

---

# **Setup Guide for CyberPilot AD Sync and Single Sign-On with Azure AD Cloud**

# Contents

- 1 Create a group in Azure AD
- 2 Azure AD User Properties
- 3 Create CyberPilot Enterprise Application in Azure AD
- 4 Setup CyberPilot Client Access in Azure AD
- 5 Set Up AD Sync in the CyberPilot App
- 6 Configure Single Sign-On in Azure AD
- 7 Configure Single Sign-On in the CyberPilot App
- 8 Whitelist notification emails from the CyberPilot App
- 9 Notify CyberPilot

---

# ① Create a Group in Azure AD

# Create a group in Azure AD

**Start by deciding which users will participate in the training.** You will likely have to coordinate with the person in your organization that is responsible for the training. They will know which users to onboard.

Then, you can start working on the AD group that will be synced to the CyberPilot App.

**This can be done in two ways:**

- 1 We recommend creating a new group for use with CyberPilot's training. This allows for a more specific and selective approach to which users will participate in the training. This guide is for this option.**
- 2** By syncing with an existing group where all the relevant users are members. Note that only one group can be synced, so if the users are in different groups, this will not work.

**Step 1:** Go to your admin view in Azure AD. <https://portal.azure.com/>

**Step 2:** Click on "Groups"

The screenshot shows the Azure portal home page. The browser address bar displays <https://portal.azure.com/#home>. A red arrow points to the address bar with the text "(1) Go to <https://portal.azure.com/>".

The page header includes the Microsoft Azure logo and a search bar with the text "Search resources, services, and docs (G+/)".

Below the header, there is a section titled "Access student benefits" with the text "Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status." and buttons for "Explore" and "Learn more".

The "Azure services" section features a grid of service tiles. A red arrow points to the "Groups" tile with the text "(2) Click on 'Groups'". The visible tiles are:

- Create a resource
- Users
- Enterprise applications
- Groups
- Microsoft Defender for...
- regist...

At the bottom of the services grid, there is a "More services" link with a right-pointing arrow.

**Step 3:** Click "New group"

**Step 4:** Ensure the group has the following settings

- Select Group type "Security"
- Fill in the Group name, e.g., "CyberPilot Awareness"
- Select Membership type "Dynamic User"

**Step 5:** Click on "Add dynamic query"

The screenshot shows the Azure Active Directory admin center interface. On the left, the 'Groups | All groups' page is visible, with a red arrow pointing to the 'New group' button labeled '(3) Click "New Group"'. The main area shows the 'New Group' configuration page with the following settings:

- Group type \***: Security (indicated by a red arrow labeled '(4) Select group type "Security"')
- Group name \***: Awareness-training CyberPilot (indicated by a red arrow labeled '(4) Fill in the group name')
- Group description**: Enter a description for the group
- Membership type \***: Dynamic User (indicated by a red arrow labeled '(4) Select membership type "Dynamic User"')
- Owners**: No owners selected
- Dynamic user members \***: Add dynamic query (indicated by a red arrow labeled '(5) 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.

**Step 6:** 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

**Step 7: Save rule**

- Click "Save"

Dashboard > New Group > Dynamic membership rules

### Dynamic membership rules

Save Discard Got feedback?

[Configure Rules](#) [Validate Rules \(Preview\)](#)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	companyName	Contains	Company name

+ Add expression + Get custom extension properties

**Rule syntax** [Edit](#)

```
{user.companyName -contains "Company name"}
```

(7) Click "Save"

(6) Set up properties to pull users into the group

## Step 8: Create the group

- Click on "Create"
- Refresh your browser (otherwise the group may not be visible)

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups >

### New Group

Got feedback?

Group type \* ⓘ  
Security

Group name \* ⓘ  
SJH-CyberPilot App

Group description ⓘ  
Users in this group are automatically created in the CyperPilot APP

Microsoft Entra roles can be assigned to the group ⓘ  
Yes No

Membership type \* ⓘ  
Dynamic User

Owners  
No owners selected

Dynamic user members \* ⓘ

**(8) Click "Create"** → **Create**



## Step 9: Locate the group and go to settings

- Note the Group (Object) ID to insert later
- Check that users are added as direct members to the group.

**It might take a while before group users are updated.**

The screenshot displays the Azure Active Directory console interface for the 'Awareness-training CyberPilot' group. The left-hand navigation pane includes sections for 'Dashboard', 'All services', 'FAVORITES', and 'Enterprise applications'. The main content area shows the group's overview, including its name, logo, and various settings. The 'Object Id' field is highlighted with a green box, and a red arrow points to it with the text '(9) Note the Group (Object) ID for later'. The 'Direct members' section is also highlighted with a green box, and a red arrow points to it with the text '(9) Check that users are added as direct members'. The 'Direct members' section shows 117 users, while the 'Group memberships' and 'Owners' sections show 0 members each.

Property	Value
Membership type	Dynamic
Source	Cloud
Type	Security
Object Id	bd1fb44b-3c6f-43c5-850c-0d4f03c8143f
Creation date	4/27/2020, 10:29:51 AM
Membership processing status	
Membership last updated	

Direct members: 117 User(s)

Group memberships: 0

Owners: 0

**Step 10:** Go to group members (click "Members")

**Step 11:** Check that your email is part of the group.

Note: Admin users are not deactivated by the AD-integration. So, if your user is removed from the AD-group your user will not be deactivated.

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > SJH-CyberPilot App

### SJH-CyberPilot App | Members

Group

Overview  
Diagnose and solve problems









Manage

- Properties
- Members**
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments

+ Add members ✕ Remove ↻ Refresh | 📄 Bulk operations ▾ | ☰ Columns | 🗨 Got feedback?

Direct members All members

Search by name

	Name	Type	Email	
<input type="checkbox"/>	 Aduser	User		Mi
<input type="checkbox"/>	 Brian English (UAT)	User		Mi
<input type="checkbox"/>	 CyberPilot Admin	User		Mi
<input type="checkbox"/>	 Karen Danish (UAT)	User		Mi
<input type="checkbox"/>	 Katerina	User		Mi
<input type="checkbox"/>	 Katya	User		Mi
<input type="checkbox"/>	 Lab08 Admin	User		Mi
<input type="checkbox"/>	 Lab08ad	User		Mi

(10) Click "Members"

(11) Check that your email is in the group

---

# ② Azure AD User Properties

# Azure AD User Properties

When the CyberPilot App synchronizes users with your Azure AD it reads each user in the Azure AD group you have created for the CyberPilot App.

If a user exists in your AD group, then the user is created/updated in the CyberPilot App.

If a user exists in the CyberPilot App, but not in your AD group, then the user is deactivated. Users with the role “Admin” are not deactivated, so that admins are not locked out of the CyberPilot App, if they are removed from the AD Group.

The CyberPilot App imports the following properties from the Azure AD user:

**User principal name, email, first name, last name, company name, department, manager, country, job title, mobile phone, office location, and preferred language.**

# USER PROPERTIES 1

## Overview of user properties in Azure AD

Home > Users >

Search

Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview

Audit logs Sign-in logs Diagnose and solve problems

Manage

Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods

Troubleshooting + Support

New support request

Overview Monitoring **Properties**

**Identity**

Display name

First name

Last name

User principal name

Object ID

Identities phone

User type Member

Creation type

Created date time Apr 11, 2023, 9:33 AM

Last password change date time Apr 12, 2023, 10:15 AM

Invitation state

External user state change date ...

Assigned licenses View

Password policies None

Password profile

Preferred language en-US

Sign in sessions valid from date ... Apr 12, 2023, 10:15 AM

**Contact Information**

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Email

Other emails

Proxy addresses View

Fax number

IM addresses View

Mail nickname sjh





**Parental controls**

Age group

Consent provided for minor

## USER PROPERTIES 2

### Overview of user properties in Azure AD

Created date time	Nov 10, 2023, 11:04 AM	Other emails	
Last password change date time	Jan 23, 2024, 3:39 PM	Proxy addresses	<a href="#">View</a>
Invitation state		Fax number	
External user state change date ...		IM addresses	
Assigned licenses	<a href="#">View</a>	Mail nickname	ben
Password policies		Parental controls 	
Password profile	<a href="#">View</a>	Age group	
Preferred language	en-US	Consent provided for minor	
Sign in sessions valid from date ...	Jan 23, 2024, 3:39 PM	Legal age group classification	
Authorization info	<a href="#">View</a>	Settings 	
Job Information 		Account enabled	Yes
Job title	Brian English "Job title"	Usage location	
Company name	Brian English "Company name"	Preferred data location	
Department	Brian English "Department" UAT	On-premises 	
Employee ID		On-premises sync enabled	No
Employee type		On-premises last sync date time	
Employee hire date		On-premises distinguished name	
Employee org data		Extension attributes	
Office location	Brian English "Office location"	On-premises immutable ID	
Manager		On-premises provisioning errors	
Sponsors			

## USER PROPERTY “Preferred Language”

If the user property “Preferred Language” is set it affects the language selected for the user in the CyberPilot App. If the property is not set, then English is the default value.

Licenses	Creation type
Devices	Created date time Apr 11, 2023, 9:33 AM
Azure role assignments	Last password change date time Apr 12, 2023, 10:15 AM
Authentication methods	Invitation state
Troubleshooting + Support	External user state change date ...
New support request	Assigned licenses <a href="#">View</a>
	Password policies None
	Password profile
	<b>Preferred language</b> en-US
	Sign in sessions valid from date ... Apr 12, 2023, 10:15 AM

CyberPilot

CyberPilot

Home

DASHBOARD

Trainings

AWARENESS >

PHISHING >

REPORTS >

Settings

ACCOUNT

USERS

BRANCHES

SYSTEM EMAILS

### Profile Settings

First Name \*  
Sam

Last Name \*  
Hepworth

Username \*  
cp.sjh

Email \*  
sjh@cyberpilot.io

Password

Confirm Password

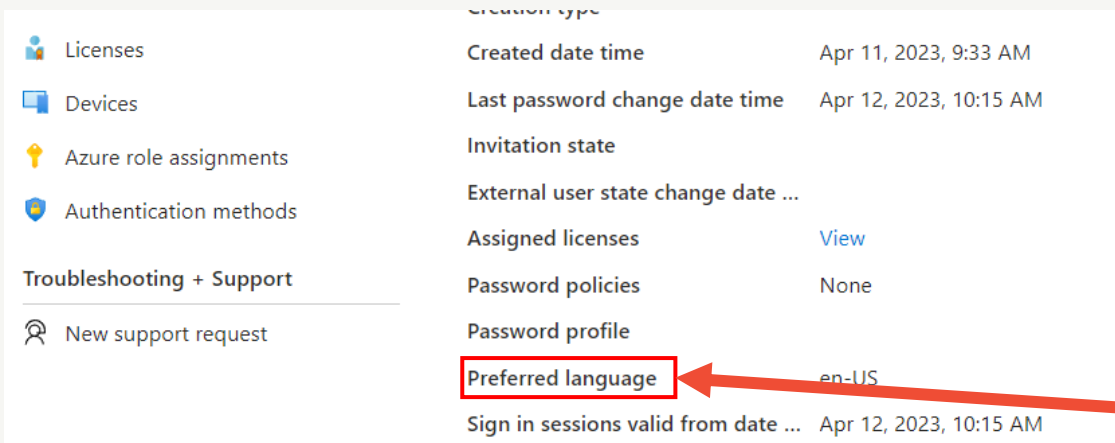
Language \*  
English [English]

### Important:

If a user manually changes their language in the CyberPilot App, then it overrides the preferred language in Azure AD

## USER PROPERTY “Preferred Language”

The user property “Preferred Language” may not be editable in your Azure AD portal, but it can be changed from <https://myaccount.microsoft.com> where it is called “Display language”.



