Upcoming Changes in FAMAuth Admin v2.19

Target Deployment Date: 8/4/26

Version 003

July 27, 2026

Revision Log

Rev #	Date	Author	Description
001	06/30/26	Marshall Keppel	Initial revision
002	7/9/26	Marshall Keppel	Added screenshots for each applicable feature
003	7/27/26	Mike Roadifer	Updated wording on a few slides.

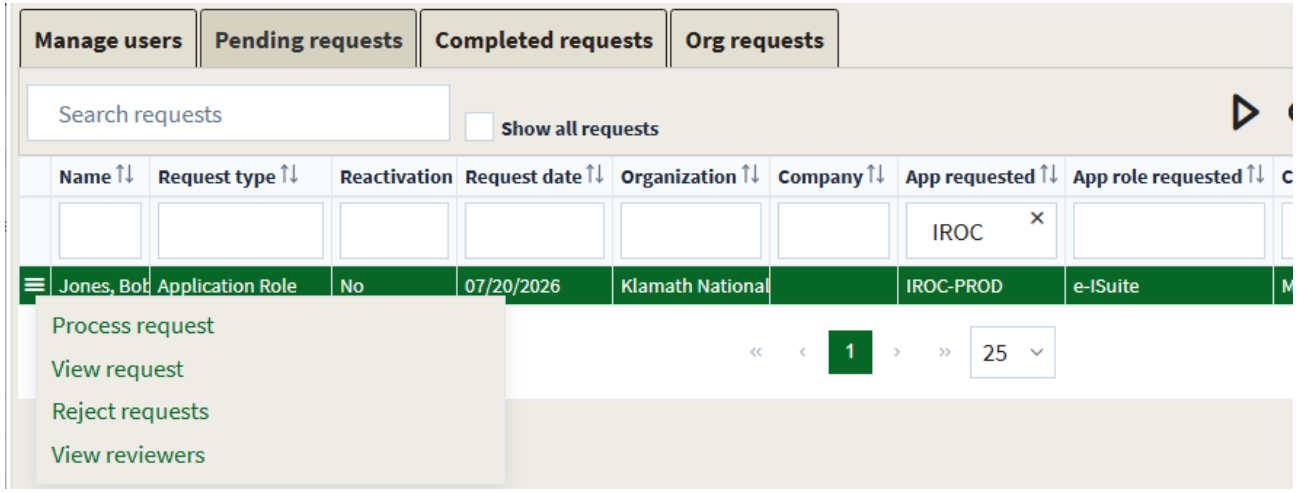
Table of Contents

Add Approver by Application Role (Part 1)

Available in QA: Yes

Currently application managers can configure application approvers at the application level, allowing application approvers to approve application access and role requests. With this update, application managers can configure approvers at the application **role** level, allowing them to assign and approve application role requests for a specific role.

In this screenshot, the user is allowed to approve requests only for the IROC e-ISuite role. Note that this role does not exist in Production and is shown only for demonstration purposes.

