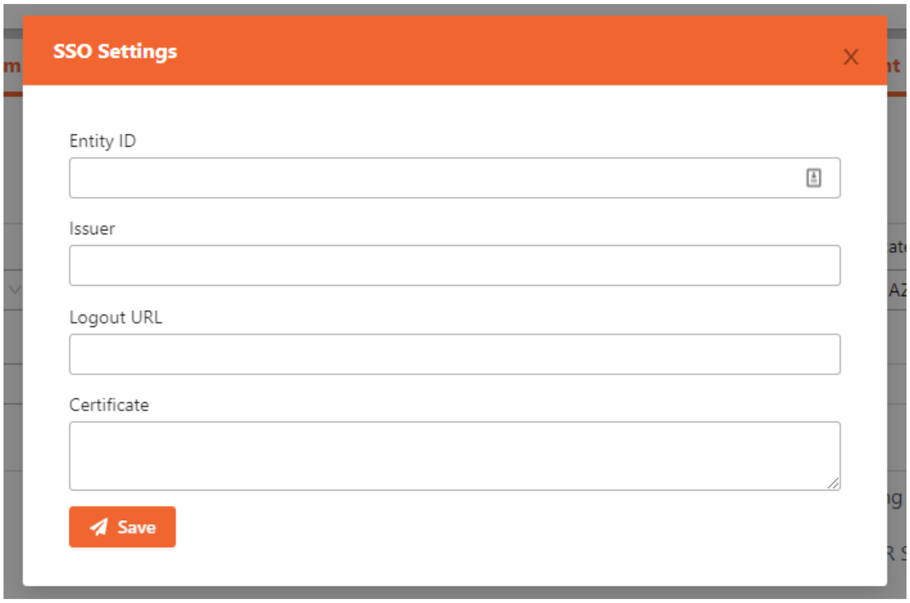
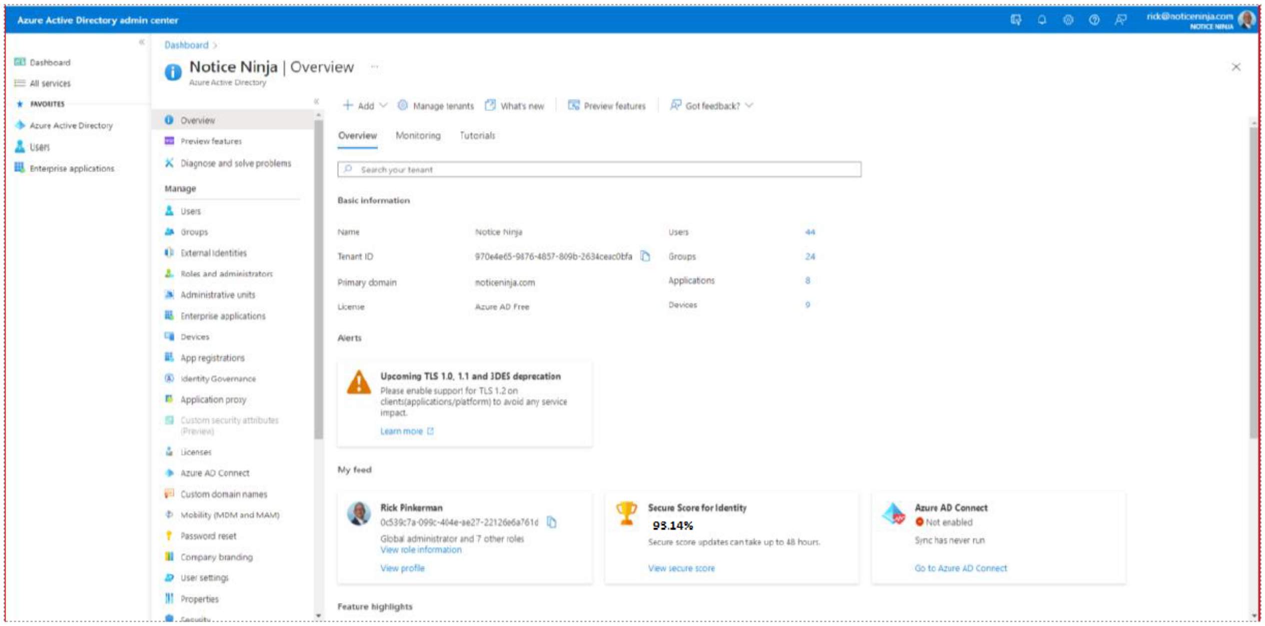
NOTICENINJA - SSO / AD / LDAP Setup:

SSO is one of the services offered to enable user to login based on their network AD account access rights. To enable SSO in NOTICENINJA you need to setup the NOTICENINJA application in your Active Directory and then add those (LDAP) settings into NOTICENINJA. This will allow IT to control what users have access to the system. Follow the below directions to setup NOTICENINJA inside your AD account.

STEP 1: SETUP NOTICENINJA IN ACTIVE DIRECTORY:

1. Add NOTICENINJA application into your Active Directory account (Create SAML Toolkit).
2. Create an AD Group for NOTCENINJA Users. The Group will be used to hold all the NOTICENINJA users.
3. Not all networks are setup the same and depending on the version of Active Directory, your settings could be a little different.
4. In the below screen are the items you will need from the AD setup to load into NOTICENINJA:





Notice Ninja | Overview

Azure Active Directory

Basic information

Name	Notice Ninja	Users	44
Tenant ID	970e4e65-9876-4857-809b-2634ceac0bfa	Groups	24
Primary domain	noticeninja.com	Applications	8
License	Azure AD Free	Devices	9

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
Learn more

My feed

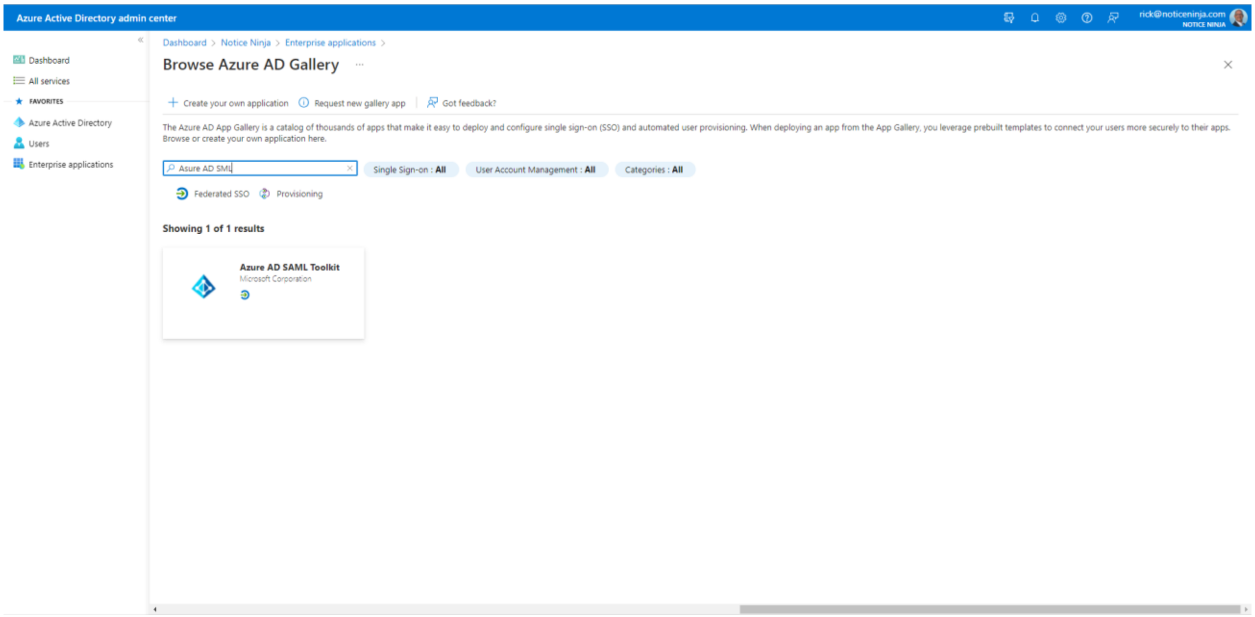
Rick Pinkerman
0c539c7a-099c-404e-ae27-22126e6a761d
Global administrator and 7 other roles
View role information
View profile

Secure Score for Identity
93.14%
Secure score updates can take up to 48 hours.
View secure score

Azure AD Connect
Not enabled
Sync has never run
Go to Azure AD Connect

Feature highlights

Load the AD SAML Toolkit in for NOTICENINJA.



