Microsoft
Entra ID

Integration with servicenow®

Satyanarayan Rout
Servicenow.satyarout@gmail.com

What is SSO (Single Sign-On)?

- Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

Satyanarayan Rout
Servicenow.satyarout@gmail.com

How does SSO work?

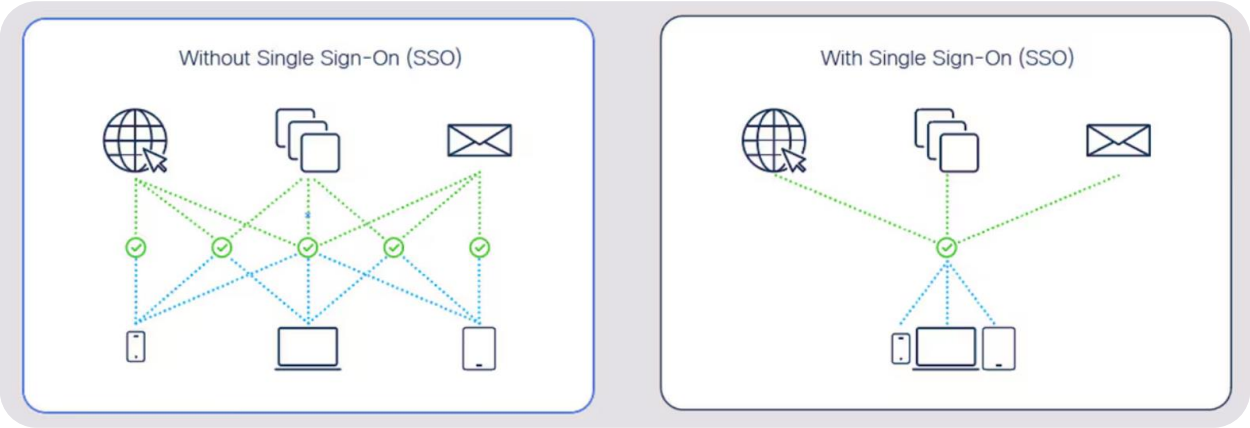
- When a user signs into an SSO service, the service creates an authentication token that verifies the user's identity. This token is a piece of digital data stored in the user's web browser or on the SSO service's servers.
- When a user attempts to access an application, the token checks with the SSO service, which passes the authentication token to the app. If the token is valid, the user is allowed to access the app. If the user has not yet signed in, they are prompted to do so through the SSO service.
- Most SSO services verify user credentials against a separate identity management system, or identity provider (IdP). The SSO service acts as an intermediary between the user and the IdP. It checks the user's login credentials against the IdP's database, but it does not manage the database itself.
- The ability to pass an authentication token to external apps and services is critical to the SSO process. This allows identity verification to take place separately from other cloud services, making SSO possible.
- Authentication tokens have their own communication standards to help ensure that they are correct and legitimate. The most common standards are Secure Authentication Markup Language (SAML) 2.0 and OpenID Connect/OAuth 2.0. These standards are like common "languages" for authentication tokens.

Satyanarayan Rout
Servicenow.satyarout@gmail.com

What are the benefits of SSO?

- In today's hybrid workforce environment, SSO can help to improve workers' productivity—especially when they need to access applications that are either on-premises or in the cloud. Password fatigue and errors are reduced as workers traverse multiple applications.

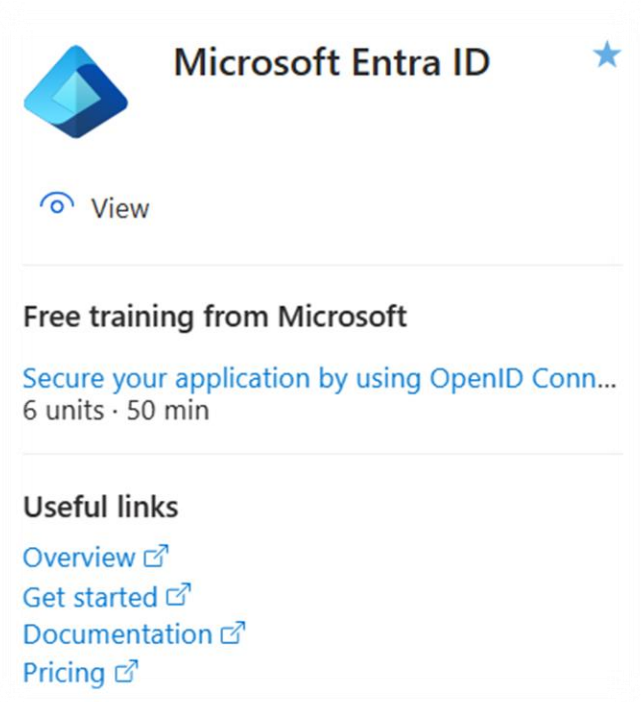
- Companies that have implemented SSO experience fewer help desk requests for password resets and other account issues. SSO can eliminate unproductive tasks while delivering cost savings.



Satyanarayan Rout
Servicenow.satyarout@gmail.com

What is Microsoft Entra ID?

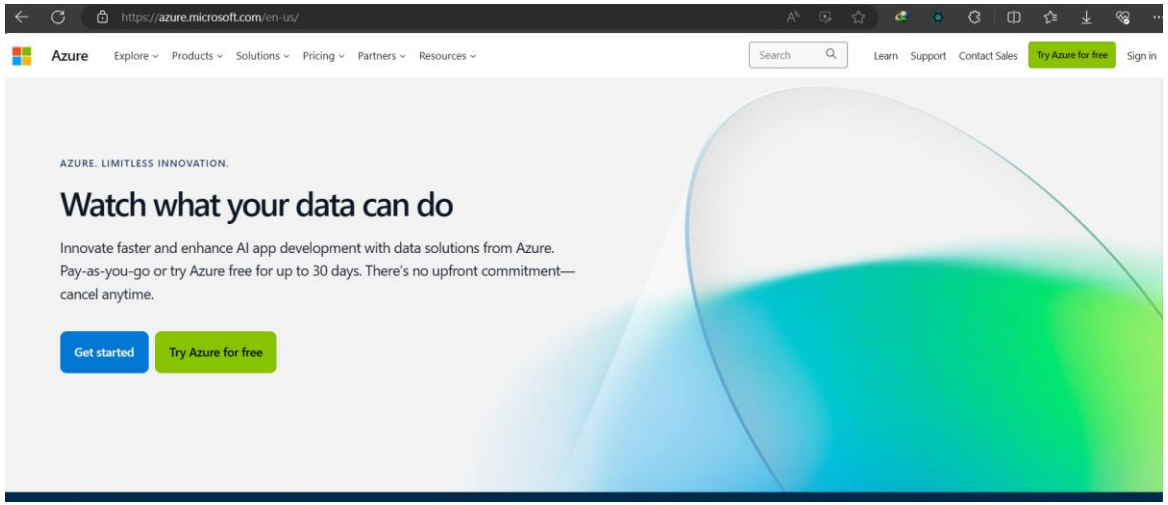
- Microsoft Entra ID is a cloud-based identity and access management service that enables your employees access external resources. Example resources include Microsoft 365, the Azure portal, and thousands of other SaaS applications.

