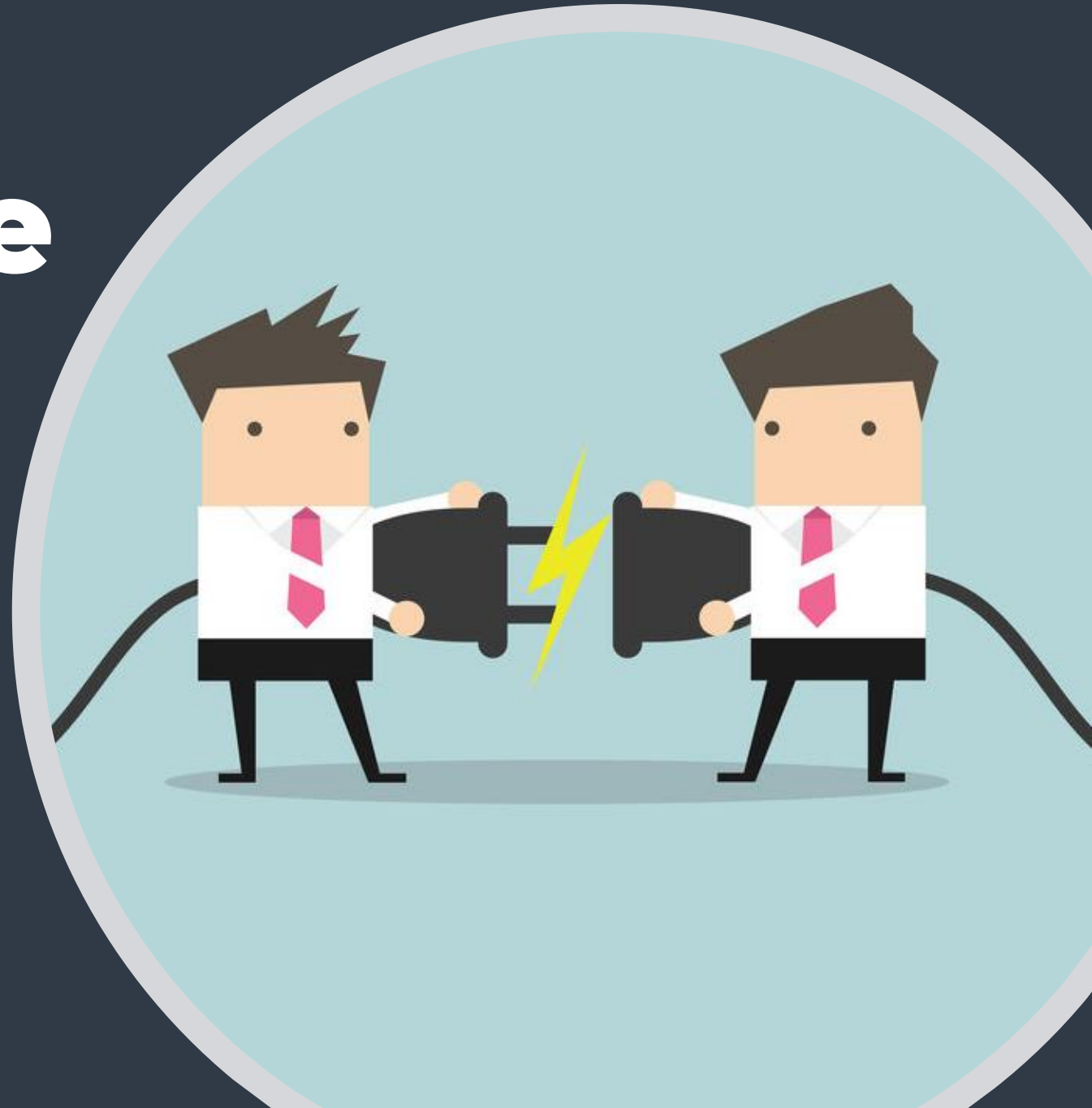


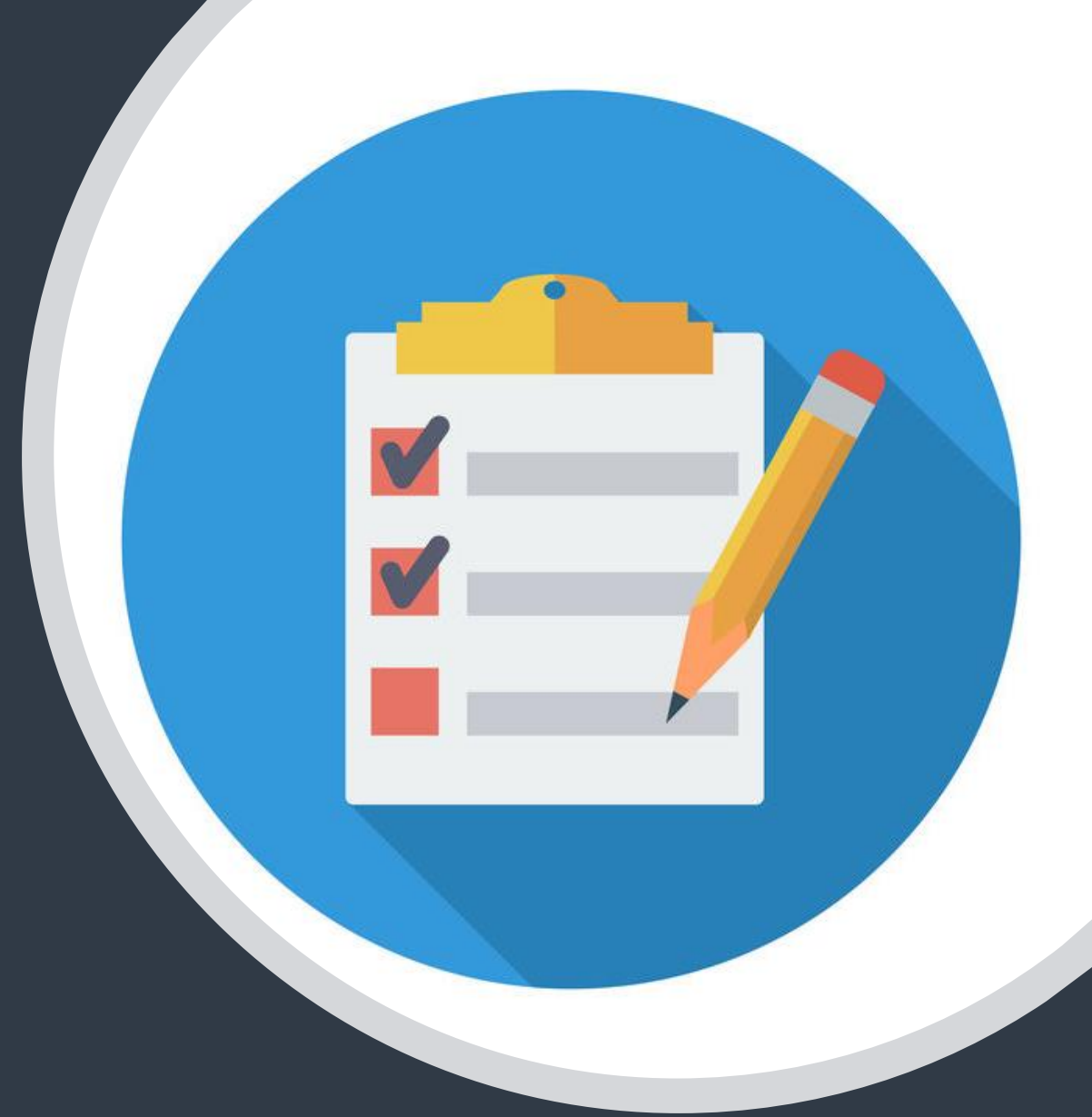
# Setup Guide

Client Azure AD  
integration with  
CyberPilot platform



# 1. Prerequisites for using Azure AD integration with the CyberPilot platform

- Requested CyberPilot for new AD Integration.  
(Needs to be unlocked for each integration).
- A person with Admin access to your organization's Azure AD.
- All of the users must have an exchange account (email) to be able to login with SSO and to be synced correctly to the platform.