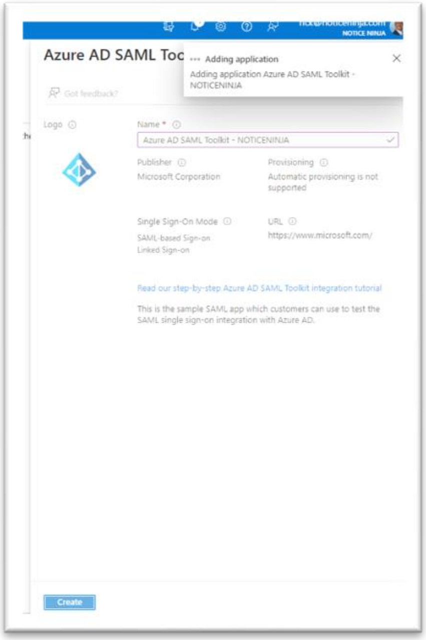
Browse Azure AD Gallery

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here.

Asure AD SML

Showing 1 of 1 results

Azure AD SAML Toolkit
Microsoft Corporation



Azure AD SAML Toc

••• Adding application

Adding application Azure AD SAML Toolkit - NOTICENINJA

Got feedback?

Logo

Name *

Azure AD SAML Toolkit - NOTICENINJA

Publisher: Microsoft Corporation

Provisioning: Automatic provisioning is not supported

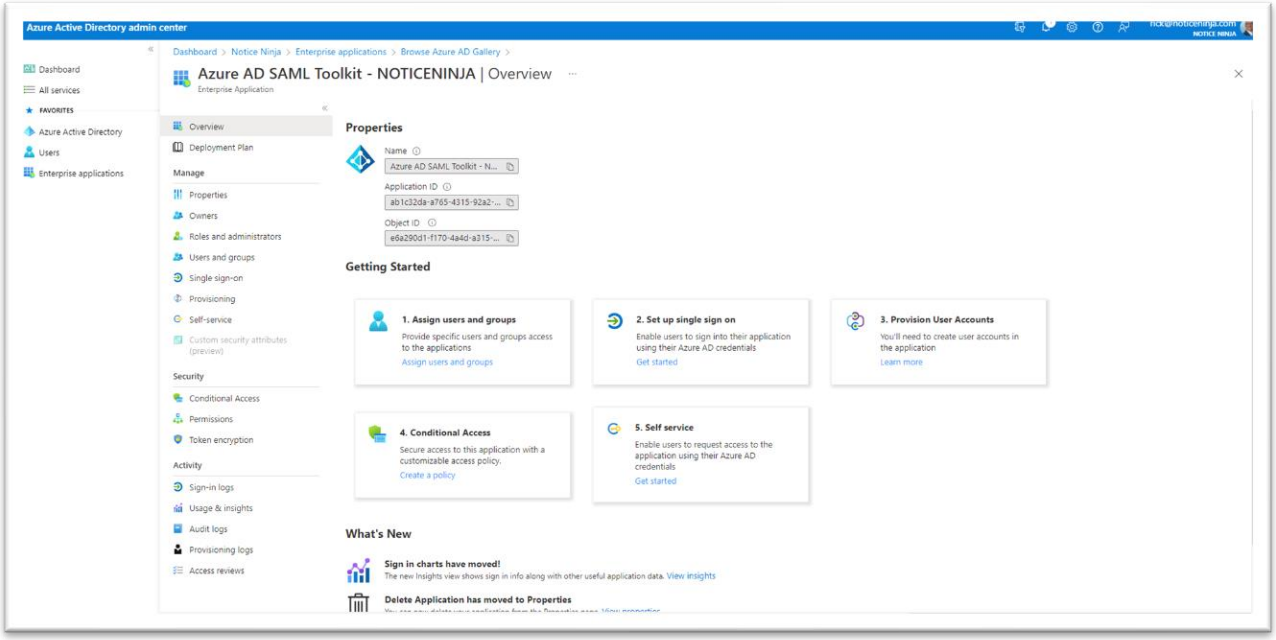
Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: https://www.microsoft.com/

Read our step-by-step Azure AD SAML Toolkit integration tutorial

This is the sample SAML app which customers can use to test the SAML single sign-on integration with Azure AD.

Verify information (Need to use Object ID – Entity ID in NOTICENINJA)



Azure Active Directory admin center

Dashboard > Notice Ninja > Enterprise applications > Browse Azure AD Gallery >

Azure AD SAML Toolkit - NOTICENINJA | Overview

Enterprise Application

Properties

Name: Azure AD SAML Toolkit - N...

Application ID: ab1c32da-a765-4315-92a2-...

Object ID: e6a290d1-f170-4a4d-a315-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
You'll need to create user accounts in the application
Learn more

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

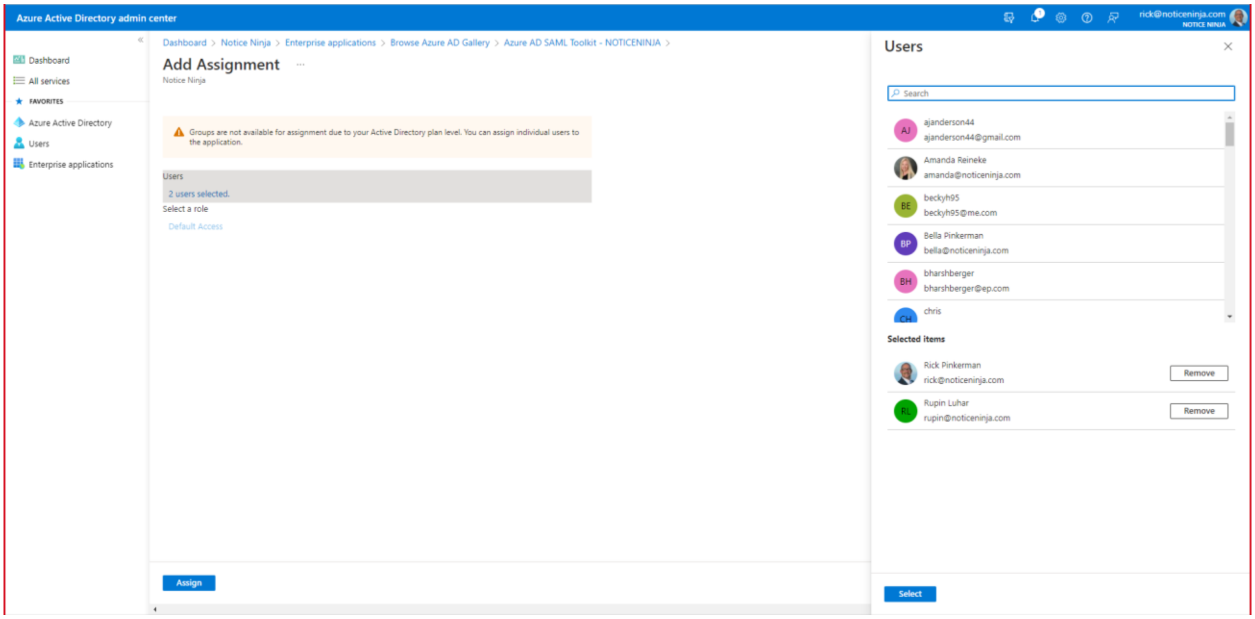
5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties

Add in the Group that will be used to store the users.



