



SSO using Azure AD Essentials

Instructions for setting up single sign-on using Azure Active Directory

February 2025, Questback

Contents

Introduction	3
Configuration.....	3
Finalizing the configuration	8

Introduction

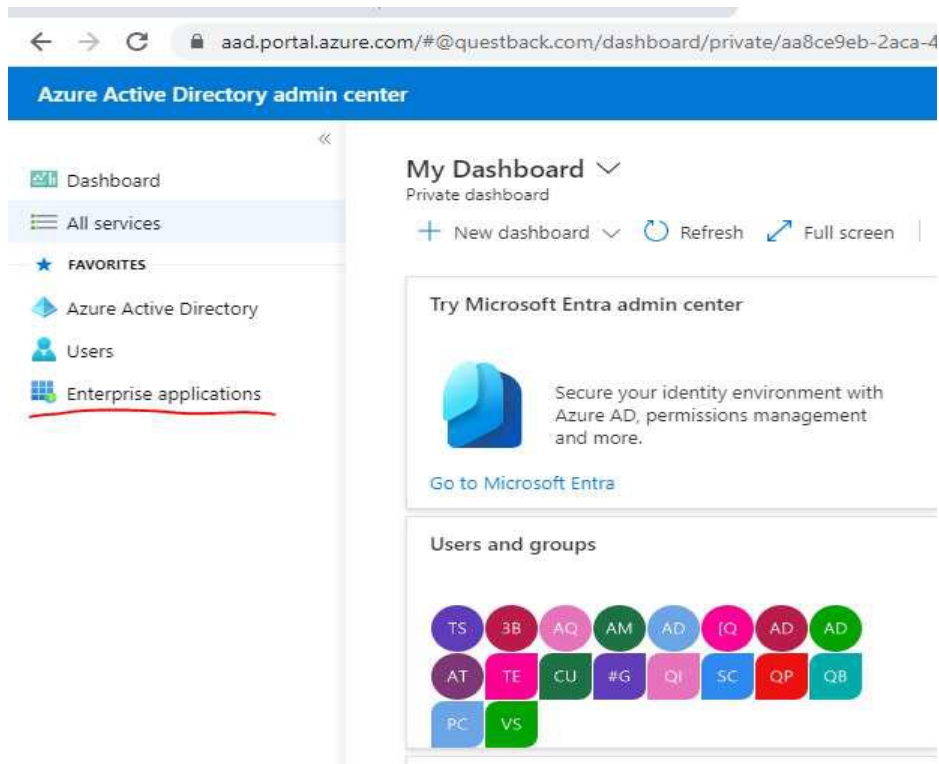
This document describes the process of setting up single sign-on (SSO) for Essentials using Azure Active Directory. To use SSO on your Essentials account must be SSO enabled. To do that you can contact support@questback.com.

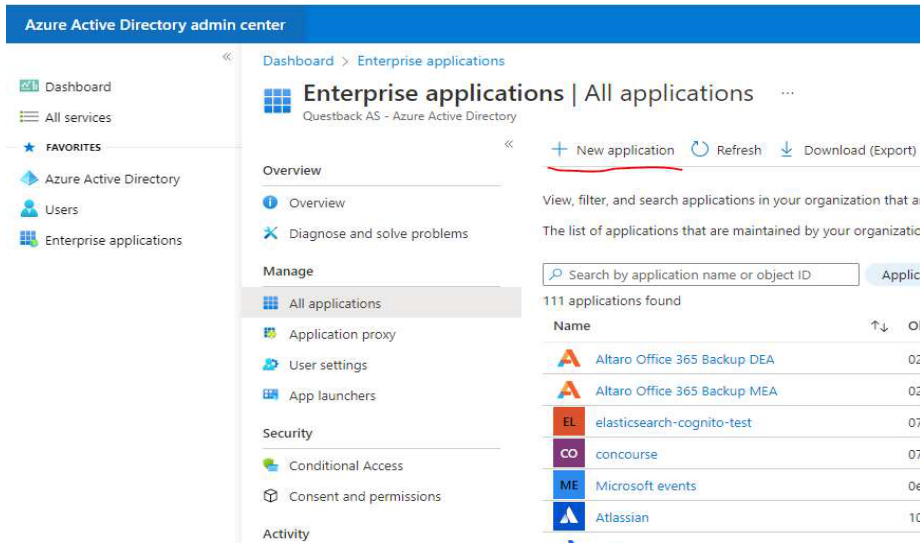
To simplify implementation, we recommend that all users on the Essentials account use their organizational email address as username.