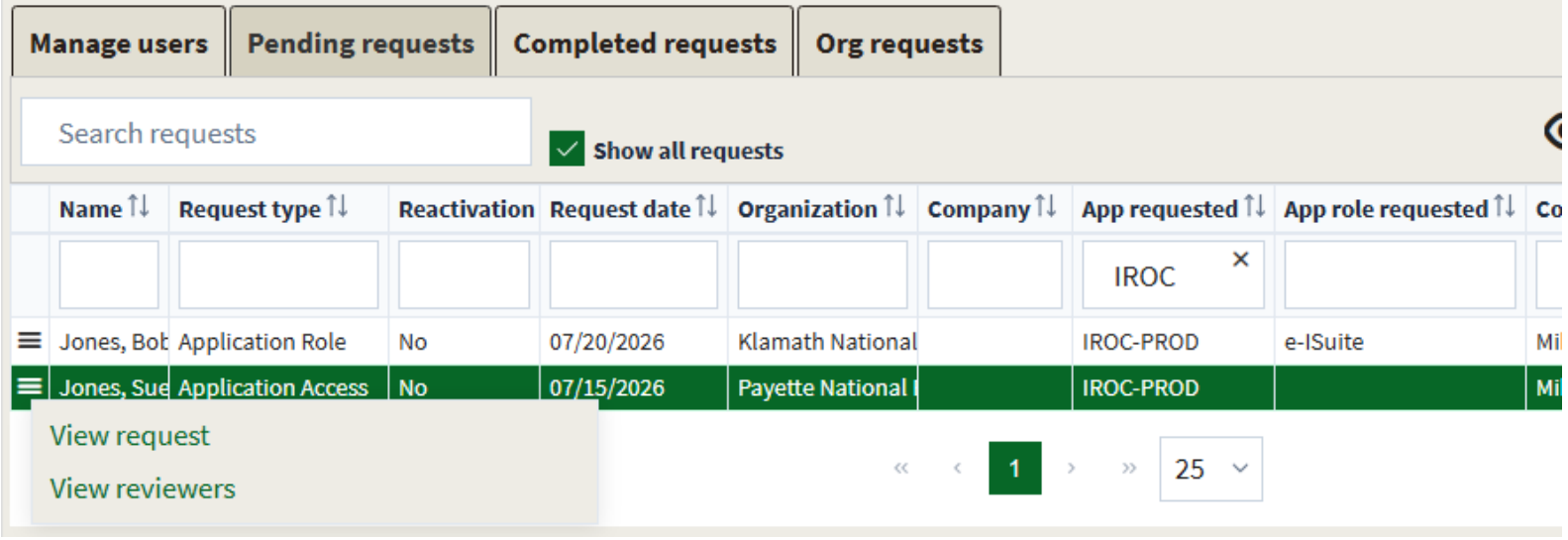


User is allowed to process requests for a specific application role.

Add Approver by Application Role (Part 2)

Available in QA: Yes

"New User", "Application Access" and other "Application Role" requests for the same application (IROC in this example) are not displayed by default but can be viewed via the "Show all requests" check box.

