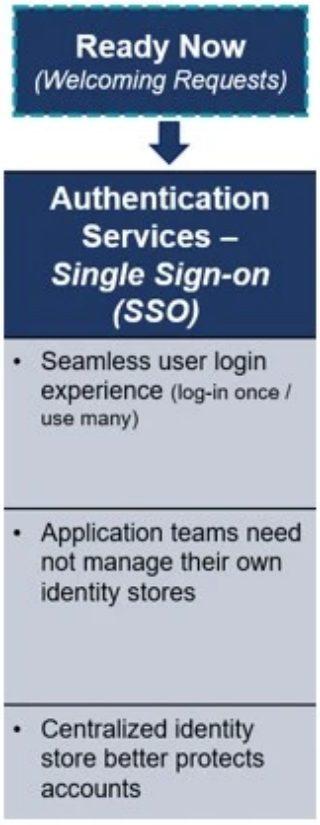
Service: Single Sign-on (SSO)

Morgan, Elena
Engineering Program Manager II IS

Responsible Team: Authentication Services



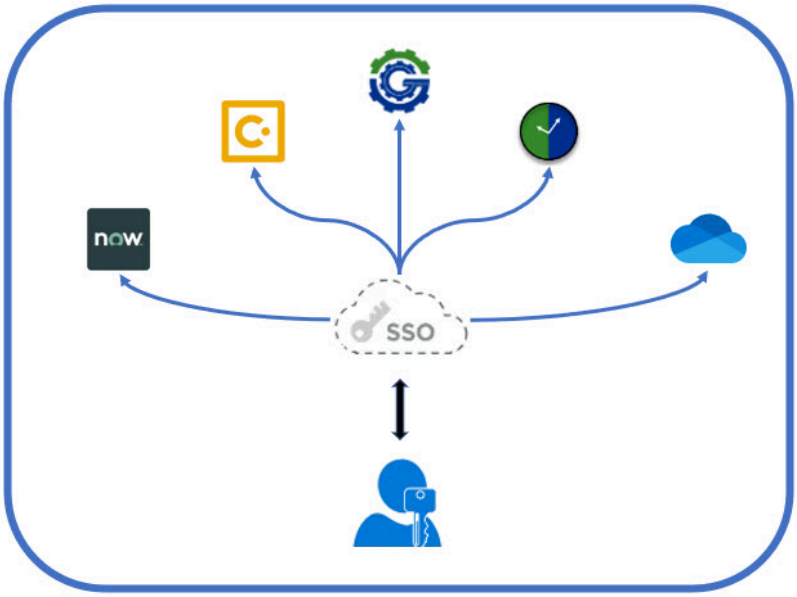
Benefits of SSO Onboarding

Single Sign-On (SSO): Login once with your username and

password to access many applications

Overview:

Single sign-on (SSO), is an authentication method that allows a user to access multiple applications with one set of login credentials. This means that once you've logged in with your username and password, you don't have to login repeatedly for every single application.



- Video explaining SSO
- Real World Use Case: Logging into a Google service such as Gmail, enables you to automatically authenticate to other Google applications such as: Google Docs, YouTube, Google Calendar.

Business Value:

- Increased Productivity
- Improved Security
- Reduced IT Costs
- Enhanced Caregiver Experience
- Improved Job Satisfaction for Caregivers

Application Eligibility:

Your application must support one of the following SSO technologies.

- SAML 2.0
- OpenID Connect (OIDC)
- WS-Fed

OAUTH 2.0 (OAuth 2.0 is used in conjunction with SAML or OIDC to provide authentication and authorization for web-based applications and APIs).

Vendor Applications: If the application is a third-party/vendor provided application, then you may need to contact the vendor to determine SSO eligibility. Here's a list of SSO eligibility questions that you can ask the vendor.

Future Offering: We are researching solutions to enable SSO for legacy on-premises applications and will share more information on this offering when available.

Process to Onboard Your Application:

Once you have determined your application is eligibility for SSO, you can follow the steps below to start the onboarding process:
You can also reference the SSO Configuration Guide for more detailed instructions.

Prerequisites:
Information we will need to know about your application:

1. APM Number (to request a new APM # : IS Knowledge Base - PSJH - Service Now APM - How to Request a New Business Application CI (service-now.com))
2. MetaData Information:
    a. Identifier (Entity ID)
    b. Reply URL (Assertion URL), Example: https://sampleapp.com
    c. For SAML Integrations: SAML Metadata File
    Metadata files may need to be obtained from the vendor.
    d. Attributes.
3. User Access Group(s) for your application. These are typically Azure Active Directory (AAD) groups.
    To request new access group(s) for your application,
    please submit an IS to EIS Security Operations Triage Request. This may take up to 10 business days to complete.
    You will need to provide the following information for the request:
    - Proposed name of the group(s) (should include application name and the needed role permission - read/write, read only, user, admin, etc.). Security Operations may ask you questions before finalizing the group name.
    - Application owner name, email address, and User Principal Name (UPN)*
    - Application usernames, email addresses, and UPNs*
    * If you need assistance finding UPN's call Service Desk at (844) 92 AskIT / (844) 922 7548.

Submit a request for SSO

1. Start the request by completing an IAM Request Intake Form
2. Select the option “I need Azure Single Sign-on for my application” under question 7.

Onboarding Process
Once the SSO request has been submitted. We will follow-up with you within 2 business days to review the request and ask for additional information.

You will need to provide the Business Application Configuration (CI) name and associated APM number for your application. This information can be found in the Configuration Management Database (CMDB).

1. Use the APM Inventory PowerBI Dashboard to find your Business Application Configuration (CI) name and associated APM number.
2. If you need to have a Business Application Configuration (CI) name and APM number created, use the Lifecycle Services Portal for guidance on how to have one created for your application.

The SSO onboarding process can usually be completed within 2 weeks for most requests once we have the required application information.

FAQs

See all

Question	Answer	Service
Have a question - need to contact us?	Join our MS Teams channel and post your question (Team Title: 'RAO Questions') https://teams.microsoft vYMkrGVQTfTr-VySnu1tXkYwdIYGk1%4 groupId=9b0f57f5-1c34-47bb-9666-0254e42c5296&tenantI 9a26-46a3-865f-615bed576786	SSO RAO IALM PAM PKI EPV EPM
What is SSO and why do we need it?	SSO or Single sign-on is an identification method that enables users to log in to multiple applications and websites with one set of credentials.	SSO

Will my application need MFA once it is SSO enabled?		Not necessarily, it will depend on where the CG is logging in from. MFA is controlled by Conditional Access. Depending on where the application is accessed from (such as from overseas unapproved countries), MFA may or may not be required. If accessing from an unapproved location – MFA is required, whether app is or is not configured for SSO.	SSO
Do I need to do an APP reg if I want my App on SSO?		No. No separate request for App Reg is required. App Reg is tied into our Tenant (Azure). App Reg and an Enterprise App are both part of it. For an App Reg with API permissions, we manage the permissions, secret, etc. through the app registration, and manage the MyApp settings with the Enterprise app. SAML is added through the enterprise app… section, and	

If an App is in Citrix, does SSO need to be set up for it?

Citrix is an App, a Workspace, we do not manage so an application being in Citrix does not mean it is on SSO. Citrix team manages those apps.

Who can access the app?

To access your app, an AAD groups needs to be created, done by