



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.



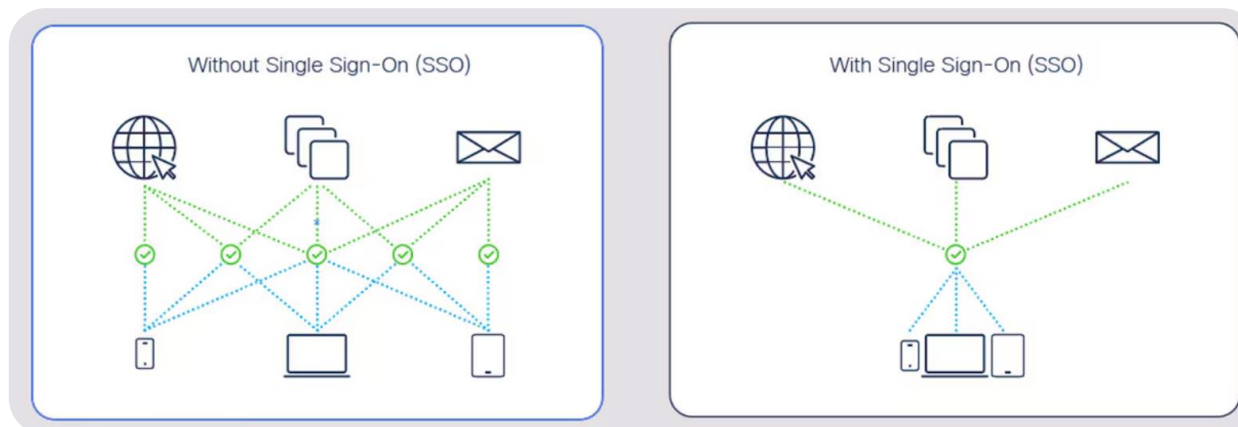
How does SSO work?

- 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.



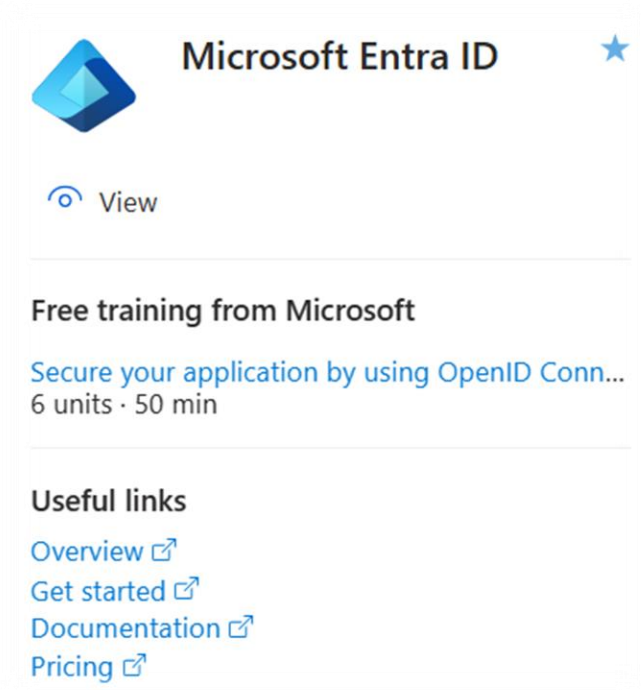
What are the benefits of SSO?

- 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.



