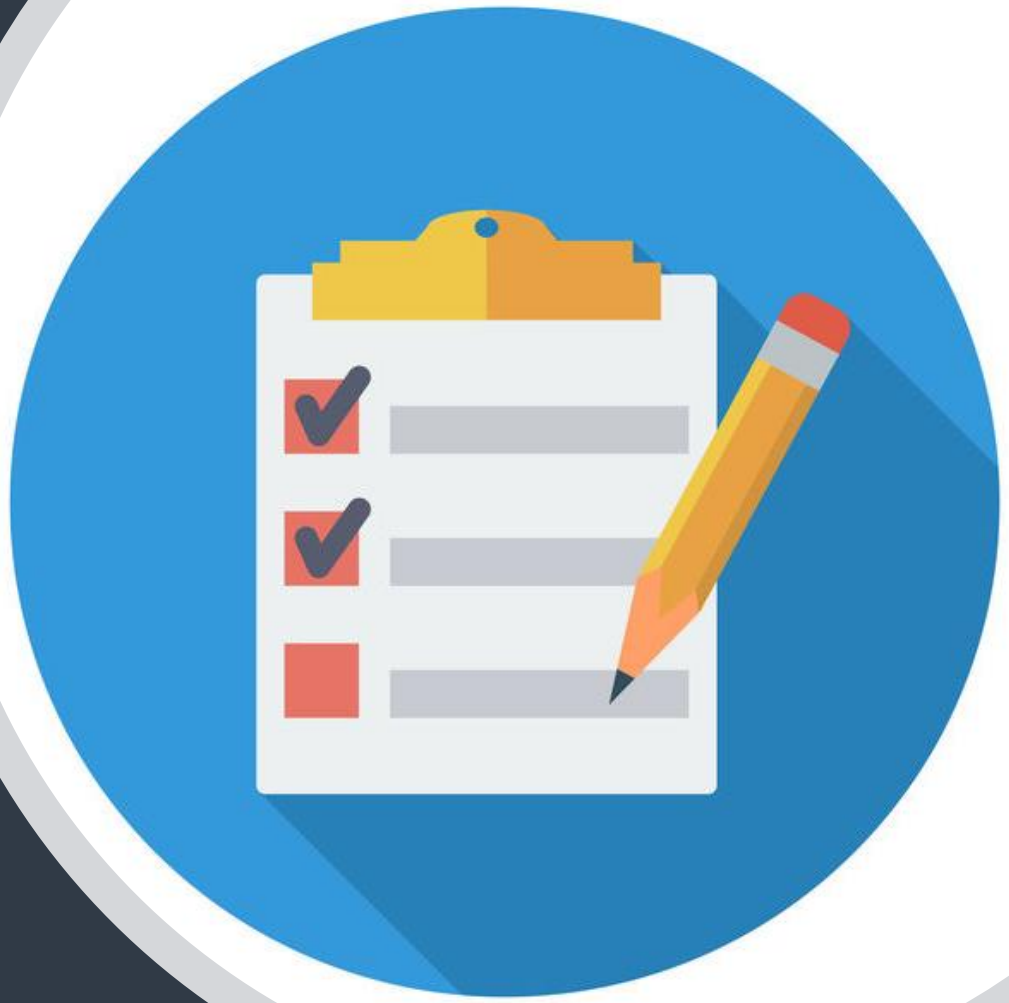
Setup Guide

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.

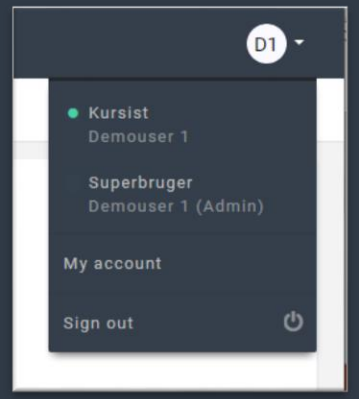


2. Preperation - Login as admin on CyberPilot Platform

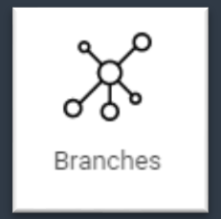
Cyberpilot platform

1. Login to your learner account via the main CyberPilot portal on www.security-platform.dk and change to admin view in the top right corner.
2. Open the menu "Branches"
3. Click on the branch with your comany 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.

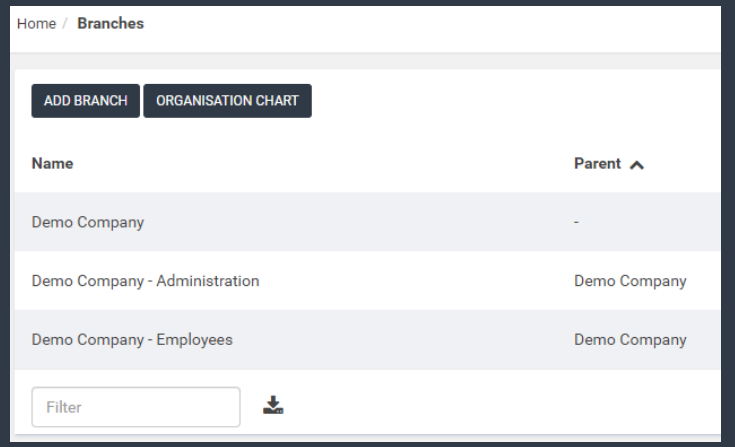
1.



