

# FAMAuth Administration Guide

## Revision Log

Rev #	Date	Revision(s)	Author
21	12/16/25	Updated for FAMAuth Admin 2.18	Marshall Keppel
20	8/4/25	Updated for FAMAuth Admin 2.17	Marshall Keppel
19	2/18/25	Updated for FAMAuth Admin 2.16	Marshall Keppel
18	8/5/24	Updated for FAMAuth Admin 2.14	Marshall Keppel
17	7/2/2024	Updated screen captures for iNAP 2.13	Mike Roadifer
16	5/13/24	Updated for iNAP 2.13	Michelle Apicella
15	3/22/2024	Updated for iNAP 2.12	Michelle Apicella
14	2/15/2024	Updated for iNAP 2.11	Michelle Apicella
13	9/12/2023	Updated for iNAP 2.10	Michelle Apicella
12	3/22/2023	Updated for iNAP 2.9	Michelle Apicella
11	2/21/2023	Updated for iNAP 2.8	Michelle Apicella
10	10/11/2022	Updated with additional iNAP 2.7 impacts	Michelle Apicella
9	7/12/2022	Updated per iNAP 2.7  (note: no updates were needed for iNAP 2.6)	Michelle Apicella
8	4/6/2022	Updated with Center Manager information from iNAP 2.5 #62 Allow User to Request Dispatch Organization	Michelle Apicella
7	3/21/2022	Updated per internal review of rev #6	Michelle Apicella
6	3/7/2022	Updated for releases 1.13.3.1 through 2.5	Michelle Apicella
5	12/20/2021	Added concept of Application Approver	Michelle Apicella
4	12/13/2021	Made a few corrections in the Understanding iNAP User Account Status section.	Mike Roadifer
3	11/30/2021	DAO is now managing this doc. Updated content based on iNAP 2.3 and current process.	Michelle Apicella
2	11/19/2021	FY21 Review and revision	Ryan Hunt
1	10/30/2019	FY20 Review and revision	Angie Hinker

---

Revision Log.....	1
Document Scope .....	3
Understanding Administrators .....	3
Understanding end-users .....	4
Applications that reside in FAMAuth Admin.....	5
Understanding User status.....	5
Administration Navigation Menu .....	6
Account Manager Role (no additional configuration).....	7
Working with the Manage users grid.....	7
Editing User Profile information .....	8
Unlinking a User from an Identity Provider System.....	10
Managing the status of a User.....	11
Application Approver Configuration .....	12
Becoming an Application Approver.....	12
Pending Requests grid .....	12
Processing a request.....	13
Rejecting Multiple Requests at once.....	17
Reactivating a user via request .....	17
Assigning an Org Unit Manager to an Org Unit.....	18
Deleting a user.....	19
Emailing application users.....	20
Working with grids .....	23
Customizing the appearance of a grid.....	23
Generate Reports .....	24

---

# Document Scope

This FAMAAuth Administration Guide explains how users are approved and managed in FAMAAuth Admin. Topics include:

- Understanding Users
- Actions permitted by an Account Manager
- Actions permitted by an Application Approver
- Actions permitted by an Approver Manager
- Working with grids.

Topics not included: Actions permitted by an Org Unit Manager. See “Org Unit Manager Guide” for this information.

## Understanding Administrators

The term “Administrator” refers to a user who has access to at least one function within FAMAAuth Admin. Access to a function can be provided in one of two ways:

1. User is assigned a FAMAAuth Admin Role.
2. User is assigned a FAM application role that has been mapped to FAMAAuth Admin administrative function (also known as an operation).

The following matrix explains how administrative functions are assigned:

<b>This administrative function:</b>	<b>Comes with this role:</b>	<b>Additional configuration required:</b>	<b>This function may be mapped to FAM Application role(s):</b>	<b>Notes:</b>
Edit Profile	Account Manager	None	N	
Remove User	Account Manager	None	N	
Change Username	Account Manager	None	N	
Create User	Account Manager	None	N	
Edit User Application Roles	Account Manager	Setup as an application approver for the related application	Y	
Reactivate User	Account Manager	None	N	
Unlink User	Account Manager	None	N	

---

<b>This administrative function:</b>	<b>Comes with this role:</b>	<b>Additional configuration required:</b>	<b>This function may be mapped to FAM Application role(s):</b>	<b>Notes:</b>
Process Org Role Request	None	Setup as an Org Unit Manager	N	
Edit Org Roles	None	Setup as an Org Unit Manager	N	
Assign Org Unit Access and Org Roles	None	Setup as an Org Unit Manager	N	
Process Access Request	Account Manager	Setup as an application approver for the related application, or, an Org Unit Manager	Y	
Maintain Application Access	Account Manager	Setup as an application approver for the related application, or an Org Unit Manager	Y	
Access Reports	All	None	Y	
N/A	Application Manager	None	N	This role creates application(s) in FAMAuth Admin and configures them to be available for access.
N/A	Approver Manager	None	Y	
Email Subscribers	Application Manager	None	N	
Helpdesk Support	Helpdesk	None	N	Helpdesk Personnel

## Understanding end-users

An end-user is a user who is in FAMAuth for the purpose of accessing applications whose authentication and authorization is provided via FAMAuth.

Once an end-user has a FAMAuth User, (s)he can be assigned access to specific application(s), as well as perform the following self-maintenance:

- Reactivate themselves when inactive or request reactivation when removed
-

- Request access to additional FAM applications, including roles

The following quick reference cards are available to the end-user to assist with some of these actions:

- [How to Request a User](#)
- [Getting Started with FAMAAuth Admin](#)

For all other maintenance the end-user must contact an Account Manager or the Help Desk for assistance.