Add Assignment

Notice Ninja

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

2 users selected.

Select a role

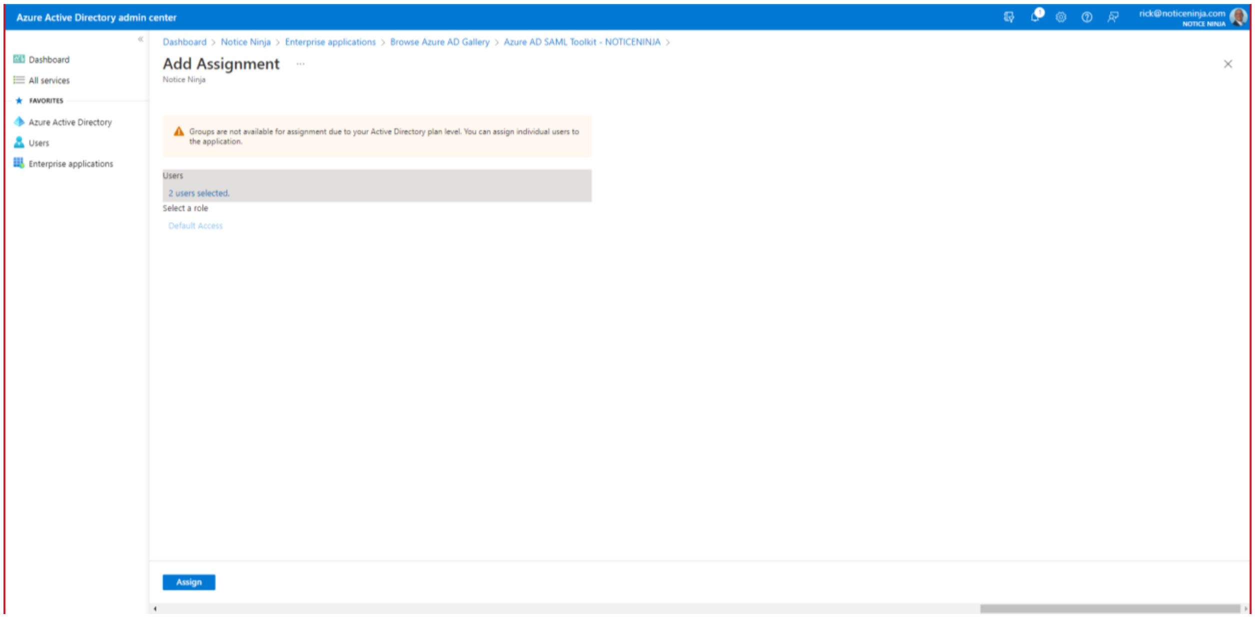
Default Access

AJ	ajanderson44 ajanderson44@gmail.com
	Amanda Reineke amanda@noticeninja.com
BE	beckyh95 beckyh95@me.com
BP	Bella Pinkerman bella@noticeninja.com
BH	bharshberger bharshberger@ep.com
CH	chris

Selected items

	Rick Pinkerman rick@noticeninja.com
RL	Rupin Luhar rupin@noticeninja.com

Add the users that will have access to NOTICENINJA.


Azure Active Directory admin center
rick@noticeninja.com
NOTICE NINJA
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Notice Ninja > Enterprise applications > Browse Azure AD Gallery > Azure AD SAML Toolkit - NOTICENINJA >
Assign

Add Assignment

Notice Ninja

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

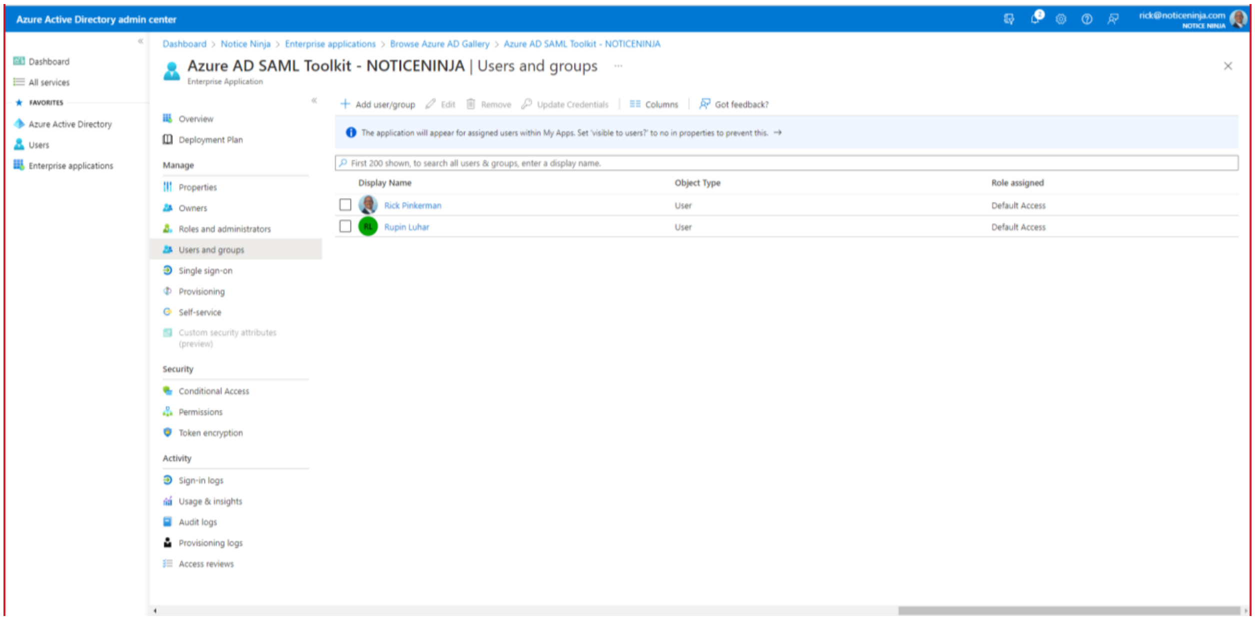
Users

2 users selected.

