

Enabling single sign-on authentication (SSO) for Azure Active Directory (Azure AD)

Background Info



This feature is available in Lucy 4.6 or newer version.

This article describes step by step instruction of the SSO integration with Azure AD. An additional information about what SSO in Lucy is designed for can be found [here](#).

What preparations need to be done before connecting to Azure AD?

- Upload or create an SSL certificate for Lucy Admin console - see [this article](#).
- Make sure you have an Administrator account in Lucy (Settings > Users) with an email address that corresponds to your account in Azure Active Directory. Both accounts must have the same email address:

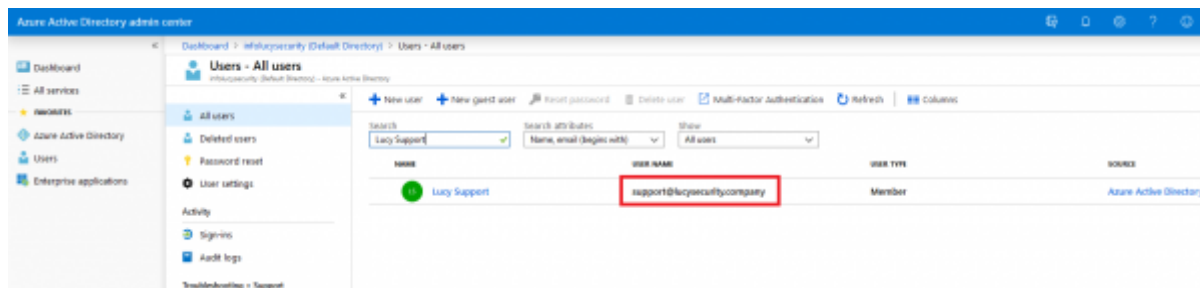
Home / Users / Lucy Support

Lucy Support

Email	<input type="text" value="support@lucysecurity.company"/>	
Country Code	<input type="text" value="Please select..."/>	
Phone	<input type="text"/>	
Two-Factor Authentication is not configured.		
Name	<input type="text" value="Lucy Support"/>	
Role	<input type="text" value="Administrator"/>	
<input type="checkbox"/> Enable incident reports notifier		
Change Password		