### ***Applications that reside in FAMAAuth Admin***

- Data Warehouse
- e-ISuite Enterprise
- EGP – Enterprise Geospatial Portal
- F&AM – FTP Site
- FAMS – FAMShare
- FEMS – Fire Environment Mapping System
- FEPP FEPMIS - Federal Excess Personal Property Federal Excess Property Management Info System
- ICBS – Interagency Cache Business System
- IgPoint – Fire Ignitions Point Website
- InciWeb - Administration
- IROC – Interagency Resource Ordering Capability
- LESO FEPMIS - Law Enforcement Support Office Federal Excess Property Management Information System
- NIROPS – National Infrared Operations Website
- NPSG – National 7-Day Significant Fire Potential
- OLMS – Operational Loads Monitoring System
- OIS – Organization Information System
- SAWTI – Santa Ana Wildfire Threat Index
- SIT-209 – National Interagency Situation Reporting System
- WFAIP – Wildland Fire Application Information Portal (Content Management)
- WFDSS NextGen – Wildland Fire Decision Support System
- WildCAD-E
- WIMS – Weather Information Management System

## **Understanding User status**

A User, regardless of if an end-user or administrative, has one of the following statuses:

- **Active.** The User can access the environment and / or applications.
  - **Inactive** – If the user does not have access to FTP or ICBS, the user is inactivated 60 days from last authorization. The User can reactivate themselves upon their next authorization, or by an Account Manager.
  - **Removed** – The User has been inactive for 330 days. The User is not able to access the environment/ applications due to either inactivity or notification to the Account Manager that the user no longer requires access i.e. seasonal workers.
-

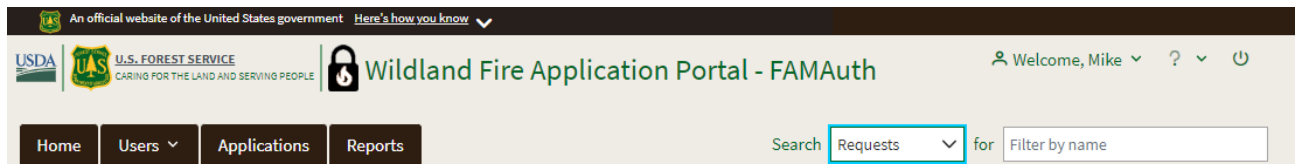
# Administration Navigation Menu

The **Navigation Menu** allows administrators to access data grids and take certain actions.

## To access the Navigation Menu

- 1 Log on to the **FAMAuth portal** (<https://famauth.wildfire.gov>) using your Login.gov or eAuth credentials.
- 2 Select **FAMAuth Admin** from the menu.

The following diagram shows the basic navigation menu. Tabs are displayed based on the role(s) the user holds and how those roles are configured.



# Account Manager Role (no additional configuration)

This section explains the functionality available to a user holding the Account Manager role, without further configuration.

In addition to the topics detailed here, the Account Manager is also responsible for:

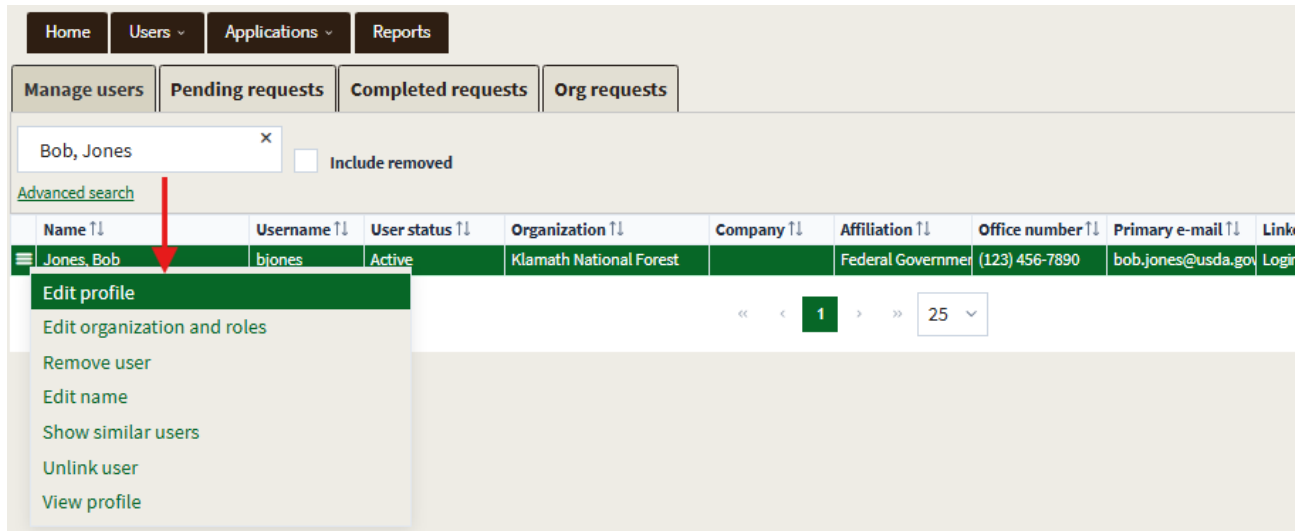
- Account Manager Quarterly Audit: It is the Application’s responsibility to perform quarterly audits of users that have access to their application. Audit reports are generated by the Project Manager or Lead iSME and sent to the application team to review. The Project Manager/Account Manager will audit the Account Managers.
- Auto Audit log: Auto generated Audit Logs are delivered monthly to FS-FAMIT Security and the Project Manager.

## Working with the Manage users grid

This **Manage users** grid allows account managers to search for users and take perform administrative functions.

### To access the Manage users grid

- 1 On the **Navigation Menu**, click the **Users** drop down menu and select **Manage users**.
- 2 Search for user(s) by entering search criteria into the **Search users** box
- 3 Select the menu icon next to the user record to access the functions



## Editing User Profile information

### To edit user's profile information

- 1 On the **Manage users** grid, select the menu icon for the **User** of your choice, and then click **Edit profile**.
- 2 Change the **User Information** and/or view the Requests and **Rules of Behavior** as appropriate, and then click the **Save or Cancel** button.

