

Quality Payment PROGRAM



Security Official: Manage Access (Approve or Deny Requests)

[Updated 10/23/2025](#)

Table of Contents

[Introduction](#)

[Security Official Approve/Deny Role Requests Step-by-Step Instructions with Screenshots](#)

1. [Sign in to the Quality Payment Program \(QPP\)](#)
2. [Navigate to Manage Access](#)
3. [View Pending Role Requests](#)
4. [Confirmation of Approved or Denied Requests](#)

[Removal of User Access](#)

1. [Navigate to Manage Access](#)
2. [Find User's Organization](#)
3. [Remove User's Access](#)
4. [Confirm Removal of User's Access](#)
5. [Confirmation of Successful Removal](#)

[Next Steps](#)

[Frequently Asked Questions](#)

[Version History](#)

Attention Representatives of Medicare Shared Savings Program (Shared Savings Program) Accountable Care Organizations (ACOs):

Shared Savings Program ACOs have a different Health Care Quality Information System (HCQIS) Access Roles and Profile system (HARP) account creation and Quality Payment Program (QPP) role management process. ACOs will no longer be able to perform these actions on qpp.cms.gov.

If your organization is a Shared Savings Program ACO, please **DO NOT** follow the information in this document. Instead, please refer to the **Medicare Shared Savings Program ACOs: Creating and Managing a HARP Account with a QPP Role in ACO-MS document (PDF)** in the [QPP Access User Guide](#) (ZIP file) for information on how to obtain a HARP account with a QPP Security Official or Staff User role and manage your role in the [ACO Management System \(ACO-MS\)](#). If you are your ACO's QPP Security Official or Staff User contact in ACO-MS, then you can sign in to qpp.cms.gov using your ACO-MS Username and Password.

Please note that the ACO-MS process only applies to representatives of a Shared Savings Program ACO, and not to the Participant TINs in the ACO. Representatives of a Participant TIN will still need to create an account on harp.cms.gov and request and manage their QPP role on qpp.cms.gov, using the information in this resource.

Introduction

This document will outline the steps a **Security Official** needs to take to **approve or deny role requests from additional users**, so they can view information about or perform an action, such as submitting performance data, completing an opt-in election, or viewing performance feedback.

All Security Officials will approve role requests by signing into gpp.cms.gov, which allows Security Officials to manage all their Quality Payment Program activities in one place.

The main **difference** between the Security Official role and the Staff User role is that Security Officials are responsible for approving (or denying) role requests from additional users for their organization. If you are the only Security Official for your organization, you will be responsible for approving all role requests.

Note: If you are a representative of a Shared Savings Program ACO, you must manage your HARP account via the [ACO Management System \(ACO-MS\)](#). Contact your ACO to make any modifications.

There are **three steps** for approving (or denying) role requests:

1. Sign into gpp.cms.gov
2. Navigate to Manage Access
3. Approve or deny Pending Requests in your queue

Helpful Hint

Consider adding a second (or third) Security Official to your organization to ensure someone is always available to approve role requests.

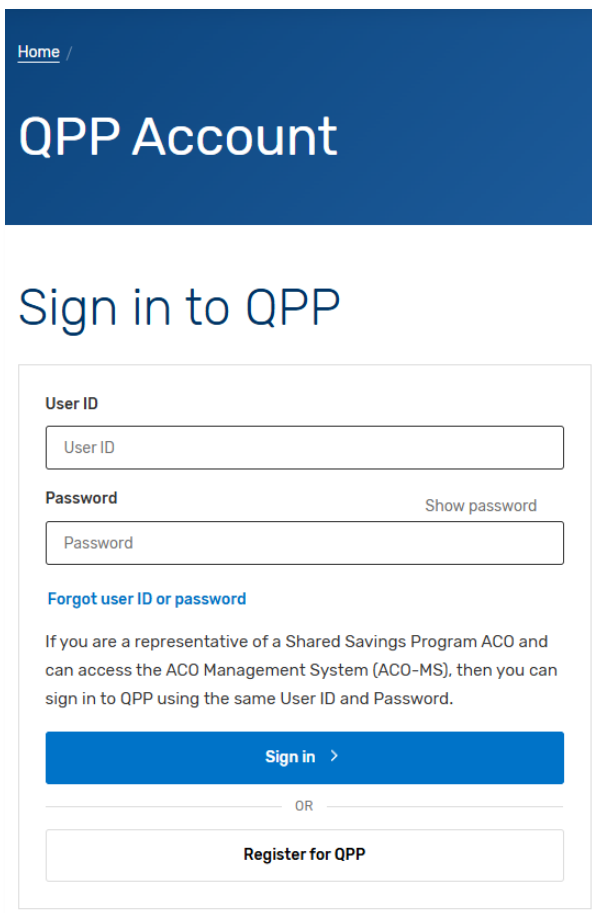
There is no limit to the number of Security Officials your organization can have.