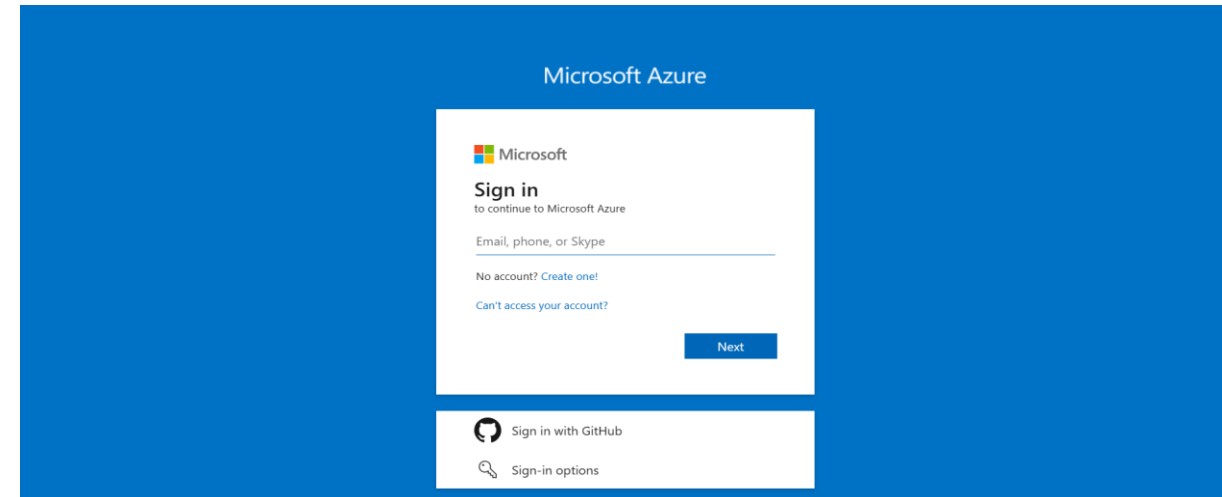
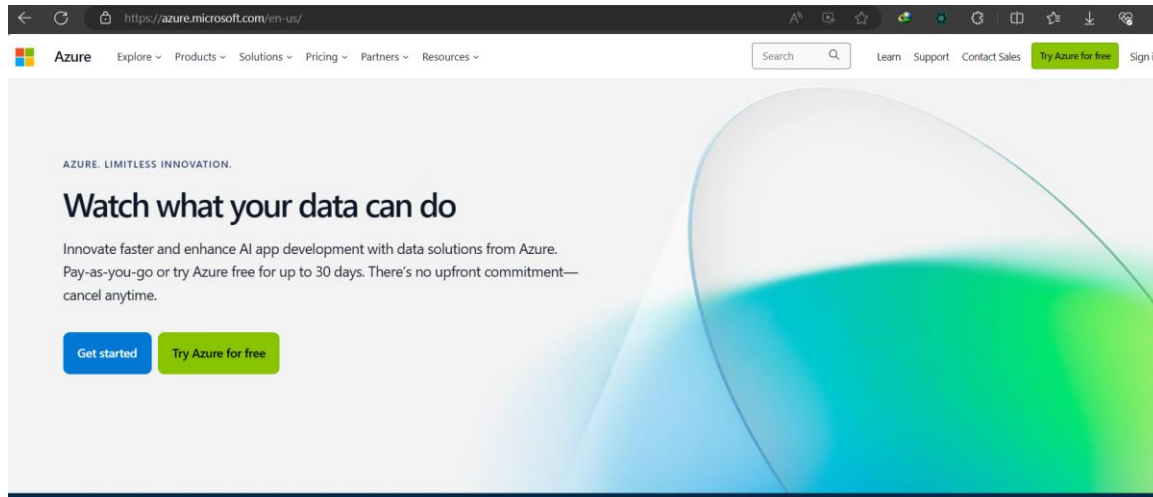
What is Microsoft Entra ID?

- 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.

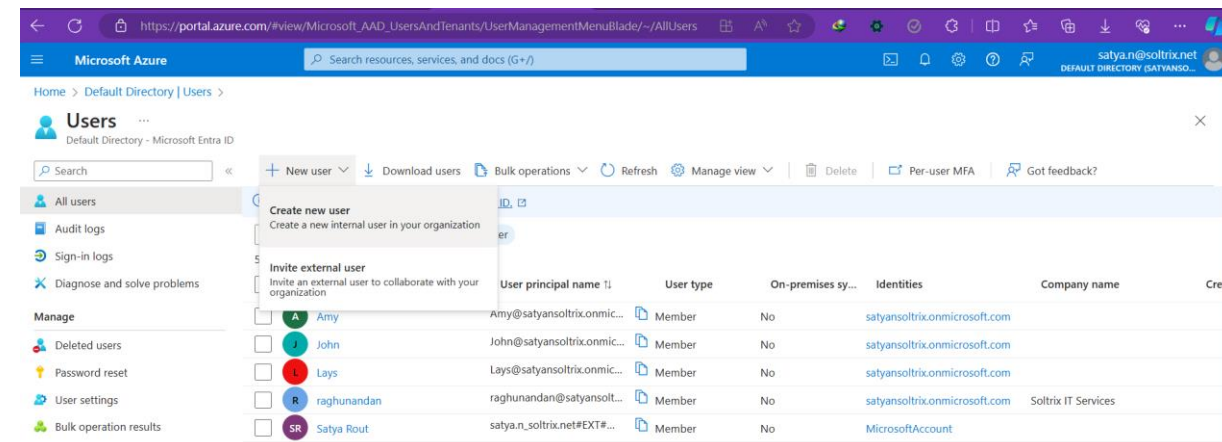


Pre-requisites for Azure SSO integration with ServiceNow

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



- Create users in Azure Entra ID.