The following diagram shows the Edit profile page. The arrows point to some of the user information available for editing.

### Edit profile

>>

**User information** —

<b>First name</b>	<b>Middle name</b>	<b>Last name</b>	
		Jones	

**Job title (optional)**

**Primary e-mail**

**Alternate e-mail (optional)** — +

Receive communications also at

<b>Office number</b>	<b>Ext (optional)</b>	<b>Mobile (optional)</b>	<b>Fax (optional)</b>
(111) 111-1111			

**State (optional)** ⓘ

Search states...

<b>Primary affiliation</b>	<b>Organizational unit</b> ⓘ
	Other (not listed) ×

Part-time/seasonal

**User created by**  
Manager, NAP (123) 456-7890  
qctesterden05@gmail.com

<b>Other organizational unit</b>	<b>Agency</b> ⓘ
	Other (not listed) ×

**Other agency**

Other

**Linked accounts** +

**FAMAuth admin roles** —

Account Manager  
 Approver Manager  
 Helpdesk

**Application and role access** +

**Requests** +

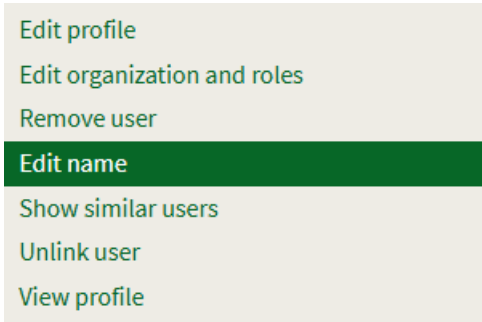
**Rules of behavior** +

**Save** **Cancel**

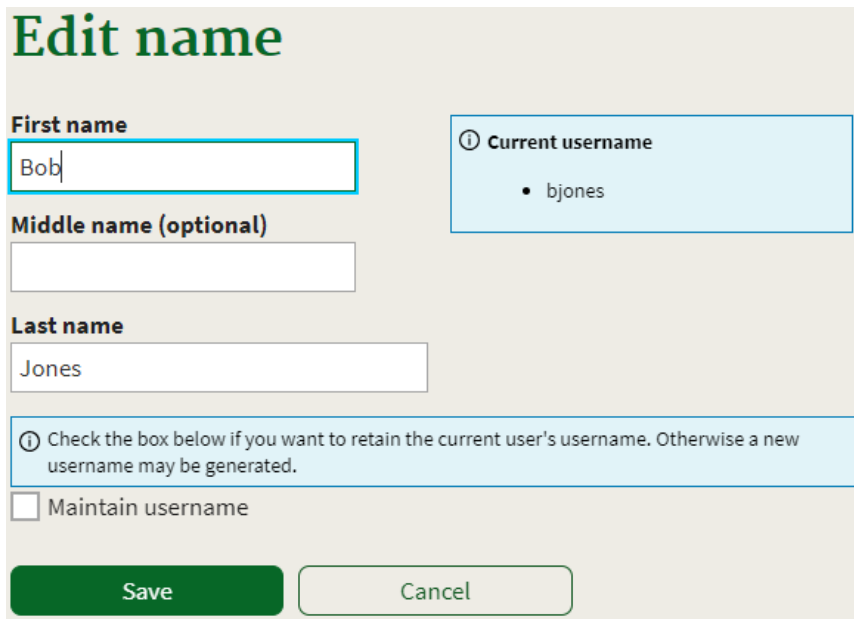
## To edit a User Profile's First, Middle, and/or Last Name

*Changing a user's First, Middle, or Last Name may result in the generation of a new User.*

- 1 On the **Manage Users** grid, select the menu icon for the **User** of your choice, and then click **Edit name**.



- 2 On the **Edit name** page, change the following information as appropriate, and then click the **Next** button
  - First Name
  - Middle Name
  - Last Name

A screenshot of the 'Edit name' form. The form has a title 'Edit name' in green. It contains three input fields: 'First name' with 'Bob', 'Middle name (optional)' which is empty, and 'Last name' with 'Jones'. To the right of the 'First name' field is a box titled 'Current username' containing a list with 'bjones'. Below the input fields is a blue box with an information icon and the text: 'Check the box below if you want to retain the current user's username. Otherwise a new username may be generated.' Below this box is a checkbox labeled 'Maintain username' which is currently unchecked. At the bottom are two buttons: 'Save' (green) and 'Cancel' (white with green border).

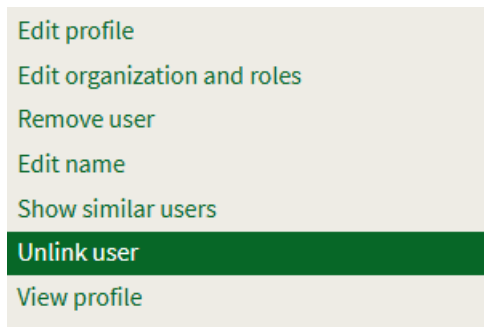
The Maintain Username checkbox allows the Account Manager to determine whether a new username should be generated. When the checkbox is selected a new username will not be generated.

## Unlinking a User from an Identity Provider System

Users may be linked to one or more Identity Provider system. Links may become problematic when users share workstations or when a link becomes stale. To address such problems, the Account Manager may unlink a user from one or more of the Identity Provider Systems. The next time the user attempts to authorize with that Identity Provider System a new link will be created.

### To unlink a user from an Identity Provider System

- 1 On the **Manage Users** grid, select the menu icon for the **User** of your choice, and then click **Unlink user**.



- 2 On the **Unlink user** page, check the box for Login.gov and/or eAuthentication, and then click **Unlink**.

### Unlink user Bob Jones

Please confirm unlinking by selecting from the following identity provider system(s).