Approval/Denial Role Request Workflow with Screenshots

Step 1: Sign in to the QPP Website

Go to qpp.cms.gov and click **Sign In**, in the upper right-hand corner.

Then, enter your **User ID** and **Password** in the requested fields, click **Sign In**, and agree to the **Statement of Truth**, (you will be prompted to provide a security code from your two-factor authentication.)



Home /

QPP Account

Sign in to QPP

User ID

Password [Show password](#)

[Forgot user ID or password](#)

If you are a representative of a Shared Savings Program ACO and can access the ACO Management System (ACO-MS), then you can sign in to QPP using the same User ID and Password.

[Sign in >](#)

OR

[Register for QPP](#)

Returning users:

Sign in with the same credentials you've previously used.

New users:

Sign in with your newly created HARP credentials.

Don't have an account?

Click [Register](#) next to Sign In and review the **Register for a HARP Account document** in this guide.

Step 2: Navigate to Manage Access

Once you are signed in to your QPP Account on qpp.cms.gov, click **Manage Access** on the left-hand navigation.

Step 3: View Pending Role Requests

As a **Security Official**, you are responsible for **reviewing** outstanding role requests from other users and either **approving** or **denying** their requests.

You can view pending role requests directly on the **Manage Access** page or by clicking a link to **View Users** associated with an organization.

The screenshot shows the 'Manage Access' page for Elizabeth Blackwell. The left-hand navigation menu includes Home, Eligibility, Performance Feedback, Manage Access (highlighted), and Help and Support. The main content area is titled 'Manage Access' and features a 'Pending Requests (2)' section. The first request is for Thomas Miller, MD (Acme Clinic, LLC), with a role of Staff User and buttons for APPROVE and DENY. The second request is for Elizabeth Blackwell (You) (Greenville Medical Clinic), with a role of Security Official and a status of 'Waiting for approval from the current Security Official(s)'. Below this is a 'Connected Organizations (3)' section with tabs for APM ENTITIES, REGISTRIES, VIRTUAL GROUPS, and PRACTICES. The 'Acme Clinic, LLC' organization is expanded, showing its TIN, address, and roles. Under 'YOUR ROLE', it lists Security Official. Under 'CMS WEB INTERFACE AND CAHPS', it lists CMS Web Interface and CAHPS Survey. Under 'USERS', it shows 3 connected users and 1 pending user, with a 'View users' link highlighted in a red box.

Note: This option **only** displays for Security Officials.

The screenshot shows the 'Manage Access' page with a different navigation menu. The left-hand navigation menu includes Performance Feedback, Doctors & Clinicians Preview, Exceptions Application, Targeted Review, Reports, Manage Access (highlighted in a red box), Registry/QCQR Self-Nomination, and Help and Support. The main content area is titled 'Manage Access' and features a 'Pending Requests' section. The first request is for Marty Swanburger (Davis Inc), with a role of Security Official and buttons for Approve and Deny. Below this is a 'Connected Organizations' section with a link to 'Connect to another organization' and tabs for Virtual Groups, APM Entities, and Practices.

Pending Requests on the Manage Access Page

This page includes any role requests you have **initiated** and any **pending requests from other users** that you need to approve or deny as a current Security Official for an organization(s).

If you are a Security Official for multiple organizations, you will see pending requests for all associated organizations on this page.

The screenshot shows the 'Manage Access' page for Elizabeth Blackwell. The left sidebar contains navigation links: Home, Eligibility, Performance Feedback, Manage Access (highlighted), and Help and Support. The main content area is titled 'Manage Access' and displays 'Pending Requests (2)'. The first request is for Thomas Miller, MD at Acme Clinic, LLC, with the role of Staff User. There are 'APPROVE' and 'DENY' buttons next to his name. The second request is for Elizabeth Blackwell (You) at Greenville Medical Clinic, with the role of Security Official. A status message indicates 'Waiting for approval from the current Security Official(s)'. The 'APPROVE' and 'DENY' buttons for this request are also highlighted with a red box.