Select a role

Default Access

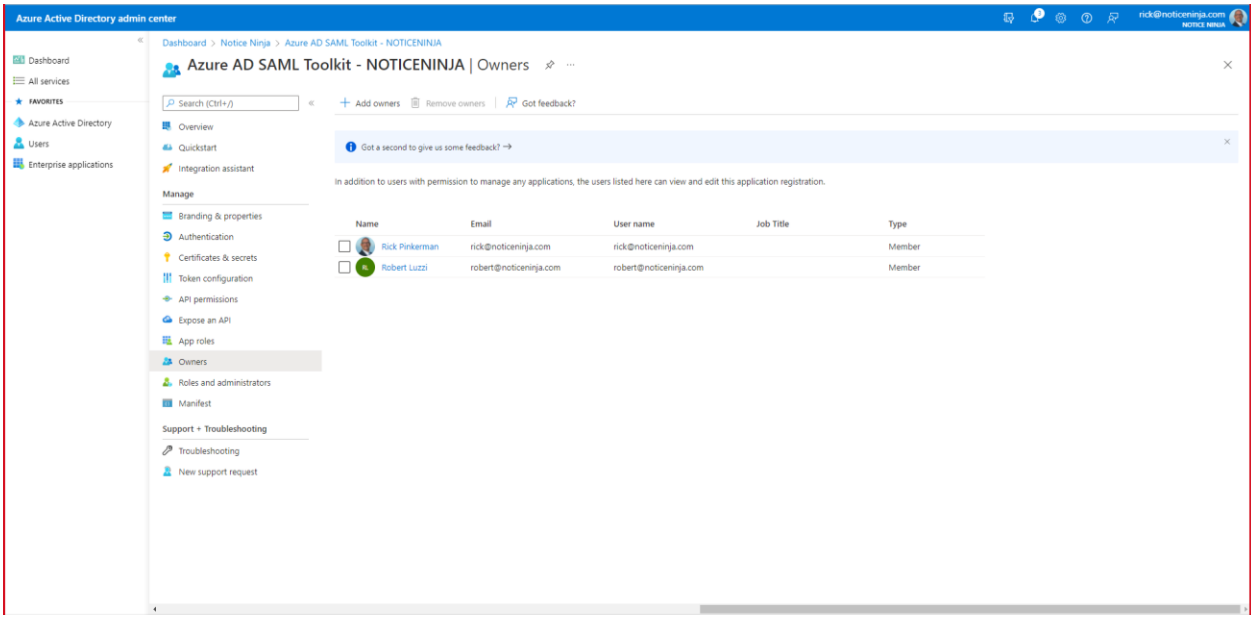
Verify users are added.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

	Display Name	Object Type	Role assigned
□	Rick Pinkerman	User	Default Access
□	Rupin Luhar	User	Default Access

Add the Owners of the Toolkit.

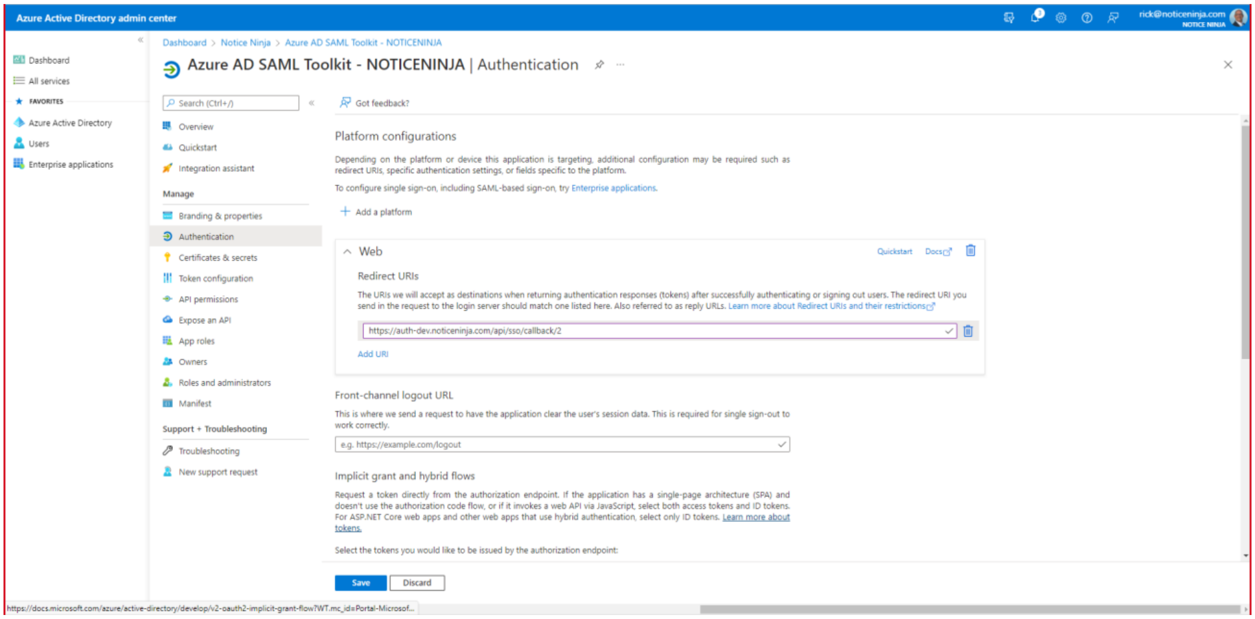


Got a second to give us some feedback? →

In addition to users with permission to manage any applications, the users listed here can view and edit this application registration.

	Name	Email	User name	Job Title	Type
□	Rick Pinkerman	rick@noticeninja.com	rick@noticeninja.com		Member
□	Robert Luzzi	robert@noticeninja.com	robert@noticeninja.com		Member

Get the Authentication (Redirect URL’s) Login / Logout.



Azure AD SAML Toolkit - NOTICENINJA | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

To configure single sign-on, including SAML-based sign-on, try Enterprise applications.

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://auth-dev.noticeninja.com/api/sso/callback/2

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

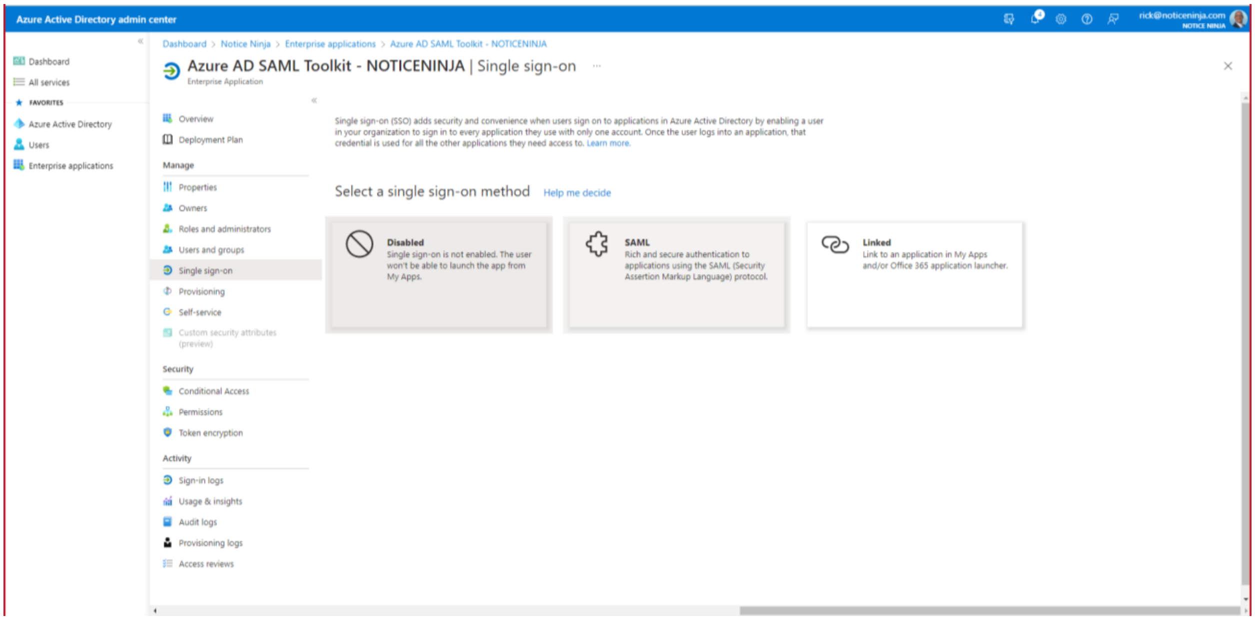
Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

https://docs.microsoft.com/azure/active-directory/develop/v2-oauth2-implicit-grant-flow?WT.mc_id=Portal-Microsof...