## 2.a. Who will participate in the Awareness Training?

The first thing to do is figure out which users will participate in the Awareness Training. You will likely have to coordinate with the person in your organization that is responsible for the Awareness Training. He/she will know which users to onboard. Once you have a clear understanding of this, you can start working with the group that will be synced to the Awareness Training. This can be done in two ways.

- 1 By syncing with an existing group where all the relevant users are members. Note that only 1 group can be synced, so if the users are in different groups this will not work. See slide 4 on how to locate the object\_id that CyberPilot needs to complete the setup.
- 2 **Create a new group for use with Awareness Training. This is recommended, since it will allow for a more specific and selective approach to which users will participate in the training.**



## 2.b. Create group in Azure AD

- 1 Go to your admin view in Azure AD.  
<https://portal.azure.com/>
- 2 Go to "Groups" and click "New group"
- 3 Settings for the group
  - Group type = Security
  - Group name = fx "CyberPilot Awareness"
  - Membership type = Dynamic user
- 4 Click on add dynamic query

NOTE: You can also choose to work with the Membership Type "Assigned" instead of "Dynamic". In this case, you will need to manually assign each user. Unfortunately, Azure AD does not currently support the option to nest groups by assigning existing groups to other groups. 😞

The image shows two screenshots of the Azure AD admin center interface. The top screenshot, labeled '2', shows the 'Groups | All groups' page with the 'New group' button highlighted in a green box. The bottom screenshot, labeled '3', shows the 'New Group' configuration page with the following settings: Group type set to 'Security', Group name set to 'Awareness-training CyberPilot', and Membership type set to 'Dynamic User'. The 'Owners' section shows 'No owners selected' and the 'Dynamic user members' section has an 'Add dynamic query' link.

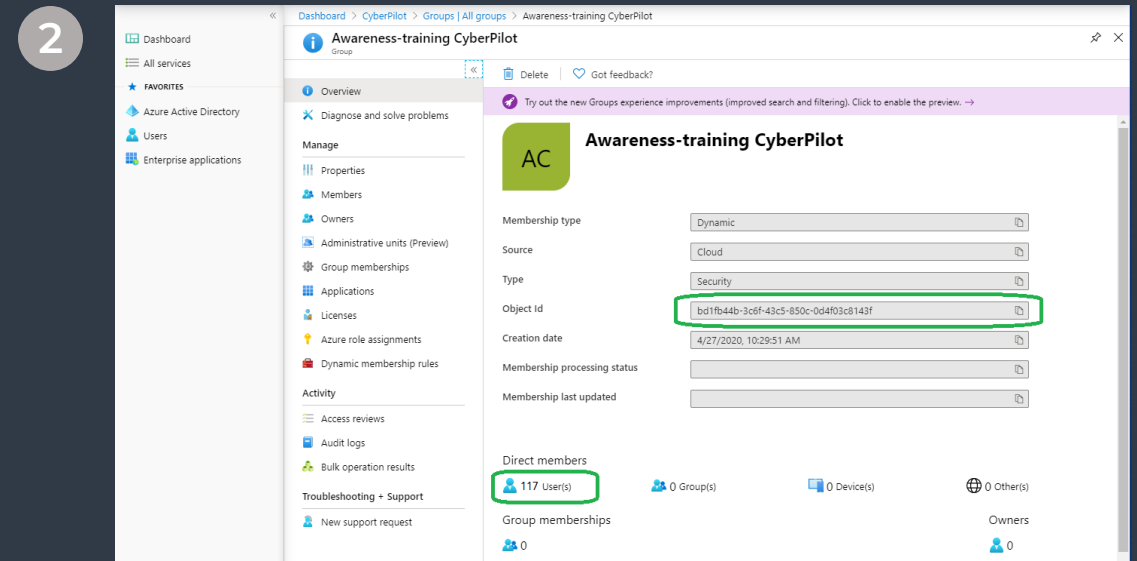
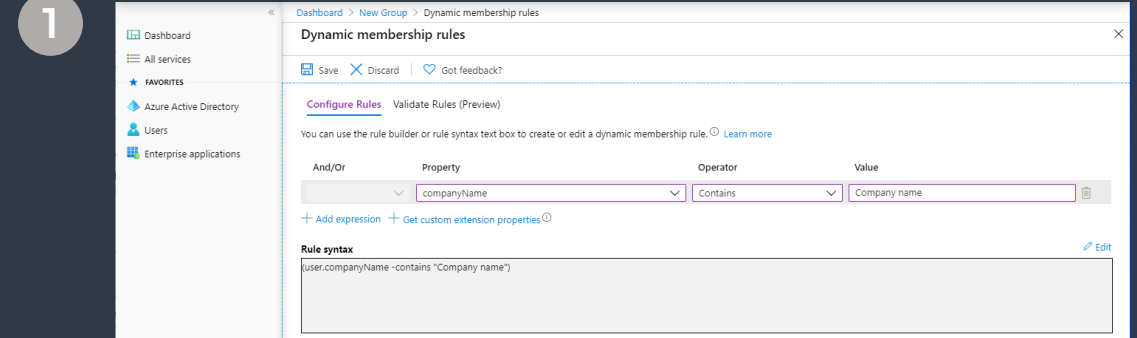
# 3. Create group(s) in Azure AD

1 Add a dynamic query that will pull users to the group.

- Choose e.g. Company Name as the property to pull for.
- You can also use rules to sort out users that should not be in a group
- Membership type = Dynamic user
- Click save and create group.

2 Locate the group and go to settings

- Check that users are added as direct members to the group. It might take a while before the changes take effect.
- Note the Group\_id to insert later



# 4. Login as an admin on the CyberPilot Platform

## CyberPilot platform

- 1 Login to your admin account on [www.security-platform.dk](http://www.security-platform.dk)
- 2 Open the menu "Branches"
- 3 Click on the branch with your company name. In case there are subbranches, you must choose the branch that does not have a parent.
- 4 Under the tab "Branch" you find the URL for your customized portal.
- 5 Click on "Settings" and choose SAML

1

2

3

4

5

Name	Parent
Demo Company	-
Demo Company - Administration	Demo Company
Demo Company - Employees	Demo Company

Home / Branches / Demo Company

BRANCH USERS COURSES CURRICULUMS SETTINGS

Name\* Demo Company

Parent branch Select branch

Domain name for branch yourcompany.security-platform.dk

UPDATE DELETE BRANCH

Home / Branches / Demo Company

BRANCH USERS COURSES CURRICULUMS SETTINGS

Name\* Demo Company

Parent branch Select branch

Domain name for branch yourcompany.security-platform.dk

SETTINGS

- OPTIONS
- LDAP
- SAML

UPDATE DELETE BRANCH

# 5. Locating the SAML settings

## CyberPilot platform

1 You have now opened the SAML settings on the CyberPilot Platform. It should look like this.

In this guide, this will be referred to as the "CyberPilot SAML settings".

