
Migration Guide for CyberPilot

Note!

This guide is for CyberPilot customers without AD-integration.

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 **security-platform.dk**
- **CyberPilot App** is the platform with the URL **app.cyberpilot.io**

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 users receive a temporary password to the CyberPilot App. They change the password at first login. For security reasons we do not migrate users existing passwords.

Contents

- 1 Whitelist Notification emails from the CyberPilot App
- 2 Notify CyberPilot that you are ready for final migration step
- 3 Day of final migration step

① 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**, 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 labeled "(1) Go to https://security.microsoft.com/" points to the browser's address bar. Another red arrow labeled "(2) Click on 'Policies & Rules'" points to the "Policies & rules" option in the left-hand navigation menu.

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

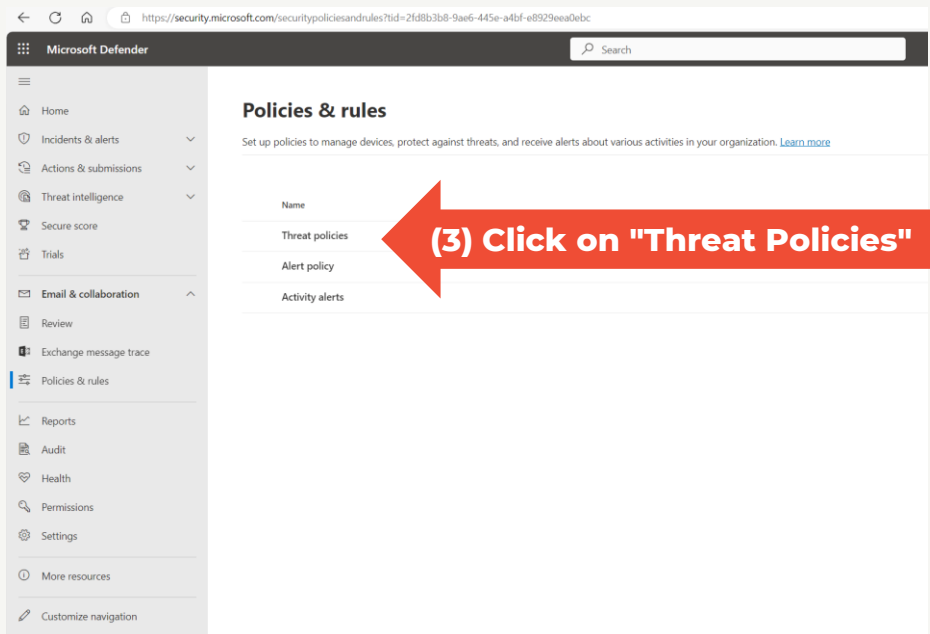
Check that you have an eligible license and the right permissions to get started with new, unified capabilities - incident management, automated investigations, and advanced hunting on Office 365, your endpoints, and your identities.

[Learn how to get started](#)

Microsoft Office 365 / Defender Guide

Step 3: Click on "Threat Policies"

Step 4: Click on "Anti-spam"



