DOCUMENTATION

osTicket
Support Ticket System

SAML Authentication

Prepared By :

Sakshi Kashyap

Prepared For :

Basket Hunt
BETA

Basket Hunt Pvt. Ltd.

Basket Hunt, H/N 111, Near Maa
Ambey Medical Hall, Habibpur,
Sahibganj, Jharkhand, India

SAML Authentication in osTicket

SAML Authentication

SAML stands for **Security Assertion Markup Language**. It is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP). It eliminates the need for multiple passwords and, with the help of single sign-on (SSO) functionality, offers a secure, easy way to access multiple applications with common login credentials.

Identity Provider — The IdP is an entity that stores user identities or resources such as usernames, passwords, and SSH keys.

Service Provider — The SP is an application or a third-party entity that provides service to an end user. SPs need authentication from the IdP to facilitate authentication for the user.

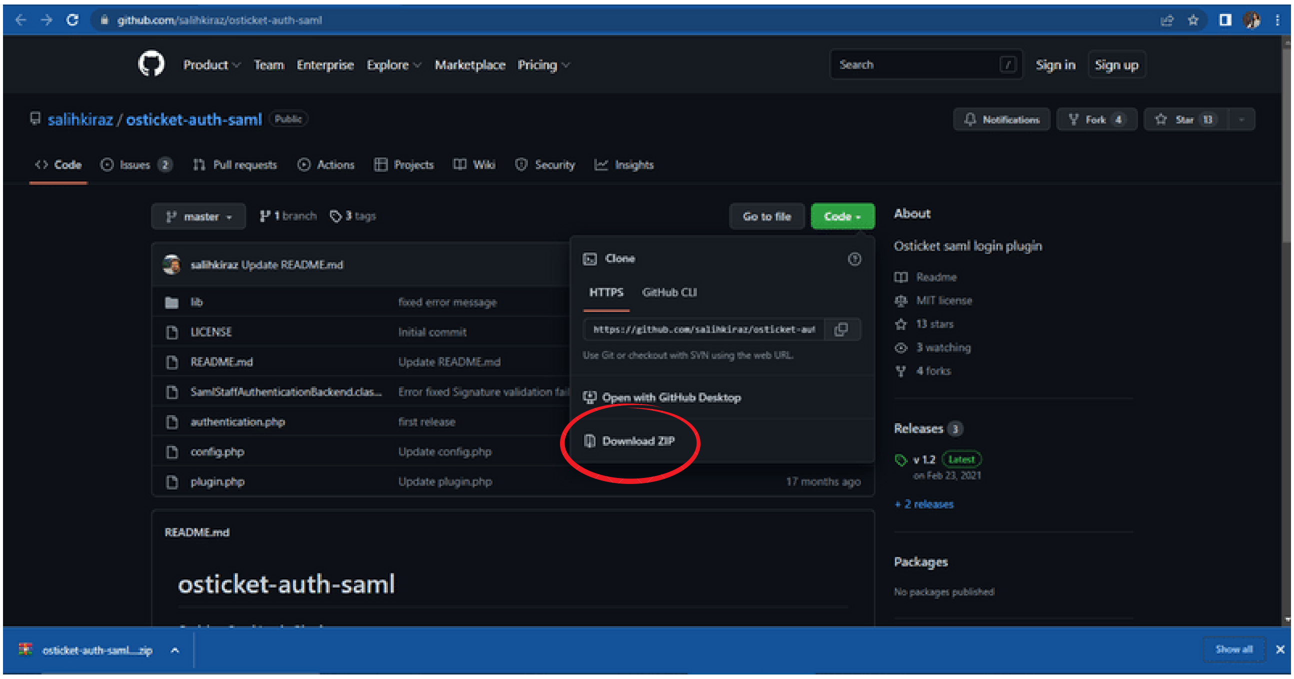
Setting up of SAML Authentication in osTicket

We will be using Microsoft Azure Active Directory as Identity Provider and osTicket application as Service Provider. The steps are as follows:

Step 1- Downloading and activating the osticket-auth-saml plugin.

Go to the link given below:
https://github.com/salihkiraz/osticket-auth-saml

Download the zip file and upload the file in plugins folder and extract it.
(Cyber panel > Websites > List Websites > File Manager > public_html > include > plugins)



salihkiraz / osticket-auth-saml Public

master · 1 branch · 3 tags

salihkiraz Update README.md

lib	fixed error message
LICENSE	Initial commit
README.md	Update README.md
SamlStaffAuthenticationBackend.clas...	Error fixed Signature validation fai
authentication.php	first release
config.php	Update config.php
plugin.php	Update plugin.php · 17 months ago

https://github.com/salihkiraz/osticket-aut

Use Git or checkout with SVN using the web URL.