- 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.

The screenshot shows the ServiceNow user management interface. On the left is a dark sidebar with a search bar and a list of navigation items: Self-Service, Business Applications, Dashboards, Service Catalog, Employee Center, Knowledge, Visual Task Boards, Incidents, Watched Incidents, My Requests, Requested Items, Watched Requested Items, My Connected Apps, and My Profile. The main area is titled 'User' and contains a form for editing the user 'Azure_admin'. The form includes fields for User ID, First name, Last name, Title, and Department. Below these are checkboxes for 'Password needs reset', 'Locked out', 'Active' (checked), 'Web service access only', and 'Internal Integration User' (checked). To the right of the form are fields for Email, Language (set to '-- None --'), Calendar integration (set to 'Outlook'), Time zone (set to 'System (America/Los Angeles)'), Date format (set to 'System (yyyy-MM-dd)'), Business phone, and Mobile phone. A 'Photo' field with a 'Click to add...' link is also present. At the top right, there's a header with 'Application scope: Global' and a red 'Update set: Default (Global)' button. At the bottom of the form are 'Update', 'Set Password', and 'Delete' buttons.

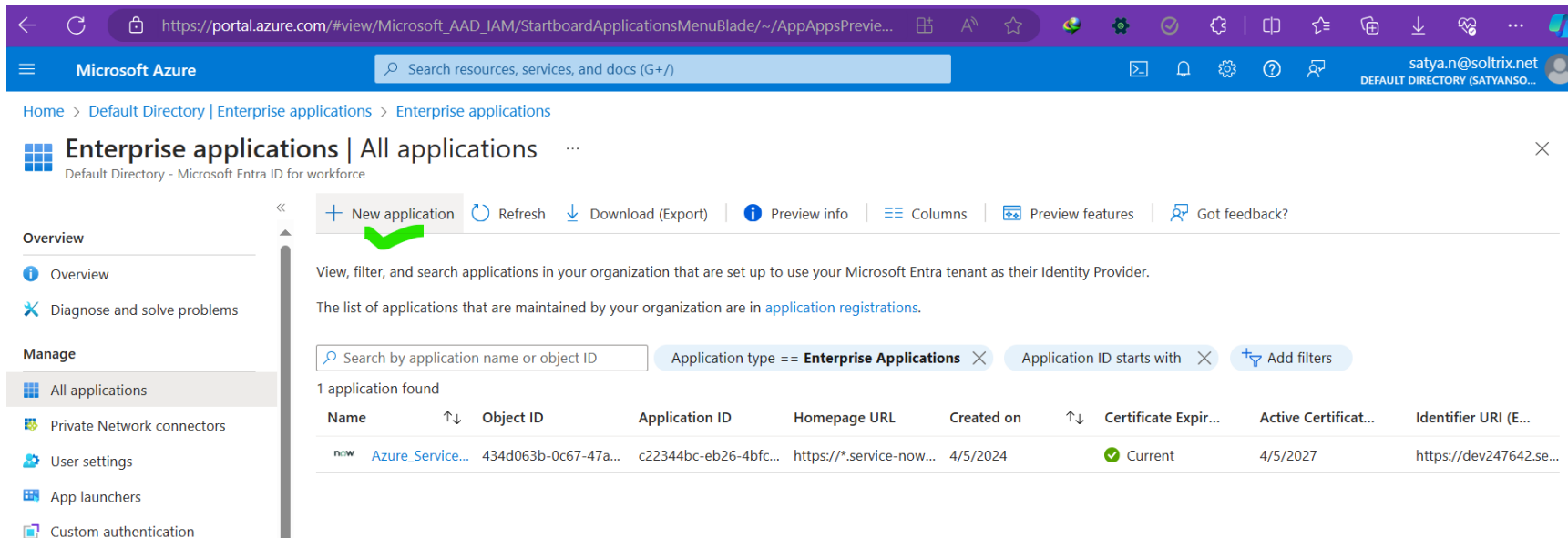
- **Activate the plugin for SSO on ServiceNow:**

