Migration Guide for CyberPilot AD-Sync and Single Sign-On with Azure AD Cloud

CyberPilot

Note!

This guide is for CyberPilot customers who use a single AD-integration and a single AD-group to synchronize and authorize users.

In this guide we refer to the old CyberPilot platform as **eFront** and the new platform as **CyberPilot App**.

- **eFront** is the platform with the URL **https://***.security-platform.dk/**
- **CyberPilot App** is the platform with the URL **https://***.app.cyberpilot.io/**

Replace ***** *in the above URLs with the subdomain assigned to your company.*

You can also see your subdomain in eFront on the branch page. The field is called "Domain name for branch". Your subdomain is part of your domain name example www.*****.security-platform.dk (replace ***** with your subdomain).

Note!

When you migrate to the CyberPilot App we make sure to migrate:

- All users including their choice of language. Note that courses are available in the same languages as in eFront (the old platform), but the user interface of the CyberPilot App is English and Danish.
- All your user’s course enrollments and their course completion history.
- All your phishing simulation campaigns and the results of these.
- All your branches and the users assigned to these.
- All our courses are available on the new platform. If you have created your own courses we convert them, so that they are also available on the new platform.
- Your AD-Sync and SSO configuration. You must only update a few settings in your own Azure AD.

Contents

1. Update CyberPilot Enterprise Application SSO in Azure AD
2. Azure AD User Properties
3. Whitelist Notification emails from the CyberPilot App
4. Notify CyberPilot that you are ready for final migration step
5. Day of final migration step

➊ Update CyberPilot Enterprise Application SSO in Azure AD

CyberPilot

Update CyberPilot Enterprise Application SSO in Azure AD

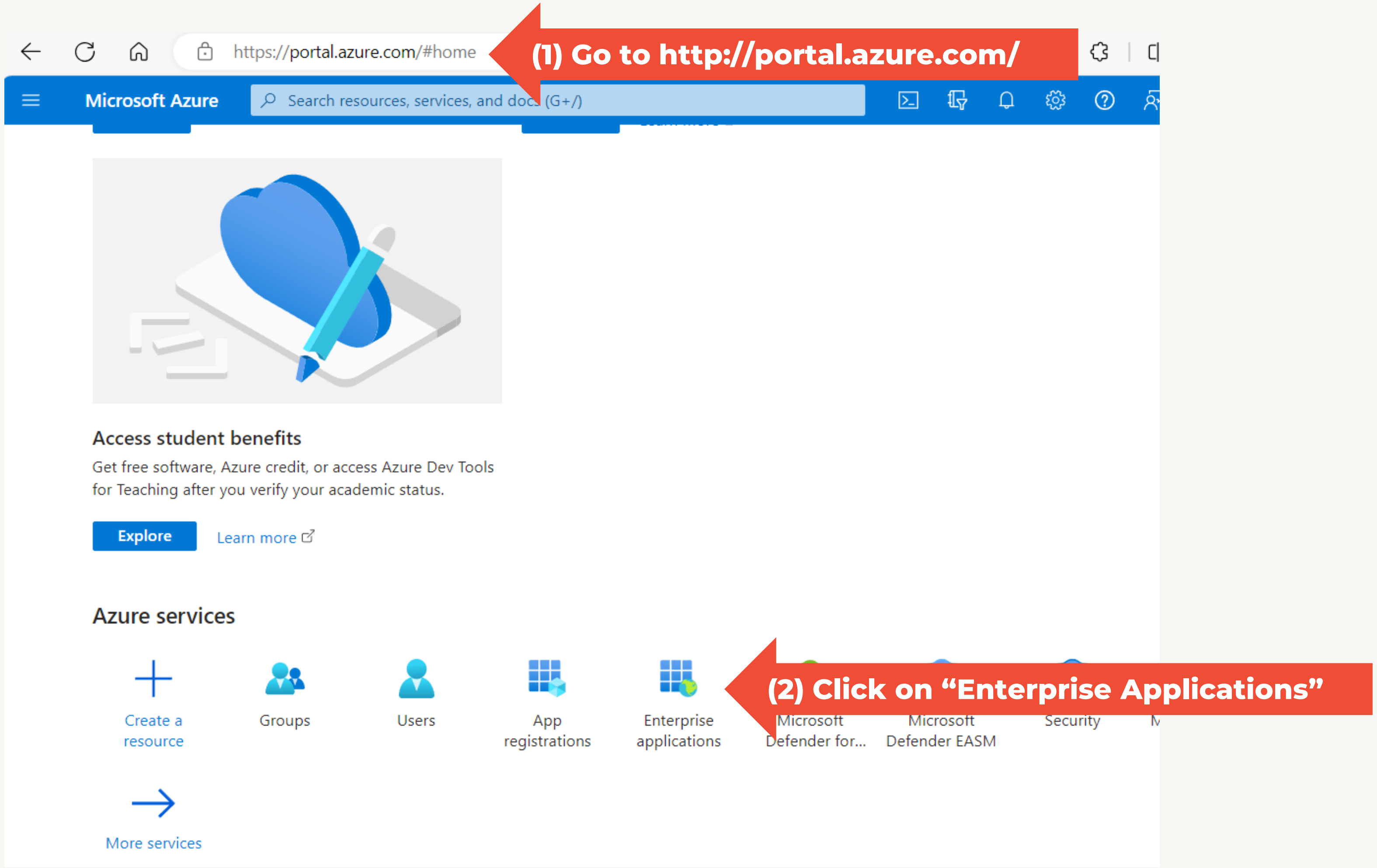
When you configured AD-integration and SSO for the old CyberPilot platform (eFront) you created an Azure AD Enterprise Application for CyberPilot.

This guide assumes that you will be reusing this Enterprise Application for the AD-integration to the new platform (CyberPilot App).

LOCATING THE CYBERPILOT ENTERPRISE APPLICATION

Step 1: Go to https://portal.azure.com/

Step 2: Click on “Enterprise Applications"



(1) Go to http://portal.azure.com/

(2) Click on “Enterprise Applications”

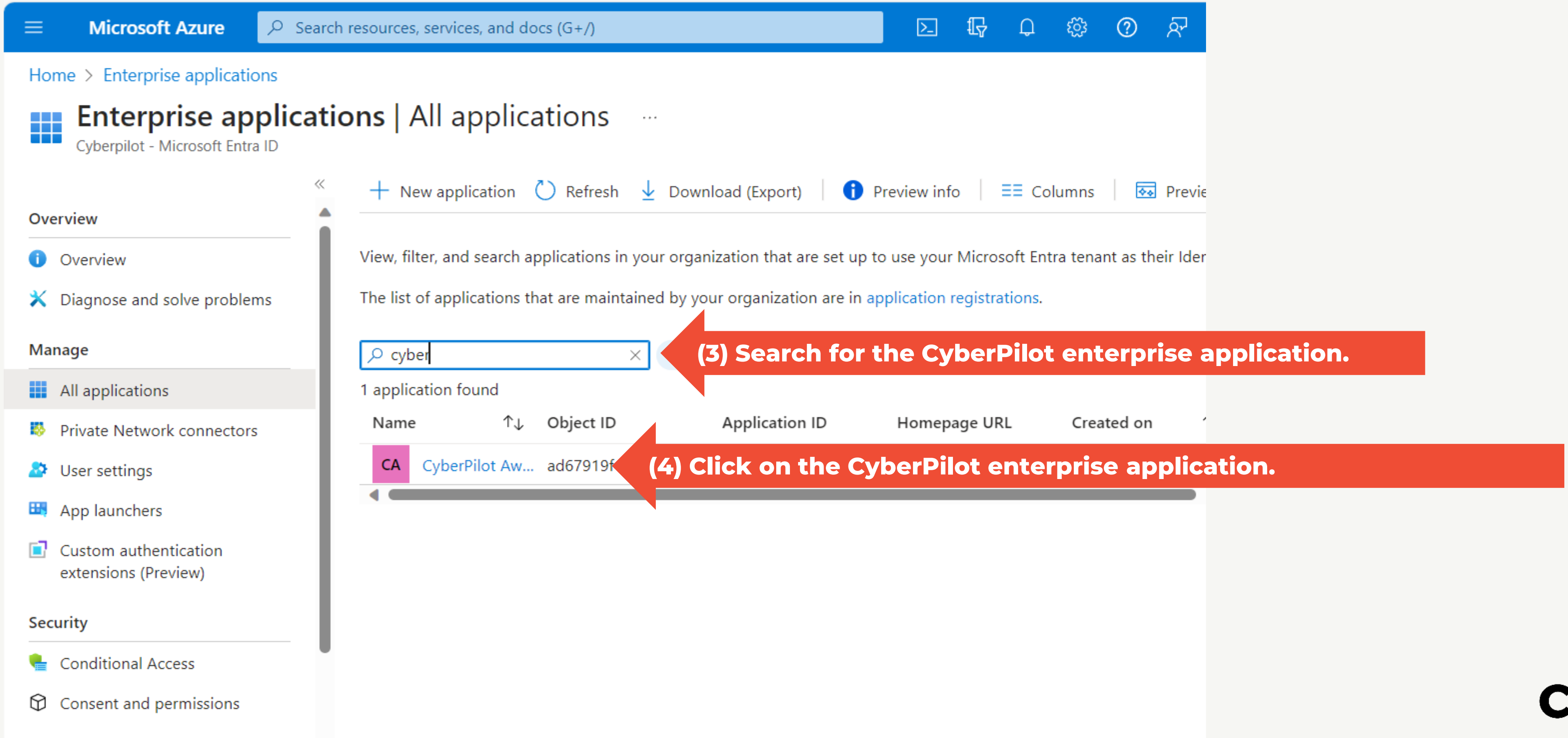
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
Explore
Learn more
Azure services
Create a resource
Groups
Users
App registrations
Enterprise applications
Microsoft Defender for...
Microsoft Defender EASM
Security
More services

LOCATING THE CYBERPILOT ENTERPRISE APPLICATION

Step 3: Search for the CyberPilot enterprise application.

Most likely you have “CyberPilot” and/or “Awareness” in the name.

Step 4: Click on CyberPilot enterprise application.



Home > Enterprise applications

Enterprise applications | All applications

Cyberpilot - Microsoft Entra ID

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

The list of applications that are maintained by your organization are in application registrations.

cyber

1 application found

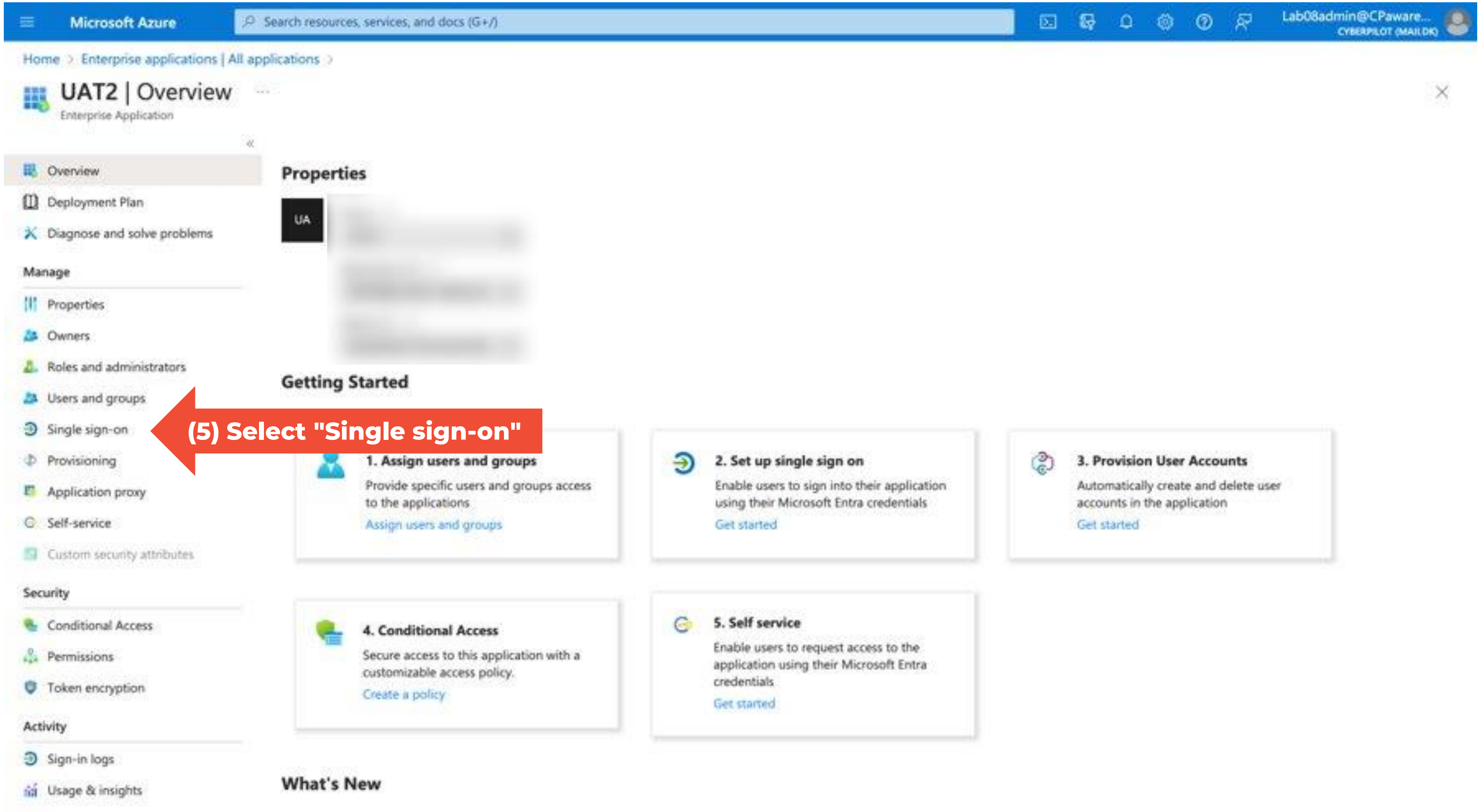
Name	Object ID	Application ID	Homepage URL	Created on
CA CyberPilot Aw...	ad67919f			

(3) Search for the CyberPilot enterprise application.

(4) Click on the CyberPilot enterprise application.