Selected	Identity provider system	E-Mail	Identity provider Id
<input type="checkbox"/>	Login.gov	bob.jones@usda.gov	4ca12f39-cdaf-460e-aa1d-ab3f2531b254

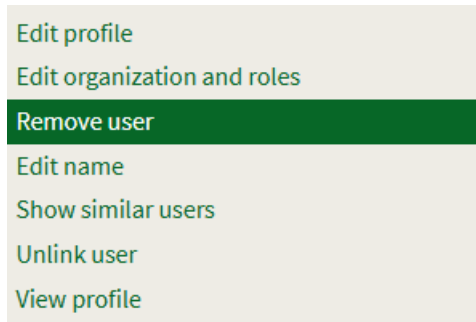
**Unlink**

## Managing the status of a User

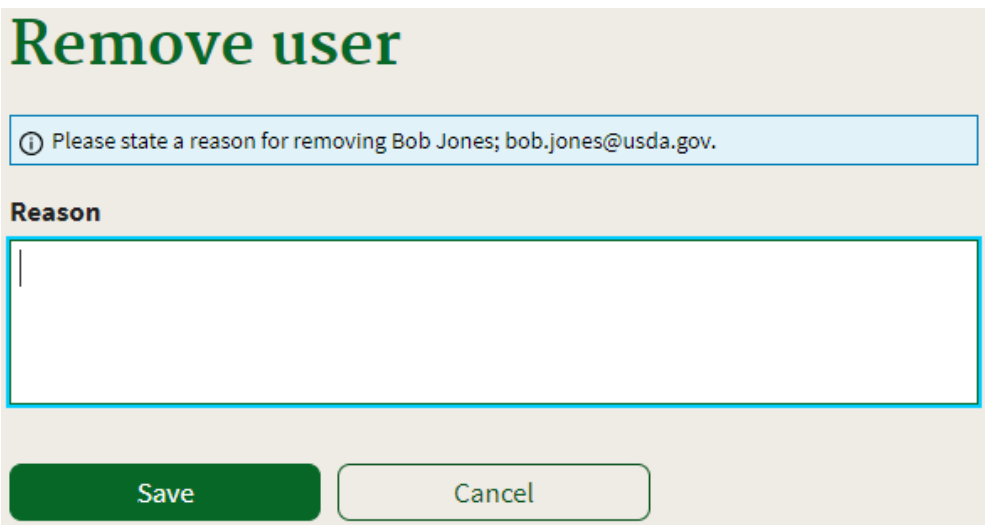
This section explains how to change the User Status of a User, including how to remove, keep disabled, and reactivate the user.

### To remove a User

- 1 On the **Manage Users** grid, select the menu icon for the **User** of your choice, and then click **Remove user**.



- 2 On the **Remove User** page, complete the **Please state a reason for removing user [username]**, and then click the **Save** button.

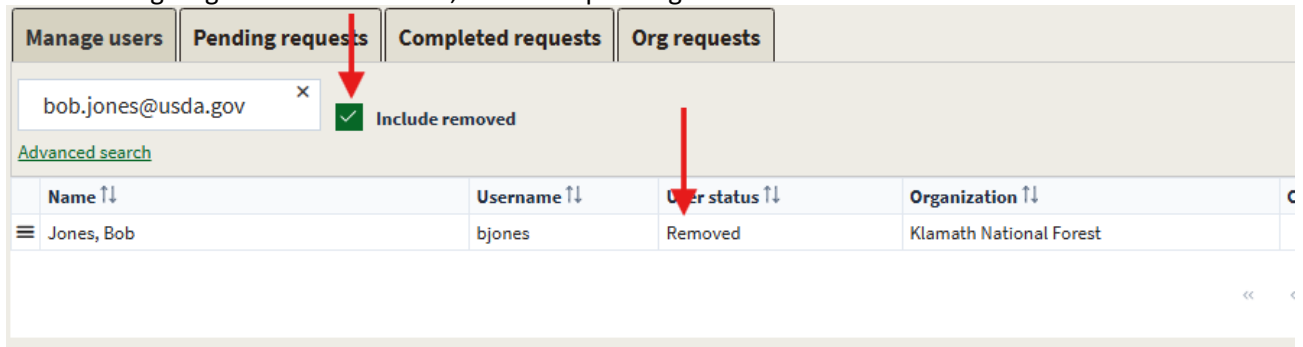


## Remove user

① Please state a reason for removing Bob Jones; bob.jones@usda.gov.

**Reason**

The following diagram shows the User, the arrow pointing to the Removed User Status.



Manage users | Pending requests | Completed requests | Org requests

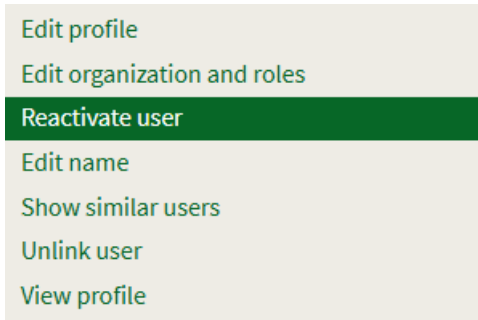
bob.jones@usda.gov  Include removed

[Advanced search](#)

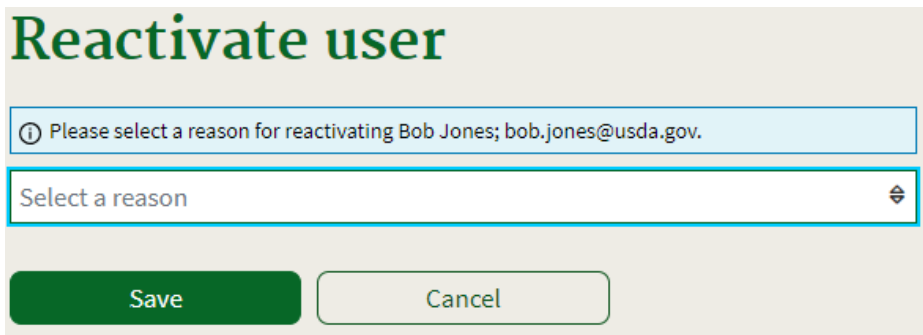
Name ↑↓	Username ↑↓	User status ↑↓	Organization ↑↓
Jones, Bob	bjones	Removed	Klamath National Forest

## To reactivate a User

- 1 On the **Manage users** grid, select the menu icon for the **Removed User** of your choice, and then click **Reactivate user**.