Microsoft Defender

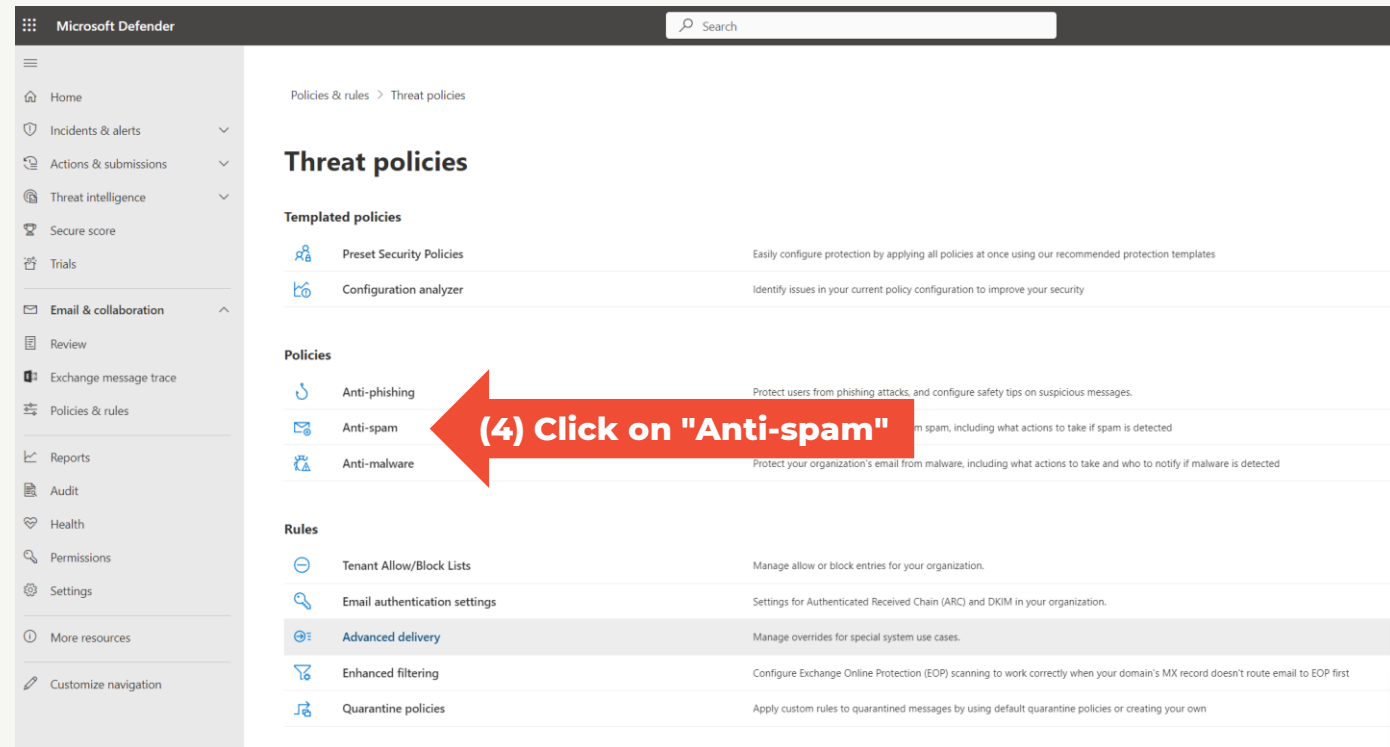
Search

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: Filter out 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

