



# Qualys Patch Management

## Release Notes

Version 1.4.5

December 15, 2020

Here's what's new in Patch Management 1.4.5!

[Enhancement to Role Based Access Control](#)

[Added Support for Sharing a Job With Other Users](#)

[Added Support for Changing Ownership of a Job](#)

[Added Filters to Search Jobs by Owner and Co-Author](#)

**Qualys 1.4.5 brings you more improvements and updates! [Learn more](#)**

## Enhancement to Role Based Access Control

Our earlier RBAC model, was more restrictive enforcing a clear compartmentalization of users from each other and basic roles only. With the new RBAC model, we have added more roles, depicting the real-life hierarchies and responsibilities. With the upgrade of the RBAC model, all existing sub-users will take the Patch User role and all the existing super-users will have all the permission defined in RBAC. All other roles will need to be explicitly managed by the superuser.

Also note, that these roles are exclusive to the Patch Management module only. The roles defined in other modules have NO correlation with that defined in Patch Management.

Role Based Access Control gives you flexibility to control access to Patch Management features based on the roles of the individual users.

Each user is assigned a pre-defined user role which determines what actions the user can take.

We have 5 OOTB (Out-of-the-box) roles for PM users. Each role, except Patch Security, is an incremental role to the previous one.

1) **Patch Reader:** This is the default role designed to most (sub-)users, present in the system today, with minimum permissions possible. This role is granted to allow users viewing/ read-only capabilities in the Dashboards developed to provide an insight into the Patching operations. This role has only view permissions on assigned jobs, assessment profiles, and dashboards.

2) **Patch Dashboard Author:** This is a special role that would be needed only for larger organizations that delegate development of dashboards to a dedicated team especially, one that does NOT operate/ manage the patching jobs. This role includes all the Patch Reader permissions.

3) **Patch User:** This role is designed for the operators of the Patching job, who interact and manage patching activities on a regular basis. In most cases, these users will also build dashboards for reporting information to their respective department/ team. This role includes all the Patch Dashboard Author permissions.

4) **Patch Security:** This role is mutually exclusive to all the earlier set of roles. It is meant for the Security Expert in organizations where IT operations and Security operations (SecOps) are owned by distinct team. These users have very limited capabilities that allow them to pass on a list of selective patches to the IT operations team to operationalize their patching on the endpoints across the organization. All the job advisories created by Patch Security user are “Partially Configured Job” and only after assigning these jobs to a Patch User/ Patch Manager, the owners can choose the right tags/ assets, schedule and other options. Only the Patch Manager role has “Change Owner” permission enabling it to take/ assign ownership of a “Partially Configured Job” to other users, with Patch Manager or Patch User roles. These users can neither own nor edit/co-edit any job.

5) **Patch Manager:** A Patch Manager has all the permissions except create job advisory permission.

Note that we recommend users to NOT create custom roles for the Patch Management users by assigning or unassigning permissions available through the default roles. Such customization of roles or change of permissions may lead to user roles not working as per the design.

### Partially Configured Job

Patching Job has 3 critical components:

a) Patch(es): One or more patches to be applied as a part of the job.

b) Asset(s)/ Tags: One or more assets on which the patches are to be applied. A logical collection of assets is referred to as Tags.

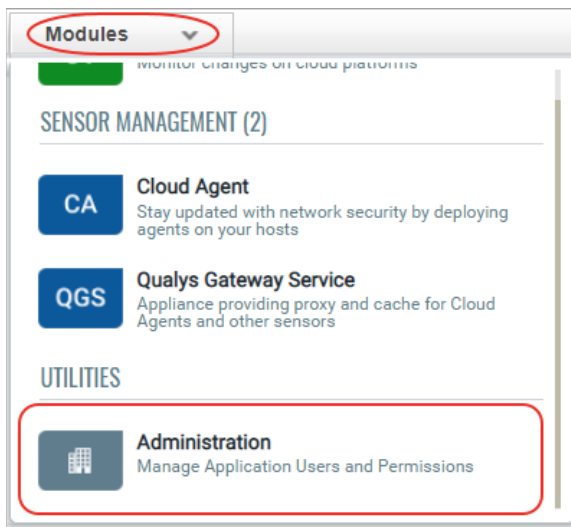
c) Schedule: The Patching job needs to be executed at a scheduled date and time. In case of a recurring Patching job, each job run is scheduled for a selected time, at a frequency across selected dates/ days of a month.