About

Osticket saml login plugin

Readme · MIT license · 13 stars · 3 watching · 4 forks

Releases 3

v 1.2 Latest on Feb 23, 2021

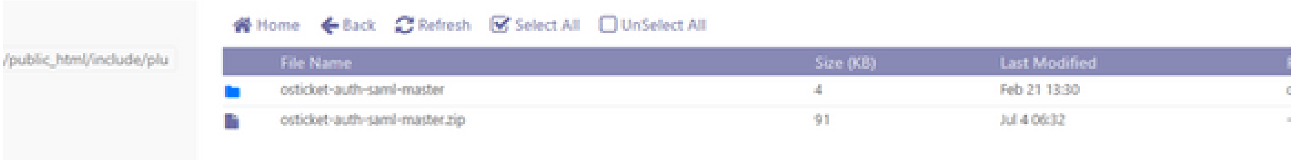
+ 2 releases

Packages

No packages published

README.md

osticket-auth-saml

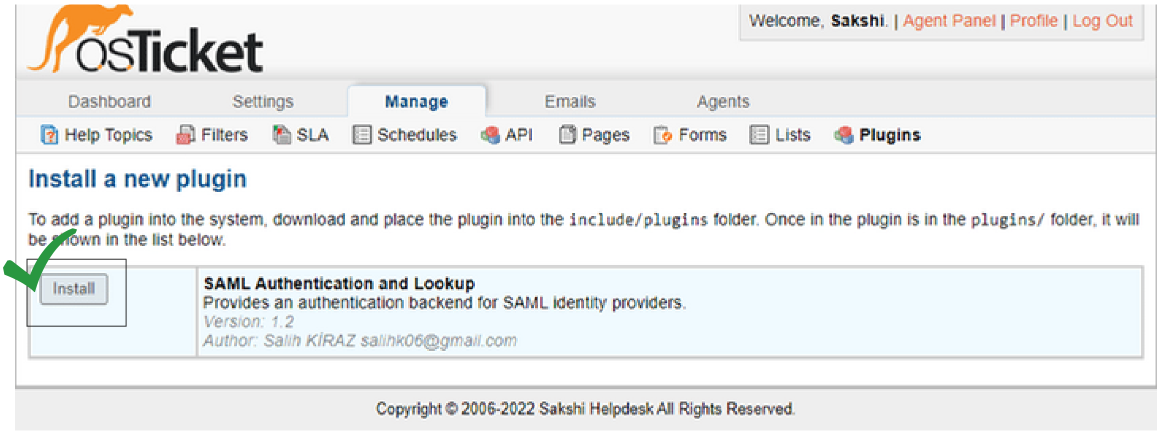


/public_html/include/plu

File Name	Size (KB)	Last Modified
osticket-auth-saml-master	4	Feb 21 13:30
osticket-auth-saml-master.zip	91	Jul 4 06:32

Now login to your osTicket helpdesk and download and install the plugin.

Admin Panel > Manage > Plugins > Add New Plugin



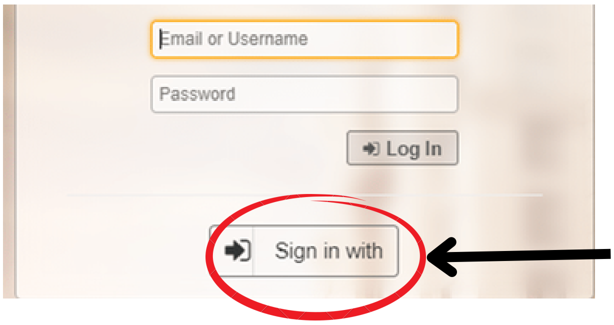
Install a new plugin

To add a plugin into the system, download and place the plugin into the include/plugins folder. Once in the plugin is in the plugins/ folder, it will be shown in the list below.

SAML Authentication and Lookup
Provides an authentication backend for SAML identity providers.
Version: 1.2
Author: Salih KIRAZ salihk06@gmail.com

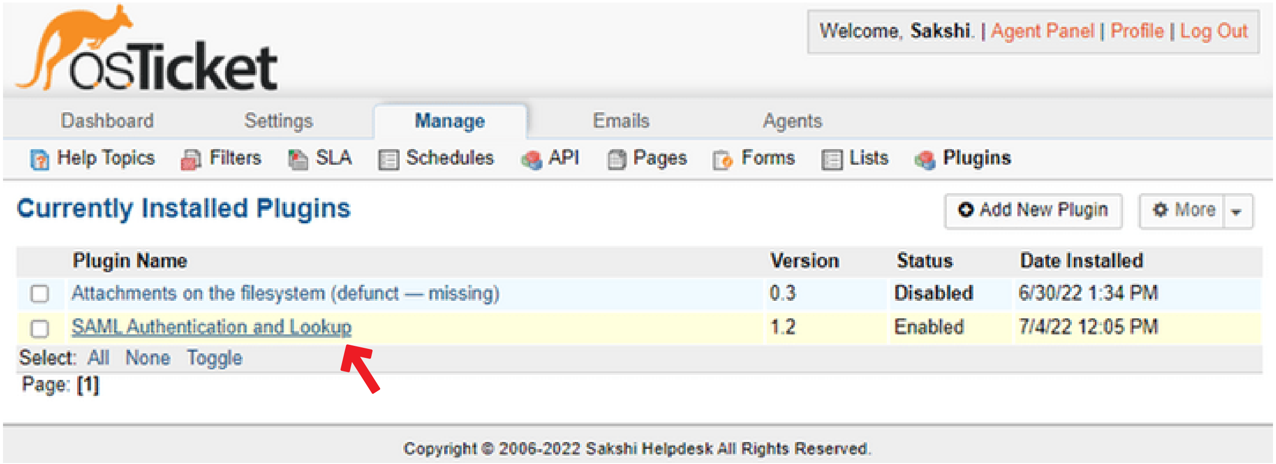
Copyright © 2006-2022 Sakshi Helpdesk All Rights Reserved.

After installing, **enable the plugin** and log out.



This button will start appearing now onwards in the login page. .

Admin Panel > Manage > Plugins > SAML Authentication and Lookup



Currently Installed Plugins

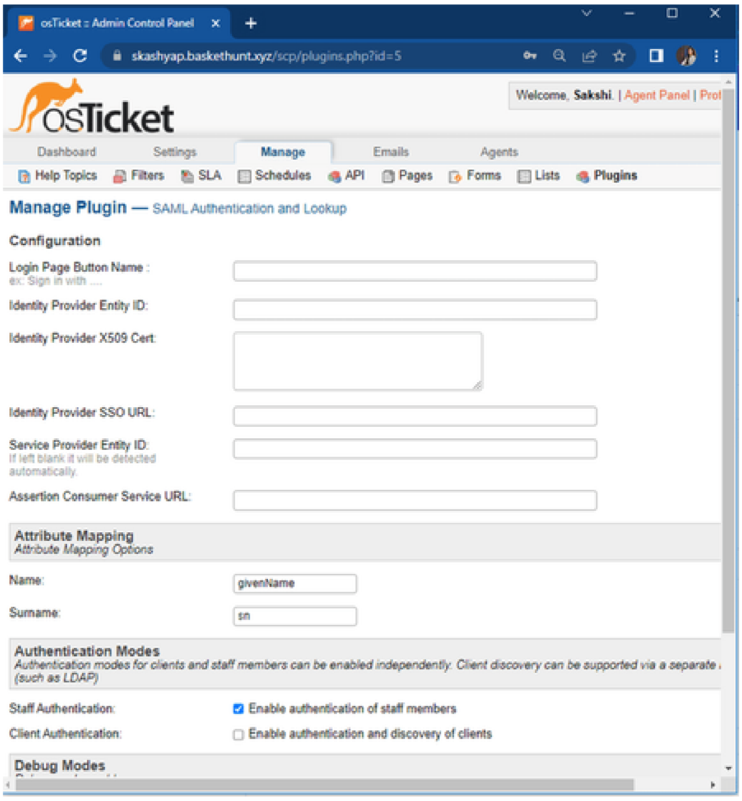
	Plugin Name	Version	Status	Date Installed
□	Attachments on the filesystem (defunct — missing)	0.3	Disabled	6/30/22 1:34 PM
□	SAML Authentication and Lookup	1.2	Enabled	7/4/22 12:05 PM

Select: All None Toggle

Page: [1]

Copyright © 2006-2022 Sakshi Helpdesk All Rights Reserved.