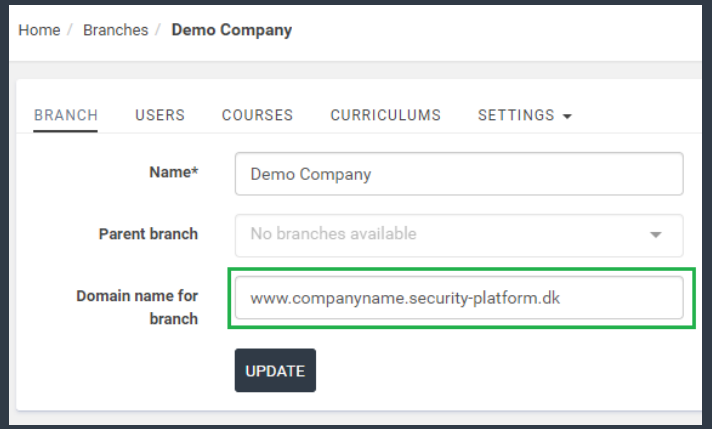
2.



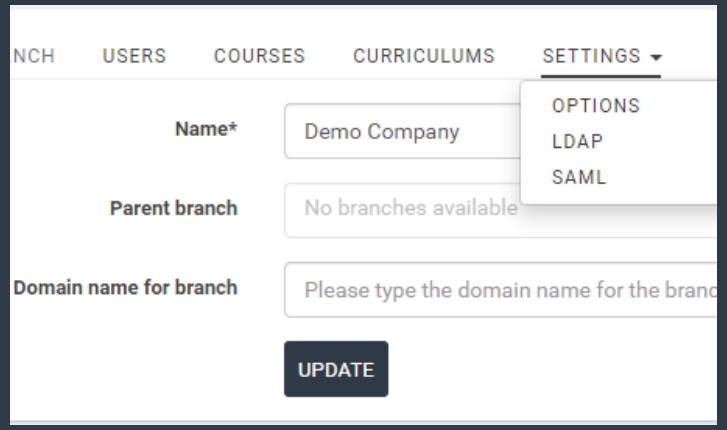
3.



4.



5.



2. Preperation - Login as admin on CyberPilot Platform

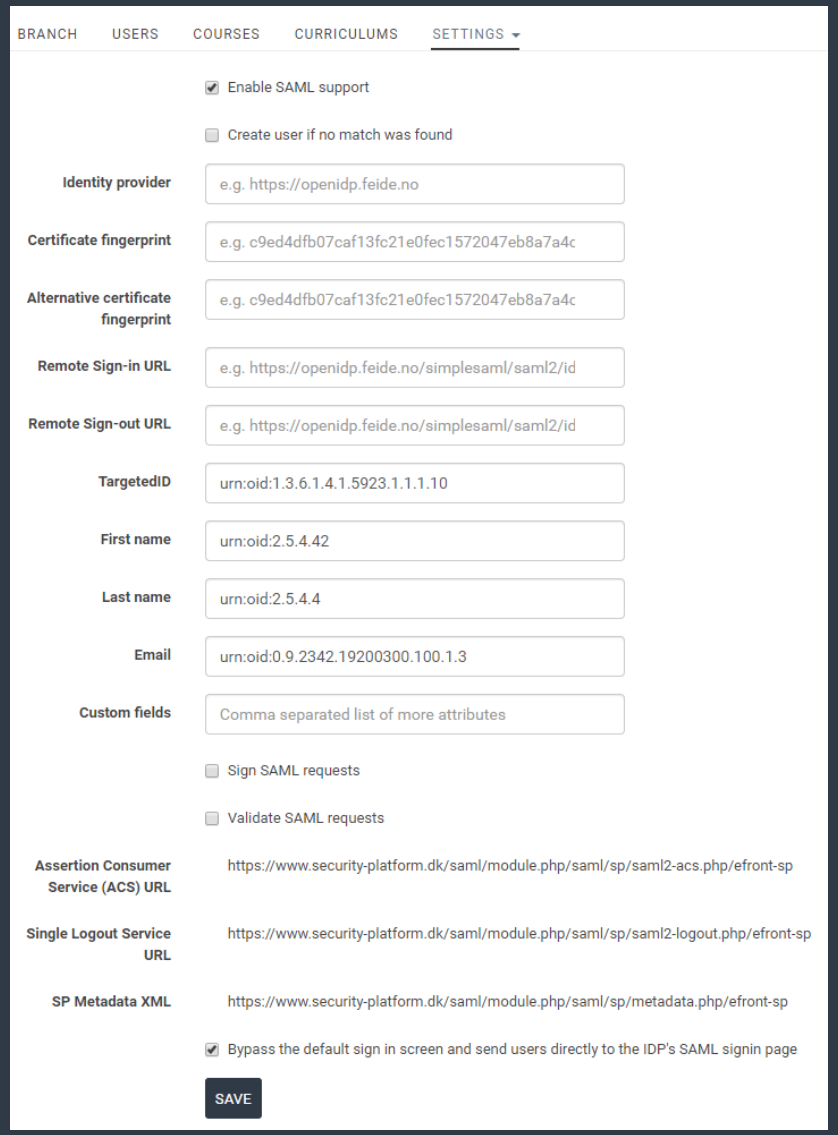
Cyberpilot platform

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.

