Integrating with NYU Single Sign-On

Contents
1. Background Information
2. Overall Process and Responsibilities

Background Information

NYU Information Technology (NYU IT) offers the NYU Login (SSO) service to support centralized NetID/password authentication and single sign-on (SSO) to web applications.

The NYU Login (SSO) service uses Shibboleth as its central software component. The overall NYU Login SSO environment is characterized by central infrastructure servers operated by NYU IT’s Identity Services group (called the Identity Provider, or IdP) with which multiple web applications (each called a Service Provider, or SP) are integrated at a technical level.

Note: In this document we shall refer to the IdP-Team (NYU IT staff managing NYU’s central IdP infrastructure) and the SP-Team (staff responsible for implementing SSO capabilities at the application end). The IdP-Team can be reached via email at idm.services@nyu.edu. Review the Project to Service Transition Checklist and Style Guide for guidance and requirements regarding Service Naming and User Interface.

An SP is a web-based application that uses the centrally-managed SSO infrastructure (the IdP) for NetID/password authentication. SSO integration is the process we follow at NYU to configure an SP to participate in the overall NYU Login (SSO) environment.

There are two approaches for implementing NYU Web SSO:
- SAML-based integrations (Beginning in the Fall of 2017, NYU introduced Multi-Factor Authentication for most services that use NYU SAML-based Single Sign-On.)
- OpenID Connect/OAuth2 integrations

SAML-based integrations use the industry-standard SAML protocol for integration between central identity provider servers and application servers.

For each SAML/application integration, configuration must be performed both on the SP side and correspondingly on the central IdP side.
NYU Login (SSO) Environment (showing NYU's IdP and sample integrated SPs)

The SAML/Shibboleth Integration Guide provides basic information for service provider (SP) integration with NYU's central Single Sign-On identity provider (IdP).

An alternative to SAML/Shibboleth is OpenID Connect for web and non-web applications. OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol that can be used for both authentication and authorization.

OAuth 2.0 (also known as OAuth2) provides a quick and easy way to have an application authenticate users with their NYU NetID without having to install any client software in your application. The process is simply handled via a short series of HTTP GET and POST methods once you register your application with the NYU IT Identity Services team.

The OIDC Integration Guide provides basic information for our OAuth 2.0 implementation for authentication.

Prior to implementation work, any questions about these specifications must be discussed and all needed information shared by technical contacts for the SP and the IdP.

For each SSO integration, NYU requires joint acceptance of an "Operational Level Agreement (OLA)" that conveys in detail the responsibilities of responsible staff members for the SP and IdP, and identifies specific individuals to be contacted for technical and administrative issues. For an SP operated by an external vendor, a sponsoring NYU department will likely sign the OLA.

**Overall Process and Responsibilities**

The overall process for SSO integration should follow these steps:

1. Submit application information questionnaire to idm.services@nyu.edu
   - If doing SAML integration, submit SAML integration questionnaire
   - If doing OpenID Connect (OIDC) integration, submit OIDC integration questionnaire
2. Project coordination call (as needed) to review questionnaire
3. Technical coordination call (as needed) to review integration details; required participants:
   - NYU IT Service Coordinator for identity services
   - SP technical implementer
   - NYU IT technical implementer
4. If doing SAML integration:
   A. Exchange necessary SAML metadata describing SP and IdP
   B. Configure SP and IdP development environments; test functionality
5. If doing OpenID Connect (OIDC) integration:
   A. We will provide OIDC credentials (we can provide credentials for both QA and Prod)
   B. Configure SP development environment with OIDC credential; test functionality
6. Plan go-live in production
   A. If doing SAML integration
      a. Exchange production SAML metadata
      b. Schedule configuration of IdP to support production SP
      c. Schedule go-live for production SP
   B. If doing OpenID Connect integration
      a. Follow the same procedure used in QA but use the production OIDC credential
7. Go-Live! (See Go-Live Checklist in SAML integration guide, page 6)
8. E-sign OLA via NYU Google Docs to idm.services@nyu.edu

While each SSO integration is unique, generally the SSO integration process will require 6-12 weeks from initial planning, through integration configuration and testing, to eventual production go-live.

For each integration project, the IdP-Team is responsible for configuration of the central IdP, adding in some standardized SAML metadata describing the specific SP and any user attributes that are to be transmitted to the SP at end-user login time. All general communications relating to the integration should be sent to the team's email address, idm.services@nyu.edu.

Most of the integration work for an SSO integration needs to take place at the SP end. Staff responsible for the SP are responsible for all changes to the SP in order for it to use the central IdP for authentication purposes. Since the required steps can vary substantially from application to application, the central identity services team can only provide general advice on SP configuration.