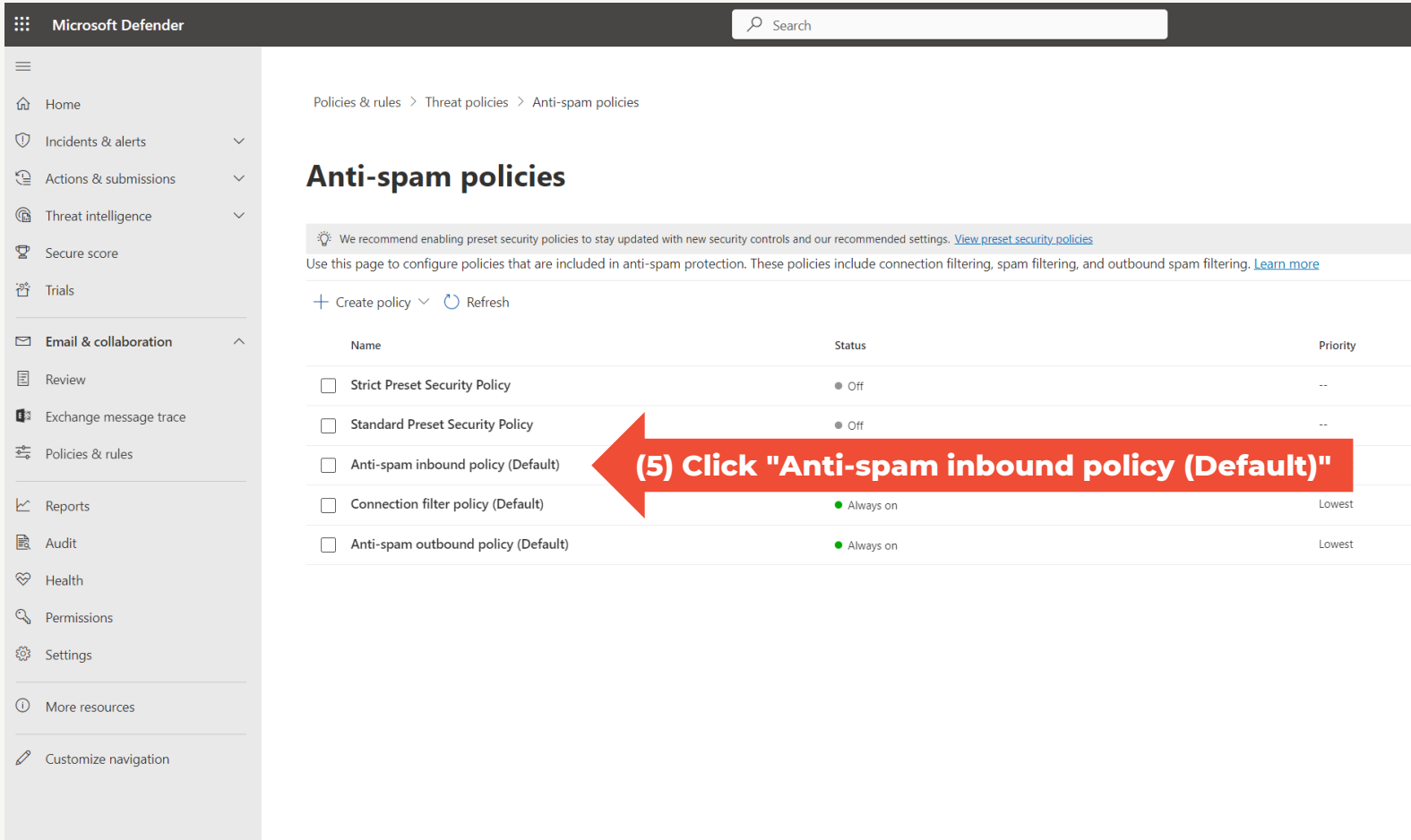
- Tenant Allow/Block Lists: Manage allow or block entries for your organization.
- Email authentication settings: Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
- Advanced delivery: Manage overrides for special system use cases.
- Enhanced filtering: Configure Exchange 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 controls for "Create policy" and "Refresh". 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 page displays a list of policies, including 'Anti-spam inbound policy (Default)' which is selected. A red arrow points to the 'Edit description' link.

(6) Scroll down

Microsoft Defender console showing the configuration page for the 'Anti-spam inbound policy (Default)'. The page displays various settings, including 'Bulk email spam action', 'Bulk email threshold', and 'URL to .biz or .info websites'. A red arrow points to the 'Edit allowed and blocked senders and domains' 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. On the left is a navigation pane with options like Home, Incidents & alerts, Actions & submissions, Trials, Email & collaboration, Review, Exchange message trace, Policies & rules, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main area displays 'Anti-spam policies' 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 |

Overlaid on the right is the 'Add senders' dialog box. It contains the instruction: 'Add an email address and press add. When you are done, click save to apply changes.' Below this is a 'Sender' input field with the placeholder 'Enter a custom sender address'. The email address 'notify@app.cyberpilot.io' has been entered and is shown as a tag. At the bottom of the dialog are 'Add senders' and 'Cancel' buttons.

(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 'Policies & rules > Threat policies > Anti-spam policies' and '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 users 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".