Current Certificate	N/A
<input type="checkbox"/> Certificate Required	

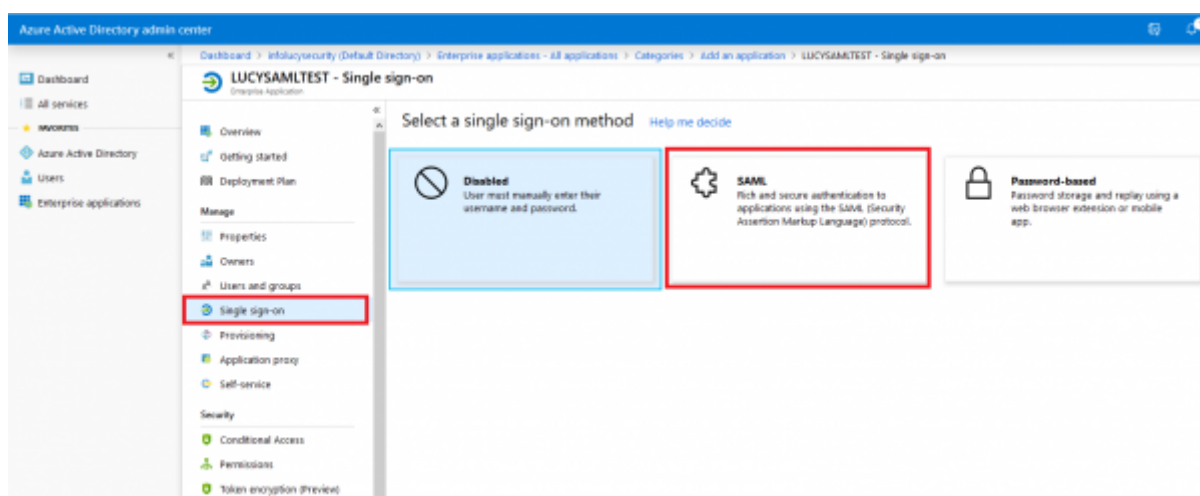
Save



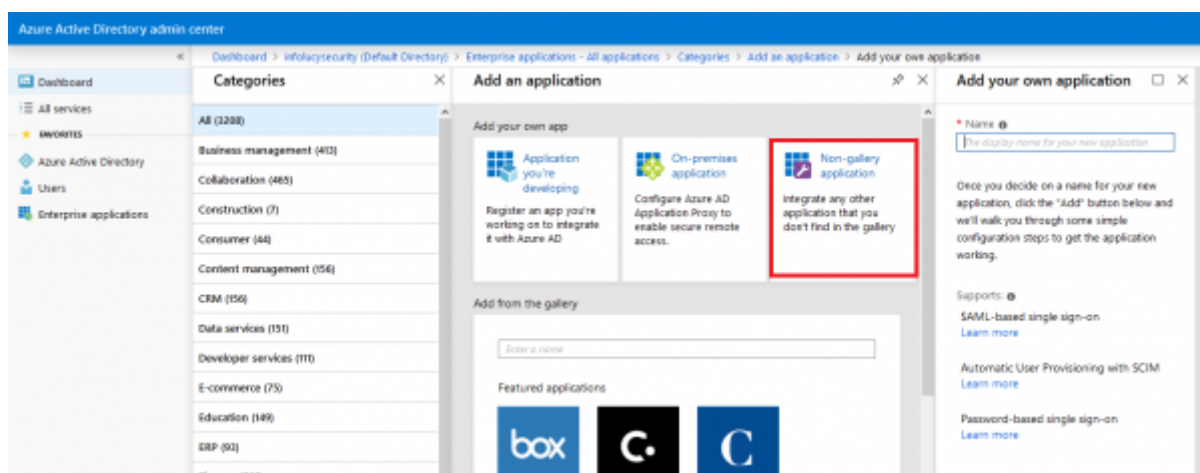
Enable Single sign-on in Lucy

- Configure SAML-based single sign-on to your non-gallery application

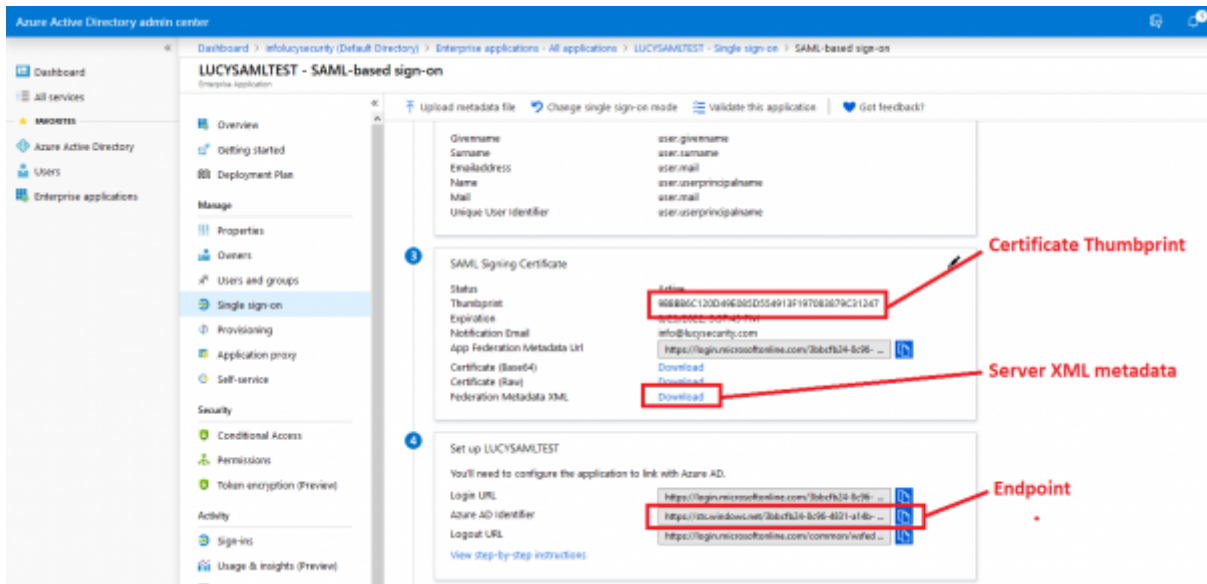
Find more about Azure AD Single Sign-on configuration [here](#)