1

BRANCH USERS COURSES CURRICULUMS SETTINGS

Enable SAML support

Create user if no match was found

Identity provider

Certificate fingerprint

Alternative certificate fingerprint

Remote Sign-in URL

Remote Sign-out URL

TargetedID

First name

Last name

Email

Custom fields

Sign SAML requests

Validate SAML requests

Assertion Consumer Service (ACS) URL

Single Logout Service URL

SP Metadata XML

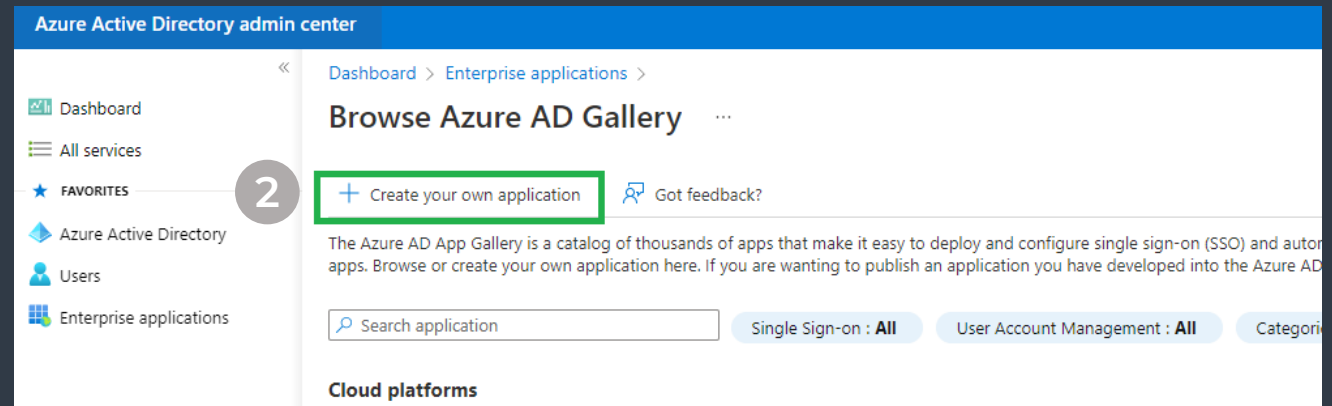
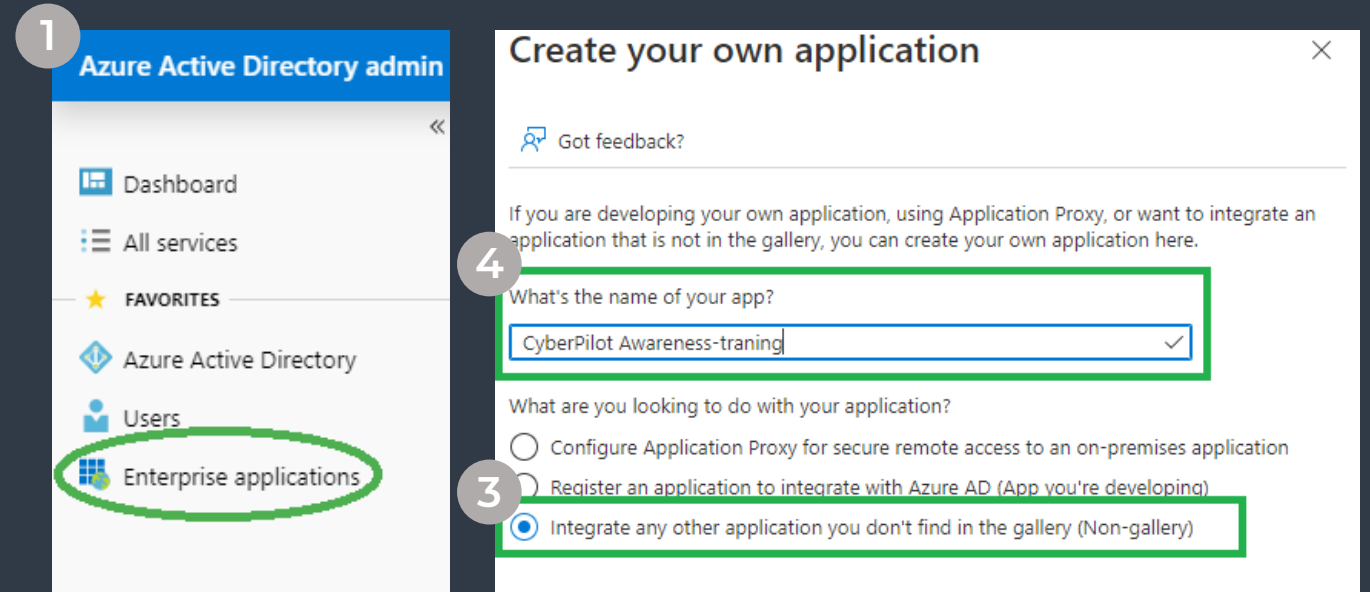
Bypass the default sign in screen and send users directly to the IDP's SAML sign-in page

SAVE

# 7. Creating an enterprise application (SSO)

## Creating an application

- 1 Click on Enterprise applications
- 2 Click on +Create your own application menu "Branches"
- 3 Select Non-gallery application  
(Integrate any other application you don't find in the gallery)
- 4 Give the application an appropriate name. Fx CyberPilot Awareness-training.  
The name is only for you own reference. CyberPilot only uses the object\_id.
- 5 Click Add and wait while the application is created.

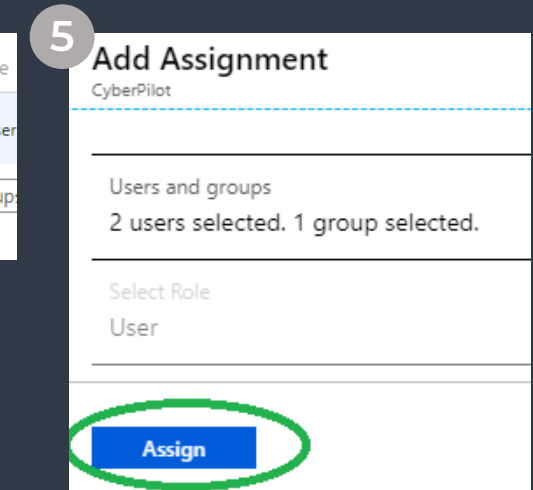
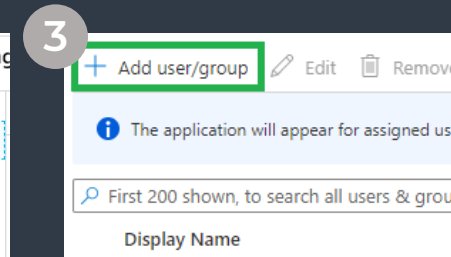
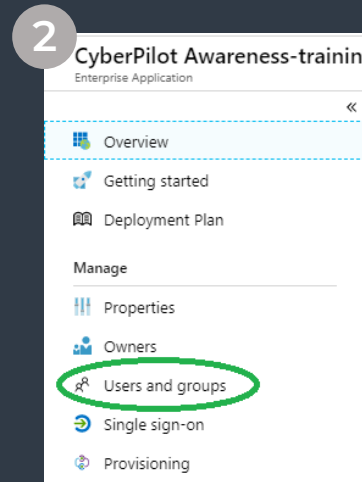
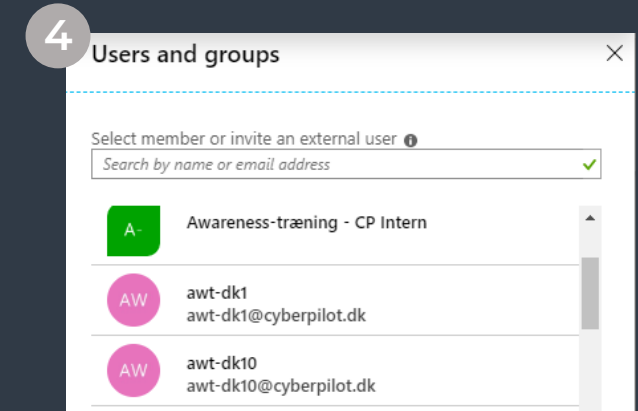
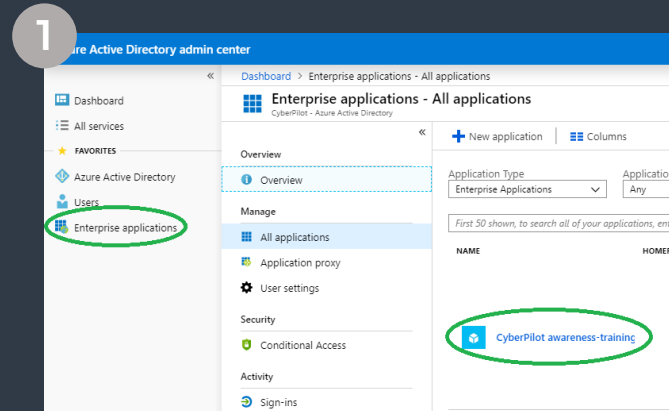