Three red arrows point to the search bar, the domain tags, and the "Add domains" button, with text labels for each step:

- (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 |

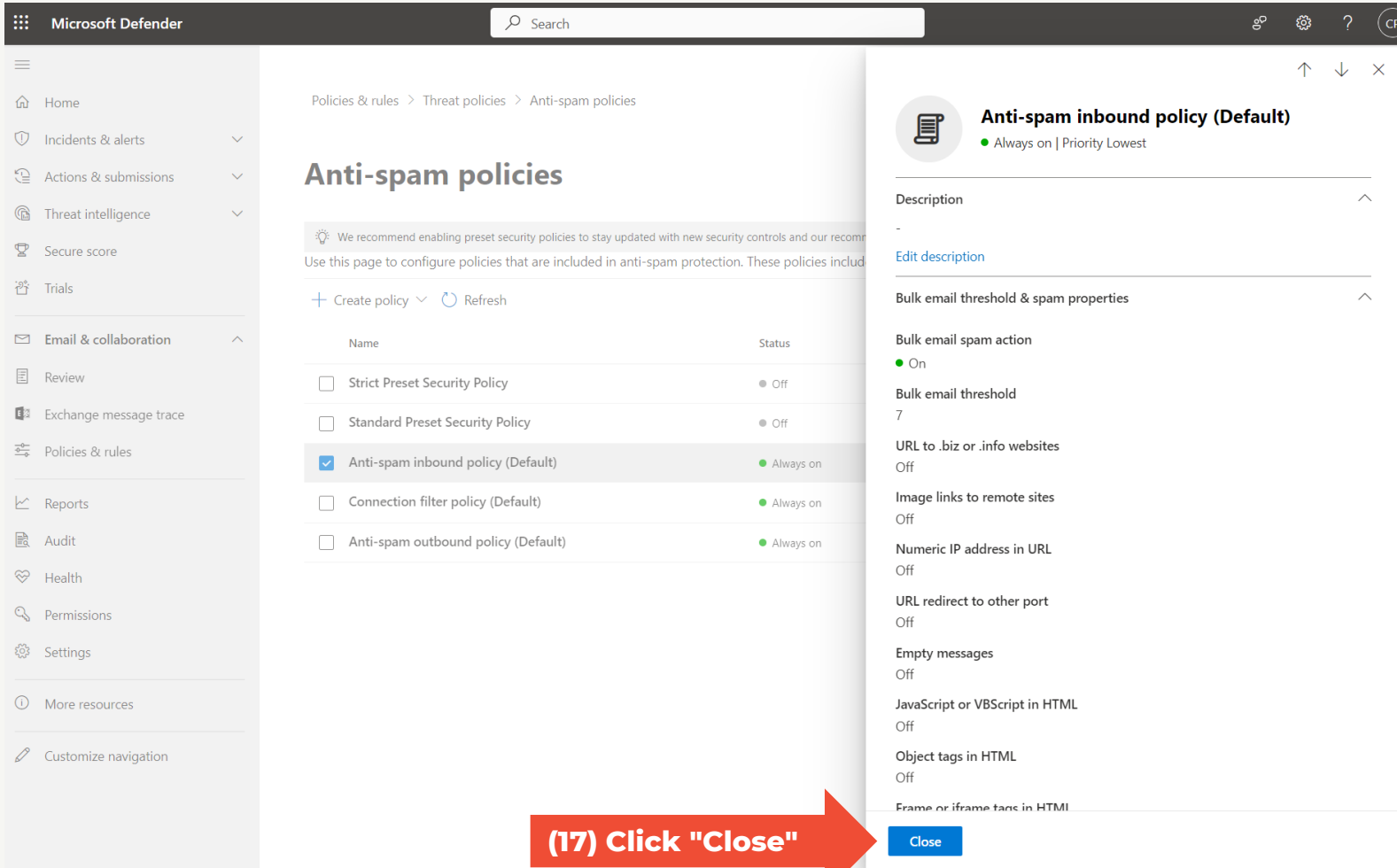
The screenshot shows the Microsoft Defender console with the 'Anti-spam policies' page open. A modal dialog titled 'Allowed and blocked senders and domains' is displayed. The dialog shows sections for 'Allowed' and 'Blocked' senders and domains. The 'Allowed' section lists 'Senders (1)' and 'Domains (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: 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 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 settings for bulk email threshold, spam properties, and various filtering options. A red arrow at the bottom of the screen points to a blue 'Close' button located at the bottom of the right-hand configuration pane.

