

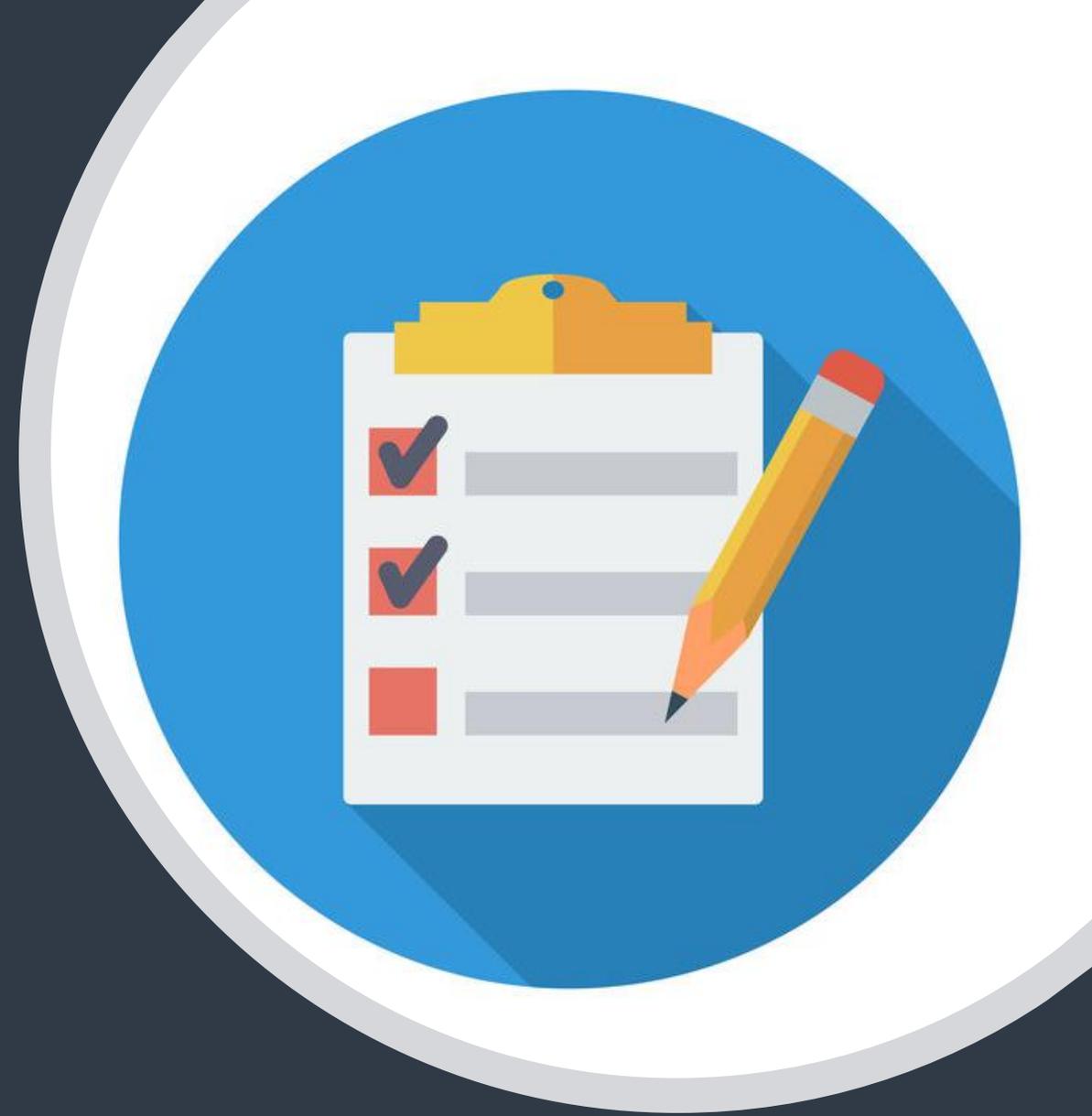
# Setup Guide

**Client Azure AD and  
CyberPilot platform  
using SAML**



# 1. Prerequisites for using SSO on the CyberPilot platform

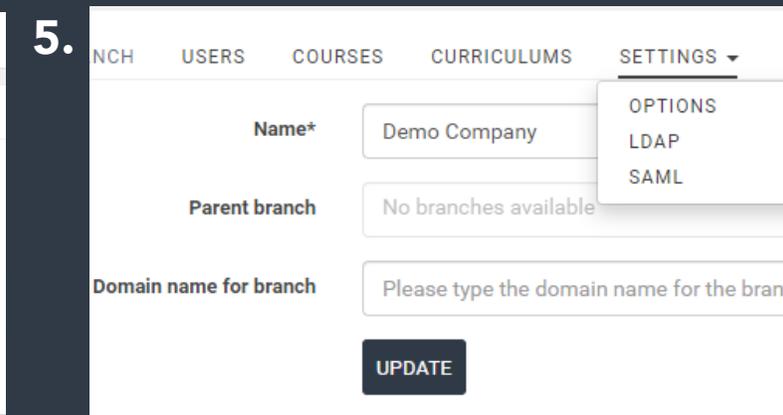
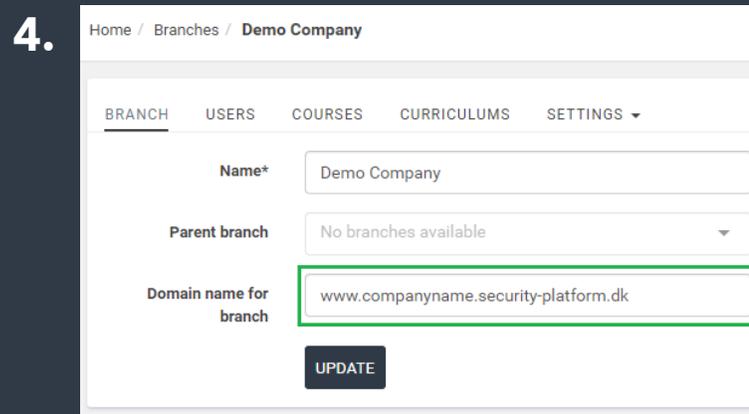
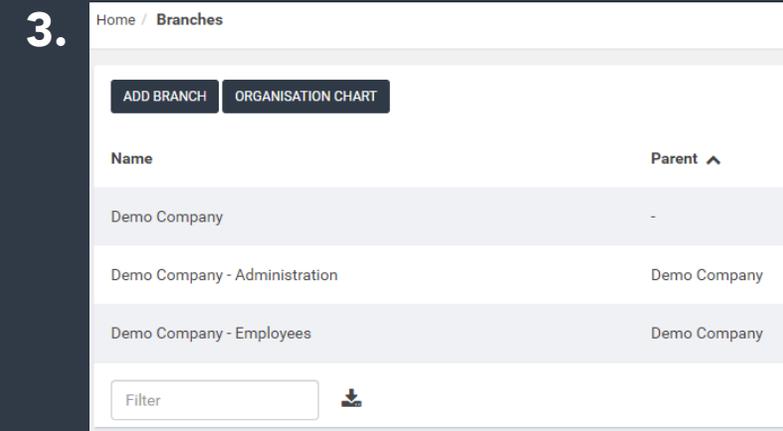
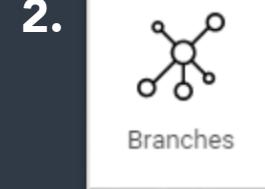
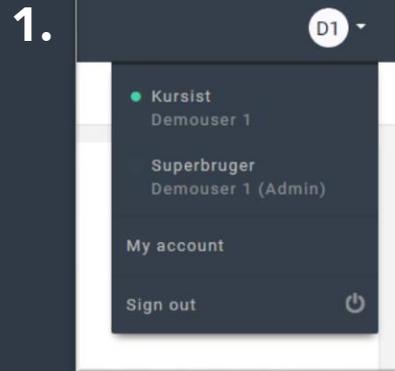
- To be able to link your Azure AD with CyberPilot' platform the you must have the following prerequisites.
- A person with Admin access to your organizations Azure AD.
- This user must have a Office 365 Premium P2 license to be able to create the application for the SSO.
- The rest of the staff members do typically not need a Premium P2 licenses to use SSO. However, you should check with your O365 provider whether your current plan allows for regular users to login via a custom SSO application.



# 2. Preperation - Login as admin on CyberPilot Platform

## Cyberpilot platform

1. Login to your learner account via the main CyberPilot portal on [www.security-platform.dk](http://www.security-platform.dk) and change to admin view in the top right corner.
2. Open the menu "Branches"
3. Click on the branch with your company name. In case there are subbranches, you should choose the branch that does not have a parent.
4. Under the tab "Branch" you find the URL for your customized portal. This is the URL that you will be logging in via. when the SSO is complete.
5. Click on "Settings" and choose SAML.