- Add a new non-gallery web app to your Azure AD, see more [here](#)



- Open Lucy Admin console
- Navigate to the **SSO Configuration** page (Settings > SSO Settings)
- Tick the option "**Enable Active Directory FS**"
- Download the [FederationMetadata.xml](#) file from Azure AD and fill the [Identity Provider Endpoint](#) and [Certificate Thumbprint](#) in Lucy



Home / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Domain name

example.domain.com

Identity Provider Endpoint

https://sts.windows.net/3bbcfb24-8c96-4831-~;

Identity Provider Server XML metadata

Browse...

LUCYSAMLTEST.xml

Identity Provider Certificate Thumbprint

7CC57CD3D58207F18622B3665BEF06EA1C

Auto Login

☐

Save

- Download a pre-configured SAML metadata file (copy the URL and paste into your web browser address bar, change the extension of the file to .XML, for example "lucy-sp.xml")

[Home](#) / [SSO Configuration](#)

SSO Configuration

☒ Enable Active Directory FS

Domain name

Identity Provider Endpoint

Identity Provider Server XML metadata

No file selected.

Identity Provider Certificate Thumbprint

Metadata Endpoint

https://domain.com/service-provider/endpoint/metadata/lucy-sp

Provider Endpoint

https://domain.com/service-provider/endpoint/lucy-sp

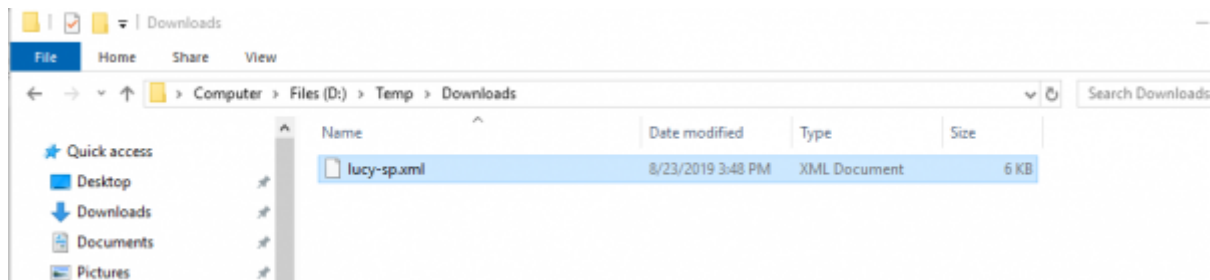
Provider Certificate

[Download Certificate](#)