| 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 |

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
Off

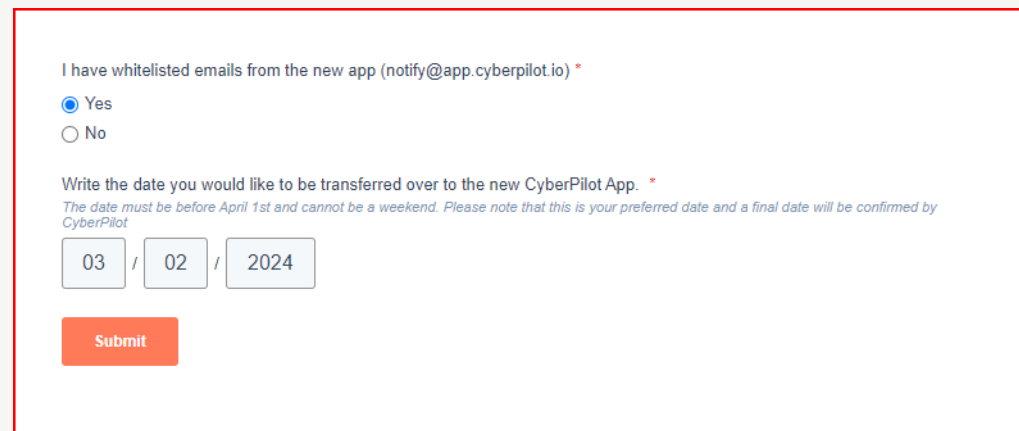
[Close](#)

② Notify CyberPilot that you are ready for final migration step

Notify CyberPilot that you are ready for the final migration step

When you 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.

A screenshot of a web form for migration confirmation. The form is enclosed in a red border. It contains a radio button question, a date picker, and a submit button.