The window appears as shown below:


osTicket :: Admin Control Panel
skashyap.baskethunt.xyz/scp/plugins.php?id=5
Welcome, Sakshi. | Agent Panel | Prof
Dashboard
Settings
Manage
Emails
Agents
Help Topics
Filters
SLA
Schedules
API
Pages
Forms
Lists
Plugins

Manage Plugin — SAML Authentication and Lookup

Configuration

Login Page Button Name :
ex: Sign in with ....

Identity Provider Entity ID:

Identity Provider X509 Cert:

Identity Provider SSO URL:

Service Provider Entity ID:
If left blank it will be detected automatically.

Assertion Consumer Service URL:

Attribute Mapping
Attribute Mapping Options

Name: givenName

Surname: sn

Authentication Modes
Authentication modes for clients and staff members can be enabled independently. Client discovery can be supported via a separate (such as LDAP)

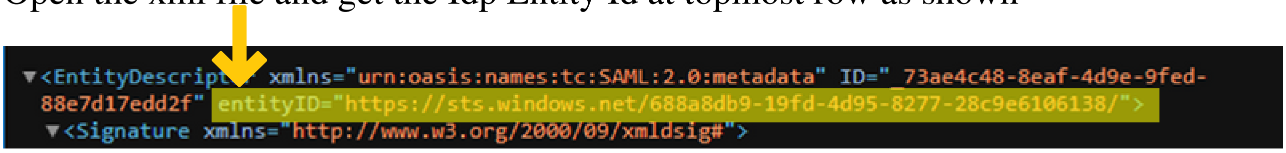
Staff Authentication: ☑ Enable authentication of staff members

Client Authentication: □ Enable authentication and discovery of clients

Debug Modes

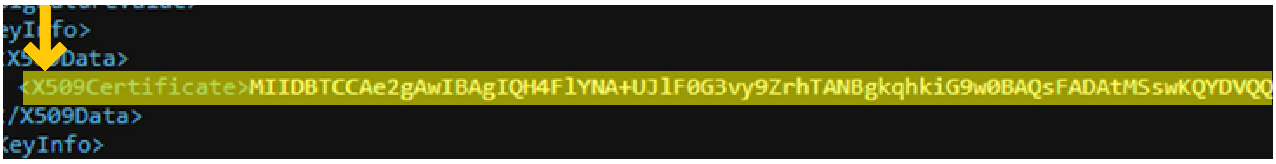
Fill the details in the above window from the xml file using the link below:
https://login.microsoftonline.com/688a8db9-19fd-4d95-8277-28c9e6106138/federationmetadata/2007-06/federationmetadata.xml