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

The screenshot displays the ServiceNow user interface. At the top, the 'servicenow' logo is on the left, and navigation links for 'All', 'Favorites', 'History', and 'Workspaces' are in the center. A search bar on the right contains the text 'Search'. Below the navigation bar, the 'Applications' tab is selected. The main content area shows a search bar with the query 'com.snc.integration.sso.multi.installer'. Below the search bar, it states '1 results for "com.snc.integration.sso.multi.installer"'. The search results list a single item: 'Integration - Multiple Provider Single Sign-On Installer' with the subtitle 'Single Sign-on (SSO)'. The description reads: 'The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML or OpenID connect(OIDC). It also supports authentication using multiple digest configurations.' To the right of the description is an 'Install' button. Below the description, the ID 'Id: com.snc.integration.sso.multi.installer' is listed, followed by 'Free' and 'by ServiceNow'. On the left side of the interface, there are filter sections: 'Listing type' with options 'Applications' and 'ServiceNow Products'; 'Obtained' with options 'Installed', 'Not Installed', 'Updates', 'Customized', and 'Installation Scheduled'; 'Price' with options 'Free' and 'Paid'; and 'License Status' with options 'Subscription not required' and 'Subscribed'.

Implementation Steps at Azure Entra ID:

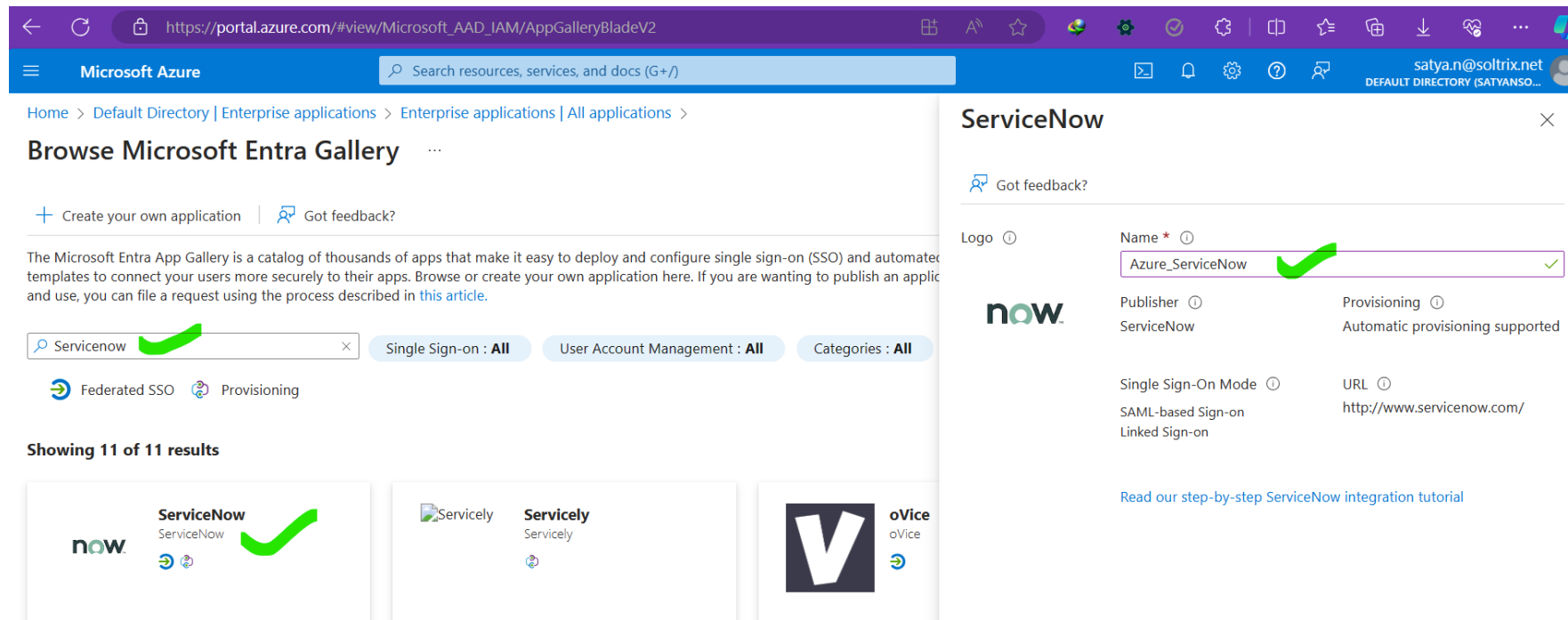
- Login to Azure portal and search for Enterprise application under Azure services: **Azure Entra ID>Enterprise application>Click on “New Application”**.



