nih-ready-step-by-step

Get NIH Ready Dashboard

Step-byStep Guide To Implement NIH Requirements

Introduction

This document provides implementation guidance for InCommon Participants to meet the National Institute of Health's (NIH)'s federation access requirements.

To enable its mission, NIH is expanding its NIH Login Service gateway to facilitate secure access to NIH IT resources by biomedical researchers, faculty, and scientists around the globe. Resources protected by the NIH Login Service include controlled-access research data and grants administration systems.

InCommon participants whose users access NIH resources via federated access need to update their identity providers meet three requirements:

- **Release Basic Information** about the people accessing NIH resources so that we can provision and manage efficient and secure acces.
- **Perform Strong Multi-factor Authentication** (MFA) to minimize risk to NIH IT resources.
- **Provide Assurance** that each person who logs in is who they say they are so that NIH can provide appropriate authorization to access NIH data.

NIH's approach, being implemented in partnership with InCommon, is to gradually enforce these requirements over time and across specific NIH services, matching each requirement to the needs of each service rather than requiring all of these measures for all of their services.

You do not need to meet all 3 requirements immediately. You also only need to perform required actions such as multi-factor authentication or providing appropriate identity proofing when the user accesses a controlled resource requiring those items.

This outline summarizes a typical login flow when a federated user accesses a NIH Login Service-protected resource:

1. User visits a restricted NIH resource requiring login;
2. User is prompted to select their institution from the NIH Where Are Your From list
3. NIH signals the user-selected federated identity provider (IdP) with request for basic information, and where applicable, MFA
4. IdP performs user login, with MFA where applicable;
5. IdP sends NIH:
    a. Basic information about the user
    b. MFA assertion, if MFA occurred during user authentication
    c. Any identity assurance assertion applicable to that user
6. NIH grants access to NIH system if information sent by the IdP meets that resource's requirements.

Checking Your Campus's Readiness

NIH provides a Compliance Check Tool to help you test your campus' readiness. Sign into the NIH Security Compliance Check Tool to determine if your campus' identity provider meets these requirements.

Rollout Schedule

NIH is rolling out the requirements in two phases:

Phase I - eRA MFA Requirement Rollout

Duration: November 2020 to September 15, 2021.

Phase I lays the foundation for a new standard of federated login to NIH systems and sites, starting with the NIH Electronic Research Administration (eRA) system. Starting September 15, 2021, a user signing into eRA using federated credentials needs to authenticate with MFA. To support the requirement, federated partners need to be able to interpret and correctly respond to this signal. Further, NIH requires basic user information including persistent unique identifier, name, email, and affiliation. This basic information equates to the REFEDS Research and Scholarship Entity Category (R&S).

The eRA modules included in this rollout are: eRACommons, ASSIST, InternetAssistedReview(IAR), CommonsMobile.

To meet Phase I goals, implement:

- Requirement I: Release Basic Information
- Requirement II: Perform Strong Multi-factor Authentication (MFA)

If your organization receives NIH grants and does not yet meet these requirements, it's not too late. Researchers can return to using campus credential whenever your IdP is ready. Use the eRA Readiness Guide to update your identity provider to enable your users to sign in to eRA using your campus credential.

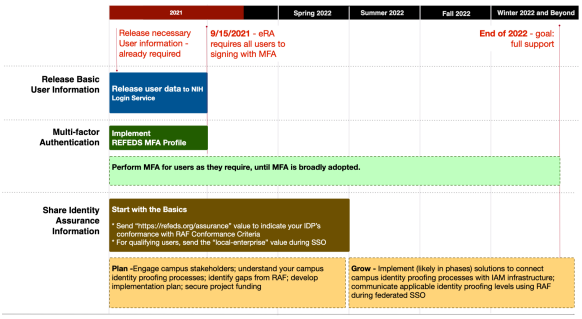
Related: NIH instruction on logging in using Federated Login

Phase II - Share Identity Assurance Level to enable user access to Controlled Access Research Data

Duration: Now to December 2022

Identity assurance is a measure of confidence that the person using a credential to login is the person to whom the credential was issued, and is in fact who they claim to be. As the NIH Login Service expands to protect additional NIH online resources, some, particularly access to sensitive controlled-access research data, will require the campus to disclose the level of identity proofing (identity assurance) in addition to performing MFA for a user signing into these sensitive resources.