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

Submit

③ Day of final migration step

Day of final migration step

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

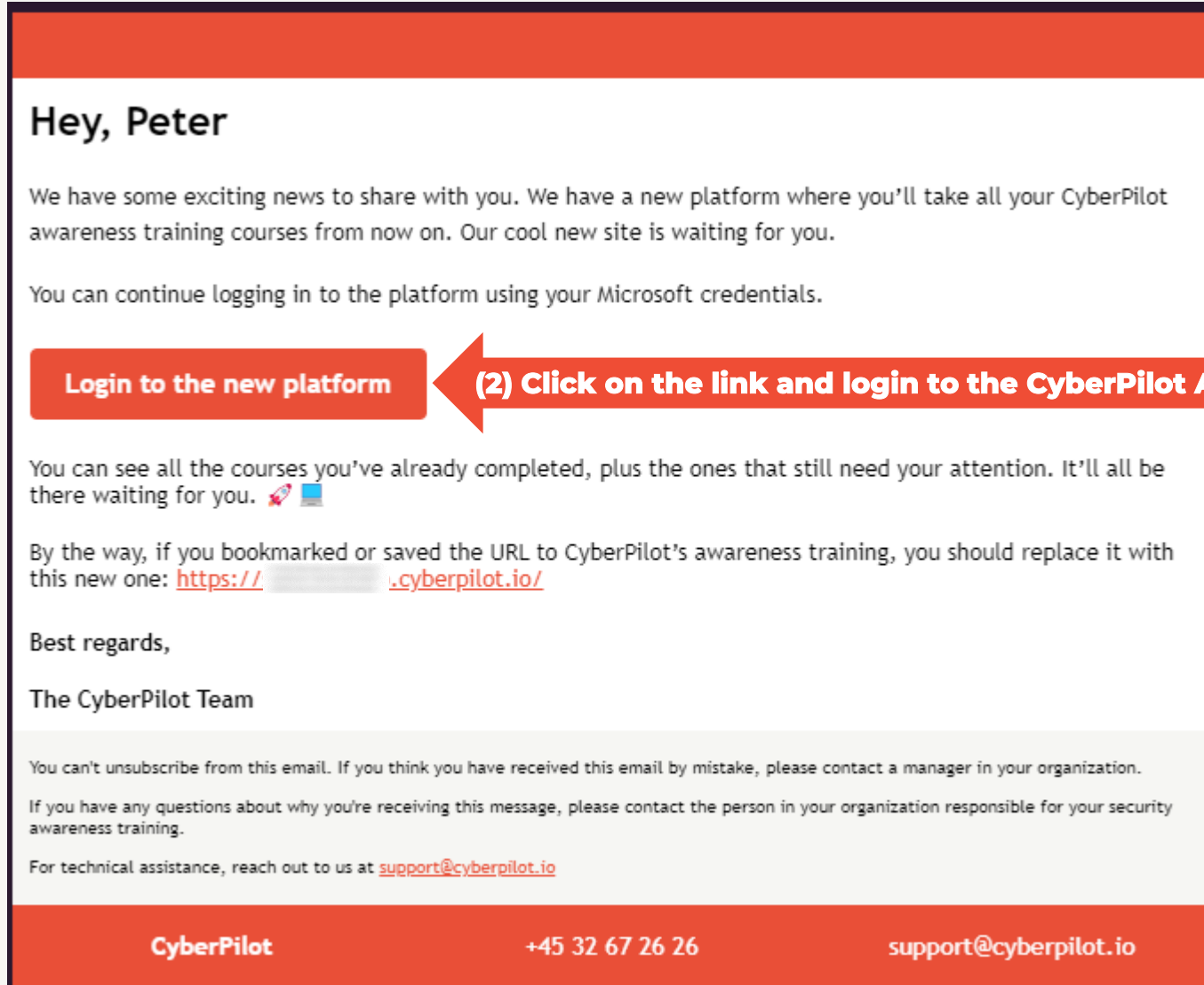
In eFront you may have both a normal user and an admin user. In the CyberPilot App you only have one user. You will therefore only receive one welcome mail.

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”



The image shows a screenshot of an email interface. At the top is a red header bar. Below it, the email content is on a white background. The text reads: 'Hey, Peter', followed by a paragraph about new training courses, and another paragraph about logging in with Microsoft credentials. A red button labeled 'Login to the new platform' is highlighted. A large red arrow points from the right towards this button, with the text '(2) Click on the link and login to the CyberPilot App' written inside the arrow. Below the button, there is more text about course progress and a URL replacement instruction. The email ends with 'Best regards, The CyberPilot Team'. At the bottom of the email content is a light grey footer with unsubscribe information and support contact details. A red footer bar at the very bottom contains the CyberPilot logo, phone number '+45 32 67 26 26', and email 'support@cyberpilot.io'.

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.

[Login to the new platform](#)

(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/](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.