Creation type

Created date time	Apr 11, 2023, 9:33 AM
Last password change date time	Apr 12, 2023, 10:15 AM
Invitation state	
External user state change date ...	
Assigned licenses	<a href="#">View</a>
Password policies	None
Password profile	
<b>Preferred language</b>	en-US
Sign in sessions valid from date ...	Apr 12, 2023, 10:15 AM

Licenses

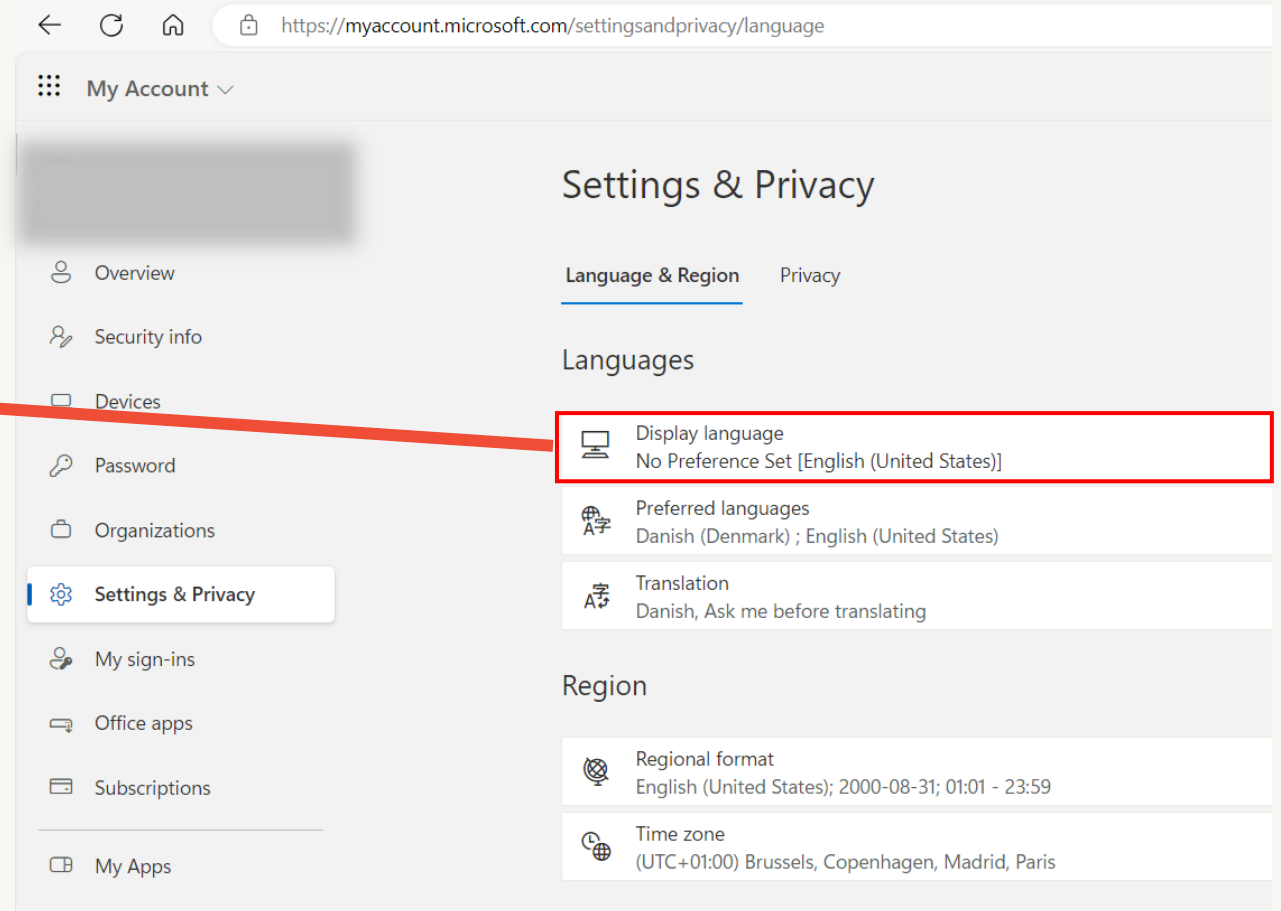
Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request






← ↻ 🏠 <https://myaccount.microsoft.com/settingsandprivacy/language>

My Account ▾



### Settings & Privacy

Language & Region Privacy

#### Languages

 Display language	No Preference Set [English (United States)]
 Preferred languages	Danish (Denmark) ; English (United States)
 Translation	Danish, Ask me before translating

#### Region

 Regional format	English (United States); 2000-08-31; 01:01 - 23:59
 Time zone	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris

Overview

Security info

Devices

Password

Organizations

**Settings & Privacy**

My sign-ins

Office apps

Subscriptions

My Apps

**Important:**  
If you need to change the Preferred Language of users other than yourself, please see this Microsoft Guide:

<https://learn.microsoft.com/en-us/microsoft-365/troubleshoot/access-management/set-language-and-region>



---

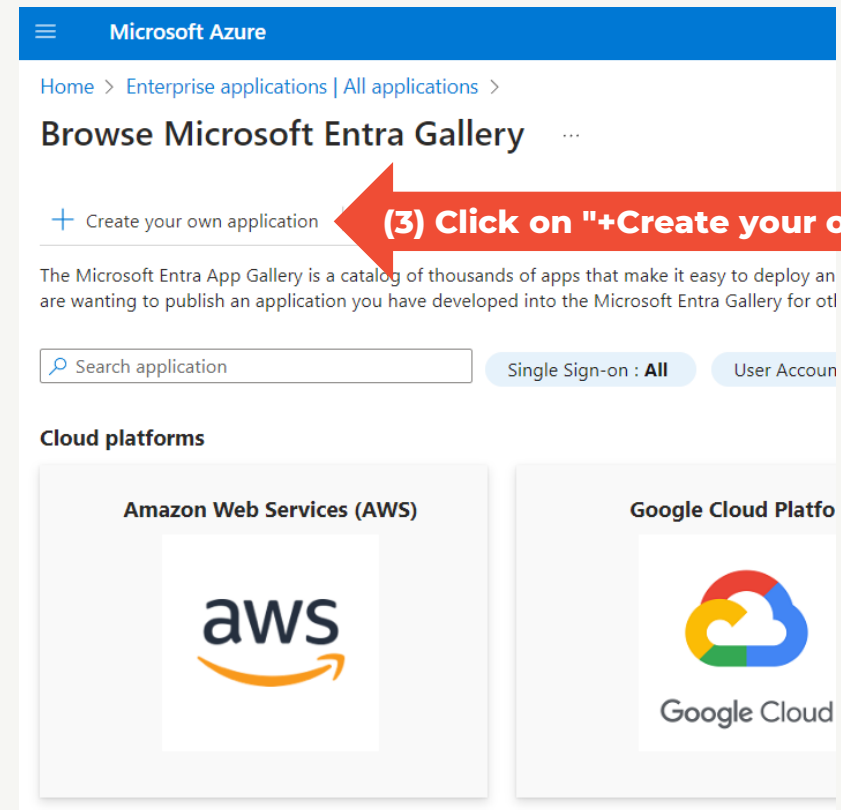
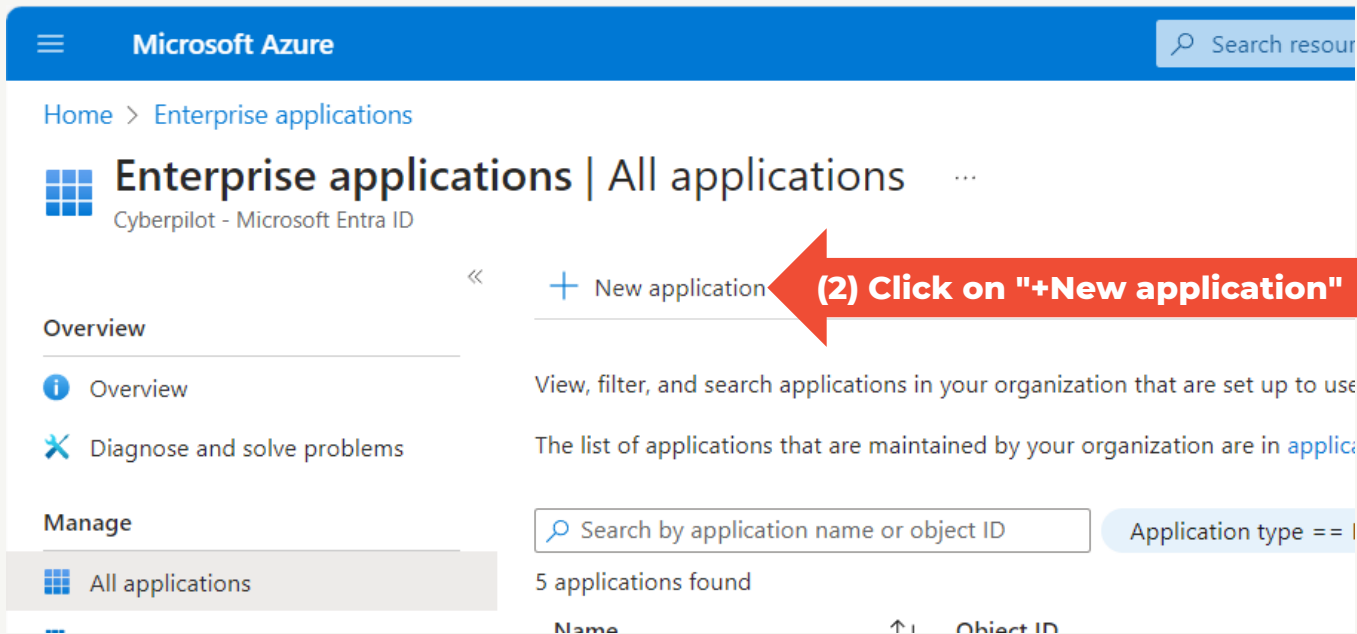
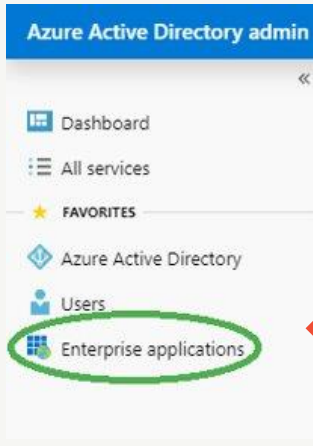
# ③ Create CyberPilot Enterprise Application in Azure AD

# CREATING THE APPLICATION

**Step 1:** Click on Enterprise applications

**Step 2:** Click on "+New application"

**Step 3:** Click on "+ Create your own application"




## CREATING THE APPLICATION

**Step 4:** Select "Integrate any other application you don't find in the gallery (Non-gallery)"

**Step 5:** Give the application an appropriate name, e.g., CyberPilot Awareness Training. The name is only for your own reference.

