 'Customize welcome message' which is currently turned off.
- 22:** Two buttons: 'Welcome Message' and 'Welcome Back Message'.
- 23:** A toggle switch labeled 'Defer sending of welcome message' which is currently turned on, with a dropdown menu set to 'Hours' and a value of '1'.
- 24:** A rich text editor for customizing the welcome message content, showing a sample message about a cybersecurity awareness program.

Welcome Message: Email sent to new users added to the platform

Welcome Back Message: Email sent to reactivated users

19. You can configure how these welcome messages are sent to users during the sync.

20. **“Send automated welcome”** will send the welcome message to newly added employees during the sync.

21. **“Customize welcome message”** will enable welcome messages to be customized. Without this option checked, the standard messages will be sent based off the Global Messages in the Partner Profile.

22. Clicking **“Welcome Message”** or **“Welcome Back Message”** will allow you to adjust the message.

23. Messages can be deferred for a period of hours or days.

24. The text within the message can be adjusted and a test message can be sent to preview.

Azure Active Directory Sync – Classic Setup

Our Azure Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuring Application Authentication - Azure AD Sync Settings Page

The screenshot displays the 'Configuring Application Authentication - Azure AD Sync Settings Page'. At the top, there is a 'Sync Type' dropdown menu set to 'Azure Active Directory' and an 'Enable' toggle switch that is turned on. Below this, there is a 'Powershell - Download and execute powershell script' section with a 'Download' button. The main configuration area includes several toggle switches: 'Send automated welcome' (on), 'Customize welcome message' (off), and two buttons for 'Welcome Message' and 'Welcome Back Message'. There are three text input fields: 'Azure AD Identifier' (highlighted with a blue box and labeled '25'), 'Enter application ID', and 'Enter certificate thumbprint'. Below these is a 'Use as Portal Logon' dropdown menu (highlighted with a blue box and labeled '26'). At the bottom, there is an 'Upload certificate' section with an 'Attachment' box for dragging and dropping files or browsing, and a note that only .pfx files will be accepted. A green 'Save' button is located at the bottom right of the form.

25. Paste the Azure Directory ID into the text box under “**Azure AD Identifier**”.

Note: Copy and paste the AAD Identifier (Directory ID) to mitigate translation error. Refer to [page 19](#) to find your directory ID.

26. Click the “**Use as Portal Logon**” dropdown to choose between Email and UserPrincipalName as the user logon Username. **We highly recommend “Email”**

Important: Once Azure Active Directory is activated; you will not be able to add users to the portal outside of this method. Our portal will sync once every hour, which may cause a delay for your users to be updated.

Azure Active Directory Sync – Classic Setup

Setup Application Authentication with Azure AD on the client Azure AD Sync Settings Page. You will be required to run a Powershell Script and access Azure AD for the client you'll be configuring Application Authentication for.

Configuring Application Authentication - Azure AD Sync Settings Page

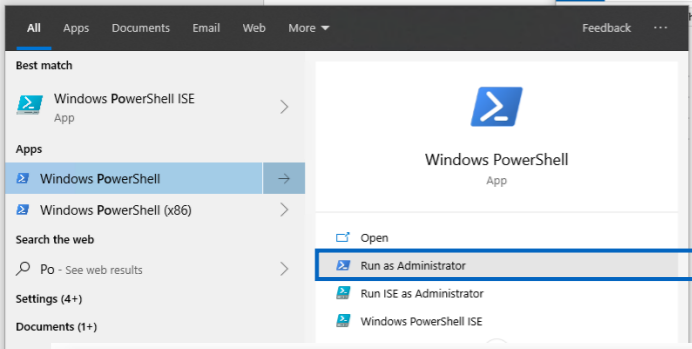
The screenshot shows the Azure AD Sync Settings Page. The 'Sync Type' is set to 'Azure Active Directory' and is enabled. The 'Powershell - Download and execute powershell script' section has a 'Download' button highlighted with a red box and the number 27. Below this, there are fields for 'Azure AD Identifier', 'Enter application ID', and 'Enter certificate thumbprint'. There are also buttons for 'Welcome Message' and 'Welcome Back Message'. The 'Upload certificate' section has an 'Attachment' field. Below the settings page, a File Explorer window shows the 'Downloads' folder with a file named 'AADSync' (3 KB) downloaded on 1/27/2020 at 10:12 AM. The file path is 'This PC > Local Disk (C:) > Users > alanl > Downloads > AADSync'.

27. Click “**Download**” to download the powershell script
28. Click “**Show in Folder**” to open your File Explorer and note the file path.

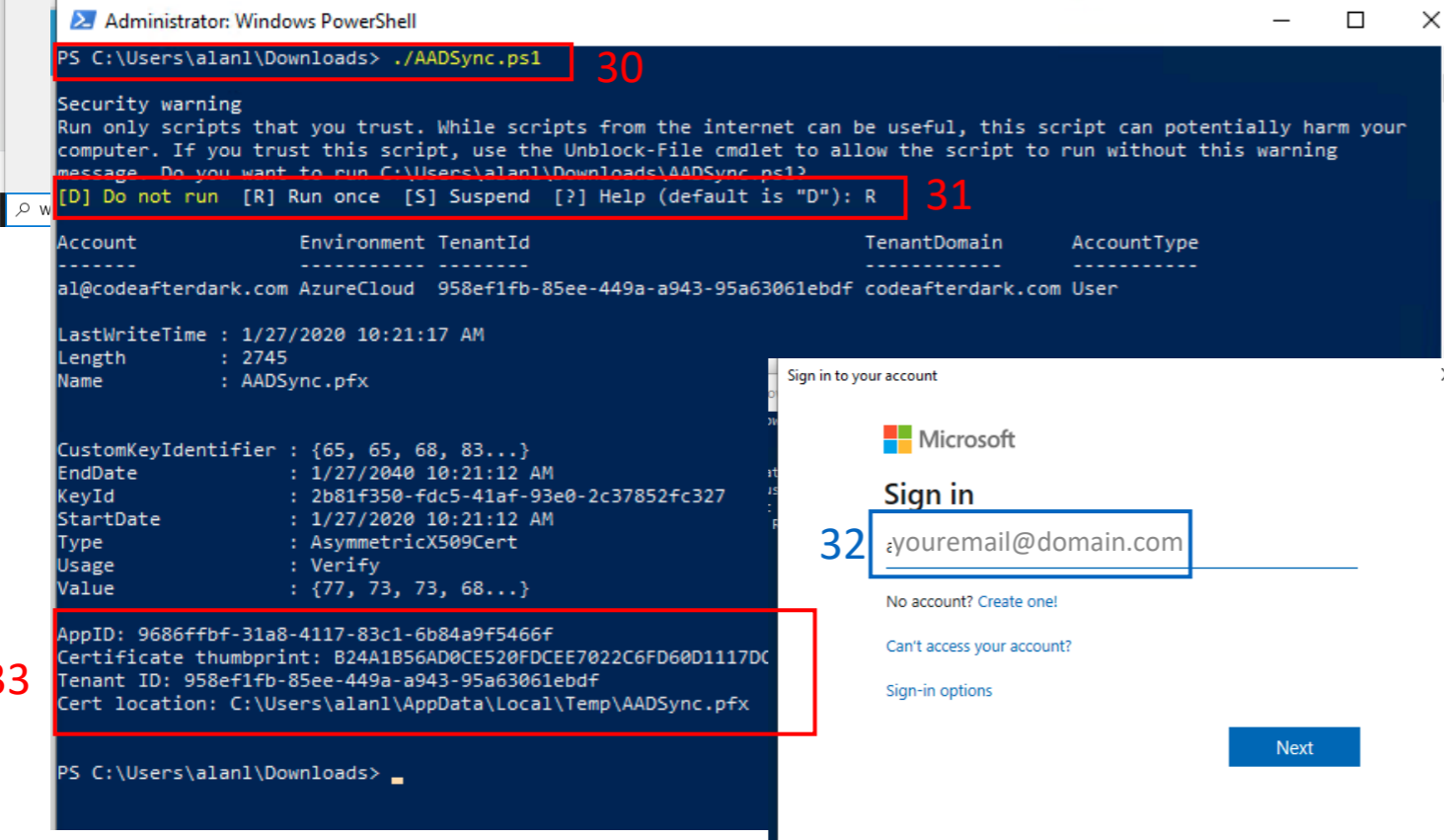
Azure Active Directory Sync – Classic Setup

Setup Application Authentication with Azure AD on the client Azure AD Sync Settings Page. You will be required to run a Powershell Script and access Azure AD for the client you'll be configuring Application Authentication for.

Configuring Application Authentication – in Windows Powershell



29



30

31

32

33

```

PS C:\Users\alan1\Downloads> ./AADSync.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\alan1\Downloads\AADSync.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R

Account      Environment TenantId      TenantDomain      AccountType
-----
al@codeafterdark.com AzureCloud  958ef1fb-85ee-449a-a943-95a63061ebdf codeafterdark.com User

LastWriteTime : 1/27/2020 10:21:17 AM
Length        : 2745
Name          : AADSync.pfx

CustomKeyIdentifier : {65, 65, 68, 83...}
EndDate           : 1/27/2040 10:21:12 AM
KeyId             : 2b81f350-fdc5-41af-93e0-2c37852fc327
StartDate         : 1/27/2020 10:21:12 AM
Type              : AsymmetricX509Cert
Usage             : Verify
Value             : {77, 73, 73, 68...}

AppID: 9686ffbf-31a8-4117-83c1-6b84a9f5466f
Certificate thumbprint: B24A1B56AD0CE520FDCEE7022C6FD60D1117DC
Tenant ID: 958ef1fb-85ee-449a-a943-95a63061ebdf
Cert location: C:\Users\alan1\AppData\Local\Temp\AADSync.pfx

PS C:\Users\alan1\Downloads>
  
```

29. Run Windows Powershell as an Administrator
30. Navigate to the directory where the script is located as noted in step 28.
31. Install **AzureAD Module** and set execution policy to unrestricted. Then, execute the AADSync.ps1 Powershell script. Enter "R" to **Run once**
32. You will be prompted to sign into the Azure Account you are configuring Application Authentication for.
33. Note the information displayed when the script has completed running: AppID, Certificate thumbprint, and Cert location.