Since implementing an identity assurance program can be complex and time confusing, we strongly recommend starting this effort as soon as possible. The Requirement III: Provide Assurance section in this guide offers additional details and implementation tips.



What happens if we miss a deadline?

In general, if miss a deadline, some of your users will be inconvenienced. Instead of using their campus credential to access resources, NIH is instructing them to create additional accounts (mostly via login.gov). However, they'll be able to return to using campus credentials once you finish implementation. Of course, it will be the user's choice at that point which credentials they will continue to use.

For eRA

eRA has already begun enforcing its MFA requirements. Use the eRA Readiness Guide to update your identity provider to enable your users to sign in to eRA using your campus credential. Otherwise, eRA is directing its users to create a user account at login.gov.

Related: NIH's instruction regarding transitioning to and using login.gov

For NCBI materials, including PubMed

NCBI transitioned to rely on federated credentials to grant user access to NCBI materials in June 2021. NBCI requires a federated IdP to release basic information. If an IdP does not meet that requirement NCBI is directing users to sign in with a login.gov or Google account.

Related: NBCI Insights: Important Changes to NCBI Accounts Coming in 2021

Implementation Details

Requirement I: Release Basic Information

To access NIH's controlled-access resources, NIH needs to know the identity of the signed in user. NIH requires federated identity provider to release basic user information defined in the REFEDS Research and Scholarship (R&S)entity category when a user signs into NIH resources.

What information do I release?

NIH requires identity providers to release a persistent unique user identifier, name, email, and affiliation for each user signing in to the NIH Login Service.

When do I need to do this?

You should do this now. NIH already requires these attributes. Your user will not be able to sign into any NIH resource using your campus credential until your identity provider meets this requirement.

How do I do it?

If your identity provider supports the REFEDS Research & Scholarship (R&S) Entity Category, you already meet this requirement.

If you do not yet support R&S, for best results, configure your identity provider to support the REFEDS Research & Scholarship (R&S) Entity Category. If you are unfamiliar with R&S, the R&S Explained in Plain English page provides a good introduction.

If you are unable to take the release-by-category approach, either for technical or policy reasons, you should configure your identity provider system to release the named user attributes to the NIH Login Service service provider (Entity ID: `https://federation.nih.gov/FederationGateway`).

Requirement II: Perform Strong Multi-factor Authentication (MFA)

First, NIH is asking your identity provider to recognize MFA authentication requests sent by the NIH Login Service using the syntax defined in the REFEDS MFA Profile. Whether your identity provider performs MFA or not, it expects your identity provider to respond using the same profile.

Second, if a NIH resource requires it (for example, eRA), a user accessing that service will need to login with a MFA technique consistent with the REFEDS MFA Profile.

How do I do it?

Minimum: Support signaling using the REFEDS MFA Profile

Whether your Identity Provider performs MFA or not, the first thing is to enable your identity provider system to communicate using the REFEDS MFA Profile. The REFEDS MFA Profile FAQ is an excellent place to start on that task.

If your identity provider software cannot support this profile, a “plug-in” may be available to add that capability to it. See the Consulting Services section below.

If Your User Accesses MFA-required Resources: Perform MFA

If your user access one or more NIH online resource that requires MFA (for example, eRA), You'll need to make sure that those users can login with MFA. If you have not yet implemented MFA broadly and want to find out who in your institution may need such access, the NIH RePORT tool is useful to help identify researchers who receive NIH grants.