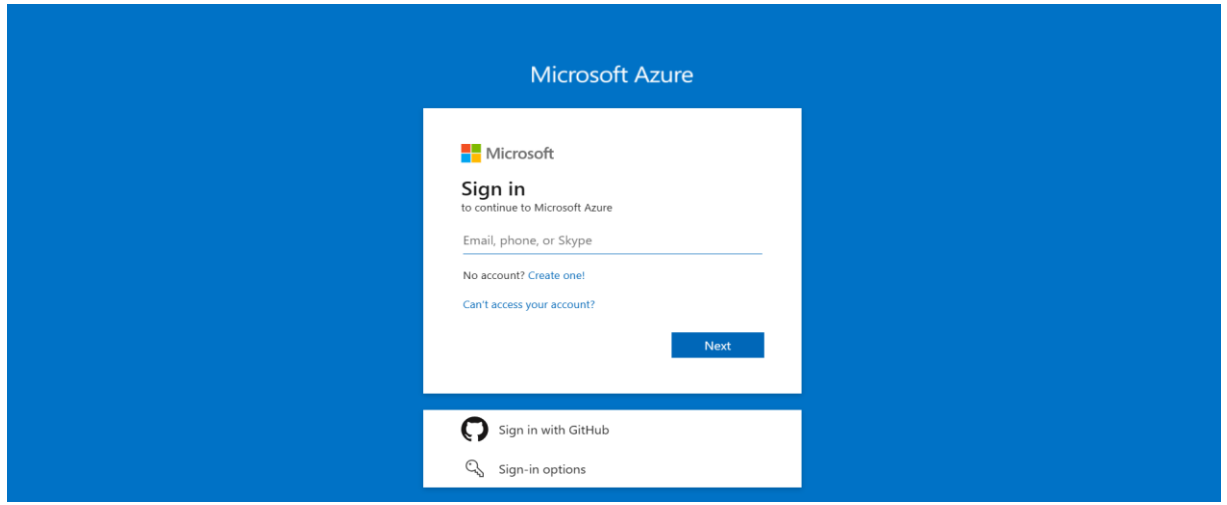


Satyanarayan Rout
Servicenow.satyarout@gmail.com

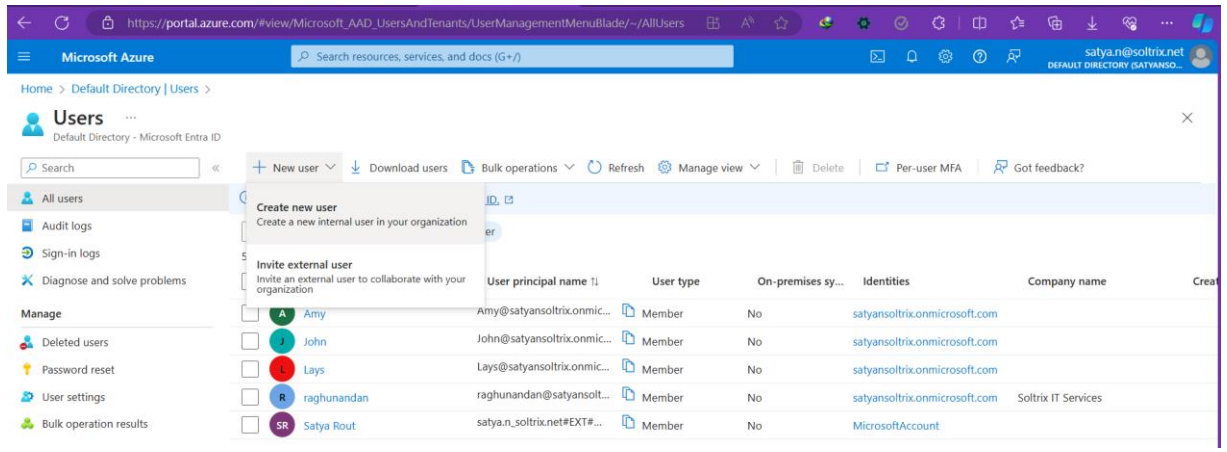
Pre-requisites for Azure SSO integration with ServiceNow

- Create an account in Microsoft Azure https://portal.azure.com/ access with one of the Active Directory.



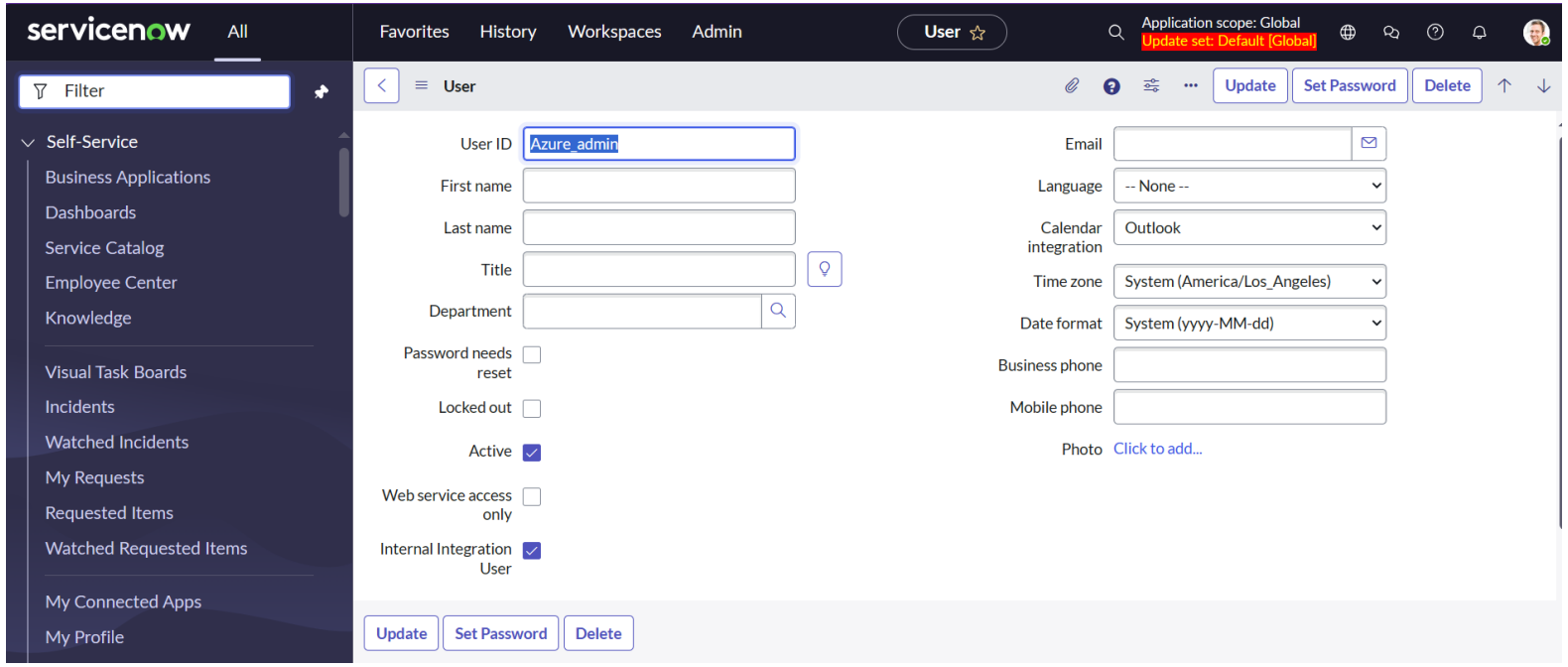


- Create users in Azure Entra ID.



