FAMAuth
Administration Guide

Revision Log

Rev #	Date	Revision(s)	Author
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

Document Scope

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

- Understanding Users
- Actions permitted by an Account Manager
- Actions permitted by an Application Approver
- Actions permitted by a Password Reset Manager
- 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 FAMAuth Admin. Access to a function can be provided in one of two ways:

1. User is assigned a FAMAuth Admin Role.

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

The following matrix explains how administrative functions are assigned:

This administrative function:	Comes with this role:	Additional configuration required:	This function may be mapped to FAM Application role(s):	Notes:
Reset Password	Password Reset	None	N	
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	

This administrative function:	Comes with this role:	Additional configuration required:	This function may be mapped to FAM Application role(s):	Notes:
Reactivate User	Account Manager	None	N	
Unlink User	Account Manager	None	N	
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	

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:

- Retrieve their forgotten FAMAuth Username, if they are a password user
- Reset their FAMAuth Password, if they are a password user
- 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 FAMAuth Admin

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

Applications that reside in FAMAuth Admin

- Data Warehouse
- e-ISuite Enterprise
- EGP – Enterprise Geospatial Portal
- F&AM – FTP Site
- 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.
- **Temporary Password**. If the user has access to FTP or ICBS the user is issued a Temporary Password when the user is approved or when the password has been reset. Temporary Passwords must be reset prior to accessing the environment and / or applications.
- **Expired Password–** If the user has access to FTP or ICBS, the user's password expires 60 days from last

password change. The User is not able to access the environment due to password expiration. Access to the environment can be attempted only after resetting the Password.

- **Disabled –** If the user has access to FTP or ICBS, the user is disabled 180 days from last login. The User is not able to access the environment and must be reactivated by an Account Manager. A user is disabled for one of the following reasons:

  - The User has been inactive for 180 days
  - The User is temporarily not needed and expected to be reactivated and used in the future, such as for seasonal workers.

- **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

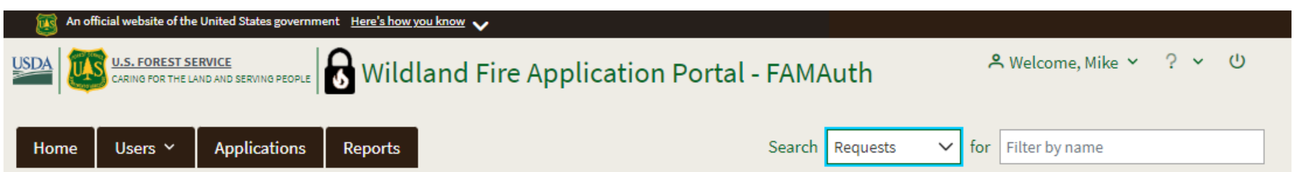
The **Navigation Menu** allows administrators to access data grids and take certain actions.

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

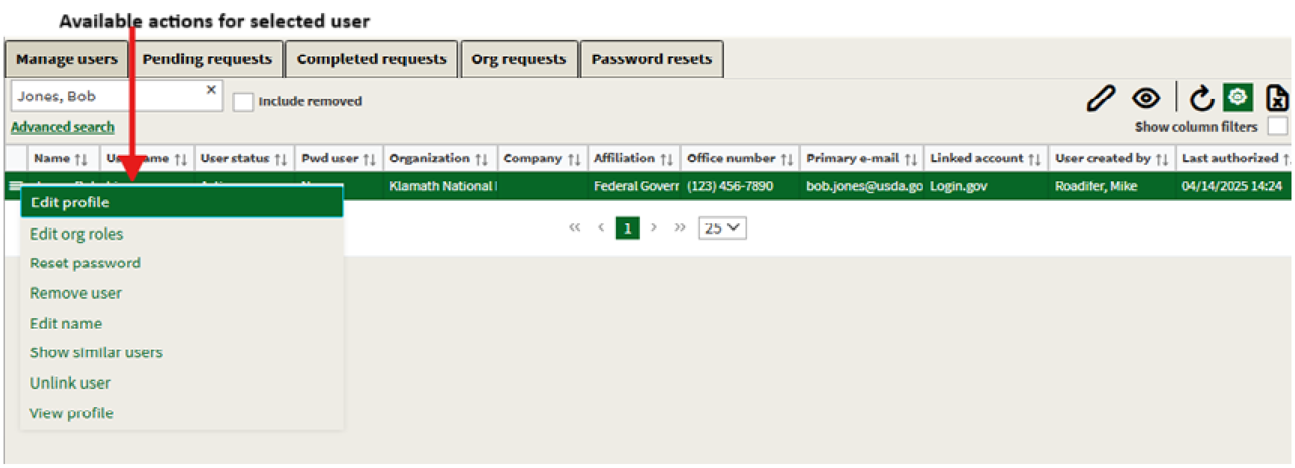
This **Manage users** grid allows account managers to search for users and take perform administrative functions.