Add SSO to the Toolkit.



Azure AD SAML Toolkit - NOTICENINJA | Single sign-on

Enterprise Application

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

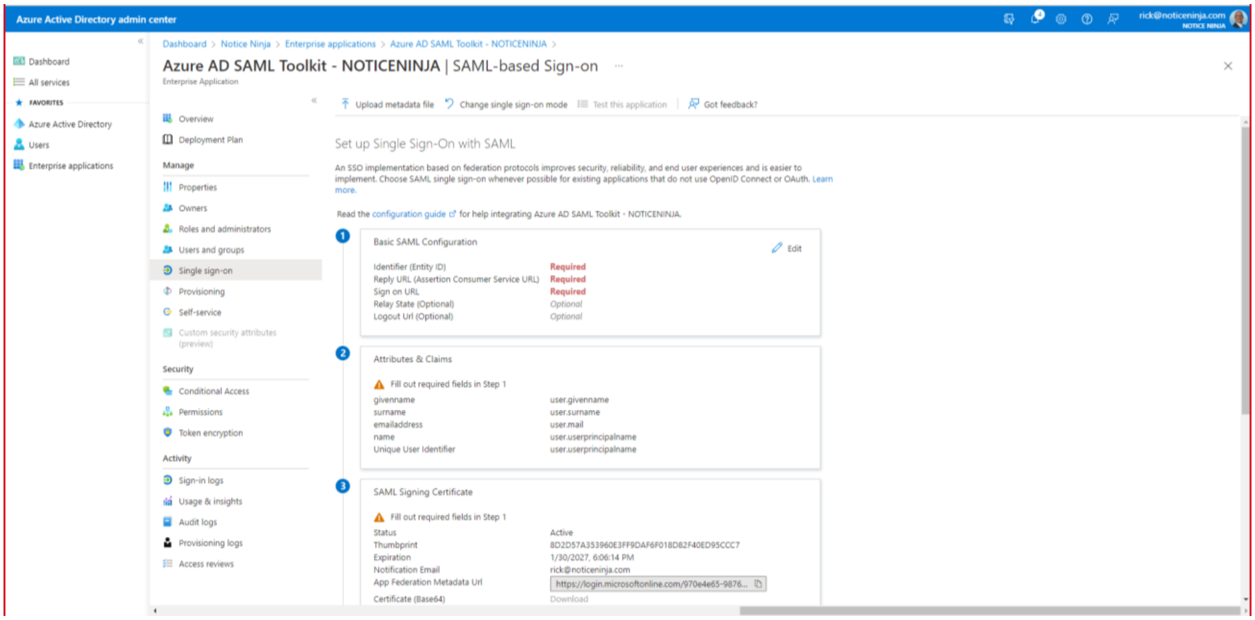
Select a single sign-on method

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Configure SSO



Azure AD SAML Toolkit - NOTICENINJA | SAML-based Sign-on

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Azure AD SAML Toolkit - NOTICENINJA.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

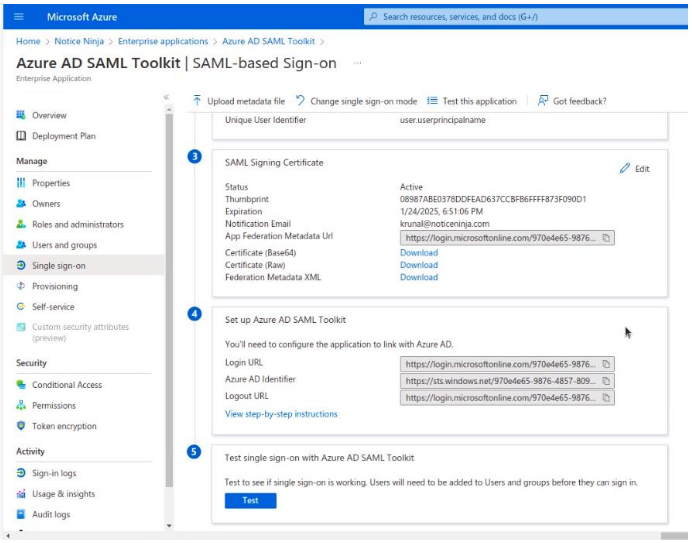
Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Fill out required fields in Step 1

Status	Active
Thumbprint	8D2D57A353960E3FF9DAF6F018D82F40ED95CCC7
Expiration	1/30/2027, 6:06:14 PM
Notification Email	rick@noticeninja.com
App Federation Metadata Url	https://login.microsoftonline.com/970e4e65-9876...
Certificate (Base64)	Download



Azure AD SAML Toolkit | SAML-based Sign-on

Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	08987ABE0378DDFEAD637CCBFB6FFFF873F090D1
Expiration	1/24/2025, 6:51:06 PM
Notification Email	krunal@noticeninja.com
App Federation Metadata Url	https://login.microsoftonline.com/970e4e65-9876...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Azure AD SAML Toolkit

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

Login URL	https://login.microsoftonline.com/970e4e65-9876...
Azure AD Identifier	https://sts.windows.net/970e4e65-9876-4857-809...
Logout URL	https://login.microsoftonline.com/970e4e65-9876...

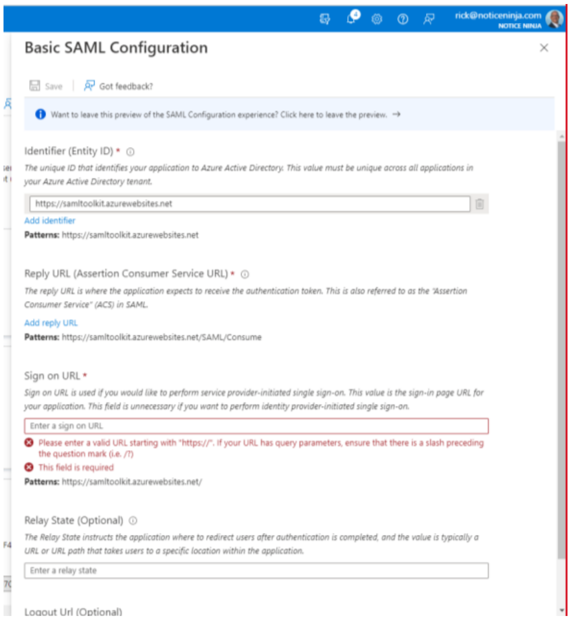
View step-by-step instructions

5 Test single sign-on with Azure AD SAML Toolkit

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

Configure the Sign on URL



Basic SAML Configuration

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

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.

https://samltoolkit.azurewebsites.net

Add identifier

Patterns: https://samltoolkit.azurewebsites.net

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.

Add reply URL

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

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.

Enter a sign on URL

Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?)