CyberPilot

Step 5: Select "Single sign-on"



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

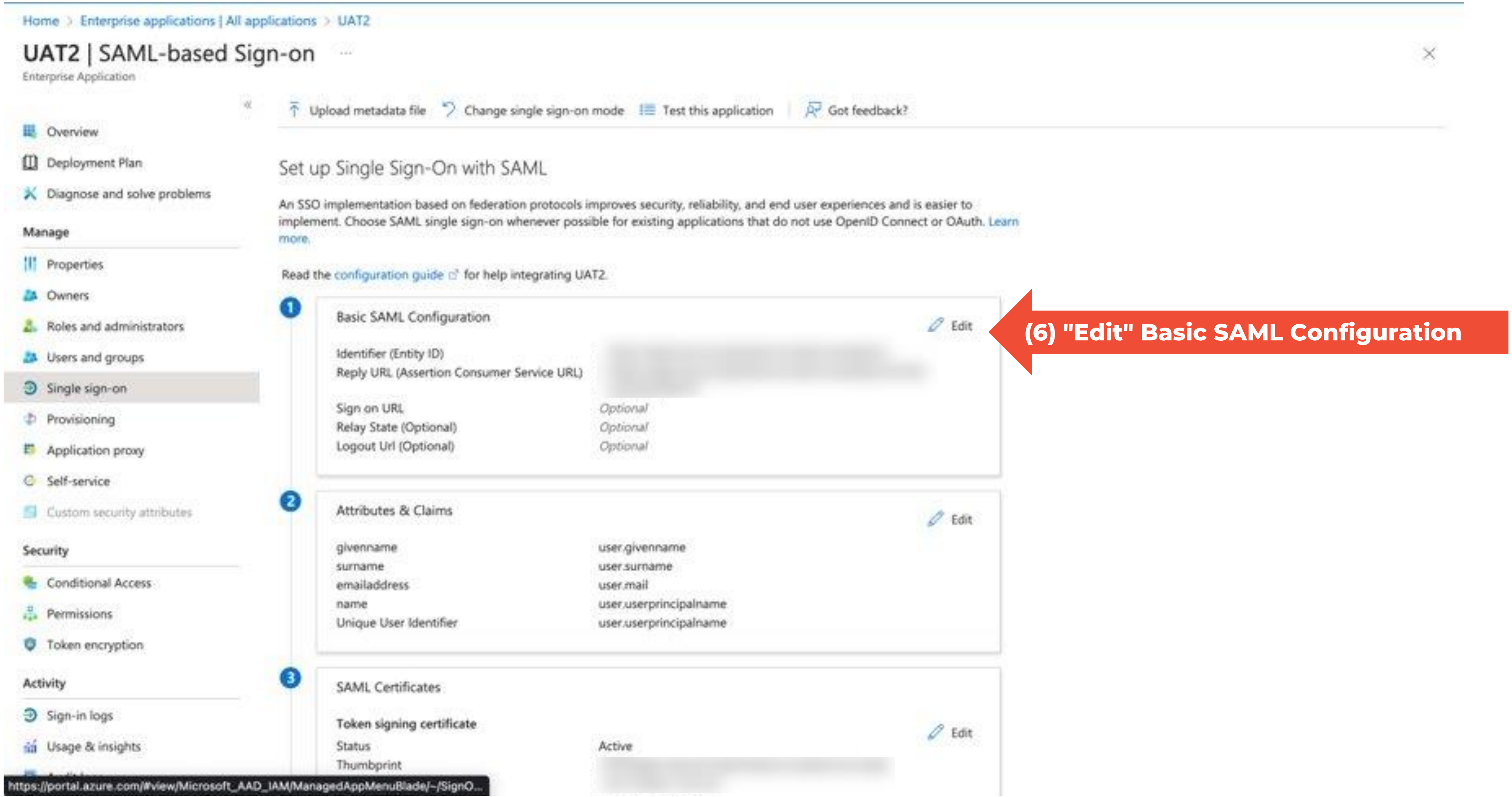
4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Microsoft Entra credentials
Get started

(5) Select "Single sign-on"

CyberPilot

Step 6: Under Basic SAML Configuration, click "Edit"



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 UAT2.

1 Basic SAML Configuration

Identifier (Entity ID)	[redacted]
Reply URL (Assertion Consumer Service URL)	
Sign on URL	*Optional*
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	[redacted]

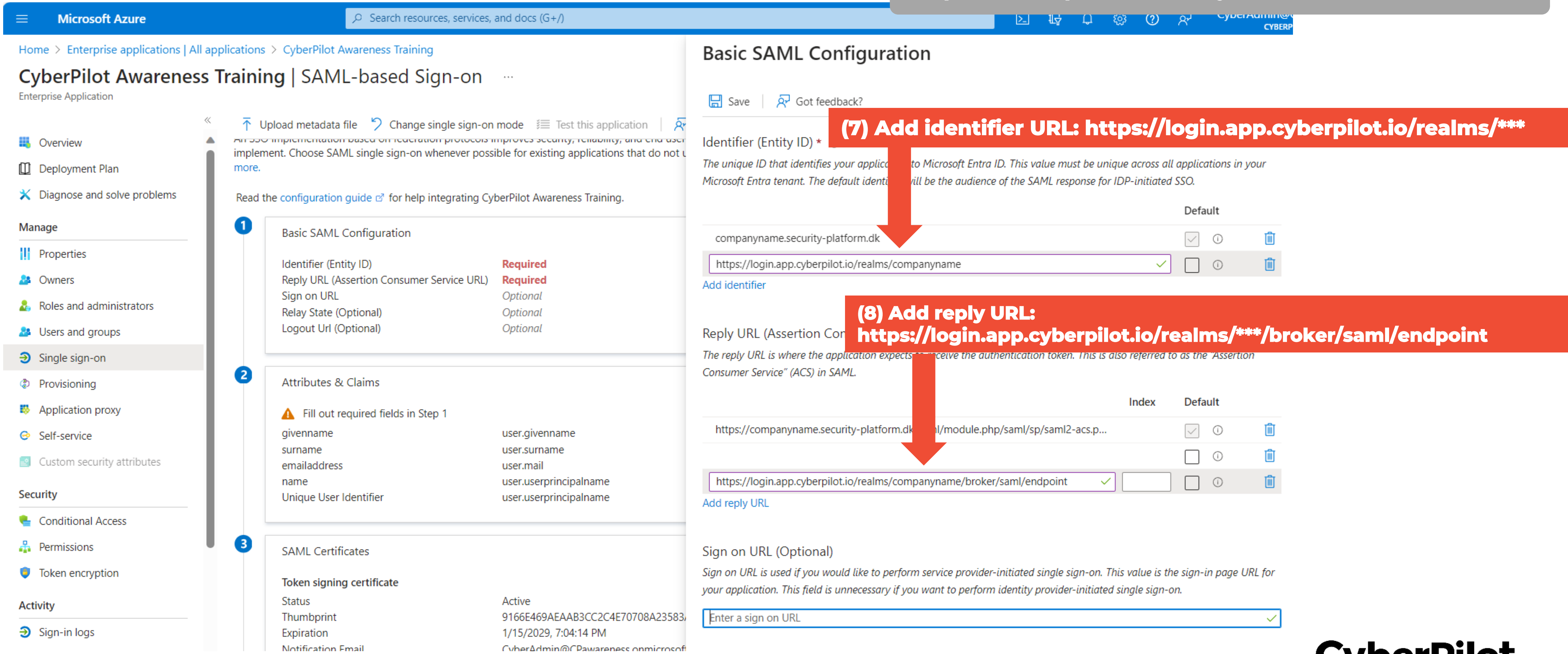
(6) "Edit" Basic SAML Configuration

CyberPilot

Step 7: Add Identifier URL: https://login.app.cyberpilot.io/realms/***
Step 8: Add Reply URL: https://login.app.cyberpilot.io/realms/***/broker/saml/endpoint

Note: You can leave the eFront Urls, and remove them after the migration is completed. This allows your users to logon to eFront until the final step of the migration.

Important: Replace * with your subdomain - see slide 2**



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Enterprise applications | All applications > CyberPilot Awareness Training

CyberPilot Awareness Training | SAML-based Sign-on ...

Enterprise Application

An SSO implementation based on federation protocols improves security, reliability, and end user ... implement. Choose SAML single sign-on whenever possible for existing applications that do not u... more.

Read the configuration guide for help integrating CyberPilot Awareness Training.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	9166E469AEAAB3CC2C4E70708A23583
Expiration	1/15/2029, 7:04:14 PM
Notification Email	CyberAdmin@CPawareness.onmicrosoft

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) *

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

	Default
companyname.security-platform.dk	☑
https://login.app.cyberpilot.io/realms/companyname ✓	□

Add identifier

(7) Add identifier URL: https://login.app.cyberpilot.io/realms/***

Reply URL (Assertion Con...

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

	Index	Default
https://companyname.security-platform.dk...l/module.php/saml/sp/saml2-acs.p...		☑
		□
https://login.app.cyberpilot.io/realms/companyname/broker/saml/endpoint ✓		□

Add reply URL

(8) Add reply URL: https://login.app.cyberpilot.io/realms/*/broker/saml/endpoint**

Sign on URL (Optional)

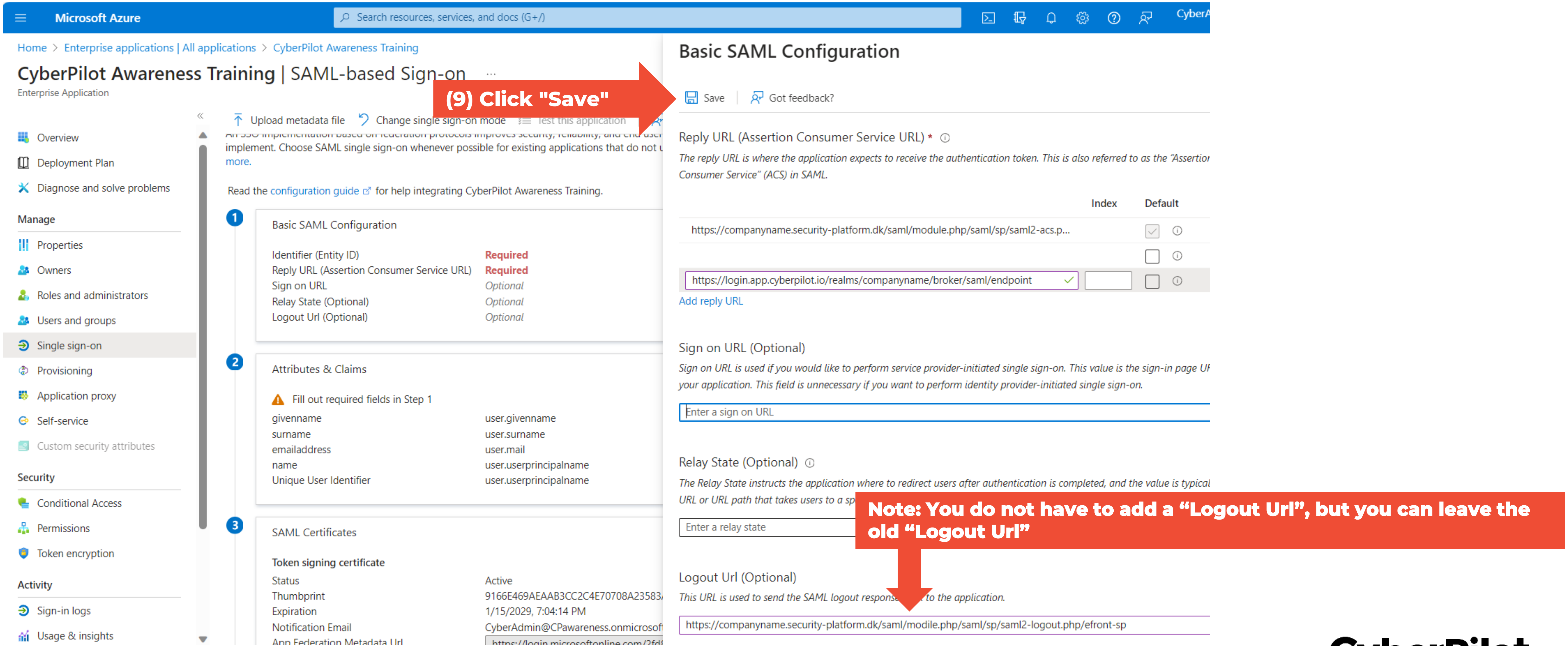
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

CyberPilot

Step 9: Click "Save“

Note: You can leave the eFront Logout URL, and remove it after the migration is completed. This allows your users to logon to eFront until the final step of the migration.



Home > Enterprise applications | All applications > CyberPilot Awareness Training

CyberPilot Awareness Training | SAML-based Sign-on ...

Enterprise Application

An SSO implementation based on federation protocols improves security, reliability, and end user ... implement. Choose SAML single sign-on whenever possible for existing applications that do not u... more.

Read the configuration guide for help integrating CyberPilot Awareness Training.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	9166E469AEAAB3CC2C4E70708A23583
Expiration	1/15/2029, 7:04:14 PM
Notification Email	CyberAdmin@CPawareness.onmicrosof
App Federation Metadata Url	https://login.microsoftonline.com/2fd

Basic SAML Configuration

Reply URL (Assertion Consumer Service URL) *

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

	Index	Default
https://companyname.security-platform.dk/saml/module.php/saml/sp/saml2-acs.p...		☑
		□
https://login.app.cyberpilot.io/realms/companyname/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 UF 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 typical URL or URL path that takes users to a sp

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout respons... to the application.

https://companyname.security-platform.dk/saml/modile.php/saml/sp/saml2-logout.php/efront-sp

(9) Click "Save"

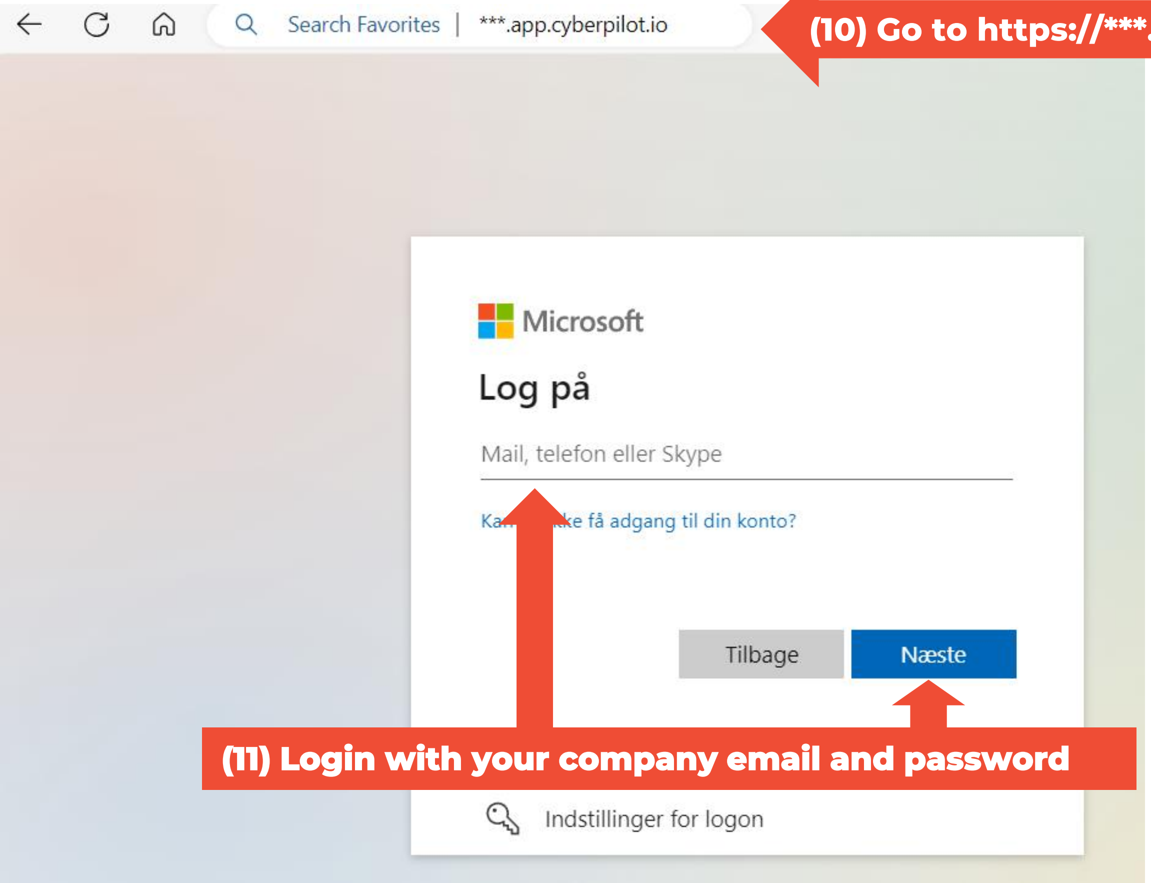
Note: You do not have to add a “Logout Url”, but you can leave the old “Logout Url”

CyberPilot

Step 10: Go to https://***.app.cyberpilot.io/ (replace *** with your subdomain) - *see slide 2*

Step 11: Login with your company email and password

Note: We recommend that you also do this test in incognito/private mode in your browser
Note: You need to have a user in eFront (the old platform) to test SSO. If you don't have that, please contact your eFront admin and ask this person to test.
Note: If you have two users in the eFront, please login with the user that have your email as username.
Note: If SSO is not working and you cannot login, you may have to contact CyberPilot support.