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

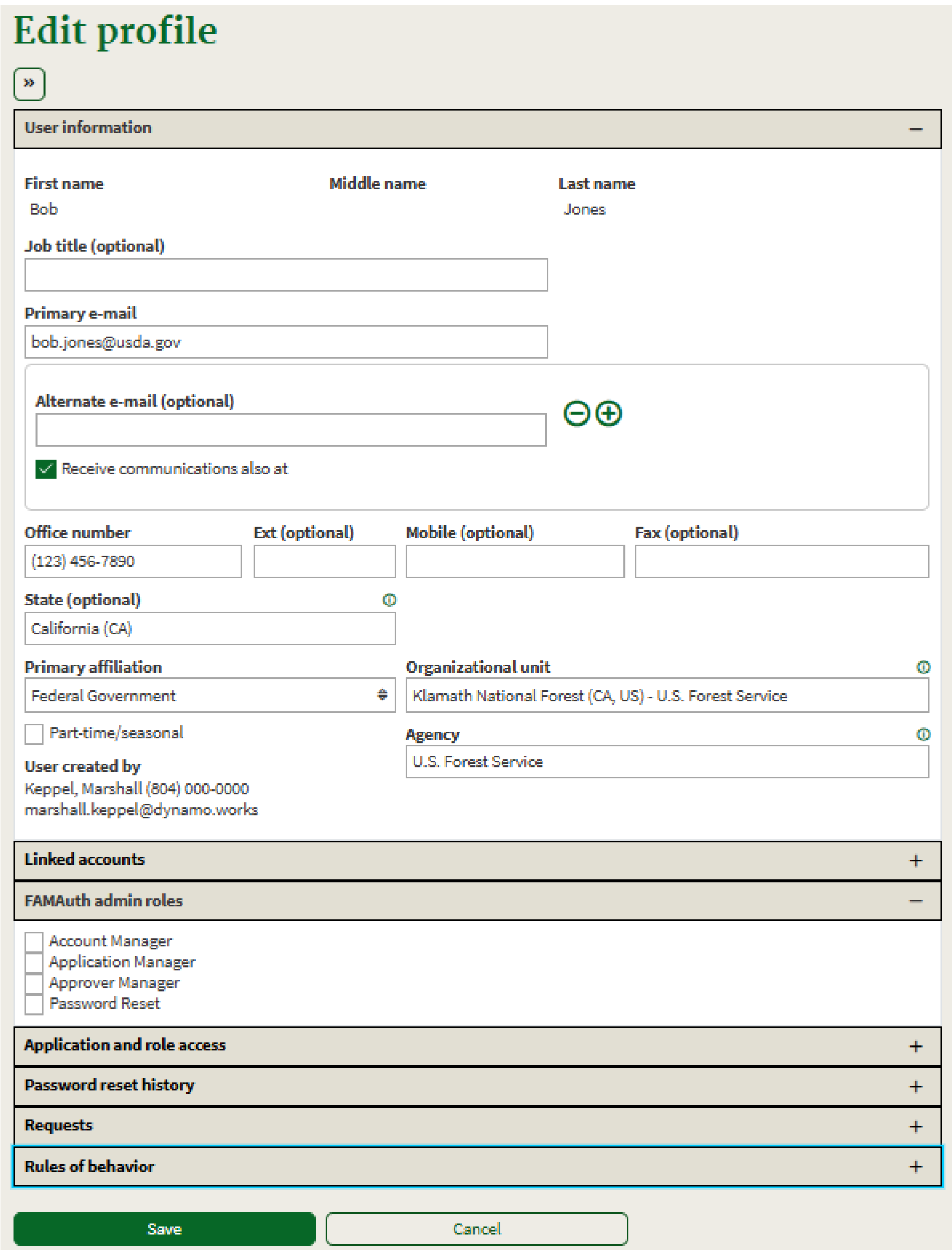


Editing User Profile information

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.

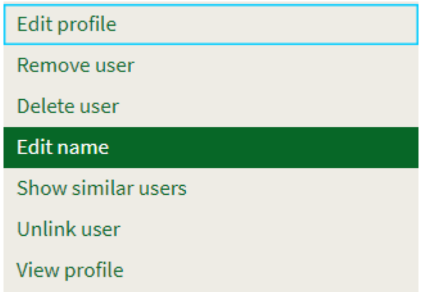
The following diagram shows the Edit profile page. The arrows point to some of the user information available for editing.



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

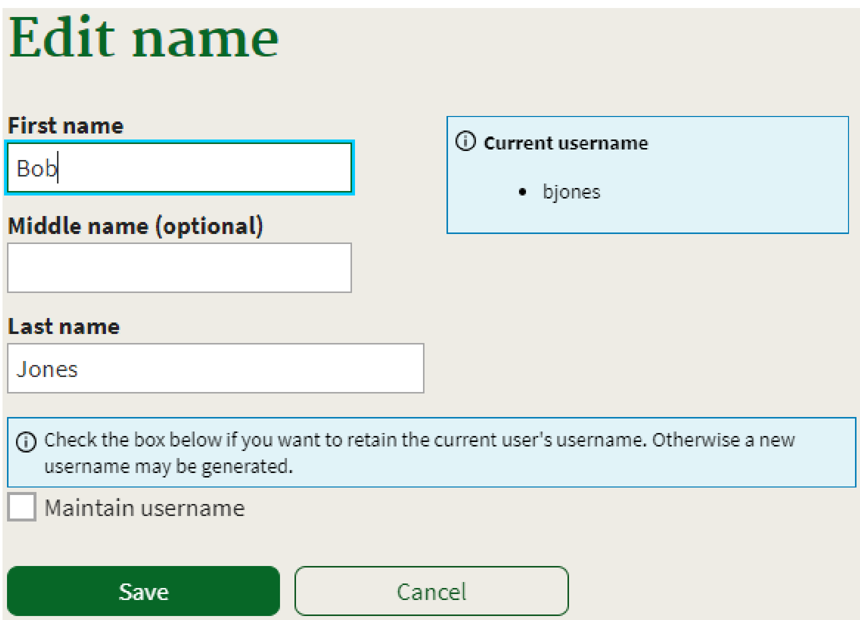
Changing a user's First, Middle, or Last Name may result in the generation of a new User.

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.



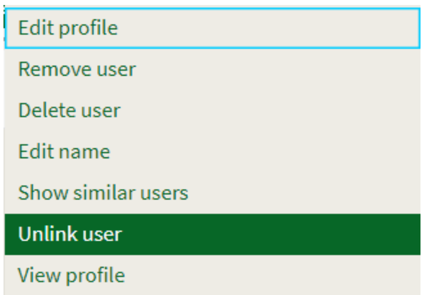
The Maintain Username checkbox allows the Account Manager to determine whether a new username should be generated. When the checkbox is selected a new username will not be generated.

Unlinking a User from an Identity Provider System

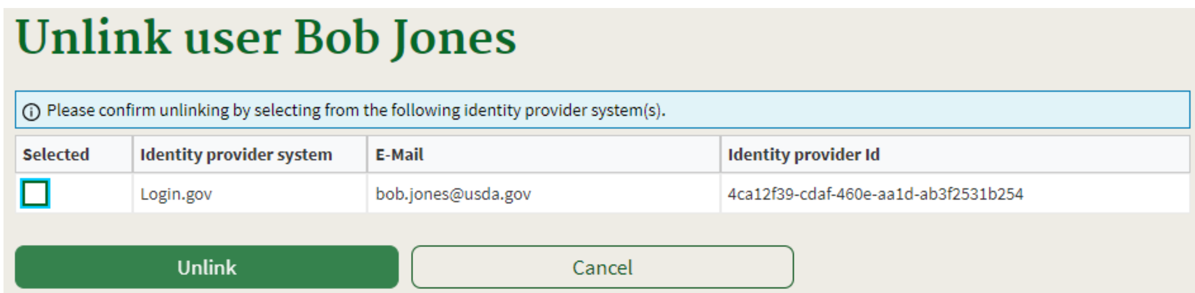
Users may be linked to one or more Identity Provider system. Links may become problematic when users share workstations or when a link becomes stale. To address such problems, the Account Manager may unlink a user from one or more of the Identity Provider Systems. The next time the user attempts to authorize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

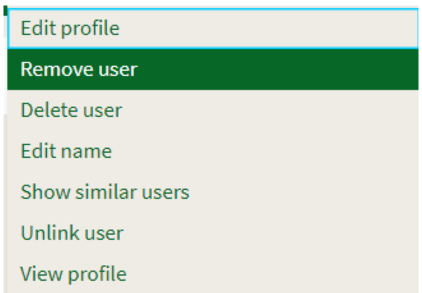


Managing the status of a User

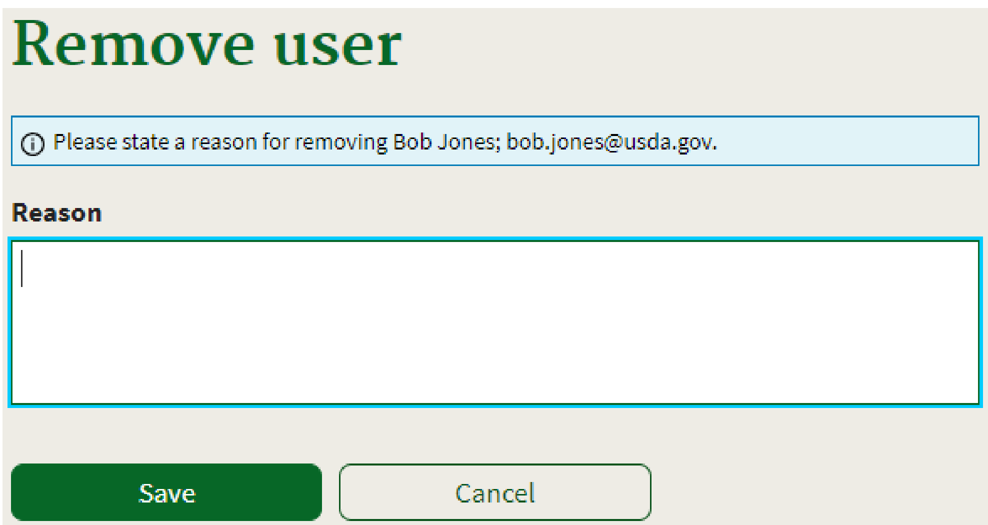
This section explains how to change the User Status of a User, including how to remove, keep disabled, and reactivate the user.

