NeSIS Federation FAQs

What are the benefits of federating the student information system?

Federation allows users to use the set of credentials most familiar with them. Campuses have their own set of credentials to access other services on campus (i.e. CANVAS, Library, Parking). With federation, users will be able to use those local campus credentials to authenticate into the student information system. Other benefits include:

- Presenting a similar user experience during authentication which ensures a familiar and secure user experience. You will use the same user interface to authenticate to all federated applications.
- The student information system will leverage security mechanisms from campus authentication processes, which minimizes the risk of having your information breached.
- Two factor authentication (2FA) processes will align with other applications on the campuses. If you are required to use 2FA, the user experience will be similar and the rules to prompt for 2FA will be consistent.
- Single sign on capabilities will be enabled to minimize the number of times users have to authenticate into multiple applications on your campus.

What changes will I see from federating the student information system?

A few changes have come along with the student information system federation project:

- Logging in: When you access the student information system, you will notice a different login screen with options for using either your TrueYou ID (NUID) or your campus NetID, so you only have to remember one username and password.
- Duo Two factor authentication: If you are a current Duo user for two factor authentication (2FA) into systems such as Firefly or Box, the student information system is another system that is protected by Duo 2FA. If you see a prompt for Duo 2FA after you log in, simply follow the same steps you’ve been following for other systems.
- Single sign-on (SSO) – Federation will provide the benefit of single sign-on to other federated applications depending on the ID you used to log in. Once signed in with an ID, simply open another tab in your browser and navigate to a site that is federated and SSO, you will not be asked to log in again.
  - If you log in with your TrueYou ID (NUID) – You can access Firefly without re-authentication.
  - If you log in with your campus Net ID – You can access XXX without re-authentication.

Why am I required to use Duo two-factor authentication now for systems that I wasn’t previously required to use it for?

If you are a current Duo user for two factor authentication (2FA) into systems such as Firefly or Box, the student information system is another system that is protected by Duo 2FA. If you see a prompt for Duo 2FA after you log in, simply follow the same steps you’ve been following for other systems.

What all systems are federated and/or have single sign-on on my campus?

Single Sign-On FAQs

What is Single Sign-On?

Single sign-on (SSO) allows a user who is already authenticated (logged in) to a participating service or website to seamlessly transition to another without requiring a second login.
**What is a Single Sign-On system?**
Single sign-on (SSO) systems are a dedicated Identity System intended for exclusively managing secure user authentication and passing user login session assertions to integrated services, instead of having each service manage their own authentication. The University of Nebraska has chosen to implement this functionality with a technology standard called SAML 2.0 in a product called Shibboleth.

**Single Sign On - Tool: Shibboleth**
A user will interact with services and systems numerous times a day when conducting their duties, and having to re-authenticate over and over can become cumbersome. Connecting a service up to Single Sign On (SSO) infrastructure allows that service to pass all user authentication over to a system that exclusively manages user authentications, and then securely passes that sign-in assertion back to the service when a user logs in. The SSO system maintains the user’s authentication session which can then be called back when the user needs to log in to a new service (that is connected to the Single Sign On system). Depending on configuration preferences, a user could stay signed in for the entire day (or longer) for services to receive authentication assertions at sign in. The more services that are integrated with Single Sign On, the fewer times a user will need to log in throughout their day.

**What Do Single Sign On and Duo Changes Mean for ME?**
Over the course of your experiences at the University of Nebraska, there have been any number of services that you log into to get whatever you need, and sometimes you've had to have a username and password for each of these services. That means you had to remember what each password and username was and which one you used and where. In short, it is all very confusing to try to remember!

Our plan is to simplify that for you; we want you to only have to remember ONE username and password. Single Sign On means that when you log into your email in the morning, and then switch over to FireFly, or Canvas, or Box, or SharePoint, or whatever, the next service will trust that you are logged in as you. This new format requires that each of these services are integrated with our Single Sign On (SSO) systems. Services put their trust in the SSO which will pass the login session for you as you go from service to service so you don't have to keep logging in, and when you do log in, it is just your one account, one password.

Duo changes mean that you might start seeing two factor prompts when logging into some services when you had not previously. This is due to how we are protecting all of our Single Sign On systems with two factor, and while users enroll to use Duo for some services like FireFly/SAP, they haven't necessarily elected to use it for things like VOIP or Canvas. As we are consolidating all of our systems, we are also making our Duo system more efficient by moving all campus Duos into one single system.

Moving to this structure means that things could be different when you log in; you might see a new screen or you might see a new prompt for your username. As we work to make our systems better and more efficient, you could see new prompts for Duo two factor protection where you might not have previously. Please know we appreciate your patience and understanding as we work through this process to improve your experience at the University of Nebraska.

**Two factor authentication / Duo FAQs**

**What is TwoFactor Authentication (2FA)?**
TwoFactor authentication (2FA) is a method of confirming your claimed identity by granting access to a system or website only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. One factor is your correct username and password and the other factor is approving a request sent to a device that you have previously registered.

**Two Factor Authentication (MultiFactor) - Tool: Duo**
Two factor authentication (2FA) adds a second layer of security to your online accounts. Two Factor Authentication is an extra step in logging into a website or service, in which after you put in your username and password, you receive a notification on your phone or other device to “approve” the login attempt. You then approve this notification to complete the sign in process, or deny the notification if you weren’t the one trying to sign in. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password. With Duo Two Factor Authentication, you know you’re the only one accessing your account.

What is the future for Identity Management initiatives such as federation, single sign-on, two factor authentication, etc? How do all of these initiatives work together to protect my information?

More information about the roadmap for identity management initiatives can be found in this presentation.