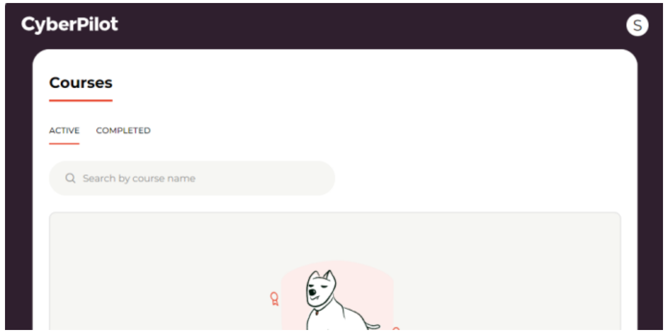
Log på

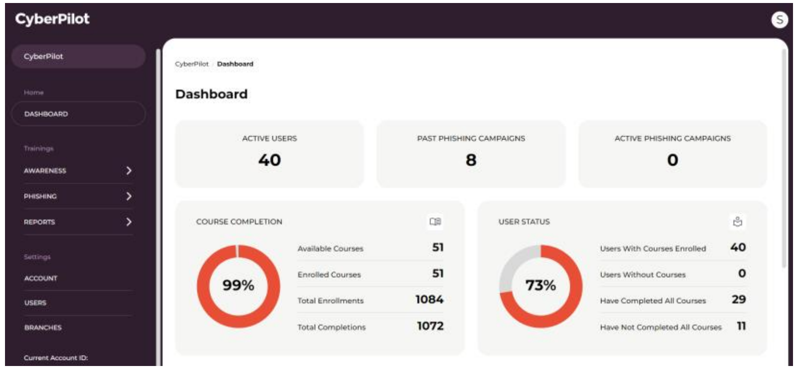
Mail, telefon eller Skype

Ka ke få adgang til din konto?

(10) Go to https://*.app.cyberpilot.io/ (replace *** with your subdomain see slide 2)**

(11) Login with your company email and password





Dashboard

ACTIVE USERS 40
PAST PHISHING CAMPAIGNS 8
ACTIVE PHISHING CAMPAIGNS 0

COURSE COMPLETION
99%
Available Courses 51
Enrolled Courses 51
Total Enrollments 1084
Total Completions 1072

USER STATUS
73%
Users With Courses Enrolled 40
Users Without Courses 0
Have Completed All Courses 29
Have Not Completed All Courses 11

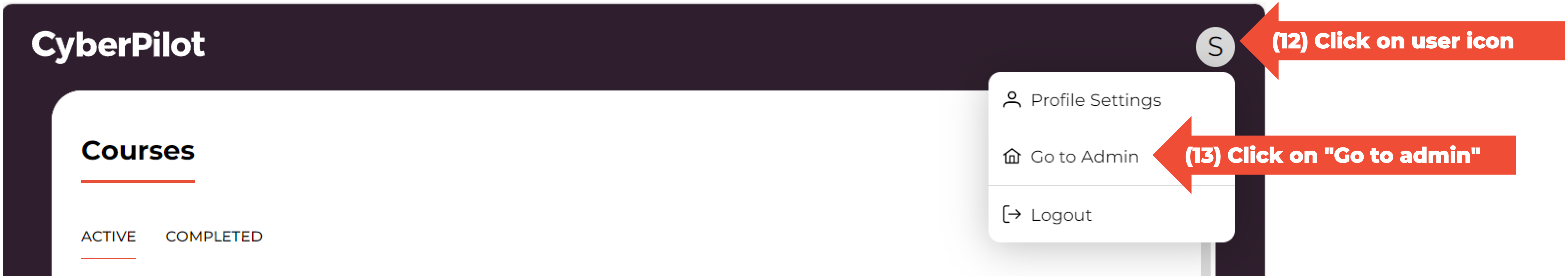
Current Account ID:

CYBERPILOT APP ADMINISTRATION

If you user has already been configured as an admin in the new platform then you will be able to go to administration. On the day of the final migration step, we make sure that your user has admin access.

Optional Step 12: Click on the user icon

Optional Step 13: Click on "Go to Admin"

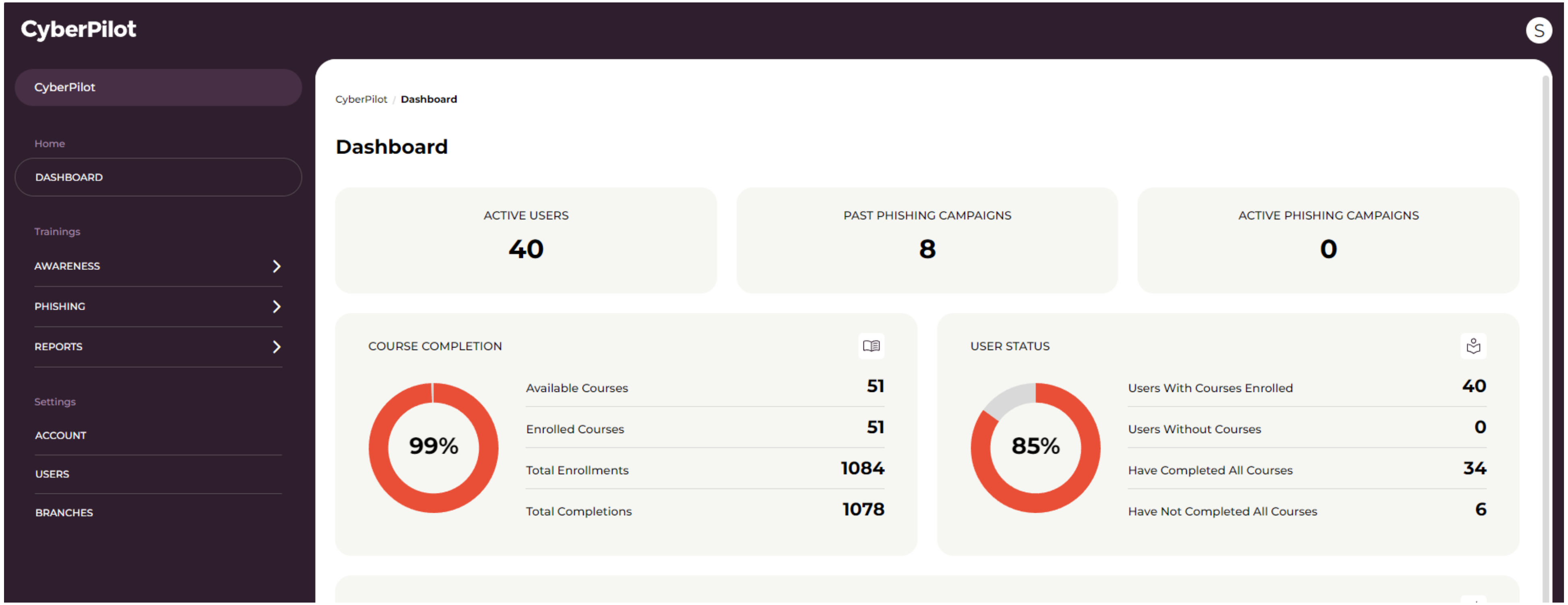


(12) Click on user icon

(13) Click on "Go to admin"

CYBERPILOT APP ADMINISTRATION
At https://www.cyberpilot.io/cyberpedia/introduction-to-cyberpilots-new-platform we have prepared an introduction video for you.

If you user is not configured as admin, then we make sure it is on the day of the final migration step.



Dashboard

ACTIVE USERS	PAST PHISHING CAMPAIGNS	ACTIVE PHISHING CAMPAIGNS
40	8	0

COURSE COMPLETION — 99%

Available Courses	51
Enrolled Courses	51
Total Enrollments	1084
Total Completions	1078

USER STATUS — 85%

Users With Courses Enrolled	40
Users Without Courses	0
Have Completed All Courses	34
Have Not Completed All Courses	6

❷ Azure AD User Properties

CyberPilot

Azure AD User Properties

When the CyberPilot App synchronize 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 create/update in the CyberPilot App.

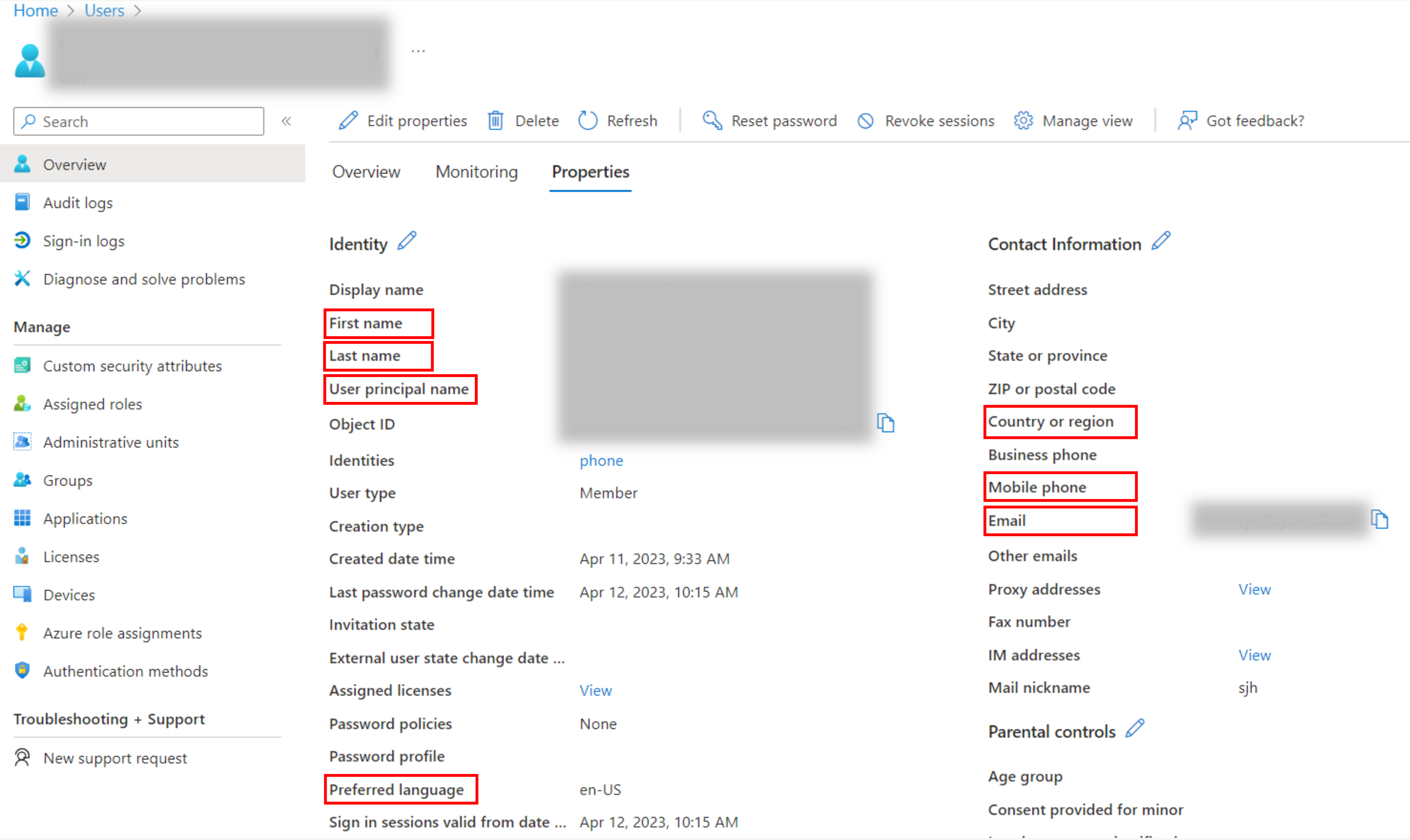
If a user exists in the CyberPilot App, but not in your AD group, then the user is deactivated. Users with the role “Admin” are not deactivated, so that admins are not locked out of the CyberPilot App, if they are removed from the AD Group.

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.

In eFront (the old platform) you needed to specify what Azure AD user properties to import. This is not needed anymore.

USER PROPERTIES 1

Overview of user properties in Azure AD



Identity

Display name	[redacted]
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	[redacted]
Other emails	
Proxy addresses	View
Fax number	
IM addresses	View
Mail nickname	sjh

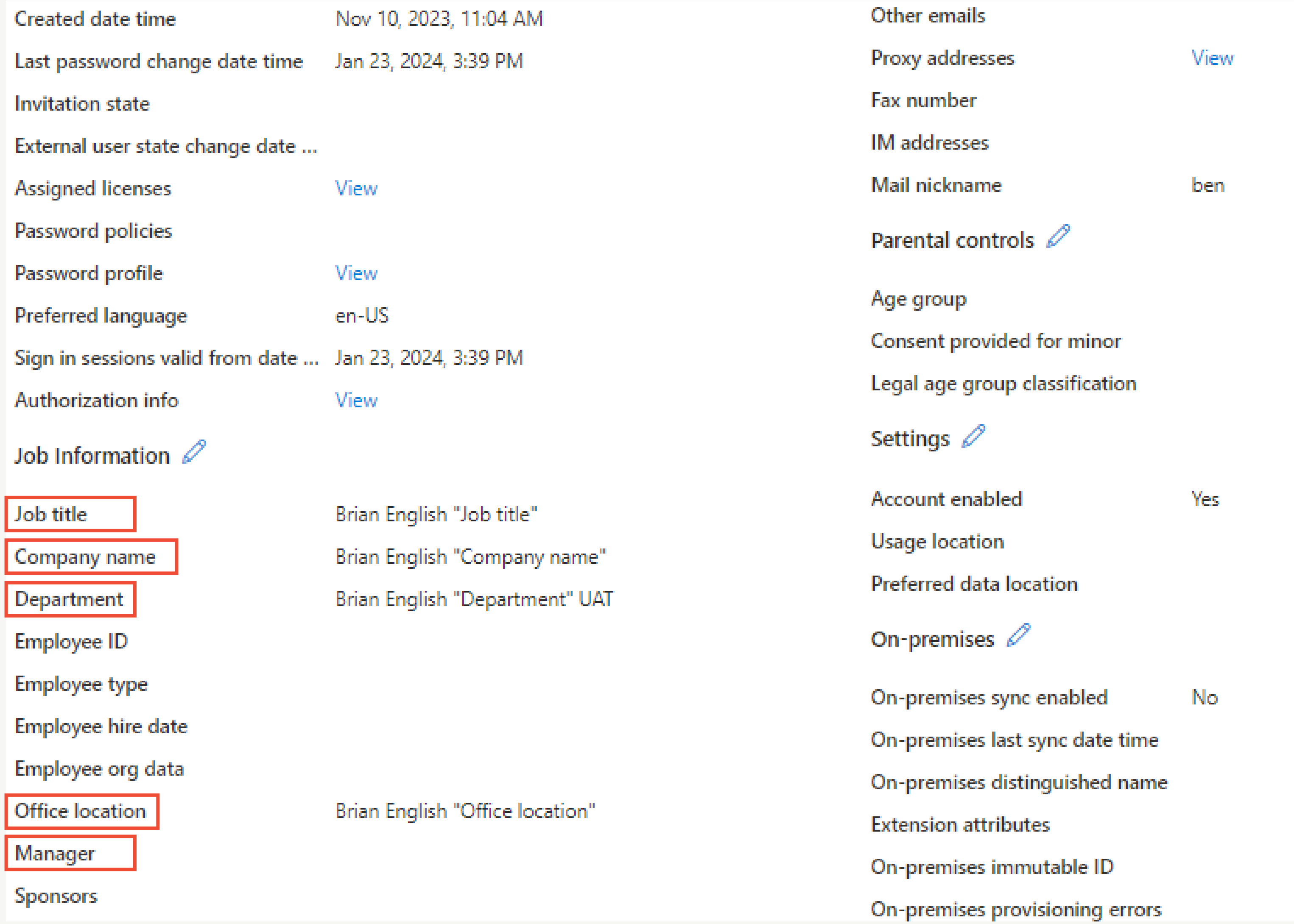
Parental controls

Age group	
Consent provided for minor	

CyberPilot

USER PROPERTIES 2

Overview of user properties in Azure AD



Created date time	Nov 10, 2023, 11:04 AM
Last password change date time	Jan 23, 2024, 3:39 PM
Invitation state	
External user state change date ...	
Assigned licenses	View
Password policies	
Password profile	View
Preferred language	en-US
Sign in sessions valid from date ...	Jan 23, 2024, 3:39 PM
Authorization info	View