To remove a User

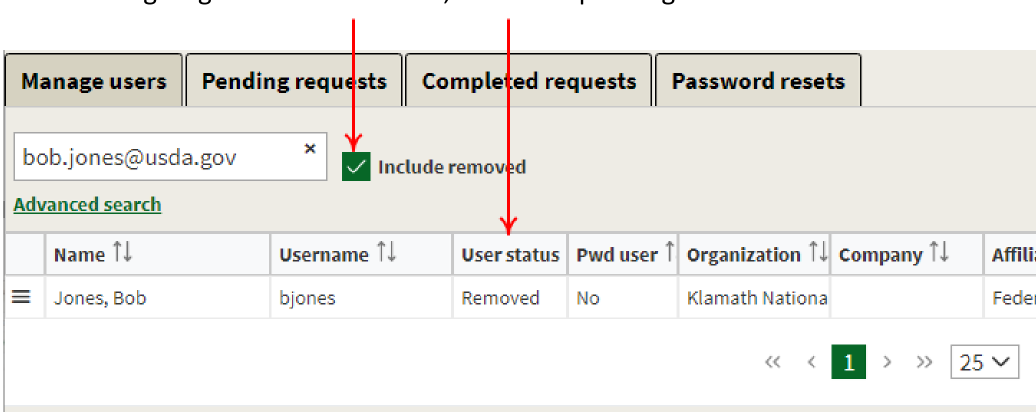
1 On the **Manage Users** grid, select the menu icon for the **User** of your choice, and then click **Remove user**.



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



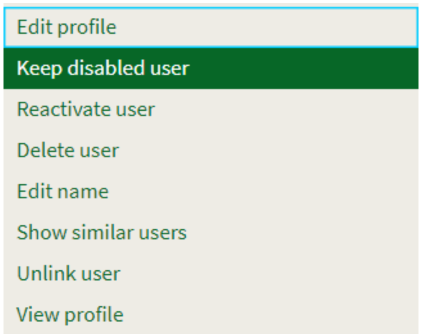
The following diagram shows the User, the arrow pointing to the Removed User Status.



To maintain a disabled User

Keep a User disabled when the user is temporarily not needed, but is expected to be reactivated and used in the future, such as for a seasonal worker.

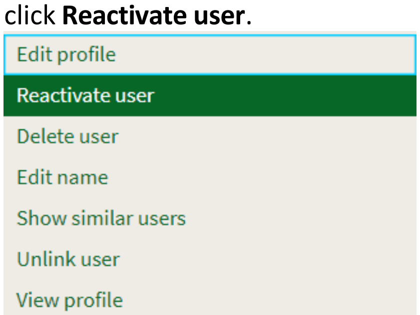
1 On the **Manage users** grid, select the menu icon for the **Disabled User** of your choice, and then click **Keep disabled user**.



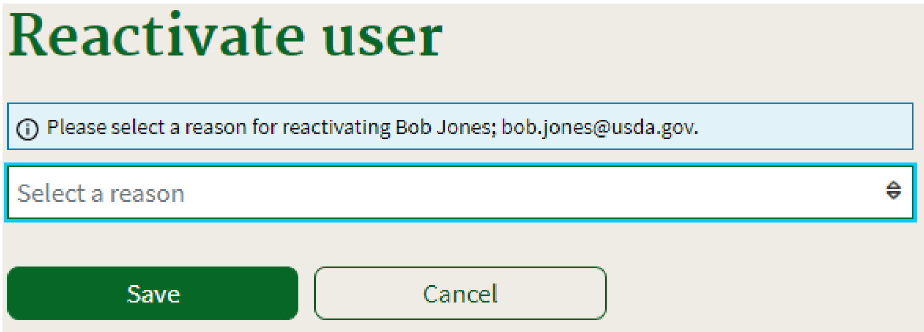
2 Click the drop-down arrow, click the **Justification**, and then click the **Save** button.

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.



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.

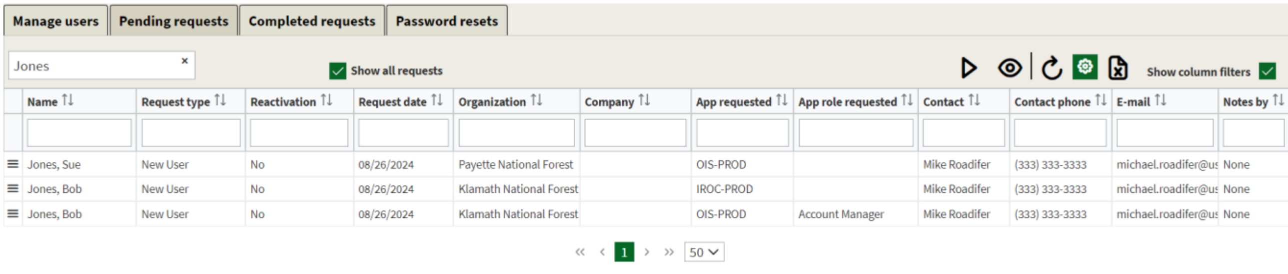
3 Select the **Access request** menu item.

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 a New User request, but the steps are the same for all types.