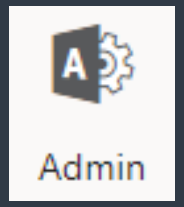


2. Preperation - Login as admin Azure AD

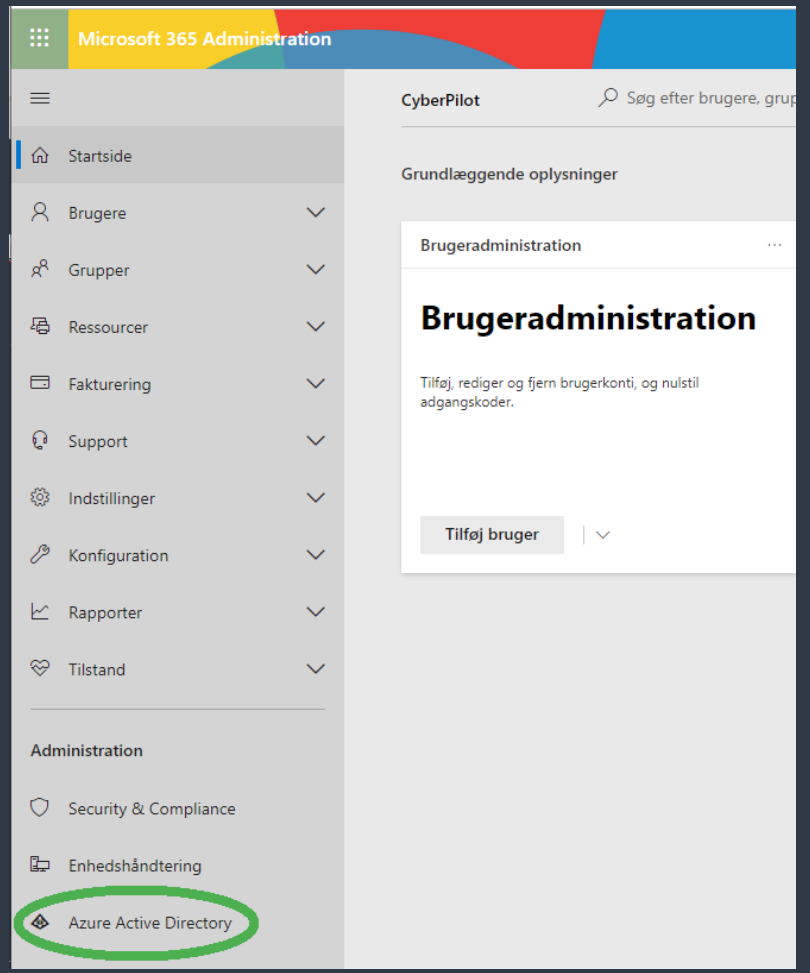
Azure AD

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

1.



2.

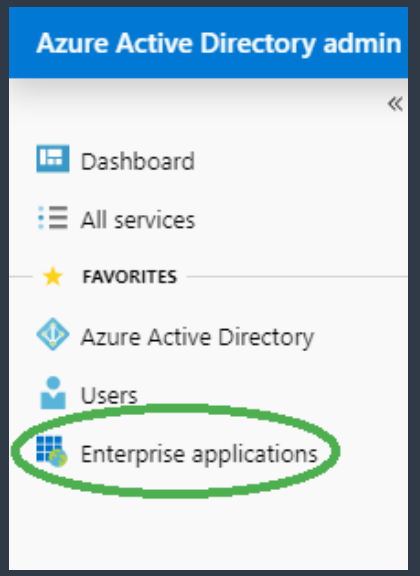


3. Configuring Azure AD

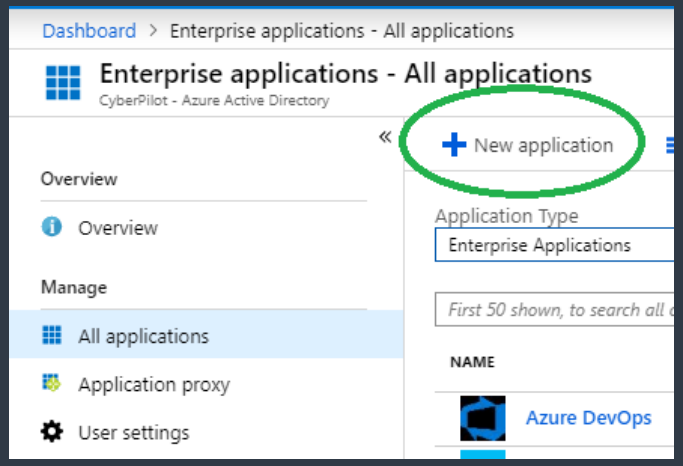
Creating an application

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.

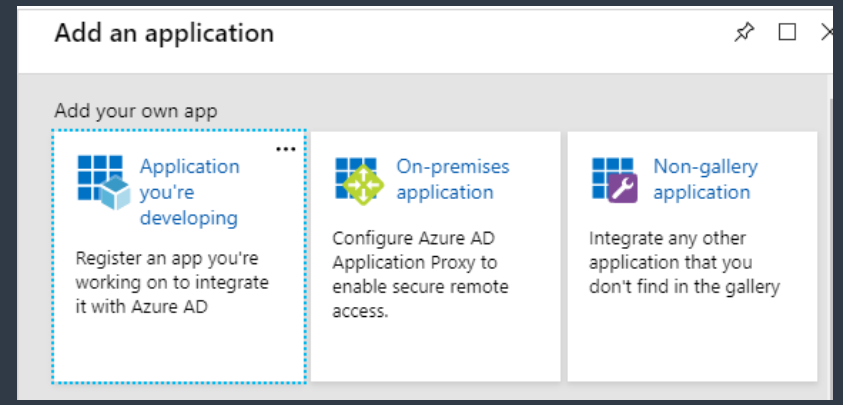
1.



