

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](#)
- [Add Approver by Application Role \(Part 2\) – Available in QA: Yes](#)
- [Add Subordinate Applications – Available in QA: Yes](#)
- [Application Rules of Behavior – Available in QA: Yes](#)
- [Restrict Verification Contact Email Domains – Available in QA: Yes](#)
- [Custom Verification Contact Info Message – Available in QA: Yes](#)
- [Users Need to View Last Authorization Dates – Available in QA: Yes](#)
- [Org unit managers no longer need access to Edit profile – Available in QA: Yes](#)

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.

Name ↑↓	Request type ↑↓	Reactivation	Request date ↑↓	Organization ↑↓	Company ↑↓	App requested ↑↓	App role requested ↑↓
Jones, Bob	Application Role	No	07/20/2026	Klamath National		IROC	e-ISuite

- Process request
- View request
- Reject requests
- View reviewers

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.

Manage users

Pending requests

Completed requests

Org requests

☒ Show all requests

	Name ↑↓	Request type ↑↓	Reactivation	Request date ↑↓	Organization ↑↓	Company ↑↓	App requested ↑↓	App role requested ↑↓	Co
							IROC ×		
≡	Jones, Bob	Application Role	No	07/20/2026	Klamath National		IROC-PROD	e-ISuite	Mil
≡	Jones, Sue	Application Access	No	07/15/2026	Payette National		IROC-PROD		Mi

View request

View reviewers

«

<

1

>

»

25 ▾

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.



Request application access and roles

To request access to more than 1 application, please click the plus button below. Once your request is reviewed, you will receive an e-mail. Please do not submit further requests until you receive this e-mail.

Application access **Instance(s)**

Select application... Select instance(s)...  

ICLIP-Interagency Cache Logistics Inventory Program
IROC-Interagency Resource Ordering Capability
WEBS-IROC Web Status

Application.
ame, e-mail or phone number).

Contractors, Vendor, enter your government contracting office personnel.

Contact's first name **Contact's last name**

Job title **Phone number** **Ext (optional)**

E-Mail

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.

The screenshot shows a web form titled "Request application access and roles". It includes a section for "Application access" with a dropdown menu set to "FSHARE-FAMShare" and an "Instance(s)" dropdown set to "QA". Below this is a section for "Request application roles for FSHARE - QA" with a checkbox for "NIROPS". The main section is "Verification contact information", which contains a blue box with instructions: "Enter the contact who can validate your need to access this application." followed by bullet points: "You CAN NOT validate your request (Do not enter your own name, e-mail or phone number).", "Agency employees: enter manager or supervisor.", and "Contractors/Vendors: enter your government contracting office personnel." Below the instructions is a checkbox for "Use existing contact". The form has fields for "Contact's first name" (containing "new"), "Contact's last name" (containing "user"), "Job title" (containing "user"), "Phone number" (containing "(223) 233-2323"), and "Ext (optional)". The "E-Mail" section is highlighted with a red box and a red arrow pointing to it. It contains a red error message: "Email domain gmail.com is not permitted. Allowed domains/suffixes: gov". Below the error message is a text input field containing "user@gmail.com". At the bottom of the form are "Submit" and "Cancel" buttons.

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.

Request application access and roles

① You will receive an e-mail when your request has been reviewed.

Application access	Instance
IROC-Interagency Resource Ordering Capability	PROD

Verification contact information

① Enter the contact who can validate your need to access this application.

- You CAN NOT validate your request (Do not enter your own name, e-mail or phone number).
- Agency employees: enter manager or supervisor.
- Contractors/Vendors: enter your government contracting office personnel.

Interagency Resource Ordering Capability instructions

- Custom user instructions (sample text)

☐ Use existing contact

Contact's first name

Contact's last name

Job title

Phone number

Ext (optional)

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.