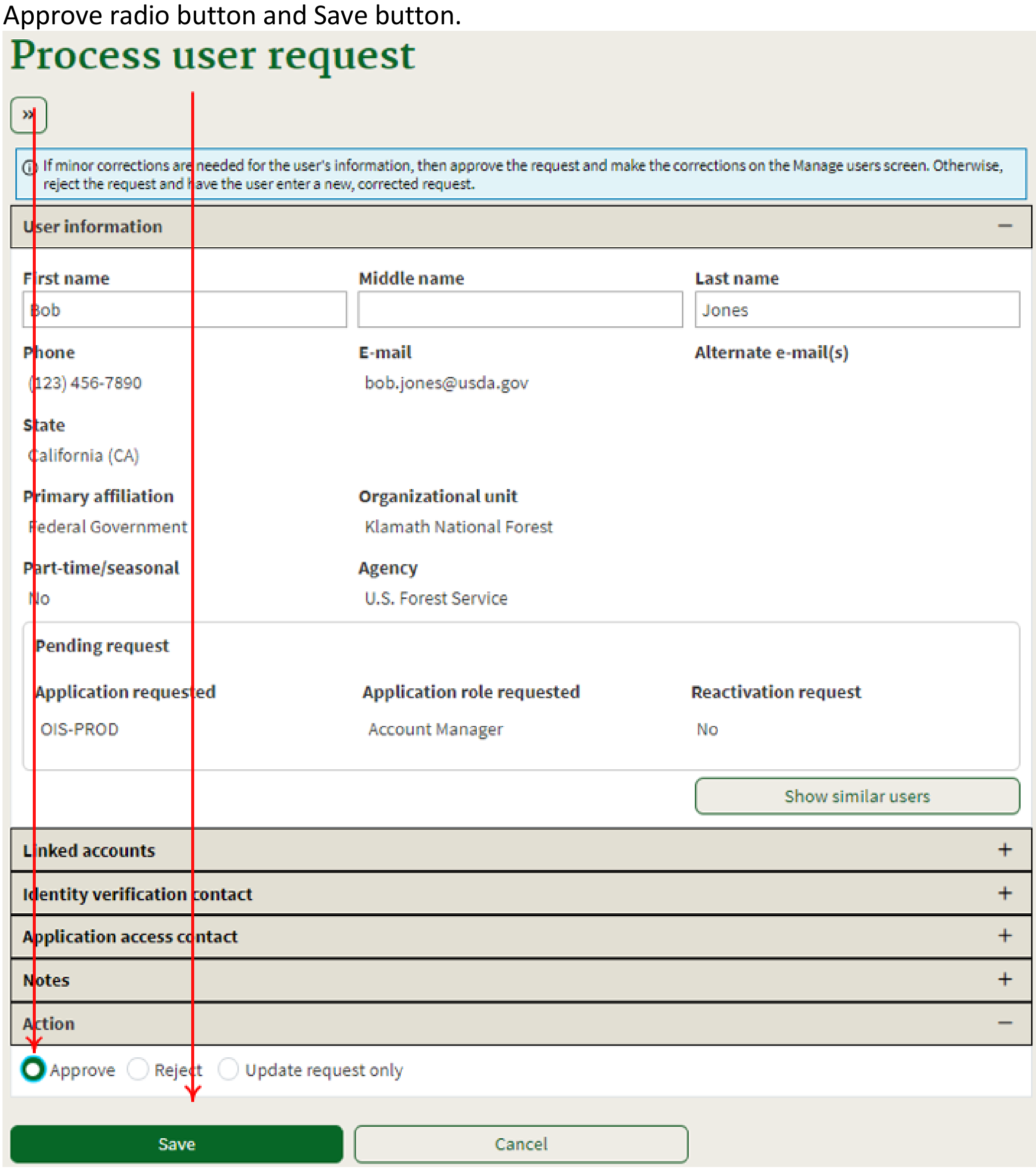
Name	Request type	Reactivation	Request date	Organization	Company	App requested	App role requested	Contact	Contact phone	E-mail	Notes by
Jones, Sue	New User	No	08/26/2024	Payette National Forest		OIS-PROD		Mike Roadifer	(333) 333-3333	michael.roadifer@us	None
Jones, Bob	New User	No	08/26/2024	Klamath National Forest		IROC-PROD		Mike Roadifer	(333) 333-3333	michael.roadifer@us	None
Jones, Bob	New User	No	08/26/2024	Klamath National Forest		OIS-PROD	Account Manager	Mike Roadifer	(333) 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.



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

  - If the user has access to FTP or ICBS the user needs a password and therefore receives two e-mails with the Subject line, "FAMauth User Information." One e-mail identifies the new User Name. The other identifies the temporary Password. The user also receives the "Application Access Request Approved" email for the application access, and "Application Role Request Approved" for each application role.

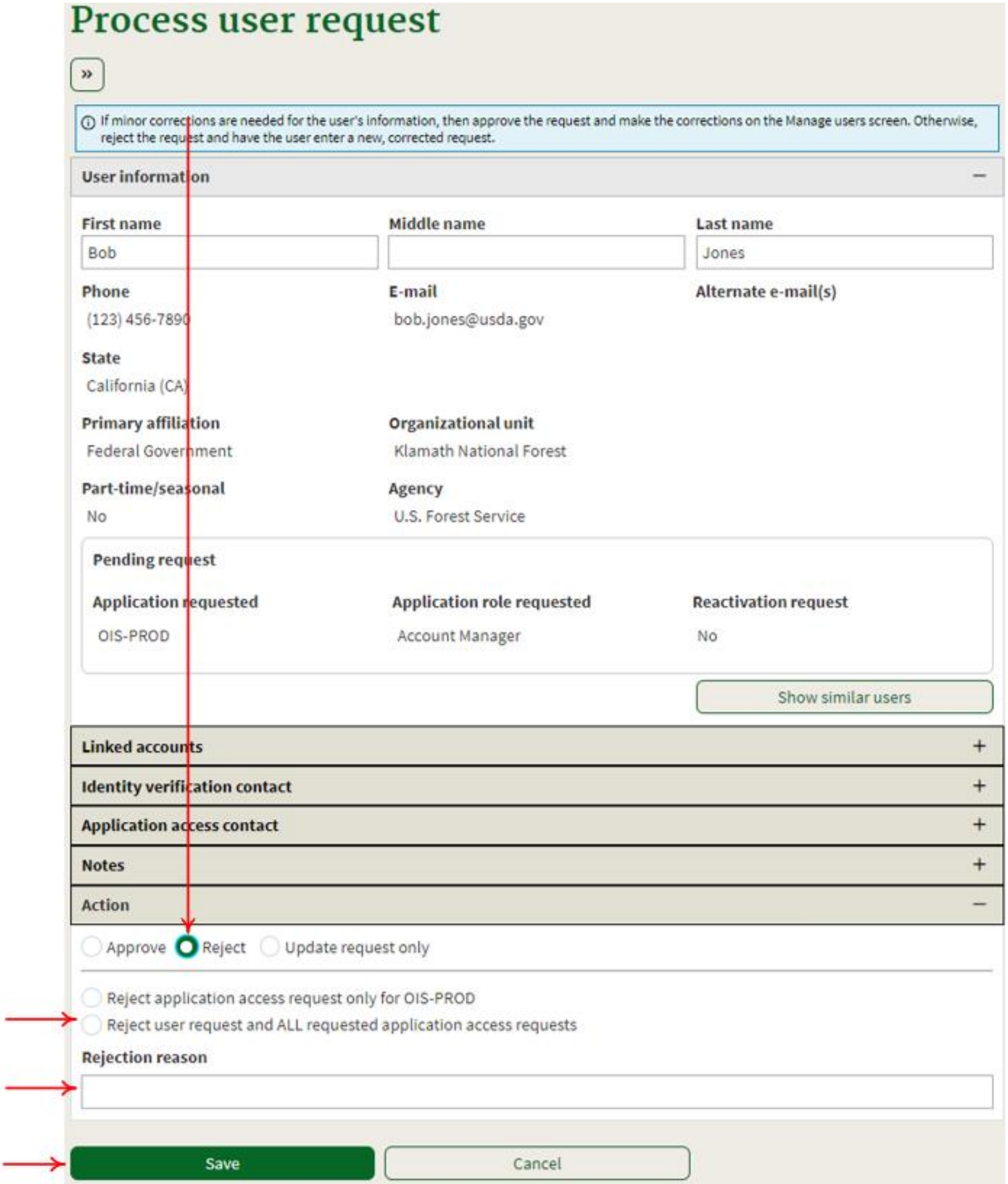
    > Your role request for Generic Role for QCHONE-A1H1 is approved.
    >
    > This is an automatically generated message. Please do not reply to this message.
    > https://famauth-qa.wildfire.gov/index.html

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.