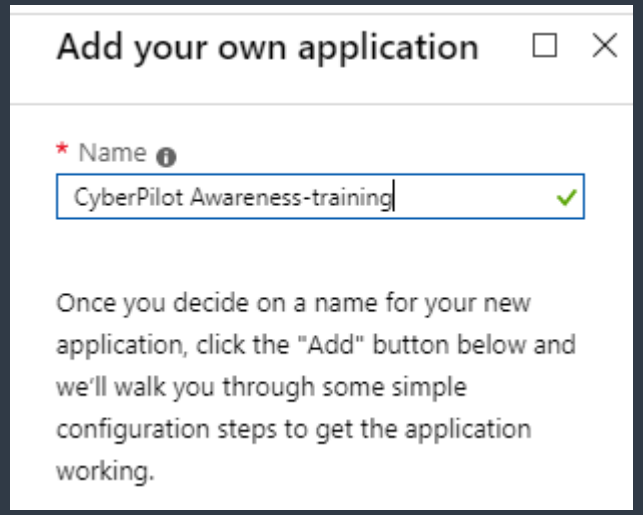
2.



3.



4.

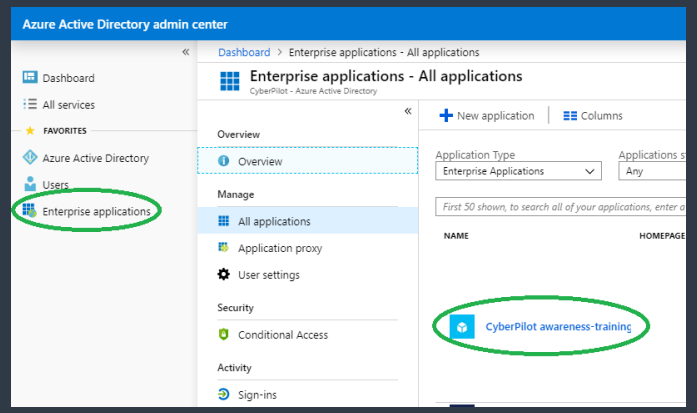


3. Configuring Azure AD

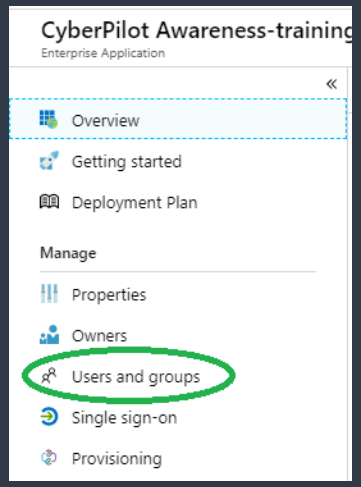
Add users/groups to application

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

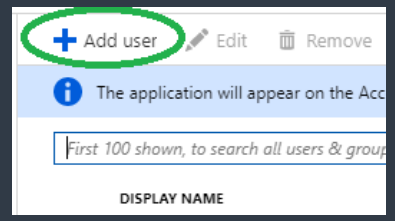
1.



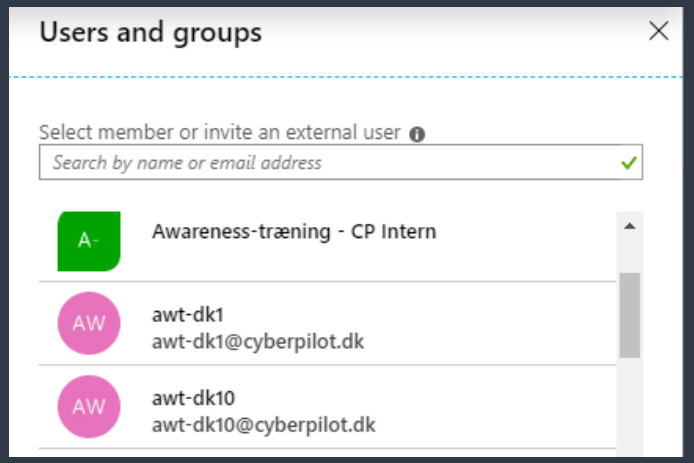
2.



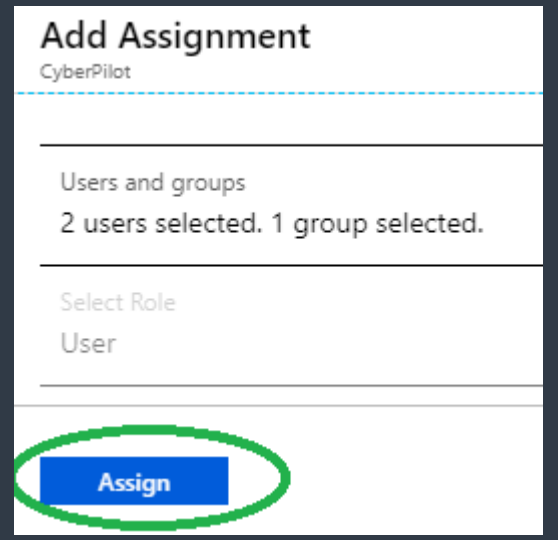
3.



4.



5.