Satyanarayan Rout
Servicenow.satyarout@gmail.com

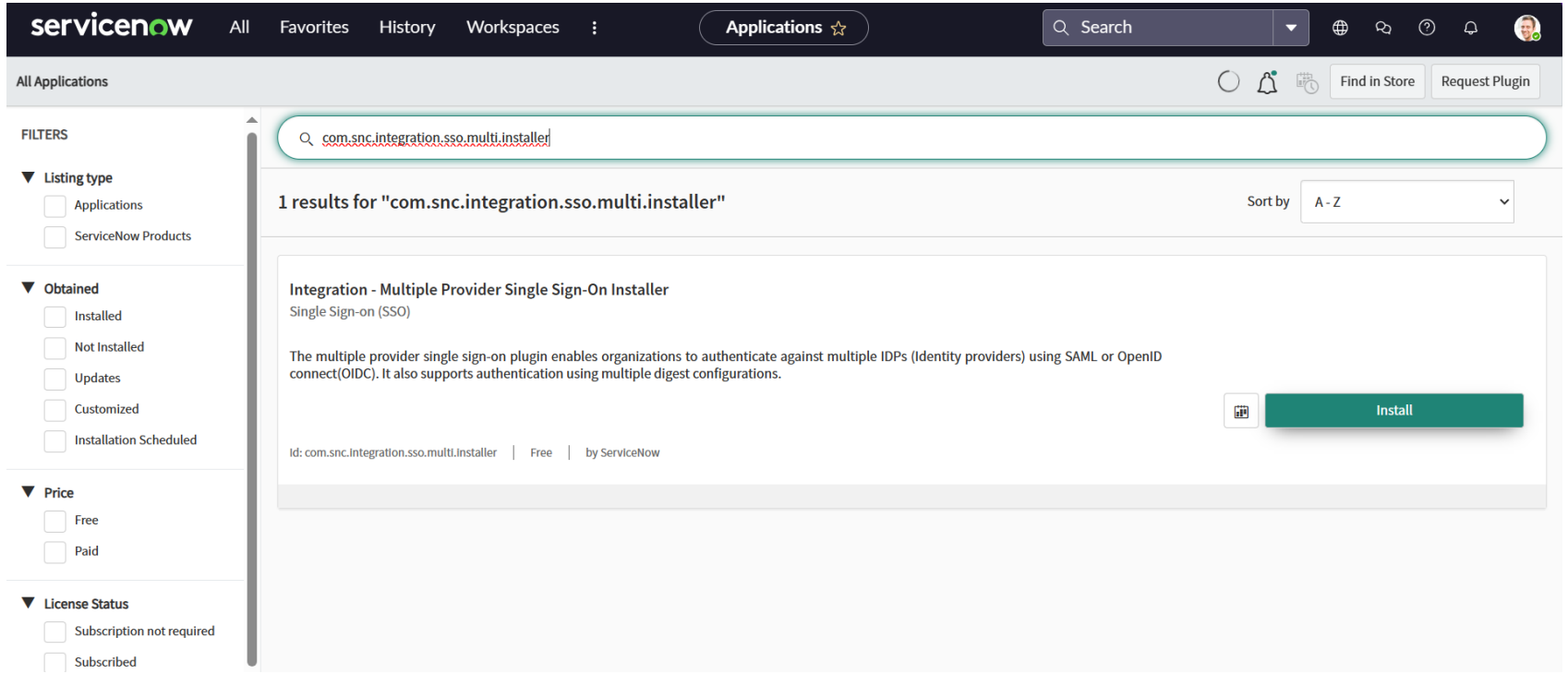
- Open your ServiceNow instance with admin access & create an integration user with Internal Integration User as “true” in user record with admin role & Save the ID,Password for future use.



Satyanarayan Rout
Servicenow.satyarout@gmail.com

- **Activate the plugin for SSO on ServiceNow:**

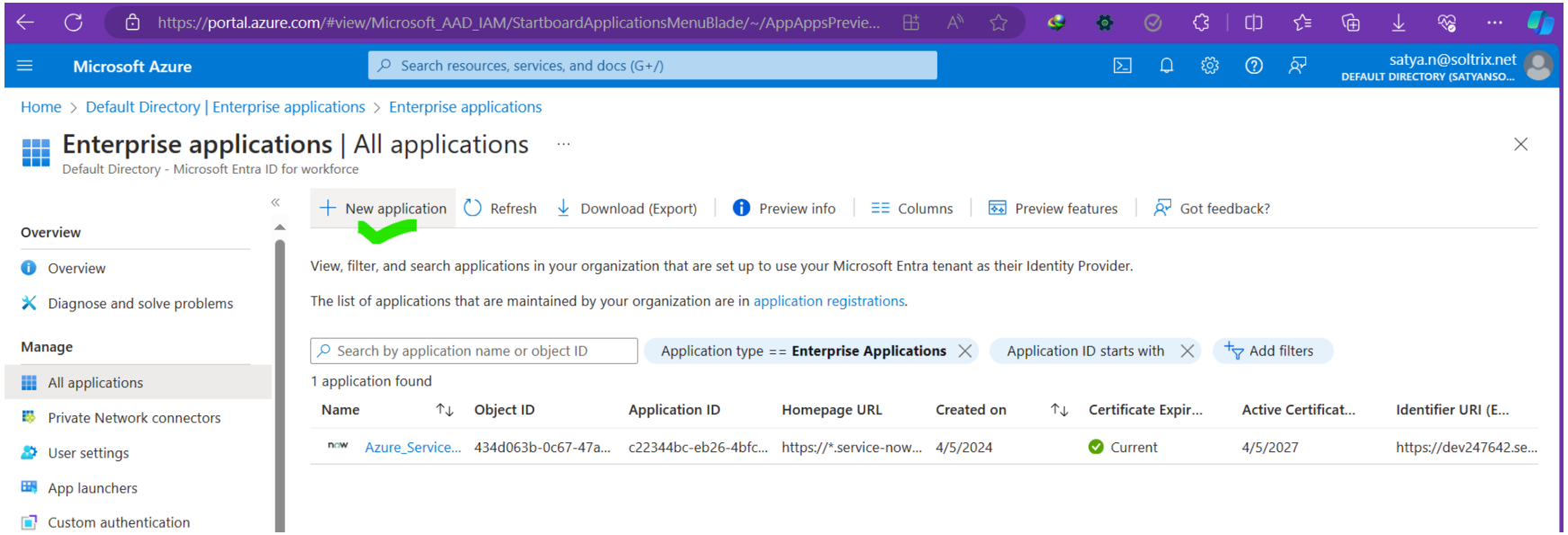
Integration - Multiple Provider Single Sign-On Installer – [**com.snc.integration.sso.multi.installer**]



Satyanarayan Rout
Servicenow.satyarout@gmail.com

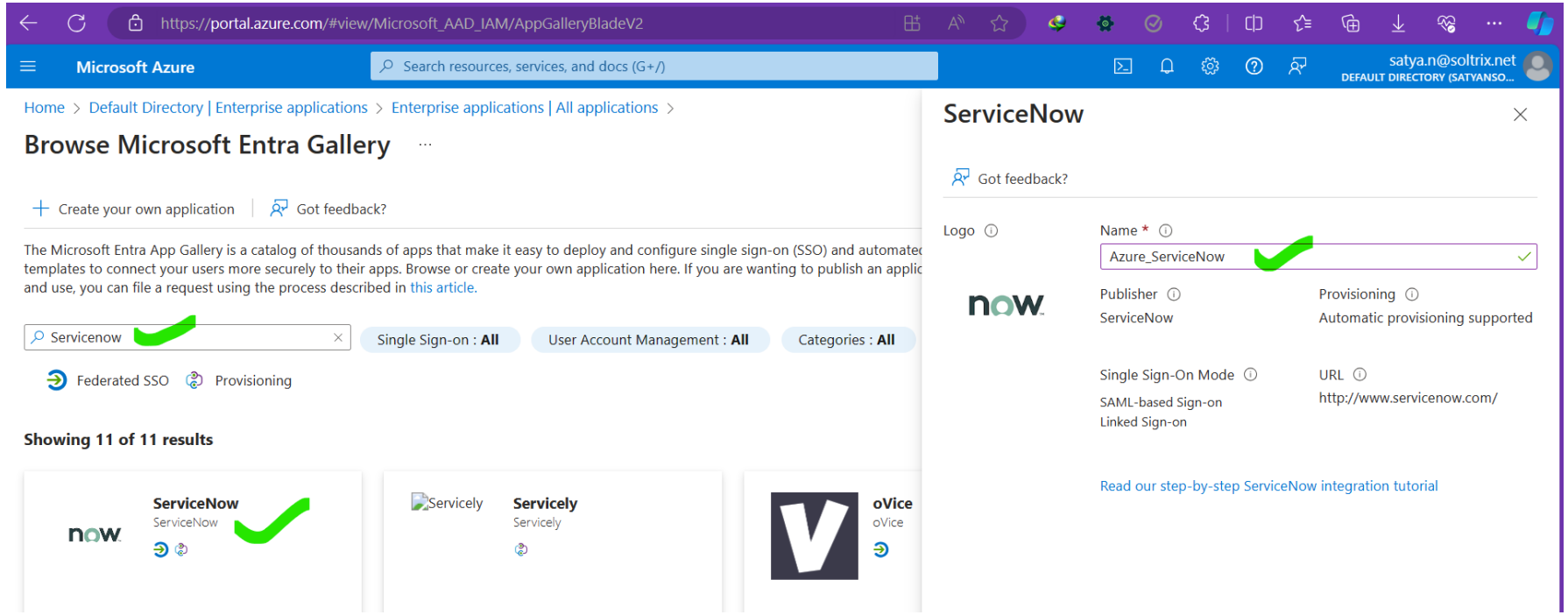
Implementation Steps at Azure Entra ID:

- Login to Azure portal and search for Enterprise application under Azure services: **Azure Entra ID>Enterprise application>Click on “New Application”.**



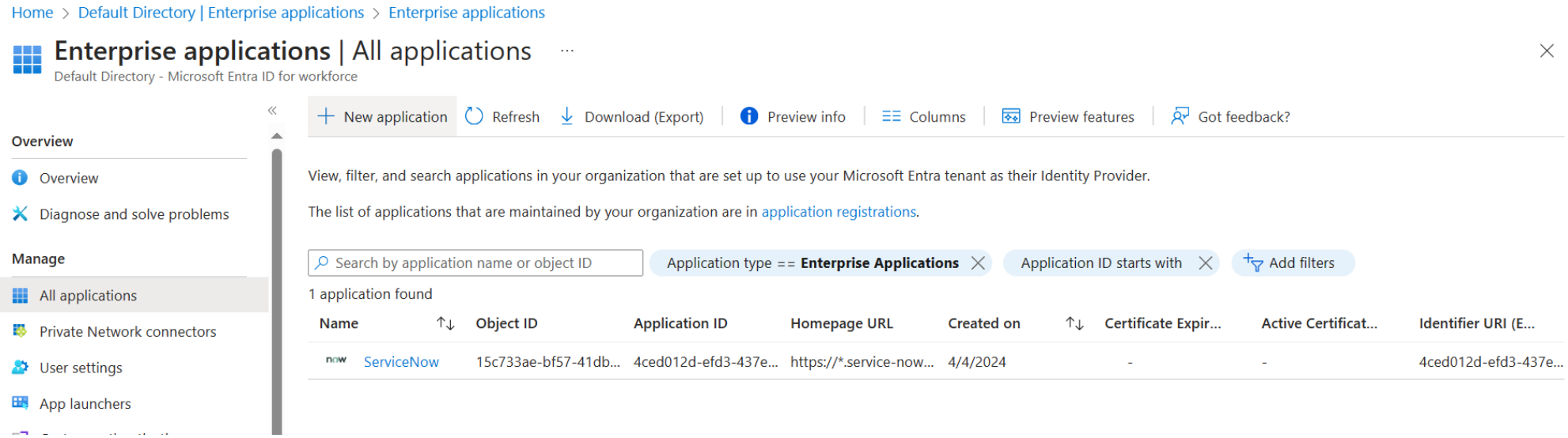
Satyanarayan Rout
Servicenow.satyarout@gmail.com

- Search for ServiceNow as shown in the screenshot below and click on ServiceNow widget. You can see a ServiceNow popup view where you can change the name (optional) and then click on “Create”. Note: Name is changed to **Azure_ServiceNow** in the below screenshot.



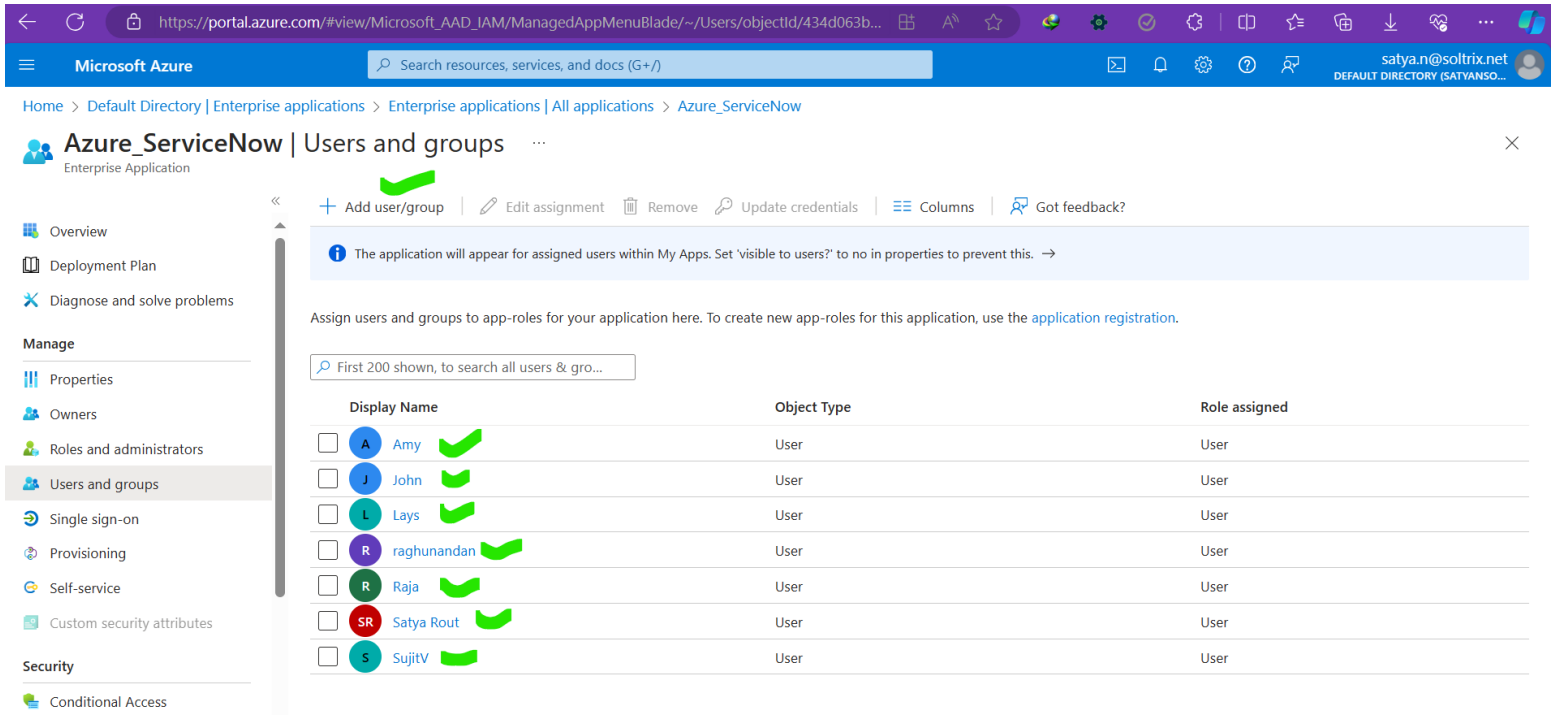
Satyanarayan Rout
Servicenow.satyarout@gmail.com

- After previous step azure will add ServiceNow application to the list of enterprise applications.