Azure Active Directory Sync – Classic Setup

Setup Application Authentication with Azure AD on the client Azure AD Sync Settings Page. You will be required to run a Powershell Script and access Azure AD for the client you'll be configuring Application Authentication for.

Configuring Application Authentication – Client Azure AD Sync Settings Page

The screenshot displays the 'Azure AD Sync Settings' page. At the top, 'Sync Type' is set to 'Azure Active Directory' and is enabled. Below this, there are options for 'Send automated welcome' (enabled) and 'Customize welcome message' (disabled). A 'Download' button is visible. The main configuration area includes fields for 'Azure AD Identifier', 'Enter application ID', and 'Enter certificate thumbprint', all of which are highlighted with a blue box and labeled '31'. Below these fields is an 'Upload certificate' section, also highlighted with a blue box and labeled '32', which contains an 'Attachment' button and a 'Browse' option. A file explorer window is open over the 'Browse' option, showing a list of files in the 'C:\Users\alan\AppData\Local\Temp' directory. The file 'AADSync.pfx' is selected, and its path is entered in the 'File name' field, which is also highlighted with a blue box and labeled '32'. A 'Save' button is highlighted with a blue box and labeled '33'.

34. Copy the Application ID and Certificate Thumbprint from the script and paste them into the “**Enter Application ID**” and “**Enter Certificate Thumbprint**” fields, respectively.

35. Click “**Attachment**” under the Upload Certificate section and paste the Certificate location file path in the “File Name” field in the file explorer and click “**Open**”

36. Click “**Save**” to save your changes. Repeat steps 1-36 for each client!

Congratulations! Your client has been set up with Azure AD Sync!

Important: Once Azure Active Directory is activated; you will not be able to add users to the portal outside of this method. Our portal will sync once every hour, which may cause a delay for your users to be updated.

Note: The initial sync may take between 3 to 5 hours before users appear in your portal. After the initial sync, updates are processed hourly.

On-Premise Active Directory Sync Setup

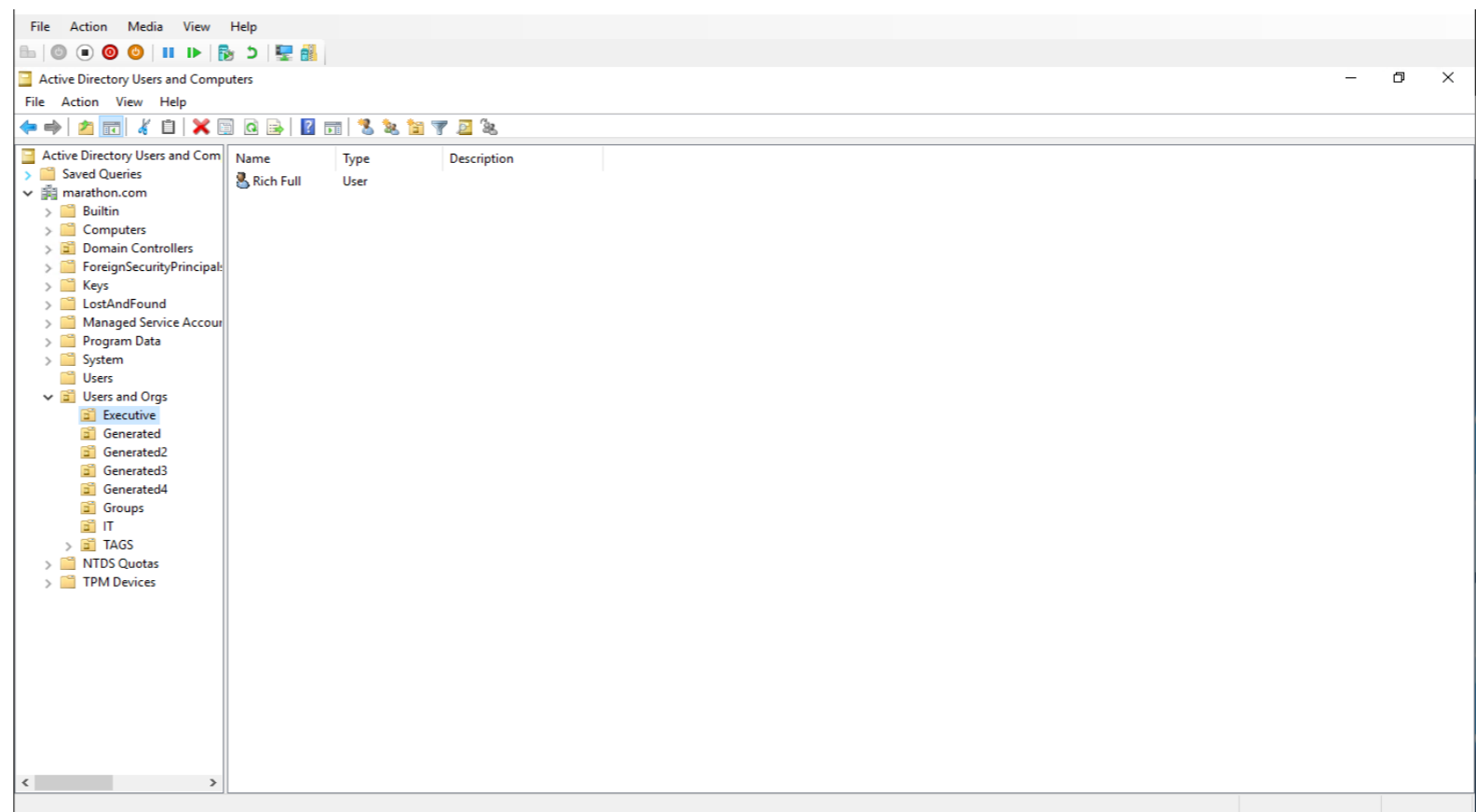
Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Setup in Active Directory Users and Computers Application

Our On-Premise Active Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Note: Any previous setups using Rocket Cyber will continue to sync and the tool can still be utilized for future syncs. For more information on the Rocket Cyber On-Premise sync options, please contact: opscore@breachsecurenow.com

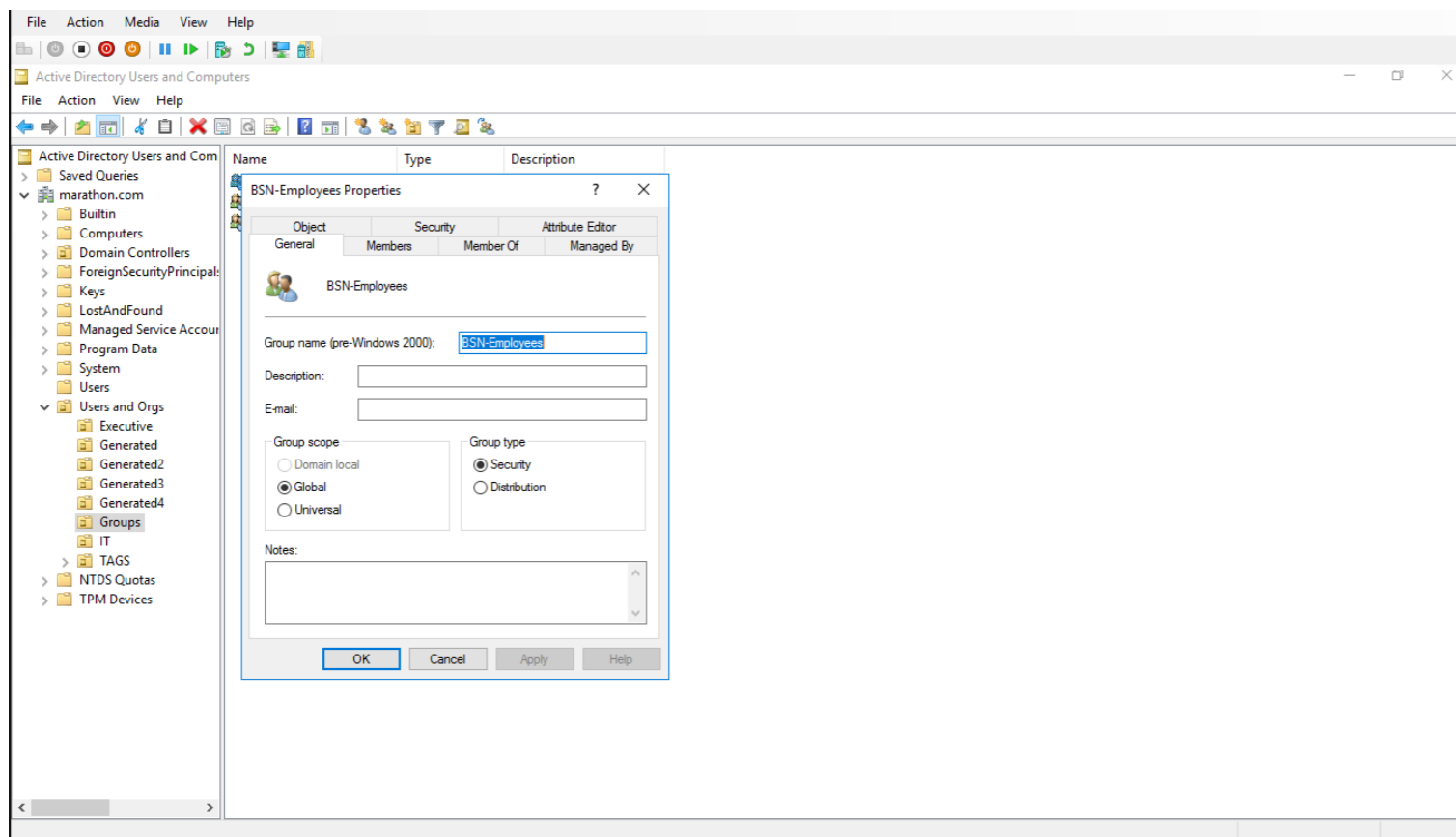
1. Open the Active Directory Users and Computers application



On-Premise Active Directory Sync Setup

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Setup in Active Directory Users and Computers Application