- 2 On the **Reactivate user** page, click the drop-down arrow, click the **Reactivation Reason**, and then click the **Save** button.

A screenshot of the 'Reactivate user' form. The title 'Reactivate user' is at the top. Below it is a text input field with a placeholder: 'Please select a reason for reactivating Bob Jones; bob.jones@usda.gov.'. Below that is a dropdown menu with the text 'Select a reason' and a downward arrow. At the bottom are two buttons: 'Save' (green) and 'Cancel' (white with green border).

## Application Approver Configuration

### *Becoming an Application Approver*

An Account Manager must be designated as an Application Approver to approve, reject or manage access to application(s) and application roles that are not organizational unit-specific. The Approver Manager is responsible for designating an Account Manager as an Application Approver. *Note:* if an application has an organizational unit hierarchy, org unit access and org roles may only be managed by an Org Unit Manager.

To be set up as an Application Approver the Account Manager must contact the Approver Manager and request to be established as an Application Approver.

The user can determine if (s)he would like to receive Email Notification when an application request is created for an application the approver is designated on.

### *Pending Requests grid*

End-users may request access to a FAM application by completing the request form. Once completed, the request is reviewed and approved by an Application Approver.

### To access the User Requests screen

---

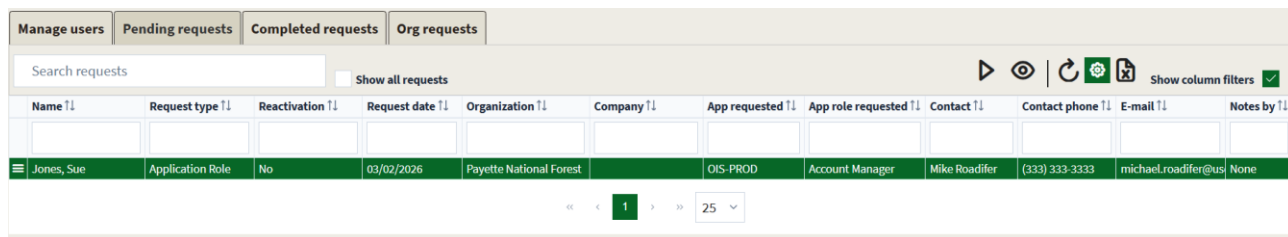
- 1 On the **Navigation Menu**, click the **Users** drop down icon.
- 2 Under the **Users** drop down icon, click the **Pending requests** menu item.
- 3 Select the **Access request** menu item.

## ***Processing a request***

Different types of requests are displayed in the Pending requests grid.:

- New User
- Reactivation
- Application Access
- Application Role

The screen shots below are for processing an Application Role request, but the steps are the same for all types.



Name	Request type	Reactivation	Request date	Organization	Company	App requested	App role requested	Contact	Contact phone	E-mail	Notes by
Jones, Sue	Application Role	No	03/02/2026	Payette National Forest		OIS-PROD	Account Manager	Mike Roadifer	(313) 333-3333	michael.roadifer@us	None

### **To approve and process a request**

- 1 Select the menu icon for the **Request** of your choice, and then click **Process Request**. *Note:* you must be an approver for the application to which access is being requested.
- 2 On the **Process user request** page, verify the **User Information**, select the **Approve** radio button, and then click the **Save** button.

The following diagram shows a sample Process User Request page. The arrows point to the Approve radio button and Save button.

# Process user request



If minor corrections are needed for the user's information, then approve the request and make the corrections on the Manage users screen. Otherwise, reject the request and have the user enter a new, corrected request.

## User information

<b>First name</b> Bob	<b>Middle name</b> 	<b>Last name</b> Jones
<b>Phone</b> (123) 456-7890	<b>E-mail</b> bob.jones@usda.gov	<b>Alternate e-mail(s)</b> 
<b>State</b> California (CA)		
<b>Primary affiliation</b> Federal Government	<b>Organizational unit</b> Klamath National Forest	
<b>Part-time/seasonal</b> No	<b>Agency</b> U.S. Forest Service	

## Pending request

<b>Application requested</b> OIS-PROD	<b>Application role requested</b> Account Manager	<b>Reactivation request</b> No
--	--	-----------------------------------

Show similar users

## Linked accounts

## Identity verification contact

## Application access contact

## Notes

## Action

Approve  Reject  Update request only

Save

Cancel

When approved, the following email notifications are sent from [donotreply@nwcg.gov](mailto:donotreply@nwcg.gov) :

- the verification contact receives an email with the Subject line, “FAMAuth User Created.”  
Subject: FAMAuth User Created

User bjones has been created.

This is an automatically generated message. Please do not reply to this message. Please contact the IIA Helpdesk if this user is not authorized at 866-224-7677.

- the user specified on the Request User page may receive two e-mails to their primary and alternate email addresses:
  - If the user does not have access to FTP or ICBS, the user does not need a password and therefore receives the “Application Access Request Approved” email.

Subject: Application Access for OIS-PROD Approved

Your access request for OIS-PROD is approved.

This is an automatically generated message. Please do not reply to this message.  
<https://famauth-qa.wildfire.gov/index.html>

### To reject an individual request

- 1 Select the menu icon for the **Request** of your choice, and then click **Process Request**.
- 2 On the **Process user request** page, verify the **User Information**, click the **Reject radio** button, enter the **Rejection reason**, select the **Rejection option** (if displayed) and then click the **Save** button.

Rejection options are displayed when the request includes application access to more than one application. The options allow the approver to only reject the application access specified on the selected request, OR, to reject all applications and the user.

