get-nih-ready-faq

1. How can institutions receive metrics on those logging in using federated MFA vs. Login.gov?

Yes, Please email help@incommon.org for metrics.

2. Is there a plan to add the eduPersonAssurance attribute to the Compliance Check Tool to verify compliance with the REFEDS Assurance Framework?

NIH provides two compliance check tools:

eRA Compliance Tool (https://auth.nih.gov/CertAuthV3/forms/eRAcompliancecheck.aspx)

The eRA Compliance tool is designed specifically for eRA, which has no identity assurance requirement and does not check eduPersonAssurance.

NIH Compliance Tool (https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx)

The NIH Compliance Tool checks the entire set of NIH requirements. In addition to incorporating eRA's requirement for REFEDS MFA, this tool also checks for eduPersonAssurance attributes aligned with the REFEDS Assurance Framework, which defines claims about the level of assurance that the user is who they say they are.

3. When and which NIH applications will require a higher LoA (Level of Assurance) given the recent disclosures about Login.gov?

As of this writing (May 2023), there is no specific timing on when and which NIH applications will start to require a higher LoA assertion. The good news is we have the infrastructure and standards in place to adopt at any given time. At the moment, eRA continues to accept multi-factor authentication (MFA) from Login.gov. However, there may be new federal standards and other NIH systems that may require higher identity assurance levels.

4. Where can I find more details regarding NIH IAM’s architecture and software requirements to support multilateralfederation implementation?

Stay tuned for future InCommon office hours for more in-depth discussions. You may also reach out to the NIH Technical Team at nihlogin.internal@mail.nih.gov for further information.

5. Will the likely/useful Assurance levels require organizations to view/verify government provided IDs (i.e. I have seen a user's drivers license or passport)? Can you talk about that? I have REFEDS MFA setup already, so Assurance is my next hill to climb.

The REFEDS Assurance Framework contains two “Identity Assurance Profiles” (IAPs) likely to be of use for some NIH services - medium and high - that are based on government issued IDs. There is also an IAP of “local-enterprise” whose meaning is essentially “we trust this user to access some of our sensitive systems, so maybe you will too”. That is not based on government issued ID, and may be useful to some NIH services at least for an interim period.

FAQ

- 1. How can institutions receive metrics on those logging in using federated MFA vs. Login.gov?
- 2. Is there a plan to add the eduPersonAssurance attribute to the Compliance Check Tool to verify compliance with the REFEDS Assurance Framework?
- 3. When and which NIH applications will require a higher LoA (Level of Assurance) given the recent disclosures about Login.gov?
- 4. Where can I find more details regarding NIH IAM’s architecture and software requirements to support multilateralfederation implementation?
- 5. Will the likely/useful Assurance levels require organizations to view/verify government provided IDs (i.e. I have seen a user's drivers license or passport)? Can you talk about that? I have REFEDS MFA setup already, so Assurance is my next hill to climb.
- 6. Is there a way to require users at a specific institution to use Federated MFA? All of our users should have MFA configuredand available, and if REFEDS MFA was requested would be enforced on our end to require it for them to log in.
- 7. The REFEDS MFA FAQ discusses the "Remember Me" feature common to many MFA implementations, but doesn't really provide a clear answer as to whether use of such a feature disqualifies a session from being eligible for the MFA assurance. Is there any guidance or community consensus on handling that?
- 8. Is it possible that the eRA user experience is driving registrations via Login.gov rather than federated logins?
- 9. Does Login.gov charge NIH for the number of external users/logins authenticating to NIH applications?
- 10. Did NIH already enforce the requirement of the REFEDS Assurance Framework in December 2022? Or did the timeline change?
- 11. How exactly does one “communicate with our researchers and support staff about using InCommon enabled campus credentials to access NIH services”? Is this more of individual advertising its capability using InCommon

As you prepare to climb that hill, you should read the report of the Assured Access working group, chartered by InCommon' Community Trust and Assurance Board. It's http://doi.org/10.26869/ti.157.1. Also, work on the REFEDS Assurance Framework version 2 is nearing completion. A public consultation period will commence in Summer 2023. It is expected that version 2 will make your job of understanding exactly how to climb that hill a little easier than before.