All these 3 components are important for the completeness of a job. If any of them is pending in a job definition, we have a Partially Configured Job.

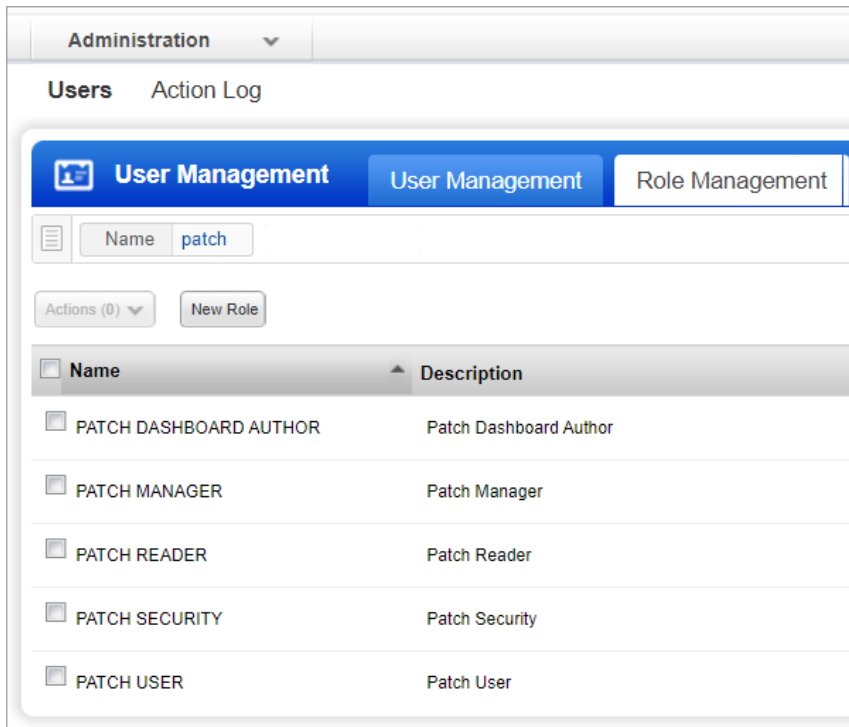
### How to find Roles

You can assign roles from our Administration utility module. Within the Administration utility, you'll find roles and their related permissions in the Role Management section. See [Qualys Administration utility Online Help](#).

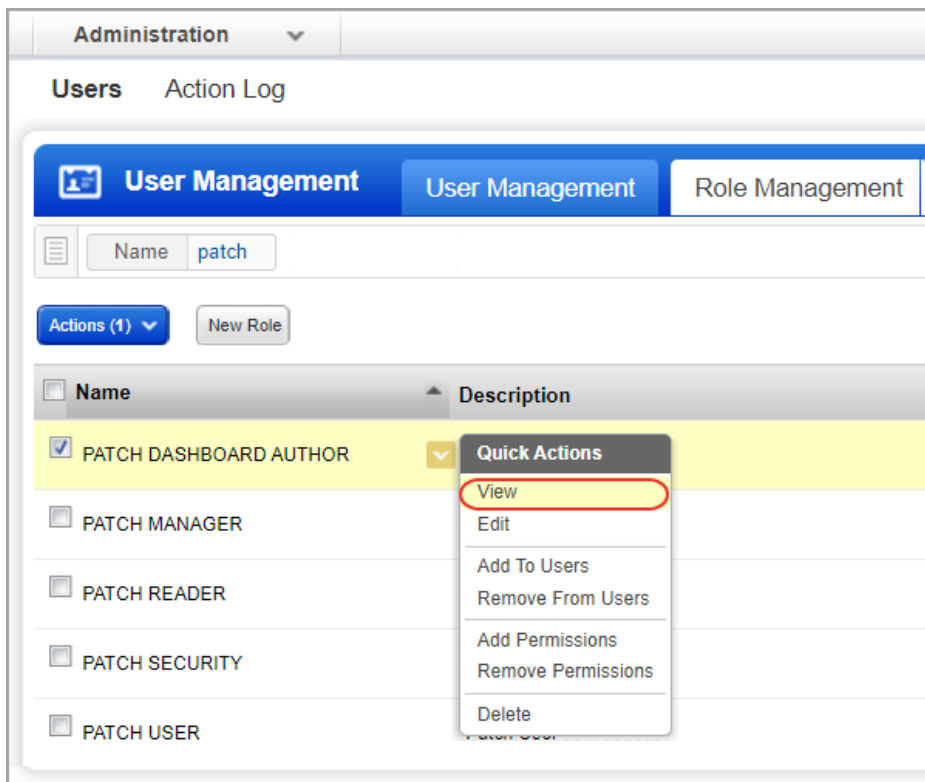
1) From the application module picker, click **Administration**.