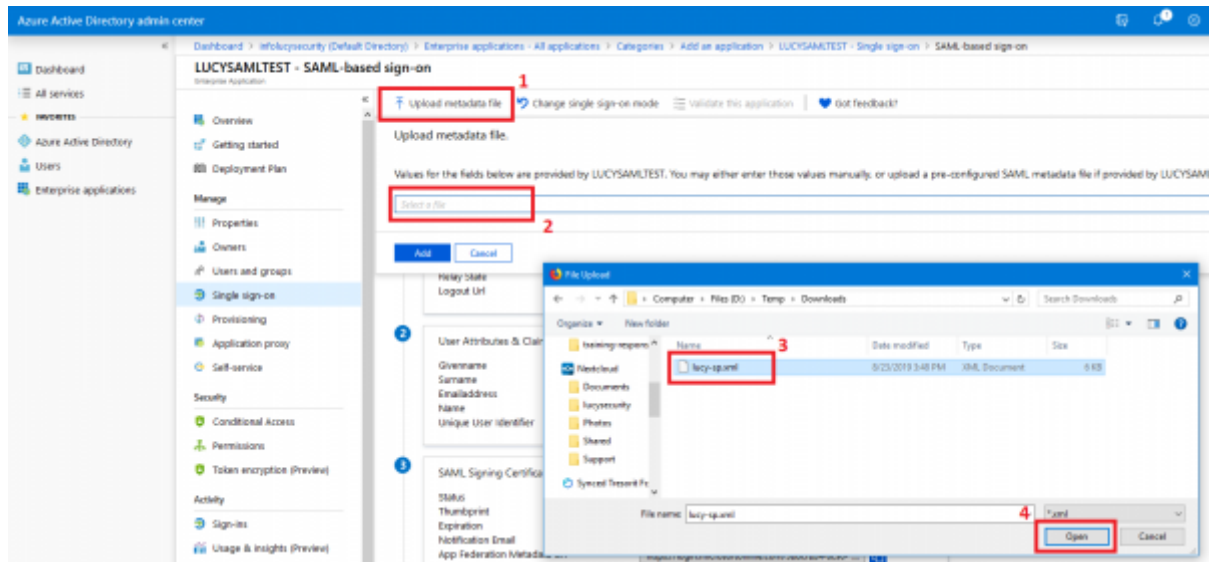
Auto Login

☐

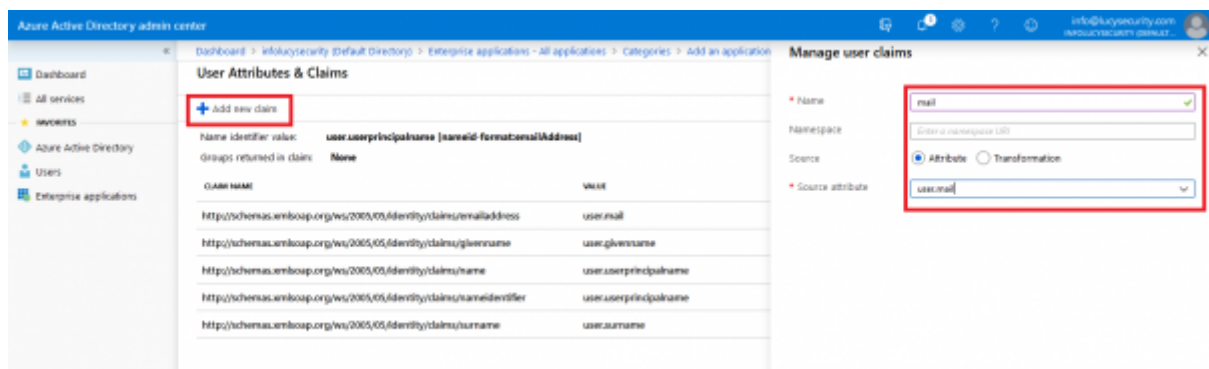
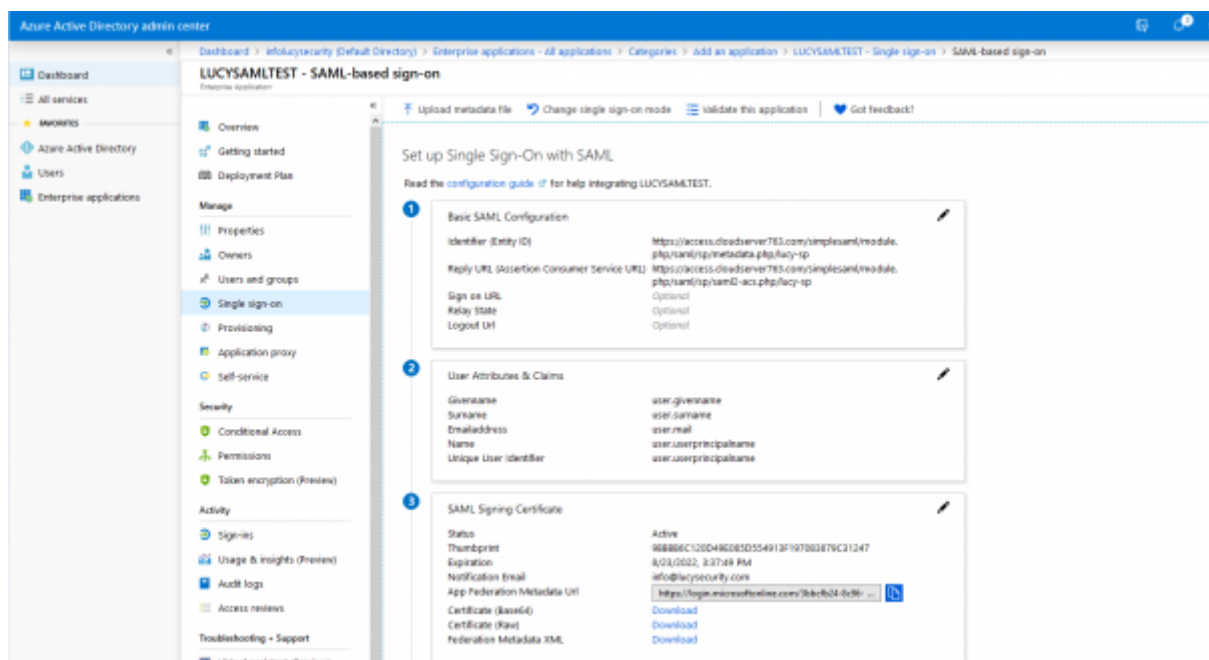
Save