# 2. Preperation - Login as admin on CyberPilot Platform

## Cyberpilot platform

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

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

*REMEMBER: You already have a CyberPilot Admin account that is connected to your normal learner (kursist) user on the platform. It is ALWAYS the learner user that you will login as, and after login you can change to admin view. This means that you will never login directly to your admin account with any 0365 credentials.*

1.

BRANCH USERS COURSES CURRICULUMS SETTINGS

Enable SAML support

Create user if no match was found

Identity provider

Certificate fingerprint

Alternative certificate fingerprint

Remote Sign-in URL

Remote Sign-out URL

TargetedID

First name

Last name

Email

Custom fields

Sign SAML requests

Validate SAML requests

Assertion Consumer Service (ACS) URL

Single Logout Service URL

SP Metadata XML

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

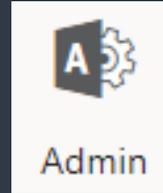
SAVE

## 2. Preperation - Login as admin Azure AD

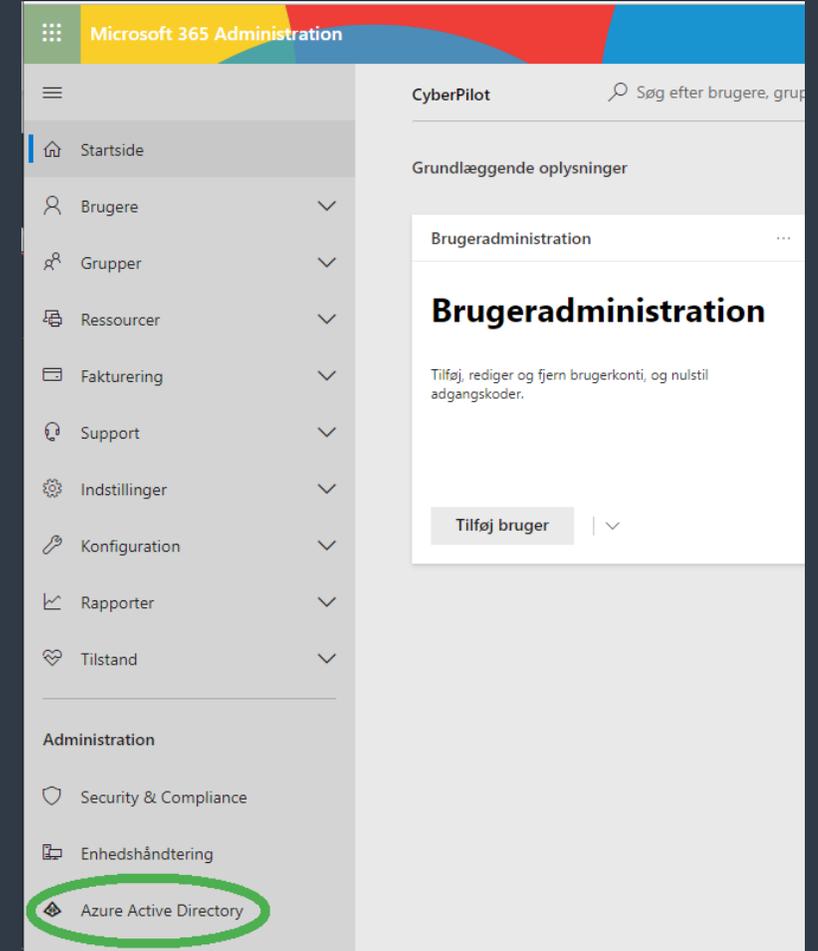
### Azure AD

1. Login to the admin module in O365
2. In the Admin module – open Azure Active directory

1.