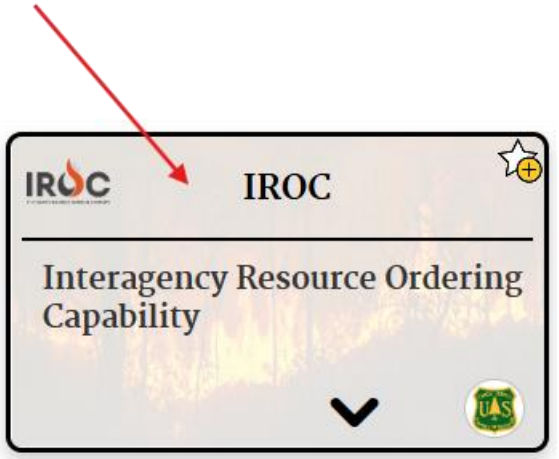


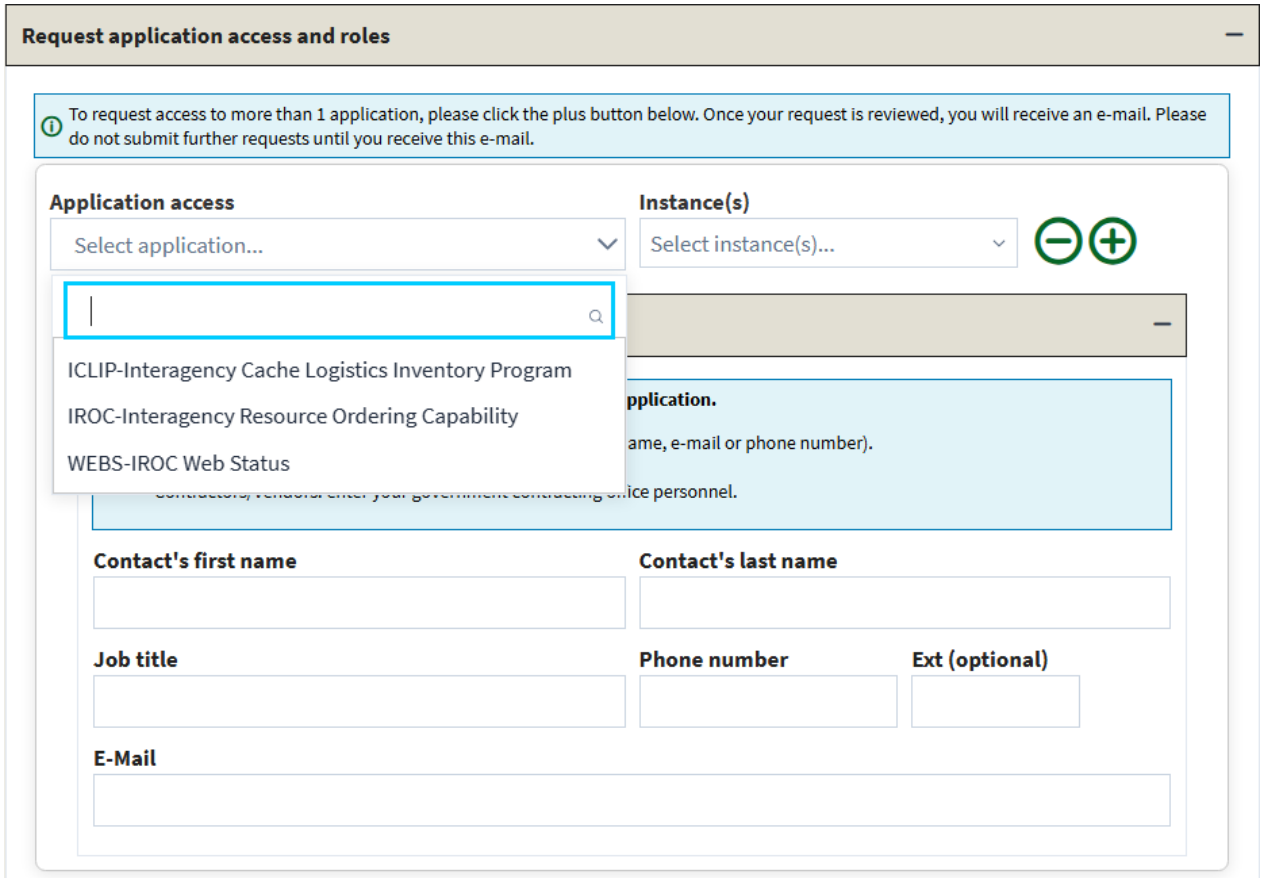
Add Subordinate Applications

Available in QA: Yes

This feature introduces the concept of subordinate applications to support future integration of roles for applications where a single tile allows access to multiple applications. In this screenshot the IROC application has been configured with two subordinate applications: ICLIP and Web Status. Users can request access and roles to IROC, ICLIP and Web Status by clicking on the parent tile (IROC) in the FAMAuth portal.

Note that this configuration does not exist in Production and is shown only for demonstration purposes.