- Upload the pre-configured SAML metadata file



- Add a new Claim "mail" that contain an e-mail address of the user, see more [here](#)



Note  The attribute user.mail is always empty if the user does not exist in your Office 365 Exchange server. Instead you will have to use the attribute user.userprincipalname or other one that contains user's email address.

- Configure Azure AD SAML token encryption, see more [here](#)

Home / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Domain name

Identity Provider Endpoint

Identity Provider Server XML metadata

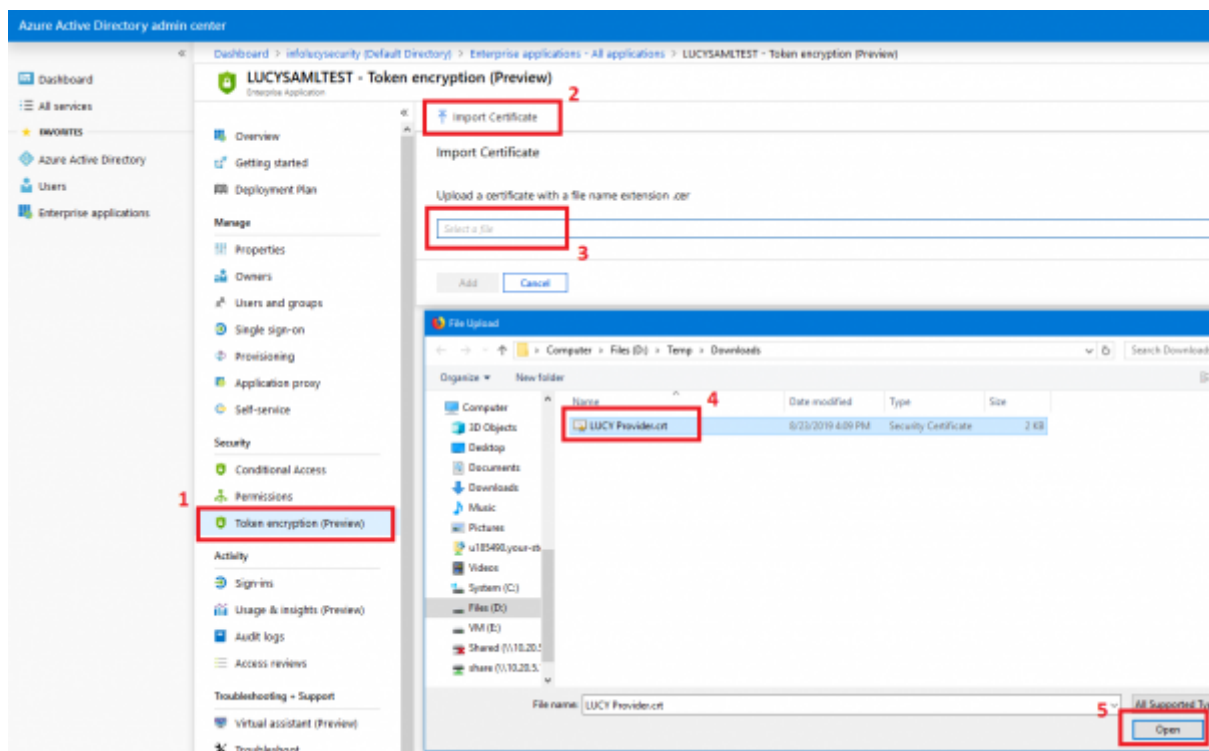
Identity Provider Certificate Thumbprint