Configuration

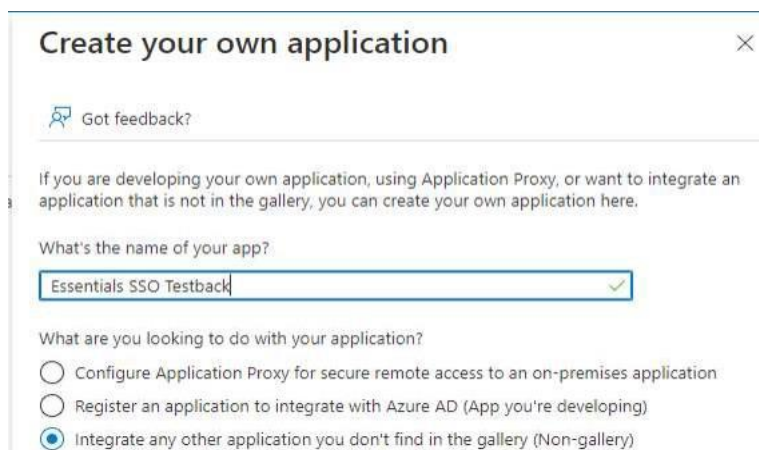
To configure SAML-based single sign-on (SSO) for Essentials in Azure Active Directory (Azure AD), you'll need to perform the following steps:

1. In the Azure AD portal, go to the "Enterprise Applications" page and select "New application" to add a new application to your Azure AD tenant.

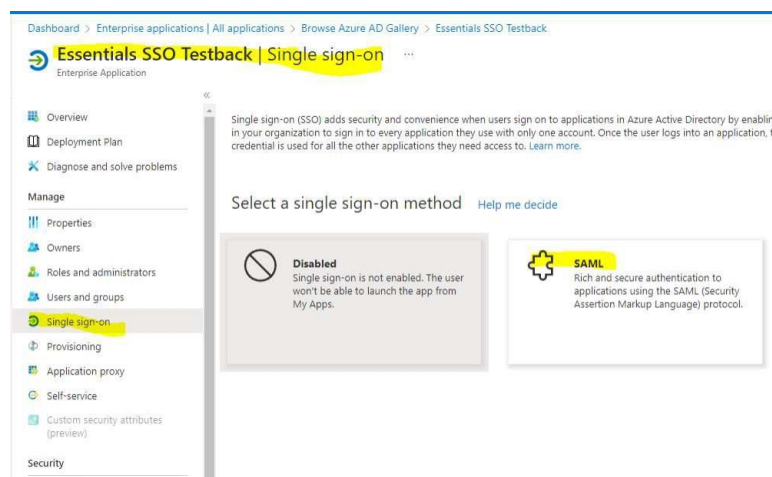




2. Select "Create your own application" and give your application a name. (For e.g. Essentials SSO)



3. After the application has been created, select "Single sign-on" from the left-hand menu and then SAML.



4. On the "Set up single sign-on with SAML" page, select the "Edit" button next to the "Basic SAML Configuration" section.

In the "Basic SAML Configuration" dialog, you'll need to enter the following information: a) Identifier (Entity ID): This is a unique identifier for your application.

<http://web2.questback.com>



b) Reply URL (Assertion Consumer Service URL): This is the URL to which Azure AD will send the SAML assertion.

<https://web2.questback.com/sso/consumerresponse>

c) Logout Url: (This URL is used to send the SAML logout response back to the application.)

<https://web2.questback.com/sso/singlelogout>


Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default


ⓘ 

Add identifier

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 "Assertion Consumer Service" (ACS) in SAML.


Index Default

ⓘ 

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 URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.




Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.



5. SAML certificate should be preconfigured with the creation of the application. But, if you want to use another certificate you'll need to select the "Edit" and then "Import Certificate" button and select the certificate file that you want to use for signing.

All certificates **must** be issued by a trusted Certificate Authority (CA). Ensure that the CA is recognized and compliant with industry standards to maintain secure communication.