Job Information

Job title	Brian English "Job title"
Company name	Brian English "Company name"
Department	Brian English "Department" UAT
Employee ID	
Employee type	
Employee hire date	
Employee org data	
Office location	Brian English "Office location"
Manager	
Sponsors	

Other emails	
Proxy addresses	View
Fax number	
IM addresses	
Mail nickname	ben

Parental controls

Age group	
Consent provided for minor	
Legal age group classification	

Settings

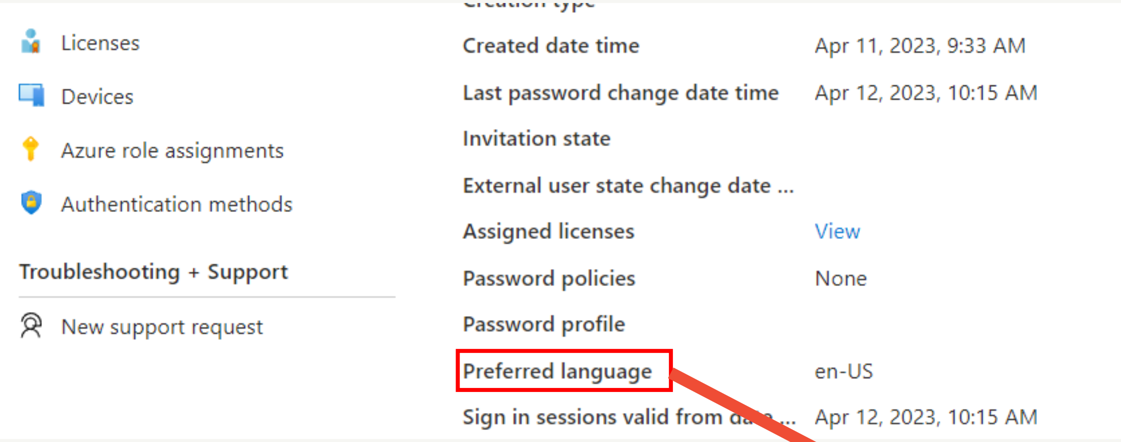
Account enabled	Yes
Usage location	
Preferred data location	

On-premises

On-premises sync enabled	No
On-premises last sync date time	
On-premises distinguished name	
Extension attributes	
On-premises immutable ID	
On-premises provisioning errors	

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. **If a user manually changed language in eFront, then the user will also have this language in the CyberPilot App.**

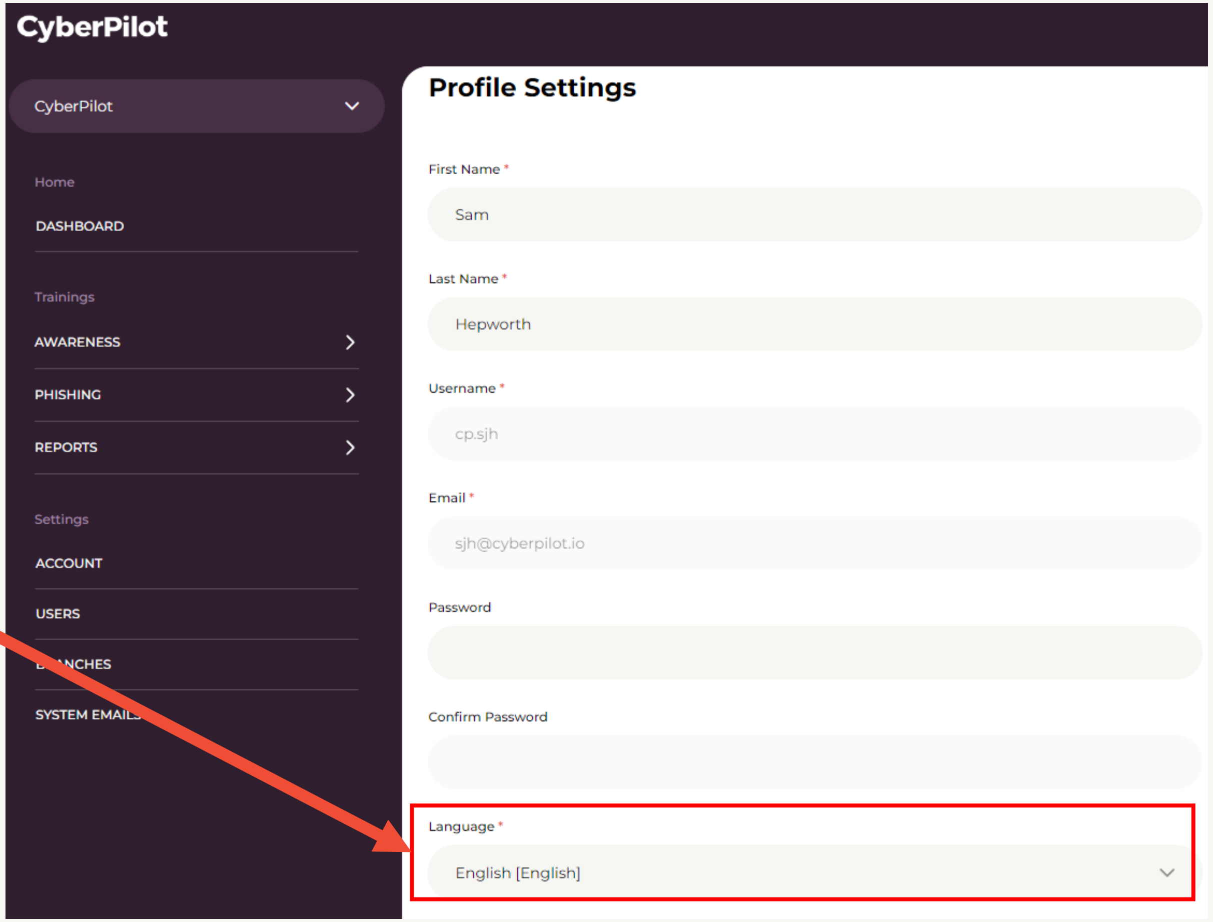


- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

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



Profile Settings

First Name *: Sam

Last Name *: Hepworth

Username *: cp.sjh

Email *: sjh@cyberpilot.io

Password

Confirm Password

Language *: English [English]

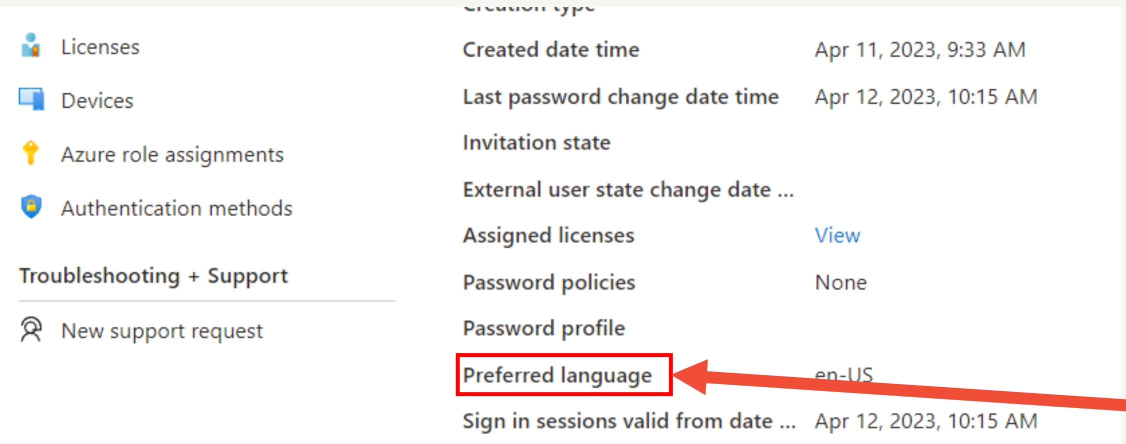
Important:

Courses in the CyberPilot App are available in the same languages as in the old platform. The CyberPilot App user interface is available in English and Danish.

If a user manually changes their language in the CyberPilot App, then it overrules 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”.

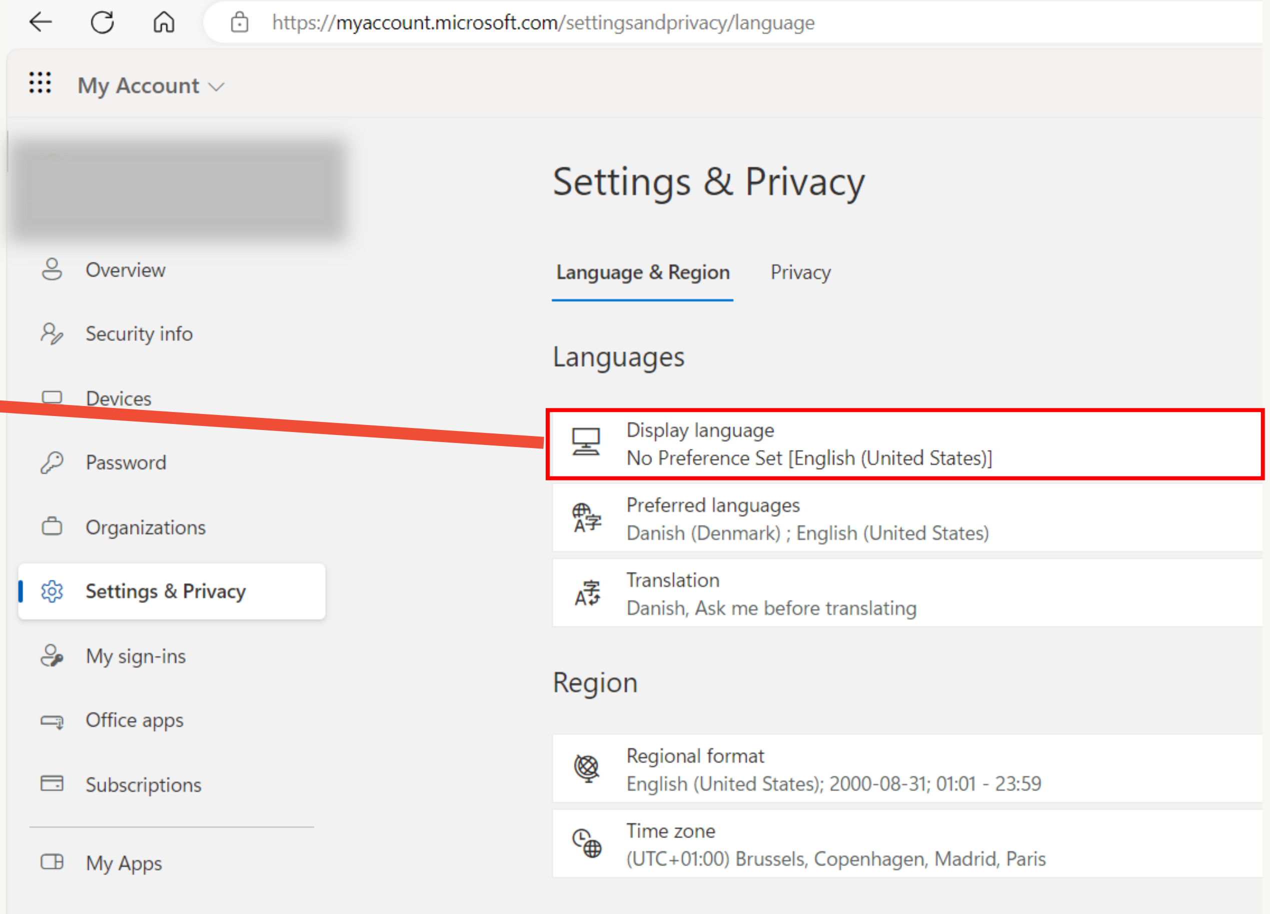


- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

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



https://myaccount.microsoft.com/settingsandprivacy/language

My Account

- Overview
- Security info
- Devices
- Password
- Organizations
- Settings & Privacy
- My sign-ins
- Office apps
- Subscriptions
- My Apps

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

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

CyberPilot

❸ Whitelist Notification emails from the CyberPilot App

CyberPilot

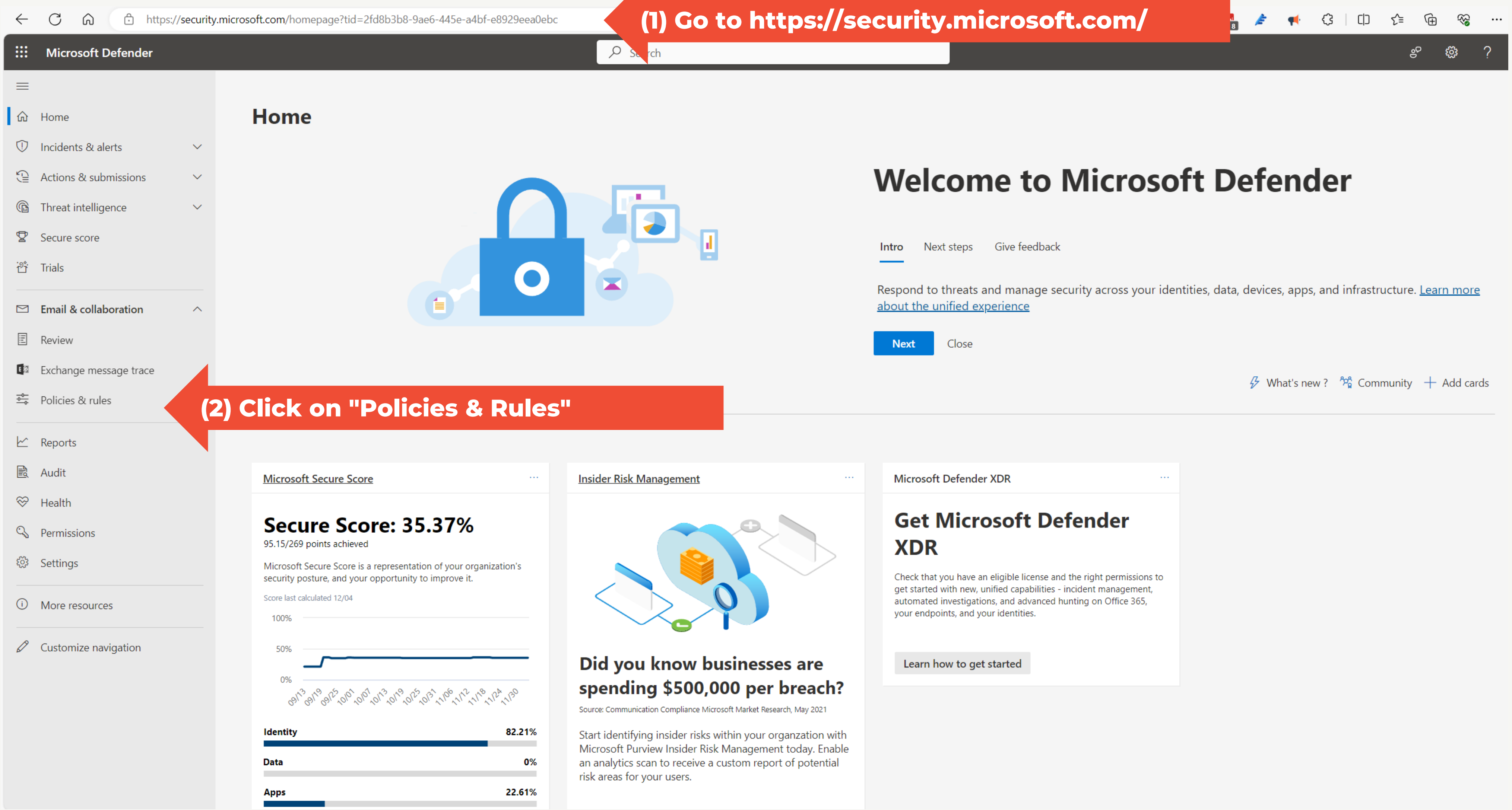
Whitelist notification emails from the CyberPilot App

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**, 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"



(1) Go to https://security.microsoft.com/

(2) Click on "Policies & Rules"

Home

Welcome to Microsoft Defender

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

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

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 organzation 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

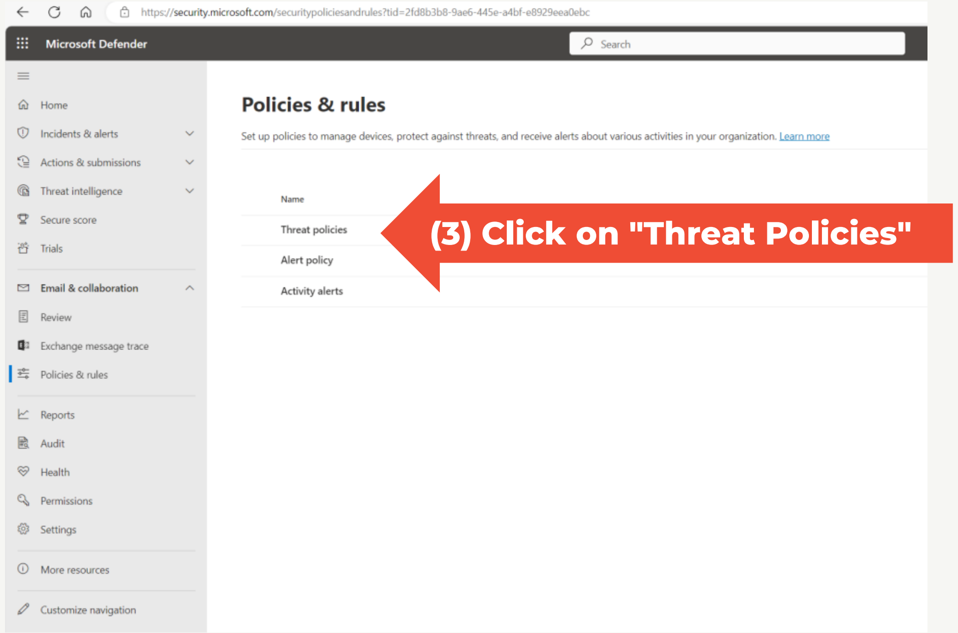
Get Microsoft Defender XDR

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.