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.”

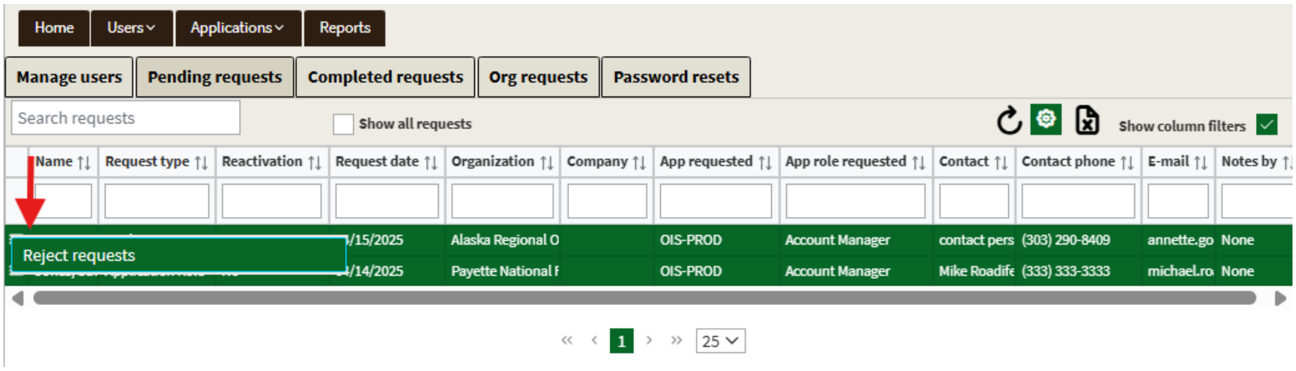
The Rita Requestor user account request has been denied because User guide screenshot.

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

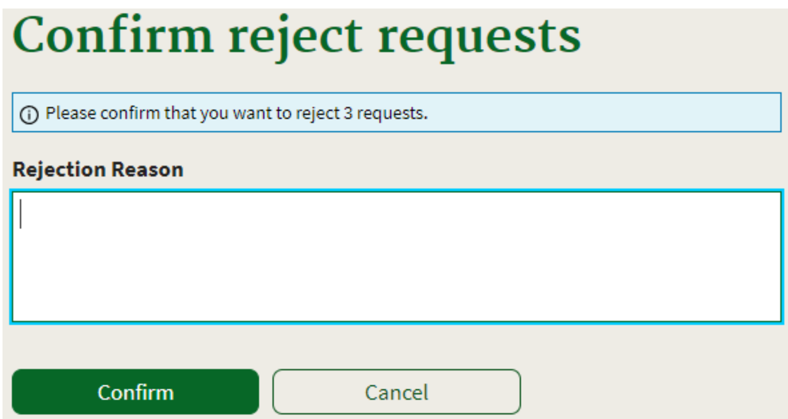
Rejecting Multiple Requests at once

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**.



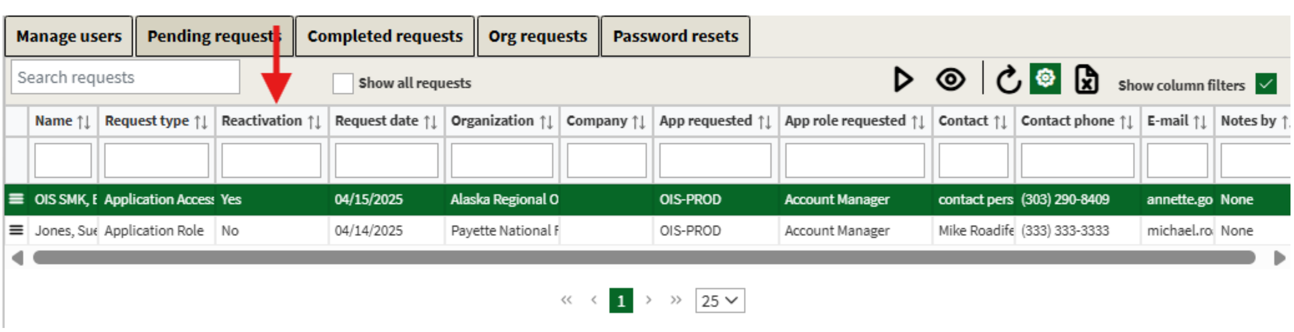
2 On the **Confirm reject requests** page, enter the reason for the rejections and then click the **Confirm** button.



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.

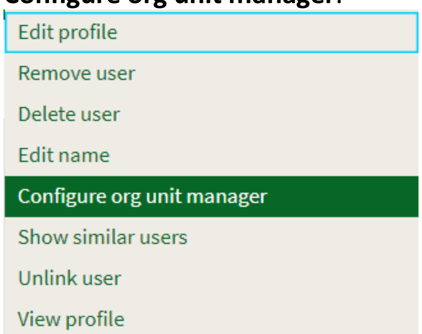
The selected request is approved, and the appropriate emails are sent based on the reactivation request type.

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**.



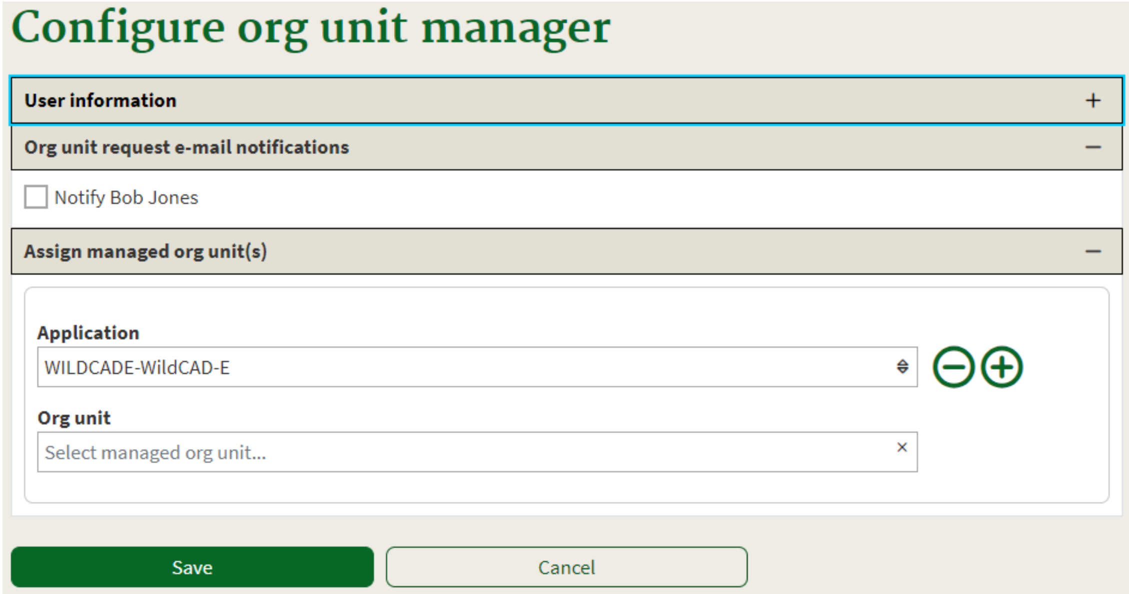
2 On the **Configure org unit manager** page, locate the **Assign managed org unit(s) panel**.