# 8. Add users/groups to the application

## Add users/groups to application

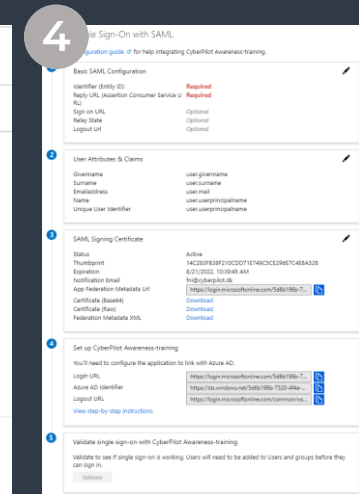
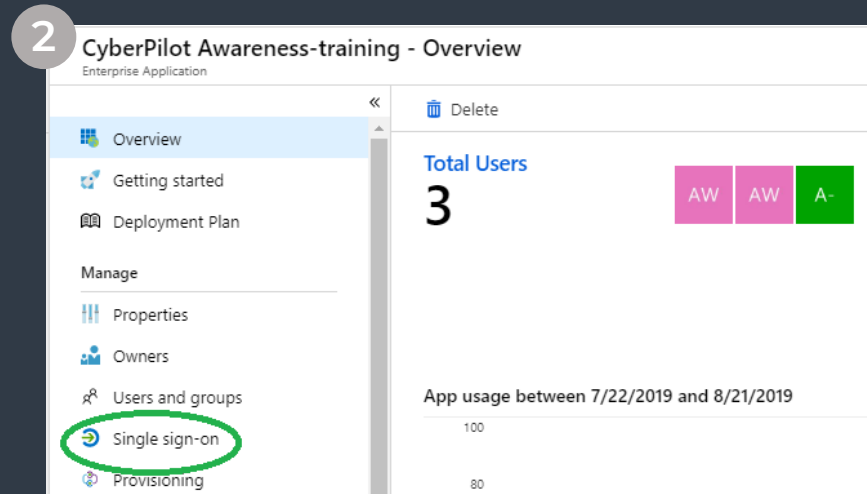
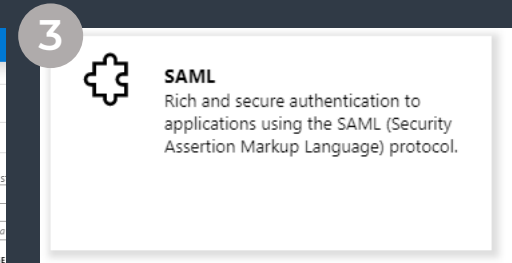
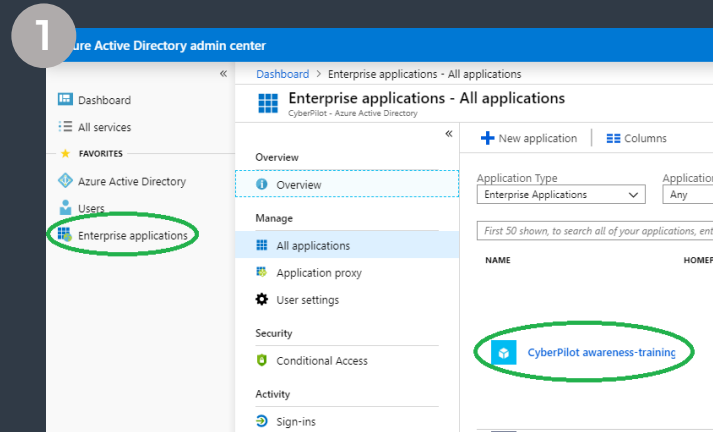
- 1 Click on Enterprise applications and open the application you created.
- 2 Select Users and groups
- 3 Click + Add user/group
- 4 Select the group that will be participating in the Awareness Training (make sure you use the group you created earlier).
- 5 When the group has been chosen – click select.
- 6 Remember to also click assign in the next menu.



# 9. Configuring the Enterprise application

## Configuring the application

- 1 Click on Enterprise applications and open the application you created.
- 2 Click on Single sign-on
- 3 Click on SAML
- 4 The SAML setup page is now ready for configuration. It contains 5 steps.



# 10. Configuring Basic SAML Settings (in Azure AD)

## Step 1 – basic SAML configuration

- 1 Insert the URL for your login page. This URL has been created for you by CyberPilot. The format should look like this (do not include https://) and chose the same that is listed under branch settings (see slide 4): **companyname.security-platform.dk**
- 2 Copy/paste the URL from CyberPilot SAML settings "Assertion Consumer Service (ACS) URL" to "Reply URL" in the Azure Application.
- 3 Copy/paste the URL from CyberPilot SAML settings "Single Logout Service URL" to "Logout URL" in the Azure Application.
- 4 Click save and close the page.
- 5 If a pop-up appears to validate the application, choose validate later

## Azure Single Sign-on Application

Basic SAML Configuration

Save Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) \*

Reply URL (Assertion Consumer Service URL) \*

Logout URL (Optional)

## CyberPilot SAML Settings

BRANCH USERS COURSES CURRICULUMS SETTINGS

Enable SAML support

Create user if no match was found

Identity provider

Certificate fingerprint

Alternative certificate fingerprint

Remote Sign-in URL

Remote Sign-out URL

TargetedID

First name

Last name

Email

Custom fields

Sign SAML requests

Validate SAML requests

Assertion Consumer Service (ACS) URL

Single Logout Service URL

SP Metadata XML

Validate single sign-on with CyberPilot Awareness-training

To ensure that single sign-on works for your application, we recommend using the validation capability (in the last step) to validate the changes you recently made. Would you like to validate now?