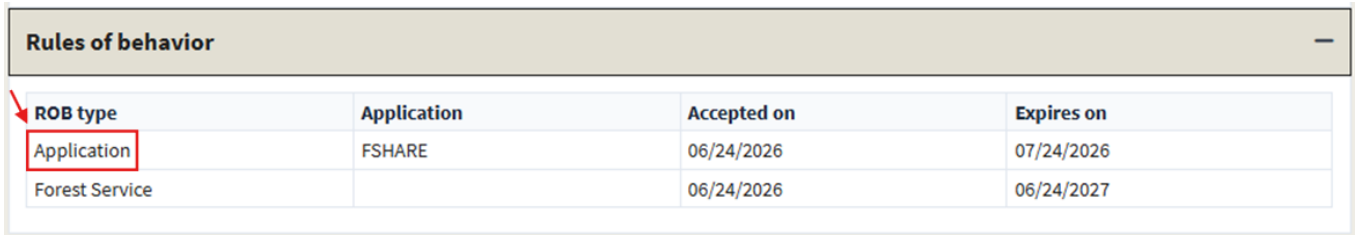
Application Rules of Behavior

Available in QA: Yes

This feature introduces the rules of behavior concept (ROB) to applications. Each application has unique security requirements, and for certain applications with more stringent requirements, there is a need for all users of the application to accept rules of behavior periodically that are specific to the application.

With this update, Application Managers will be able to enable an application ROB and configure custom ROB text along with a frequency that is required for accepting the application's ROB (e.g., every 365 days a user must accept the application ROB). When a new user or a user with an expired application ROB agreement launches the application, the system will display the application ROB, and the user will be required to accept the ROB to access the application.

In addition, this feature introduces the ROB Compliance report, a report designed to show the ROB status for each user. Users and Application Managers will also be able to check ROB information from the Rules of behavior panel on the user profile (see screenshot below).



Rules of behavior —

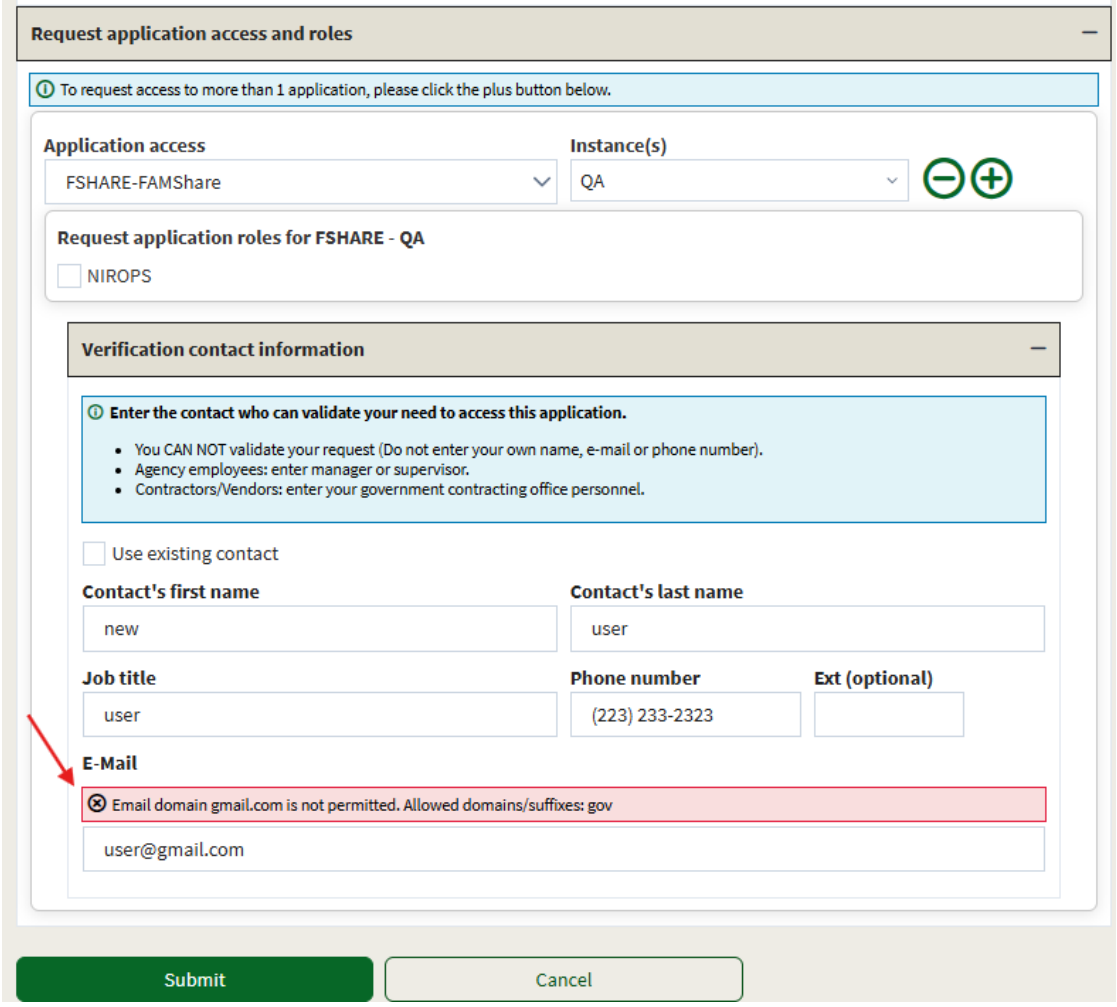
ROB type	Application	Accepted on	Expires on
Application	FSHARE	06/24/2026	07/24/2026
Forest Service		06/24/2026	06/24/2027