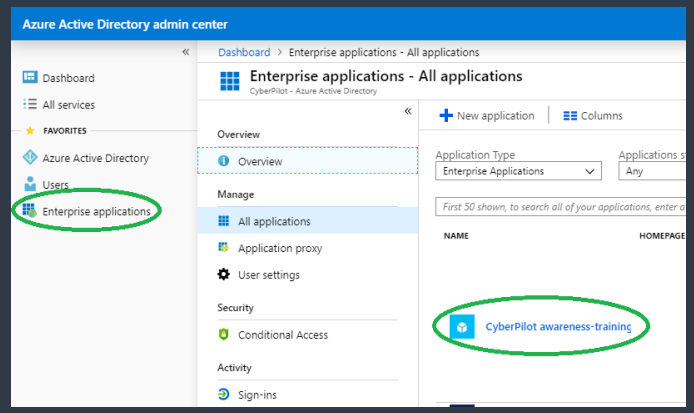


3. Configuring Azure AD Application

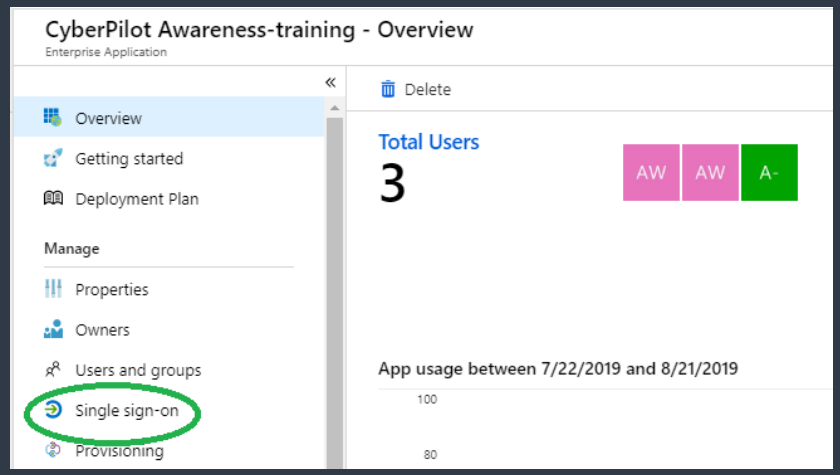
Configuring the application

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.

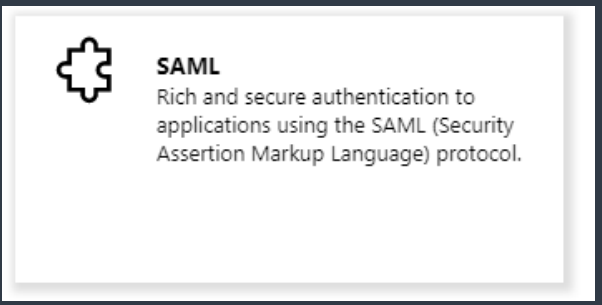
1.



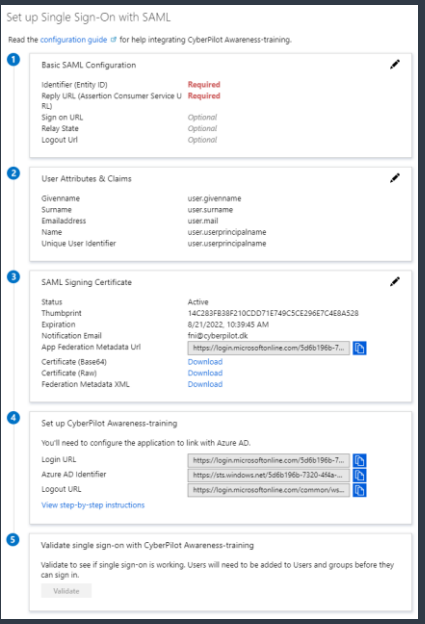
2.



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

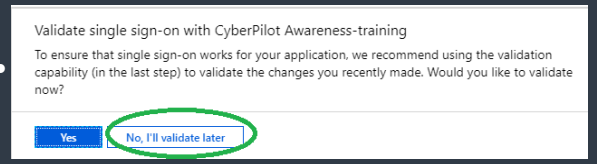
2. Copy/paste the URL from CyberPilot SAML settings. "Assertion Consumer Service (ACS) URL" to "Reply URL" in the Azure Application.

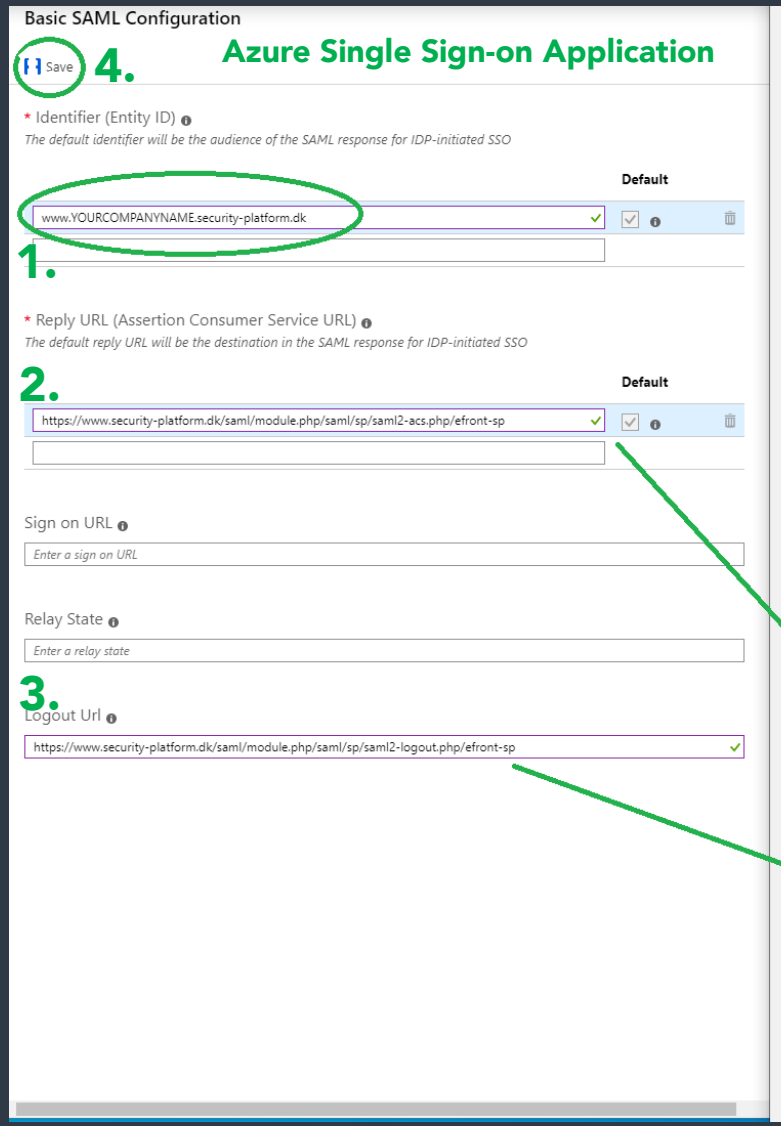
3. Copy/paste the URL from CyberPilot SAML settings "Single Logout Service URL" to "Logout URL" in the Azure Application.

