RESEARCHNEWS
Washington University in St.Louis

National Institutes of Health (NIH) - Adjusted Approach and Timing to Transition eRA Commons Accounts to Use Two-Factor Authentication

This is a follow up to the previous NIH Office of Extramural Research guidance. The NIH would like to remind you eRA Commons needs you to use two-factor authentication [also known as multi-factor authentication] to make your eRA account more secure.

Instead of requiring all users to transition to Login.gov by September 15, 2021, eRA will begin a phased approach for enforcing the two-factor authentication requirement. This phased approach will apply to everyone. All scientific account holders should take action now, while administrative account holders will be required to move to two-factor authentication in early 2022.

Although the NIH now has two ways you can comply with the two-factor authentication requirement – Login.gov and InCommon Federated – we do not use InCommon Federated at WashU. You must use Login.gov.

- **Use Login.gov**
  - Use of Login.gov also has the advantage of allowing users to sign into various government agency systems with a single set of credentials. You can use your Login.gov credentials to access Grants.gov, the System for Award Management (sam.gov), MyNCBI (see login tips), SciENcv, MyBibliography and other Federal systems.
  - It is a simple, one-time, three-step process to associate your eRA account with your Login.gov account. Go to the eRA Commons home screen, click on LOGIN.GOV, and follow the on-screen prompts (This cheat sheet provides detailed steps and screenshots so you can see how easy it really is!).

New Timeline
Starting on September 15, 2021, eRA will begin a phased approach for requiring the use of two-factor authentication.

For users who only have a scientific account:

- Users who have a scientific account should start using two-factor authentication now to access eRA systems before they are required to transition. Starting September 15, 2021, the requirement to transition will be enforced on a rolling basis as follows:
  - All PIs and key personnel associated with an application or Research Performance Progress Report (RPPR) will be required to transition to the use of two-factor authentication 45 days after the submission of their competing grant application (Type 1 or Type 2) or their RPPR. After 45 days, you will not be able to access eRA Commons until you set up and use a two-factor authentication service, Login.gov.

For users who only have one or more administrative accounts:

- The NIH is exempting administrative account holders from the requirement to use two-factor authentication until early 2022, when eRA will implement support for users with multiple accounts.

The NIH encourages administrations with only a single administrative account (signing official, administrative official, etc.) to start using Login.gov, for two-factor authentication, now to access eRA systems.

Administrators with multiple eRA administrative accounts should not yet transition their accounts.

For users with both a scientific and administrative account:

- Users with both a scientific account and an administrative account (for instance, principal investigator and signing official) should start using two-factor authentication for their scientific account now.
- Wait to switch your administrative account as eRA is working on a solution that will support users with multiple eRA accounts that should be available in early 2022.
- If you have already transitioned your administrative account to use two-factor authentication, but not your scientific account, you should request the eRA Service Desk remove the two-factor authentication account association from your eRA administrative account and have it added to your eRA scientific account. This should be done before your scientific account is required to transition.

Exceptions to the Adjusted Timeline and Approach

For reviewers:

- The transition for reviewers (those with the IAR role) is ongoing and unchanged. Reviewers will continue to be required to use two-factor authentication as soon as they are enabled for a review meeting.

For non-NIH eRA partner agency applicants/recipients:

- The updated plan applies only to NIH applicants/recipients; while **eRA partner agency users** are encouraged to move to two-factor authentication now, they are not required to at this time (except for reviewers whose transition is ongoing; or applicants/recipients who apply to NIH or have an NIH grant).

eRA account credential maintenance will continue, at least for now, but will be much easier. Even though we are requiring the use of two-factor authentication, you will still need to maintain your eRA Commons username and password for the time being and will get reminders to renew those annually. The good news is that the NIH is moving from passwords to passphrases — a set of random words or a sentence at least 15 characters long — effective the end of 2021. A major plus of this move is you will need to change your passphrase only once a year (as opposed to the current NIH policy that passwords need to be changed every 120 days).

Additional Tips

- Make sure your Commons account is active and you know your password before you begin the process to associate your Login.gov with your Commons account. If you need to reset your eRA account password, please do this first by using the Forgot Password/Unlock Account? link on the main Commons home screen.
- To initiate the process of setting up your Login.gov to work with your eRA account, make sure to start from the eRA Commons home screen and select the Login.gov login. Do not go straight to Login.gov.

Resources

- Webpage: Two-Factor Authentication: Accessing eRA Modules via Login.gov
  For a flyer, videos, FAQs and more
- Guide Notice: NOT-OD-21-172
- Brochure: Transition Plan for Two-Factor Authentication Requirement for Accessing eRA Systems *(August 6, 2021)*

Help

If you run into issues with associating your Login.gov account with your eRA account, please contact the eRA Service Desk. You can also refer to Login.gov for additional help.