- Under the “Users and Orgs” folder, right-click the “Groups” folder and click New → Group to create the **BSN-Employees** group with the following parameters:

Group Type: Security

Group Name: BSN-Employees

Group Description: PII/PHI Protect Standard Users

- Add users that should have standard employee access to the PII/PHI Protect Portal

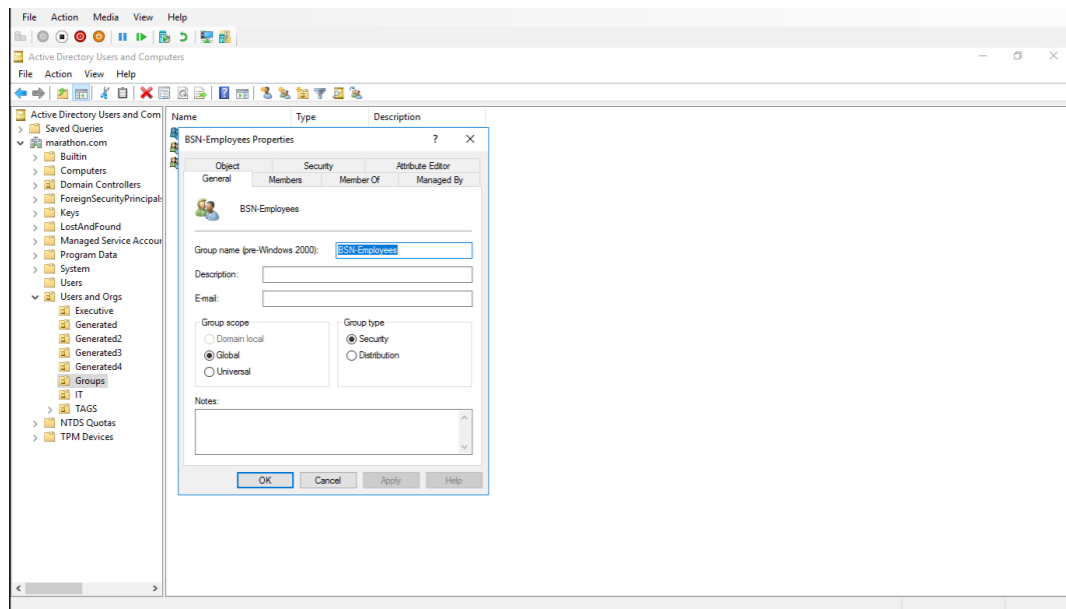
Note: Be sure not to assign non-user accounts to this group as portal accounts WILL be created for all users assigned to this group. If you assign users to this group and to the BSN-Manager group, the manager role will take precedence.

Important: Nested groups are not supported. This means you cannot have a standard group for all employees and then include the employees’ group in the BSN-Employees group. Each user must be placed individually within each of the BSN groups.

On-Premise Active Directory Sync Setup

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Setup in Active Directory Users and Computers Application



Important: When entering the above security groups, spaces are NOT permitted before, after, or within the string. The highest access level group will take precedence. For example, a user in the BSN-Managers group do not need to be added to the BSN-Employees group.

4. Create the following **optional** groups with the same parameters:

BSN-Managers – For client manager access

Group Description: PII/PHI Protect Manager Role

- Only assign users to this group that should have manager access and view employee progress.

BSN-ManagerAdmins – For client administrator-level access

Group Description: PII/PHI Protect Manager Admin role

- Only assign users to this group that should have manager access, view employee progress, manage phishing campaigns, and bulk upload users. Standard manager accounts **do not** have this functionality.

BSN-PartnerAdmins – for your internal MSP account only

Group Description: PII/PHI Protect Partner Administrator Role

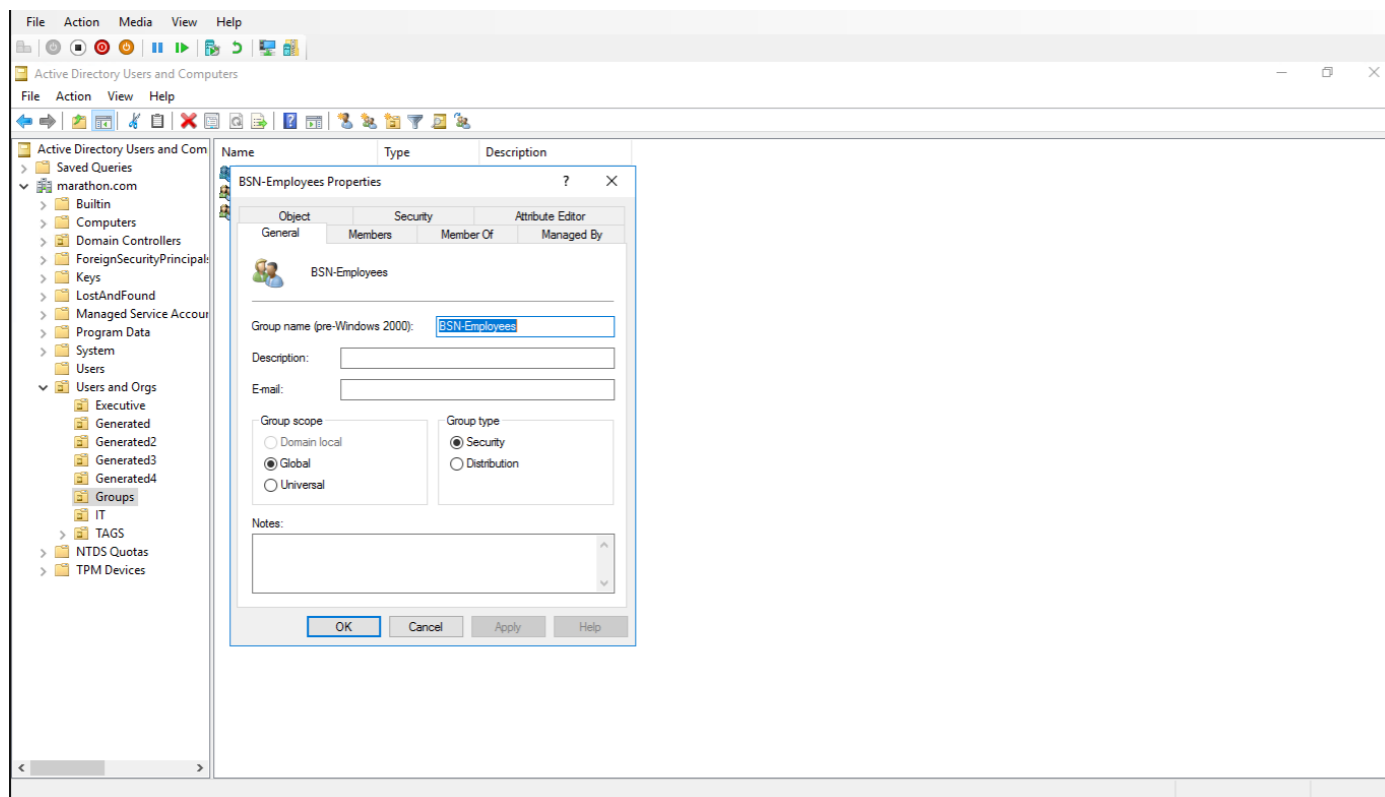
- This user has the **highest** level of access and will have all administrative functions for **all accounts** within your portal.

This group is to ONLY be used for your company's internal Breach Prevention Platform (BPP) Account

On-Premise Active Directory Sync Setup

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Setup in Active Directory Users and Computers Application



Note: Use tags to track metrics for specific departments and sent targeted phishing campaigns.

5. **Optional:** Create Tag Groups.

Tags are used for creating specific groups, typically to separate users by department, to create groups you'd like to send specific phishing emails to, or to simplify tracking in the portal.

Group Type: Security

Group Name: BSN-TAG-**tagname**

*tagname will be the tag you want the users associated with.

Example: BSN-TAG-Executive Team, BSN-TAG-Finance, etc.

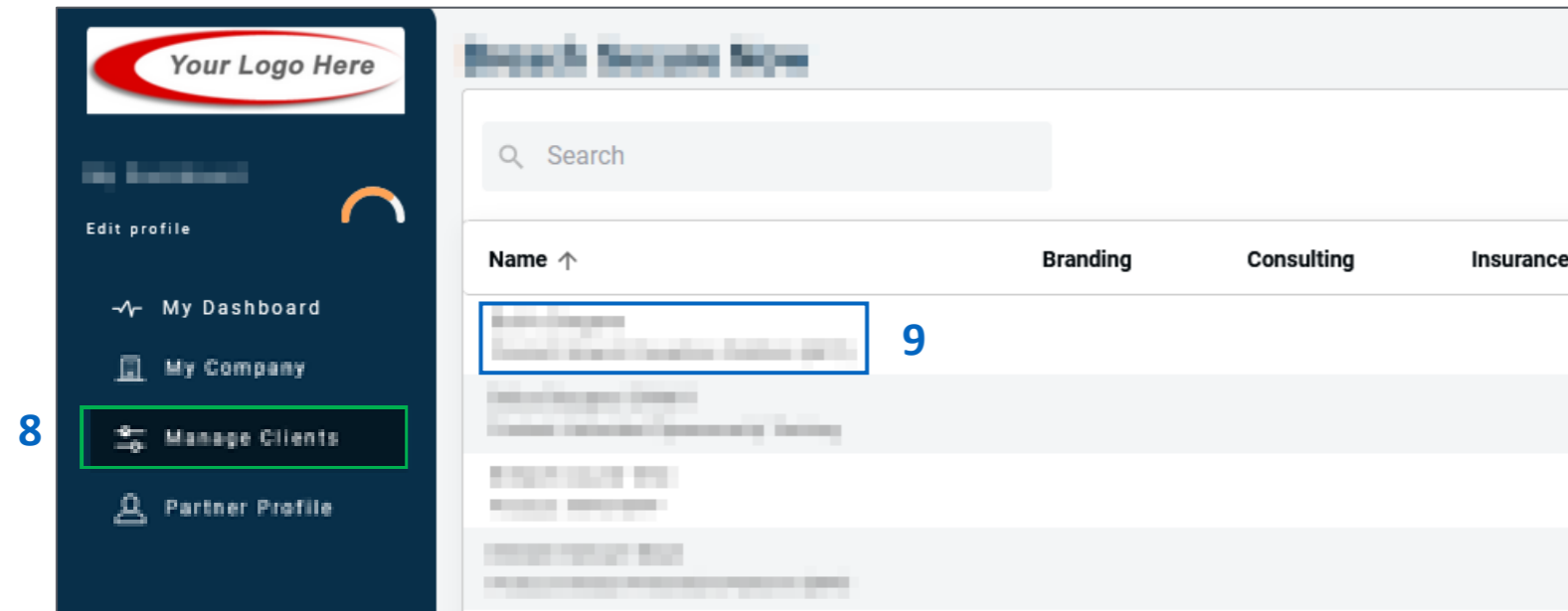
Group Description: Optional field if you would like to add details on the tag you created.

