

Upcoming Changes in FAMAuth Admin v2.18

Target Deployment Date: (May 12, 2026)



Version 005

April 29, 2026

Revision Log

Rev #	Date	Author	Description
001	10/14/25	Marshall Keppel	Initial revision
002	01/20/26	Marshall Keppel	Added the following features: <ul style="list-style-type: none">• Remove Vendor DUNS (INAP#613)• Add Support for Unassignable Roles (INAP#614)• Remove LDAP (INAP#619)• Add Support for Dependent Roles (INAP#621)
003	02/23/26	Marshall Keppel	Added screenshots for each feature and updated Available in QA status to Yes
004	3/18/26	Marshall Keppel	Added the following features: <ul style="list-style-type: none">• Add Request Org Roles to Authorization Flow (INAP#630)
005	4/29/26	Mike Roadifer	Edits to order of slides, text and screenshots

Table of Contents

- [Remove Username and Password Authentication – Available in QA: Yes](#)
- [Org Access and Role Improvements \(Part 1\) – Available in QA: Yes](#)
- [Org Access and Role Improvements \(Part 2\) – Available in QA: Yes](#)
- [Unassignable Roles – Available in QA: Yes](#)
- [Dependent Roles – Available in QA: Yes](#)
- [Require Org Access for Users – Available in QA: Yes](#)
- [Remove Vendor DUNS – Available in QA: Yes](#)

Remove Username and Password Authentication

Available in QA: Yes

Username and password authentication is no longer supported, as all FAM applications are now using FAMAAuth with Login.gov or eAuthentication for multi-factor authentication (MFA).

With these changes, the concept of “password users” and all password functionality (e.g., Change Password, Reset Password, Recover Username, etc.) no longer exist within the system.

The Temporary Password, Expired Password, and Disabled statuses for users also no longer exist and all associated functionality (e.g., Keep disabled user screen) is removed.

The screenshot displays the Wildland Fire Application Portal - FAMAAuth interface. At the top, it says "Authenticated by: eAuth". Below this, there's a navigation bar with a "Welcome, [redacted]" dropdown menu. A dropdown menu is open, listing several options: "Change or reset FAMAAuth password", "Forgot my FAMAAuth password", "Forgot my FAMAAuth username", "Edit/view profile", "Request app access and roles", "Request org roles", "View my requests", and "Logout". The first three options are crossed out with red lines. Below the navigation bar, there's a section for "Application select one of the tiles be".

Below the navigation bar, there's a "Manage users" tab selected. The "Manage users" section shows a search bar, an "Include removed" checkbox, and an "Advanced search" section. The "Advanced search" section has columns for "Name", "Username", "User status", "Pwd user", and "Organization". A table row is visible with the following data: [redacted], [redacted], Disabled Inactive, Yes, Rocky Mountain Ra. The "Pwd user" column header and the "Yes" value in the table row are crossed out with red lines. A dropdown menu is open for the first row, listing options: "Edit profile", "Keep disabled user", "Reactivate user", "Remove user", "Delete user", "Edit name", "Show similar users", "Unlink user", and "View profile". The "Keep disabled user" option is crossed out with a red line.

Org Access and Role Improvements (Part 1)

Available in QA: Yes

For applications with org unit roles (such as WildCAD-E), assigning org unit access and roles is currently performed in two steps. Org unit access is assigned on the “Edit profile” screen, and roles are assigned on the “Edit org unit roles” screen.

For users with access to many org units, the “Edit profile” screen becomes unwieldy due to the vertical length of the “Org unit access” section.

Assigning org unit access and roles is now combined into one step on the new “Edit organization and roles” screen, accessed from the menu item of the same name on the “Manage users” grid. The “Org unit access” section has been removed from “Edit profile”.

Edit organization and roles for [redacted]

Application: WILDCADE-WildCAD-E Show user information

My managed org units Search

Org unit name	Org unit ID
Coeur d Alene Dispatch Center	US-ID-CDC
Montrose Interagency Dispatch Center	US-CO-MTC

Assigned org unit access Search

Org unit name	Org unit ID	Temporary until
Alaska Coastal Dispatch Center	US-AK-ACDC	<input type="text"/>

Assigned roles at Alaska Coastal Dispatch Center

Instance	Org role	Assigned
TEST	Center Administrator	<input type="checkbox"/>
TEST	Read Only	<input checked="" type="checkbox"/>
TEST	Dispatcher	<input type="checkbox"/>
TEST	Resource Status	<input type="checkbox"/>
TEST	Roster	<input type="checkbox"/>

Save Save and continue Cancel

Org Access and Role Improvements (Part 2)

Available in QA: Yes

The “Org role access” panel on the Edit/View Profile screen currently displays the org unit roles that are assigned to a user. For users with access to many org units, this becomes unwieldy due to the vertical length of the panel.

This panel has been replaced with the “Assigned org role access” panel which provides expand and collapse capability to reduce the vertical length.

In this new panel, users are also allowed to remove their own org unit access.