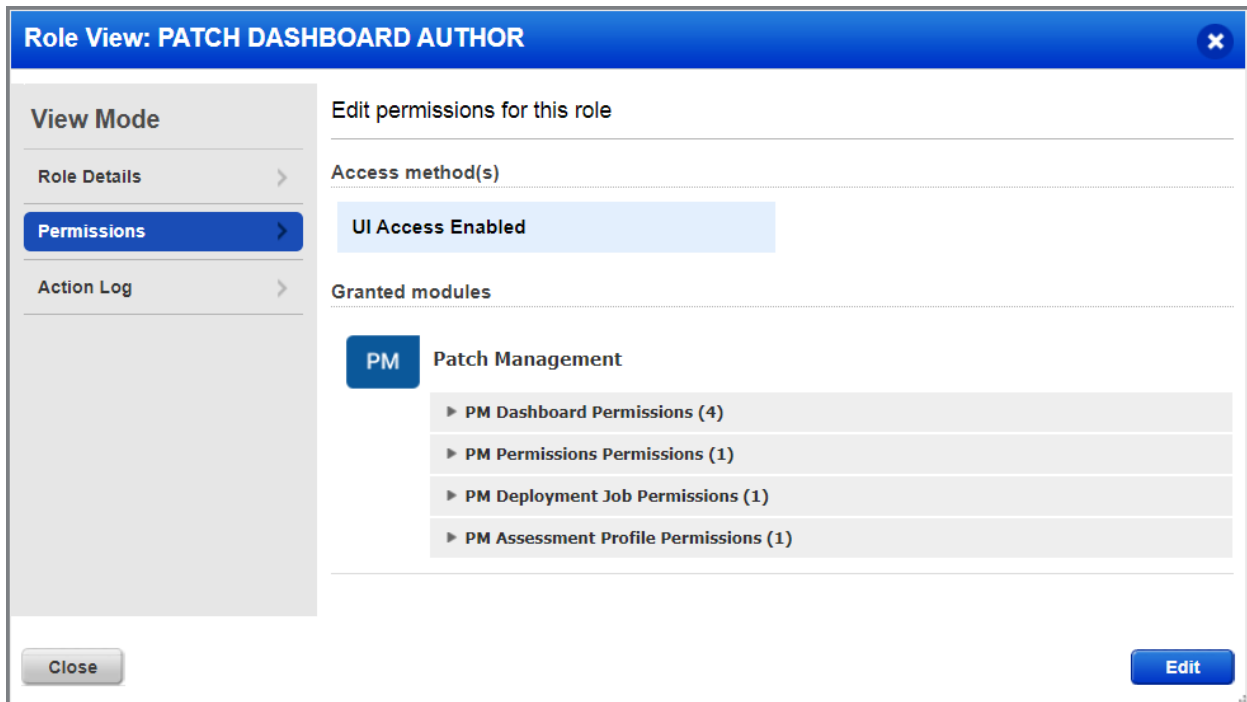
2) Go to the **Role Management tab** and enter "patch" in the search box to view all the patch management roles.



3) Select a role from the list and from the **Quick Actions** menu, click **View**.



4) On the **Roles View** screen, go to the **Permissions** tab to view the permission for the selected role.