6. Is there a way to require users at a specific institution to use Federated MFA? All of our users should have MFA configuredand available, and if REFEDS MFA was requested would be enforced on our end to require it for them to log in.

REFEDS MFA mitigates the risk that an unauthorized person gains access to resources granted to an authorized person. It is up to the relying party or service provider to determine whether to accept that risk or mitigate it with MFA. That decision will likely not depend on what institution a user belongs to - they'll either require MFA and always ask for it using REFEDS MFA, or they won't require MFA and never ask for it. That said, it may be possible for you to configure your Identity Provider to always perform MFA whether or not it has been requested. This is a fairly common approach for single sign-on systems used within an organization since some services are not designed to be able to request MFA.

7. The REFEDS MFA FAQ discusses the "Remember Me" feature common to many MFA implementations, but doesn't really provide a clear answer as to whether use of such a feature disqualifies a session from being eligible for the MFA assurance. Is there any guidance or community consensus on handling that?

The most recent version (1.2) of the REFEDS MFA Profile addresses this. It explicitly avoids setting any time limit, but does insist that the "authentication instant" federation protocol element be correctly set with the time at which the user last performed MFA (the beginning of the current "Remember Me" window). That enables relying parties to know how fresh or stale the MFA is and they can apply their own policies on MFA freshness. Version 1.2 also requires the Identity Provider to respect the "forced authentication" federation protocol element, which requires the user to fully reauthenticate, ensuring the relying party that the MFA session is quite fresh.

There is a caveat to this answer. As of this writing (May 2023), version 1.2 of the REFEDS MFA Profile is under consultation, a period in which comments are solicited and feedback taken into account in the final revision. So it's possible that these statements may be amended before version 1.2 is finalized.

8. Is it possible that the eRA user experience is driving registrations via Login.gov rather than federated logins?

eRA was the first NIH system to promote Login.gov, which was available for multi-factor authentication (MFA) before federated logins were an option. We are in the process of encouraging people to use federated university credentials as an additional option to Login.gov.

On a related note, users can link their federated logins (campus credentials) to their eRA account even if they've already linked a Login.gov account to their eRA account. The process is the same as that used for Login.gov. Press the "Commons Login" button and choose "Login with Federated Account". If your federated login is MFA protected and your campus Identity Provider has implemented the REFEDS MFA Profile, then the eRA system will accept the login and ask the user to login to their eRA Commons account, which has its own password. Once that's done, their federated account, along with their Login.gov account, are both linked to their eRA Commons account. Either may be used to login to eRA subsequently.

9. Does Login.gov charge NIH for the number of external users /logins authenticating to NIH applications?

Yes, there is a minimal charge but it has been suspended at the moment. It is currently free for two years.

- enabled campus credentials to access NIH?
- 12. I have been periodically checking the "Get NIH Ready" page at https://spaces.at.internet2.edu/display/federation/get-nih-ready for updates but it has not been modified since 2021. Can that page be updated and continue to be updated?
- 13. Is it possible for NIH to let institutions know which of its researchers are using Login.gov to access eRA?
- 14. Can NIH contact individuals using Login.gov and suggest they use federated login instead?
- 15. Years ago, the perception among our researchers was that NIH had hundreds of individual projects, each with their own set of local credentials. How did NIH encourage adoption within and across to address this type of perception that pushes back against adoption?
- 16. I recall a recommendation that organizations assert the lowest level of assurance which meant we trust id proofed individuals to access local systems and services. Should we still go ahead with that? Or will the assurance requirement for NIH be a higher level, Cappuccino or Espresso?

Related Links

- 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
- eRA Security Compliance Check Tool

10. Did NIH already enforce the requirement of the REFEDS Assurance Framework in December 2022? Or did the timeline change?

NIH did not enforce the REFEDS Assurance Framework in December 2022, rather the focus was on developing the infrastructure and service enhancement to comply with the REFEDS Assurance specifications. NIH is expecting a large number of its downstream applications to require REFEDS assurance signals by December 2024.