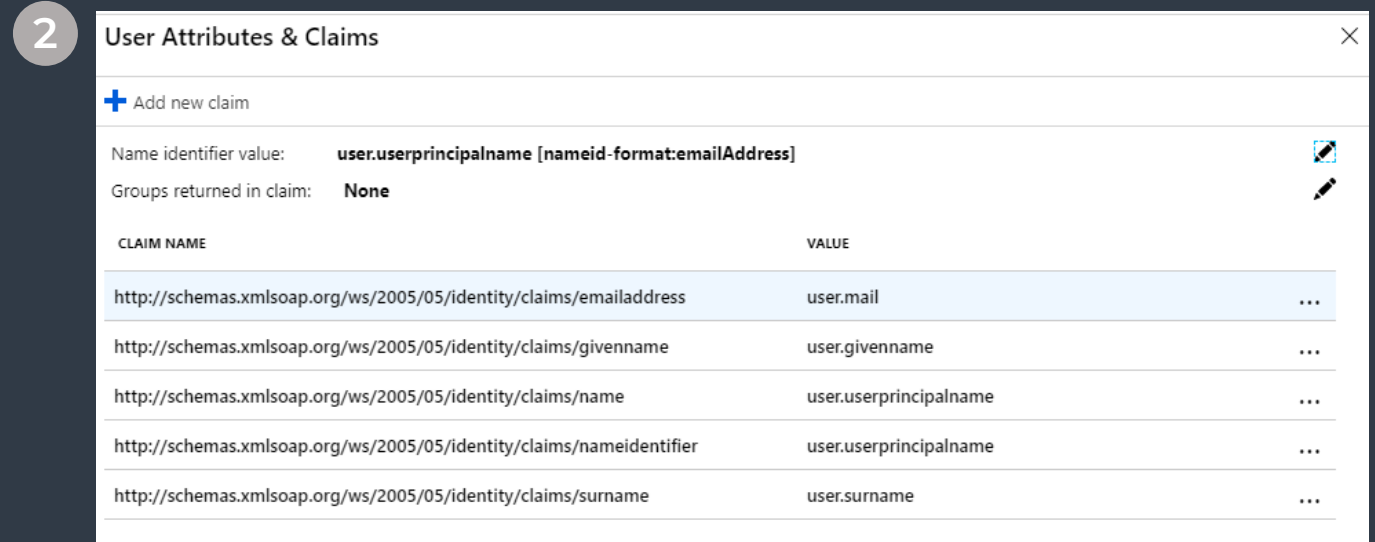
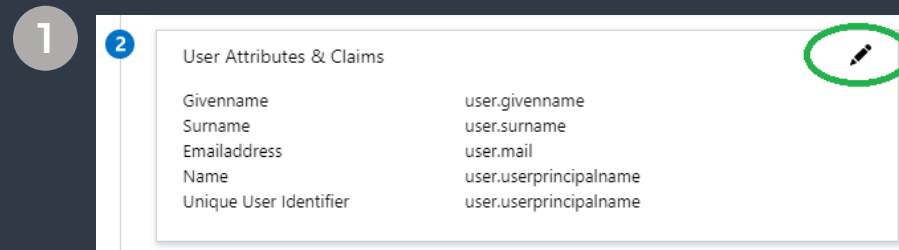
Yes

# 11. Configuring Claims and Attributes (in CP SAML settings)

## Step 2 – Attributes and Claims

1 Click edit on step 2 – User Attributes and claims (in the Single Sign-on settings in the Azure Application)

2 In the menu, you find the CLAIM NAMES. These must be copy/pasted into the CyberPilot SAML Settings. See next page.



# 12. Configuring Claims and Attributes (in CP SAML settings)

- 1 Insert the entire URL from the Azure application (step 2) into the CyberPilot SAML settings
- 2 Remember to click save in the CyberPilot SAML Settings

## Azure Single Sign-on Application

Dashboard > Enterprise applications > CyberPilot SSO > SAML-based Sign-on >

### User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ⋮]

Additional claims

Claim name	Value
<del>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</del>	<del>user.mail</del>
<del>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</del>	<del>user.givenname</del>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ⋮
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ⋮

## CyberPilot SAML Settings

Create user if no match was found

Identity provider

Certificate fingerprint

Alternative certificate fingerprint

Remote Sign-in URL

Remote Sign-out URL

TargetedID

First name

Last name

Email

# 13. Configuring SAML

## Steps 3+4

- 1 Copy/paste the URLs into the CyberPilot SAML Settings from the Azure AD enterprise application steps 3/4. Click save

The screenshot displays the CyberPilot SAML Settings configuration interface, divided into two main sections: 'SAML Signing Certificate' (Step 3) and 'Set up CyberPilot Awareness-training' (Step 4). The interface is split into two panes. The left pane shows the 'SAML Signing Certificate' section with fields for Status (Active), Thumbprint (14C283FB38F210CDD71E749C5CE296E7C4E8A528), Expiration (8/21/2022, 10:39:45 AM), Notification Email (fni@cyberpilot.dk), App Federation Metadata Url (https://login.microsoftonline.co...), and Certificate (Base64), Certificate (Raw), and Federation Metadata XML (all with Download links). The right pane shows the 'Set up CyberPilot Awareness-training' section with fields for Identity provider (https://sts.windows.net/5d6b196b-7320-4f4a-92c...), Certificate fingerprint (14C283FB38F210CDD71E749C5CE296E7C4E8A5), Alternative certificate fingerprint (e.g. c9ed4dfb07caf13fc21e0fec1572047eb8a7a4c), and Remote Sign-in URL (https://login.microsoftonline.com/5d6b196b-7320...). Green arrows indicate the mapping of data from the left pane to the right pane: the Thumbprint is copied to the Certificate fingerprint field, the App Federation Metadata Url is copied to the Identity provider field, and the Azure AD Identifier is copied to the Remote Sign-in URL field. The interface also includes a top navigation bar with 'BRANCH', 'USERS', 'COURSES', 'CURRICULUMS', and 'SETTINGS' (with a dropdown arrow). The 'Enable SAML support' checkbox is checked, and the 'Create user if no match was found' checkbox is unchecked.

**3** SAML Signing Certificate

Status: Active

Thumbprint: 14C283FB38F210CDD71E749C5CE296E7C4E8A528

Expiration: 8/21/2022, 10:39:45 AM

Notification Email: fni@cyberpilot.dk

App Federation Metadata Url: https://login.microsoftonline.co...

Certificate (Base64): Download

Certificate (Raw): Download

Federation Metadata XML: Download

**4** Set up CyberPilot Awareness-training

You'll need to configure the application to link with Azure AD.

Login URL: https://login.microsoftonline.co...

Azure AD Identifier: https://sts.windows.net/5d6b19...

BRANCH USERS COURSES CURRICULUMS SETTINGS

Enable SAML support

Create user if no match was found

Identity provider: https://sts.windows.net/5d6b196b-7320-4f4a-92c...

Certificate fingerprint: 14C283FB38F210CDD71E749C5CE296E7C4E8A5

Alternative certificate fingerprint: e.g. c9ed4dfb07caf13fc21e0fec1572047eb8a7a4c

Remote Sign-in URL: https://login.microsoftonline.com/5d6b196b-7320...

# 14. Finalizing setup

## CyberPilot SAML settings

- 1 In the Cyberpilot settings, make sure that the shown settings are ticked active.
- 2 Leave the remaining options unticked.
- 3 Click save.
- 4 Open a new browser window and go to your custom branch URL. See slide 4. on where to find your unique URL.

The screenshot shows the SAML configuration interface for a branch named 'Demo Company'. The page has a navigation bar with 'BRANCH', 'USERS', 'COURSES', 'CURRICULUMS', and 'SETTINGS'. The 'SETTINGS' section is active, showing various SAML-related options and input fields. The 'Enable SAML support' checkbox is checked, while 'Create user if no match was found' is unchecked. Several input fields contain URLs for identity providers, fingerprints, and sign-in/sign-out endpoints. At the bottom, there is a 'SAVE' button.