CyberPilot

Microsoft Office 365 / Defender Guide

Step 3: Click on "Threat Policies"
Step 4: Click on "Anti-spam"

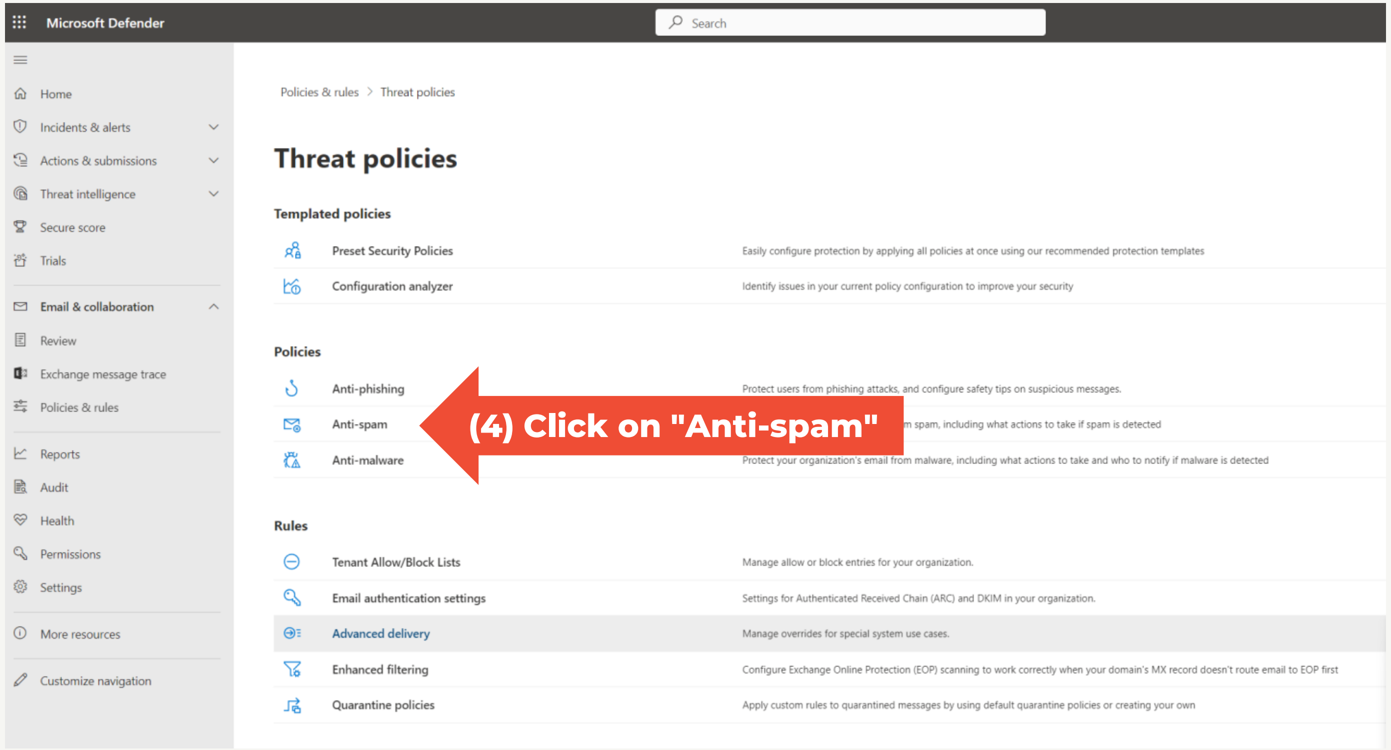


Policies & rules

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"



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	m 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

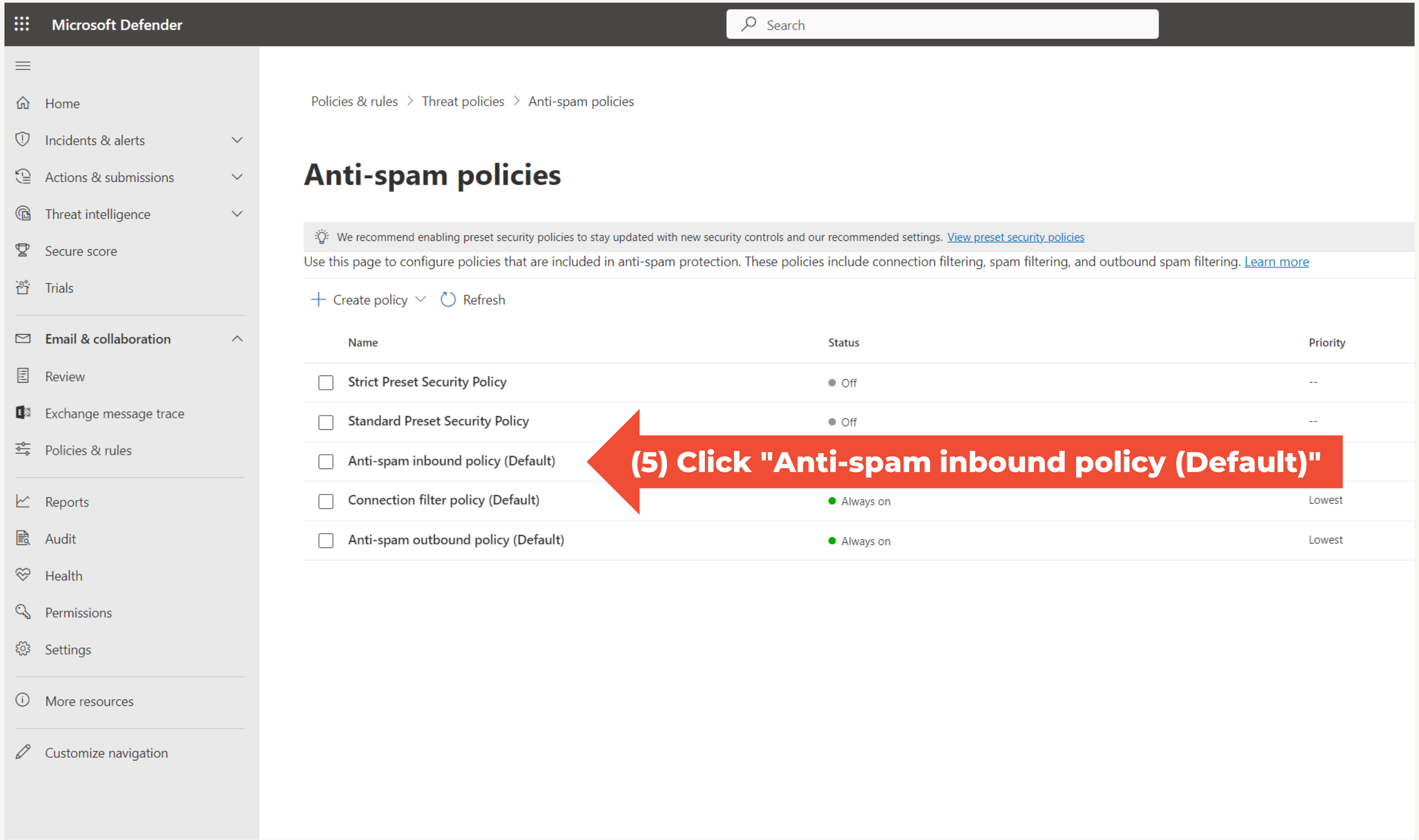
(4) Click on "Anti-spam"

CyberPilot

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



Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls and our recommended settings. View preset security policies

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and outbound spam filtering. Learn more

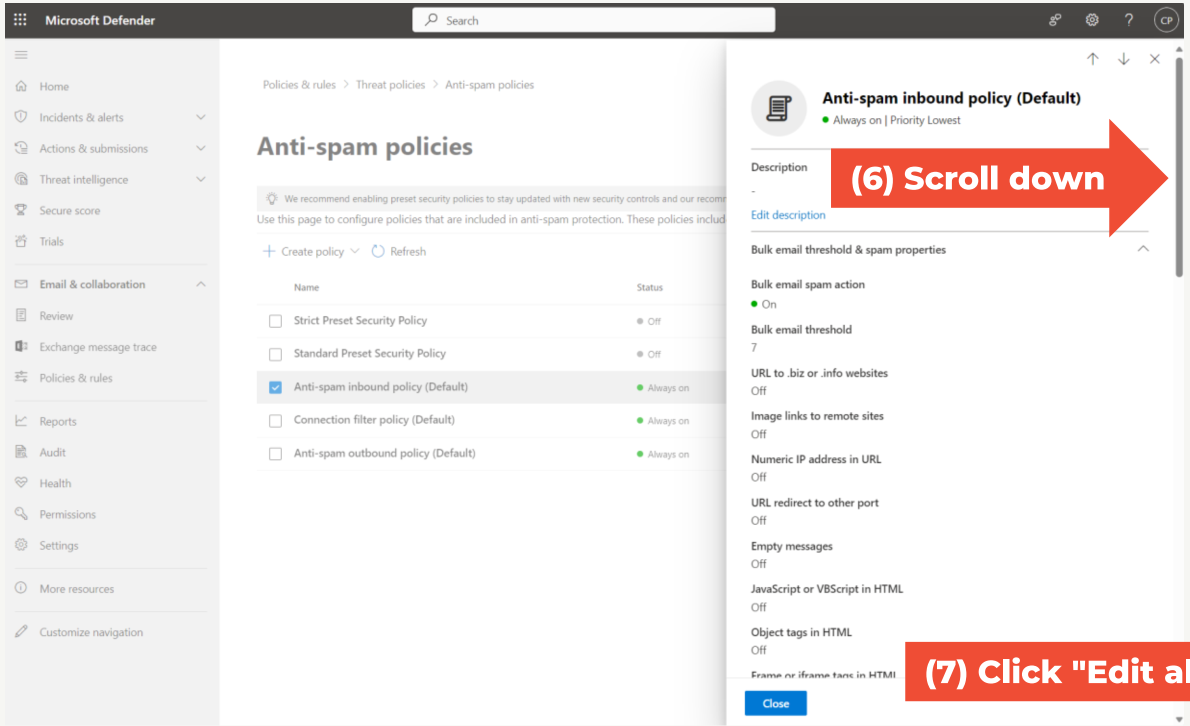
	Name	Status	Priority
□	Strict Preset Security Policy	● Off	--
□	Standard Preset Security Policy	● Off	--
□	Anti-spam inbound policy (Default)		
□	Connection filter policy (Default)	● Always on	Lowest
□	Anti-spam outbound policy (Default)	● Always on	Lowest

(5) Click "Anti-spam inbound policy (Default)"

CyberPilot

Microsoft Office 365 / Defender Guide

Step 6: Scroll down
Step 7: Click "Edit allowed and blocked senders and domains"



Policies & rules > Threat policies > Anti-spam policies

Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls and our recomm

Use this page to configure policies that are included in anti-spam protection. These policies includ

	Name	Status
☐	Strict Preset Security Policy	● Off
☐	Standard Preset Security Policy	● Off
☑	Anti-spam inbound policy (Default)	● Always on
☐	Connection filter policy (Default)	● Always on
☐	Anti-spam outbound policy (Default)	● Always on

Anti-spam inbound policy (Default)
● Always on | Priority Lowest

Description
-
Edit description

Bulk email threshold & spam properties

Bulk email spam action
● On

Bulk email threshold
7

URL to .biz or .info websites
Off

Image links to remote sites
Off

Numeric IP address in URL
Off

URL redirect to other port
Off

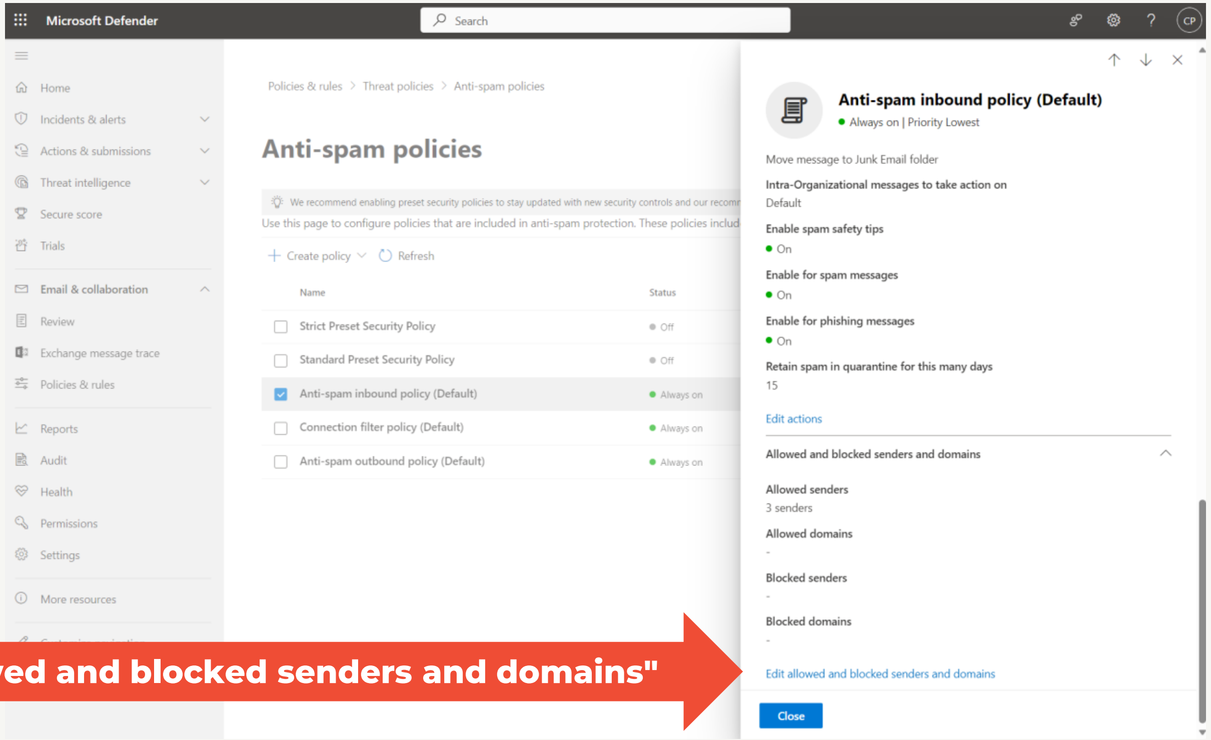
Empty messages
Off

JavaScript or VBScript in HTML
Off

Object tags in HTML
Off

Frame or iframe tags in HTML

(6) Scroll down



Policies & rules > Threat policies > Anti-spam policies

Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls and our recomm

Use this page to configure policies that are included in anti-spam protection. These policies includ