The screenshot displays the Azure portal interface for managing Enterprise applications. The breadcrumb navigation shows 'Home > Default Directory | Enterprise applications > Enterprise applications'. The page title is 'Enterprise applications | All applications'. The left sidebar contains sections for 'Overview' (Overview, Diagnose and solve problems) and 'Manage' (All applications, Private Network connectors, User settings, App launchers, Custom authentication). The main content area includes a '+ New application' button with a green checkmark, a 'Refresh' button, and a 'Download (Export)' button. Below these are filters for 'Application type == Enterprise Applications' and 'Application ID starts with'. A table lists the applications, with one application 'Azure_Service...' shown. The table columns are Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiration, Active Certificate, and Identifier URI (E...).

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiration	Active Certificate	Identifier URI (E...
Azure_Service...	434d063b-0c67-47a...	c22344bc-eb26-4bfc...	https://*.service-now...	4/5/2024	Current	4/5/2027	https://dev247642.se...

- 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.



The screenshot displays the Microsoft Azure portal interface. The main heading is "Browse Microsoft Entra Gallery". A search bar contains the text "ServiceNow". Below the search bar, there are filters for "Single Sign-on : All", "User Account Management : All", and "Categories : All". The results section shows "Showing 11 of 11 results". The first result is the ServiceNow application, which is highlighted with a green checkmark. A popup window for the ServiceNow application is open, showing the "Name" field set to "Azure_ServiceNow" with a green checkmark. Other fields visible in the popup include "Publisher" (ServiceNow), "Provisioning" (Automatic provisioning supported), "Single Sign-On Mode" (SAML-based Sign-on), and "URL" (http://www.servicenow.com/). A link to "Read our step-by-step ServiceNow integration tutorial" is also present.

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

Home > Default Directory | Enterprise applications > Enterprise applications

Enterprise applications | All applications

Default Directory - Microsoft Entra ID for workforce

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Private Network connectors
- User settings
- App launchers