Restrict Verification Contact Email Domains

Available in QA: Yes

Application Approvers have noticed that verification contacts with email domains outside of the government are sometimes not reachable when attempting to contact them to verify an application access or role request. Application Approvers have also noticed that verification contacts with a “gov” email address domain are typically more reliable, and thus, they have requested the ability to restrict verification contact email domains.

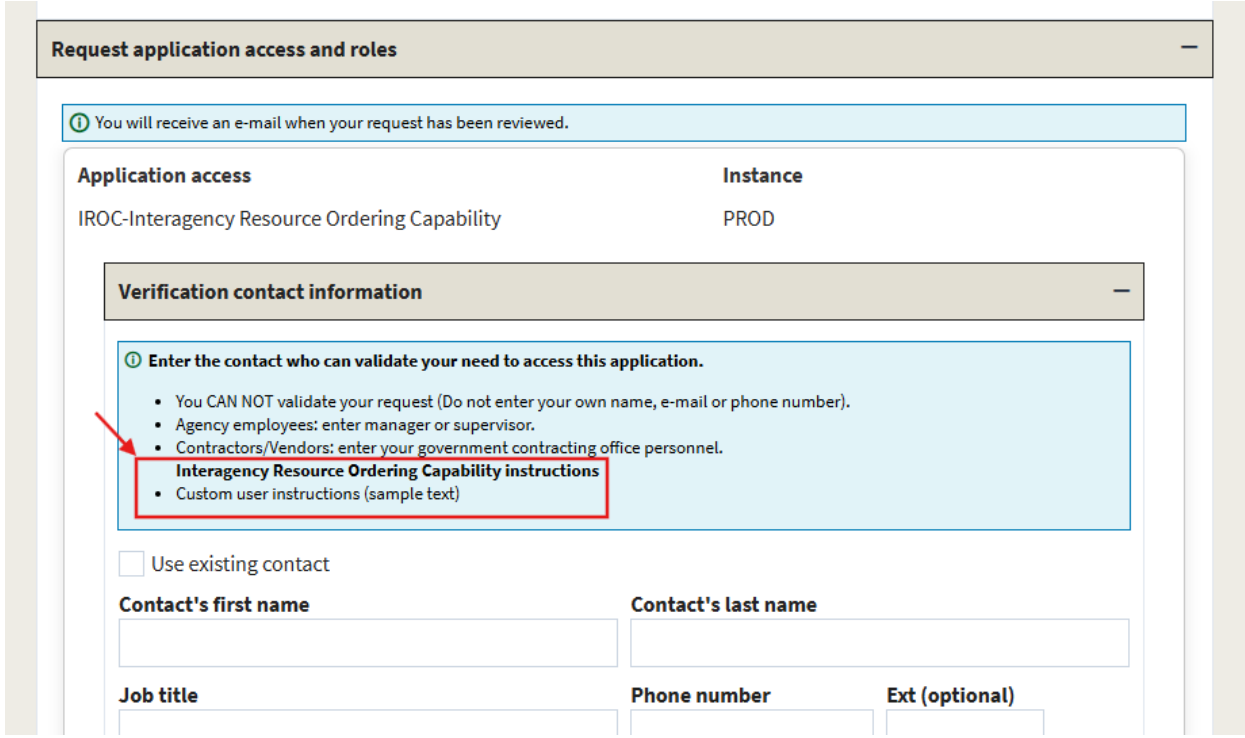
This feature grants Application Managers the ability to configure acceptable email domains for verification contacts at the application level. By inputting “gov” for the permitted email domains, as an example, users will no longer be able to enter a verification contact with an email domain that is not “gov” and will receive an error message indicating the email domain is not valid.