	Name	Status
☐	Strict Preset Security Policy	● Off
☐	Standard Preset Security Policy	● Off
☑	Anti-spam inbound policy (Default)	● Always on
☐	Connection filter policy (Default)	● Always on
☐	Anti-spam outbound policy (Default)	● Always on

Anti-spam inbound policy (Default)
● Always on | Priority Lowest

Move message to Junk Email folder

Intra-Organizational messages to take action on
Default

Enable spam safety tips
● On

Enable for spam messages
● On

Enable for phishing messages
● On

Retain spam in quarantine for this many days
15

Edit actions

Allowed and blocked senders and domains

Allowed senders
3 senders

Allowed domains
-

Blocked senders
-

Blocked domains
-

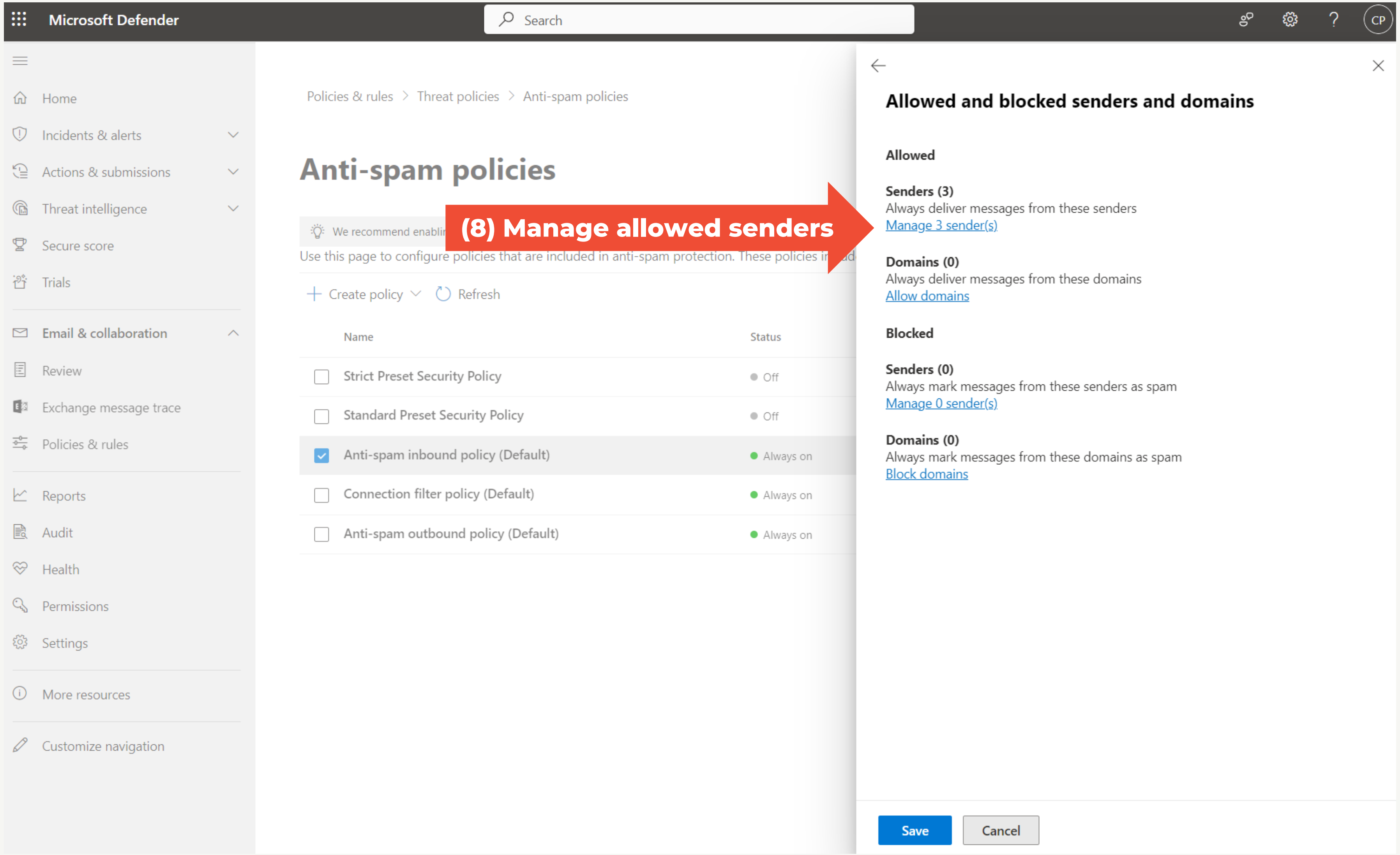
Edit allowed and blocked senders and domains

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

CyberPilot

Microsoft Office 365 / Defender Guide

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



Anti-spam policies

We recommend enabli

Use this page to configure policies that are included in anti-spam protection. These policies in

	Name	Status
□	Strict Preset Security Policy	● Off
□	Standard Preset Security Policy	● Off
☑	Anti-spam inbound policy (Default)	● Always on
□	Connection filter policy (Default)	● Always on
□	Anti-spam outbound policy (Default)	● Always on

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

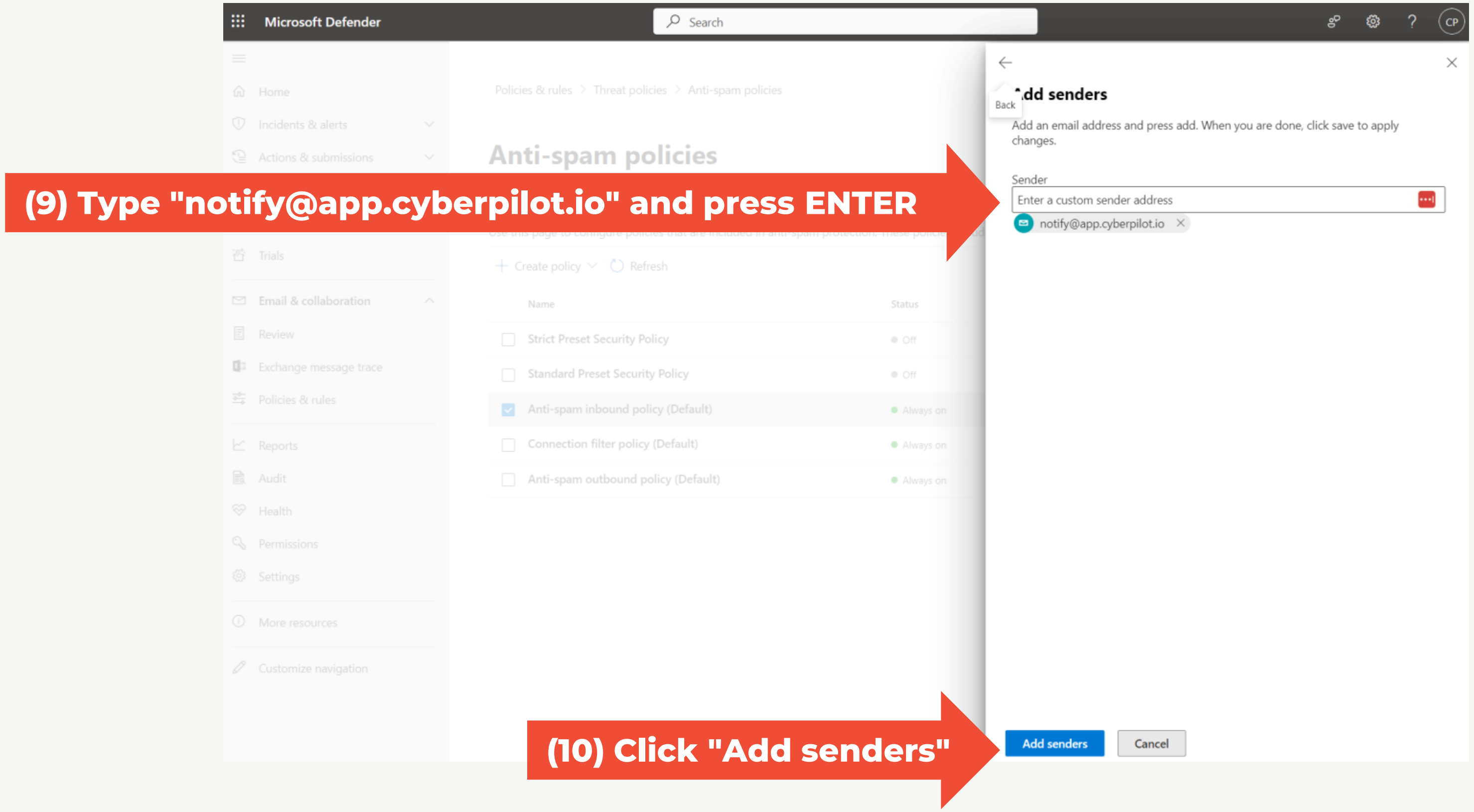
Senders (0)
Always mark messages from these senders as spam
Manage 0 sender(s)

Domains (0)
Always mark messages from these domains as spam
Block domains

CyberPilot

Microsoft Office 365 / Defender Guide

Step 9: Type notify@app.cyberpilot.io and press ENTER
Step 10: Click "Add Senders"

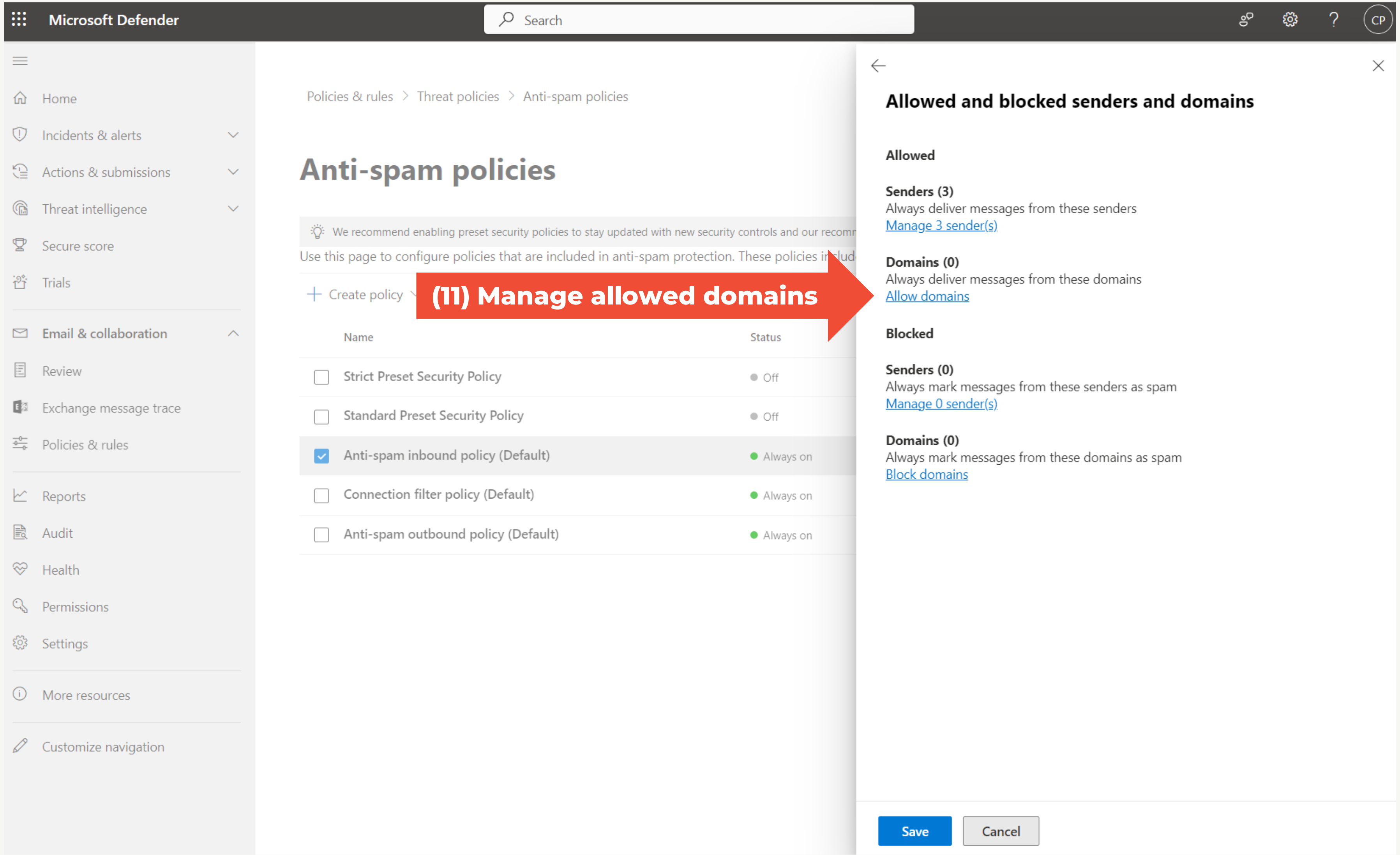


(9) Type "notify@app.cyberpilot.io" and press ENTER

(10) Click "Add senders"

Microsoft Office 365 / Defender Guide

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



Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls and our recomm

Use this page to configure policies that are included in anti-spam protection. These policies includ

	Name	Status
□	Strict Preset Security Policy	● Off
□	Standard Preset Security Policy	● Off
☑	Anti-spam inbound policy (Default)	● Always on
□	Connection filter policy (Default)	● Always on
□	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

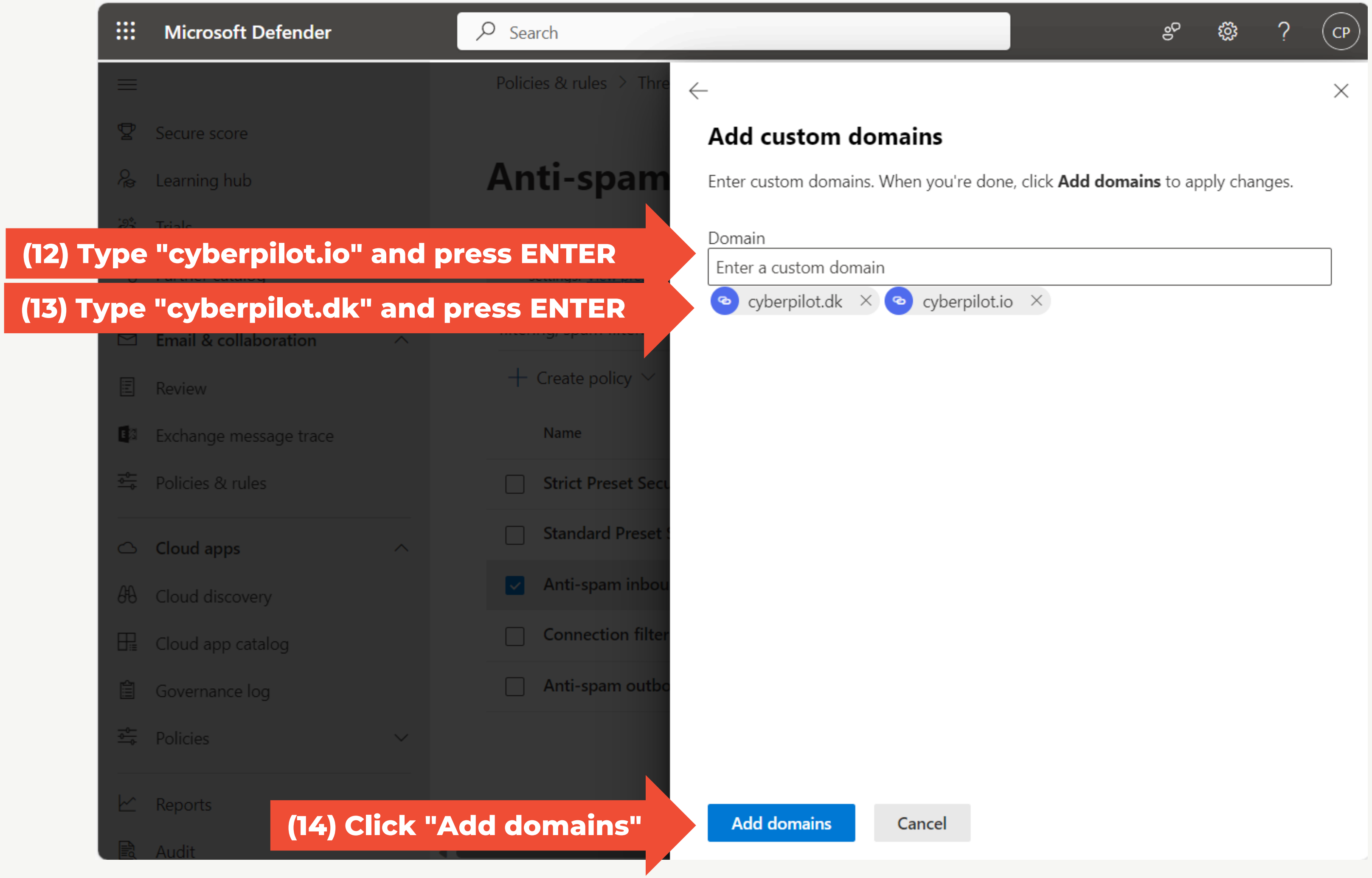
Blocked

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

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"



Add custom domains

Enter custom domains. When you're done, click **Add domains** to apply changes.