Assigned org role access			
Search access			
Access	Expiration date	Assigned	Remove
<ul style="list-style-type: none"> ▼ WILDCADE-WildCAD-E <ul style="list-style-type: none"> ▼ Boise Interagency Dispatch Center [US-ID-BDC] <ul style="list-style-type: none"> TEST-Center Administrator ▼ Coeur d Alene Dispatch Center [US-ID-CDC] <ul style="list-style-type: none"> TEST-Dispatcher TRN-Dispatcher ▼ Great Plains Interagency Dispatch Center [US-SD-GPC] <ul style="list-style-type: none"> TEST-Dispatcher TRN-Roster > Texas Interagency Coordination Center [US-TX-TIC] ▼ Tucson Interagency Dispatch Center [US-AZ-TDC] <ul style="list-style-type: none"> TEST-Dispatcher 		Yes	<input type="checkbox"/>

Unassignable Roles

Available in QA: Yes

Roles within FMAuth can now be configured as Unassignable to support future needs for applications such as IROC.

The screenshots (captured from FMAuth QA) show the IROC Vendor role as one that can be requested and approved but cannot be assigned without a request. The role is not shown when assigning roles.

Request application access and roles

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
IROC-Interagency Resource Ordering Capability	PROD

Request application roles for IROC - PROD

- IROC Vendor
- IROC Other Role

Application and role access

IROC-PROD × Show all Show column filters

Access	Last authorized	Assigned
✓ IROC-PROD Interagency Resource Ordering Capability		<input checked="" type="checkbox"/>
IROC Other Role		<input type="checkbox"/>

Show history

Dependent Roles

Available in QA: Yes

Roles within FAMAAuth can now be configured with a dependency to support future needs for applications such as IROC.

The screenshot (captured from FAMAAuth QA) shows the message that is displayed after the IROC Dispatch Manager is assigned to a user. The IROC Dispatch Manager and IROC Dispatcher have been configured such that IROC Dispatcher is automatically assigned along with IROC Dispatch Manager.

Note: A given dependent role combination can be configured with two application roles or two org roles for an application; linking an application role with an org role is not supported.

The screenshot displays the 'Manage users' tab in the FAMAAuth system. At the top, there are three tabs: 'Manage users', 'Pending requests', and 'Completed requests'. Below the tabs is a search bar with a placeholder and an 'X' icon, and an 'Include removed' checkbox. A link for 'Advanced search' is visible. A table lists user information with columns for Name, Username, User status, Organization, and a partially visible 'Number' column. One user is listed with 'Active' status and 'Washington O' organization. A green success message box is overlaid on the right side of the table, stating: 'Success The following dependent roles were also assigned for IROC-PROD: IROC Dispatcher because it is dependent upon IROC Dispatch Manager'.

Require Org Access for Users

Available in QA: Yes

For applications with org unit roles (such as WildCAD-E), gaining access is a two-step process. Users first request access to the application. Upon approval, they must then use the “Request org roles” menu item to request one or more roles at an org unit.

Applications can now be configured in FMAAuth to require that users have access to at least one org unit. With this configuration enabled, when a user clicks the application tile FMAAuth will detect that the user does not have any assigned org units and will automatically redirect the user to the “Request org roles” screen.

The intent of this feature is to simplify instructions for a new user, in that they only need to be told to click on their application tile.




Request org roles

Org role request status

Application	Instance	Org unit name	Org unit ID	Org role	Status
OIS-Organization Information Sys	PROD	National Interagency Coordination Cer	US-ID-NIC	Unit ID Manager	Assigned
OIS-Organization Information Sys	PROD	National Interagency Coordination Cer	US-ID-NIC	Organization Manager	Assigned
WILDCADE-WildCAD-E	DEV	Alaska Coastal Dispatch Center	US-AK-ACDC	Center Administrator	Assigned
WILDCADE-WildCAD-E	DEV	Coeur d Alene Dispatch Center	US-ID-CDC	Center Administrator	Assigned
WILDCADE-WildCAD-E	DEV	Montrose Interagency Dispatch Center	US-CO-MTC	Center Administrator	Assigned
WILDCADE-WildCAD-E	TEST	Alaska Coastal Dispatch Center	US-AK-ACDC	Center Administrator	Assigned
WILDCADE-WildCAD-E	TEST	Coeur d Alene Dispatch Center	US-ID-CDC	Center Administrator	Assigned
WILDCADE-WildCAD-E	TEST	Montrose Interagency Dispatch Center	US-CO-MTC	Center Administrator	Assigned

Request roles

To request roles at more than one org unit, please click the plus button below.

Application	Instance(s)	Org unit
WILDCADE-WildCAD-E	Select instance(s)  	
		Select org unit

Submit **Cancel**

Remove Vendor DUNS

Available in QA: Yes

On April 4, 2022, the federal government stopped using the DUNS number to uniquely identify entities. Now, entities doing business with the federal government use the Unique Entity ID (UEI) created in SAM.gov.

DUNS is removed from FAMAAuth and will no longer appear as a field on the User Profile for vendors. Vendors no longer have the option of providing a DUNS number to identify their business and are required to enter a UEI as a company identifier when requesting a new user in FAMAAuth.

Request access

Select access type

The first step is to determine if you are a vendor. If you or the company you work for has contracted resources, you are considered a vendor.

I am not a vendor

I am a vendor needing to status resources

Enter user information

First name: DEMO Middle name (optional): Last name: USER

Job title (optional):

Primary e-mail: user@demo.com

Primary e-mail confirm:

Alternate e-mail (optional):

Receive communications also at

Office number: Ext (optional): Mobile (optional): Fax (optional):

State:

Primary affiliation: Contractor/Vendor Part-time/seasonal

~~DUNS number~~

UEI

Company

Thank you!

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