« + New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

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

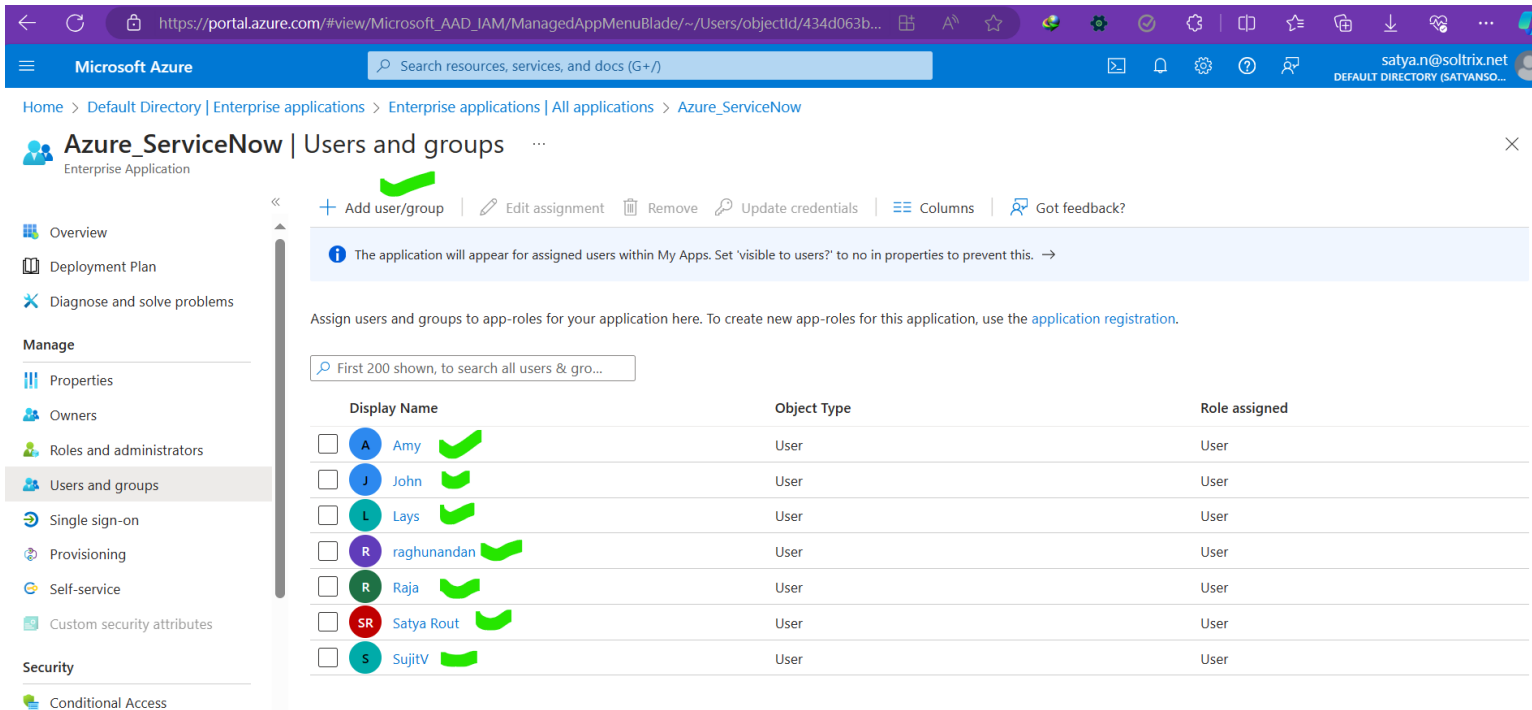
The list of applications that are maintained by your organization are in [application registrations](#).

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

1 application found

Name	↑↓	Object ID	Application ID	Homepage URL	Created on	↑↓	Certificate Expir...	Active Certificat...	Identifier URI (E...
now ServiceNow		15c733ae-bf57-41db...	4ced012d-efd3-437e...	https://*.service-now...	4/4/2024		-	-	4ced012d-efd3-437e...

- 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**.



Microsoft Azure

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Azure_ServiceNow

Azure_ServiceNow | Users and groups

Enterprise Application

+ Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

✓

i 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](#).

First 200 shown, to search all users & gro...

	Display Name	Object Type	Role assigned
<input type="checkbox"/>	A Amy ✓	User	User
<input type="checkbox"/>	J John ✓	User	User
<input type="checkbox"/>	L Lays ✓	User	User
<input type="checkbox"/>	R raghunandan ✓	User	User
<input type="checkbox"/>	R Raja ✓	User	User
<input type="checkbox"/>	SR Satya Rout ✓	User	User
<input type="checkbox"/>	S SujitV ✓	User	User

Manage

- Overview
- Deployment Plan
- Diagnose and solve problems
- Users and groups**
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes
- Security
- Conditional Access

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.**

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar shows 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb trail indicates the path: 'Home > Default Directory | Enterprise applications > Enterprise applications | All applications >'. The main content area is titled 'Azure_ServiceNow | Overview' and shows the application's properties and getting started steps.

Properties

Property	Value
Name	Azure_ServiceNow
Application ID	c22344bc-eb26-4bfc-b3cc-...
Object ID	434d063b-0c67-47a2-a0e6-...

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 Microsoft Entra credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)

- 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**”.

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar shows 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb trail reads: 'Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Azure_ServiceNow'. The main heading is 'Azure_ServiceNow | SAML-based Sign-on', with a subheading 'Enterprise Application'. On the left, a sidebar menu lists various options: 'Overview', 'Deployment Plan', 'Diagnose and solve problems', 'Manage' (with sub-items: 'Properties', 'Owners', 'Roles and administrators', 'Users and groups'), 'Single sign-on' (highlighted), 'Provisioning', and 'Self-service'. The main content area is titled 'Set up Single Sign-On with SAML' and includes a description of SSO implementation. Below this, there's a section for 'Basic SAML Configuration' with a table of fields and values. The fields are: Identifier (Entity ID), Reply URL (Assertion Consumer Service URL), Sign on URL, Relay State (Optional), and Logout Url (Optional). The values are: https://dev247642.service-now.com, https://dev247642.service-now.com/navpage.do, https://dev247642.service-now.com/navpage.do, Optional, and Optional. There are green checkmarks next to the first three fields, indicating they are correctly configured. An 'Edit' link is visible next to the configuration box.