**Step 6:** Click "Create" and wait while the application is created

### Create your own application ×

 Got feedback?

---

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

✓

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

**We found the following applications that may match your entry**  
We recommend using gallery applications when possible.

**(5) Name the CyberPilot application**

**(4) Select "Integrate any other application you don't find in the gallery (Non-gallery)"**

**(6) Click "Create" (and wait for the application to be created)**

## ADDING USERS/GROUPS TO THE APPLICATION

**Step 7:** Ensure that you are on the page for the application you just created

**Step 8:** Click "Assign users and groups"

**Step 9:** Click "+ Add user/group"

Microsoft Azure

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

**CyberPilot Awareness Training | Overview**  
Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

**Properties**

CA

Name ⓘ  
CyberPilot Awareness Traini... [copy]

Application ID ⓘ  
a3ee543e-80f1-45ca-a5e2-... [copy]

Object ID ⓘ  
ad67919f-c3cf-49fd-8dcc-f5... [copy]

**Getting Started**

**1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)

**(7) Make sure you are on the CyberPilot enterprise application**

Microsoft Azure

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > CyberPilot Aw

**CyberPilot Awareness Training | Users and groups**  
Enterprise Application

+ Add user/group

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners

The application will appear for assigned users within My App

Assign users and groups to app-roles for your application here

First 200 shown, to search all users & gro...

Display Name

**(9) Click "+ Add user/group"**

**(8) Click "Assign users and groups"**

## ADDING USERS/GROUPS TO THE APPLICATION

**Step 10:** Click on "None Selected" (the text below "Users and groups")

**Step 11:** Select "Groups" to search for groups

**Step 12:** Search for the CyberPilot group you created earlier

**Step 13:** Mark the CyberPilot group

**Step 14:** Click on "Select"

**Step 15:** Click on "Assign"

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > CyberPilot Awareness Training | Users and groups >

### Add Assignment

Cyberpilot

Users and groups  
None Selected **(10) Click "None selected" (text below "Users and groups")**

Select a role  
User

Microsoft Azure Search resources, services, and docs (G+)

... > Browse Microsoft Entra Gallery > CyberPilot Awareness Training | Users and groups >

### Add Assignment

Cyberpilot

⚠ When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

Users and groups  
1 group selected.

Select a role  
User


**Assign** **(15) Click "Assign"**

Users and groups

Try changing or adding filters if you don't see what you're looking for.

Search  
cyber **(12) Enter the name of the group you created**  
2 results found

All Users Groups **(11) Select "Groups"**

	Name	Type	Email
<input checked="" type="checkbox"/>	 SJH-CyberPilot App	Group	

**Select** **(14) Click "Select"**

## SET PERMISSIONS FOR THE APPLICATION

Navigate to application in App registrations:

**Step 16:** Search for "App registrations"

**Step 17:** Click "App registrations"

**Step 18:** Open the CyberPilot application you created

The image shows a sequence of three screenshots from the Microsoft Azure portal, illustrating the steps to locate and open a specific application.

**Step 16:** The first screenshot shows the search bar at the top of the Azure portal with the text "app registrations" entered. A red arrow points to the search bar with the text "(16) Search for 'App registrations'".

**Step 17:** The second screenshot shows the search results for "App registrations". The "App registrations" service is highlighted in the list. A red arrow points to this service with the text "(17) Click 'App registrations'".

**Step 18:** The third screenshot shows the "All applications" page. The search bar contains "CyberPilot Awareness-training". The search results show "1 applications found" and a list with one entry: "CA CyberPilot awareness-training". A green box highlights this entry, and a red arrow points to it with the text "(18) Open the CyberPilot application".

# SET PERMISSIONS FOR THE APPLICATION

Navigate to Microsoft Graph:

**Step 19:** Click "API permissions"

**Step 20:** Click "+Add a permission"

**Step 21:** Click "Microsoft Graph"

Microsoft Azure

Home > App registrations > CyberPilot awareness-training

CyberPilot awareness-training | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission.

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 permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

API / Permissions name	Type	Description	Admin consent required
		user profile	No

### Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, and SharePoint through a single endpoint.

**Azure Communication Services**  
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams.

**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server.

**Azure Rights Management Services**  
Allow validated users to access protected content.

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal.

**Data Export Service for Microsoft Dynamics 365**  
Export data from Microsoft Dynamics CRM organization to an external destination.

**Dynamics 365 Central**  
Programmatic access to functionality in Dynamics Central.

**Dynamics CRM**  
Access the capabilities of CRM business software and ERP systems.

**Flow Service**  
Embed flow templates and manage flows.

**Intune**  
Programmatic access to Intune resources.

**Office 365 Management APIs**  
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity.

**OneNote**  
Create and manage notes, lists, pictures, files, and more in OneNote notebooks.

**Power BI Services**  
Programmatic access to Dashboard resource as Datasets, Tables, and Reports.

## SET PERMISSIONS FOR THE APPLICATION

Add permissions to the application:

**Step 22:** Click "Application permissions"

**Step 23:** Under Directory, select "Directory.Read.All"

- This gives CyberPilot read access to user properties such as "title"

**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.

**(22) Click "Application permissions"**

▼ Directory (1) **(23) Find and open Directory**

<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

**(23) Enable "Directory.Read.All"**



## SET PERMISSIONS FOR THE APPLICATION

Add permissions to the application:

**Step 24:** Under GroupMember, enable "GroupMember.Read.All"

- This gives CyberPilot the right to read members of the group

**Step 25:** Under User, enable "User.Read.All"

- This gives CyberPilot the right to read user properties

Permission	Description	State
GroupMember.Read.All	Read all group memberships	Checked
GroupMember.ReadWrite.All	Read and write all group memberships	Unchecked

(25) Find and Open User

(25) Enable "User.Read.All"

Permission	Description	State
User.Export.All	Export user's data	Unchecked
User.Invite.All	Invite guest users to the organization	Unchecked
User.ManageIdentities.All	Manage all users' identities	Unchecked
User.Read.All	Read all users' full profiles	Checked
User.ReadWrite.All	Read and write all users' full profiles	Unchecked

# SET PERMISSIONS FOR THE APPLICATION

Grant admin consent for permissions:

**Step 26:** Click "Add permissions"

**Step 27:** Click "Grant admin consent for..."

**Step 28:** Click "Yes" to confirm

Microsoft Azure Search resources, services, and docs (G+)

## 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 signed-in user.

Select permissions

Start typing a permission to filter these results

Permission	Admin consent required
> AccessReview	
> Acronym	

**Add permissions**

**(26) Click "Add permissions"**

Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations > CyberPilot Awareness Training

## CyberPilot Awareness Training | API permissions

Search Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission to reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

### 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 permissions includes all the permissions the application needs. [Learn more about permissions and consent](#)

Grant admin consent for Cyberpilot

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (3)			
Directory.Read.All	Application	Read directory data	Yes
GroupMember.Read.All	Application	Read all group memberships	Yes
User.Read.All	Application	Read all users' full profiles	Yes

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

**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.

**(27) Click "Grant admin consent for ..."**

**(28) Click "Yes" to confirm**

---

# ④ Setup CyberPilot Client Access in Azure AD

**Step 1:** Go to <https://portal.azure.com/>

**Step 2:** Click on "App registrations"

The screenshot shows the Microsoft Azure portal home page. A red arrow points to the address bar with the text "(1) Go to https://portal.azure.com/". Below the navigation bar, there are three main cards: "Start with an Azure free trial", "Manage Microsoft Entra ID", and "Access student benefits". Under the "Azure services" section, there is a row of icons for "Create a resource", "Users", "Groups", "Enterprise applications", "Microsoft Entra Password...", "App registrations", "Configuration Group Values", "Quickstart Center", "Virtual machines", and "More services". A red arrow points to the "App registrations" icon with the text "(2) Click 'App registrations'". At the bottom, there is a "Resources" section with tabs for "Recent" and "Favorite", and a table with columns for "Name", "Type", and "Last Viewed".

portal.azure.com/#home


Microsoft Azure

Search resources, services, and docs (G+)

Lab08admin@CPaware...  
CYBERPILOT (MAIL.DK)

### Welcome to Azure!


Don't have a subscription? Check out the following options.



#### Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).


[Start](#)



#### Manage Microsoft Entra ID

Azure Active Directory is becoming Microsoft Entra ID. Secure access for everyone.

[View](#) [Learn more](#)





#### Access student benefits


Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.