The screenshot shows the 'SAML-based Sign-on' configuration page in Azure AD. The 'SAML Certificates' section is highlighted with a red circle. The 'Token signing certificate' is active and shows the following details:

Property	Value
Status	Active
Thumbprint	0451795201C08680E004C9367A5477D41F0C183C
Expiration	12/20/2025, 10:14:48 AM
Notification Email	Adnan.Spahic@questback.com
App Federation Metadata Url	https://login.microsoftonline.com/dc79dd1a-883e...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

The 'SAML Signing Certificate' dialog box is also visible, showing the same certificate details and options to 'Import Certificate' or 'Got feedback?'.

6. After you've configured the basic SAML settings, you'll need to configure the attribute mapping. This involves specifying which attributes in Azure AD should be included in the SAML assertion that is sent to your application. To do this, select the "Edit" button next to the "Attributes & Claims" section and then click on the existing claim name:

The screenshot shows the 'Attributes & Claims' configuration page. The 'Required claim' section contains one claim:

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	Multiple conditions [nam... ***

The 'Additional claims' section is currently empty, showing 'No claims configured'.

Fill out fields as shown on image below:

Dashboard > Enterprise applications | All applications > Browse Azure AD Gallery > Essentials SSO Testback | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim

Save Discard changes Got feedback?

Name: nameidentifier

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Email address

Source: Attribute

Source attribute: Select from drop down or type a constant

Claim conditions: Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. [Read the documentation](#) for more information.

User type	Scoped Groups	Source	Value
Members	1 groups	Attribute	user.mail
Select from drop down	Select groups	Attribute Transformation	

Advanced SAML claims options

Remember to assign group to the claim conditions. In this example we select all users group.

7. Finally, you'll need to assign users or groups to the application. To do this, select the "Users and groups" menu item from the left-hand menu and then select the "Add user/group" button to add users or groups to the application.

Azure Active Directory admin center

Dashboard > Essentials SSO Testback | Users a

Add Assignment

Questback AS

Users and groups

None Selected

Select a role

User

Assign

Users and groups

all

- AU All Users
- AL AllFin_security_group
- AllFin_security_group@questback365.onmicrosoft.com

Selected items

No items selected

Select

Finalizing the configuration

Now your account needs to be configured in Essentials. Please send the metadata url of your installation to support@questback.com.

Your metadata typically looks like this:

<https://login.microsoftonline.com/dc79da1b-883e-128c-b396-dc9fb7f66bf1/federationmetadata/2007-06/federationmetadata.xml?appid=377d5d6e-3504-4f1a-a6e5-f5aac01e26f5>

Once that has been added to your Essentials account, the SSO configuration is completed and you should be able to test SSO from your Azure AD by clicking on button Test->Test sign in.

The screenshot shows the Questback web application interface. At the top, there is a navigation bar with the following statistics: Aktive Quester: 0, Avsluttede Quester: 1, Invitasjoner: 19, Svar: 1, and Svarprosent: 5%. Below this, the user is greeted with "Velkommen Adnan Spahic".

The main content area features a "Min historikk" (My history) table with the following data:

Min historikk	Sist åpnet	Svar	Svarprosent
Delete sub-Q	17.11.2022	100	0%
Test quest - Validaton message(1)	17.11.2022	0	0%
Test new servers	21.09.2022	54	0%
Asset overview	18.05.2022	1	0%
Anonymous test	20.03.2022	1	0%

To the right of the table is a "Professional services fra Questback" section with a "Kontakt oss" button. Below the table is a "LAG QUEST" button and a "TILBAKESTILL LAYOUT" link.

The dashboard is organized into several panels:

- AKTIVE QUESTER:** Du har ingen aktive Quester ennå.
- PLANLAGTE QUESTER:** Du har ingen planlagte Quester ennå.
- MIN HISTORIKK:** A list of questions with their last access dates:
 - Delete sub-Q (17.11.2022)
 - Test quest - Validaton message(1) (17.11.2022)
 - Test new servers (21.09.2022)
 - Asset overview (18.05.2022)
 - Anonymous test (20.03.2022)
- SVAR (3):** A panel for answers, currently empty.

You should now have SAML-based SSO configured for Essentials application in Azure AD.

Copyright © 2025 Questback AS. All Rights Reserved.