This field is required

Patterns: https://samltoolkit.azurewebsites.net/

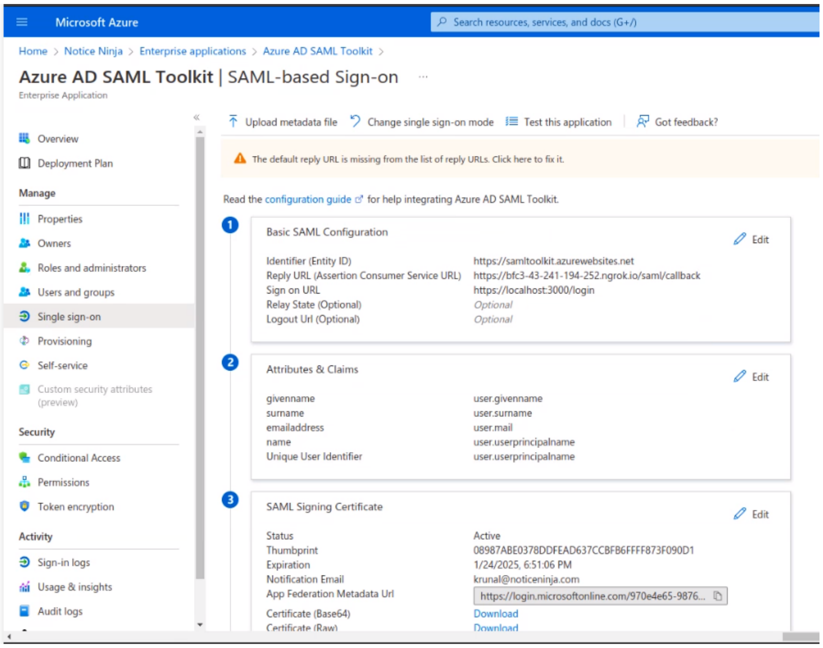
Relay State (Optional)

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.

Enter a relay state

Logout Url (Optional)

Verify changes



Azure AD SAML Toolkit | SAML-based Sign-on

Enterprise Application

The default reply URL is missing from the list of reply URLs. Click here to fix it.

Read the configuration guide for help integrating Azure AD SAML Toolkit.

1 Basic SAML Configuration

Identifier (Entity ID)	https://samltoolkit.azurewebsites.net
Reply URL (Assertion Consumer Service URL)	https://bfc3-43-241-194-252.ngrok.io/saml/callback
Sign on URL	https://localhost:3000/login
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

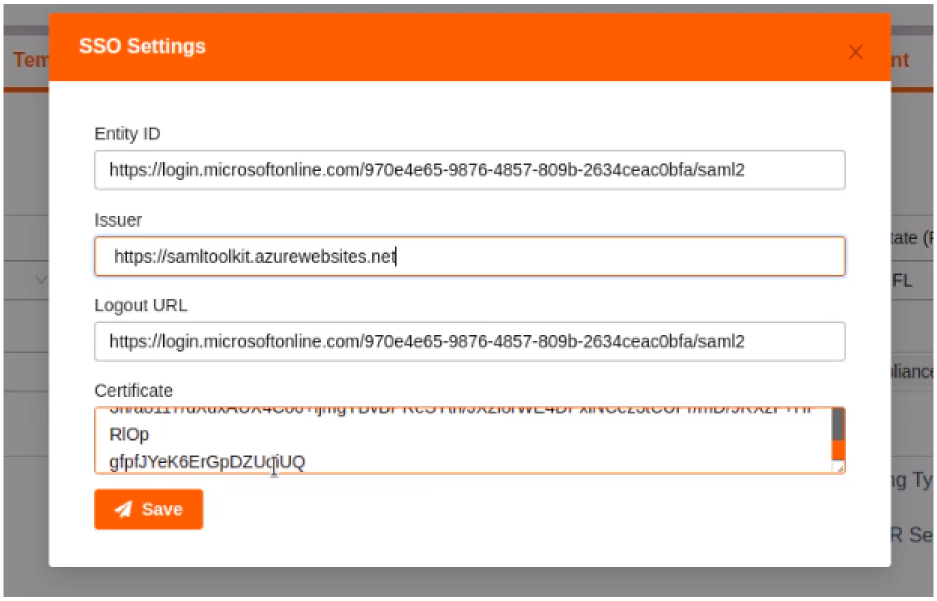
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	08987ABE0378DDFEAD637CCBFB6FFFF873F090D1
Expiration	1/24/2025, 6:51:06 PM
Notification Email	krunal@noticeninja.com
App Federation Metadata Url	https://login.microsoftonline.com/970e4e65-9876...
Certificate (Base64)	Download
Certificate (Raw)	Download

Use the setting from AD to fill out the NOTICENINJA SSO option.

The header names should match up to your AD descriptions. There could be some differences depending on the version of AD in use.



SSO Settings

Entity ID

https://login.microsoftonline.com/970e4e65-9876-4857-809b-2634ceac0bfa/saml2

Issuer

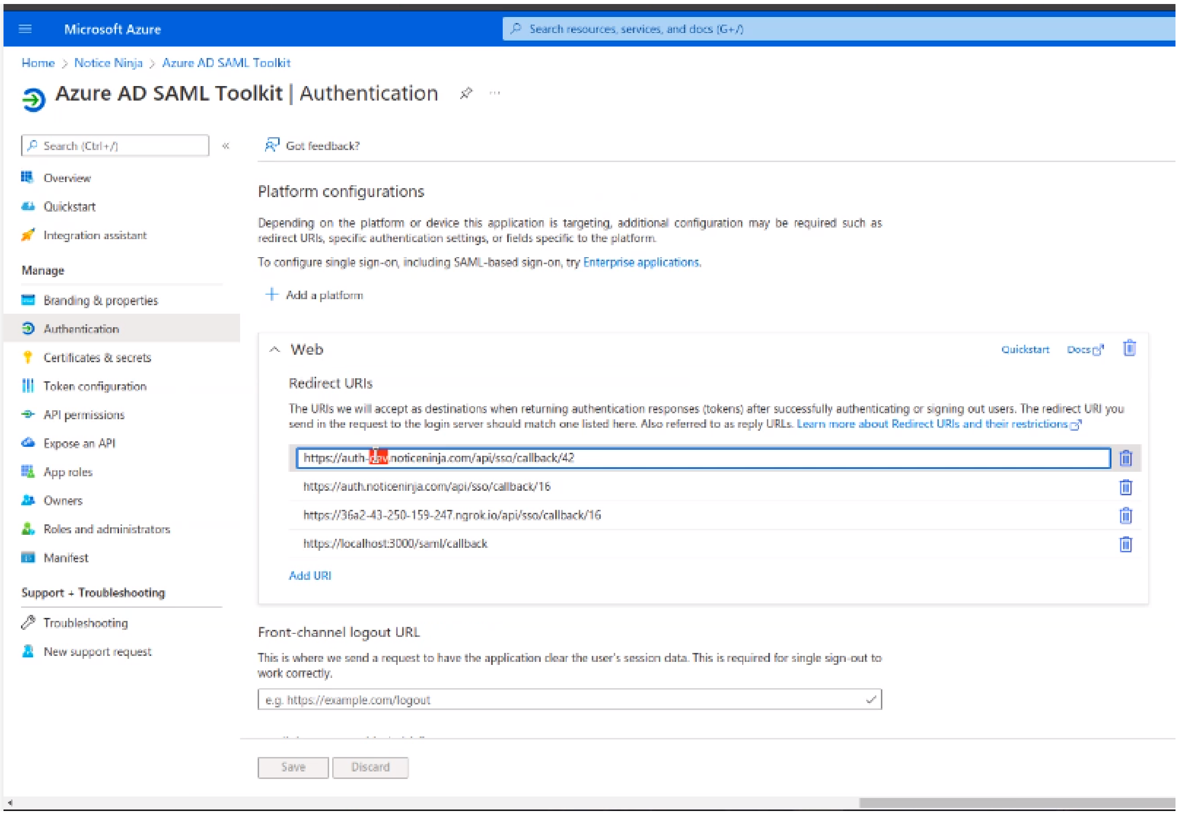
https://samltoolkit.azurewebsites.net

Logout URL

https://login.microsoftonline.com/970e4e65-9876-4857-809b-2634ceac0bfa/saml2

Certificate

RlOp
gfpfJYeK6ErGpDZUqiUQ



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

To configure single sign-on, including SAML-based sign-on, try Enterprise applications.