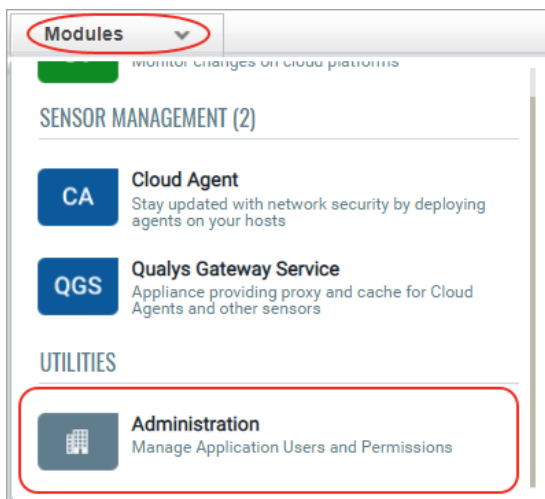
## How are tags used to grant access to assets?

An asset tag is a tag assigned to one or more assets. Tag scopes define what assets the user can view when creating a job or when user go to Assets tab in patch management.

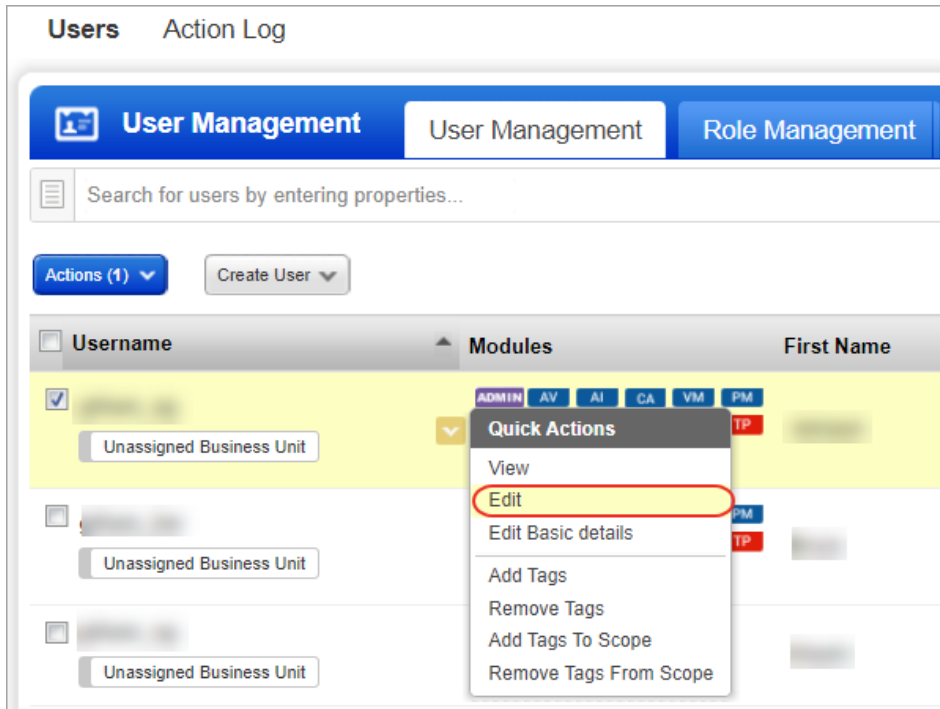
Assigning a tag to an asset enables you to grant users access to that asset by assigning the same tag to the users scope. Want to define tags? It's easy - just go to the Asset Management (AM) application.

To assign asset tags to the user,

1) Go to the **Administration** module and then from the **User Management** tab search a or select the user.