[Explore](#) [Learn more](#)


### Azure services


[Create a resource](#)


[Users](#)


[Groups](#)


[Enterprise applications](#)


[Microsoft Entra Password...](#)

[App registrations](#)

[Configuration Group Values](#)

[Quickstart Center](#)

[Virtual machines](#)

[More services](#)

### Resources

[Recent](#) [Favorite](#)

Name	Type	Last Viewed
------	------	-------------

<https://portal.azure.com/#create/hub>

(2) Click "App registrations"

**Step 3:** Click "All applications"

**Step 4:** Search of the CyberPilot enterprise application you created

**Step 5:** Click on the CyberPilot enterprise application you created

Microsoft Azure

Home >

## App registrations

+ New registration | Endpoints | Troubleshooting | Refresh | Download | Preview feature

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) for Microsoft Graph. [Learn more](#)

All applications | Owned applications | Deleted applications

cyber

1 applications found

Display name ↑↓

CA CyberPilot Awareness Training

**(3) Click on "All applications"**

**(4) Search for the enterprise application you created for CyberPilot**

**(5) Click on the enterprise application you created for CyberPilot**

**Step 6:** Copy the following values to paste later in the CyberPilot application:

- Application (client) ID
- Directory (tenant) ID
- *Note: you also need the Group (object) ID that you copied on slide 9*

**Step 7:** Click on "Add a certificate or secret"

Home > App registrations >

## CyberPilot Awareness Training

Search

Delete Endpoints Preview features

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

### Essentials

Display name <a href="#">CyberPilot Awareness Training</a>	Client credentials <a href="#">Add a certificate or secret</a>
Application (client) ID [Redacted]	Redirect URIs [Redacted]
Object ID [Redacted]	Application ID URI <a href="#">Add an Application ID URI</a>
Directory (tenant) ID [Redacted]	Managed application in local directory <a href="#">CyberPilot Awareness Training</a>
Supported account types <a href="#">My organization only</a>	

**(6) Copy Application (client) ID**

**(6) Copy Directory (tenant) ID**

**(7) Click "Add a certificate or secret"**

# CREATE A CLIENT SECRET FOR THE CREATED ENTERPRISE APPLICATION

**Step 8:** Click "+ New client secret"

**Step 9:** Insert a description, e.g., CyberPilot Awareness Training

**Step 10:** Set expire date to 24 months

**Step 11:** Click "Add"

Home > App registrations > CyberPilot Awareness Training

## CyberPilot Awareness Training | Certificates & secrets

Search << Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators

Credentials enable confidential applications to identify themselves to the scheme). For a higher level of assurance, we recommend using a certificate.

Application registration certificates, secrets and federated credentials can be used to authenticate applications.

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

A secret string that the application uses to prove its identity when requested.

+ New client secret

Description	Expires	Valid from
No client secrets have been created for this application.		

Add

**(8) Click "+ New client secret"**

**(9) Enter a description**

**(10) Set expires to 24 months**

**(11) Click "Add"**

# CREATE A CLIENT SECRET FOR THE CREATED ENTERPRISE APPLICATION

**Step 12:** Copy secret value to a safe location. **Note: You will not be able to see this value again, so it is very important that you make a copy and store it in a safe place, such as a password manager.**

**Step 13:** Copy secret ID and store it in a safe location.

Home > App registrations > CyberPilot Awareness Training

CyberPilot Awareness Training | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

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
CyberPilot Awareness Training	1/21/2026	[Redacted]	[Redacted]

(12) Copy secret value

(13) Copy secret ID



---

# ⑤ Set Up AD Sync in the CyberPilot App

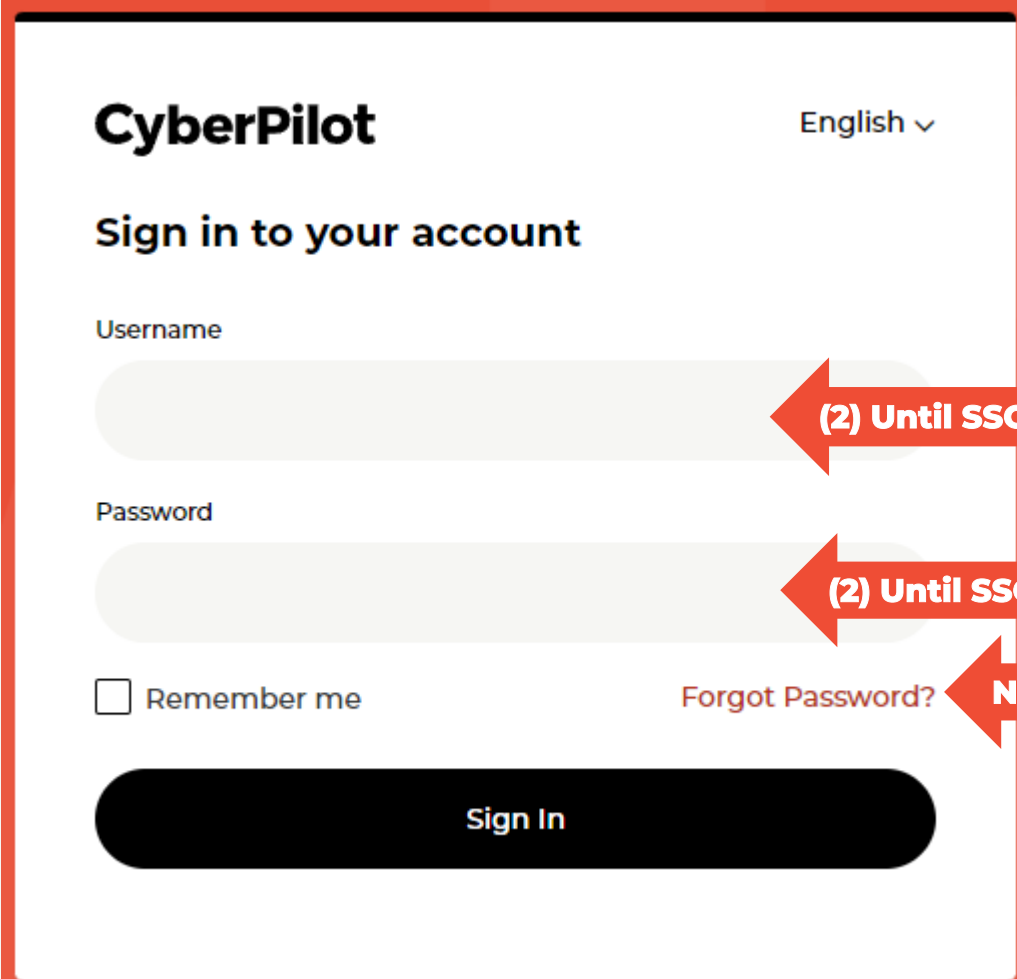
# CONFIGURING AD SYNC IN THE CYBERPILOT APP

## Step 1:

- Open the email you have received from CyberPilot where your subdomain is specified
- Note down the subdomain

**Step 2:** Log in to [https://\\*\\*\\*.app.cyberpilot.io](https://***.app.cyberpilot.io) (replace \*\*\* with your subdomain)

- Note until SSO is configured you still need to use your CyberPilot username and password.



The screenshot shows the CyberPilot login interface. At the top left is the 'CyberPilot' logo, and at the top right is a language selector set to 'English'. Below the logo is the heading 'Sign in to your account'. There are two input fields: 'Username' and 'Password'. Below the 'Username' field is a red arrow pointing left with the text '(2) Until SSO is configured use your CyberPilot username (your email)'. Below the 'Password' field is a red arrow pointing left with the text '(2) Until SSO is configured use your CyberPilot password'. Below the 'Remember me' checkbox is a red arrow pointing left with the text 'Note: Until SSO is configured you can reset your CyberPilot password'. At the bottom is a black 'Sign In' button. The CyberPilot logo is also present in the bottom right corner of the slide.

**CyberPilot** English ▾

**Sign in to your account**

Username

(2) Until SSO is configured use your CyberPilot username (your email)

Password

(2) Until SSO is configured use your CyberPilot password

Remember me [Forgot Password?](#)

Note: Until SSO is configured you can reset your CyberPilot password

**Sign In**

**CyberPilot**

## CONFIGURING AD SYNC IN THE CYBERPILOT APP

**Step 3:** Click on the user icon

**Step 4:** Click on "Go to Admin"



**Step 5:** Go to "Account" and Click "Azure AD"

**Step 6:** Enter the Application (Client) ID you have noted down – see *slide 30*

**Step 7:** Enter the Client Secret Value you have noted down – see *slide 32*

**Step 8:** Enter the Directory (Tenant) ID you have noted down – see *slide 30*

**Step 9:** Enter the Group (Object) ID you have noted down – see *slide 9*

**Step 10:** Slide the toggle to "Enable Sync"

**Step 11:** Click "Save"

The screenshot shows the CyberPilot interface. On the left is a dark sidebar with a menu. The main content area is titled "Account / Azure AD CyberPilot" and "GENERAL INFORMATION AZURE AD". Below this is the "Azure AD Configurations" section with several input fields and a toggle. Red arrows with numbers 5 through 11 point to the following elements:

- (5) Click "Account"**: Points to the "ACCOUNT" menu item in the sidebar.
- (5) Click "Azure AD"**: Points to the "AZURE AD" tab in the "GENERAL INFORMATION" section.
- (6) Enter Application (Client) ID - See slide 30**: Points to the "Application (Client) ID" input field.
- (7) Enter Client Secret Value - See slide 32**: Points to the "Client Secret > Value" input field.
- (8) Enter Directory (Tenant) ID - See slide 30**: Points to the "Directory (Tenant) ID" input field.
- (9) Enter Group (Object) ID - See slide 9**: Points to the "Group > Object ID" input field.
- (10) Slide to "Enable Sync"**: Points to the "Enable Sync" toggle switch.
- (11) Click "Save"**: Points to the "Save" button at the bottom.

When you have saved the Azure AD settings, you can initiate synchronization of users to test that synchronization works.

**Step 12:** Click "Force AD Sync"

**Step 13:** Check that synchronization is successful.

The screenshot shows the CyberPilot interface for configuring Azure AD. The left sidebar contains navigation options: Home, DASHBOARD, Trainings, AWARENESS, PHISHING, REPORTS, Settings, ACCOUNT, USERS, BRANCHES, and SYSTEM EMAILS. The main content area is titled "CyberPilot Azure AD" and has tabs for GENERAL INFORMATION, AZURE AD (selected), and SSO. A notification banner at the top states: "Last AD Sync was on Feb 06, 2024 11:30, status: Synced". Below this is the "Azure AD Configurations" section with fields for Application (Client) ID, Client Secret > Value, Directory (Tenant) ID, and Group > Object ID. The "Enable Sync" toggle is turned on. At the bottom are "Save" and "Force AD Sync" buttons. Two red arrows with text annotations point to the notification and the "Force AD Sync" button.