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.

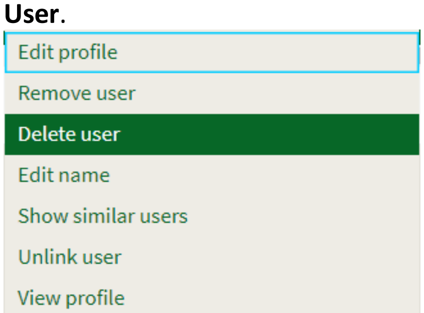


Deleting a user

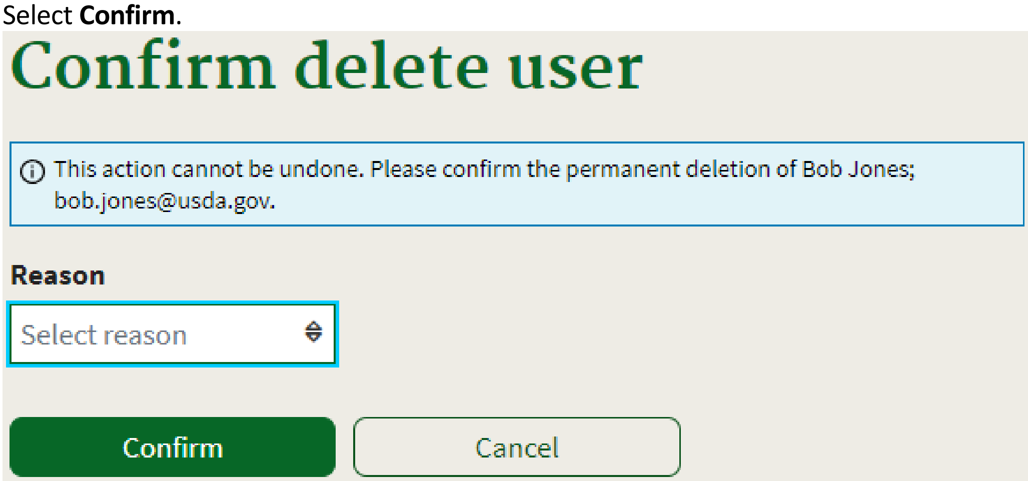
An Application Approver can delete a user if they are an approver for all of the application(s) the user has access to. When a user is deleted all information about the user is removed.

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**.



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**.

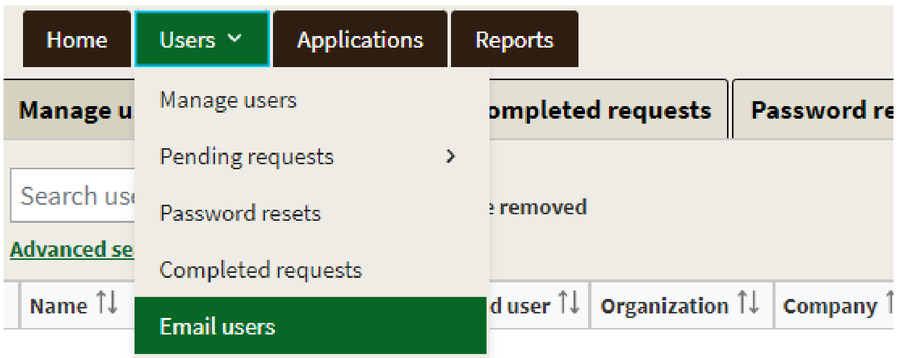


Emailing application users

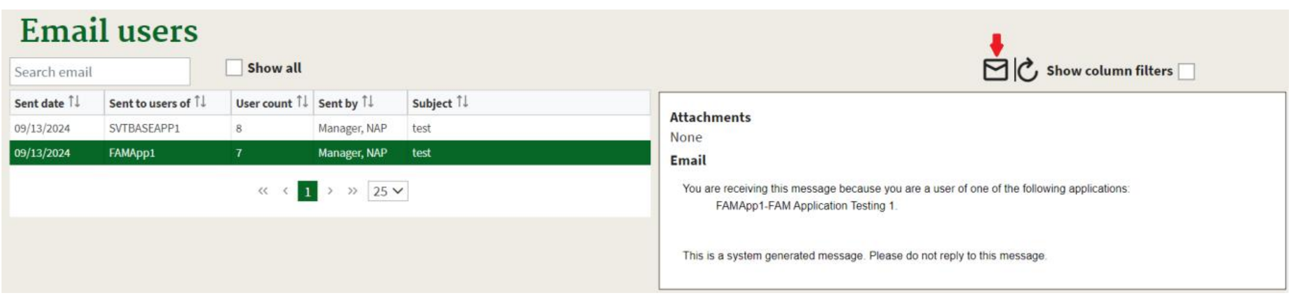
An Application Approver can generate an email to all users of one or more applications that the approver configured for.

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.



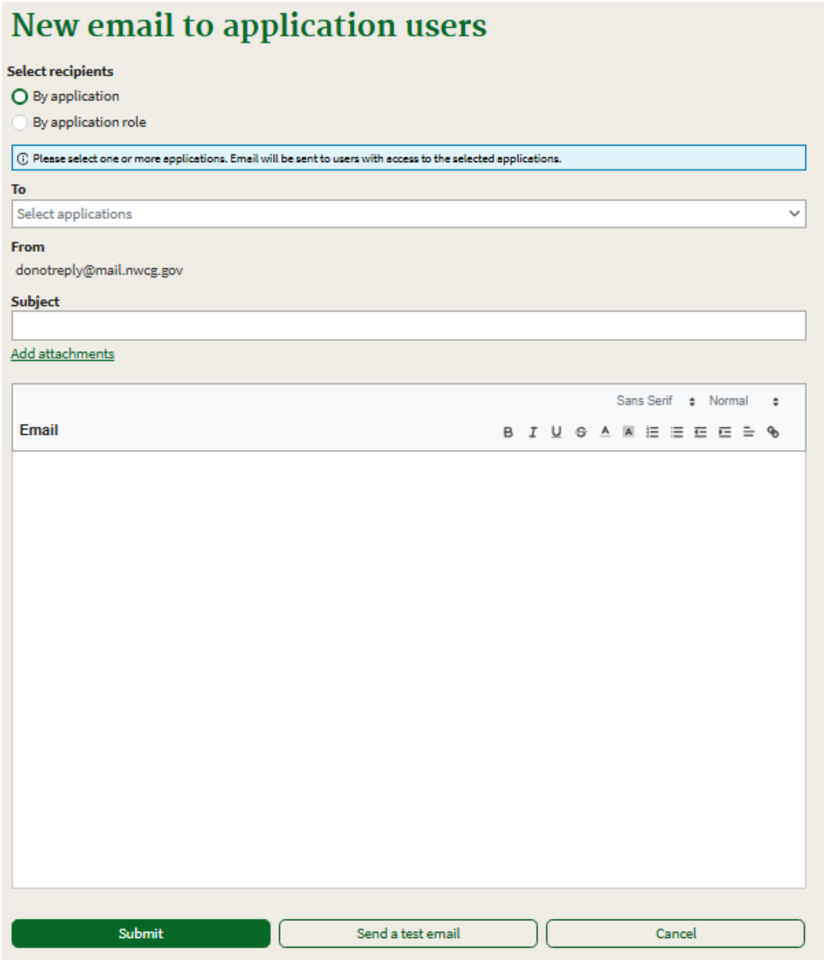
3 On the **New email to application users** screen, ensure the **By application** radio button is selected. From the **To** dropdown checklist, select one or more of the applications for which you are an approver.