The following diagram shows the Process User Request page after clicking the Reject radio button. The arrows point to the Reject action, Reject options, Rejection reason text box and the Save button.

# Process user request



ⓘ If minor corrections are needed for the user's information, then approve the request and make the corrections on the Manage users screen. Otherwise, reject the request and have the user enter a new, corrected request.

User information		
<b>First name</b>	<b>Middle name</b>	<b>Last name</b>
Bob		Jones
<b>Phone</b>	<b>E-mail</b>	<b>Alternate e-mail(s)</b>
(123) 456-7890	bob.jones@usda.gov	
<b>State</b>		
California (CA)		
<b>Primary affiliation</b>	<b>Organizational unit</b>	
Federal Government	Klamath National Forest	
<b>Part-time/seasonal</b>	<b>Agency</b>	
No	U.S. Forest Service	
<b>Pending request</b>		
<b>Application requested</b>	<b>Application role requested</b>	<b>Reactivation request</b>
OIS-PROD	Account Manager	No
<a href="#">Show similar users</a>		
<b>Linked accounts</b> +		
<b>Identity verification contact</b> +		
<b>Application access contact</b> +		
<b>Notes</b> +		
<b>Action</b> -		
<input type="radio"/> Approve <input checked="" type="radio"/> <b>Reject</b> <input type="radio"/> Update request only		
<input type="radio"/> Reject application access request only for OIS-PROD		
<input type="radio"/> Reject user request and ALL requested application access requests		
<b>Rejection reason</b>		
<input type="text"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

When rejected, the user, and the verification contact specified on the Request User page, receive an e-mail with the Subject line, "FAMAuth User Rejected."

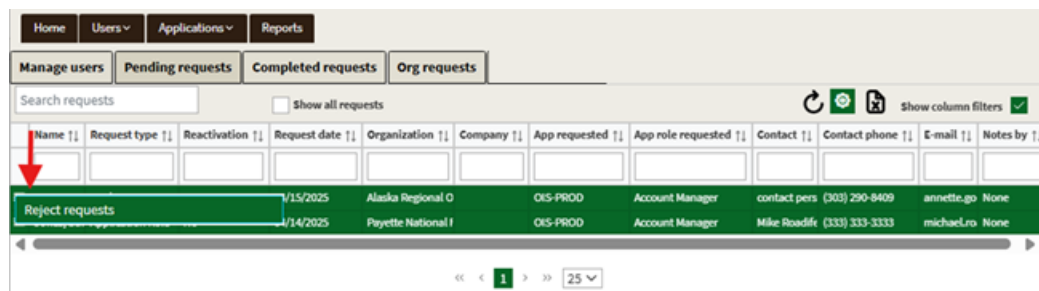
The Rita Requestor user account request has been denied because User guide screenshot.

This is an automatically generated message. Please do not reply to this message.  
<https://famauth-qa.wildfire.gov/index.html>

## Rejecting Multiple Requests at once

Multiple requests can be rejected in one action.

- 1 Select more than one request using the CTRL key. Select the menu icon, and then **Reject requests**.



- 2 On the **Confirm reject requests** page, enter the reason for the rejections and then click the **Confirm** button.

### Confirm reject requests

Please confirm that you want to reject 3 requests.

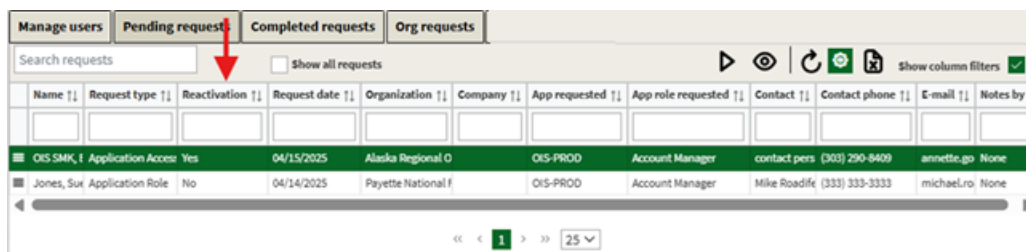
**Rejection Reason**

**Confirm** **Cancel**

All requests in the selection are rejected and the appropriate emails are sent based on the rejected requests' type.

## Reactivating a user via request

Users in the Removed status may submit a request for reactivation. Once submitted, an Application Approver can follow the steps below to complete the reactivation:



- 1 Select the menu icon for the reactivation **Request**, and then click **Process Request**. *Note:* you must be an approver for the application to which access is being requested.
- 2 On the **Process user request** page, verify the **User Information**, select the **Approve** radio button, and then click the **Save** button.

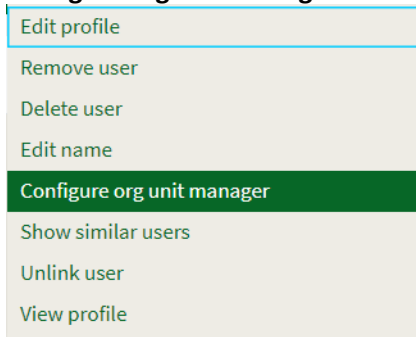
The selected request is approved, and the appropriate emails are sent based on the reactivation request type.

## ***Assigning an Org Unit Manager to an Org Unit***

An Org Unit Manager is a user with an application role that is mapped to the Manage Org Unit operation. An Org Unit Manager can grant and remove users' org unit access and org roles to/from applications that are Org unit-specific. In addition to having the application role that is mapped to the operation, an Application Approver must configure which Org Unit(s) the Org Unit Manager manages.

### **To configure which Org unit(s) an Org Unit Manager can manage**

- 1 On the **Manage Users** grid, select the menu icon for the **User** of your choice, and then click **Configure org unit manager**.