**(13) Check that synchronization is successful.**

**(12) Click Force AD Sync"**

Current Account ID:  
4f626ddf-b20c-4e45-b531-81e1c57a5473

**Step 14:** Click on "Users"

**Step 15:** Check that the users from the Azure AD Group are automatically created

*Note: It may take up to 24 hours before users are created*

**Step 16:** Click on "..."

**Step 17:** Click on "Edit"

The screenshot shows the CyberPilot web interface. On the left is a dark sidebar with navigation items: CyberPilot, Home, DASHBOARD, Trainings, AWARENESS, PHISHING, REPORTS, Settings, ACCOUNT, USERS, and BRANCHES. The 'USERS' item is highlighted. The main content area is titled 'Users' and contains a table of user records. A red callout box at the top center says '(15) Check that users are created as expected' with an arrow pointing to the table. A red callout box on the left says '(14) Click "Users"' with an arrow pointing to the sidebar. A red callout box on the right says '(16) Click "..."' with an arrow pointing to the ellipsis menu of a user row. A red callout box at the bottom right says '(17) Click "Edit"' with an arrow pointing to the 'Edit' option in the dropdown menu. The table has columns: Name, Username, Email, Updated, Active, Role, and Actions. The 'Updated' column shows 'Jan 22, 2024' for all rows. The 'Active' column shows 'Active' for all rows. The 'Role' column shows 'User' for all rows. The 'Actions' column contains a three-dot menu for each row.

Name ↑↓	Username	Email	Updated ↑↓	Active ↑↓	Role	Actions
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮
[blurred]	[blurred]	[blurred]	Jan 22, 2024	Active	User	⋮

## Step 18: Set the user role to "Admin" (if it is not already admin)

**CyberPilot**

CyberPilot

Home

DASHBOARD

Trainings

AWARENESS >

PHISHING >

REPORTS >

Settings

ACCOUNT

**USERS**

BRANCHES

Current Account ID:  
4f626ddf-b20c-4e45-b531-81e1c57a5473

### Edit User Sam de Jongh Hepworth

Username \*

First Name \*

Sam de Jongh

Last Name \*

Hepworth

Email \*

New Password

Role \*

Admin

Language \*

English [English]

Branch

Select

Set user as active

**(18) Make sure that your SSO user has role: "Admin"**

---

# ⑥ Configure Single Sign-On in Azure AD



**Step 1:** Login to the CyberPilot App, go to the admin view, and click on "Account"

**Step 2:** Click on "General Information"

**Step 3:** Note down the subdomain allocated to your company

Note: If a subdomain is not allocated to your company, please contact CyberPilot support.

The screenshot displays the CyberPilot Admin Dashboard. On the left sidebar, the 'Account' menu item is highlighted with a red arrow and the text '(1) Click "Account"'. The main content area shows the 'Account' settings page, with the 'GENERAL INFORMATION' tab selected, indicated by a red arrow and the text '(2) Click "General Information"'. Below the tab, the 'Name' field contains 'CyberPilot'. The 'Account Subdomain' field contains 'cyberpilot', which is highlighted with a red arrow and the text '(3) Note down the subdomain allocated to your company'.

**Step 4:** Go to <https://portal.azure.com/>

**Step 5:** Click on "Enterprise applications"

The screenshot shows the Microsoft Azure portal home page. A red arrow points to the address bar with the text "(4) Go to https://portal.azure.com/". Below the navigation bar, there are three main sections: "Start with an Azure free trial", "Manage Microsoft Entra ID", and "Access student benefits". Under the "Azure services" section, a red arrow points to the "Enterprise applications" icon with the text "(5) Click 'Enterprise applications'". The "Enterprise applications" icon is highlighted in blue. Below the "Enterprise applications" icon, there are several sub-icons: "password...", "registrations", "Group Values", "Center", and "machines".

portal.azure.com/#home


(4) Go to <https://portal.azure.com/>

Microsoft Azure Search resources, services, and docs (G+)

Lab08admin@CPaware... CYBERPILOT (MAIL.DK)

### Welcome to Azure!


Don't have a subscription? Check out the following options.



#### Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).


[Start](#)



#### Manage Microsoft Entra ID

Azure Active Directory is becoming Microsoft Entra ID. Secure access for everyone.

[View](#) [Learn more](#)




#### Access student benefits


Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#) [Learn more](#)


### Azure services




[Create a resource](#)




[Users](#)




[Groups](#)




[Enterprise applications](#)




[password...](#)




[registrations](#)




[Group Values](#)



[Center](#)



[machines](#)



[More services](#)

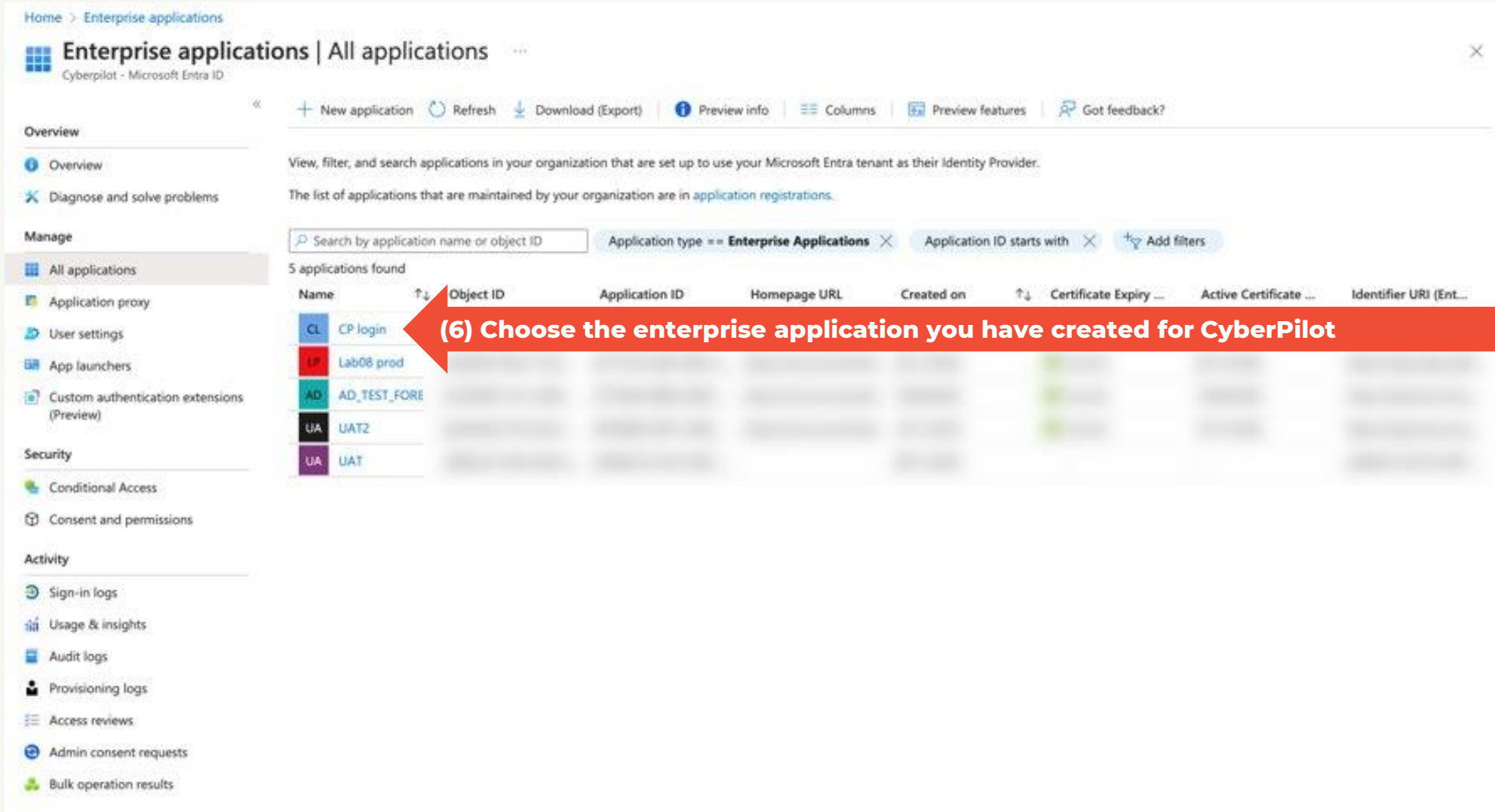
### Resources

[Recent](#) [Favorite](#)

Name	Type	Last Viewed
------	------	-------------

<https://portal.azure.com/#create/hub>

## Step 6: Choose the application you would like to use for syncing users and authorizing



Home > Enterprise applications

### Enterprise applications | All applications

Cyberpilot - Microsoft Entra ID

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Application proxy
- User settings
- App launchers
- Custom authentication extensions (Preview)

Security

- Conditional Access
- Consent and permissions

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews
- Admin consent requests
- Bulk operation results

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

5 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry	Active Certificate	Identifier URI (Ent...
CL CP login							
LP Lab08 prod							
AD AD_TEST_FORE							
UA UAT2							
UA UAT							

**(6) Choose the enterprise application you have created for CyberPilot**

## Step 7: Select "Single sign-on"

Microsoft Azure

Search resources, services, and docs (G+)

Lab08admin@CPaware...  
CYBERPILOT (MAIL/DK)

Home > Enterprise applications | All applications >

### UAT2 | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

**(7) Select "Single sign-on"**

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

#### Properties

UA

#### Getting Started

- 1. Assign users and groups**  
Provide specific users and groups access to the applications.  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Microsoft Entra credentials.  
[Get started](#)
- 3. Provision User Accounts**  
Automatically create and delete user accounts in the application.  
[Get started](#)
- 4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)
- 5. Self service**  
Enable users to request access to the application using their Microsoft Entra credentials.  
[Get started](#)

#### What's New

## Step 8: Under Basic SAML Configuration, click "Edit"

The screenshot displays the Azure portal interface for configuring SAML-based Sign-on for an application named UAT2. The left-hand navigation pane is visible, with 'Single sign-on' selected. The main content area is titled 'Set up Single Sign-On with SAML' and includes an introductory paragraph and a link to the configuration guide. Below this, there are three numbered sections:

- Basic SAML Configuration**: This section contains fields for Identifier (Entity ID), Reply URL (Assertion Consumer Service URL), Sign on URL (Optional), Relay State (Optional), and Logout URL (Optional). An 'Edit' button is located to the right of this section.
- Attributes & Claims**: This section lists attributes and their corresponding values, such as givenname (user.givenname), surname (user.surname), emailaddress (user.mail), name (user.userprincipalname), and Unique User Identifier (user.userprincipalname). An 'Edit' button is located to the right of this section.
- SAML Certificates**: This section shows the Token signing certificate, its status (Active), and its thumbprint. An 'Edit' button is located to the right of this section.

A red arrow points from the text '(8) "Edit" Basic SAML Configuration' to the 'Edit' button in the Basic SAML Configuration section.