Satyanarayan Rout
Servicenow.satyarout@gmail.com

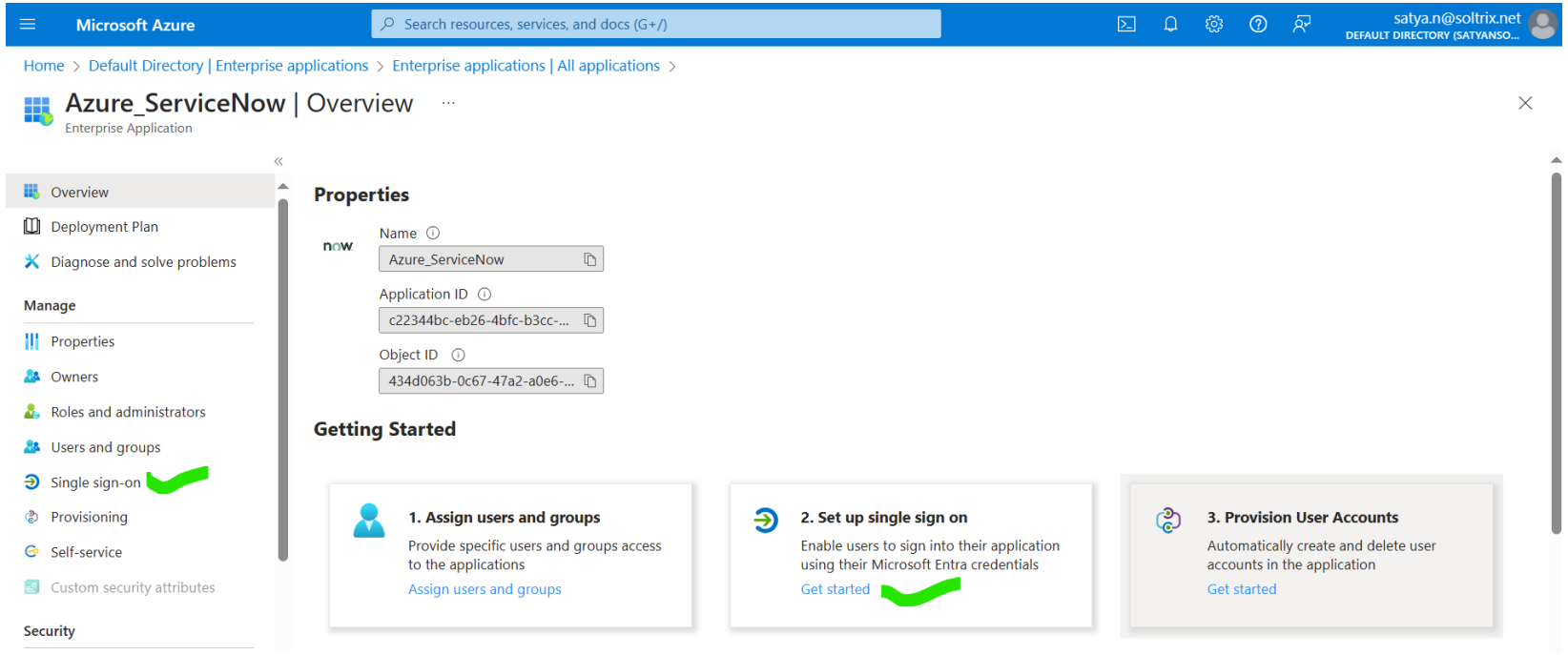
- Users which were created as a part of prerequisite in Azure Entra ID should be assigned to the new application which is created as a part of previous steps. In order to do so navigate to **Enterprise Applications → All applications → Click on the new application which is created in previous step (Azure_ServiceNow)→ Click on Assign users and groups.**



Satyanarayan Rout
Servicenow.satyarout@gmail.com

Next we need to configure SSO in Azure for ServiceNow App:

- To Configure SSO we need to setup single sign on. Navigate to **Enterprise Applications → All applications → Click on the new application which is created in previous step (Azure_ServiceNow)→ Check for Set up single sign on and click on Get started.**



Satyanarayan Rout
Servicenow.satyarout@gmail.com

- Click on SAML & then edit for “**Basic SAML Configuration**”.

Provide Your Instance Details in the format shown below:

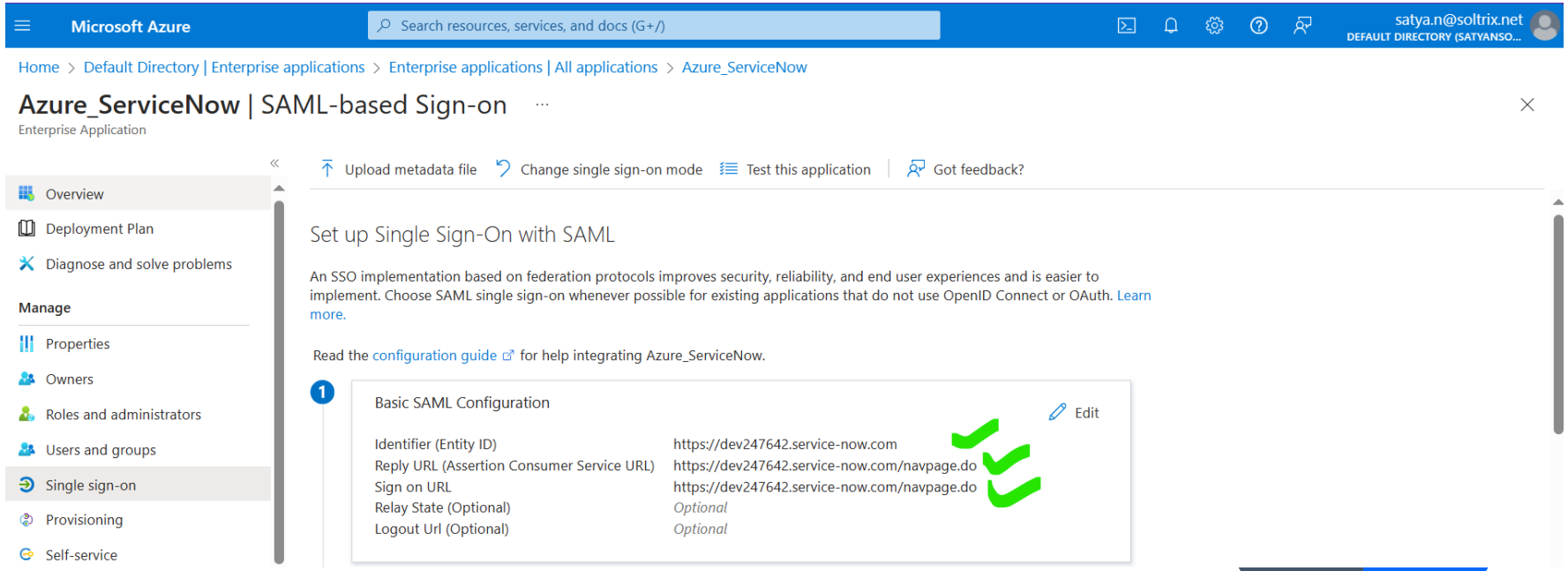
Provide your ServiceNow URL in Identifier (**Entity ID**) as shown below:

https://dev247642.service-now.com/

Reply URL and **Sign on URL** as:

https://dev247642.service-now.com/navpage.do

Click “**Save**”.