6. Assign users to the group. Note: Users must already be in one of the BSN-Employees, Managers, or PartnerAdmins groups.

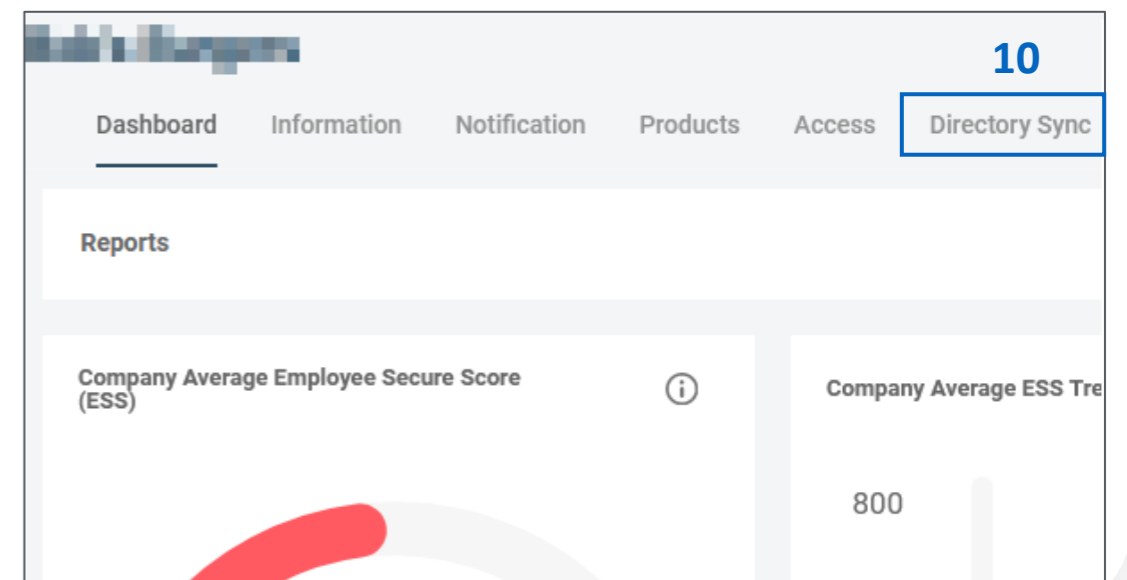
Configurations within the PII Protect Portal

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Navigating to the Directory Sync tab



7. Log in as a Partner Administrator to the PII-Protect portal [here](#).
8. Select the **"Manage Clients"** app.
9. Select the account you are setting up OnPrem AD sync on.
10. Select the **"Directory Sync"** tab.



Configurations within the PII Protect Portal

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Enabling the sync

11. Under the Sync Type, select **"On Premise Active Directory"** from the Sync Type dropdown.
12. Enable the sync.
13. Copy the **"Agent Client ID"** and paste it somewhere for reference (i.e. Notepad).
14. Note your selection for **"use as portal login"** (email or UPN).
15. Select the **"Save"** button on the right.

Note: If you do not save, the Client ID will not be held, which prevents the OnPrem agent from connecting.

The screenshot displays the 'Directory Sync' configuration page. At the top, there is a navigation bar with tabs for Information, Notification, Products, Access, Directory Sync (selected), Users, Dark Web, Training Reports, Phishing, and Employee Assessments. The main content area includes:

- 11:** A dropdown menu for 'Sync Type' with 'OnPremiseActiveDirectory' selected.
- 12:** An 'Enable' toggle switch that is turned on.
- 13:** A text input field for 'Agent Client ID' containing a long alphanumeric string.
- 14:** A dropdown menu for 'Use as Portal Logon' with 'Email' selected.
- 15:** A green 'Save' button with a checkmark.

Other visible elements include 'Send Welcome Messages' (enabled), 'Use custom message' (disabled), and buttons for 'Welcome Message' and 'Welcome Back Message'. A link to 'Click here to download Directory Sync Agent' is also present.

Configurations within the PII Protect Portal

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Configuring Messaging & Notification – On-Premise AD Sync Settings Page

The screenshot displays the 'Directory Sync' settings page. On the left, a sidebar shows the user 'Wendy Smallfoot' and navigation options like 'My Dashboard', 'My Company', 'Manage Clients', and 'Partner Profile'. The main content area includes a 'Sync Type' dropdown set to 'On Premise Active Directory' (17), an 'Enable' toggle (18), and buttons for 'Send automated welcome' (17), 'Customize welcome message' (18), 'Welcome Message' (19), and 'Welcome Back Message' (19). A 'Customize message' dialog is open, featuring a 'Defer sending of welcome message' toggle (20) and a 'How many hours?' dropdown set to '1'. Below this are two rich text editors for 'Before link text' (21) and 'After link text', both containing sample security awareness messages. At the bottom, there are 'Save Draft', 'Cancel', and 'Publish' buttons.

Welcome Message: Email sent to new users added to the platform

Welcome Back Message: Email sent to reactivated users

16. Before downloading the agent, consider configuring how Welcome messages are sent to users during the sync.

17. “**Send automated welcome**” will send the welcome message to newly added employees during the sync.

18. “**Customize welcome message**” will enable welcome messages to be customized. Without this option checked, the standard messages will be sent based off the Global Messages in the Partner Profile.

19. Clicking “**Welcome Message**” or “**Welcome Back Message**” will allow you to adjust the message.

20. Messages can be deferred for a period of hours or days.

21. The text within the message can be adjusted and a test message can be sent to preview.

Downloading the On-Premise Directory Sync Agent

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Downloading and installing

22. Click the link **“Click here to download Directory Sync Agent”** to download the OnPrem AD sync installation file.
23. Run the installation file.
24. Paste the Client ID into the AD agent install window.
25. Select **“Install Now”**

Note: OnPrem Agent can only be installed on Windows Server 2016 or higher.

Note: When adding a new user to the groups:

- a. Make sure the email field is filled out for users under properties (automatically applied if connected to exchange server.)
- b. Add to a BSN security group.

The image shows two screenshots from a web application. The top screenshot is the configuration page for the On-Premise Active Directory Sync Agent. It features a dropdown menu for 'Sync Type' set to 'OnPremiseActiveDirectory', an 'Enable' toggle switch, and options for 'Send Welcome Messages' and 'Use custom message'. There are buttons for 'Welcome Message' and 'Welcome Back Message'. Below these are fields for 'Agent Client ID' (containing a masked ID) and 'Use as Portal Logon' (set to 'User Principal Name'). A blue box highlights a link 'Click here to download Directory Sync Agent' next to the number '22'. A green 'Save' button is at the bottom right.

The bottom screenshot is the 'AD Agent Install' dialog box. It contains the text: 'To install the Active Directory Agent you need to enter the ID provided you when you downloaded the installer.' Below this is a 'ClientId:' label and an empty text input field, with the number '24' next to it. At the bottom, there is a large blue button with a checkmark icon and the text 'Install Now', with the number '25' next to it. A 'Cancel' button is located below the 'Install Now' button.

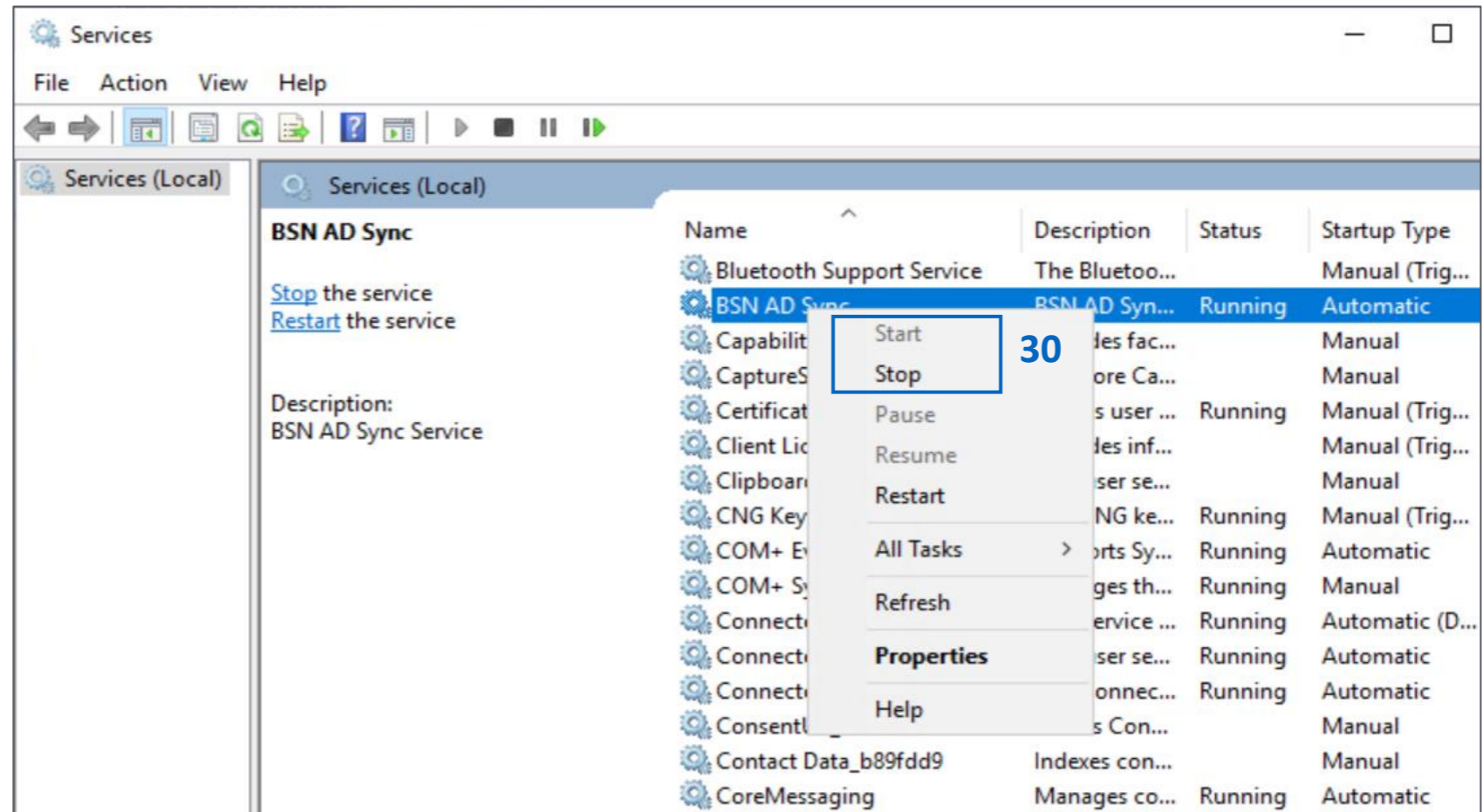
Downloading the On-Premise Directory Sync Agent