Domain: Enter a custom domain

cyberpilot.dk ✕ cyberpilot.io ✕

Add domains | Cancel

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

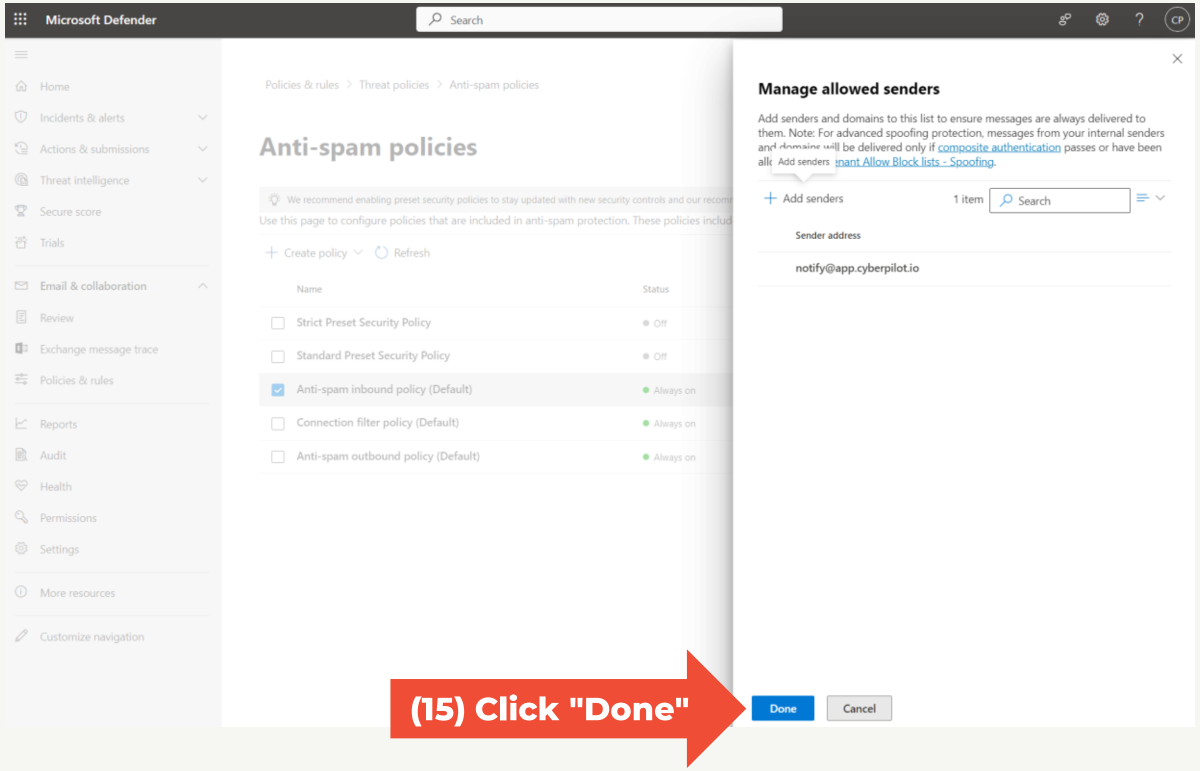
(13) Type "cyberpilot.dk" and press ENTER

(14) Click "Add domains"

CyberPilot

Microsoft Office 365 / Defender Guide

Step 15: Click "Done"
Step 16: Click "Save"



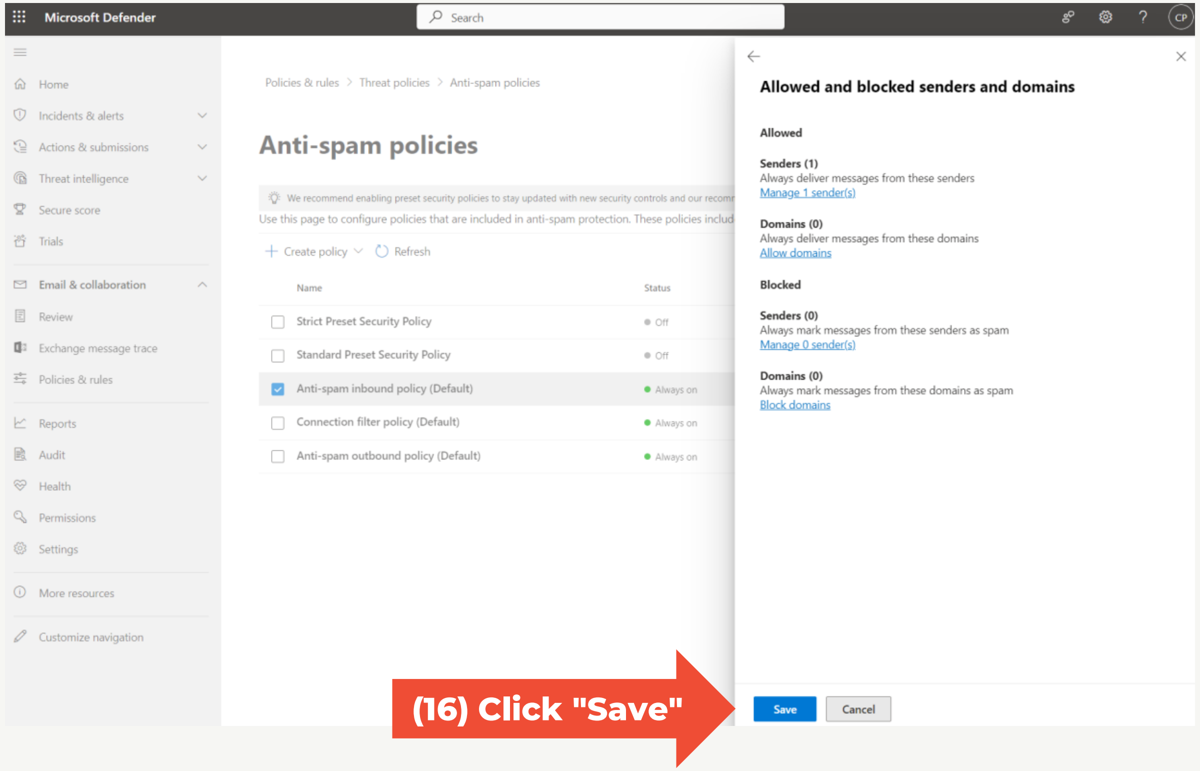
Manage allowed senders

Add senders and domains to this list to ensure messages are always delivered to them. Note: For advanced spoofing protection, messages from your internal senders and domains will be delivered only if composite authentication passes or have been allo Add senders enant Allow Block lists - Spoofing.

+ Add senders   1 item   Search

Sender address
notify@app.cyberpilot.io

(15) Click "Done"



Allowed and blocked senders and domains

Allowed

Senders (1)
Always deliver messages from these senders
Manage 1 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

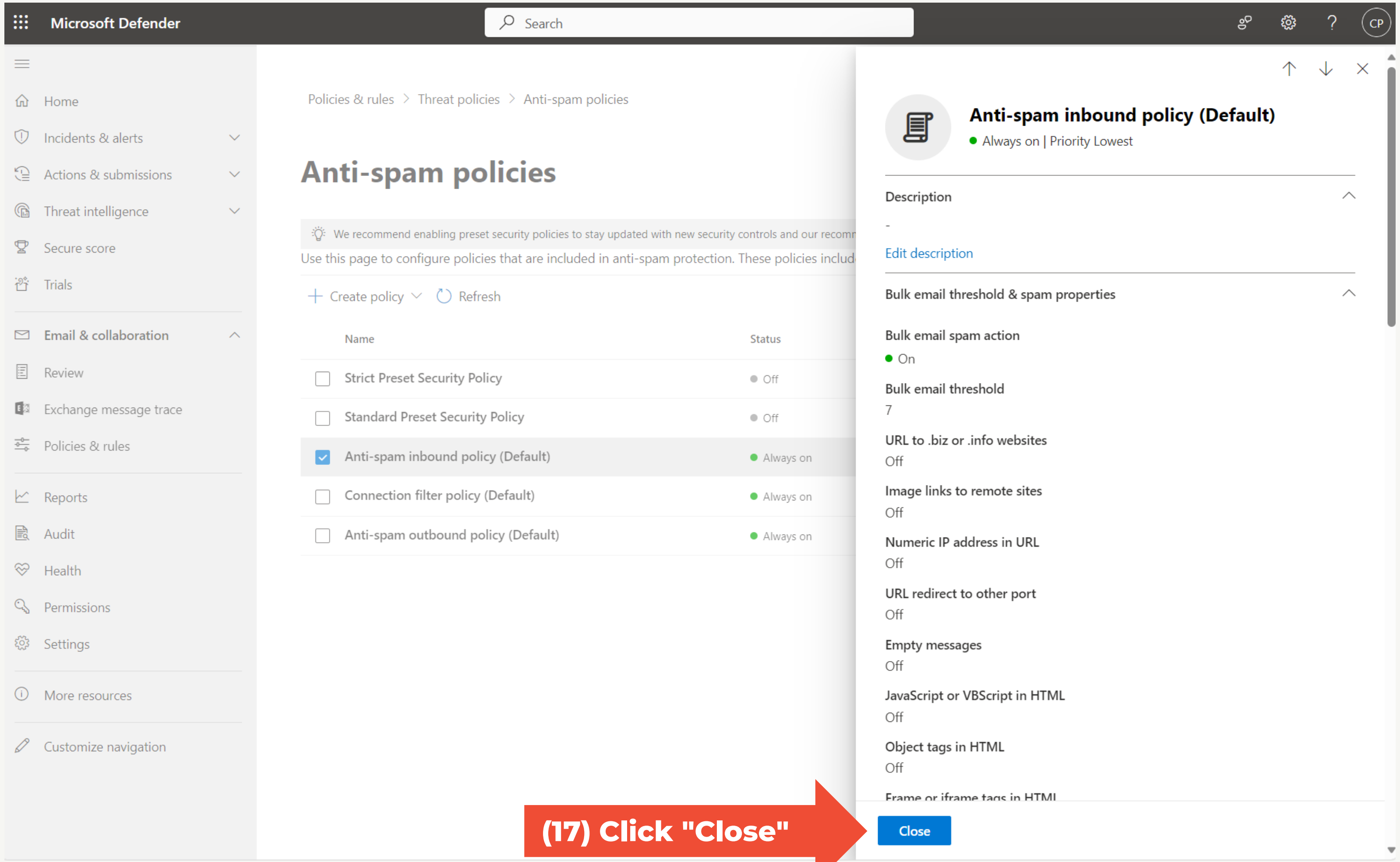
(16) Click "Save"

CyberPilot

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



Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls and our recomm

Use this page to configure policies that are included in anti-spam protection. These policies includ

	Name	Status
□	Strict Preset Security Policy	● Off
□	Standard Preset Security Policy	● Off
☑	Anti-spam inbound policy (Default)	● Always on
□	Connection filter policy (Default)	● Always on
□	Anti-spam outbound policy (Default)	● Always on

Anti-spam inbound policy (Default)

● Always on | Priority Lowest

Description

-

Bulk email threshold & spam properties

Bulk email spam action
● On

Bulk email threshold
7

URL to .biz or .info websites
Off

Image links to remote sites
Off

Numeric IP address in URL
Off

URL redirect to other port
Off

Empty messages
Off

JavaScript or VBScript in HTML
Off

Object tags in HTML
Off

Frame or iframe tags in HTML

(17) Click "Close"

CyberPilot

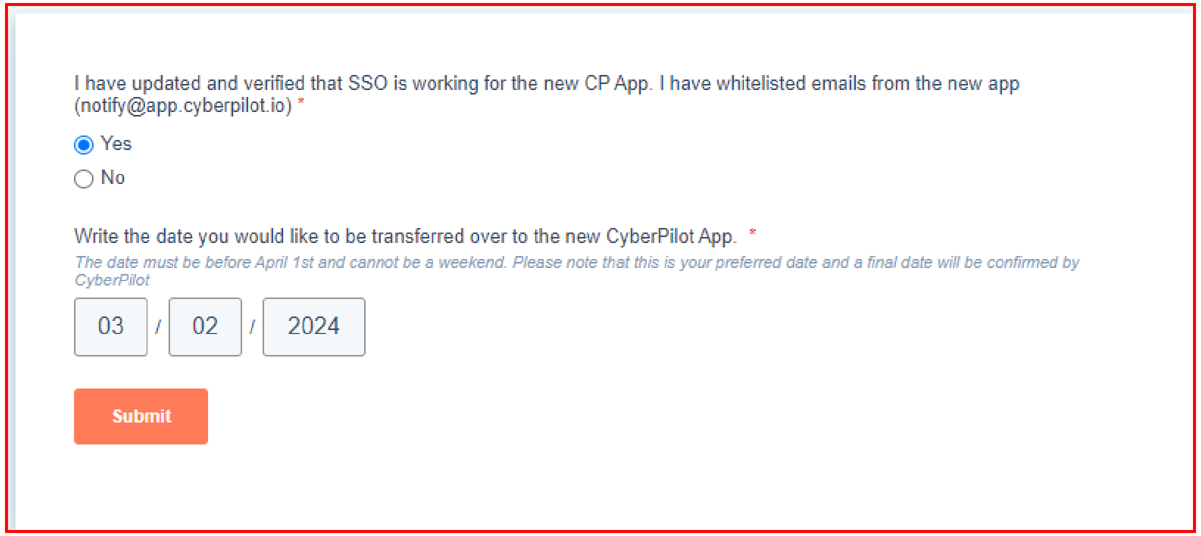
❹ Notify CyberPilot that you are ready for final migration step

CyberPilot

Notify CyberPilot that you are ready for the final migration step

When you have confirmed that you can login to the new platform using SSO and have whitelisted our emails you are ready for the final migration step.

In the mail you received from us, there is a link to a form where you can confirm that you are ready for the next migration step and propose a date for this.



I have updated and verified that SSO is working for the new CP App. I have whitelisted emails from the new app (notify@app.cyberpilot.io) *

● Yes

○ No

Write the date you would like to be transferred over to the new CyberPilot App. *

The date must be before April 1st and cannot be a weekend. Please note that this is your preferred date and a final date will be confirmed by CyberPilot

03 / 02 / 2024

❺ Day of final migration step

Day of final migration step

The day we complete the migration you and all your users receive a welcome to the new platform mail.