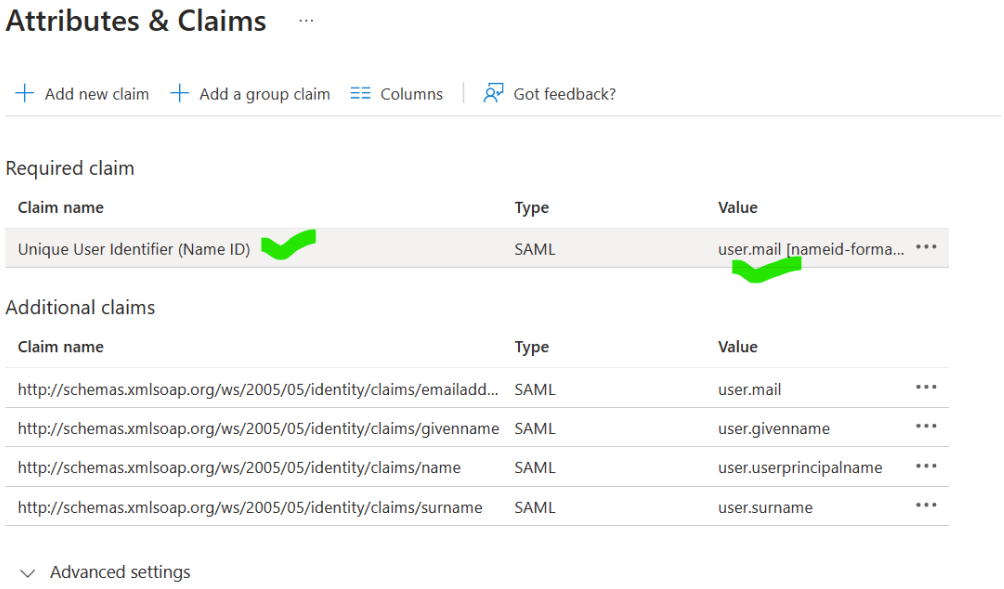
Satyanarayan Rout
Servicenow.satyarout@gmail.com

- **Check for Attributes & Claims → Click on Edit.**

Click on Value field under required claim as shown in screenshot below.

We need to change the value to user.mail . Once property is updated click on Save.

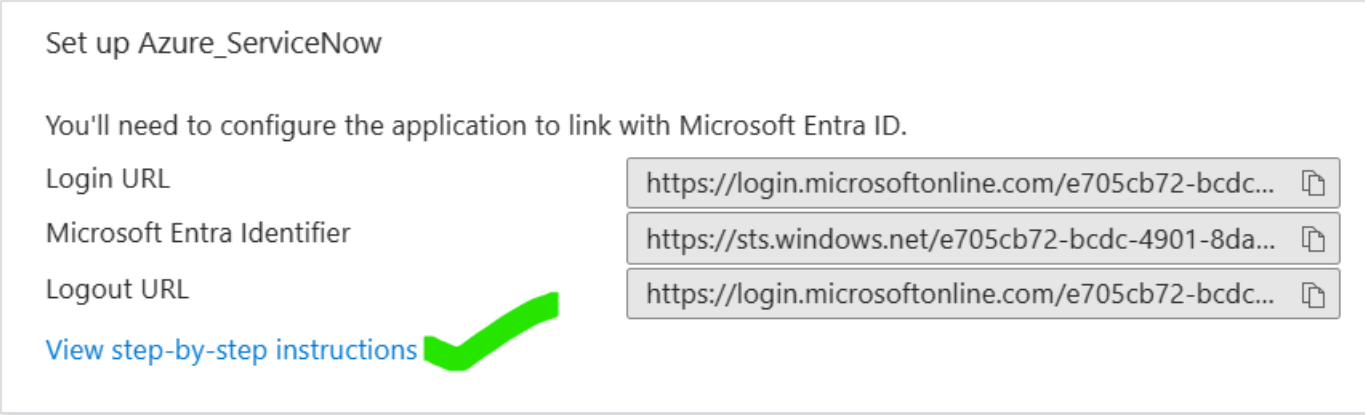
Note: We are changing this to user.mail since email is the common point in ServiceNow.

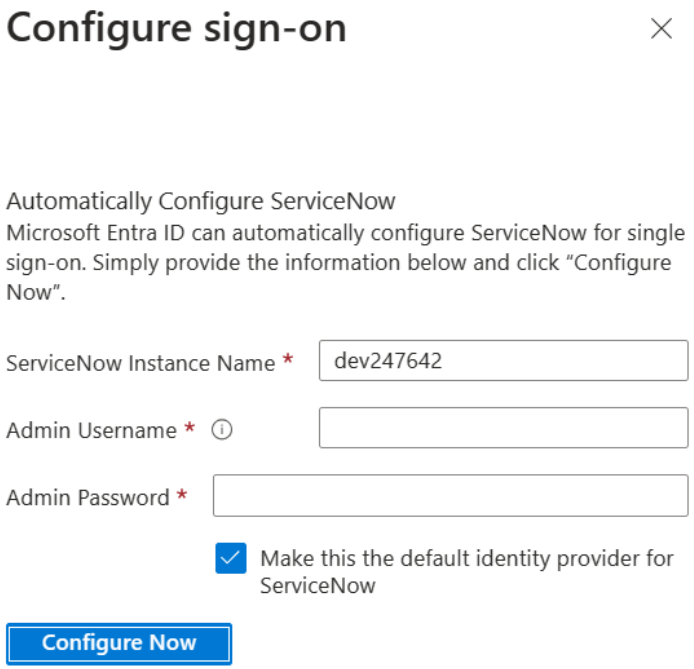


Satyanarayan Rout
Servicenow.satyarout@gmail.com

- Check the Set up Created application (Azure_ServiceNow) and Click on View step-by-step Instructions:

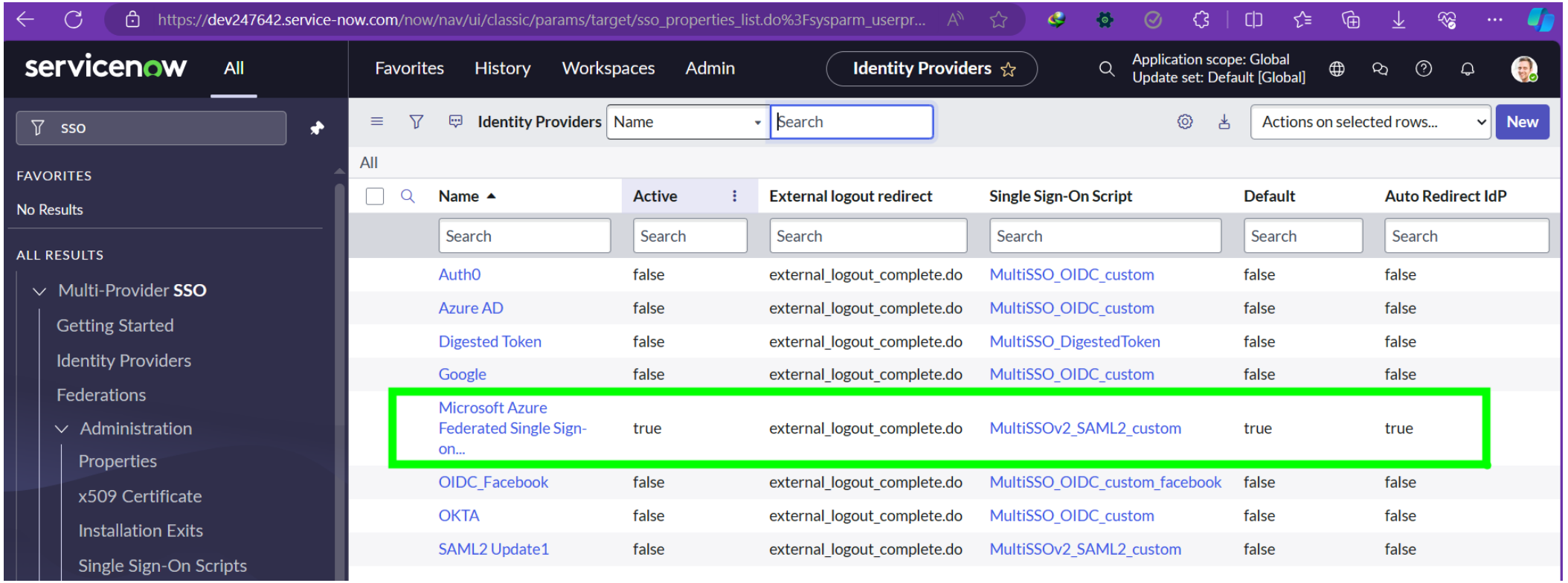
Provide the Username and Password of the user created in ServiceNow as a part of prerequisite **Azure_admin(Internal Integration User)** and click on Configure Now.