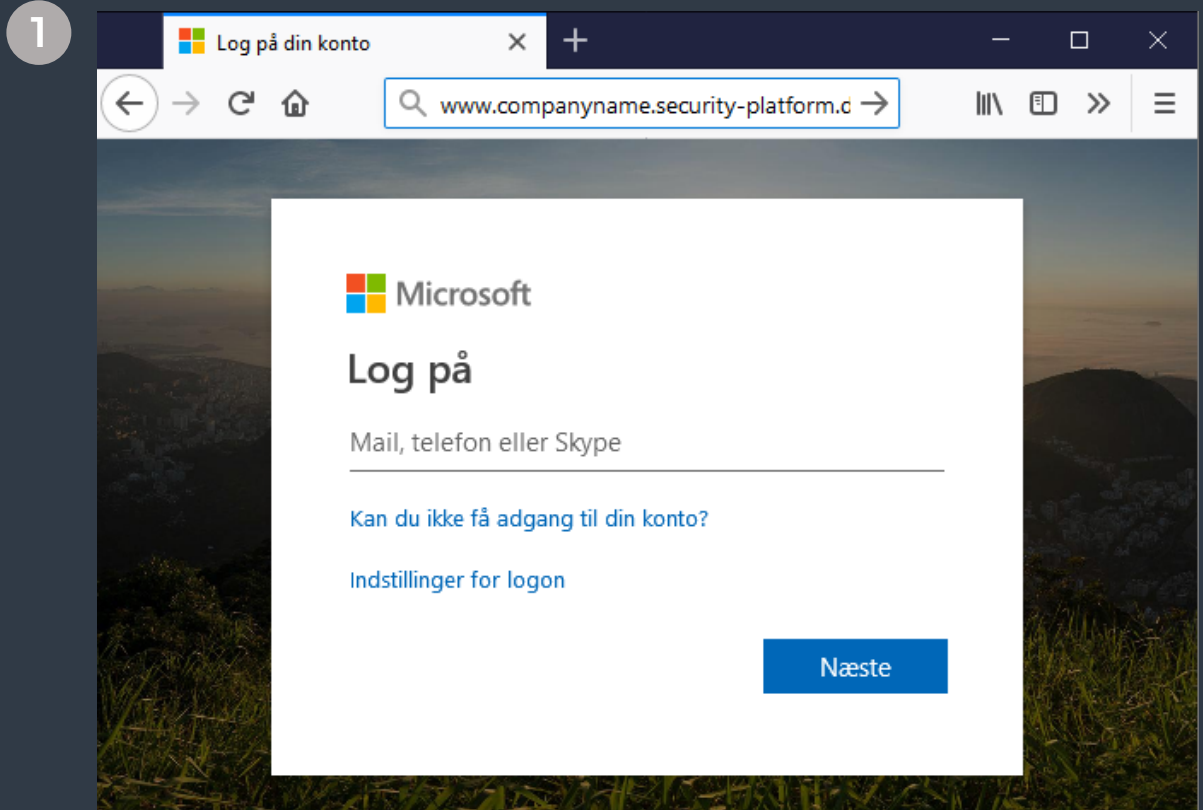
Setting	Value
Enable SAML support	<input checked="" type="checkbox"/>
Create user if no match was found	<input type="checkbox"/>
Identity provider	https://sts.windows.net/5d6b196b-7320-4f4a-92c2-
Certificate fingerprint	29D38C71F8681A9E28DD09B8A4622A0FB4ECA
Alternative certificate fingerprint	e.g. c9ed4dfb07ca1f3fc21e0fec1572047eb8a7a4cl
Remote Sign-in URL	https://login.microsoftonline.com/5d6b196b-7320-4
Remote Sign-out URL	https://login.microsoftonline.com/common/wsfeder:
TargetedID	http://schemas.xmlsoap.org/ws/2005/05/identity/clc
First name	http://schemas.xmlsoap.org/ws/2005/05/identity/clc
Last name	http://schemas.xmlsoap.org/ws/2005/05/identity/clc
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/clc
Custom fields	Comma separated list of more attributes
Sign SAML requests	<input type="checkbox"/>
Validate SAML requests	<input type="checkbox"/>
Assertion Consumer Service (ACS) URL	https://www.security-platform.dk/saml/module.php/saml/sp/saml2-acs.php/efront-sp
Single Logout Service URL	https://www.security-platform.dk/saml/module.php/saml/sp/saml2-logout.php/efront-sp
SP Metadata XML	https://www.security-platform.dk/saml/module.php/saml/sp/metadata.php/efront-sp
Bypass the default sign-in screen and send users directly to the IDP's SAML sign-in page	<input checked="" type="checkbox"/>

# 15. Testing SSO

## Checking the login page

- 1 Go to your custom URL. You should see something similar to this.
- 2 NOTE: When logging in through this portal, you will need to use your O365 credentials instead of your old CyberPilot login. Please try logging in to check if it works as intended.
- 3 NOTE: You will only be able to login if you are actually a member of the group registered in the SSO application AND you are also registered on the Awareness Training platform.

When you have tested that the login works, proceed to the second part of the setup concerning Auto-sync. If it does not work as intended, retrace this guide to see if anything was missed. If it still does not work, contact CyberPilot.

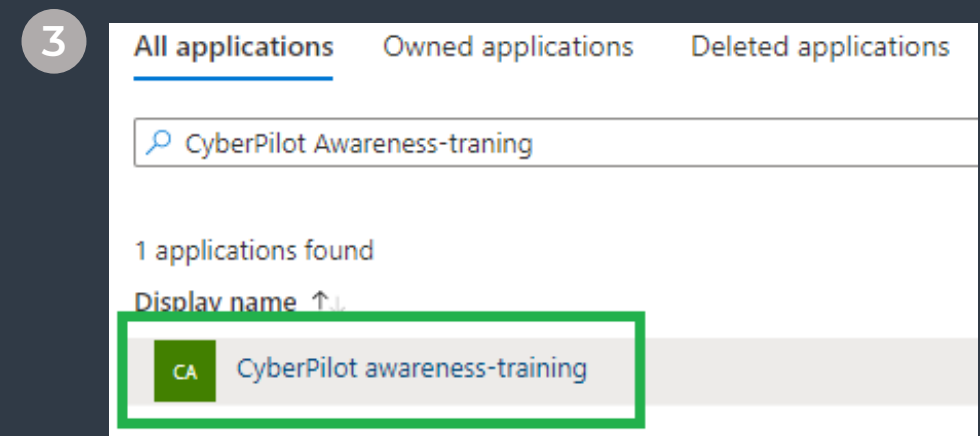
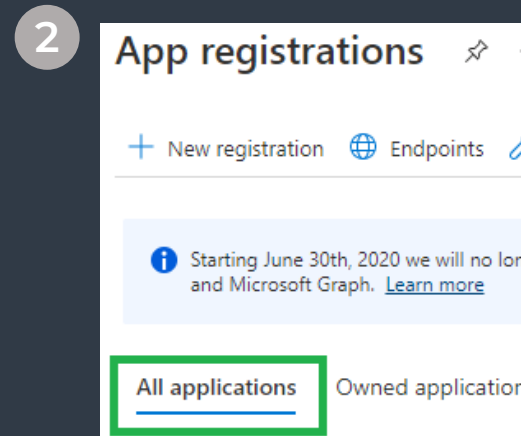
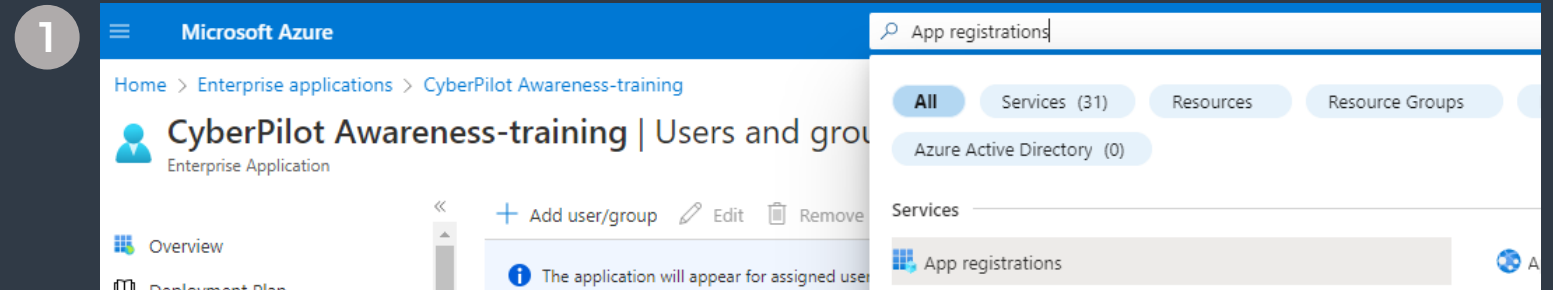