11. How exactly does one “communicate with our researchers and support staff about using InCommon enabled campus credentials to access NIH services”? Is this more of individual advertising its capability using InCommon enabled campus credentials to access NIH?

To a large extent the answer depends on how research computing support is organized at your campus. Some campuses have research support people employed within a research computing center, in Research Administration, associated with an Institutional Review Board, or provided by central IT. If your campus is organized in one of these ways, your best approach is probably to locate those people, help them to understand that their clients’ campus credentials can be used with NIH, and ask that they make their clients aware.

If that’s not the case, you’ll first need to determine how to identify which researchers on your campus interact with NIH. Groups like research computing centers, Research Administration, Institutional Review Boards, and an academic technologies group within central IT are probably the best places to start. The NIH RePORT site (https://report.nih.gov/) can list Principal Investigators at your campus with active NIH awards, and that might also yield a starting point.

When you finally do communicate with someone, let them know that the NIH eRA system lets them associate their campus credential with their eRA account, exactly the same way as they did with their Login.gov credential. Then they are free to use either one to login to eRA. The automated process starts by simply logging in to eRA using their campus credential.

12. I have been periodically checking the "Get NIH Ready" page at https://spaces.at.internet2.edu/display/federation/get-nih-ready for updates but it has not been modified since 2021. Can that page be updated and continue to be updated?

Yes, it will be updated with this FAQ. We’re also thinking about some other changes to make, and of course as more NIH data services start to require MFA and/or identity assurance (see question 10 above) we’ll be making corresponding updates to the Get NIH Ready wiki page.

13. Is it possible for NIH to let institutions know which of its researchers are using Login.gov to access eRA?

We will look into this and work with the eRA team to check if that is possible. There are permission and privacy concerns to take into consideration. Once we’ve discussed this internally, we will share updates and discuss ways for your institution to promote federated MFA.

14. Can NIH contact individuals using Login.gov and suggest they use federated login instead?

With respect to eRA, no. Their requirement is multi-factor authentication and they don’t have a preference whether people use their federated credentials or Login.gov. It is about choice and personal preference. However, there may be other NIH systems in the future that require federated credentials to meet multi-factor authentication requirements instead of Login.gov.

15. Years ago, the perception among our researchers was that NIH had hundreds of individual projects, each with their own set of local credentials. How did NIH encourage adoption within and across to address this type of perception that pushes back against adoption?

There are a few NIH systems that require local credentials, and they are making a move away from it. If there are systems that you are aware of requiring local credentials, provide us the names of those systems and we can look into it. Our team supports the effort on federated credentials, and we have the capability to allow those systems to use federated credentials.

16. I recall a recommendation that organizations assert the lowest level of assurance which meant we trust id proofed individuals to access local systems and services. Should we still go ahead with that? Or will the assurance requirement for NIH be a higher level, Cappuccino or Espresso?

Yes, you should go ahead with that, ie, sending the “IAP/local-enterprise” identity assurance claim. Partly because it may in fact be accepted by some NIH services, at least for an interim period, and partly because implementing this specific claim has little to no dependence on institutional policy or processes, making it as easy as possible to implement. You can assert it for groups of users who are already permitted access to one of several types of institutional systems. Which ones? Their qualifying characteristics are listed in the report of InCommon’s Assured Access working group, http://doi.org/10.26869/ti.157.1.

Cappuccino and Espresso are profiles that bundle several different types of REFEDS Assurance Framework claims together. They include identity assurance claims of IAP/medium and IAP/high, respectively. You should also start planning to support these claims, per question 10 above.

By the way, the “local-enterprise” form of identity assurance isn’t necessarily of lower value than that provided by examining government issued IDs. The former is a direct expression of risk acceptance by the campus. An NIH service owner, who makes such risk decisions for their service, may well be satisfied with that. It’s akin to how they’ve been assured of their users’ identities all along, based on eRA’s processes that determine validity of each user as a campus person.