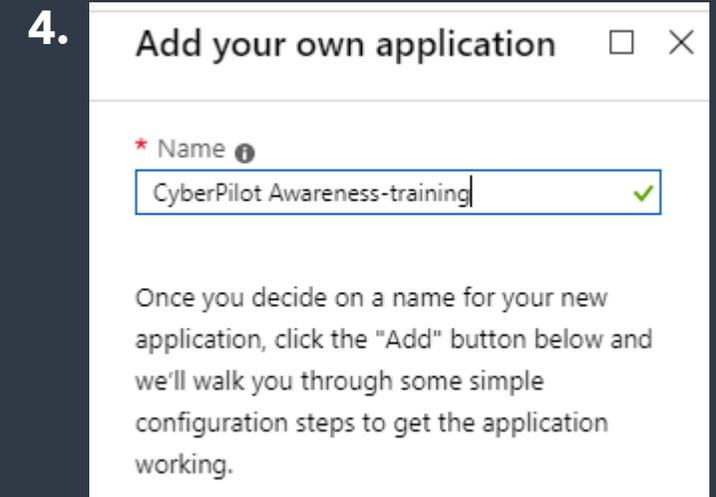
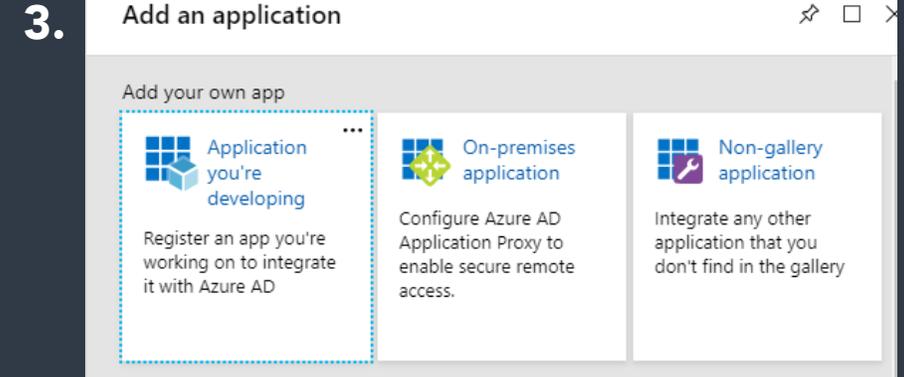
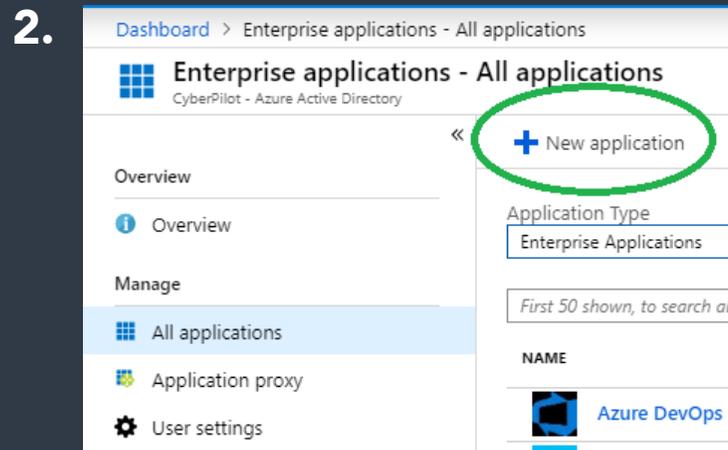
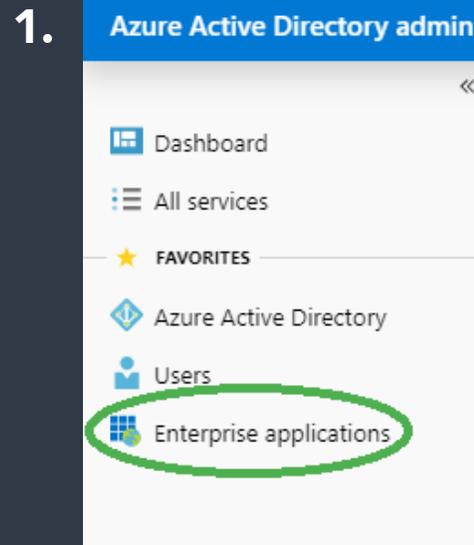
2.