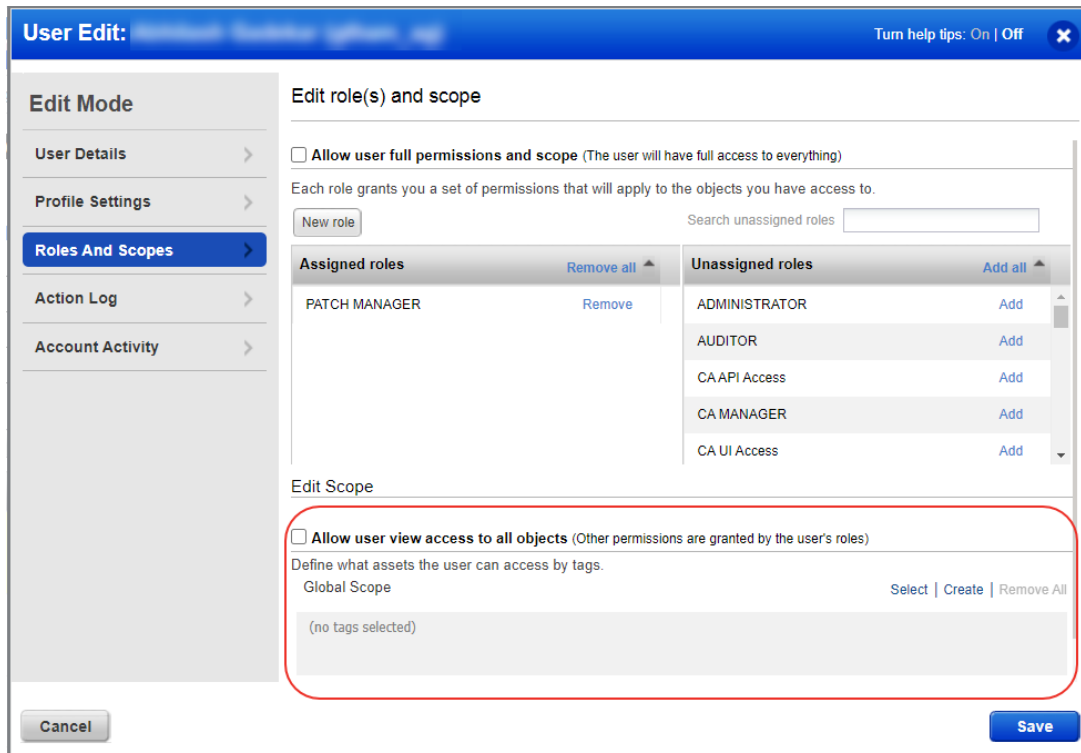


2) From the Quick Actions menu, click **Edit**.



3) On the **User Edit** screen, go to the **Roles and Scopes** tab.

4) In the **Edit Scope** section, select one or more asset tags that you want to assign to the user. Then click **Save**.



## User Roles Comparison

The following table provides a comparison of privileges granted to user roles for Patch Management. Note that Assigned Jobs of a user are the jobs that the user has created or permission to edit as a co-author.

Privileges	Patch Manager	Patch User	Patch Dashboard Author	Patch Reader	Patch Security
<b>Manage License Permissions</b>					
Manage License	Y				
<b>Assessment Profile Permissions</b>					
Create Profile	Y				
Edit Profile	Y				
Delete Profile	Y				
View Profile	Y	Y	Y	Y	Y
<b>Deployment Job Permissions</b>					
Change Job Owner(ship)	Y				
View Any Job	Y				
Edit Any Job	Y				
Enable/disable any Job	Y				
Delete Any Job	Y				
Create job	Y	Y			
Edit Assigned Job	Y	Y			
Enable/disable Assigned Job only	Y	Y			
Add Remove Patches To Job only	Y	Y			
Delete Assigned Job	Y	Y			
View Assigned Job	Y	Y	Y	Y	Y
<b>PM Dashboard Permissions</b>					
Create Dashboard	Y	Y	Y		
Edit Dashboard	Y	Y	Y		
Delete Dashboard	Y	Y	Y		
View Dashboard	Y	Y	Y	Y	Y
<b>Advisory Permissions</b>					
Create Job Advisory					Y

## Added Support for Sharing a Job With Other Users

A job can be shared with other users by making them co-authors of the job, allowing them to edit/operate the job equivalent to the creator, provided they have the same (or higher) role and same (or larger) asset scope assigned to them for administration.

Job creation page now have an addition step “Job Access” that lets you assign co-authors to jobs.

← Create: **Deployment Job**

STEPS 6/7

- 1 Basic Information
- 2 Select Assets
- 3 Select Patches
- 4 Schedule
- 5 Options
- 6 **Job Access**
- 7 Confirmation

### Job Access

Select the Co-Author users who can edit this job.