Custom Verification Contact Info Message

Available in QA: Yes

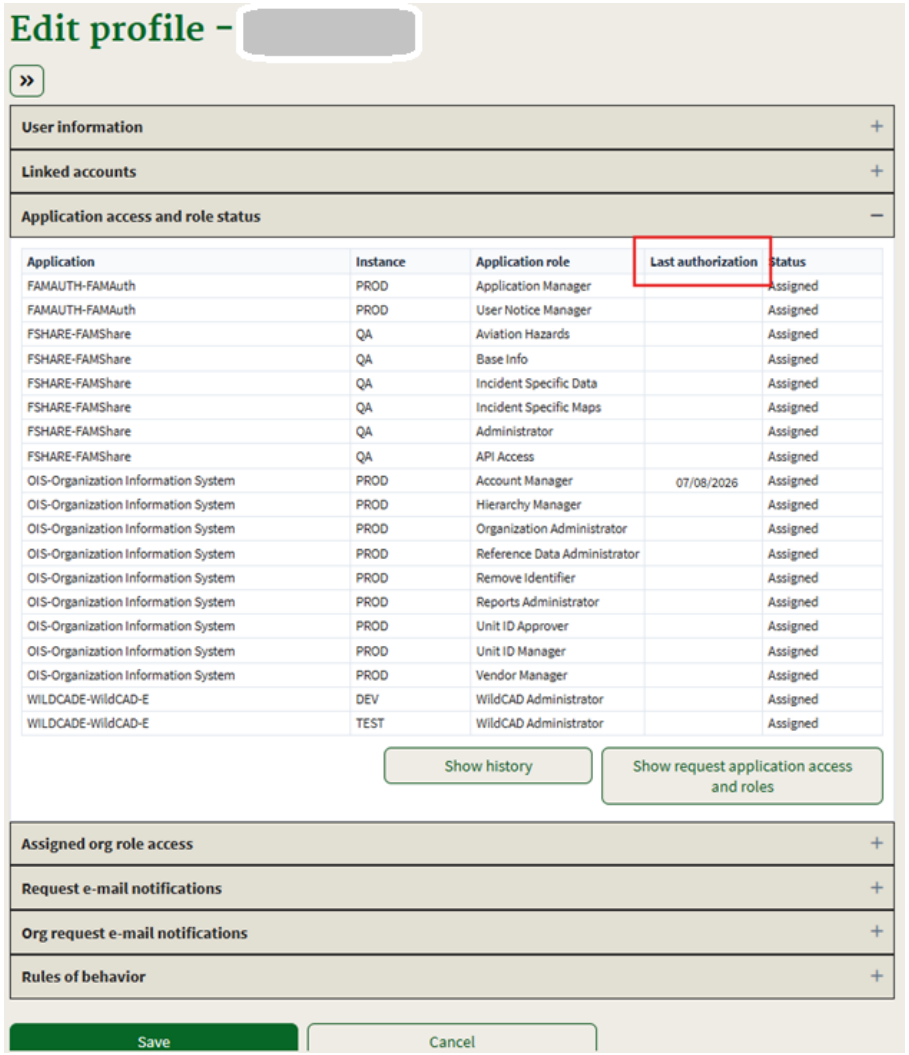
The purpose of this feature is to provide functionality for creating custom user instruction text for a given application that will dynamically display in the verification contact panel for users when requesting application access or roles for the application.