# 3. Configuring Azure AD

## Creating an application

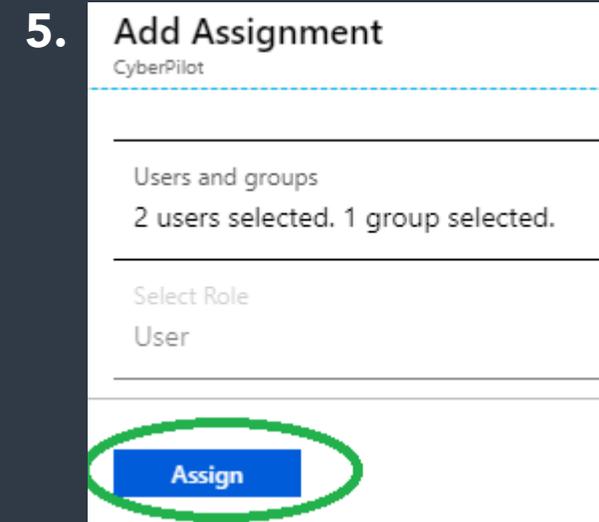
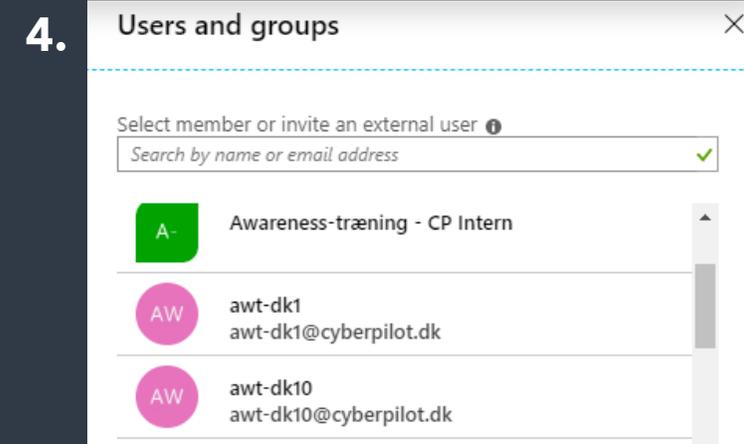
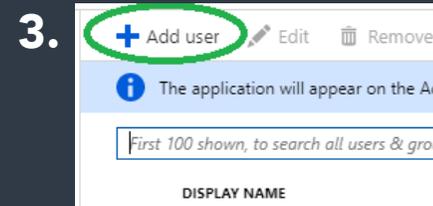
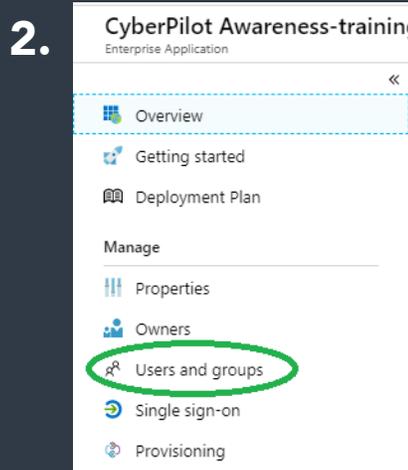
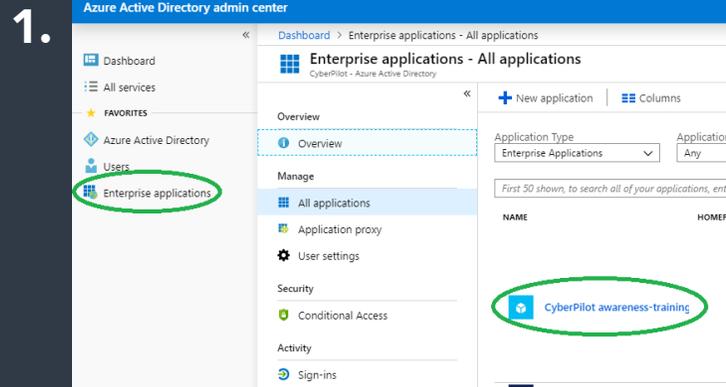
1. Click on Enterprise applications
2. Click on +New application
3. Select Non-gallery application
4. Give the application an appropriate name. Fx CyberPilot Awareness-training.
5. Click Add and wait while the application is created.



# 3. Configuring Azure AD

## Add users/groups to application

1. Click on Enterprise applications and open the application you created.
2. Select Users and groups
3. Click +Add user
4. Select the users and/or groups that will be participating in the Awareness-training
5. When all users/groups have been chosen – click select.
6. Remember to also click assign in the next menu.