Basic SAML Configuration	
Identifier (Entity ID)	https://dev247642.service-now.com
Reply URL (Assertion Consumer Service URL)	https://dev247642.service-now.com/navpage.do
Sign on URL	https://dev247642.service-now.com/navpage.do
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

- **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.

Attributes & Claims 

givenname

surname

emailaddress

name

Unique User Identifier



user.givenname

user.surname

user.mail

user.userprincipalname

user.mail

 Edit 


Attributes & Claims ...

+ Add new claim



+ Add a group claim

≡ Columns

|

 Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID) 	SAML	user.mail [nameid-forma... *** 

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

✓ Advanced settings

- 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.

Set up Azure_ServiceNow

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

https://login.microsoftonline.com/e705cb72-bcdc...

Microsoft Entra Identifier

https://sts.windows.net/e705cb72-bcdc-4901-8da...

Logout URL

https://login.microsoftonline.com/e705cb72-bcdc...

View step-by-step instructions

Configure sign-on

Automatically Configure ServiceNow

Microsoft Entra ID can automatically configure ServiceNow for single sign-on. Simply provide the information below and click "Configure Now".

ServiceNow Instance Name *

dev247642

Admin Username *

Admin Password *

☒ Make this the default identity provider for ServiceNow

Configure Now

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

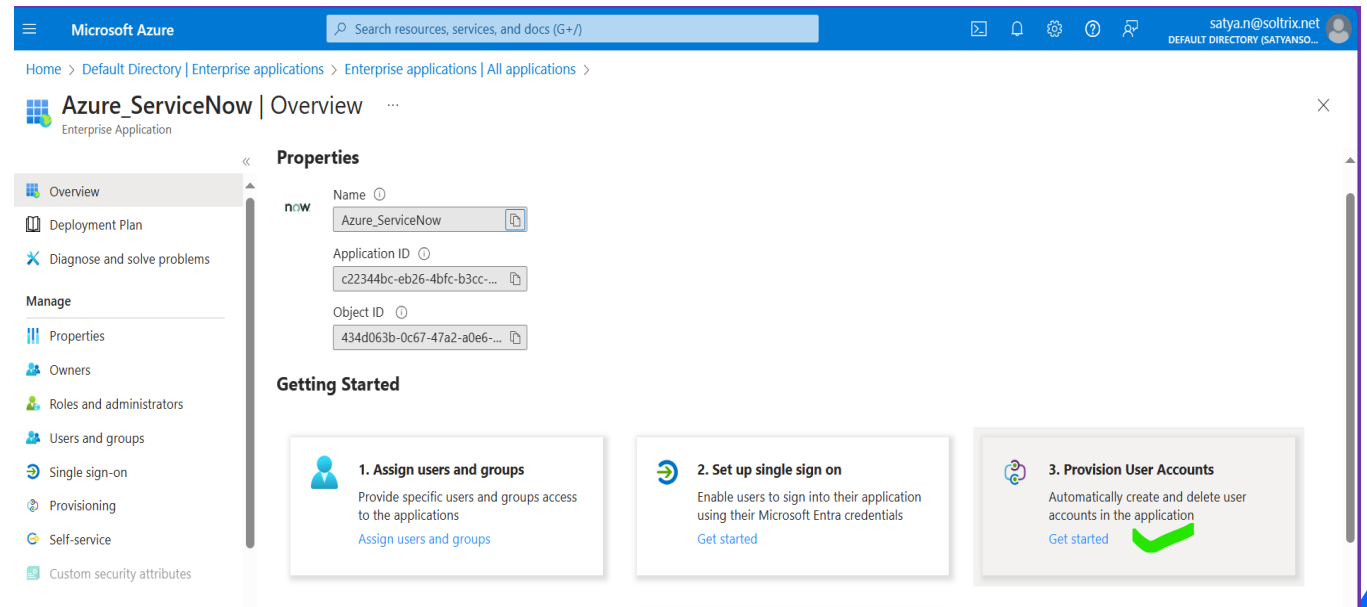
The screenshot shows the ServiceNow web interface for managing Identity Providers. The left sidebar contains navigation links for 'Multi-Provider SSO' and 'Administration'. The main content area displays a table of Identity Providers. The 'Microsoft Azure Federated Single Sign-on...' entry is highlighted with a green box, indicating it is the active or newly created provider.