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 pay be of type pdf, docx, png, xlsx and cannot exceed 20 MB.

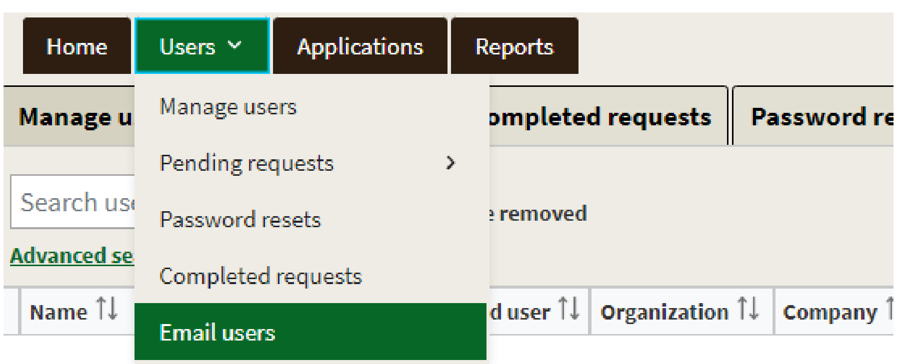
7 Select **Submit**. The email is sent to each non-removed unique user with access to at least one of the applications selected in the **To** checklist. The email is sent to the user's primary email address and any applicable alternate email addresses.



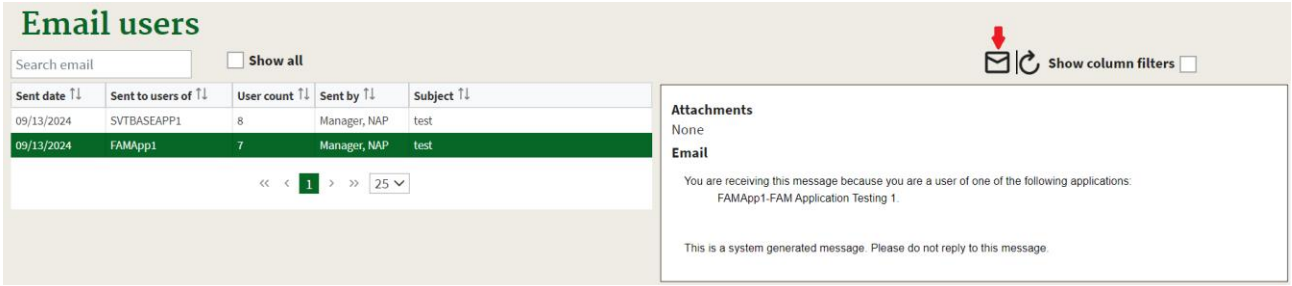
An Application Approver can also generate an email to users by application role for an application that the approver is configured for.

To email application users by role

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** screen, select the **By application role** radio button. From the **To** dropdown checklist, select the application for which you are an approver.

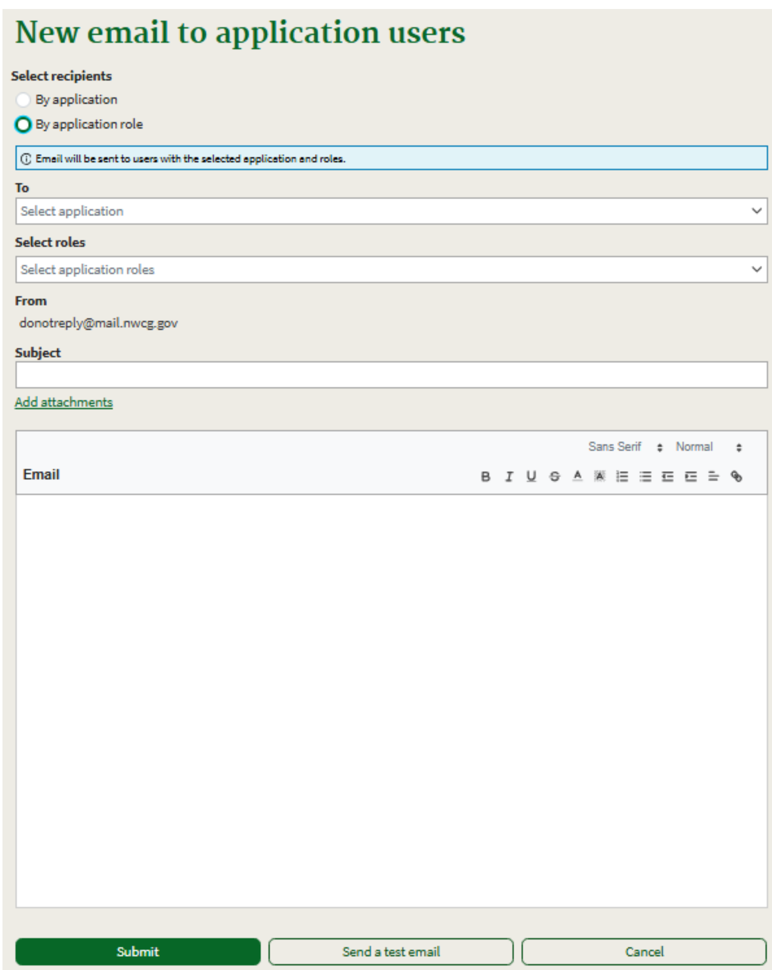
4 From the **Select roles** dropdown checklist, select one or more application roles.

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 pay 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.

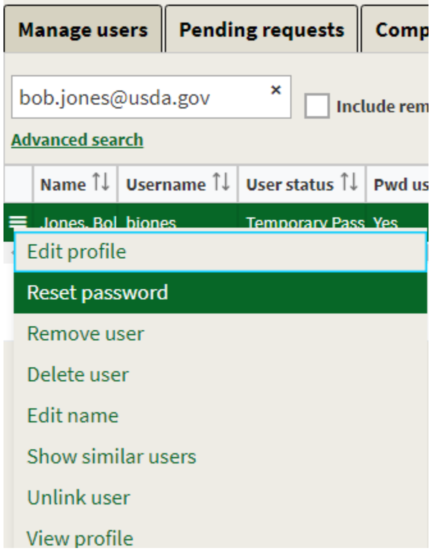


Password Reset Manager Role

To reset a Password, the user must have the **Password Reset Manager** role

1 On the **Manage Users** grid, search for the **User** of your choice.

2 Select the menu icon on the **User**, and then click **Reset Password**.

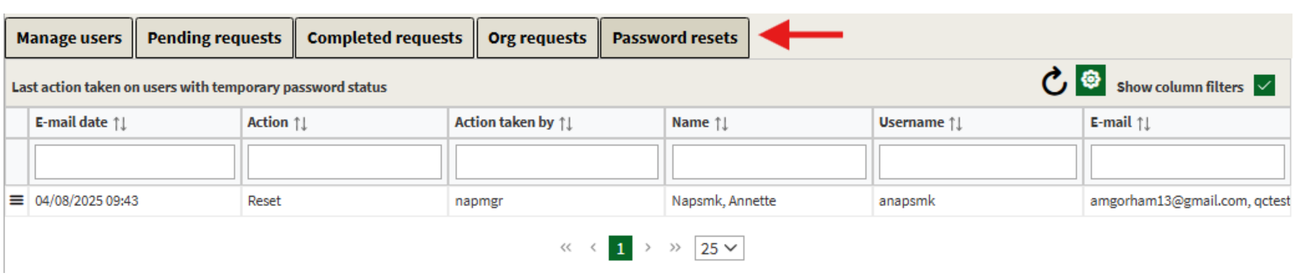


Once reset, the user receives an e-mail message from donotreply@nwcg.gov, to their primary and alternate email addresses, that identifies their temporary Password. The user must reset this temporary Password before accessing the portal.