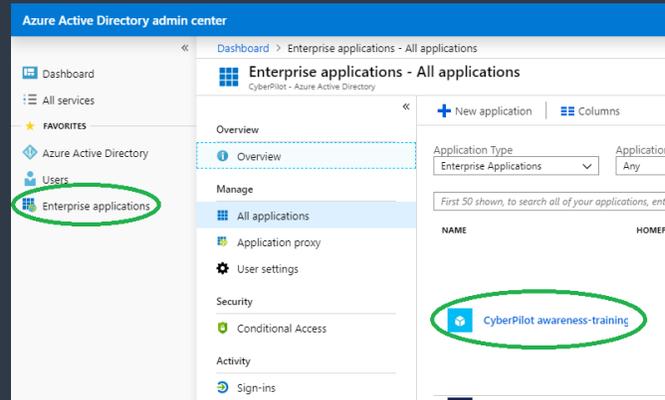


# 3. Configuring Azure AD Application

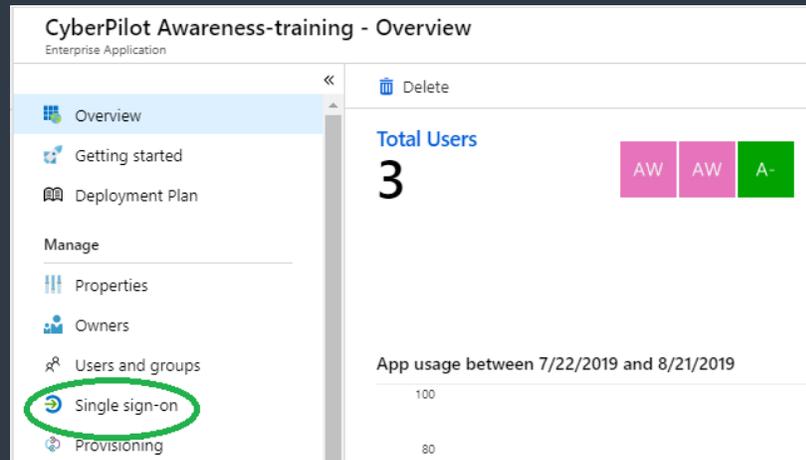
## Configuring the application

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

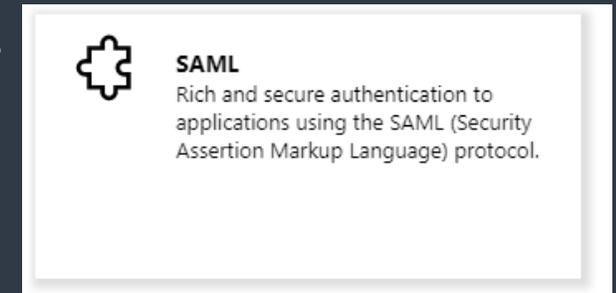
1.



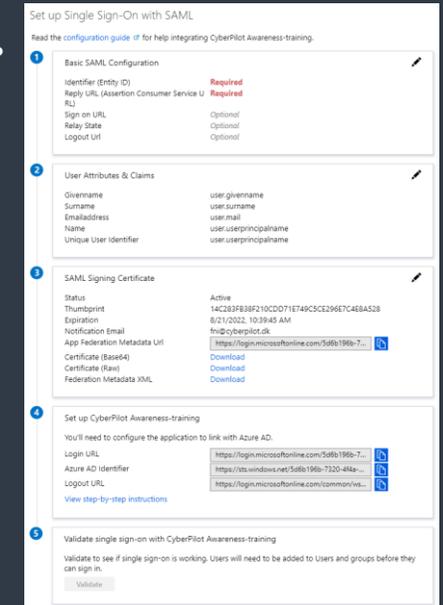
2.



3.



4.



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

## Step 1 – basic SAML configuration

1. Insert the URL for your loginpage. This URL has been created to you by CyberPilot. I has the format:

[www.companyname.security-platform.dk](http://www.companyname.security-platform.dk)

2. Copy/paste the URL from CyberPilot SAML settings. "Assertion Consumer Service (ACS) URL" to "Reply URL" in the Azure Application.

3. Copy/paste the URL from CyberPilot SAML settings "Single Logout Service URL" to "Logout URL" in the Azure Application.

4. Click save and close the page.

5. If a pop appears to validate the application. Choose validate later

5.