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://auth-dev.noticeninja.com/api/sso/callback/42

https://auth.noticeninja.com/api/sso/callback/16

https://36a2-43-250-159-247.ngrok.io/api/sso/callback/16

https://localhost:3000/saml/callback

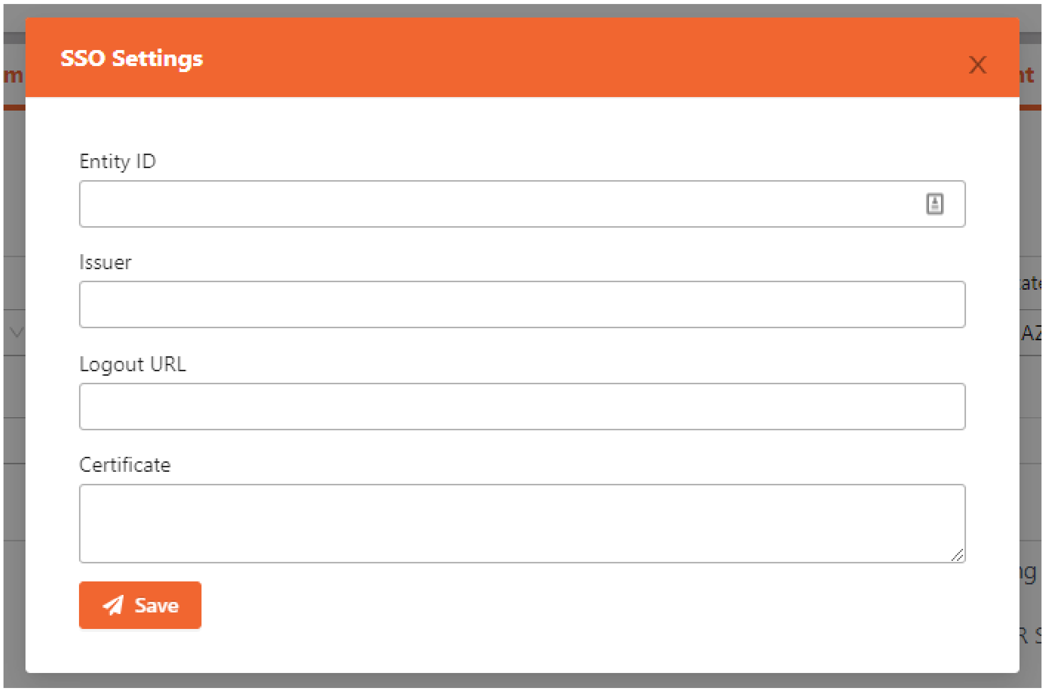
Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

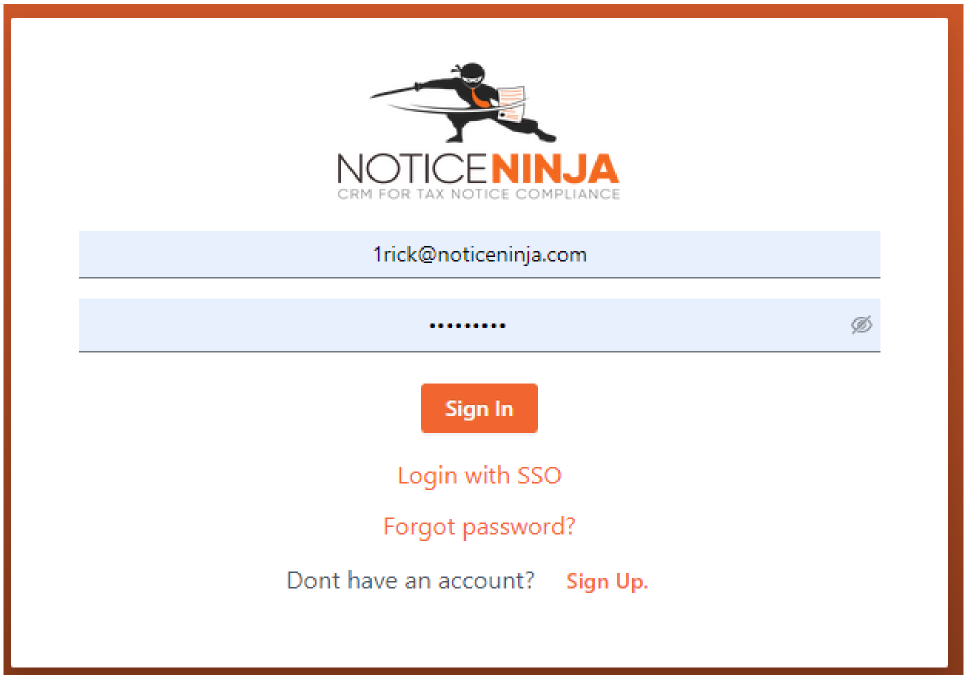
<u>STEP 2:</u> CONFIGURE NOTICENINJA SSO SETTINGS: Now that you have setup NOTICENINJA in AD you need to link NOTICENINJA to your AD settings. Once this is done users will be able to log in using SSO.

1. Open Settings > My Co Info tab > ENABLED FEATURES > SSO Settings.
2. Enter the details from your AD Setup.
3. Click Save.



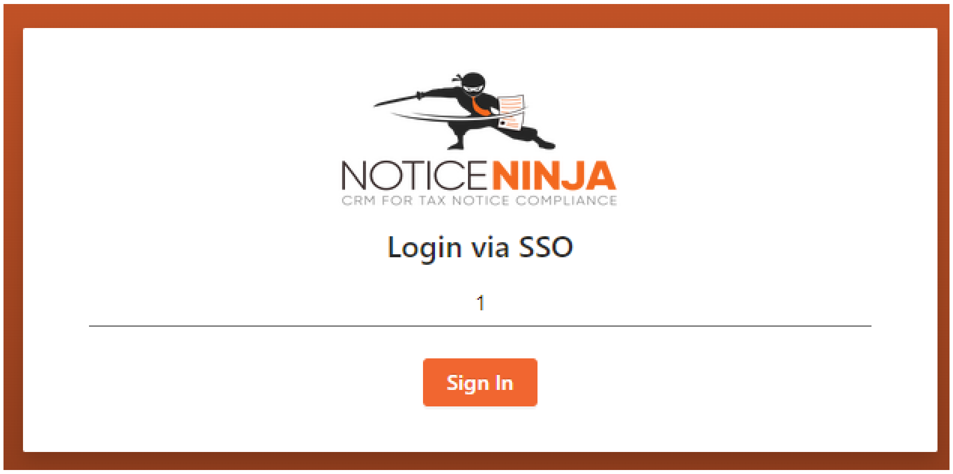
<u>STEP 3:</u> NEW USER LOGIN: Once SSO is setup new users will be added to log into the system as follows:

1. 1st time User Sign in.
2. Open the NOTICENINJA login screen.
3. Select the Login with SSO option.
4. Enter your account number (Shows on the main screen)
5. AD Security messages comes up. Enter user and password the 1st time.
6. User added to system with Security Role = User (with no options checked)
7. NOTICENINJA Admin to configure the UI security settings.