Users Need to View Last Authorization Dates

Available in QA: Yes

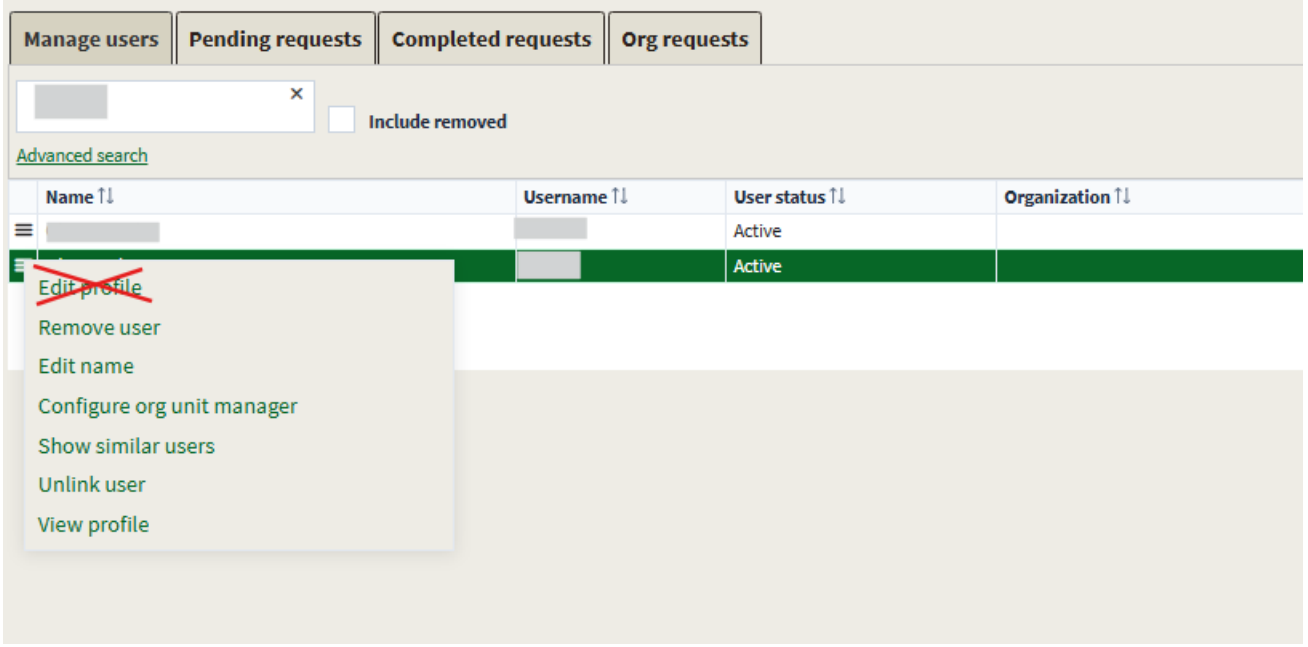
Currently, only account managers or users with reports access can view the last authorization dates for users. With this update, a new column has been added to the **Application access and role status grid** on the Edit profile page, the **Last authorization**, allowing users to view the most recent date they were authorized for each application instance that they have access to.



Org unit managers no longer need access to Edit profile

Available in QA: Yes

Org unit managers previously required access to the **Edit profile** page for other users in order to assign org units. Because org unit assignment has moved to the **Edit organization and roles** page, org unit managers no longer have a need to edit the profile for other users. Therefore, the **Edit profile** menu item will no longer display for org unit managers when managing users.



Thank you!

Please reach out to Ryan Hunt (Ryan.Hunt2@usda.gov) or Mike Roadifer (Michael.Roadifer@usda.gov) for more information.