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

Yes

No, I'll validate later

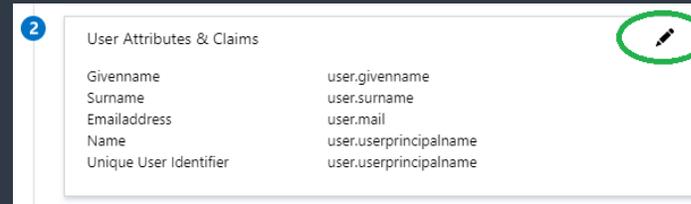
The image shows two side-by-side screenshots. The left screenshot is the 'Basic SAML Configuration' page for an 'Azure Single Sign-on Application'. It features several input fields: 'Identifier (Entity ID)' with the value 'www.YOURCOMPANYNAMEsecurity-platform.dk' circled in green and labeled '1.'; 'Reply URL (Assertion Consumer Service URL)' with the value 'https://www.security-platform.dk/saml/module.php/saml/sp/saml2-acs.php/efront-sp' circled in green and labeled '2.'; and 'Logout URL' with the value 'https://www.security-platform.dk/saml/module.php/saml/sp/saml2-logout.php/efront-sp' circled in green and labeled '3.'. A 'Save' button is circled in green and labeled '4.'. The right screenshot is the 'CyberPilot SAML Settings' page, showing various configuration options like 'Enable SAML support', 'Identity provider', 'Certificate fingerprint', and 'Remote Sign-in URL'. A green arrow points from the 'Reply URL' field in the left screenshot to the 'Assertion Consumer Service (ACS) URL' field in the right screenshot. Another green arrow points from the 'Logout URL' field in the left screenshot to the 'Single Logout Service URL' field in the right screenshot. A 'SAVE' button is visible at the bottom of the right screenshot.

# 5. Configuring Claims and attributes (in CP SAML settings)

## Step 2 – Attributes and claims

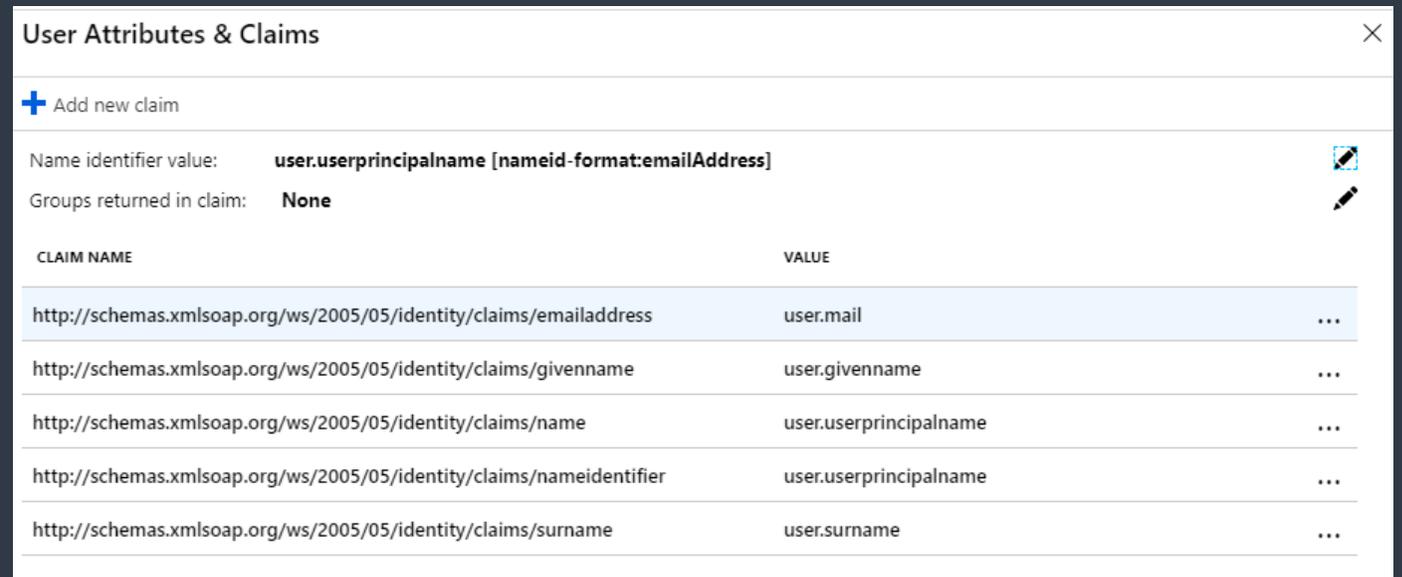
1. Click edit on step 2- User Attributes and claims (in the Single Sign-on settings in the Azure Application)
2. In the menu you find the CLAIM NAME's. These must be copy/pasted into the CyberPilot SAML Settings. See next page.

