eRA-readiness-guide-step4

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.

4. My IdP won't be ready in time. What will happen?

Starting September 15, eRA will require all users signing in using a federated credential to sign in with MFA. When a user attempts to sign in to eRA using your campus credential, the NIH Login SP will send your IdP an authentication request with the https://refeds.org/profile/mfa AuthnContextClassRef (See: https://wiki.refeds.org/display/ASS/How+to+request+authentication+contexts). Depending on you IdP implementation, several scenarios may happen:

A. Your IdP does not support REFEDS MFA Profile. It displays a user facing error.

This scenario should not occur in a properly implemented SAML IdP. The IdP is supposed to respond directly to the requesting SP when it encounters an unknown/unsupported AuthnContext.

If your IdP displays a user-facing error message when it encounters an unsupported AuthnContext request, make sure that error message connects the user with the appropriate campus help desk who has knowledge of eRA's MFA rollout and can help the user regain access to eRA.

B. Your IdP does not support REFEDS MFA Profile. It sends the user back to NIH Login SP with an SAML error.

On receiving that SAML error, the NIH Login SP displays an error message to the user. The message prompts 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 with the appropriate campus help desk who has knowledge of eRA's MFA rollout and can help the user regain access to eRA.

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

C. Your IdP supports REFEDS MFA Profile; it displays a user-facing message for non-MFA-enabled users.

This scenario should not occur. If the use is unable to sign in with MFA, the correct REFEDS MFA Profile behavior is to for the IdP to respond to the SP with a SAML assertion illustrated in Example 1 in https://wiki.refeds.org/display/ASS/How+to+request+authentication+contexts. See D.

One exception here may be if you have the ability to guide the use through the MFA set up flow so that the user can complete MFA authentication within that transaction.

D. Your IdP supports REFEDS MFA Profile, but the user is not MFA-enabled. The IdP redirects the user's browser to the NIH Login SP with NoAuthnContext status in the SAML response.

(See: https://wiki.refeds.org/display/ASS/How+to+request+authentication+contexts)

On receiving that SAML error, the NIH Login SP displays an error message to the user. The message prompts 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 with the appropriate campus help desk who has knowledge of eRA's MFA rollout and can help the user regain access to eRA.

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