For security purposes, the Account Manager is not notified of the user's Temporary Password.

Password resets grid

The Password resets grid shows the most recent Password Reset record for users that are still in the Temporary Password state. The following diagram shows the Password Reset grid. To see the full history of Password Resets for a user go to the user's View Profile page.



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

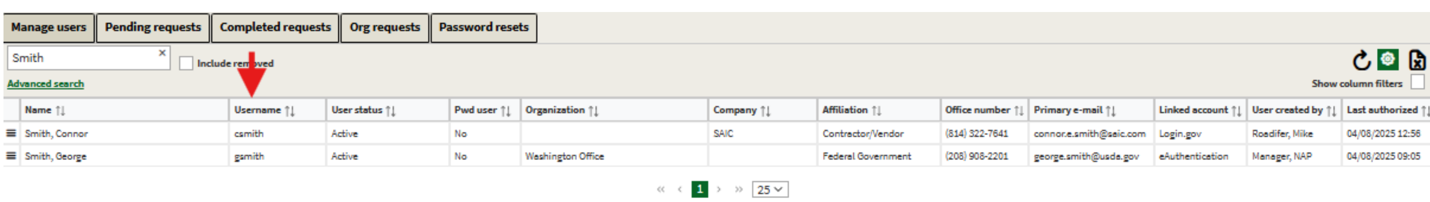
The sample screens in this task show how to alphabetize the Username column.

---

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.



To change the order of columns in the grid

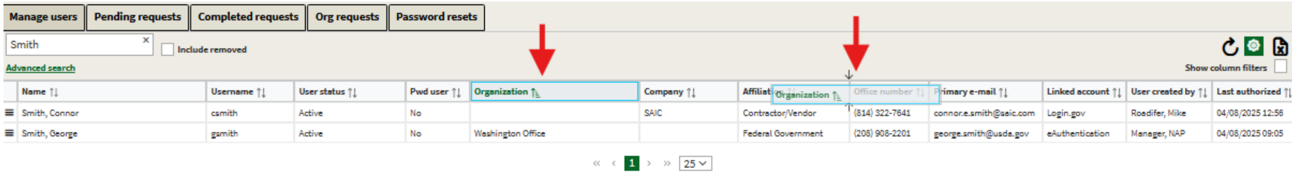
The sample screens in this task show how to move a column using a drag-and-drop operation.

---

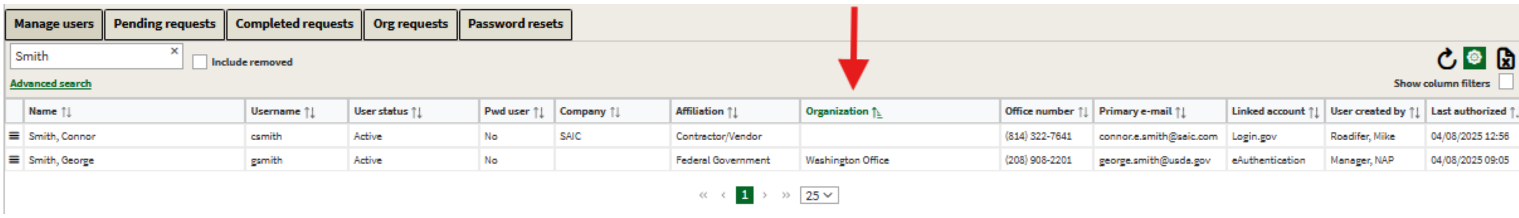
1 Using your mouse, point to, and then click and hold the **Column Heading** of your choice.

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.



The following diagram shows the resulting Manage Users grid.



To change the width of a column

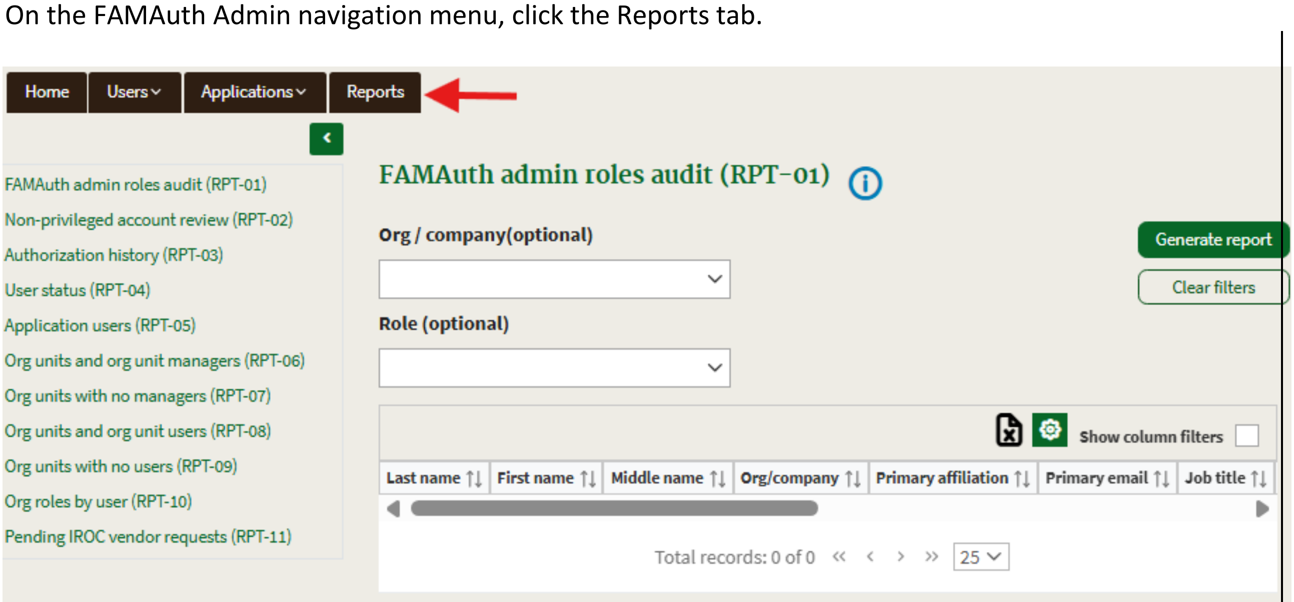
1. Using your mouse, rest the pointer on the right of the **Column Boundary** you want to change until it becomes a resize cursor.
2. Click and hold the **Column Boundary**, drag to the desired width, and then release.

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.



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.