Metadata Endpoint

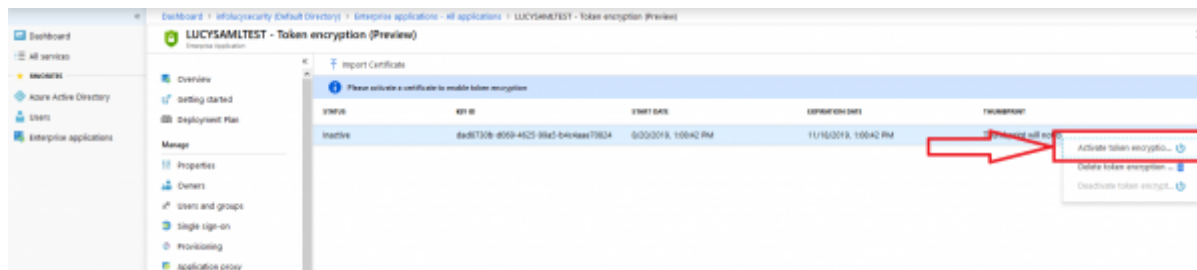
Provider Endpoint

Provider Certificate

Auto Login ☐

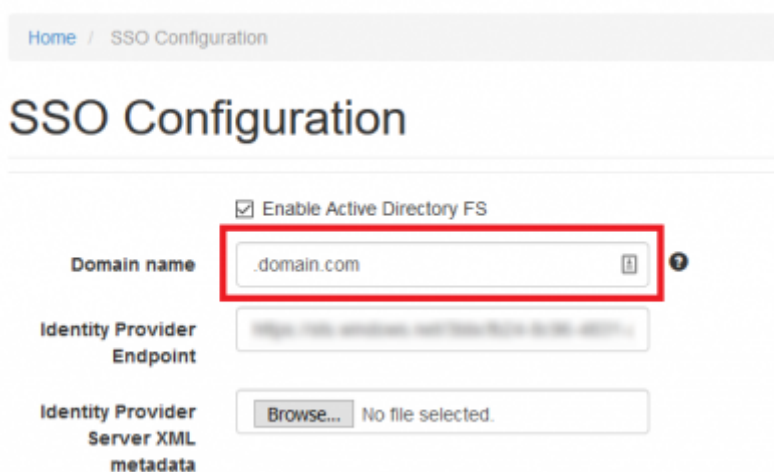


Do not forget to activate the encryption for the uploaded certificate



- (optional) You may also configure a domain name that Azure AD will use to receive authentication requests. Azure supports both single domain and range of subdomains, however, for this you need to use a wildcard SSL certificate. By default, Lucy is configured to use system domain.

To enable support for the subdomains, set the value in the Domain field in the following way ".domain.com"



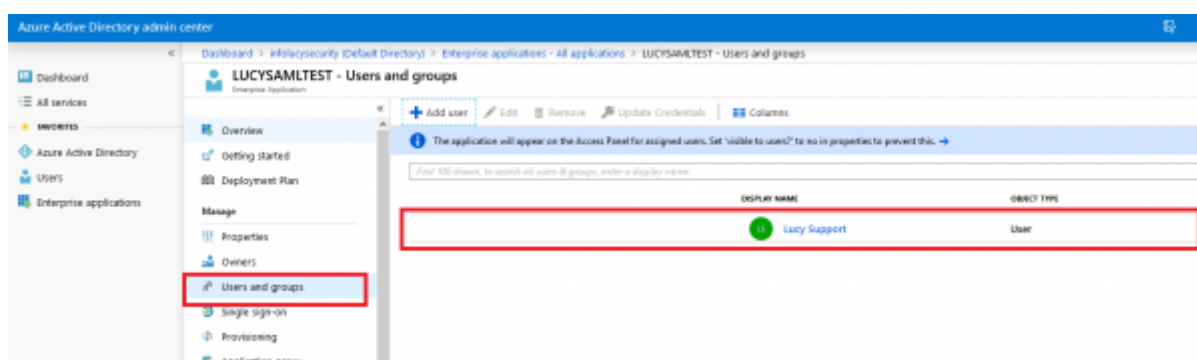
Using wildcard domain name will allow you to use different subdomains in your campaigns.