**Step 9:** Add Identifier URL: [https://login.app.cyberpilot.io/realms/\\*\\*/](https://login.app.cyberpilot.io/realms/**/)

**Step 10:** Add Reply URL: [https://login.app.cyberpilot.io/realms/\\*\\*/broker/saml/endpoint](https://login.app.cyberpilot.io/realms/**/broker/saml/endpoint)

**Step 11:** Click "Save"

**Important:** Replace **\*\*\*** with your subdomain - see slide 34

Microsoft Azure

Home > Enterprise applications | All applications > UAT2

UAT2 | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Basic SAML Configuration

Save Got feedback?

Identifier (Entity ID) \*

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://login.app.cyberpilot.io/realms/subdomainname

Add identifier

Reply URL (Assertion Consumer Service URL) \*

The reply URL is where the application expects to receive the authentication tokens. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

https://login.app.cyberpilot.io/realms/subdomainname/broker/saml/endpoint

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

1 Basic SAML Configuration

Identifier (Entity ID) https://

Reply URL (Assertion Consumer Service URL) https://

Sign on URL Option

Relay State (Optional) Option

Logout Url (Optional) Option

2 Attributes & Claims

givenname user.gi

surname user.su

emailaddress user.mi

name user.us

Unique User Identifier user.us

3 SAML Certificates

Token signing certificate

Status Active

Thumbprint D47A0,

Expiration 14/11/;

(11) Click "Save"

(9) Add identifier URL: [https://login.app.cyberpilot.io/realms/\\*\\*/](https://login.app.cyberpilot.io/realms/**/)

(10) Add identifier URL: [https://login.app.cyberpilot.io/realms/\\*\\*/broker/saml/endpoint](https://login.app.cyberpilot.io/realms/**/broker/saml/endpoint)

## Step 12: Copy App Federation Metadata URL for later (when setting up SSO in CyberPilot App)

*You need to paste the metadata URL later!*

Microsoft Azure

Home > Enterprise applications | All applications > AD\_TEST\_FORENEDE

### AD\_TEST\_FORENEDE | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

#### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating AD\_TEST\_FORENEDE.

- Basic SAML Configuration**
  - Identifier (Entity ID)
  - Reply URL (Assertion Consumer Service URL)
  - Sign on URL
  - Relay State (Optional)
  - Logout Url (Optional)
- Attributes & Claims**

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

<b>Token signing certificate</b>	Active
Status	Active
Thumbprint	D995E8A3ADE5FC37F0179A3ED64EE2ED8400C0CA
Expiration	19/09/2026, 15:02:57
Notification Email	CyberAdmin@CPawareness.onmicrosoft.com
App Federation Metadata Url	<code>https://login.microsoftonline.com/2fd8b3b8-9ae6...</code>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

**(12) Copy App Federation Metadata URL**

---

# ⑦ Configure Single Sign-On in the CyberPilot App



# CONFIGURING SINGLE SIGN-ON IN THE CYBERPILOT APP

**Step 1:** In Admin mode, go to "Account"

**Step 2:** Click on "SSO"

**Step 3:** Enable "Uses SSO"

**Step 4:** Select "Import config"

**Step 5:** Paste App Federation Metadata URL from Slide 40

**Step 6:** Click "Save"

The screenshot shows the CyberPilot Admin interface. On the left is a dark sidebar with a menu. The main content area is white and shows the 'SSO Config' page. Red arrows with numbers 1 through 6 point to specific elements: (1) 'ACCOUNT' in the sidebar, (2) 'SSO' in the top navigation, (3) the 'Uses SSO' toggle switch, (4) the 'Import config' radio button, (5) the 'Import URL' input field, and (6) the 'Save' button at the bottom.

**CyberPilot**

CyberPilot

Account / SSO CyberPilot

GENERAL INFORMATION AZURE AD SSO

**(2) Click "SSO"**

**SSO Config**

Uses SSO **(3) Enable "Uses SSO"**

Manual config  Import config **(4) Select "Import config"**

Display Name

Import URL \*

**(5) Paste App Federation Metadata URL from slide 47**

Save **(6) Click "Save"**

**(1) Click "Account"**

**Step 7:** Go to [https://\\*\\*\\*.app.cyberpilot.io](https://***.app.cyberpilot.io) (replace \*\*\* with your subdomain) - see slide 34

**Step 8:** Login with your company email and password

*Note: We recommend that you also do this test in incognito/private mode in your browser.*

*Note: If SSO is not working, you may be unable to login. In this case contact CyberPilot support.*

The image shows a sequence of two screenshots. The first screenshot is a browser window displaying the Microsoft login page. The address bar shows the URL `https://***.app.cyberpilot.io`. A red arrow points from a red callout box below to the address bar. The login page has the Microsoft logo, the text "Log på", and a text input field containing "Mail, telefon eller Skype". Below the input field is a link that says "Kan du ikke få adgang til din konto?". At the bottom of the login form are two buttons: "Tilbage" (grey) and "Næste" (blue). A red arrow points from a red callout box below to the "Næste" button. The second screenshot shows the CyberPilot dashboard. The dashboard has a dark sidebar with navigation options: Home, DASHBOARD, Trainings, AWARENESS, PHISHING, REPORTS, Settings, ACCOUNT, USERS, and BRANCHES. The main content area is titled "Dashboard" and contains several metrics: ACTIVE USERS (40), PAST PHISHING CAMPAIGNS (8), ACTIVE PHISHING CAMPAIGNS (0), COURSE COMPLETION (99%), and USER STATUS (73%). The COURSE COMPLETION section includes a table with the following data:

Metric	Value
Available Courses	51
Enrolled Courses	51
Total Enrollments	1084
Total Completions	1072

The USER STATUS section includes a table with the following data:

Metric	Value
Users With Courses Enrolled	40
Users Without Courses	0
Have Completed All Courses	29
Have Not Completed All Courses	11

At the bottom of the sidebar, it says "Current Account ID:".

**(8) Login with your company email and password**

---

# ⑧ Whitelist Notification emails from the CyberPilot App

# Whitelist notification emails from the CyberPilot App

To ensure that emails from the CyberPilot App will not end up in your spam folders, we recommend that you whitelist emails from the CyberPilot App in your spam emails filter.

Emails from the CyberPilot App always come from [notify@app.cyberpilot.io](mailto:notify@app.cyberpilot.io), so you only need to whitelist one sender address. Other emails from CyberPilot always comes from the domains **cyberpilot.dk** and **cyberpilot.io** and we recommend also whitelisting these domains.

# Microsoft Office 365 / Defender Guide

**Step 1:** Go to <https://security.microsoft.com/>

**Step 2:** Click on "Policies & Rules"

The screenshot shows the Microsoft Defender web interface. A red arrow points to the address bar with the text "(1) Go to https://security.microsoft.com/". Another red arrow points to the "Policies & rules" menu item in the left sidebar with the text "(2) Click on 'Policies & Rules'".

**Home**

## Welcome to Microsoft Defender

[Intro](#) [Next steps](#) [Give feedback](#)

Respond to threats and manage security across your identities, data, devices, apps, and infrastructure. [Learn more about the unified experience](#)

[Next](#) [Close](#)

[What's new?](#) [Community](#) [+ Add cards](#)

### Microsoft Secure Score

**Secure Score: 35.37%**  
95.15/269 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 12/04

Category	Percentage
Identity	82.21%
Data	0%
Apps	22.61%

### Insider Risk Management

**Did you know businesses are spending \$500,000 per breach?**

Source: Communication Compliance Microsoft Market Research, May 2021

Start identifying insider risks within your organization with Microsoft Purview Insider Risk Management today. Enable an analytics scan to receive a custom report of potential risk areas for your users.

### Microsoft Defender XDR

**Get Microsoft Defender XDR**

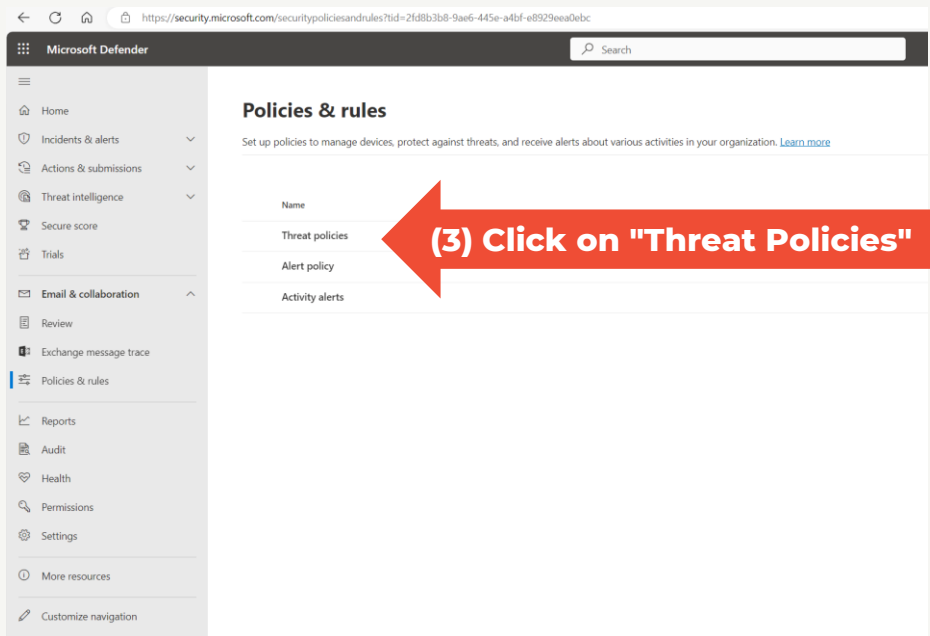
Check that you have an eligible license and the right permissions to get started with new, unified capabilities - incident management, automated investigations, and advanced hunting on Office 365, your endpoints, and your identities.