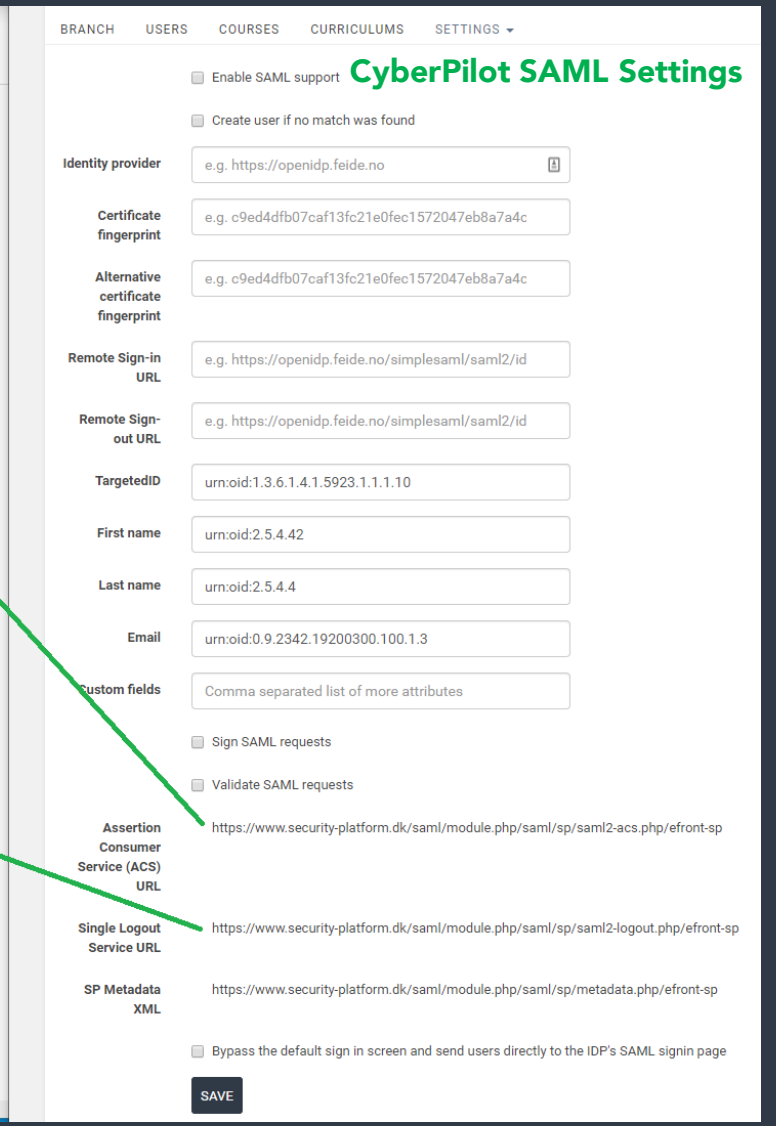
4. Click save and close the page.

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

5.