Each request will identify the name of the requester, the role they are requesting, and the organization they represent.

Select **Approve** or **Deny** next to each name as appropriate.

Pending Requests

This screenshot shows a single pending request for Marty Swanburger at Davis Inc, with the role of Security Official. There are 'Approve' and 'Deny' buttons next to his name, both highlighted with a red box.

Connected Organizations [Connect to another organization](#)

Pending Requests Connected Users Page

1. Under Connected Organizations, you can filter by the **organization name** you are interested in reviewing.
2. Click **View Users** (only visible to Security Officials) to view all of that organization's **connected users**.

The screenshot shows the 'Connected Organizations' page with tabs for 'Virtual Groups', 'APM Entities', and 'Practices' (selected). It indicates '3 Practices'. One practice is highlighted: 'ITTestOrg-60-fake60' with TIN: 000043660 and address: 33165 Anderson Underpass Apt. 438 Suite 1370, Richardstad, KS 725250761890104. Below the practice name, there are two columns: 'USERS' showing '11 connected users' and 'YOUR ROLE' showing 'Security Official'. A 'View users' button is highlighted with a red box.

Here you can view **all users** associated with the organization, including users from the organization whose requests have been accepted (connected users) and users whose requests are **pending**. Select **Approve** or **Deny** next to each name as appropriate.

Manage Access
Greenville Medical Organization
TIN# 000793654

Pending Requests (1)

Thomas Miller, MD Greenville Medical Clinic	Role Staff User	APPROVE	DENY
---	---------------------------	----------------	-------------

Connected Users (3)

Kelly Dunn kelly@greenvillemedical.com	Role Security Official
Laura Fortran kelly@greenvillemedical.com	Role Staff User
Liz Lordis kelly@greenvillemedical.com	Role Security Official

The **Pending Requests** section will identify the name of the requester and the role they are requesting.

Account Home
Davis Inc
TIN: 000549237

Connected Users
Davis Inc

Pending Requests

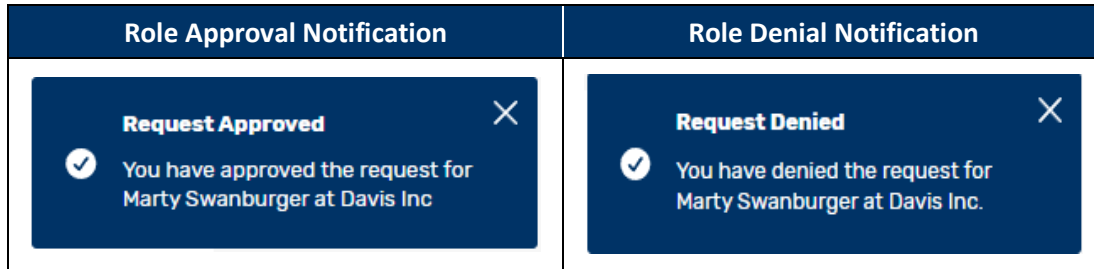
Marty Swanburger Davis Inc	Role Security Official	Approve	Deny
--------------------------------------	----------------------------------	----------------	-------------

Connected Users

Confirmation of Approval or Denial

You will receive a pop-up notification and an email notification confirming your decision to approve or deny a role request.

The users you are approving and denying roles for will also receive an email notification informing them of your decision.



Removal of User Access

As a Security Official, you are responsible for managing your organization's access.