[Learn how to get started](#)

# Microsoft Office 365 / Defender Guide

**Step 3:** Click on "Threat Policies"

**Step 4:** Click on "Anti-spam"



Microsoft Defender

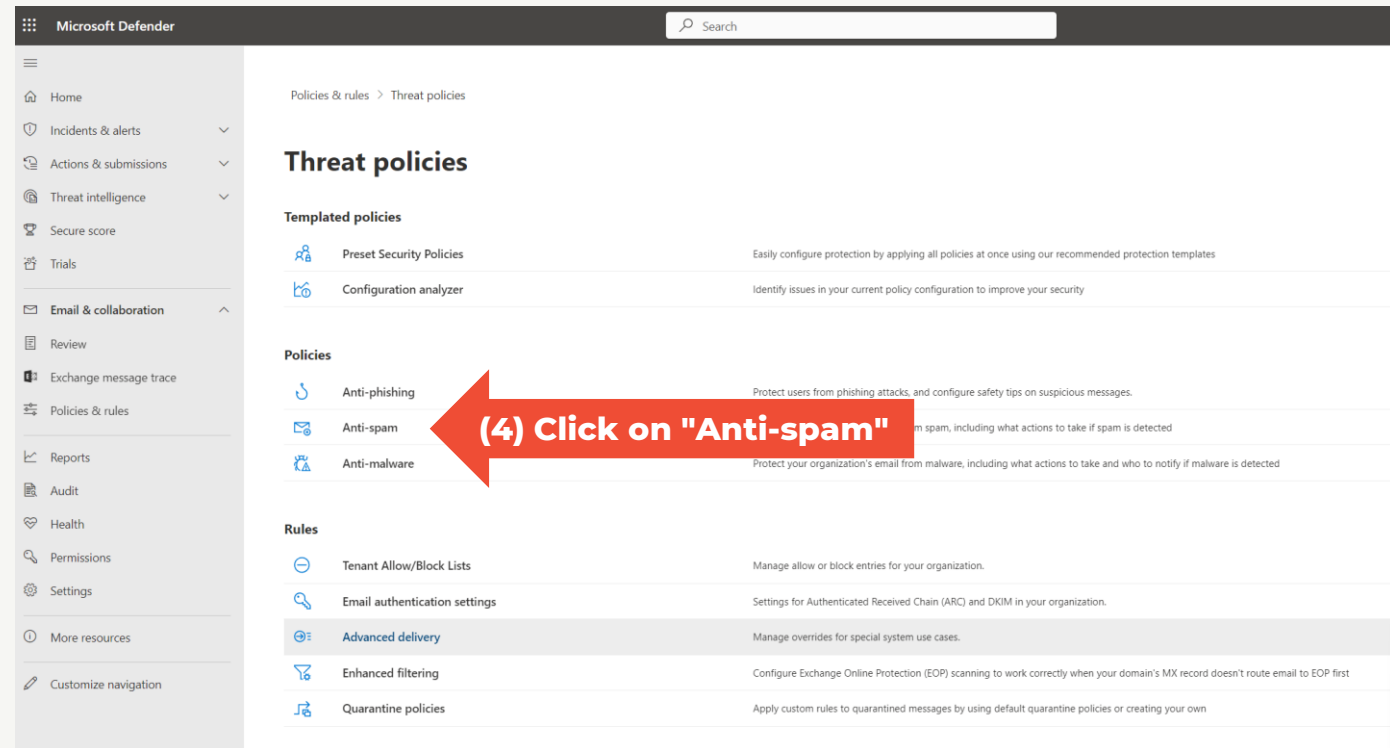
Search

### Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. [Learn more](#)

Name
Threat policies
Alert policy
Activity alerts

**(3) Click on "Threat Policies"**



Microsoft Defender

Search

Policies & rules > Threat policies

## Threat policies

### Templated policies

- Preset Security Policies: Easily configure protection by applying all policies at once using our recommended protection templates
- Configuration analyzer: Identify issues in your current policy configuration to improve your security

### Policies

- Anti-phishing: Protect users from phishing attacks, and configure safety tips on suspicious messages.
- Anti-spam: Protect your organization's email from spam, including what actions to take if spam is detected
- Anti-malware: Protect your organization's email from malware, including what actions to take and who to notify if malware is detected

### Rules

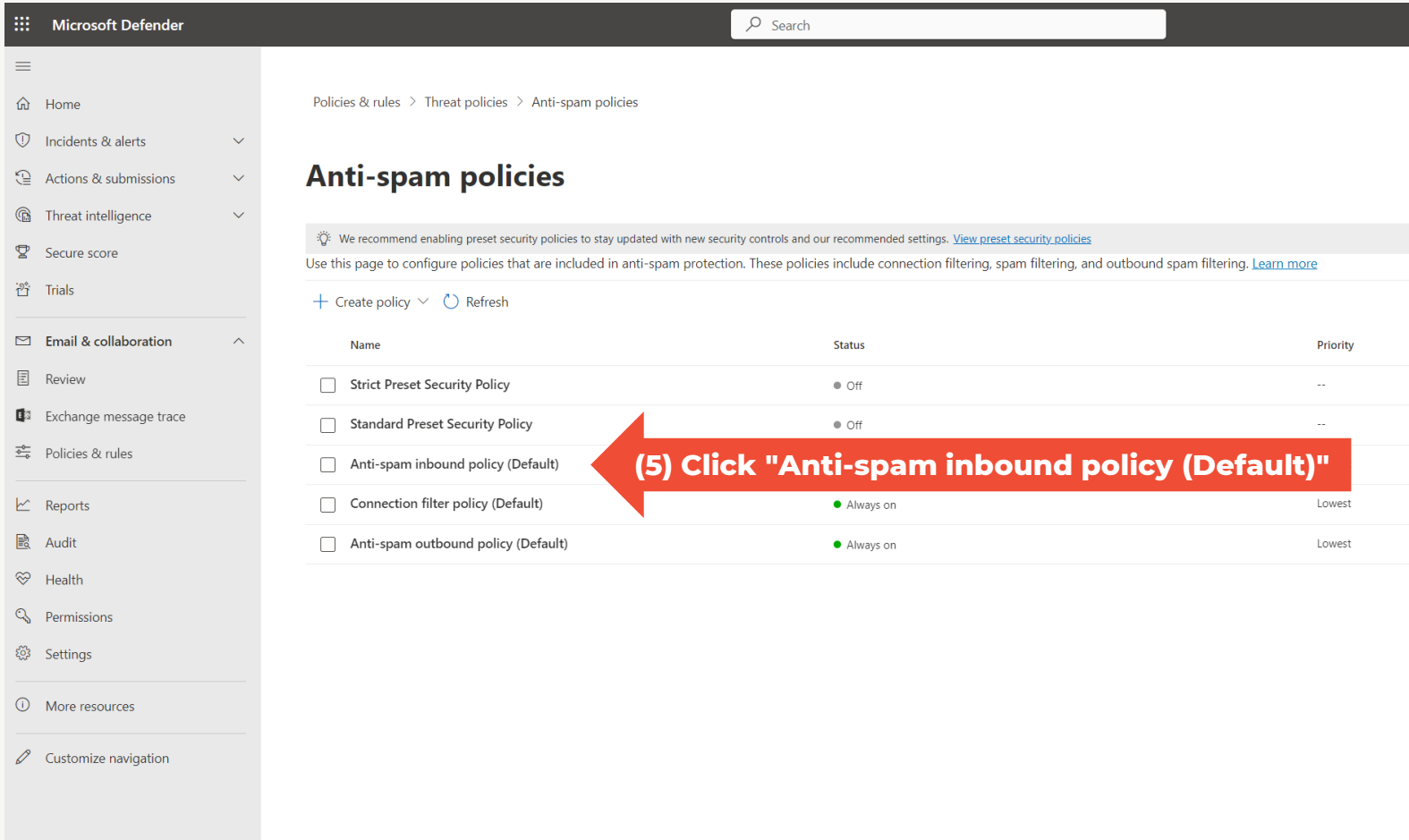
- Tenant Allow/Block Lists: Manage allow or block entries for your organization.
- Email authentication settings: Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
- Advanced delivery: Manage overrides for special system use cases.
- Enhanced filtering: Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
- Quarantine policies: Apply custom rules to quarantined messages by using default quarantine policies or creating your own

**(4) Click on "Anti-spam"**

# Microsoft Office 365 / Defender Guide

## Step 5: Click on "Anti-spam inbound policy (Default)"

*Note: If you have customized Defender Anti-spam inbound policies, you may have to edit another policy*



The screenshot shows the Microsoft Defender console interface. The left sidebar contains navigation options: Home, Incidents & alerts, Actions & submissions, Threat intelligence, Secure score, Trials, Email & collaboration, Review, Exchange message trace, Policies & rules, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area is titled 'Anti-spam policies' and includes a breadcrumb trail: Policies & rules > Threat policies > Anti-spam policies. A notification banner suggests enabling preset security policies. Below this, there are '+ Create policy' and 'Refresh' buttons. A table lists the following policies:

Name	Status	Priority
<input type="checkbox"/> Strict Preset Security Policy	● Off	--
<input type="checkbox"/> Standard Preset Security Policy	● Off	--
<input type="checkbox"/> Anti-spam inbound policy (Default)	● Always on	Lowest
<input type="checkbox"/> Connection filter policy (Default)	● Always on	Lowest
<input type="checkbox"/> Anti-spam outbound policy (Default)	● Always on	Lowest

A red arrow points to the 'Anti-spam inbound policy (Default)' row, with the text '(5) Click "Anti-spam inbound policy (Default)"' overlaid on it.

# Microsoft Office 365 / Defender Guide

**Step 6:** Scroll down

**Step 7:** Click "Edit allowed and blocked senders and domains"

Microsoft Defender console showing the 'Anti-spam policies' page. The 'Anti-spam inbound policy (Default)' is selected. A red arrow points to the 'Edit description' link.

**(6) Scroll down**

Microsoft Defender console showing the 'Anti-spam inbound policy (Default)' configuration page. The 'Edit allowed and blocked senders and domains' link is highlighted. A red arrow points to this link.

**(7) Click "Edit allowed and blocked senders and domains"**



# Microsoft Office 365 / Defender Guide

**Step 8:** In section "Allowed" click on "Manage sender(s)"

The screenshot shows the Microsoft Defender console interface. The left sidebar contains navigation options: Home, Incidents & alerts, Actions & submissions, Threat intelligence, Secure score, Trials, Email & collaboration, Review, Exchange message trace, Policies & rules, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area displays 'Anti-spam policies' with a breadcrumb trail: Policies & rules > Threat policies > Anti-spam policies. A red arrow points to the text '(8) Manage allowed senders' overlaid on the page. Below this, a table lists the policies:

Name	Status
<input type="checkbox"/> Strict Preset Security Policy	● Off
<input type="checkbox"/> Standard Preset Security Policy	● Off
<input checked="" type="checkbox"/> Anti-spam inbound policy (Default)	● Always on
<input type="checkbox"/> Connection filter policy (Default)	● Always on
<input type="checkbox"/> Anti-spam outbound policy (Default)	● Always on

The right-hand pane shows the configuration for the selected policy, titled 'Allowed and blocked senders and domains'. It is divided into 'Allowed' and 'Blocked' sections. Under 'Allowed', there are 'Senders (3)' and 'Domains (0)'. Under 'Blocked', there are 'Senders (0)' and 'Domains (0)'. Each section includes a description and a link to manage the items. At the bottom of the pane are 'Save' and 'Cancel' buttons.

