eRA-readiness-guide-step3

DISCLAIMER: Rolling out MFA requirements among eRA users spanning hundreds of organizations is a massive undertaking. As the project unfolds, details shift. This guide reflects our best interpretation of eRA's latest plan as it happens. Things may change. If you are seeing different behaviors, please let us know at help@incommon.org.

About this Guide

Readiness Assessment

1. Are my users accessing eRA via my IdP today?
2. Is my IdP ready to support eRA's MFA requirements?
3. **My IdP is ready. What do I need to know?**
4. My IdP won't be ready in time. What will happen?

Appendix

3. My IdP is ready. What do I need to know?

eRA is turning on the requirement on September 15. The following behavior will not take effect until that day.

What will my user's sign-in experience look like?

On September 15, along with turning on the MFA requirement, eRA will update its login page to include all InCommon IdPs in its "Login with Federated Account" drop down. Users who have been signing in using that option will likely continue to do so and some users who have been using their eRA Commons accounts may try to use their university credentials.

If a user chooses the "Login with Federated Account" option, they are redirected to the selected campus IdP to sign in. Assuming the authentication process completes and the user is redirected back to NIH Login SP, the table below summarizes a user's possible sign-in experience upon returning to NIH Login SP:

	User signs in with MFA	**User signs in without MFA**
User has accessed eRA using this credential before	Sign-in successful.	NIH Login SP displays "MFA-required" error message; prompt user to visit IdP's error URL page, or as an alternative to getting their campus account MFA-enabled, create a Login.gov account. Tip: What information should be on the error URL page?
User has not accessed eRA using this credential before	eRA triggers account registration/linking to prompt the user to establish a new eRA user record or link to an existing one.	Same as above.

Make sure the your IdP's Error URL page has the right information

When NIH Login cannot grant user access to requested resources due to missing requirements (e.g, MFA), NIH Login displays an error message to the user. The message will prompt the user to visit your IdP's Error URL page to get additional help. Make sure the web page at your IdP's Error URL has information connecting the user to a campus help desk that can help them through the transition.

Advise the help desk(s) to be prepared to recognize a request for help from one of their eRA users and understand that the user needs to become MFA-enabled, or perhaps needs help with using the school's MFA technology.

In addition to prompting the user to visit your Error URL page, NIH's "MFA required" error message also suggests creating a login.gov account as an alternative to getting their campus account MFA-enabled. To learn more, see:
https://era.nih.gov/register-accounts/access-era-modules-via-login-gov.htm

What is NIH/eRA telling its users about signing in using federated credentials?

eRA has posted a support article:
https://era.nih.gov/register-accounts/access-modules-with-federated-account.htm

About the eRA account registration / linking

eRA tracks all of its users with an internal user record. When a user signs in to eRA using a federated credential, eRA uses the user identifier sent in the SAML assertion to look up the internal local record linked to that identifier. If no record is found, eRA prompts the user to either create a new record or link to an existing one by logging in using one of the other available sign-in methods.

Once linked the user can use any of the linked credentials (eRA-issued credential, login.gov account, campus federated SSO credential, etc) to sign in.

Understanding eRA accounts: https://era.nih.gov/register-accounts/understanding-era-commons-accounts.htm