When do I need to do this?

eRA, one of the resources already requires federated users to sign in with MFA. If your organization receives NIH grants and does not yet meet NIH's MFA requirement, use the eRA Readiness Guide to update your identity provider to enable your users to sign in to eRA using your campus credential.

Requirement III: Provide Assurance

Identity assurance is a measure of confidence that the person using a credential to login is the person to whom the credential was issued, and is in fact who they claim to be. NIH is asking Federated partners to use the REFEDS Assurance Framework (RAF) to communicate a user's identity assurance level at user sign-in time. RAF defines four identity assurance levels: low, medium, high, and local-enterprise. The first three reflect increasing rigor of identity proofing and credential management processes used, while the fourth conveys that the institution is satisfied with the level of identity assurance for its own critical internal operations, which may give relying parties sufficient confidence for their own purposes.

How do I do it?

Identity assurance exists on a spectrum of confidence levels from low to very high confidence. Not all NIH resources will require user to achieve the highest identity assurance level. Further, developing a mature identity proofing and credential process to meet higher identity assurance level can be time consuming. We recommend a gradual, phased approach:

Step 1: Start with the Basics - Indicate your IdP's conformance with RAF Conformance Criteria.

When to do it: Now

The first step in this process is to configure your identity provider to release the RAF prefix value of "https://refeds.org/assurance". This signals that you meet the RAF "Conformance Criteria", i.e., your identity provider meets the conformance criteria defined in section 3 of the REFEDS Assurance Framework. All InCommon Participants already meet these criteria because they are a part of InCommon's Baseline Expectations program.

Technical Configuration: Releasing assurance information via eduPersonAssurance

Step 2: Send "local-enterprise" value where applicable.

When to do it: As soon as possible.

As soon as you are able, configure your identity provider to release the “local-enterprise” value for users who meet the requirements. The REFEDS Assurance Framework Implementation Guidance for the InCommon Federation provides details on how to determine which user meets this requirement.

The local-enterprise identity assurance type is designed to convey that the credential belongs to a user you trust to sign into your own institution’s critical systems. Sharing this information should be an easier first step since institutions likely already maintain an accurate user list for these systems. Doing so does not depend upon a deep understanding of business processes and integration of IAM systems with business systems to capture identity proofing information.

Step 3: Plan and Grow; implement additional assurance levels.

When to do it: by December 2022*

Using the REFEDS Assurance Framework Implementation Guidance for the InCommon Federation as support, iInstitutions should establish a task force consisting of stakeholders from IT and major person data stewards to develop strategy, identify funding, and devise implementation plan to communicate a user’s identity proofing levels using the values defined in the REFEDS Assurance Framework.

Institution should begin the discovery and planning process as soon as possible so that it can budget, if needed, for full implementations in the 2022-23 fiscal year.

* We recognize that implementing an identity assurance program can be a complex endeavor requiring significant time and effort from multiple stakeholders in your institution. Becoming fully NIH ready may be a journey measured in years, not months. There is no immediate expectation that institutions will immediately meet the highest levels of identity assurance. In fact, different NIH resources will require a varying subset of these requirements. Depending on the specific resources your users access, you may not need to implement all identity assurance levels. Right now, we are asking you to start the planning process: understand identity assurance concepts and inventory your campus processes around identity proofing. Most importantly, begin taking the first steps.

About the NIH Login Service

NIH Login Service is an access gateway protecting dozens of NIH online resources with varying access requirements. When a user signs into a resource protected by the NIH Login Service, it verifies the authentication and user information sent in the SAML assertion, compares them with the resource's requirements, and routes the user to the resource if the information sent meets the resource's requirements.

Resources

- REFEDS MFA Profile
- REFEDS Research and Scholarship (R&S)
- REFEDS Assurance Framework
- R&S Explained in Plain English
- REFEDS Assurance Working Group wiki
- Assured Access Working Group wiki
- NIH Security Compliance Check Tool