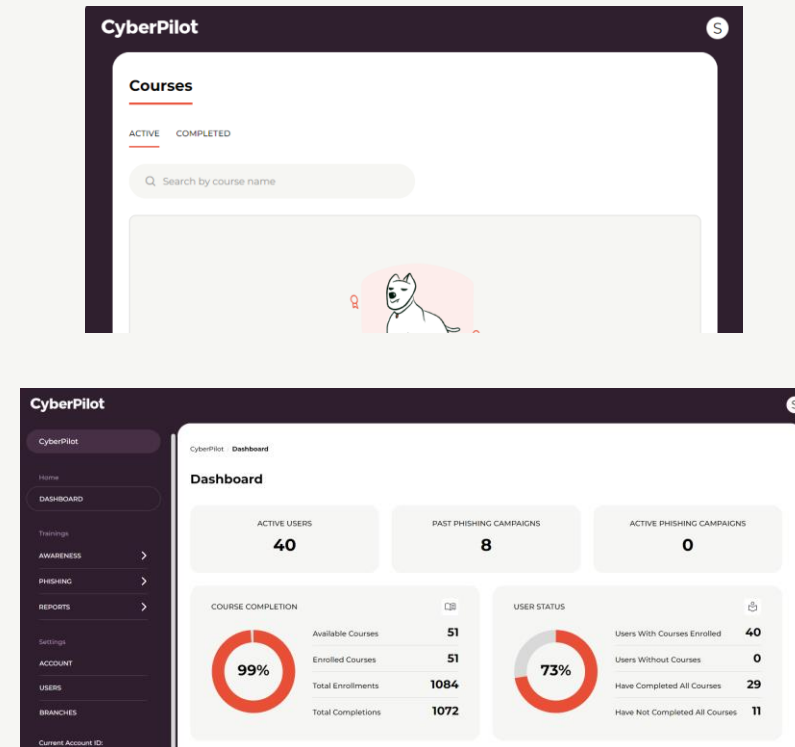
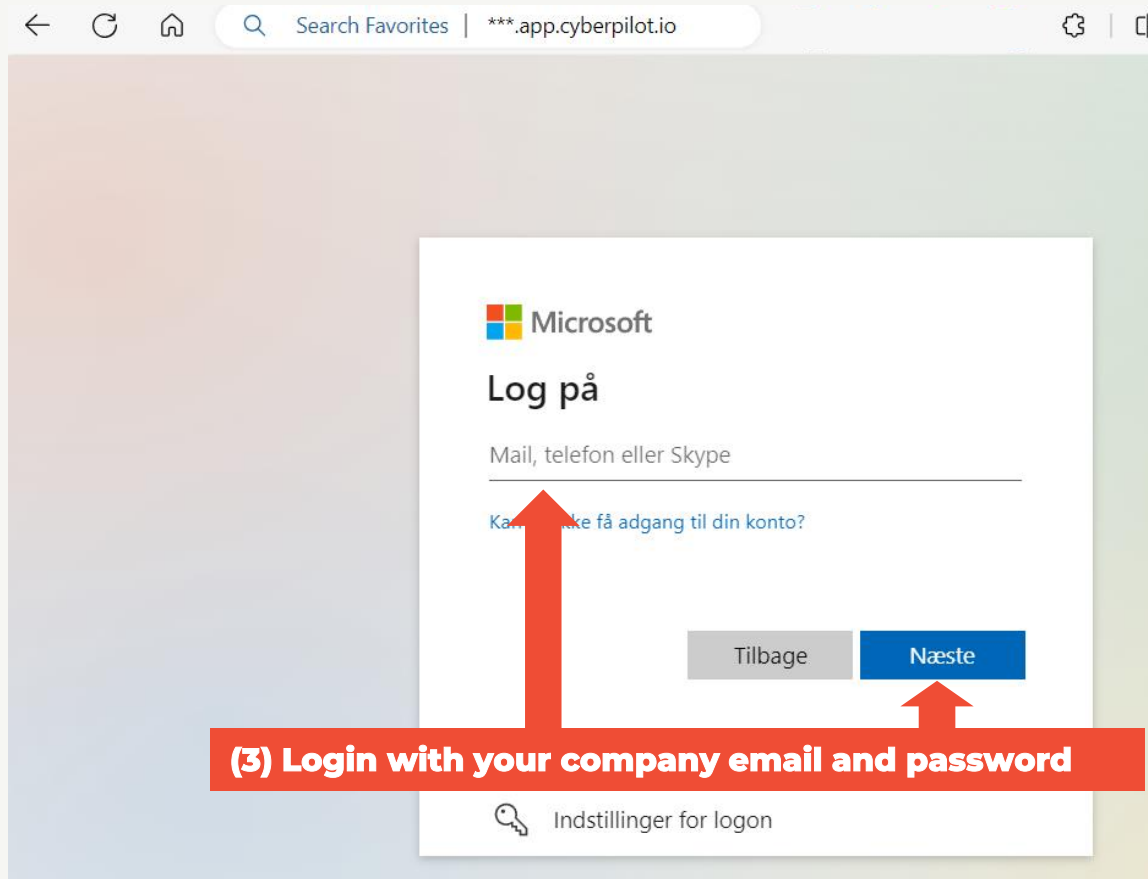
If you have any questions about why you're receiving this message, please contact the person in your organization responsible for your security awareness training.