Open the xml file and get the Idp Entity Id at topmost row as shown-



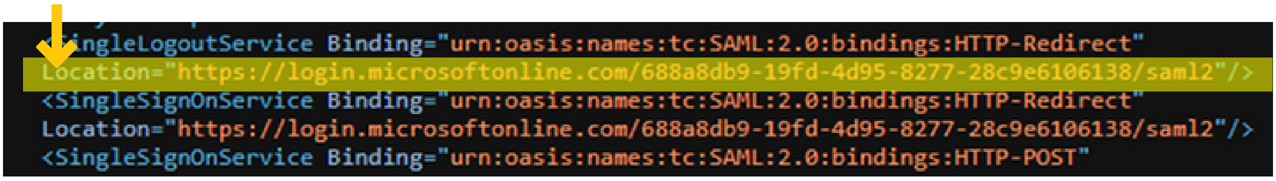
```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_73ae4c48-8eaf-4d9e-9fed-
 88e7d17edd2f" entityID="https://sts.windows.net/688a8db9-19fd-4d95-8277-28c9e6106138/">
  ▼<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

Idp X509 Certificate:



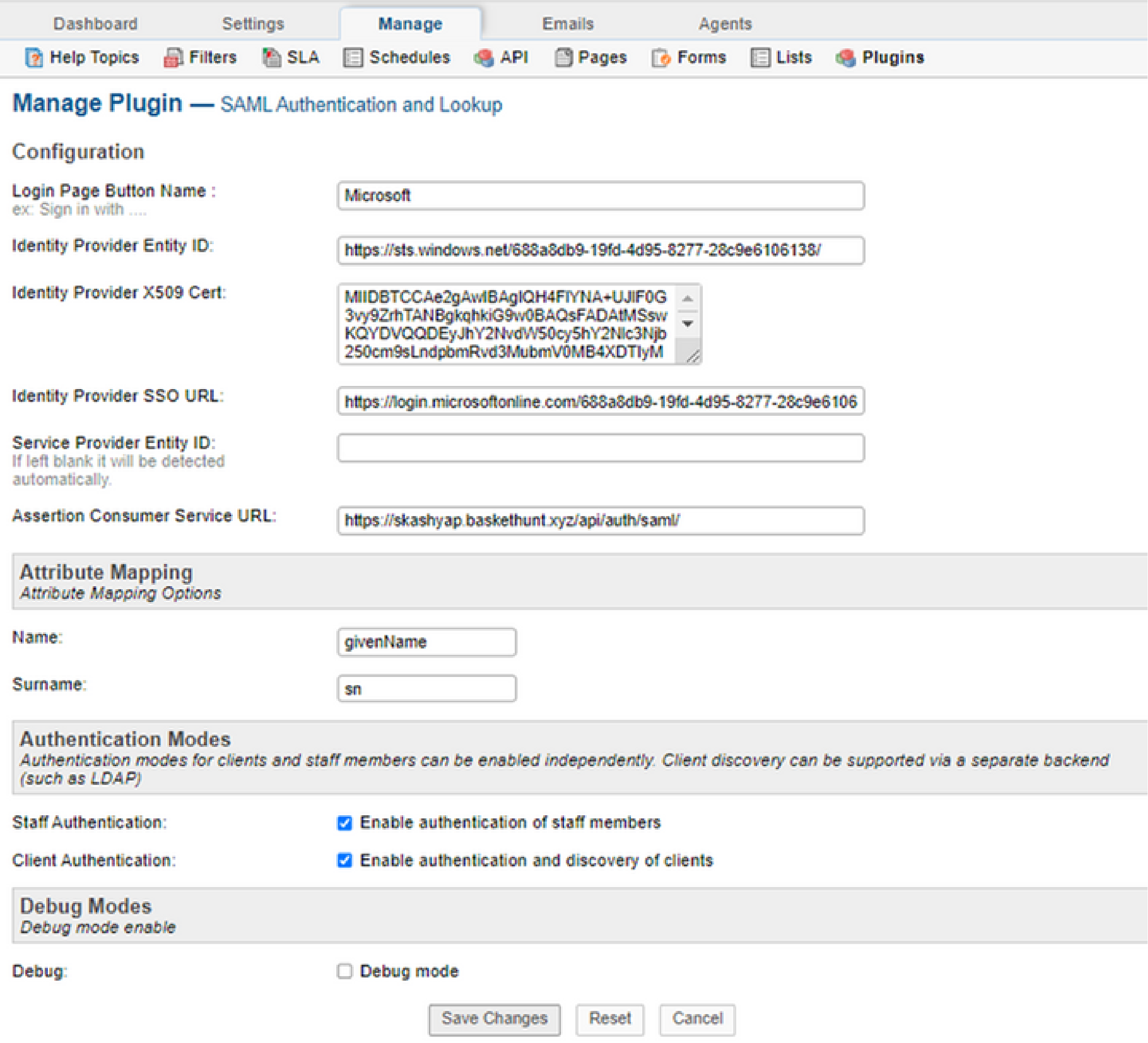
```
eyInfo>
X509Data>
 <X509Certificate>MIIDBTCCAe2gAwIBAgIQH4FlYNA+UJlF0G3vy9ZrhTANBgkqhkiG9w0BAQsFADAtMSswKQYDVQQ
/X509Data>
KeyInfo>
```

Idp SSO URL:



```
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://login.microsoftonline.com/688a8db9-19fd-4d95-8277-28c9e6106138/saml2"/>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://login.microsoftonline.com/688a8db9-19fd-4d95-8277-28c9e6106138/saml2"/>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
```

Complete the details and save changes.



Manage Plugin — SAML Authentication and Lookup

Configuration

Login Page Button Name :
ex: Sign in with ....
Microsoft

Identity Provider Entity ID:
https://sts.windows.net/688a8db9-19fd-4d95-8277-28c9e6106138/

Identity Provider X509 Cert:
MIIDBTCCAe2gAwIBAgIQH4FlYNA+UJlF0G
3vy9ZrhTANBgkqhkiG9w0BAQsFADAtMSsw
KQYDVQQDEyJhY2NvdW50cy5hY2Nlc3Njb
250cm9sLndpbmRvd3MubmV0MB4XDTIyM

Identity Provider SSO URL:
https://login.microsoftonline.com/688a8db9-19fd-4d95-8277-28c9e6106

Service Provider Entity ID:
If left blank it will be detected automatically.

Assertion Consumer Service URL:
https://skashyap.baskethunt.xyz/api/auth/saml/

Attribute Mapping
Attribute Mapping Options

Name:
givenName

Surname:
sn

Authentication Modes
Authentication modes for clients and staff members can be enabled independently. Client discovery can be supported via a separate backend (such as LDAP)

Staff Authentication: ☑ Enable authentication of staff members

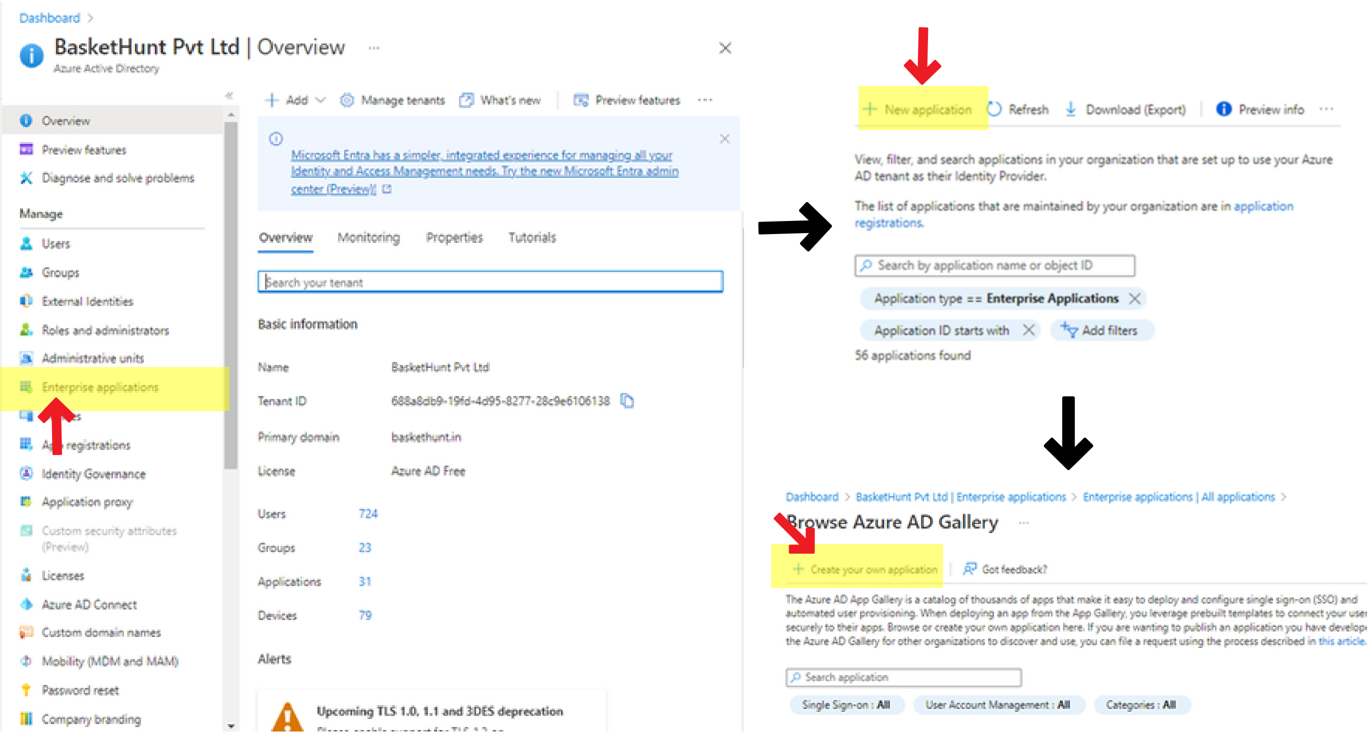
Client Authentication: ☑ Enable authentication and discovery of clients

Debug Modes
Debug mode enable

Debug: ☐ Debug mode

Now, working on the Identity Provider (Idp), here we have used Microsoft Azure Active Directory. Get access to your Microsoft Azure AD account and login.

Create your own new application on Azure AD by following the steps below:



Dashboard >

BasketHunt Pvt Ltd | Overview ...

Azure Active Directory

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center (Preview)!

Basic information

Name	BasketHunt Pvt Ltd