# 16. Set permissions for the application

## Navigate to application in App registrations:

- 1 Go to App registrations
- 2 Select All applications
- 3 Open the application you created



# 17. Set permissions for the application

## Navigate to Microsoft Graph:

- 1 Select API permissions under Manage
- 2 +Add a permission
- 3 Select Microsoft Graph

The screenshot displays the Microsoft Azure portal interface for managing API permissions. The left-hand navigation pane shows the 'API permissions' option selected. The main content area is titled 'CyberPilot awareness-training | API permissions'. A table lists the configured permissions, with a '+ Add a permission' button highlighted. The right-hand pane, titled 'Request API permissions', shows a list of commonly used Microsoft APIs, with 'Microsoft Graph' highlighted.

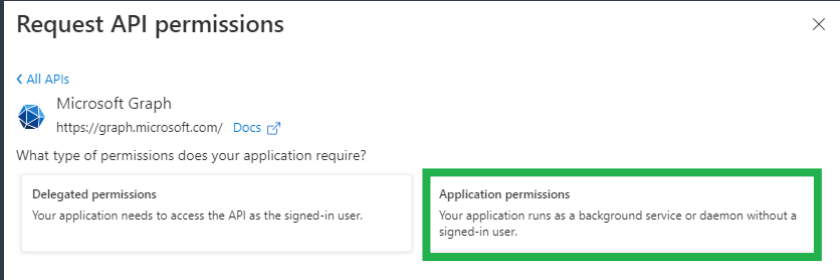
API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

# 18. Set permissions for the application

## Add permissions to the application:

- 1 Select "Application permissions"
- 2 Under Directory check Directory.Read.All  
This gives CyberPilot the right to read fields like "Manager"
- 3 Under GroupMember check GroupMember.Read.All  
This gives CyberPilot the right to read members of the group
- 4 Under User check User.Read.All  
This gives CyberPilot the right to read user properties

1



Request API permissions

< All APIs

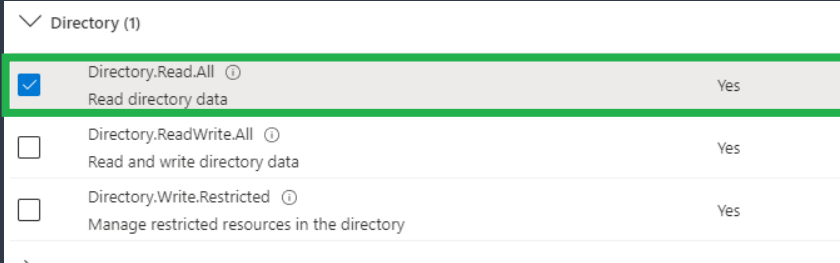
Microsoft Graph  
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

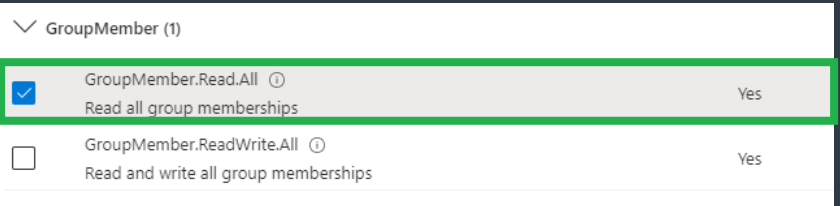
2



Directory (1)

<input checked="" type="checkbox"/>	Directory.Read.All Read directory data	Yes
<input type="checkbox"/>	Directory.ReadWrite.All Read and write directory data	Yes
<input type="checkbox"/>	Directory.Write.Restricted Manage restricted resources in the directory	Yes

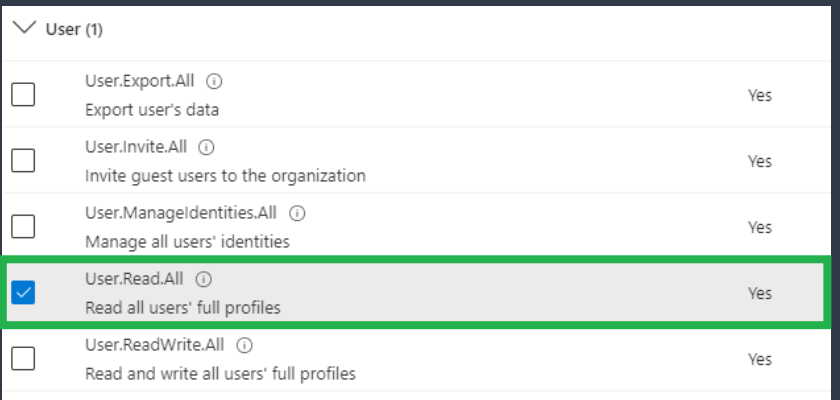
3



GroupMember (1)

<input checked="" type="checkbox"/>	GroupMember.Read.All Read all group memberships	Yes
<input type="checkbox"/>	GroupMember.ReadWrite.All Read and write all group memberships	Yes

4



User (1)

<input type="checkbox"/>	User.Export.All Export user's data	Yes
<input type="checkbox"/>	User.Invite.All Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All Manage all users' identities	Yes
<input checked="" type="checkbox"/>	User.Read.All Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadWrite.All Read and write all users' full profiles	Yes

# 19. Set permissions for the application

## Grant admin consent for permissions:

- 1 Grant admin consent for "Company name"
- 2 Confirm

1

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for CyberPilot

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3) ...				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for CyberPi... ...
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for CyberPi... ...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for CyberPi... ...

2

API permissions

« Refresh Got feedback?

**Grant admin consent confirmation.**

Do you want to grant consent for the requested permissions for all accounts in CyberPilot? This will update any existing admin consent records this application already has to match what is listed below.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for CyberPilot