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Forced Sync

Congratulations! Your client's Active Directory is now syncing with the PII/PHI Protect Portal!

Note: The sync frequency is every 2 hours, but to sync right away, you need to start and stop the service.



26. Navigate to the **"Server Manager."**

27. Select **"Tools"** on the top right.

28. Select **"Services."**

29. Locate **"BSN ADSync"**

30. Right-click on the application and select **"Stop"** and then right-click and select **"Start."**

31. Refresh the PII-Protect portal and the user will be on the user list.

Additional Information for On-Premise Directory Sync

Simply configure your settings inside the Active Directory application, install our home-grown Active Directory Sync Agent, and setup in the Breach Secure Now portal to easily manage your user access for all your On-Premise AD clients.

Noteworthy information

- If the user is deleted in PII-Protect, and not deleted on the agent, they will be readded.
- If the user is added in the PII-Protect portal with an email that is not on the directory, they will not be impacted and can be managed in the portal.
- If a user with the same email address is added in PII-Protect, it will link the two accounts and merge them. No duplicate will be created.
- It is recommended to preform all directory management from the agent side.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

The screenshot shows the 'New Project' page in the Google Cloud Console. The browser address bar is console.developers.google.com. The page title is 'New Project'. The 'Project name' field is highlighted with a blue box and labeled '1', containing the text 'GSuiteSecureNowIntegration'. Below it, the 'Organization' dropdown is set to 'say-thx.net'. The 'Location' dropdown is also set to 'say-thx.net'. At the bottom, the 'CREATE' button is highlighted with a blue box and labeled '2'.

Create a new project to be used for the Breach Secure Now integration

1. Navigate to the following page: <https://console.developers.google.com/projectcreate> and sign into your account with your Admin credentials. If required, agree to the Terms and Services.
2. Type a unique name into the “**Project Name**” box, we suggest using: **GSuiteSecureNowIntegration**
3. Click the “**Create**” button to create the project.

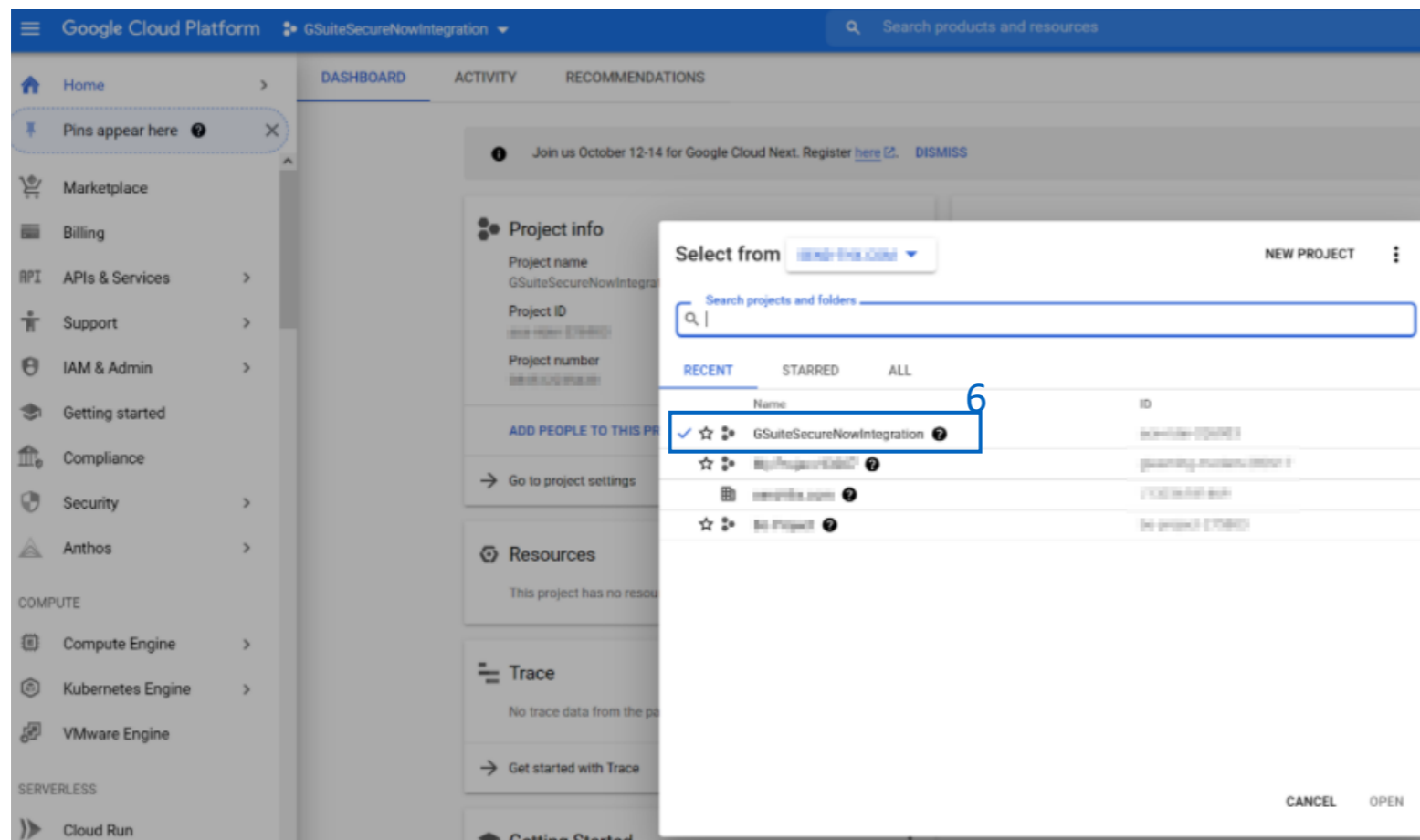
G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

Create a service account to be used for this project

5. Navigate to the following page:
<https://console.cloud.google.com/projectselector2/iam-admin/serviceaccounts?supportedpurview=project>
6. Select the name of the project you just created: **GSuiteSecureNowIntegration**



G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

The screenshot shows the Google Cloud Platform console interface for creating a service account. The sidebar on the left is expanded to 'IAM & Admin', and 'Service Accounts' is selected. The main panel displays the 'Create service account' wizard. The 'Service account details' section includes fields for 'Service account name' (securenowsync), 'Service account ID' (securenowsync), and 'Service account description'. The 'Grant this service account access to project' and 'Grant users access to this service account' sections are optional. The 'CREATE AND CONTINUE' button is highlighted.

Create a service account to be used for this project

7. On the left sidebar, select “**IAM & Admin**” then select “**Service Accounts**”
8. Click the “**+ Create Service Account**” button at the top of the page.
9. Enter the Service account name: securenowsync
10. Enter an optional “**Service account description.**”
11. Click the “**Create and Continue**” button.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

The screenshot shows the Google Cloud Platform console interface. The left sidebar is open to 'IAM & Admin' > 'Service Accounts'. The main content area is titled 'Create service account' and shows a progress bar with three steps: 1. Service account details (checked), 2. Grant this service account access to project (optional) (checked), and 3. Grant users access to this service account (optional). The 'Service account permissions (optional)' section is active, with a description: 'Grant this service account access to GSuiteSecureNowIntegration so that it has permission to complete specific actions on the resources in your project. [Learn more](#)'. A dropdown menu is open under 'Select a role', showing a list of roles. The 'Owner' role is selected and highlighted with a blue box. The 'Owner' role is also highlighted in the 'Condition' column. A blue box highlights the 'Select a role' dropdown, and another blue box highlights the 'Owner' role in the list. A blue box also highlights the 'Owner' role in the 'Condition' column.

Create a service account to be used for this project

12. Click “**Select a role**” and choose “**Owner**” to grant service account access to the project owner.

13. Click “**Continue.**”

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

The screenshot shows the Google Cloud Platform IAM & Admin console. The top navigation bar includes the Google Cloud Platform logo, the project name 'GSuiteSecureNowIntegration', and a search bar. The left sidebar shows the 'IAM & Admin' menu with 'Service Accounts' selected. The main content area displays 'Service accounts for project "GSuiteSecureNowIntegration"'. A table lists service accounts, with one entry for 'secrenowsync' having a status of '✓'. The 'Actions' column for this entry is highlighted with a blue box and the number 14. A dropdown menu is open, showing options: 'Manage details', 'Manage permissions', 'Manage keys' (highlighted with a blue box and the number 14), 'View metrics', 'View logs', 'Disable', and 'Delete'. Below this, the 'Keys' section for the 'secrenowsync' service account is shown. The 'ADD KEY' button is highlighted with a blue box and the number 15. The 'Create new key' button is highlighted with a blue box and the number 15. A 'Create key (optional)' dialog box is open, showing the 'JSON' key type selected (highlighted with a blue box and the number 16) and the 'CREATE' button highlighted with a blue box and the number 17.