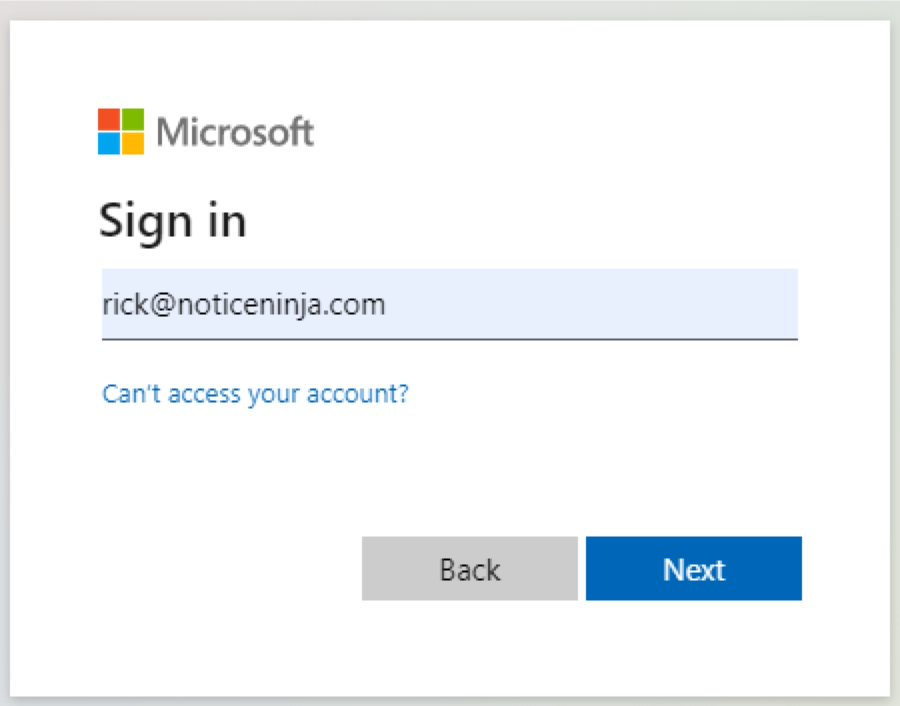
1rick@noticeninja.com

•••••••••



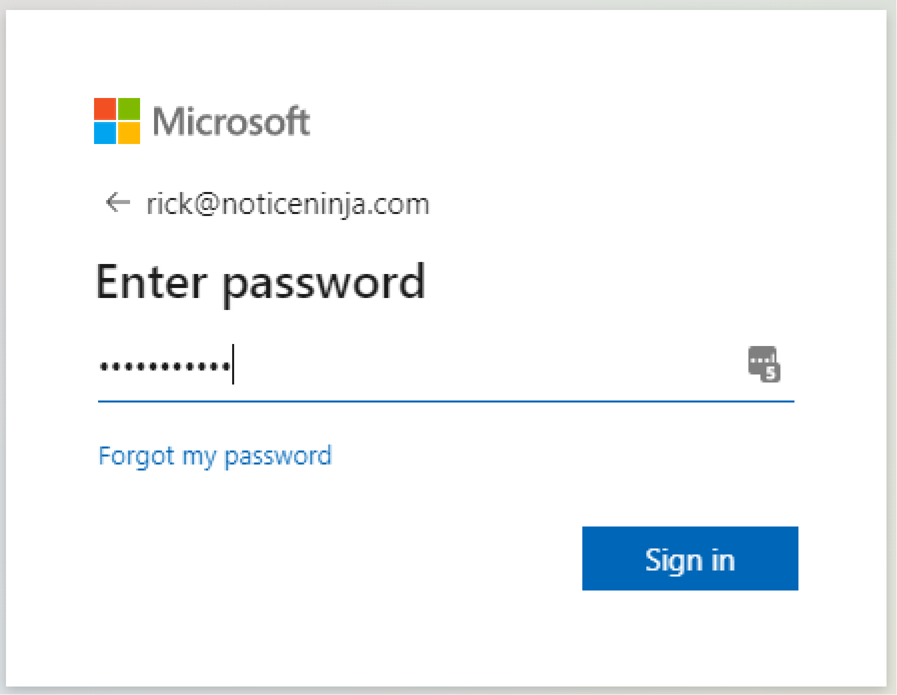
Login via SSO

1



Sign in

rick@noticeninja.com

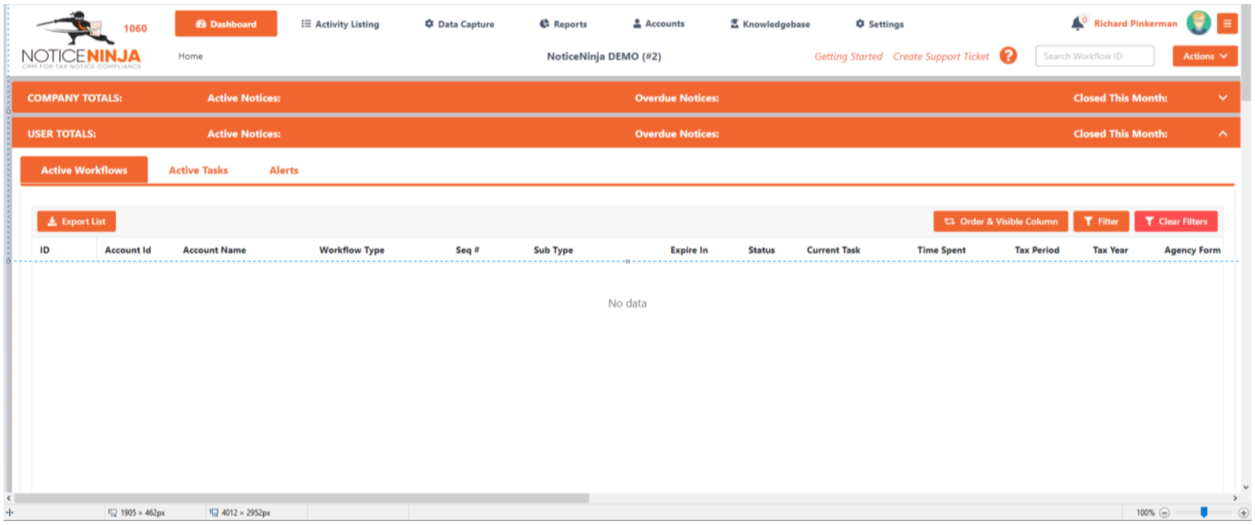


rick@noticeninja.com

Enter password

•••••••••••

The user is logged into NOTICENINJA and can perform basic functions.



NoticeNinja DEMO (#2)

COMPANY TOTALS: Active Notices: Overdue Notices: Closed This Month:

USER TOTALS: Active Notices: Overdue Notices: Closed This Month:

ID	Account Id	Account Name	Workflow Type	Seq #	Sub Type	Expire In	Status	Current Task	Time Spent	Tax Period	Tax Year	Agency Form

No data