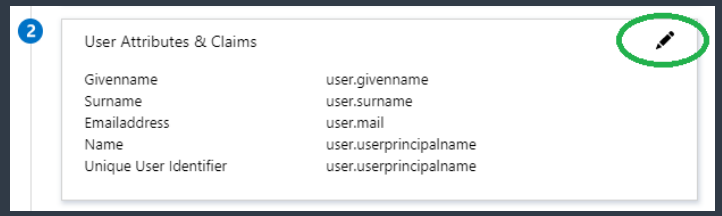


5. Configuring Claims and attributes (in CP SAML settings)

Step 2 – Attributes and claims

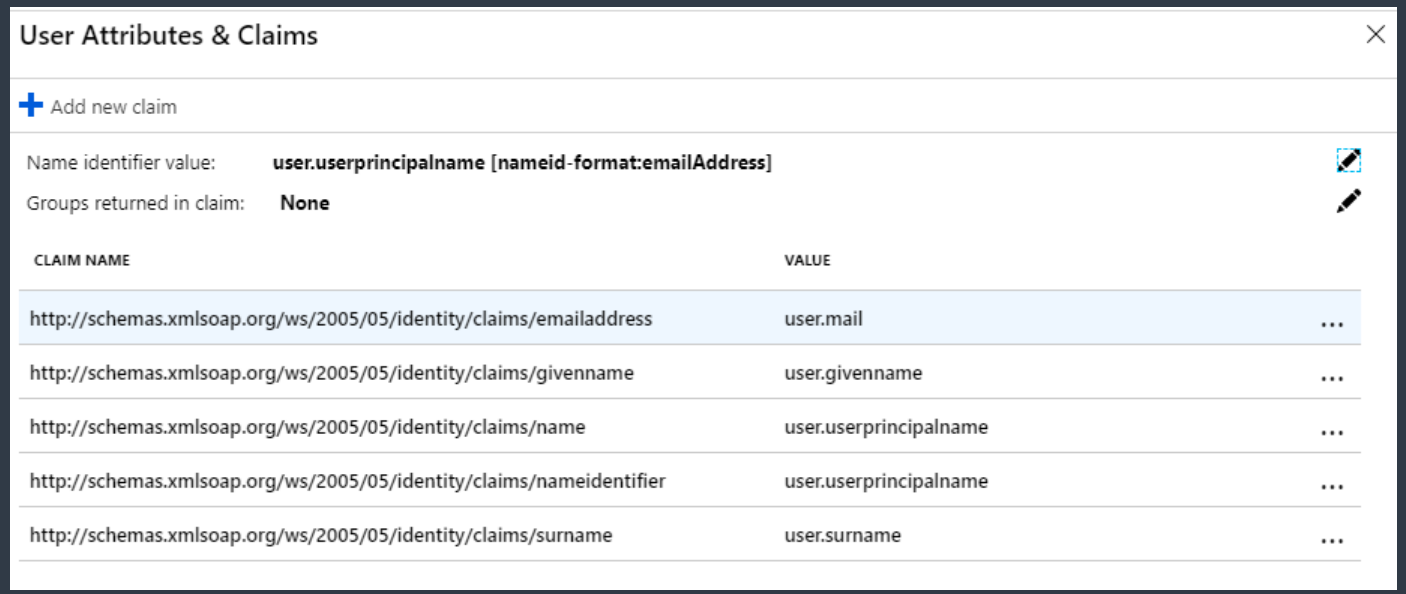
1. Click edit on step 2- User Attributes and claims *(in the Single Sign-on settings in the Azure Application)*
2. In the menu you find the CLAIM NAME's. These must be copy/pasted into the CyberPilot SAML Settings. See next page.

1.



3.

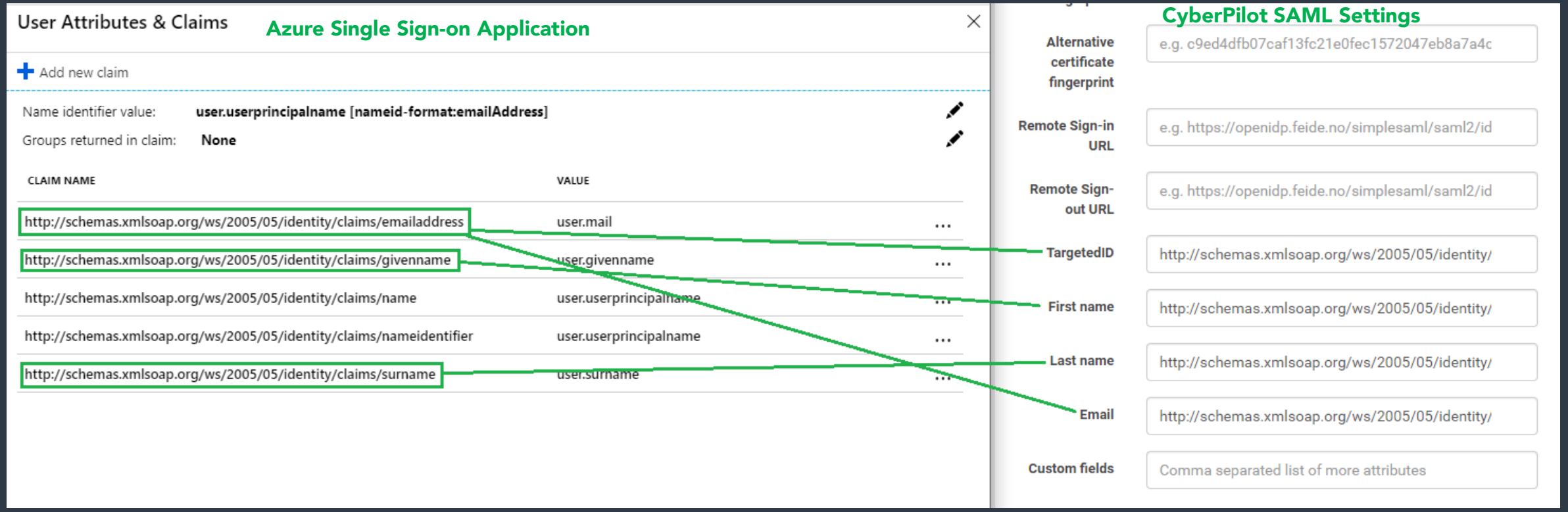
2.