Satyanarayan Rout
Servicenow.satyarout@gmail.com

- Note: After completion of this step, you can see an Identity Provider record being created in ServiceNow for Azure.



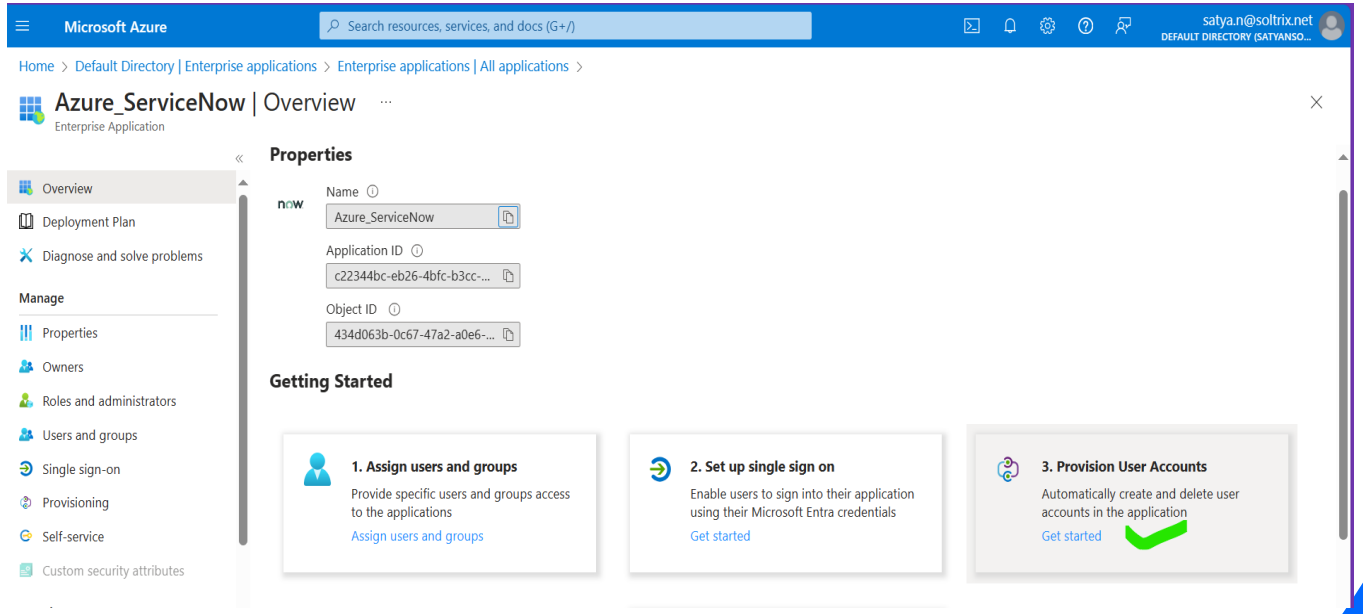
Satyanarayan Rout
Servicenow.satyarout@gmail.com

• Provisioning user accounts in Azure Entra ID:

Navigate to **Enterprise Applications → All applications → Click on the new application which is created in previous step (Azure_ServiceNow)→ Check for Provision User Accounts and click on Get started.**

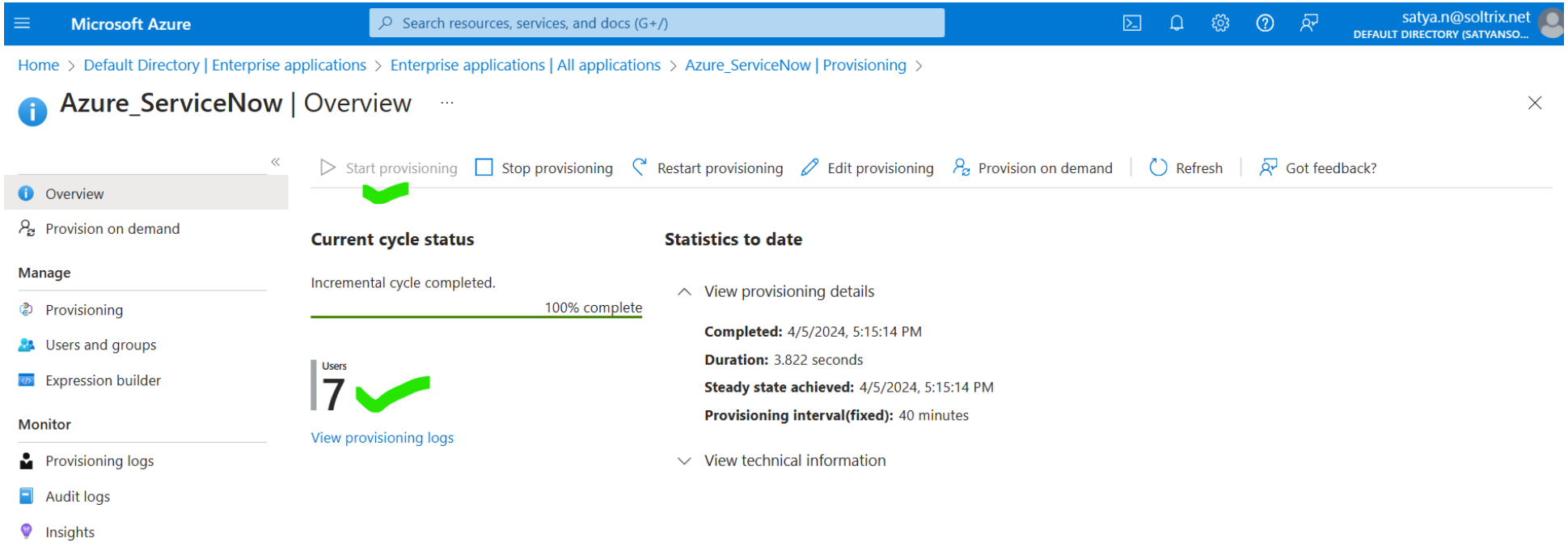
- Change the Provisioning Mode to Automatic. Provide the instance details along with admin credentials and Test Connection and click on SAVE.

- **Note:** You need to provide admin credentials and not the credentials for the user you have created as a part of prerequisite.