- 2 On the **Configure org unit manager** page, locate the **Assign managed org unit(s)** panel.
  - 3 In the **Application** field search for and select the application to which the org unit access applies.
  - 4 In the **Org unit** field search for and select the org unit that the org unit manager will manage access to.
  - 5 If the Org unit Manager does not want to receive emails each time a request for an org role to the designated org unit is created, deselect the **Notify** checkbox in the **Org request e-mail notifications panel**.
  - 6 If the Org unit Manager will manage access and org roles to another org unit, use the **+** to add another instance of the Application and Org unit fields and repeat these steps.
-

## Configure org unit manager

<b>User information</b>	+
<b>Org unit request e-mail notifications</b>	-
<input type="checkbox"/> Notify Bob Jones	
<b>Assign managed org unit(s)</b>	-
<p><b>Application</b></p> <p>WILDCADE-WildCAD-E <span>⊕</span> <span>⊖</span></p> <p><b>Org unit</b></p> <p>Select managed org unit... <span>×</span></p>	
<p><b>Save</b> <b>Cancel</b></p>	

### Deleting a user

An Application Approver can delete a user if they are an approver for all of the application(s) the user has access to. When a user is deleted all information about the user is removed.

#### To delete a user

- 1 On the **Manage Users** grid, select the menu icon for the **User** of your choice, and then click **Delete user**.

Edit profile
Remove user
<b>Delete user</b>
Edit name
Show similar users
Unlink user
View profile

- 2 On the **Confirm delete user** dialog, select the **Reason** for the deletion. If Other is selected, enter text in the Other reason box.
- 3 Select **Confirm**.

## Confirm delete user

**ⓘ** This action cannot be undone. Please confirm the permanent deletion of Bob Jones; bob.jones@usda.gov.

**Reason**

Select reason ⊕

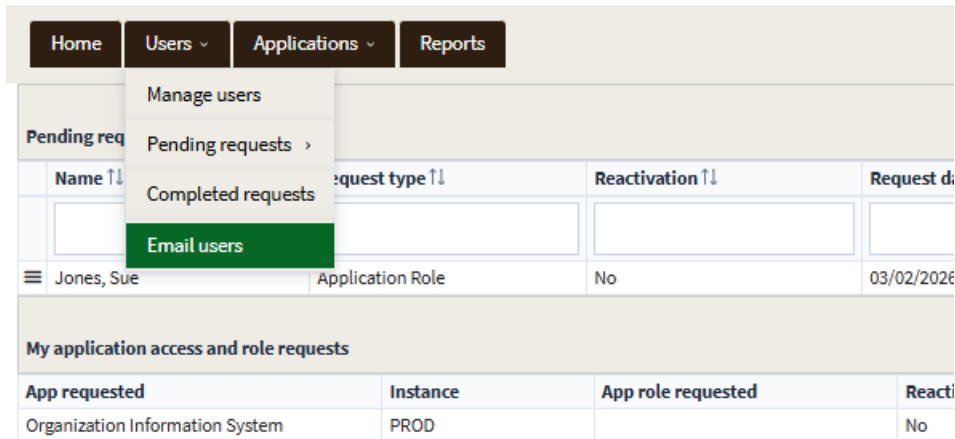
**Confirm** **Cancel**

## Emailing application users

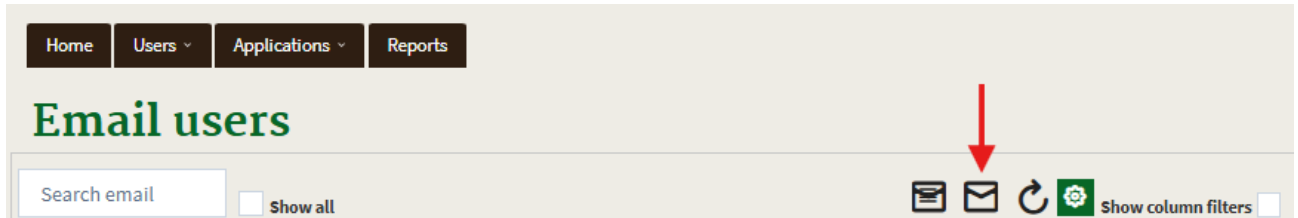
An Application Approver can generate an email to all users of one or more applications that the approver configured for.

### To email application users

- 1 From the Users menu, select the **Email users** menu item

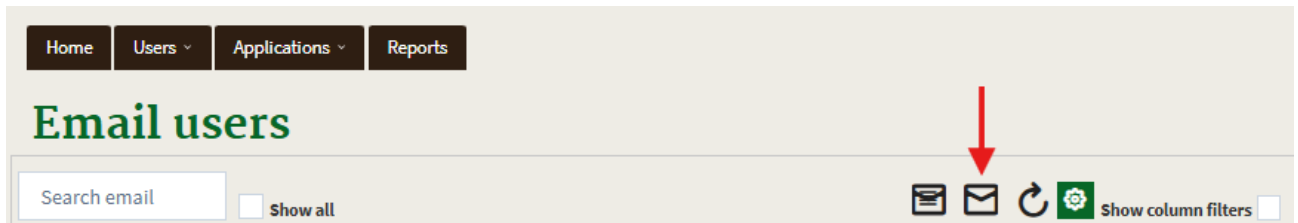


- 2 On the **Email users** screen, click the **Send a new email** button indicated by the red arrow.



- 3 On the **New email to application users** screen, ensure the **By application** radio button is selected. From the **To** dropdown checklist, select one or more of the applications for which you are an approver.
- 4 Enter a **Subject**.
- 5 Enter the text of the Email. The default text is pre-populated in the Email field and may be edited/removed by the email author.
- 6 Optionally add an attachment. Attachments may be of type pdf, docx, png, xlsx and cannot exceed 20 MB.
- 7 Select **Submit**. The email is sent to each non-removed unique user with access to at least one of the applications selected in the **To** checklist. The email is sent to the user's primary email address and any applicable alternate email addresses.