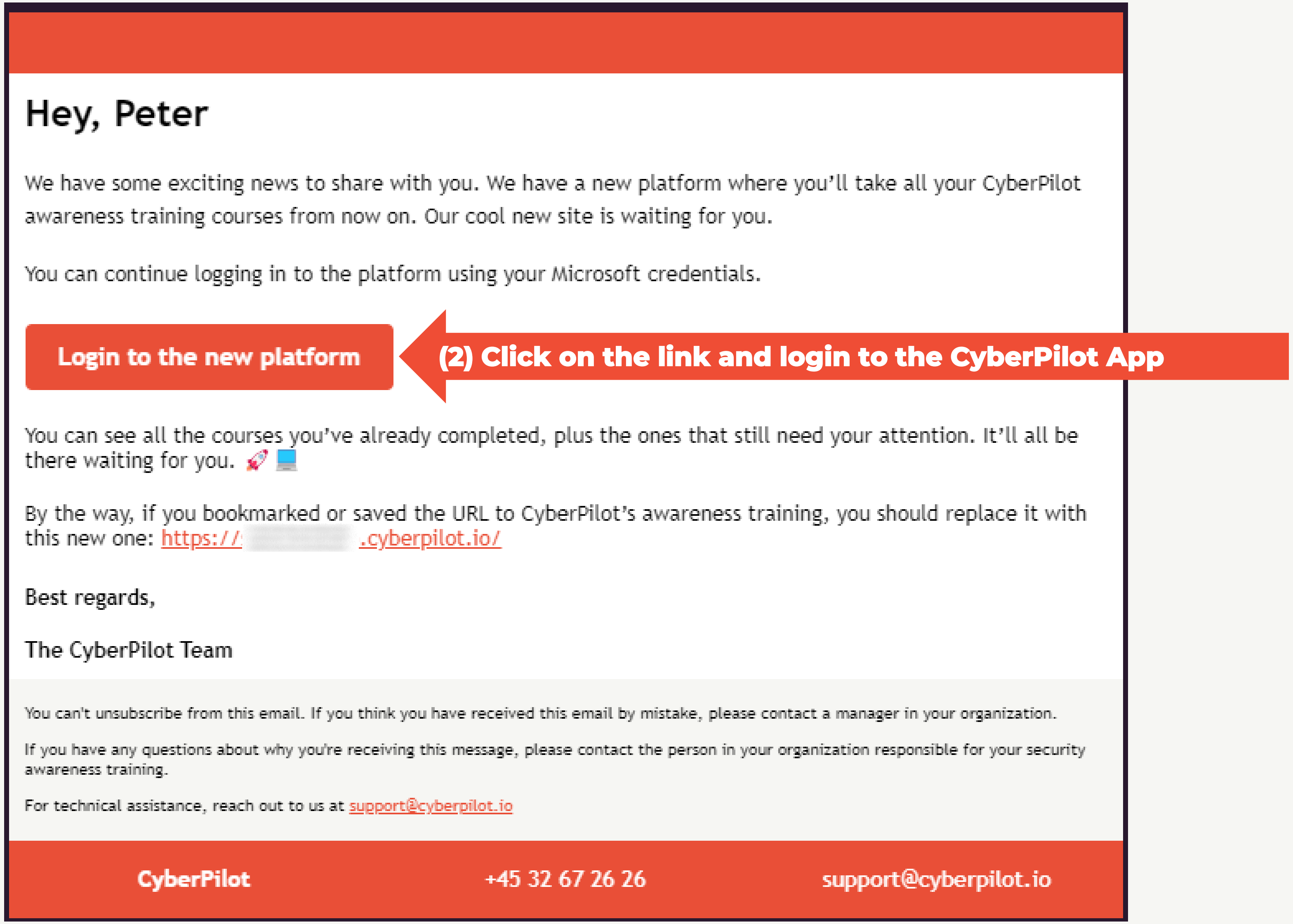
In eFront you may have both a normal user and an admin user. In the CyberPilot App you only have one user. You will therefore only receive one welcome mail.

From this day you and your users must login to https://***.app.cyberpilot.io/ (replace *** with the subdomain assigned to your company.)

LOGGING IN TO THE CYBERPILOT APP

Step 1: Open the welcome email you have received from CyberPilot

Step 2: Click on “Login to the new platform“



Hey, Peter

We have some exciting news to share with you. We have a new platform where you’ll take all your CyberPilot awareness training courses from now on. Our cool new site is waiting for you.

You can continue logging in to the platform using your Microsoft credentials.

(2) Click on the link and login to the CyberPilot App

You can see all the courses you’ve already completed, plus the ones that still need your attention. It’ll all be there waiting for you. 🚀 💻

By the way, if you bookmarked or saved the URL to CyberPilot’s awareness training, you should replace it with this new one: https://[redacted].cyberpilot.io/

Best regards,

The CyberPilot Team

You can't unsubscribe from this email. If you think you have received this email by mistake, please contact a manager in your organization.

If you have any questions about why you're receiving this message, please contact the person in your organization responsible for your security awareness training.

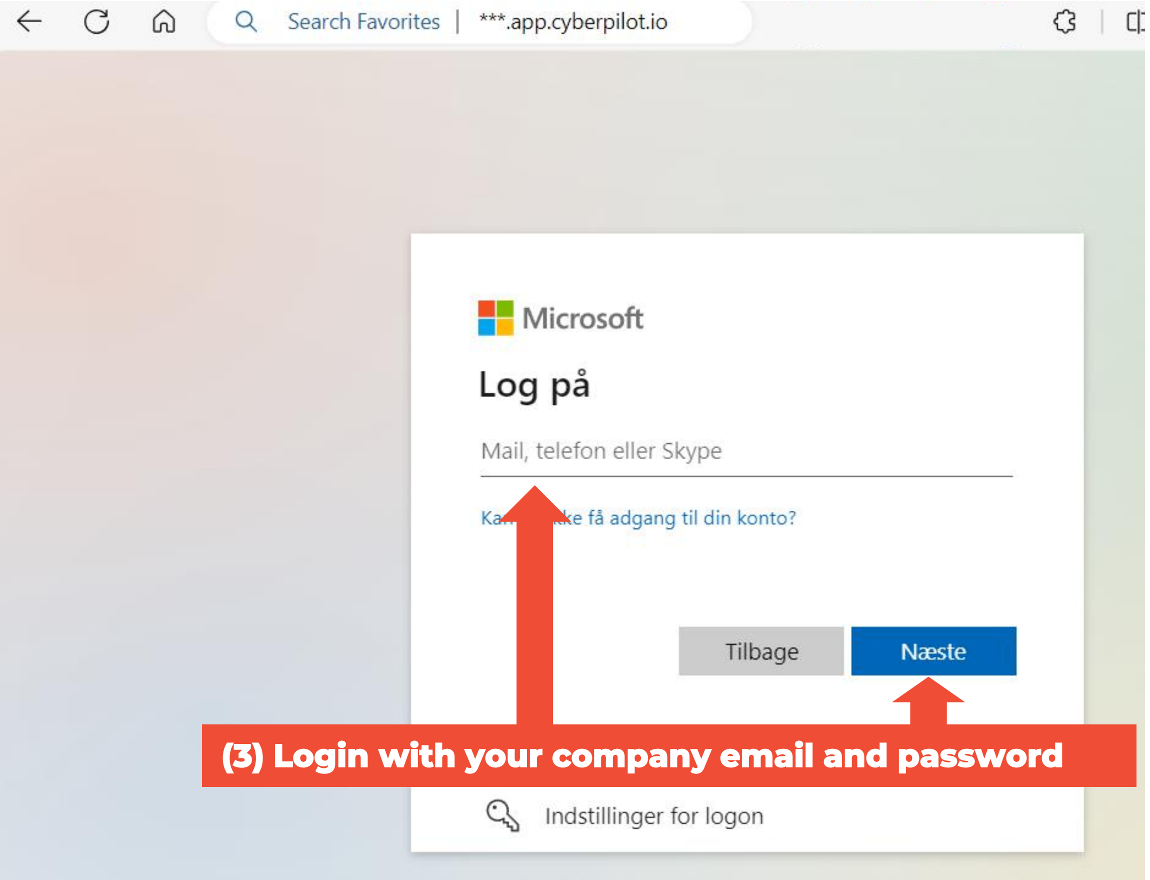
For technical assistance, reach out to us at support@cyberpilot.io

CyberPilot   +45 32 67 26 26   support@cyberpilot.io

CyberPilot

Step 3: Login with your company email and password

Note: If you have two users in eFront (the old platform) please login with the user that have your email as username.

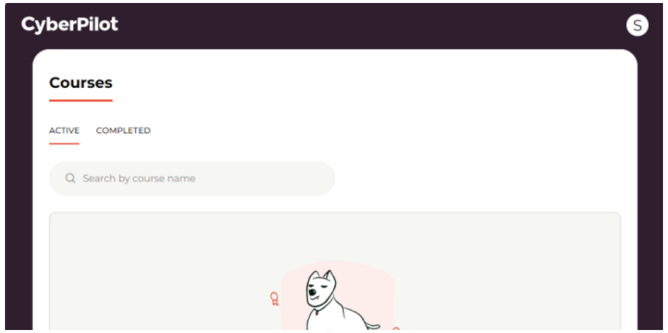


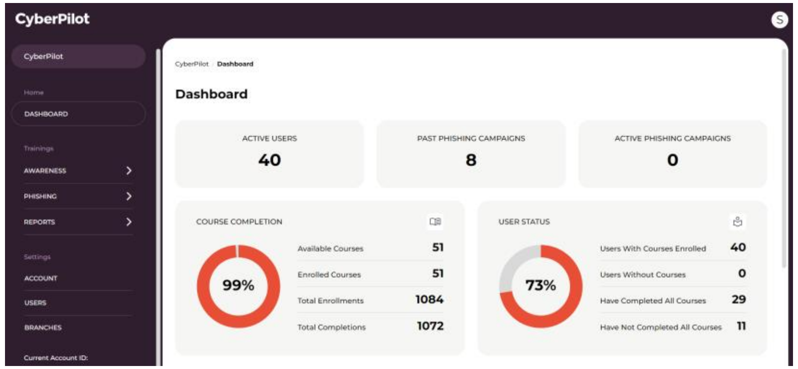
Log på

Mail, telefon eller Skype

Ka ke få adgang til din konto?

(3) Login with your company email and password





Dashboard

ACTIVE USERS	PAST PHISHING CAMPAIGNS	ACTIVE PHISHING CAMPAIGNS
40	8	0

COURSE COMPLETION: 99%

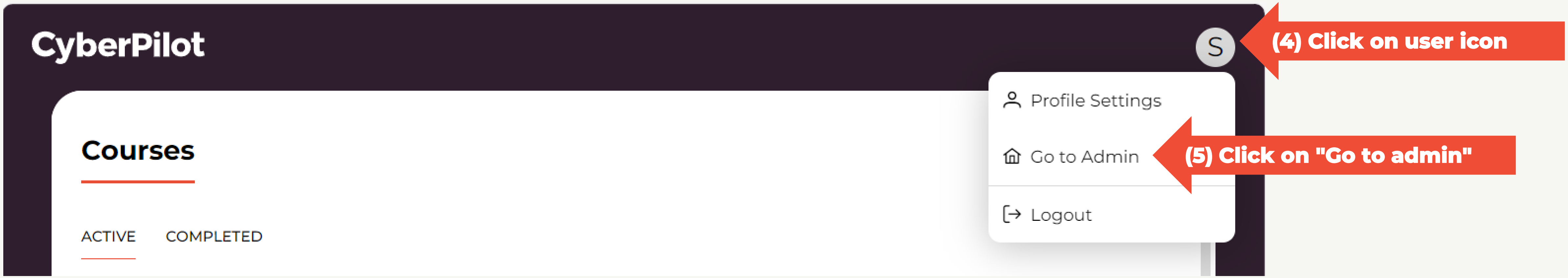
Available Courses	51
Enrolled Courses	51
Total Enrollments	1084
Total Completions	1072

USER STATUS: 73%

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

CYBERPILOT APP ADMINISTRATION

Step 4: Click on the user icon
Step 5: Click on "Go to Admin"

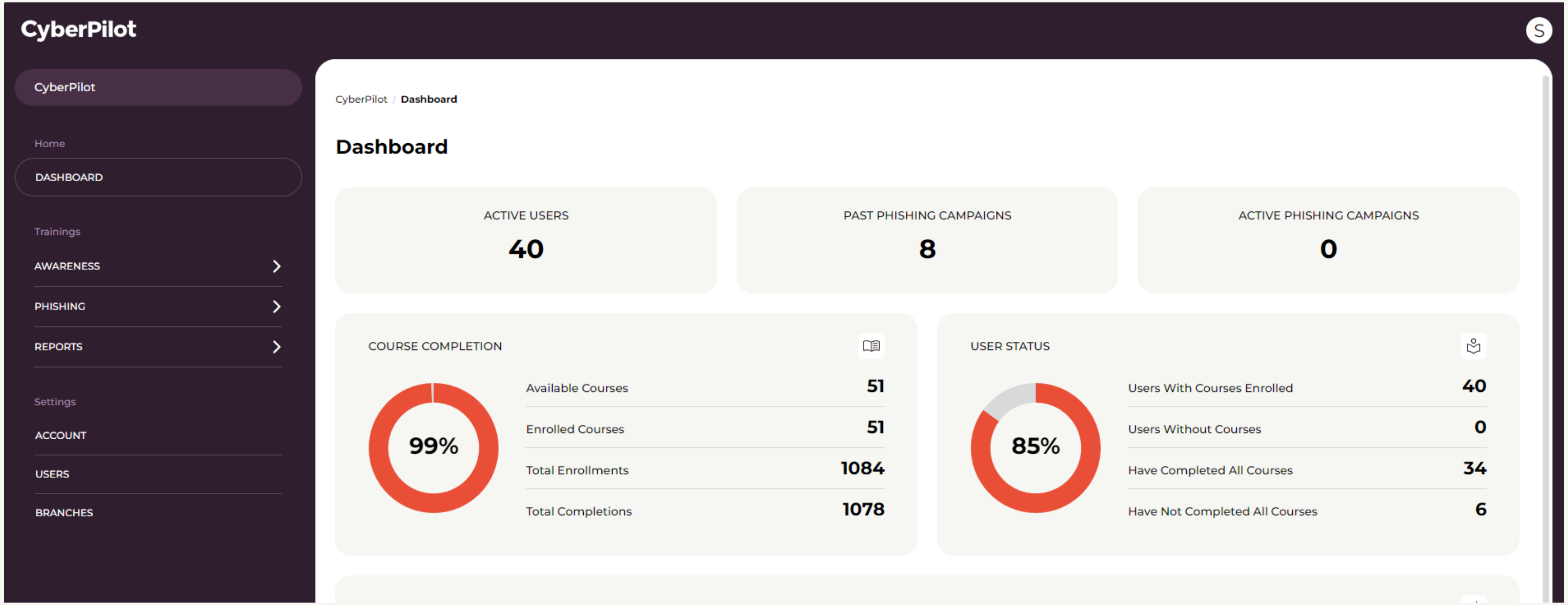


(4) Click on user icon

(5) Click on "Go to admin"

CYBERPILOT APP ADMINISTRATION

At https://www.cyberpilot.io/cyberpedia/introduction-to-cyberpilots-new-platform we have prepared an introduction video for you.



CyberPilot

CyberPilot

Home

DASHBOARD

Trainings

AWARENESS

PHISHING

REPORTS

Settings

ACCOUNT

USERS

BRANCHES

CyberPilot / Dashboard

Dashboard

ACTIVE USERS	PAST PHISHING CAMPAIGNS	ACTIVE PHISHING CAMPAIGNS
40	8	0

COURSE COMPLETION

99%

Available Courses	51
Enrolled Courses	51
Total Enrollments	1084
Total Completions	1078

USER STATUS

85%

Users With Courses Enrolled	40
Users Without Courses	0
Have Completed All Courses	34
Have Not Completed All Courses	6

Done

CyberPilot