# Microsoft Office 365 / Defender Guide

**Step 9:** Type `notify@app.cyberpilot.io` and press ENTER

**Step 10:** Click "Add Senders"

The screenshot shows the Microsoft Defender console interface. The main area displays 'Anti-spam policies' with a list of policies. A modal dialog box titled 'Add senders' is open on the right. The dialog contains a text input field with the value 'notify@app.cyberpilot.io' and a blue 'Add senders' button at the bottom. Two red arrows are overlaid on the image: one pointing to the 'Add senders' button and another pointing to the input field.

**(9) Type "notify@app.cyberpilot.io" and press ENTER**

**(10) Click "Add senders"**

# Microsoft Office 365 / Defender Guide

**Step 11:** In section "Allowed" click on "Allowed domains"

The screenshot shows the Microsoft Defender console interface. The left sidebar contains navigation options: Home, Incidents & alerts, Actions & submissions, Threat intelligence, Secure score, Trials, Email & collaboration, Review, Exchange message trace, Policies & rules, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area displays 'Anti-spam policies' with a breadcrumb trail: Policies & rules > Threat policies > Anti-spam policies. A table lists several policies, with 'Anti-spam inbound policy (Default)' selected. A red arrow points from the text '(11) Manage allowed domains' to the 'Allowed domains' link in the 'Allowed and blocked senders and domains' pane. This pane shows 'Allowed' senders (3) and domains (0), and 'Blocked' senders (0) and domains (0). At the bottom of the pane are 'Save' and 'Cancel' buttons.

Name	Status
<input type="checkbox"/> Strict Preset Security Policy	● Off
<input type="checkbox"/> Standard Preset Security Policy	● Off
<input checked="" type="checkbox"/> Anti-spam inbound policy (Default)	● Always on
<input type="checkbox"/> Connection filter policy (Default)	● Always on
<input type="checkbox"/> Anti-spam outbound policy (Default)	● Always on

**(11) Manage allowed domains**

**Allowed and blocked senders and domains**

**Allowed**

**Senders (3)**  
Always deliver messages from these senders  
[Manage 3 sender\(s\)](#)

**Domains (0)**  
Always deliver messages from these domains  
[Allow domains](#)

**Blocked**

**Senders (0)**  
Always mark messages from these senders as spam  
[Manage 0 sender\(s\)](#)

**Domains (0)**  
Always mark messages from these domains as spam  
[Block domains](#)

**Save** **Cancel**

# Microsoft Office 365 / Defender Guide

**Step 12:** Type cyberpilot.io and press ENTER

**Step 13:** Type cyberpilot.dk and press ENTER

**Step 14:** Click "Add domains"

The screenshot shows the Microsoft Defender console interface. A dialog box titled "Add custom domains" is open, allowing the user to enter custom domains. The dialog box contains a search bar with the placeholder text "Enter a custom domain". Below the search bar, two domain tags are visible: "cyberpilot.dk" and "cyberpilot.io". At the bottom of the dialog box, there are two buttons: "Add domains" and "Cancel".

**(12) Type "cyberpilot.io" and press ENTER**

**(13) Type "cyberpilot.dk" and press ENTER**

**(14) Click "Add domains"**

# Microsoft Office 365 / Defender Guide

**Step 15:** Click "Done"

**Step 16:** Click "Save"

The screenshot shows the Microsoft Defender console with the 'Anti-spam policies' page open. A modal dialog titled 'Manage allowed senders' is displayed. The dialog contains a search bar with '1 item' and a list of sender addresses. The address 'notify@app.cyberpilot.io' is listed. At the bottom of the dialog, there are 'Done' and 'Cancel' buttons. A red arrow points to the 'Done' button with the text '(15) Click "Done"'. The background shows the 'Anti-spam policies' page with a table of policies:

Name	Status
<input type="checkbox"/> Strict Preset Security Policy	● Off
<input type="checkbox"/> Standard Preset Security Policy	● Off
<input checked="" type="checkbox"/> Anti-spam inbound policy (Default)	● Always on
<input type="checkbox"/> Connection filter policy (Default)	● Always on
<input type="checkbox"/> Anti-spam outbound policy (Default)	● Always on

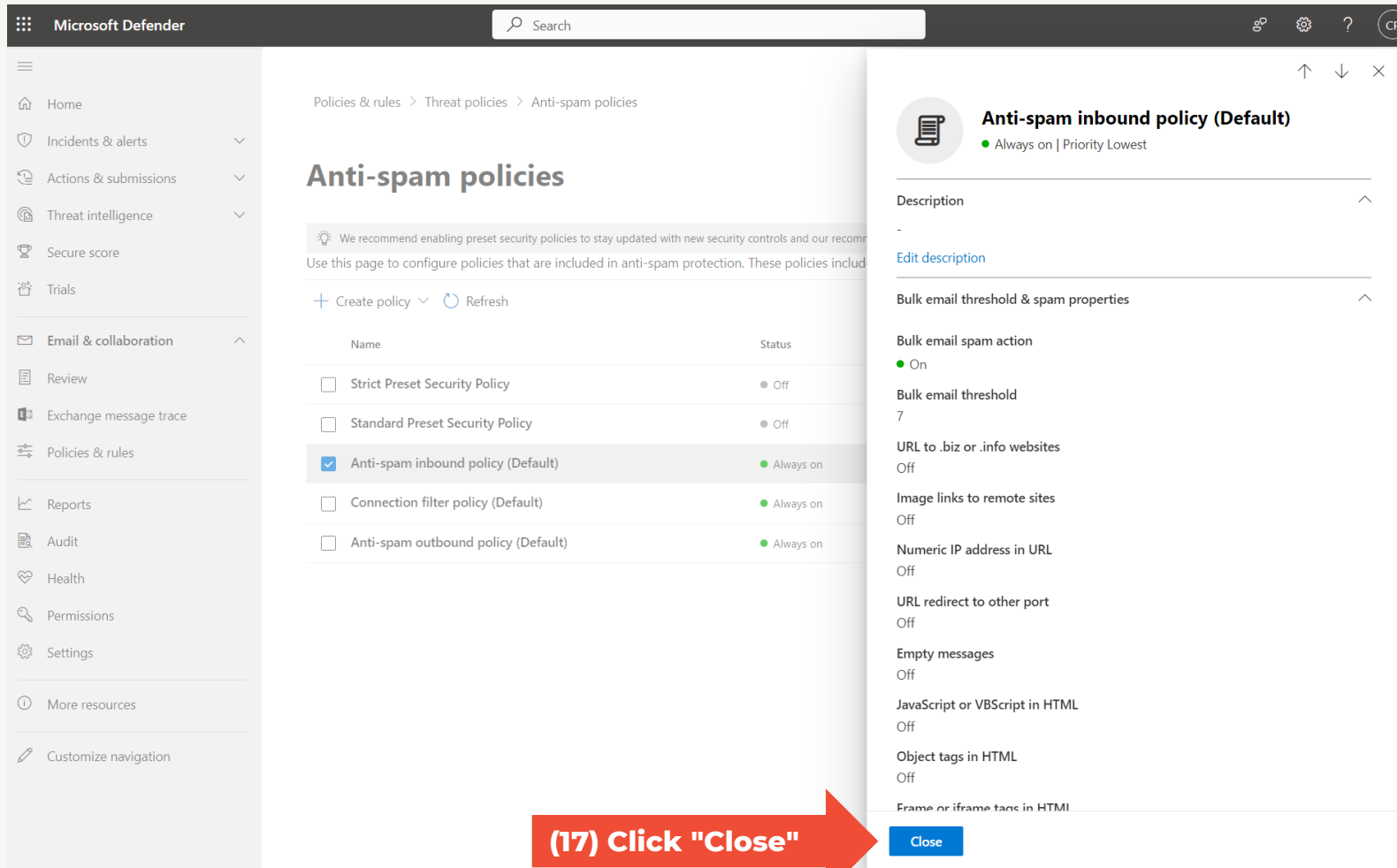
The screenshot shows the Microsoft Defender console with the 'Anti-spam policies' page open. A modal dialog titled 'Allowed and blocked senders and domains' is displayed. The dialog shows sections for 'Allowed' and 'Blocked' senders and domains. The 'Allowed' section lists 'Senders (1)' and 'Domains (0)'. The 'Blocked' section lists 'Senders (0)' and 'Domains (0)'. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons. A red arrow points to the 'Save' button with the text '(16) Click "Save"'. The background shows the 'Anti-spam policies' page with a table of policies:

Name	Status
<input type="checkbox"/> Strict Preset Security Policy	● Off
<input type="checkbox"/> Standard Preset Security Policy	● Off
<input checked="" type="checkbox"/> Anti-spam inbound policy (Default)	● Always on
<input type="checkbox"/> Connection filter policy (Default)	● Always on
<input type="checkbox"/> Anti-spam outbound policy (Default)	● Always on

# Microsoft Office 365 / Defender Guide

## Step 17: Click on "Close"

You have now whitelisted emails from notify@app.cyberpilot.io, cyberpilot.dk and cyberpilot.io to ensure that emails from CyberPilot will not end up in your spam folders



The screenshot shows the Microsoft Defender console interface. The left sidebar contains navigation options like Home, Incidents & alerts, Actions & submissions, Threat intelligence, Secure score, Trials, Email & collaboration, Reports, Audit, Health, Permissions, Settings, and More resources. The main content area displays the 'Anti-spam policies' configuration page. A table lists several policies, with 'Anti-spam inbound policy (Default)' selected and its status set to 'Always on'. A right-hand pane shows the configuration details for this policy, including a 'Close' button at the bottom. A red arrow points to this button with the text '(17) Click "Close"'. The breadcrumb path at the top reads 'Policies & rules > Threat policies > Anti-spam policies'.

Name	Status
<input type="checkbox"/> Strict Preset Security Policy	● Off
<input type="checkbox"/> Standard Preset Security Policy	● Off
<input checked="" type="checkbox"/> Anti-spam inbound policy (Default)	● Always on
<input type="checkbox"/> Connection filter policy (Default)	● Always on
<input type="checkbox"/> Anti-spam outbound policy (Default)	● Always on

---

# 9 Notify CyberPilot

# Notify CyberPilot

Thanks for completing our guide 🙌

Please let your CyberPilot contact know, so that we can finalize your onboarding.