1.



3.

2.



# 5. Configuring Claims and attributes (in CP SAML settings)

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

Azure Value	CyberPilot SAML field
User.mail	TargetedID + Email
User.givenname	First name
User.surname	Last name

**User Attributes & Claims** **Azure Single Sign-on Application**

+ Add new claim

Name identifier value: **user.userprincipalname [nameid-format:emailAddress]**

Groups returned in claim: **None**

CLAIM NAME	VALUE
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a>	user.mail
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	user.givenname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	user.userprincipalname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a>	user.userprincipalname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>	user.surname

**CyberPilot SAML Settings**

Alternative certificate fingerprint: e.g. c9ed4dfb07caf13fc21e0fec1572047eb8a7a4c

Remote Sign-in URL: e.g. https://openidp.feide.no/simplesaml/saml2/id

Remote Sign-out URL: e.g. https://openidp.feide.no/simplesaml/saml2/id

TargetedID: http://schemas.xmlsoap.org/ws/2005/05/identity/

First name: http://schemas.xmlsoap.org/ws/2005/05/identity/

Last name: http://schemas.xmlsoap.org/ws/2005/05/identity/

Email: http://schemas.xmlsoap.org/ws/2005/05/identity/

Custom fields: Comma separated list of more attributes

# 6. Configuring Step 3 and 4

## Step 3+4

1. Copy/paste the URL's onto the CyberPilot SAML Settings. Click save

The screenshot displays the CyberPilot SAML Settings configuration page, divided into two main sections: 'SAML Signing Certificate' (Step 3) and 'Set up CyberPilot Awareness-training' (Step 4). The right side of the page shows the SAML configuration form with various fields. Green boxes and lines highlight the mapping of values from the left panel to the right panel.

**Step 3: SAML Signing Certificate**

- Status: Active
- Thumbprint: 14C283FB38F210CDD71E749C5CE296E7C4E8A528
- Expiration: 8/21/2022, 10:39:45 AM
- Notification Email: fni@cyberpilot.dk
- App Federation Metadata Url: https://login.microsoftonline.co...
- Certificate (Base64): Download
- Certificate (Raw): Download
- Federation Metadata XML: Download

**Step 4: Set up CyberPilot Awareness-training**

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

- Login URL: https://login.microsoftonline.co...
- Azure AD Identifier: https://sts.windows.net/5d6b19...
- Logout URL: https://login.microsoftonline.co...

**SAML Configuration Form (Right Panel)**

- Enable SAML support:
- Create user if no match was found:
- Identity provider: https://sts.windows.net/5d6b196b-7320-4f4a-92c2...
- Certificate fingerprint: 14C283FB38F210CDD71E749C5CE296E7C4E8A5
- Alternative certificate fingerprint: e.g. c9ed4dfb07caf13fc21e0fec1572047eb8a7a4c
- Remote Sign-in URL: https://login.microsoftonline.com/5d6b196b-7320...
- Remote Sign-out URL: https://login.microsoftonline.com/common/wsfed

**Annotations:**

- The Thumbprint value from Step 3 is copied into the Certificate fingerprint field.
- The Login URL from Step 4 is copied into the Remote Sign-in URL field.
- The Azure AD Identifier from Step 4 is copied into the Identity provider field.
- The Logout URL from Step 4 is copied into the Remote Sign-out URL field.

# 7. Finalizing setup

## CyberPilot SAML settings

1. In the Cyberpilot settings make sure that these settings are ticked active.
2. Leave the remaining options unticked.
3. Click save
4. Open a new browser window and go to your custom branch URL.

1.  Enable SAML support

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

2.  Create user if no match was found

Sign SAML requests

Validate SAML requests

3. Home / Branches / Demo Company

BRANCH USERS COURSES CURRICULUMS SETTINGS ▾

Name\* Demo Company

Parent branch No branches available ▾

Domain name for branch www.companyname.security-platform.dk

UPDATE

# 7. Finalizing setup

## Checking the login page

1. Go to your custom URL. You should see something similar to this.
2. Note, that when logging in through this portal, you will need to use your O365 credentials instead of your old CyberPilot login. Please try logging in to check, if it works as intended.
3. Note, that users will not be able to login until they have an active user in the CyberPilot system. So before any of your users can access the site, we need to create them on the platform first.
4. Remember to inform CyberPilot if everything works as expected 😊

1.