Create a service account to be used for this project

14. In the “Actions” column, click the three vertical dots, then click the “**Manage Keys**” option.

15. Click the “**Add Key**” dropdown and select “**Create new key**”

16. In the sidebar that appears, select the “**JSON**” key type.

17. Click the “**Create**” button. The JSON file will be downloaded to your local computer. Store this somewhere safe, you will need to reference this later.

18. Once the file has been downloaded and saved, click the “**Done**” button.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

The screenshot shows the Google Cloud Platform IAM & Admin console. The left sidebar is labeled 'IAM & Admin' and includes options like IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federat..., Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Manage Resources, and Release Notes. The main content area is titled 'securenowsync' and has tabs for DETAILS, PERMISSIONS, KEYS, METRICS, and LOGS. The 'DETAILS' tab is selected. Under 'Service account details', the 'Name' field contains 'securenowsync' and has a 'SAVE' button next to it. The 'Description' field is empty and has a 'SAVE' button. Below that, the 'Email' and 'Unique ID' fields are visible. Under 'Service account status', there is a green checkmark indicating the account is active and a 'DISABLE SERVICE ACCOUNT' button. At the bottom, there is a link to 'SHOW DOMAIN-WIDE DELEGATION'.

- Enable G-Suite Domain-Wide Delegation
19. Click the “**Details**” section to modify your securenowsync service account.
20. Type in “securenowsync” in the “Name” field and click save

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console

```

1  {
2    "type": "service_account",
3    "project_id": "mindful-path-273115",
4    "private_key_id": "22468c8080c478670405300e66a0b0404a0423",
5    "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvQIBADoBgkqhkiG9w0BAQI\n6    "client_email": "securenowsync@mindful-path-273115.iam.gserviceaccount.com",
7  23 "client_id": "113628692295934966129",
8    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
9    "token_uri": "https://oauth2.googleapis.com/token",
10   "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
11   "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/secure
12  }
```

The screenshot shows the Google Admin console interface. At the top, there's a search bar and navigation icons. Below that, the 'Domain-wide Delegation' page is visible, showing a table of API clients. A blue box labeled '22' highlights the 'Add new' button. A modal dialog box titled 'Add a new client ID' is open in the foreground. It contains a text input field for 'Client ID' (labeled '23'), a checkbox for 'Overwrite existing client ID', and a larger text input field for 'OAuth scopes (comma-delimited)' (labeled '24'). At the bottom right of the dialog, there are 'CANCEL' and 'AUTHORIZE' buttons, with 'AUTHORIZE' labeled '25'.

Delegate domain-wide authority to the service account

21. Navigate to:

<https://admin.google.com/ac/owl/domainwideelegation>

22. Click the “**Add new**” button

23. Locate and open the JSON file downloaded in step 17 on [page 39](#) with any file editor. Copy the “**client_id**” value (excluding quotation marks) and paste that value into the **Client ID** field.

24. Paste the following value into the **OAuth Scopes** field:

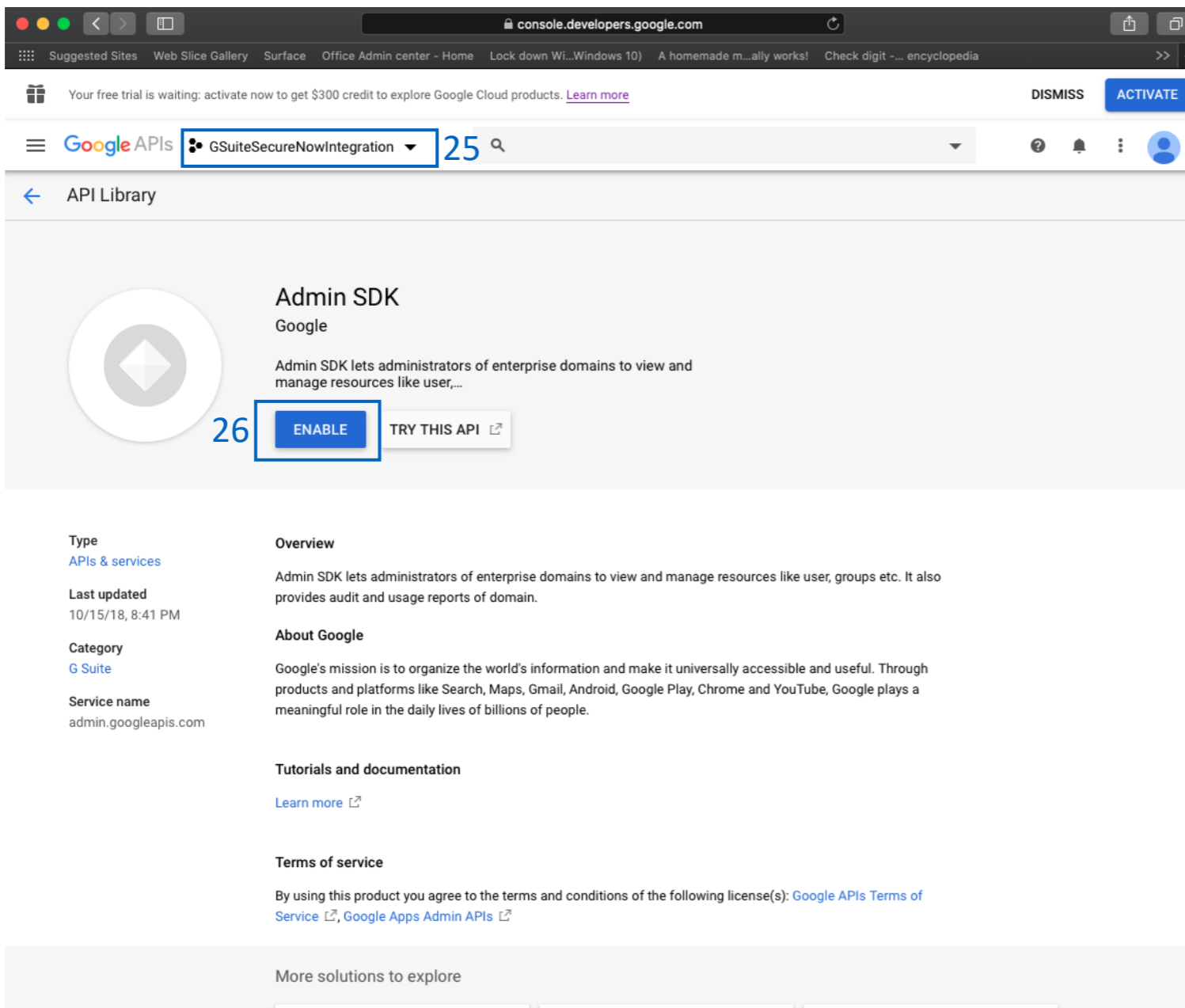
`https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.customer.readonly`

25. Click the “**Authorize**” button and the new scope will appear.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Setup in Google Console



The screenshot shows the Google API Library interface. At the top, there's a search bar with 'GSuiteSecureNowIntegration' entered. Below the search bar, the 'Admin SDK' API is displayed. The 'ENABLE' button is highlighted with a red box and the number 26. The page also includes sections for 'Type', 'Last updated', 'Category', 'Service name', 'Overview', 'About Google', 'Tutorials and documentation', and 'Terms of service'.

Enable Admin API for the project

24. Navigate to:

<https://console.developers.google.com/apis/library/admin.googleapis.com>

25. Confirm the

GSuiteSecureNowIntegration project is selected next to the Google API logo. Click the dropdown and select this project if it is not shown by default.

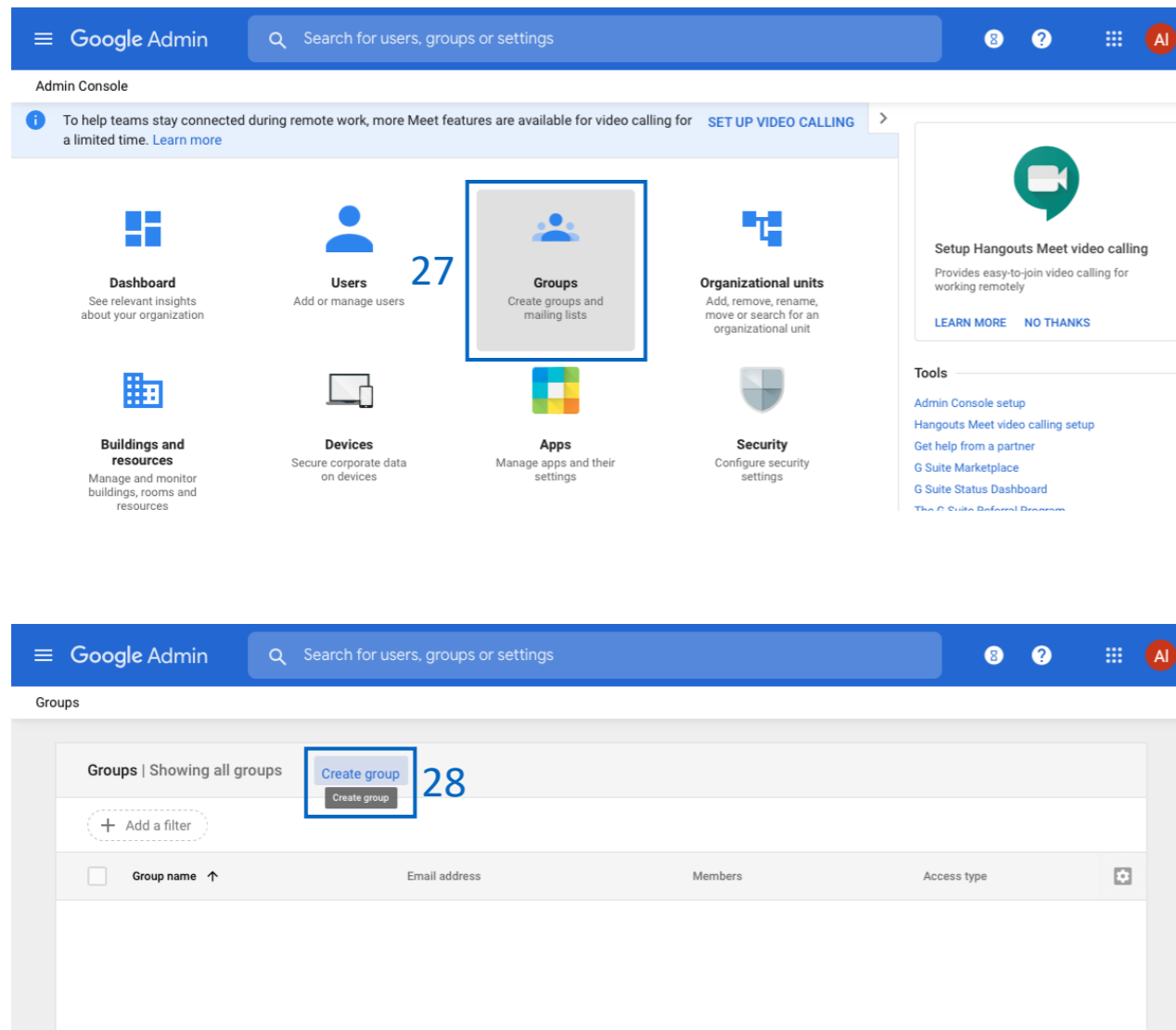
26. Click “**Enable**” button.