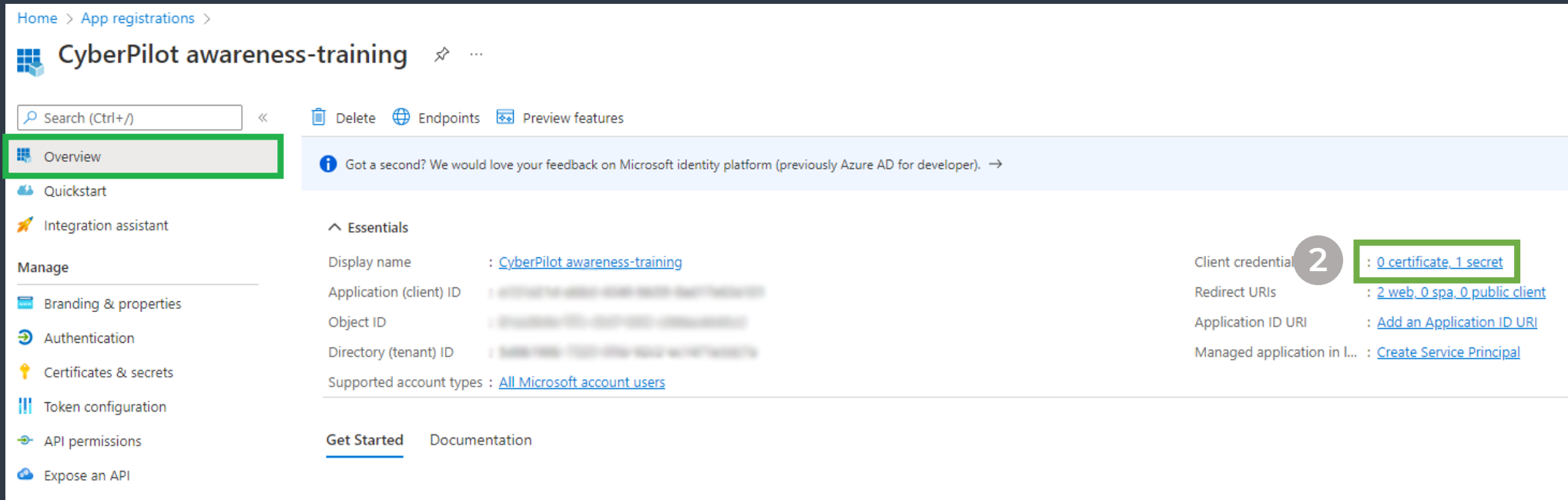
API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3) ...				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for CyberPi... ...
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for CyberPi... ...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for CyberPi... ...

To view and manage permissions and user consent, try [Enterprise applications](#).

# 20. Setting up Auto-sync

## Go to Client Secret:

- 1 Go to overview
- 2 Click "0 certificate. 0 secret"



# 21. Setting up Auto-sync

Create a Client Secret for the created enterprise application:

- 1 Select + New client secret
- 2 Insert description
- 3 Set expire date to 24 months
- 4 Click Add
- 5 Copy the Value for the new Client Secret for later use

The screenshot shows the Azure portal interface for managing application secrets. On the left, the 'Certificates & secrets' page for the 'CyberPilot awareness-training' application is visible. A green box highlights the '+ New client secret' button, with a circled '1' next to it. Below this, a table lists existing client secrets. The 'Expires' column shows '12/3' with a circled '5' next to it, and the 'Value' column shows a redacted secret value with a circled '5' next to it. On the right, the 'Add a client secret' dialog is open. The 'Description' field contains 'Secret for CyberPilot Autosync' with a circled '2' next to it. The 'Expires' dropdown menu is set to '24 months' with a circled '3' next to it.

Home > App registrations > CyberPilot awareness-training

CyberPilot awareness-training | Certificates & secrets

Search (Ctrl+/) << Got feedback?

Overview  
Quickstart  
Integration assistant

Manage

Branding & properties  
Authentication  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No description	12/3	[Redacted]	[Redacted]

Add a client secret

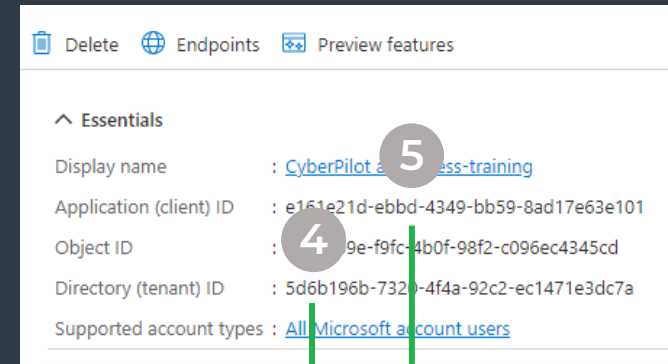
Description: Secret for CyberPilot Autosync

Expires: 24 months

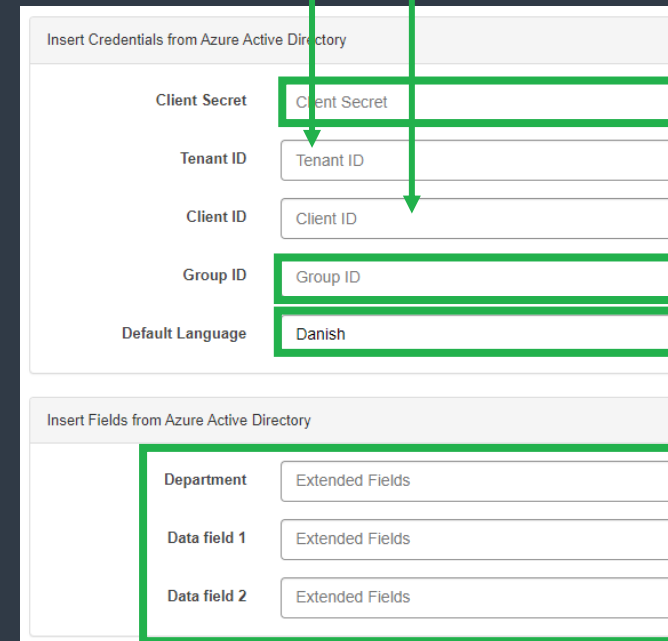
# 22. Setting up Auto-sync

## Insert:

- 1 Go back to overview
- 2 Open AD Integration on Awareness platform
- 3 Insert Client Secret from slide 21
- 4 Insert Directory (tenant ID)
- 5 Insert Application (client ID)
- 6 Insert Group ID from slide 3
- 7 Select default language  
(Default language are only for users where language is not set in AD)
- 8 If you want to synchronize extra fields from AD, Select Fields in the Extended Fields dropdown



Azure Application registration



CyberPilot AD Integration

# 12. Setting up Auto-sync

## Insert:

- 1 Click Save  
(Only group id, language and extended fields will be visible after inserting information)
- 2 Check the connection: In the left bottom corner, you can see the number of users pulled from the AD group.

Insert Credentials from Azure Active Directory

Client Secret: Client Secret

Tenant ID: Tenant ID

Client ID: Client ID

Group ID: abc12345-1234-abcd-12ab-1234567890abc

Default Language: Danish

Insert Fields from Azure Active Directory

Data field 1: Extended Fields

Data field 2: Extended Fields

Data field 3: Extended Fields

SAVE

2

3 DATA SUCCESSFULLY SAVED, 6 USERS FOUND IN AD GROUP



## 23. Whitelisting and handover to CyberPilot

- 1 Open the email that you received prior to the setup process.
- 2 Here you will find the email address that must be whitelisted in your system. Make sure this is done.
- 3 Notify CyberPilot that these steps have been completed by replying to the email.
- 4 Wait for confirmation from CyberPilot that everything is working as expected.



## 24. Ready to go – and plan for the future

- 1 Make sure that all the users that will participate in the training are added to the group that CyberPilot is syncing.
- 2 Discuss and plan with the person responsible for the Awareness Training program in your company, which processes need to be in place when new users need to be onboarded or offboarded.
  - How will you make sure that new employees are added to the group that CyberPilot is syncing? Is it a task to be done by a person or perhaps by a rule in Azure AD?
  - Also make sure you have a process for how employees that leave the company are removed/deleted from the group.
  - Users that are removed from your AD group will only be "deactivated" on the CyberPilot platform. Therefore, an admin user will have to delete users manually e.g. once a year. Who will take care of that?
- 3 The person responsible for the Awareness Training program will coordinate the rest of the start-up process. Once the setup is done, you can activate the Auto-sync and the syncing process will run once every 24h.