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

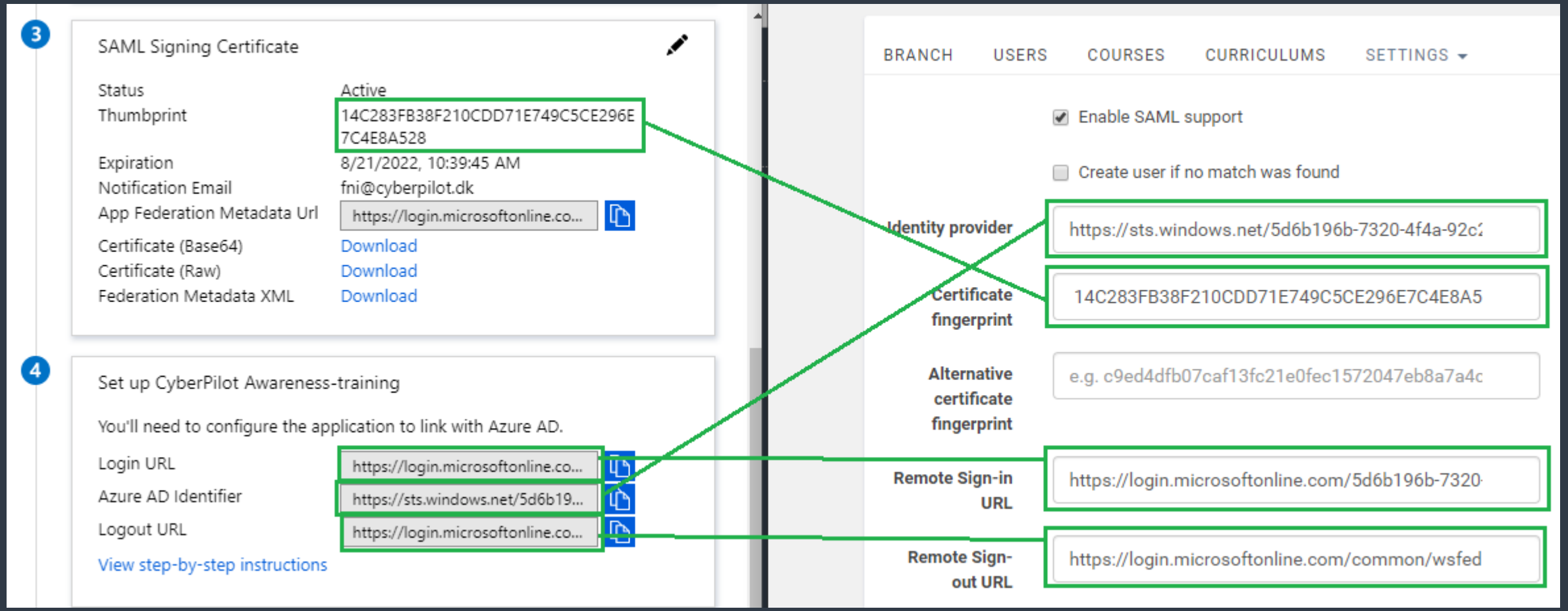
Azure Value	CyberPilot SAML field
User.mail	TargetedID + Email
User.givenname	First name
User.surname	Last name



6. Configuring Step 3 and 4

Step 3+4

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

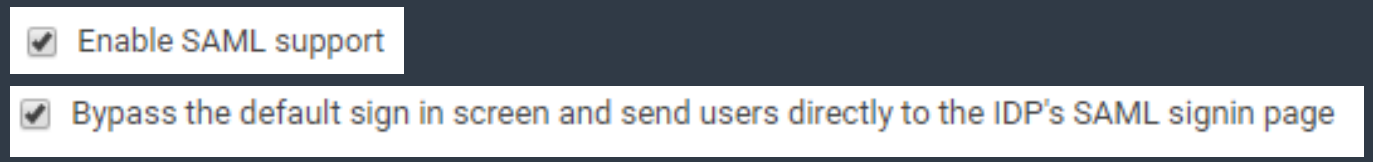


7. Finalizing setup

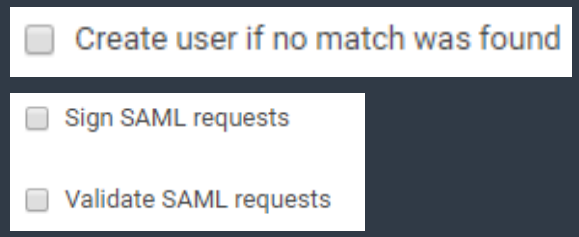
CyberPilot SAML settings

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.

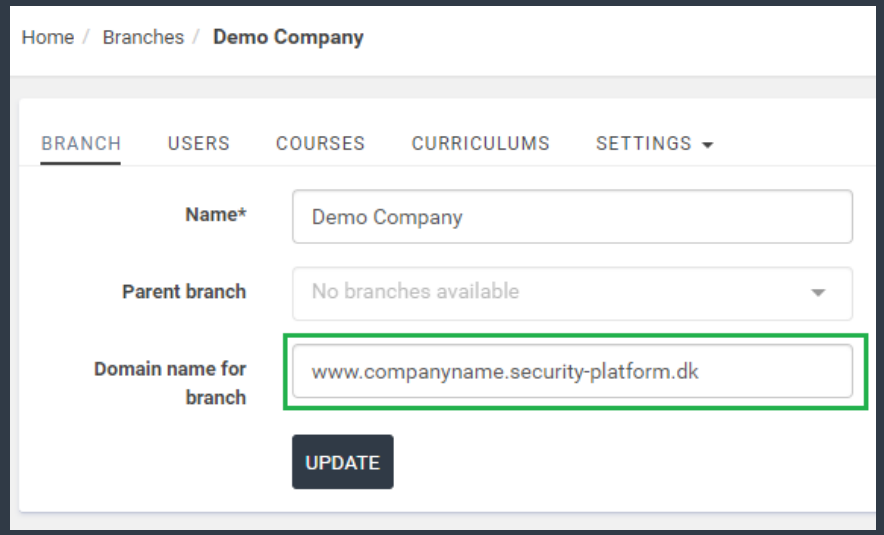
1.



2.



3.



7. Finalizing setup

Checking the login page

1. Go to your custom URL. You should see something similar to this.
2. Note, that when loggin in through this portal, you will need to use your O365 credentials instead of your old CyberPilot login. Please try loggin 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.