That's it! Your G-Suite Project is setup!
Continue to the next page to setup Groups inside the Google Console.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Creation of User Groups in Google Console



Create groups for designating the level of access inside the portal. The possible access levels are listed from lowest to highest and contain all features of the lower access levels:

- **BSN-Employees** – basic employee access
- **BSN-Managers** – access to reporting within a client
- **BSN-ManagerAdmins** – access to manage phishing and bulk manage users within a client
- **BSN-PartnerAdmins** – This user has the **highest** level of access and will have all administrative functions for all accounts within your portal. **This group is to ONLY be used for your company's internal account**

Follow the steps below for creating all desired groups:

27. Inside the Google Admin Console, click “**Groups**” to open the Groups dashboard
28. Inside the Groups dashboard, click “**Create group**”

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Creation of User Groups in Google Console

29

30

31

32

29. Provide the following “**Group Details**” for the desired group:

- Name - **BSN-Employees**
Description – Employee group for users
Group email – bsn-employees
- Name - **BSN-Managers**
Description – Manager group for users
Group email – bsn-managers
- Name – **BSN-ManagerAdmins**
Description – Manager Admin group for users
Group email – bsn-manageradmins
- Name – **BSN-PartnerAdmins**
Description – Partner Admin group
Group email – bsn-partneradmins

This is to ONLY be used for your company's internal account

- See next page for Tag descriptions (Optional)

33

30. Click “**Next**”

31. Setup desired access settings

32. Click “**Create Group**”

33. Click to add users to the created group

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Creation of Tags Groups in Google Console - Optional

The image shows two screenshots of the Google Admin console 'Create group' wizard. The top screenshot is the 'Group information' step, and the bottom screenshot is the 'Group settings' step.

Group information step:

- Name:** [Redacted]
- Description:** [Redacted]
- Group email:** [Redacted]@say-thx.net
- Group owner(s):** Search for a user's name or email

Group settings step:

- Access type:** Custom (selected)
- Access settings table:**

	Group Owners	Group Managers	Group Members	Entire Organization	External
Contact owners	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View members	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View topics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Publish posts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Membership settings					
Manage members	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Add, invite, approve					
Who can join the group					
Only invited users					

Optional: Create Tag Groups.

Tags are used for creating specific groups, typically to separate users by department, to create groups you'd like to send specific phishing emails to, or to simplify tracking in the portal.

Group Name: BSN-TAG-**tagname**

*tagname will be the tag you want the users associated with.

Example: BSN-TAG-Executive Team, BSN-TAG-Finance, etc.

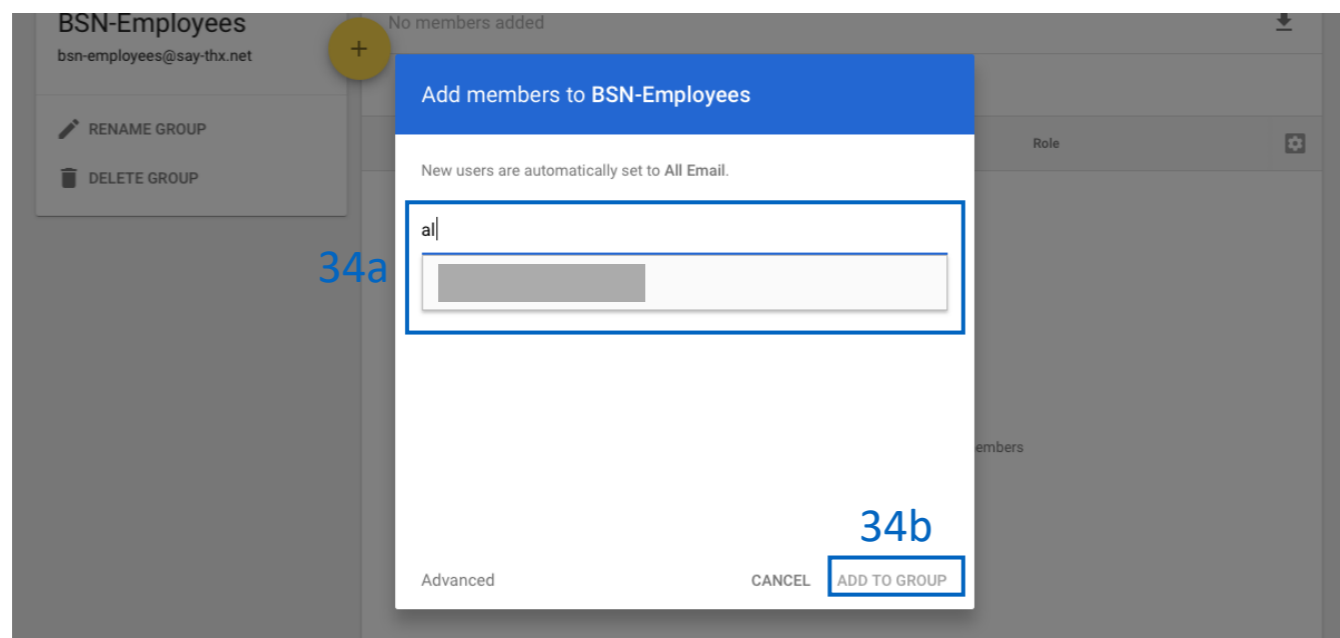
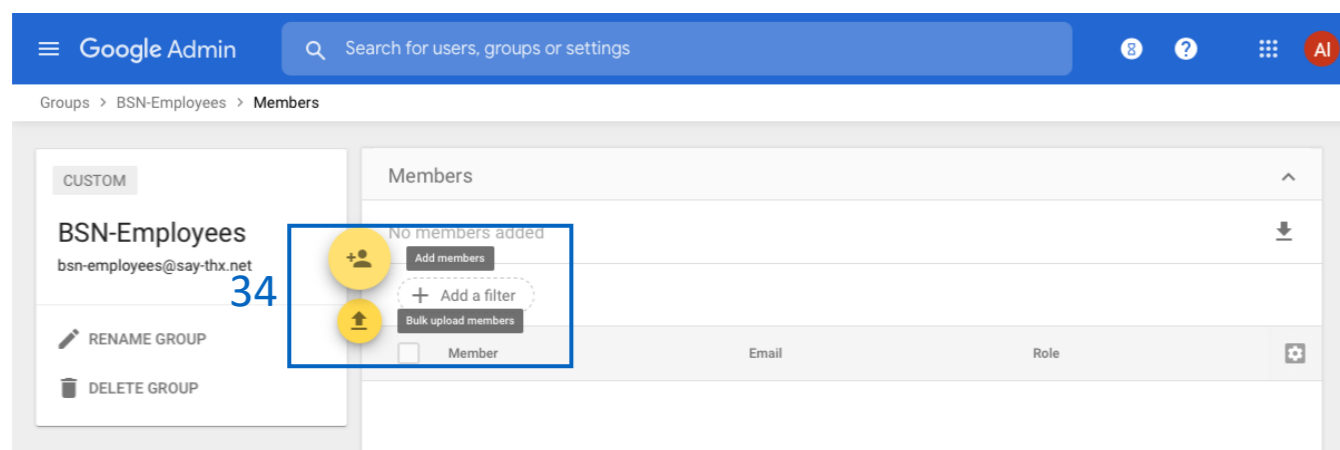
Group Description: Optional field if you would like to add details on the tag you created.

Back in your Groups dashboard, create another group using the process on the previous page but using the Tag selections above.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Adding Members to a Group in Google Console



Inside the Group Details dashboard:

34. Add members to the desired group:

a) Click the **add user icon** to add users one at a time:

- Begin typing the name of the user you would like to add to the group, click the user's email address, and click "Add to Group"

b) Or click the bulk upload members to import users in bulk

35. Repeat for all desired groups

Note: A user can only be in one access group. Access levels are on a hierarchy. All access levels contain the functionality as the access levels below it, simply add users to the highest level of access they should have. **However**, the user can be in one access group as well as one Tag group.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuration in the PII Protect Portal

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			✓	✗

36. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in select “Manage Clients” to access your client list (above).

37. Select the client you want to sync with Google Workspace/G-Suite Sync.

38. Select the “**Directory Sync**” tab and use the Sync Type drop-down selector to select “Google G-Suite”.

39. Click “**Enable**”

38

38-39

Sync Type: Google G-Suite Enable

Send automated welcome Customize welcome message

Configure messages and notification settings
Client: ABC Worldwide
Prior to enabling G-suite directory Sync. Be sure that you have added the users in the portal to either the BSN-Managers group.