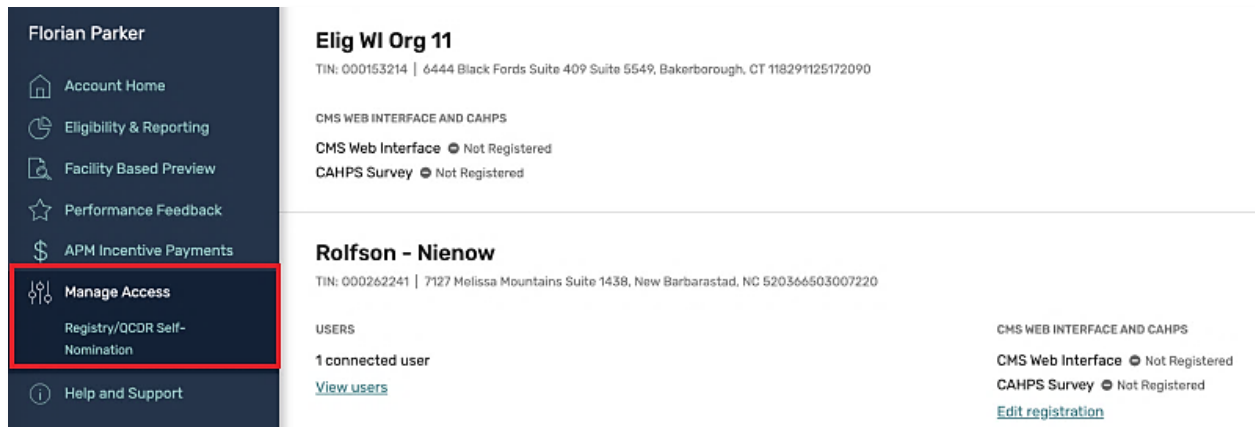
If a staff member leaves your organization or no longer needs access to the organization's QPP information, you and the organization's other Security Officials (if applicable) are responsible for removing their access.

To remove a user's access, you will follow four steps:

1. Navigate to Manage Access
2. Find User's Organization
3. Remove User's Access
4. Confirm Removal of User's Access

Step 1: Navigate to Manage Access

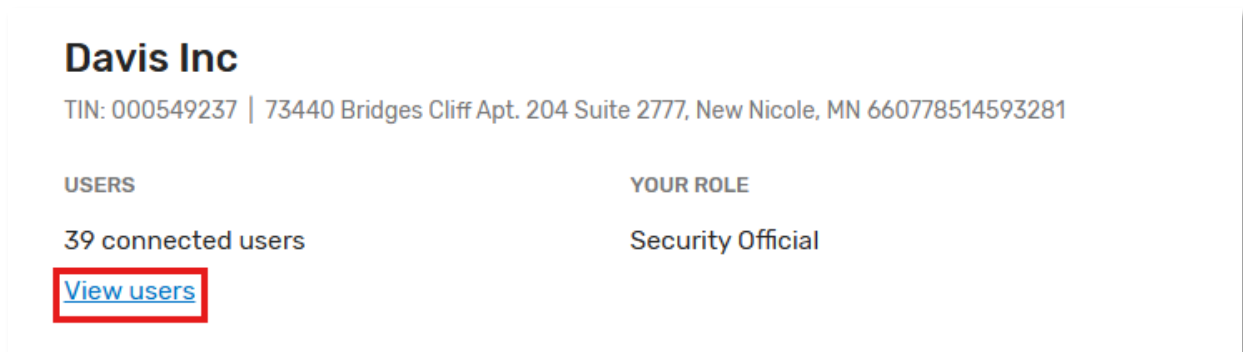
Click **Manage Access** on the left-hand navigation.



The screenshot shows a user profile for Florian Parker. On the left is a dark navigation menu with the following items: Account Home, Eligibility & Reporting, Facility Based Preview, Performance Feedback, APM Incentive Payments, **Manage Access** (highlighted with a red box), Registry/OCDR Self-Nomination, and Help and Support. The main content area displays two organizations: 'Elig WI Org 11' and 'Rolfson - Nienow'. For 'Elig WI Org 11', it shows the TIN: 000153214, address, and status for CMS Web Interface and CAHPS Survey. For 'Rolfson - Nienow', it shows the TIN: 000262241, address, and status for CMS Web Interface and CAHPS Survey. A 'View users' link is visible under the Rolfson - Nienow organization.

Step 2: Find the User's Organization

From your Connected Organizations, find the organization that the user is associated with and click **View Users**.



The screenshot shows the details for 'Davis Inc'. It includes the TIN: 000549237 and address: 73440 Bridges Cliff Apt. 204 Suite 2777, New Nicole, MN 660778514593281. Below this, there are two columns: 'USERS' and 'YOUR ROLE'. Under 'USERS', it says '39 connected users' and a 'View users' link is highlighted with a red box. Under 'YOUR ROLE', it says 'Security Official'.

Step 3: Remove User's Access

From the organization's Connected Users, find the user's name, and click **Remove Access**.

Connected Users	
Nirmal Test Elig Org 24	Role Security Official X Remove Access
Florian Parker Elig Org 24	Role Security Official
Aurelie Farrell Elig Org 24	Role Security Official X Remove Access

Note: You cannot remove your own access. If you need to remove your access, another Security Official associated with the organization must do so.