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

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

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.



CYBERPILOT APP ADMINISTRATION

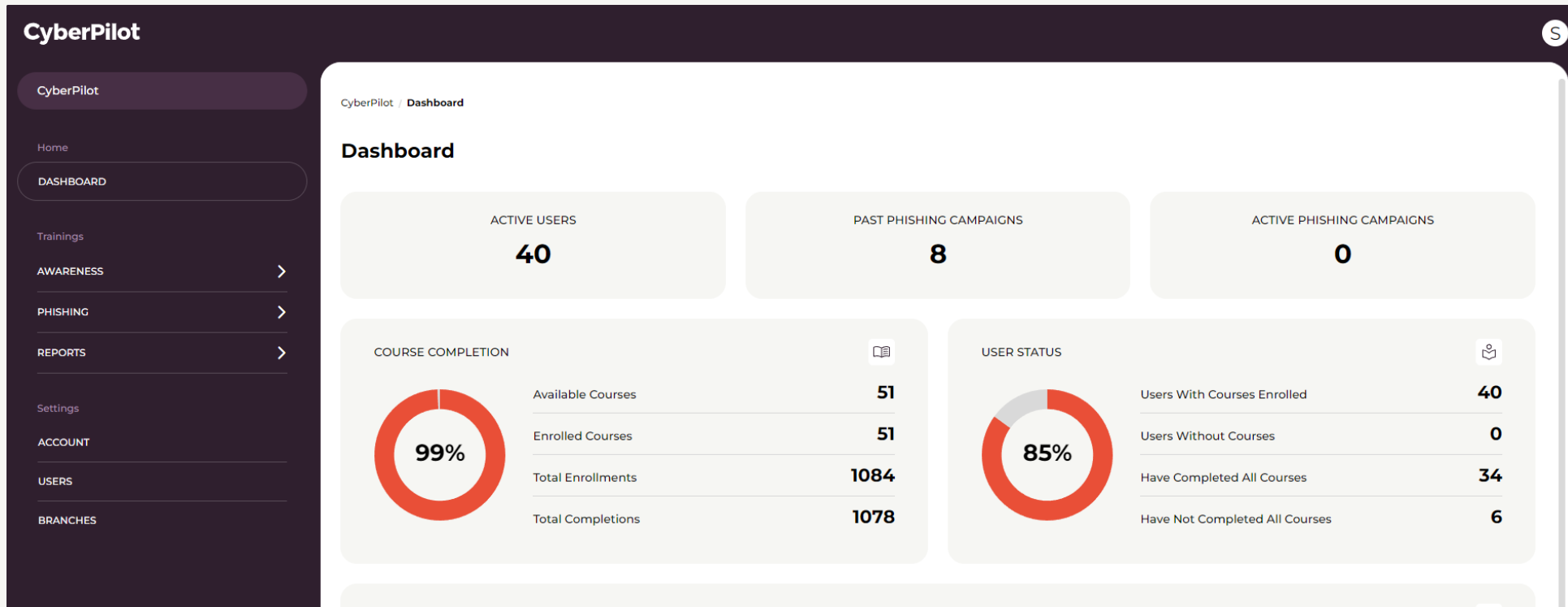
Step 4: Click on the user icon

Step 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.



Done