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuring Messaging & Notification Settings – G-Suite Sync Settings Page

The screenshot displays the 'Directory Sync' settings page. At the top, there is a navigation bar with tabs: Dashboard, Information, Notification, Products, Access, Directory Sync (selected), Users, Dark Web, Training Reports, and Phishing. Below the navigation, the 'Sync Type' is set to 'Google G-Suite'. A blue box labeled '41' highlights the 'Send automated welcome' toggle, which is turned on. Another blue box labeled '42' highlights the 'Customize welcome message' toggle, also turned on. A third blue box labeled '43' highlights two buttons: 'Welcome Message' and 'Welcome Back Message'. Below these, a section titled 'Configure messages and notification settings' for 'Client: ABC Worldwide' is visible. A modal window titled 'Customize message' is open, showing a 'Defer sending of welcome message' toggle (44) which is turned on, with a 'How many hours?' dropdown set to '1'. A blue box labeled '45' highlights the 'Send Test' button. The modal also contains two rich text editors: 'Before link text' and 'After link text', both containing sample cybersecurity-related text. At the bottom of the modal are 'Save Draft', 'Cancel', and 'Publish' buttons.

40. You can configure how these welcome messages are sent to users during the sync.

41. **“Send automated welcome”** will send the welcome message to newly added employees during the sync.

42. **“Customize welcome message”** will enable welcome messages to be customized. Without this option checked, the standard messages will be sent based off the Global Messages in the Partner Profile.

43. Clicking **“Welcome Message”** or **“Welcome Back Message”** will allow you to adjust the message.

44. Messages can be deferred for a period of hours or days.

45. The text within the message can be adjusted and a test message can be sent to preview.

Welcome Message: Email sent to new users added to the platform

Welcome Back Message: Email sent to reactivated users

G-Suite Directory Sync Setup

Our G-Suite Directory Synchronization feature allows you to manage users inside the PII/PHI Protect portal with ease. Add, Modify, or Deactivate users as soon as they're in your client's system so they can get up to speed on cybersecurity, without a hitch.

Configuring Application Authentication – G-Suite Sync Settings Page

Dashboard Information Notification Products Access **Directory Sync** Users Dark Web Training Reports Phishing

Sync Type: Google G-Suite Enable

Send automated welcome Customize welcome message

Configure messages and notification settings
Client: ABC Worldwide
Prior to enabling G-suite directory Sync. Be sure that you have added the users in the portal to either the BSN-Managers group.

Ex: mail@mail.com **46**

Upload G-suite configuration file **47**

Attachment
Drag & Drop your files or Browse

* Only .json files will be accepted

48

46. Input your **G-Suite Admin Email Address**

47. Click the “**Choose File**” button and select the JSON file that was downloaded on [page 28](#).

48. Click “**Save**” to save your changes and finalize G-Suite synchronization for this client! Repeat steps 1 – 50 for each client!

Important: Once G-Suite Directory is activated; you will not be able to add users to the portal outside of this method. Our portal will sync once every hour, which may cause a delay for your users to be updated.

Bulk User Management via CSV

Managing users in bulk with our CSV template has never been easier. In just a few clicks, users can get onboarded into your client's PII/PHI Protect portal and start working towards cybersecurity awareness in minutes.

Configuration in the PII Protect Portal

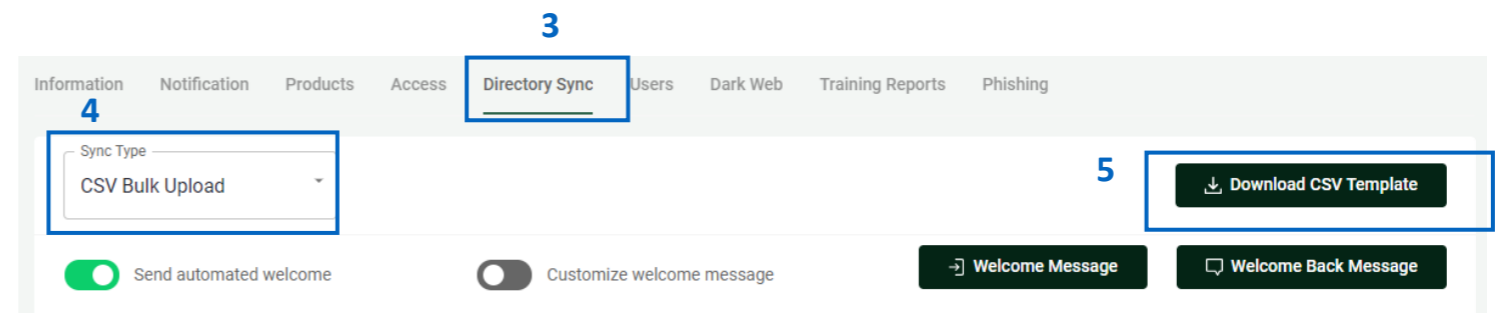
Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's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

3. Select the “**Directory Sync**” tab and use the Sync Type drop-down selector to select “Google G-Suite”.

4. Click “**Download CSV Template**” to download the current list of users inside the portal you'd like to modify. If you are uploading new users to the portal, a blank template will download.



Bulk User Management via CSV

Managing users in bulk with our CSV template has never been easier. In just a few clicks, users can get onboarded into your client's PII/PHI Protect portal and start working towards cybersecurity awareness in minutes.

Configuring Messaging & Notification Settings – CSV Bulk Upload Settings Page

The screenshot displays the 'Directory Sync' settings page for 'CSV Bulk Upload'. The interface includes a navigation bar with tabs for Information, Notification, Products, Access, Directory Sync, Users, Dark Web, Training Reports, and Phishing. The main content area features a 'Sync Type' dropdown set to 'CSV Bulk Upload' and a 'Download CSV Template' button. Below these are three main settings: 'Send automated welcome' (checked), 'Customize welcome message' (unchecked), and buttons for 'Welcome Message' and 'Welcome Back Message'. A modal window titled 'Customize message' is open, showing options to 'Defer sending of welcome message' (checked), a 'Welcome message' dropdown set to 'Hours', and a 'How many hours?' dropdown set to '1'. The modal also contains two rich text editors for 'Before link text' and 'After link text', both with a 'Send Test' button. At the bottom of the modal are 'Save Draft', 'Cancel', and 'Publish' buttons.

Welcome Message: Email sent to new users added to the platform

Welcome Back Message: Email sent to reactivated users

6. You can configure how these welcome messages are sent to users during the sync.
7. **“Send automated welcome”** will send the welcome message to newly added employees during the sync.

8. **“Customize welcome message”** will enable welcome messages to be customized.

Without this option checked, the standard messages will be sent based off the Global Messages in the Partner Profile.

9. Clicking **“Welcome Message”** or **“Welcome Back Message”** will allow you to adjust the message.

10. Messages can be deferred for a period of hours or days.

11. The text within the message can be adjusted and a test message can be sent to preview.

Bulk User Management via CSV

Managing users in bulk with our CSV template has never been easier. In just a few clicks, users can get onboarded into your client's PII/PHI Protect portal and start working towards cybersecurity awareness in minutes.

CSV Template Modification & Uploading

1	userID	firstName	lastName	email	phoneNumber	phoneNumberExt	cellNumber	managers	transaction	tag
2	OTQ3OTQ	Employee 1	Last Name	employee1@domain.com					A	Finance
3	OTQ3OTU	Employee 2	Last Name	employee2@domain.com					A	Sales
4	OTQ3OTY	Manager 1	Last Name	manager1@domain.com				x	M	Sales
5	OTQ3OTc	Employee 3	Last Name	employee3@domain.com					D	Sales
6	OTQ3OTg	Employee 4	Last Name	employee4@domain.com					A	Marketing
7										

12. Modify the required fields as needed.

Note: Do NOT modify header names or column A or your upload will fail.

Required Fields:

- firstName
- lastName
- email
- transaction

Optional Fields:

- managers
 - Place an "X" in this column to assign manager access to this user. Leave this column blank for employees.
- phoneNumber & phoneNumberExt
- Tag
 - Use tags to send filtered phishing emails and have access to more detailed reporting based on department.

Transaction column key: This column prompts the system to take one of the following actions when importing your user file into the system and is used to manage access to the system. This field **MUST** be completed for each user in this file or else you will receive an error.

- A** - Add or reactivate user (user will be notified)
- D** - Deactivate user (user will *not* be notified)
- M** - Modify user information (default for existing users)

Bulk User Management via CSV

Managing users in bulk with our CSV template has never been easier. In just a few clicks, users can get onboarded into your client's PII/PHI Protect portal and start working towards cybersecurity awareness in minutes.

CSV Template Modification & Uploading

The screenshot shows the 'Hermeys Dentistry' user management interface. The navigation bar includes 'Dashboard', 'Information', 'Notification', 'Products', 'Access', 'Directory Sync', 'Users', 'Dark Web', 'Training Reports', and 'Phishing'. The 'Directory Sync' section is active, showing a 'Sync Type' dropdown set to 'CSV Bulk Upload' and a 'Download Existing Users Of Template' button. Below this are two toggle switches: 'Send automated welcome' and 'Customize welcome message', both turned on. There are also 'Welcome Message' and 'Welcome Back Message' buttons. The 'Upload and files' section is highlighted with a blue box and labeled '13'. It contains an 'Attachment' area with the text 'Drag & Drop your files or Browse' and a note '* Only .csv files will be accepted'. A green 'Save' button with a checkmark is highlighted with a blue box and labeled '14'. At the bottom, there is a 'Helpful hints for ensuring upload success' section.

13. Once your file is formatted correctly, saved locally, and ready for import, navigate back to your Bulk Manage Users page (refer to [pages 39– 41](#)) for the client you wish to edit and click the “**Choose File**” button. Select the file you would like to upload and hit “**Open**”.

14. Click “**Save**” to upload the file and begin processing.

Congratulations! You’ve successfully uploaded a file to modify the users for that client! If you receive any errors or have any questions, reach out to us at operations@breachsecurenow.com

IMPORTANT: Please note that user uploads are processed every 15 minutes, so there may be a delay for your changes to show.



 **You're All Set!**

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

Email: Operations@breachsecurenow.com

Phone: (877) 275 – 4545