Tenant ID	688a8db9-19fd-4d95-8277-28c9e6106138
Primary domain	baskethunt.in
License	Azure AD Free

Users	724
Groups	23
Applications	31
Devices	79

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID
Application type == Enterprise Applications
Application ID starts with
Add filters

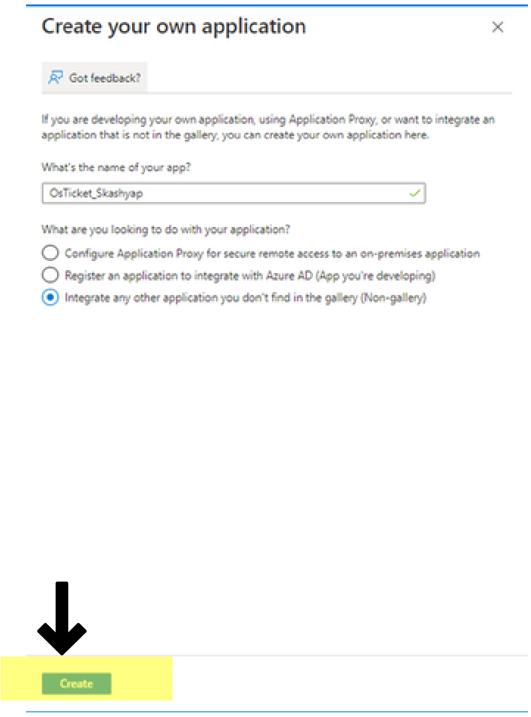
56 applications found

Dashboard > BasketHunt Pvt Ltd | Enterprise applications > Enterprise applications | All applications >

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 user securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have develop the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Now, give the application name and click on 'Create'.



Create your own application

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

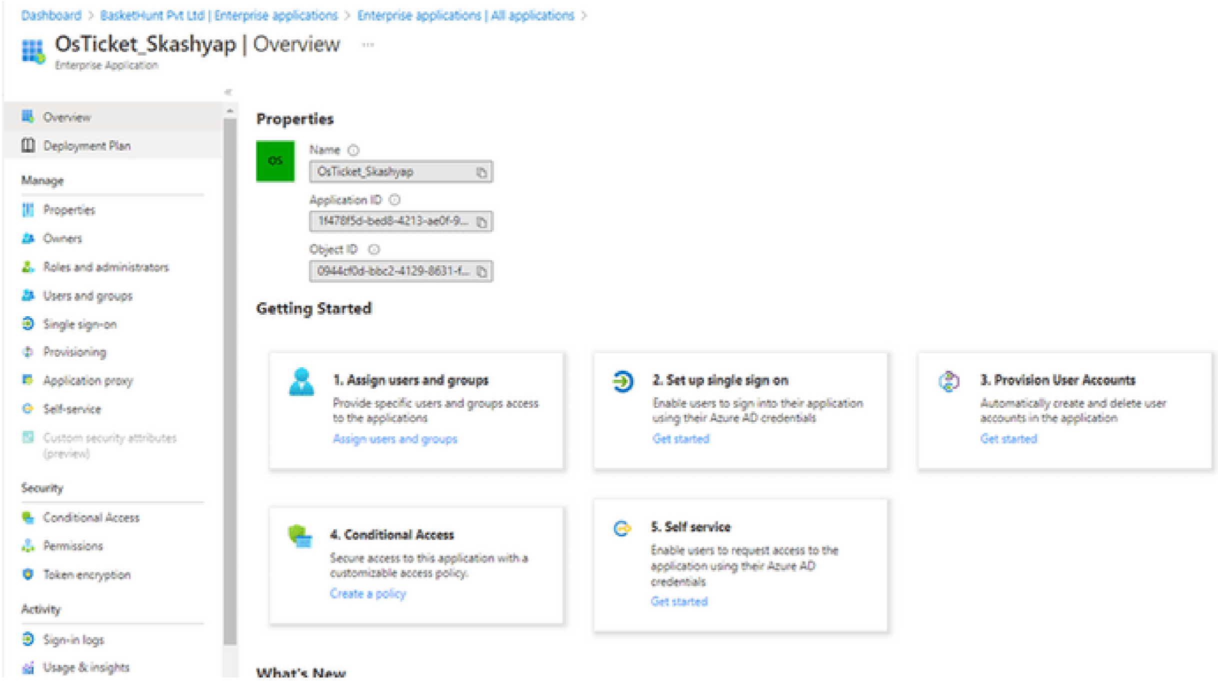
OsTicket_Skashyap

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

The new application is created.

Open the application and a window similar to the one shown below will appear.



Properties

Name: OsTicket_Skashyap

Application ID: 1f478f5d-bed8-4213-ae0f-9...

Object ID: 0944cf0d-bbc2-4129-8631-f...

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

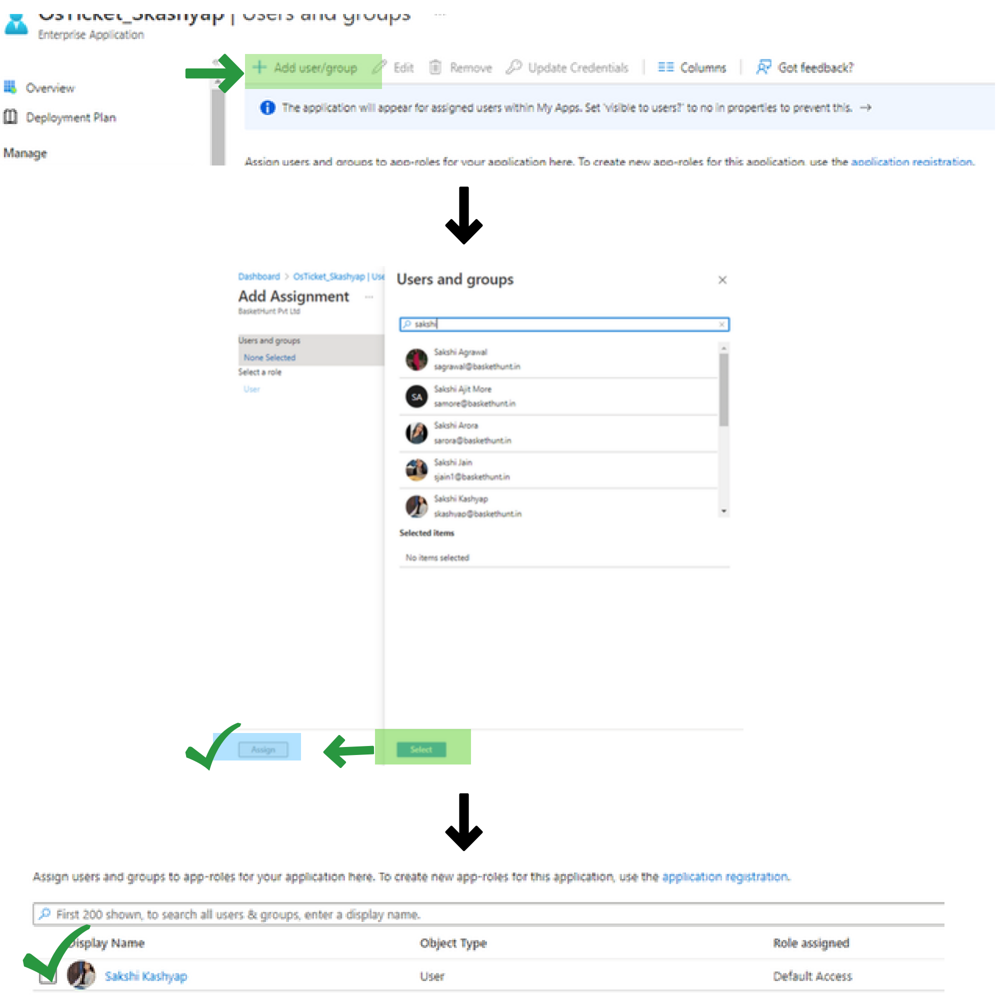
3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

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

1. Assign Users and Groups



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

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

sakshi

Sakshi Agrawal
sagrawal@baskethunt.in

Sakshi Ajit More
samore@baskethunt.in

Sakshi Arora
sarora@baskethunt.in

Sakshi Jain
sjain1@baskethunt.in

Sakshi Kashyap
skashyap@baskethunt.in

Selected items

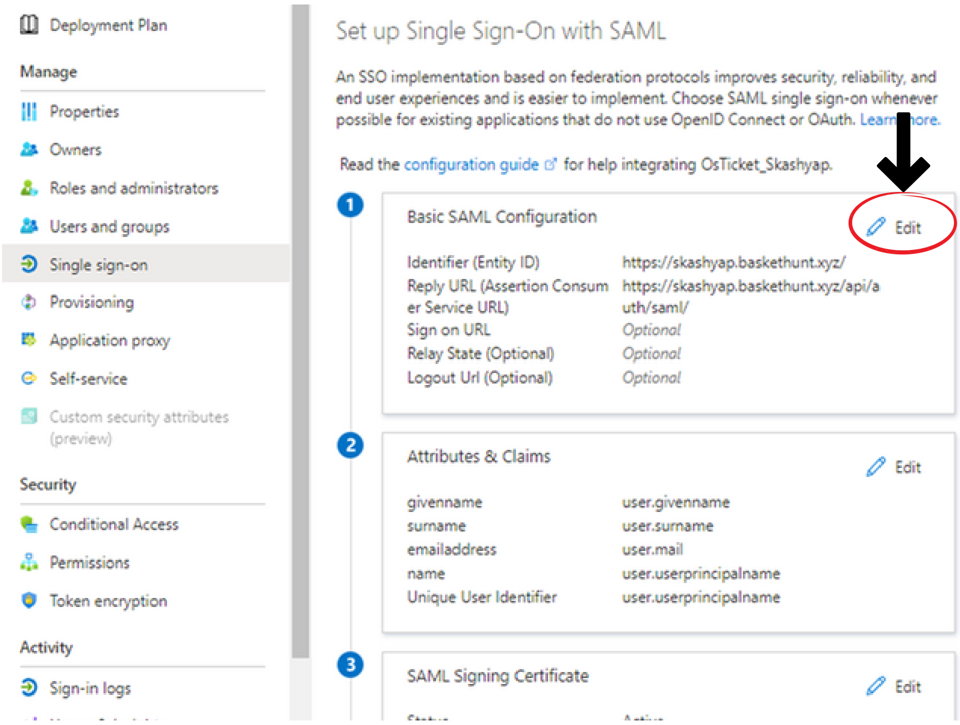
No items selected

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
Sakshi Kashyap	User	Default Access

2. Set up Single Sin 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 OsTicket_Skashyap.