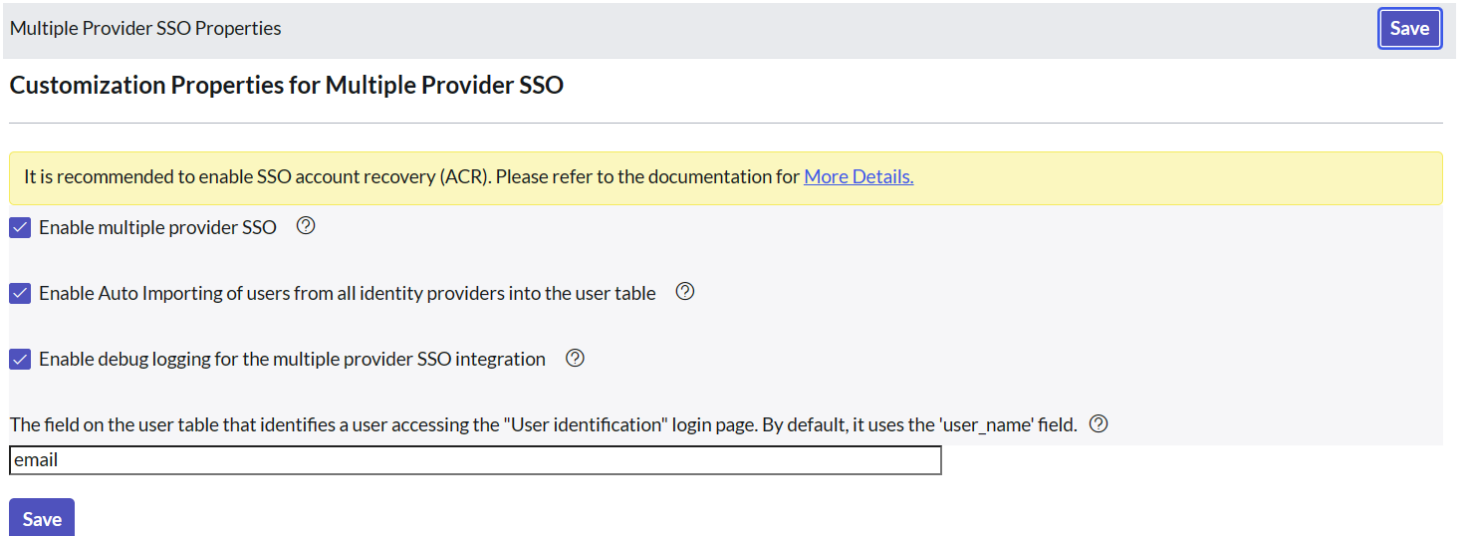
Satyanarayan Rout
Servicenow.satyarout@gmail.com

- **Navigate to Manage → Provisioning → Click on Start Provisioning**
- Provisioning interval is set to 40 Minutes by default. Once Provisioning is started data will be synced up to ServiceNow approximately within next 40 Minutes.



Satyanarayan Rout
Servicenow.satyarout@gmail.com

- **Implementation Steps at ServiceNow:**
- Navigate to Multi Provider SSO → Administration → Properties. Check the below properties and click Save.
- Enable Multiple provider SSO → True.
- Enable Auto Importing of users from all identity providers into the user table → True
- Enable debug logging for the multiple provider SSO integration → True.
- The field on the user table that identifies a user accessing the “User identification” login page. By default, it uses the ‘user_name’ field. → email.



Satyanarayan Rout
Servicenow.satyarout@gmail.com

- Navigate to sys_properties.LIST and search for **glide.authenticate.multisso.test.connection.mandatory** . Update this property to false.
- Note: If this property is not present in the instance, then create one for the same and

update to false.

- Navigate to Identity Providers and open the record created for Azure. Click on Set as Auto Redirect Idp related link.Once this is enabled It will start redirecting to SSO login when you try to login with ServiceNow instance URL.

- For Auto provisioning of users from Azure to ServiceNow check the Auto Provisioning User check box to True under User Provisioning tab. Also check the Create AuthContextClass to true under Advanced tab.

Satyanarayan Rout
Servicenow.satyarout@gmail.com

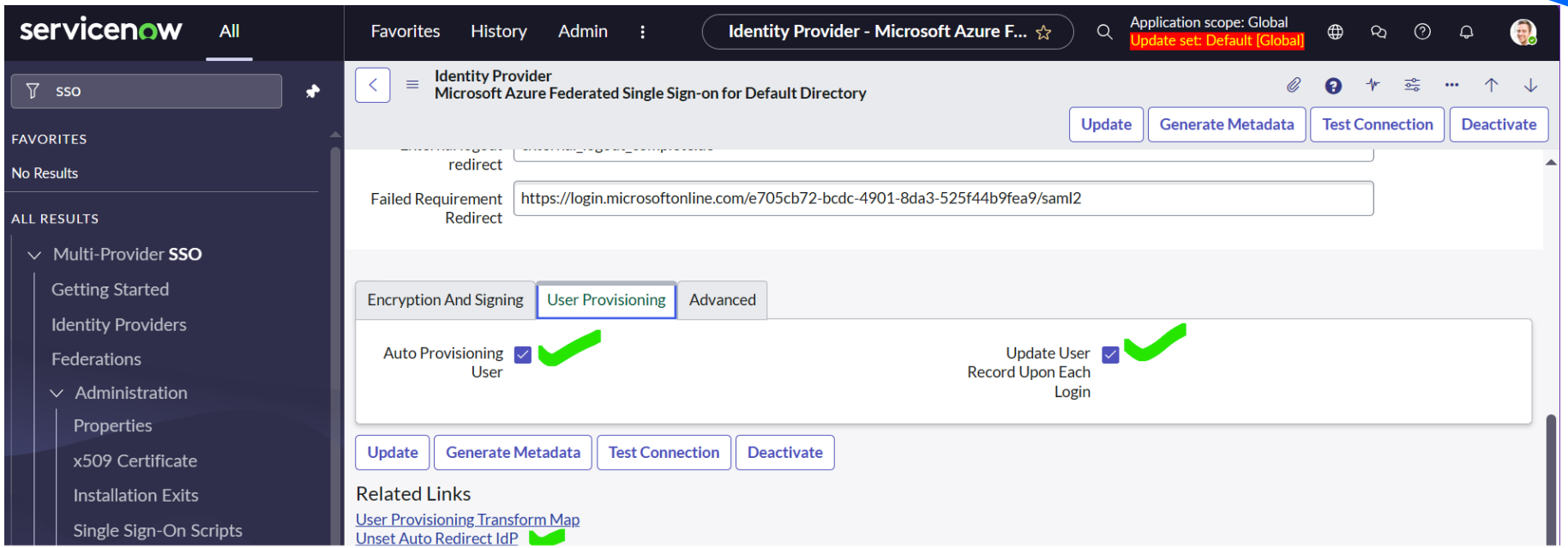
- Navigate to sys_properties.LIST and search for **glide.authenticate.multisso.test.connection.mandatory** . Update this property to false.
- Note: If this property is not present in the instance, then create one for the same and

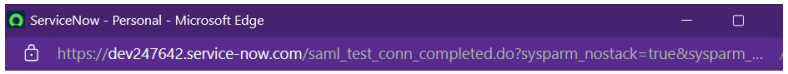
update to false.

- Navigate to Identity Providers and open the record created for Azure. Click on Set as Auto Redirect Idp related link.Once this is enabled It will start redirecting to SSO login when you try to login with ServiceNow instance URL.

- For Auto provisioning of users from Azure to ServiceNow check the Auto Provisioning User check box to True under User Provisioning tab. Also check the Create AuthContextClass to true under Advanced tab.

Satyanarayan Rout
Servicenow.satyarout@gmail.com





SSO Login Test Results

- SAML Login response received
- SAML Assertion retrieved
- Signature Validated
- Certificate Validated
- AudienceRestriction/Condition Validated
- Certificate Issuer Validated
- Subject Confirmation Validated

SSO Logout Test Results

- Cannot logout of IDP's session
  IDP's logout URL not set. So, cannot logout the IDP session.

SSO Test Connection Summary

SSO Login tests succeeded. SSO Logout tests failed. IDP Configuration can be activated by clicking 'Activate' button. Users will be able to login and logout of the instance, but will not be logged out of the IDP. Please refer to the logs for test details.

Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

Satyanarayan Rout
Servicenow.satyarout@gmail.com

Thank you!!!

Satyanarayan Rout
Servicenow.satyarout@gmail.com