Name	Active	External logout redirect	Single Sign-On Script	Default	Auto Redirect IdP
Auth0	false	external_logout_complete.do	MultiSSO_OIDC_custom	false	false
Azure AD	false	external_logout_complete.do	MultiSSO_OIDC_custom	false	false
Digested Token	false	external_logout_complete.do	MultiSSO_DigestedToken	false	false
Google	false	external_logout_complete.do	MultiSSO_OIDC_custom	false	false
Microsoft Azure Federated Single Sign-on...	true	external_logout_complete.do	MultiSSOv2_SAML2_custom	true	true
OIDC_Facebook	false	external_logout_complete.do	MultiSSO_OIDC_custom_facebook	false	false
OKTA	false	external_logout_complete.do	MultiSSO_OIDC_custom	false	false
SAML2 Update1	false	external_logout_complete.do	MultiSSOv2_SAML2_custom	false	false

• 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.



- **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.

The screenshot displays the Microsoft Azure portal interface for the 'Azure_ServiceNow | Provisioning' page. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for 'satya.n@soltrix.net'. The breadcrumb trail shows the path: Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Azure_ServiceNow | Provisioning >.

The main heading is 'Azure_ServiceNow | Overview'. Below this, a toolbar contains several actions: 'Start provisioning' (highlighted with a green checkmark), 'Stop provisioning', 'Restart provisioning', 'Edit provisioning', 'Provision on demand', 'Refresh', and 'Got feedback?'. A left sidebar lists navigation options under 'Manage' (Overview, Provision on demand) and 'Monitor' (Provisioning logs, Audit logs, Insights).

The 'Current cycle status' section indicates 'Incremental cycle completed.' with a progress bar at '100% complete'. It also shows '7 Users' with a green checkmark and a link to 'View provisioning logs'.

The 'Statistics to date' section includes expandable details: 'View provisioning details' (expanded) showing 'Completed: 4/5/2024, 5:15:14 PM', 'Duration: 3.822 seconds', 'Steady state achieved: 4/5/2024, 5:15:14 PM', and 'Provisioning interval(fixed): 40 minutes'; and 'View technical information' (collapsed).

- **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.

More Details.' There are three checked checkboxes: 'Enable multiple provider SSO', 'Enable Auto Importing of users from all identity providers into the user table', and 'Enable debug logging for the multiple provider SSO integration'. Below these is a text field for 'The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field.' with the value 'email' entered. A 'Save' button is at the bottom left."/>

Multiple Provider SSO Properties Save

Customization Properties for Multiple Provider SSO

It is recommended to enable SSO account recovery (ACR). Please refer to the documentation for [More Details](#).

☒ Enable multiple provider SSO ⓘ

☒ Enable Auto Importing of users from all identity providers into the user table ⓘ

☒ Enable debug logging for the multiple provider SSO integration ⓘ

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

Save

- 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.

- 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.

servicenow

All

SSO

Favorites

No Results

ALL RESULTS

Multi-Provider SSO

Getting Started

Identity Providers

Federations

Administration

Properties

x509 Certificate

Installation Exits

Single Sign-On Scripts

Favorites

History

Admin

Identity Provider - Microsoft Azure F...

Application scope: Global
Update set: Default [Global]

Identity Provider

Microsoft Azure Federated Single Sign-on for Default Directory

Update

Generate Metadata

Test Connection

Deactivate

Failed Requirement Redirect

https://login.microsoftonline.com/e705cb72-bcdc-4901-8da3-525f44b9fea9/saml2

Encryption And Signing

User Provisioning

Advanced

Auto Provisioning User

Update User Record Upon Each Login

Update

Generate Metadata

Test Connection

Deactivate

Related Links

[User Provisioning Transform Map](#)

[Unset Auto Redirect IdP](#)

ServiceNow - Personal - Microsoft Edge

https://dev247642.service-now.com/saml_test_conn_completed.do?sysparm_nostack=true&sysparm_...

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.

Thank you!!!