1 Basic SAML Configuration

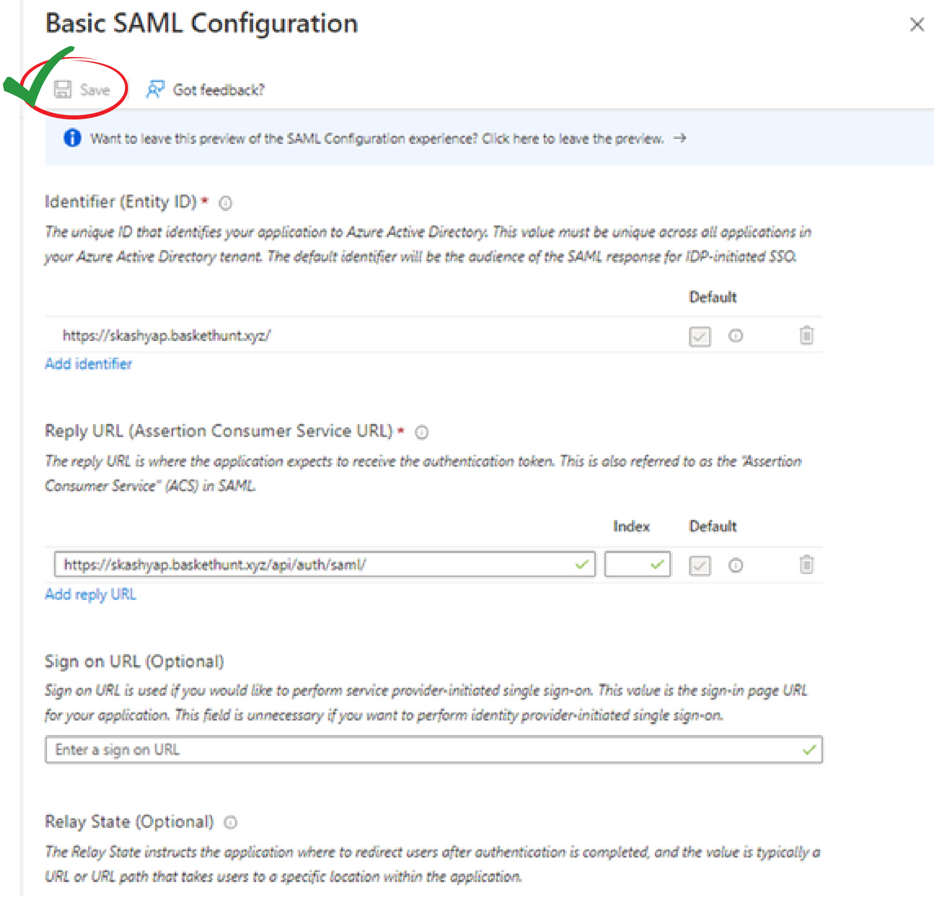
Identifier (Entity ID)	https://skashyap.baskethunt.xyz/
Reply URL (Assertion Consumer Service URL)	https://skashyap.baskethunt.xyz/api/auth/saml/
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

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

3 SAML Signing Certificate

Add the identifier (entity id) and Reply URL and save changes.



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. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

https://skashyap.baskethunt.xyz/

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.

https://skashyap.baskethunt.xyz/api/auth/saml/

Sign on URL (Optional)

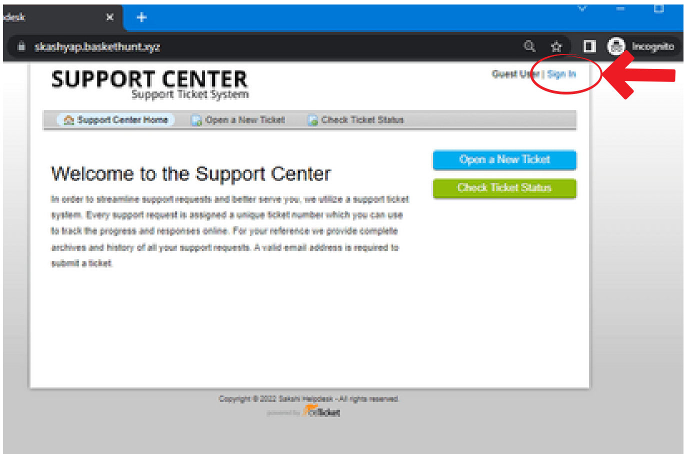
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

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.

Now open a new incognito window and give the address of your osTicket Helpdesk.



skashyap.baskethunt.xyz

Incognito

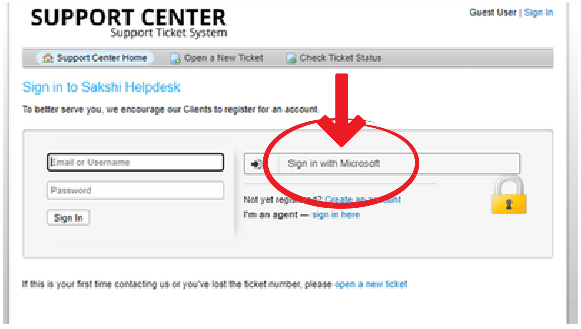
SUPPORT CENTER
Support Ticket System

Guest User | Sign In

Welcome to the Support Center

In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required to submit a ticket.

Copyright © 2022 Sakshi Helpdesk - All rights reserved.



SUPPORT CENTER
Support Ticket System

Guest User | Sign In

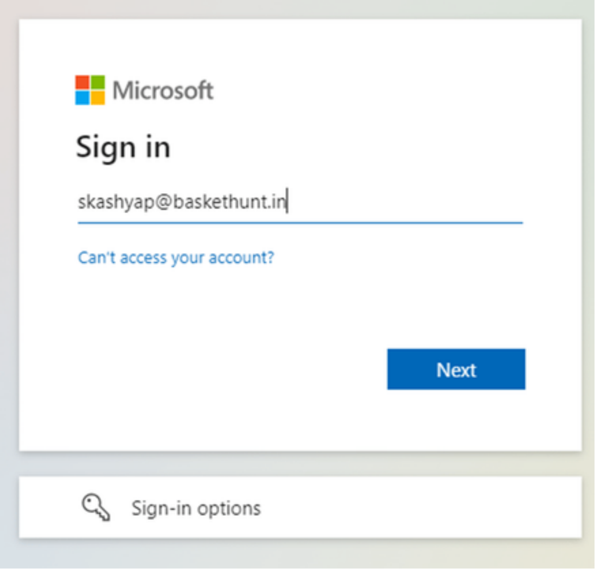
Sign in to Sakshi Helpdesk

To better serve you, we encourage our Clients to register for an account.

Not yet registered? Create an account

I'm an agent — sign in here

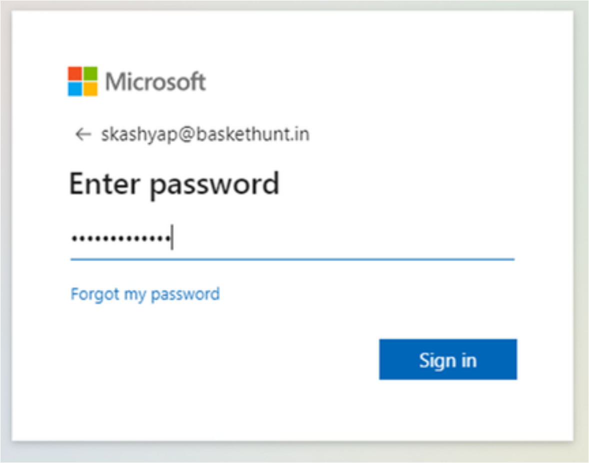
If this is your first time contacting us or you've lost the ticket number, please open a new ticket



Microsoft

Sign in

skashyap@baskethunt.in



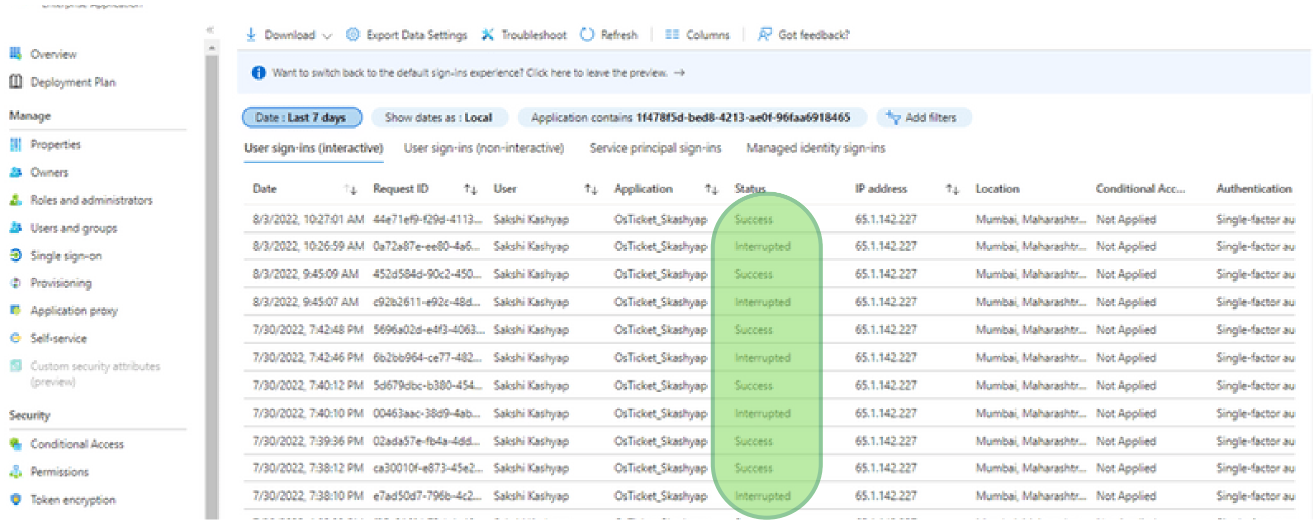
Microsoft

← skashyap@baskethunt.in

Enter password

••••••••••••