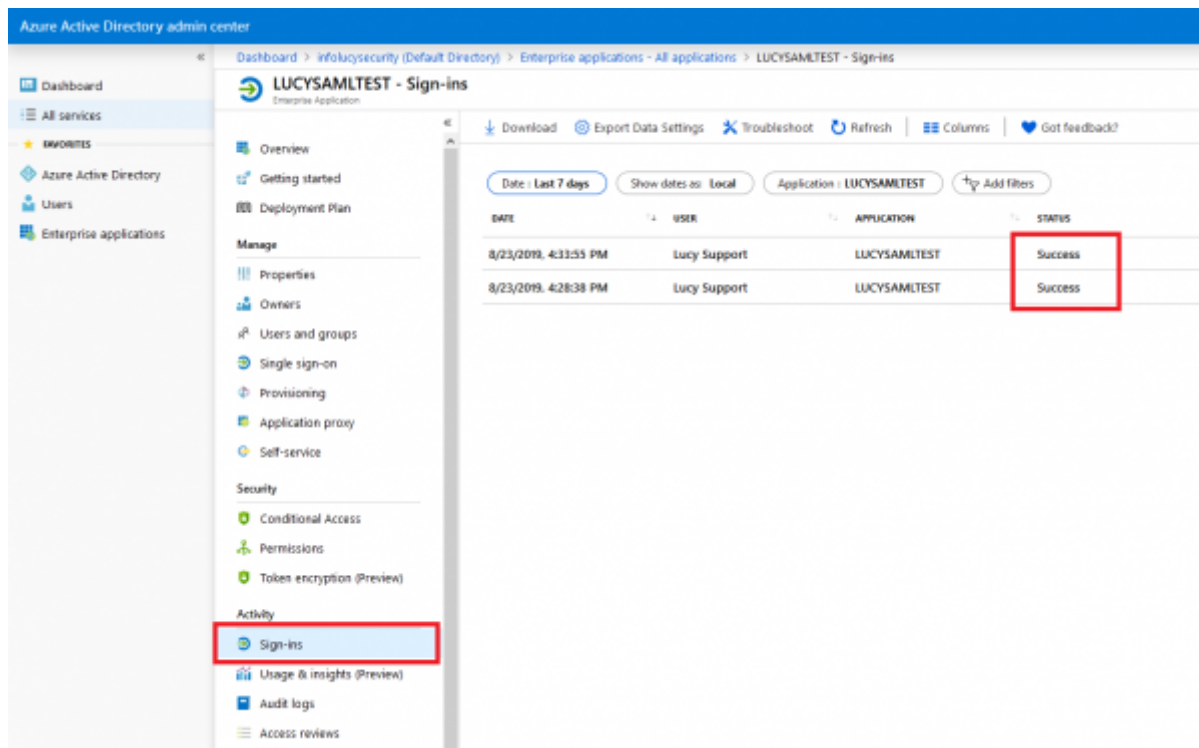
Please note, Azure AD does not support multiple second-level domains in a single application.

Testing Authentication

- Make sure you have added users to your app



- Navigate to the **SSO Configuration** page in Lucy Admin console and click the button **Test**



Troubleshoot problems

- I am redirected back to Lucy's login page after successful authorization through the Single sign-on.

If you are getting back to the login page, try checking the Claim rules (see the section [Enable Single sign-on in Lucy](#), "Add a new Claim 'mail'..."). There must be a claim named "mail", with empty "Namespace" and Source attribute that contains user email address. For example:

Manage claim

Save Discard changes

* Name mail ✓

Namespace Enter a namespace URI

* Source ☒ Attribute ☐ Transformation

* Source attribute user.userprincipalname

Claim conditions

From:
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=sso_azure&rev=1573720726

Last update: 2019/11/14 09:38