Add these users (1) as Co-Authors to this job Add Users

FIRST NAME	LAST NAME	USERNAME	EMAIL	Remove All
Bruce				✕

Cancel Previous Next

Note that co-authors of a job do not have permission to add/remove assets to/from the job but they can add/remove asset tags to/from the job. Though co-authors of a job can add an asset tag to the job, only the assets that are in the owner's asset scope will be picked up when the job is run. Remember that execution of a job is restricted by the tag scope of the job owner.

## Added Filters to Search Jobs by Owner and Co-Author

As per the new RBAC model, the Jobs tab will show all the jobs in your subscription but you can view or edit details of jobs that you have created or have permission to edit as a co-author. On the Jobs page, we added two new job filters: Own jobs and Co-Author Jobs to let you filter jobs by owner, co-author or both.

Patch Management ▾ DASHBOARD PATCHES ASSETS **JOBS** CONFIGURATION

### Jobs

24 Total Jobs

STATUS Enabled 24

status: `Enabled`

Actions (0) Create Job

Filters

- Job Filter
- Own Jobs
- Co-Author Jobs

STATUS	NAME
Enabled	ds_auto-View... Install Job



## Added Support for Changing Ownership of a Job

Our earlier RBAC model, was more restrictive enforcing a clear compartmentalization of users from each other and basic roles only. With the new RBAC model, we have added more roles, depicting the real-life hierarchies and responsibilities.

A job can now be shared with other users by making them Co-Authors of the job. Co-authors should have the same (or higher) role and same (or larger) asset scope assigned to them for administration so that they can edit/ operate the job equivalent to the creator (owner).

If you want to temporarily allow additional users to edit/ manage a job, you can make them Co-Author(s) of the job. This can be done by adding the users to the job under the Job Access options while creating a job.

If you want to permanently transfer ownership of a job to another user, you could achieve that by changing the ownership of the job.

To change the owner of the job, you must have “Change Owner” permission i.e. “Patch Manager” role. You can change ownership of jobs, in bulk or on individual jobs. From the Jobs tab, select a one or more job(s) and then from the Quick Actions menu, choose "Change Job Owner" option. Select the username of the new Job owner and click Apply. A message confirms that the job ownership is transferred to the selected user

	FIRST NAME	LAST NAME	USERNAME	EMAIL
<input checked="" type="checkbox"/>	Bruce			
<input type="checkbox"/>				
<input type="checkbox"/>				

If the new owner has the same (or higher) role but a different asset scope assigned to them, the jobs could execute differently. The endpoints targeted by the job will be limited to the assets that are common between the asset scope of original owner and the new owner. A Patch Manager would need to revise the asset scope of the new user to ensure execution of the job as before the ownership change.

If the new owner has a role lower than Patch Manager OR Patch User, the jobs may not execute at all. If a job, especially a partially configured one, created as an advisory, it has No Owner. Ownership for such a job needs to be established by explicitly assigning an owner to such “Partially Configured Jobs”.

## Issues Addressed

- We fixed an issue where a custom widget created to show asset count by patch status had discrepancy in the count values. The widget showed a big difference in asset count when it was created and when user revisit the patch dashboard from other dashboard. After the fix, the widget shows correct asset count for the selected patch status.
- We fixed an issue where the Patch Management count widget was showing incorrect percentage on the selected superset. After the fix the widget is showing correct percentage.
- We fixed an issue where when the Patch Management takes the user from the dashboard to the Patches tab to show a widget query in the search token box then if the user was selecting one of the predefined filters from the left pane, the QQL query instead of getting added to the existing query in the search token bar in the patch context, it was getting added to the search token bar in the asset context below the patch QQL query. After the fix, the QQL query is appended to the existing QQL query.
- We now do not include an asset tag that is part of the assessment profile in the update profile request if the asset tag is deleted from Asset View module.
- We fixed an issue where jobs created by the sub users were not shown on the Jobs tabs if no asset tags are assigned to the user. We now show the jobs of the users that has no asset tags assigned.
- We will now skip the immediate and run once jobs that are timed out from the next manifest as these job will never succeed on the agent. Skipping such jobs saves processing time for sending timed out jobs in the manifest and sending timed out messages for these jobs.
- We have made an improvement to the scheduling of recurring jobs when the job is disabled and enabled again.