This is how you will be logged in using SAML authentication. The success status can be seen on Azure AD by going on **Sign-in Logs** option as shown below.



Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 7 days** | Show dates as : **Local** | Application contains **1f478f5d-bed8-4213-ae0f-96faa6918465** | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive) | Service principal sign-ins | Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...	Authentication
8/3/2022, 10:27:01 AM	44e71ef9-f29d-4113...	Sakshi Kashyap	OsTicket_Skashyap	Success	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
8/3/2022, 10:26:59 AM	0a72a87e-ee80-4a6...	Sakshi Kashyap	OsTicket_Skashyap	Interrupted	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
8/3/2022, 9:45:09 AM	452d584d-90c2-450...	Sakshi Kashyap	OsTicket_Skashyap	Success	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
8/3/2022, 9:45:07 AM	c92b2611-e92c-48d...	Sakshi Kashyap	OsTicket_Skashyap	Interrupted	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:42:48 PM	5696a02d-e4f3-4063...	Sakshi Kashyap	OsTicket_Skashyap	Success	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:42:46 PM	6b2bb964-ce77-482...	Sakshi Kashyap	OsTicket_Skashyap	Interrupted	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:40:12 PM	5d679dbc-b380-454...	Sakshi Kashyap	OsTicket_Skashyap	Success	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:40:10 PM	00463aac-38d9-4ab...	Sakshi Kashyap	OsTicket_Skashyap	Interrupted	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:39:36 PM	02ada57e-fb4a-4dd...	Sakshi Kashyap	OsTicket_Skashyap	Success	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:38:12 PM	ca30010f-e873-45e2...	Sakshi Kashyap	OsTicket_Skashyap	Success	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au
7/30/2022, 7:38:10 PM	e7ad50d7-796b-4c2...	Sakshi Kashyap	OsTicket_Skashyap	Interrupted	65.1.142.227	Mumbai, Maharashtr...	Not Applied	Single-factor au