- 3 On the **New email** screen, select the **By application role** radio button. From the **To** dropdown checklist, select the application for which you are an approver.
- 4 From the **Select roles** dropdown checklist, select one or more application roles.
- 5 Enter a **Subject**.
- 6 Enter the text of the Email. The default text is pre-populated in the Email field and may be edited/removed by the email author.
- 7 Optionally add an attachment. Attachments may be of type pdf, docx, png, xlsx and cannot exceed 20 MB.
- 8 Select **Submit**. The email is sent to each non-removed unique user with access to at least one of the application roles selected in the **Select roles** checklist. The email is sent to the user's primary email address and any applicable alternate email addresses.

**New email to application users**

Select recipients

By application

By application role

📄 Email will be sent to users with the selected application and roles.

To

Select application

Select roles

Select application roles

From

donotreply@mail.nwcg.gov

Subject

[Add attachments](#)

Email

Sans Serif Normal

B I U G A [list] [list] [list] [list]

Submit Send a test email Cancel

# Working with grids

This section explains how to organize and display information on the Manage Users grid and on the Pending requests grid. It also explains how to use the menu to perform User Management functions. Topics include:

- Customizing the appearance of a grid
- Using shortcuts.

## Customizing the appearance of a grid

You can perform a variety of actions to tailor the appearance of the Manage Users and Pending request grids, including how to:

- list columns in alphabetical order
- reorder columns
- perform a search
- resize columns.

---

*You may find many other ways to customize the appearance of a grid on the User Management screen.*

---

### To list column contents in alphabetical order

---

*The sample screens in this task show how to alphabetize the Username column.*

---

- 1 Using your mouse, point to, and then click and hold the **Column Heading** of your choice.
- 2 Click the **Column Heading** of your choice.

The following diagram shows the Manage Users grid. The arrow points to the highlighted Username column.

Name	Username	User status	Organization	Company	Affiliation	Office number	Primary e-mail	Linked account	User created by	Last authorized
Smith, Connor	csmith	Active		SAIC	Contractor/Ve	(814) 322-7641	connor.e.smith@sa	Login.gov	Roadifer, Mike	03/06/2026 09:58
Smith, George	gsmith	Active	Washington Office		Federal Govern	(708) 908-2201	george.smith@usd	eAuthentication	Manager N&P	02/20/2026 09:45

### To change the order of columns in the grid

---

*The sample screens in this task show how to move a column using a drag-and-drop operation.*

---

- 1 Using your mouse, point to, and then click and hold the **Column Heading** of your choice.
  - 2 Drag the selected column to the position immediately to the left of the desired location, and then release.
-

The following diagram shows the Organization column selected by the mouse and the drag-and-drop operation to move the Organization column after the Affiliation column.

Name	Username	User status	Organization	Company	Affiliation	Office number	Primary e-mail	Linked account	User created by	Last authorized
Smith, Connor	csmith	Active		SAIC	Contractor/Ve	(814) 322-7641	connor.e.smith@sa	Login.gov	Roadifer, Mike	03/06/2026 09:58
Smith, George	gsmith	Active	Washington Office		Federal Govern	(208) 908-2201	george.smith@usdi	eAuthentication	Manager, NAP	02/20/2026 09:45
Smith, Joseph	jsmith	Active		Synergy BIS	Contractor/Ve	(717) 331-0976	joseph.smith5@usc	eAuthentication	Roadifer, Mike	02/20/2026 09:45

The following diagram shows the resulting Manage Users grid.

Name	Username	User status	Company	Affiliation	Organization	Office number	Primary e-mail	Linked account	User created by	Last authorized
Smith, Connor	csmith	Active	SAIC	Contractor/Ve		(814) 322-7641	connor.e.smith@sa	Login.gov	Roadifer, Mike	03/06/2026 09:58
Smith, George	gsmith	Active		Federal Govern	Washington Office	(208) 908-2201	george.smith@usdi	eAuthentication	Manager, NAP	02/20/2026 09:45
Smith, Joseph	jsmith	Active	Synergy BIS	Contractor/Ve		(717) 331-0976	joseph.smith5@usc	eAuthentication	Roadifer, Mike	02/20/2026 09:45

### To change the width of a column

- 1 Using your mouse, rest the pointer on the right of the **Column Boundary** you want to change until it becomes a resize cursor.
- 2 Click and hold the **Column Boundary**, drag to the desired width, and then release.

## Generate Reports

FAMAuth Admin users can generate content in a grid that allows them to monitor and assess FAMAuth Admin data to support their operations and oversight.

### To generate a report

- 1 On the FAMAuth Admin navigation menu, click the Reports tab.

Home Users Applications Reports

FAMAuth admin roles audit (RPT-01)  
Non-privileged account review (RPT-02)  
Authorization history (RPT-03)  
User status (RPT-04)  
Application users (RPT-05)  
Org units and org unit managers (RPT-06)  
Org units with no managers (RPT-07)  
Org units and org unit users (RPT-08)  
Org units with no users (RPT-09)  
Org roles by user (RPT-10)  
Pending IROC vendor requests (RPT-11)

### FAMAuth admin roles audit (RPT-01) i

Org / company(optional)

Role (optional)

Generate report

Clear filters

Show column filters

Last name ↑↓	First name ↑↓	Middle name ↑↓	Org/company ↑↓	Primary affiliation ↑↓	Primary email ↑↓	Job title ↑↓
--------------	---------------	----------------	----------------	------------------------	------------------	--------------

Total records: 0 of 0 << < > >> 25

- 2 Select a report from the report menu on the left panel. You can hide the report menu by clicking on the “Hide reports menu button”; bring back the reports menu by clicking on the “show reports menu button”.
- 3 Clicking on the Information button shows a report’s description, click on the x to hide the description text.
- 4 If the report has filtering parameters you can select options from dropdown lists, checkboxes, or autocomplete suggestions.
- 5 Click the “Generate report” button to populate the grid with the selected report content. Changing the filters does not automatically regenerate the content in the grid.
- 6 Follow the Working with grids guide in this document.