Edit profile - [Redacted]

>>

User information +

Linked accounts +

Application access and role status -

Application	Instance	Application role	Last authorization	Status
FAMAUTH-FAMAuth	PROD	Application Manager		Assigned
FAMAUTH-FAMAuth	PROD	User Notice Manager		Assigned
FSHARE-FAMShare	QA	Aviation Hazards		Assigned
FSHARE-FAMShare	QA	Base Info		Assigned
FSHARE-FAMShare	QA	Incident Specific Data		Assigned
FSHARE-FAMShare	QA	Incident Specific Maps		Assigned
FSHARE-FAMShare	QA	Administrator		Assigned
FSHARE-FAMShare	QA	API Access		Assigned
OIS-Organization Information System	PROD	Account Manager	07/08/2026	Assigned
OIS-Organization Information System	PROD	Hierarchy Manager		Assigned
OIS-Organization Information System	PROD	Organization Administrator		Assigned
OIS-Organization Information System	PROD	Reference Data Administrator		Assigned
OIS-Organization Information System	PROD	Remove Identifier		Assigned
OIS-Organization Information System	PROD	Reports Administrator		Assigned
OIS-Organization Information System	PROD	Unit ID Approver		Assigned
OIS-Organization Information System	PROD	Unit ID Manager		Assigned
OIS-Organization Information System	PROD	Vendor Manager		Assigned
WILDCADE-WildCAD-E	DEV	WildCAD Administrator		Assigned
WILDCADE-WildCAD-E	TEST	WildCAD Administrator		Assigned

Show historyShow request application access and roles

Assigned org role access +

Request e-mail notifications +

Org request e-mail notifications +

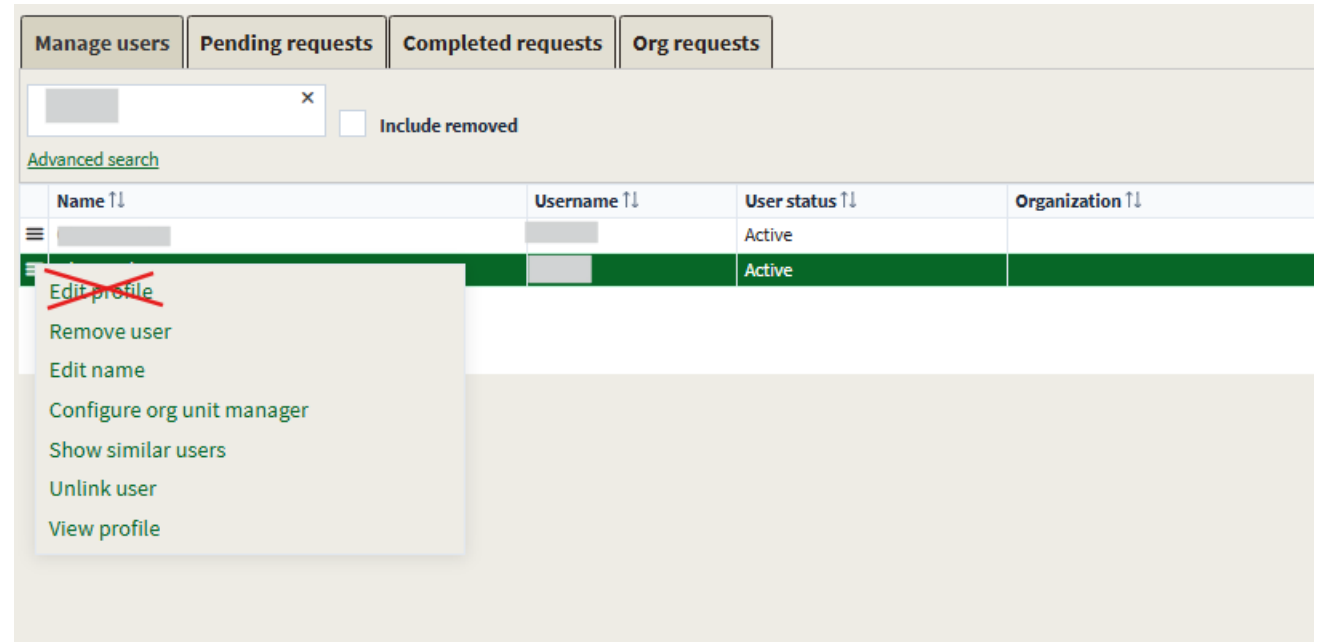
Rules of behavior +

SaveCancel

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.