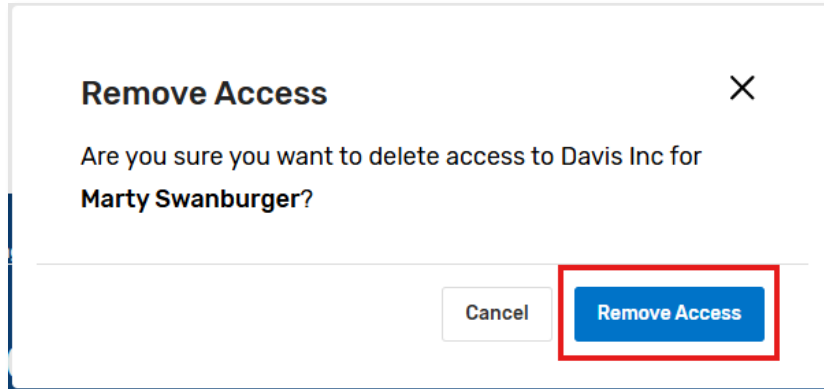
If you are the organization's only Security Official, contact the Quality Payment Program using the information at the bottom of each page of this document. When you contact the Quality Payment Program, please be prepared with your organization's TIN.

Marty Swanburger Davis Inc	Role Security Official X Remove Access
--------------------------------------	---

Step 4: Confirm Removal of User's Access

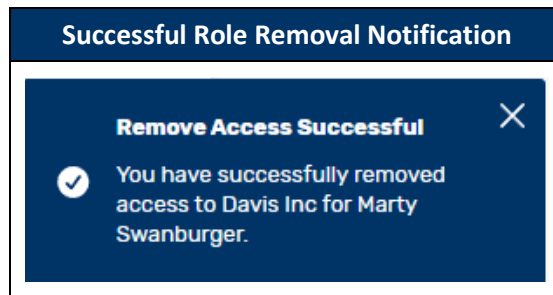
After clicking Remove Access, you will be asked to confirm the removal of the user's access by clicking **Yes, Remove Access**.

If you accidentally selected the wrong user, you can cancel by clicking **No, Cancel Action**.



Confirmation of Successful Access Removal

Once you confirm the removal of a user's access, you will be redirected back to your Connected Organizations and receive a **confirmation notification** in the lower right corner.



Next Steps

- Monitor your email for pending role request notifications so you can quickly approve them.
- Consider asking another person in your organization to request the Security Official role, so there is always someone available to approve requests.

Helpful Hint

Consider creating a recurring calendar reminder to sign in to qpp.cms.gov so you can review and approve any pending requests during high volume request periods.

Frequently Asked Questions

1. How are requesters notified of my decision to approve or deny their request?

Requesters will receive an email telling them whether their request was approved or denied. This email will be sent to the email address they provided when registering for their HARP account.

2. I accidentally denied a request that I meant to approve. What do I do?

Contact the person whose request you denied and ask them to resubmit their request. If you don't know how to contact the person, you will need to wait for them to resubmit the request on their own.

3. How many requests should I expect to approve?

The number of requests you receive will depend on the size of your organization and how your organization will submit data. Generally, you should anticipate a higher volume of requests before and during the submission period and the targeted review period. For additional information on the submission period for this program year, please visit the [QPP website](#).

4. How do I remove a user who should no longer be authorized for my organization?

If you are a Security Official, you can remove another user's access for your organization under **Manage Access**. For step-by-step instructions on removing a user's access, visit [Removal of Roles and Access](#) in this resource.

You cannot remove your own access. If your access needs to be removed, ask another Security Official at your organization to remove your access. If you are the only Security Official at your organization, contact the Quality Payment Program using the information at the bottom of each page of this resource for assistance. Please come prepared with your organization's Tax Identification Number (TIN).

Version History

Date	Change Description
10/23/2025	Updated workflow and screenshots to align with current functionality.
09/13/2024	Updated QPP Access User Guide link on page 1.
11/04/2021	Added Shared Savings Program ACO Management (ACO-MS) callout in introduction.
03/20/2020	<ul style="list-style-type: none">Identified additional actions one can perform with QPP access. Corrected typos about the number of steps needed.Added Quality Payment Program contact information for those who are hearing impaired.
12/02/2019	Updated to include user access removal process.
07/01/2019	Updated Supporting documents in the guide.
12/18/2018	Original posting.