# Qualys Certificate View v3.1.0
API Release Notes

Version 3.1.0

June 02, 2023

Qualys Certificate View API gives you many ways to integrate your programs and API calls with Qualys capabilities.

### What's New

# Tag-Based User Scoping

With this release, a manager user can restrict sub user's access to assets and certificates based on Tag Based User scope

**Note**: By default, the manager user has access to all the assets and tags.

Asset Tagging provides a flexible way to organize the assets in your environment. An asset tag is a tag assigned to one or more assets. You can assign a tag to assets; then allow users to access those assets by assigning the same tag in their scope. The tag scopes determine which assets a user is allowed to access and view.

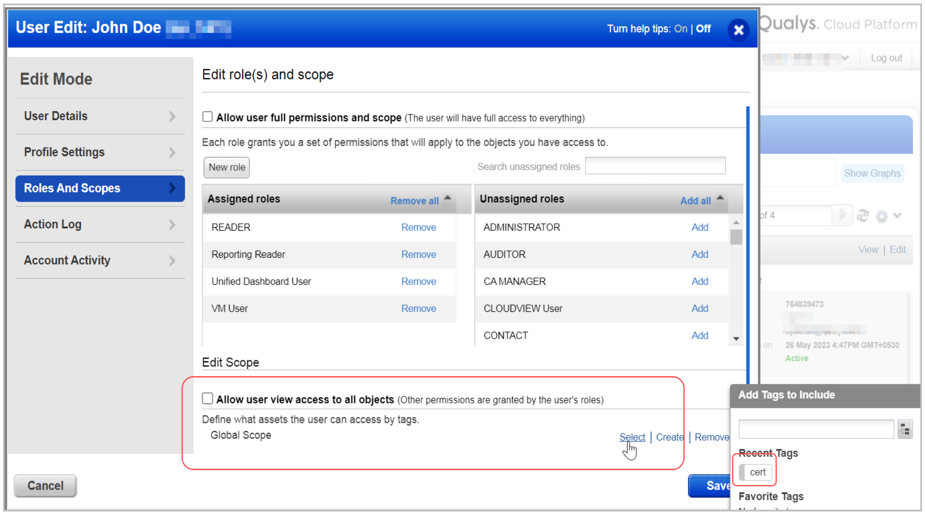
If you have assigned a parent tag to a user, then the user has access to assets from the parent tag and all its child tags. Now a user can see only those assets on which parent or its child tags are assigned. If a user is assigned only a child tag then the user can view assets with this child tag.

For example, if a manager user has assigned CloudAgent tag to a user John. The user John can view only those certificates associated with assets on which CloudAgent or its child tags are assigned. Let's assume the manager user has 1000k assets, the CloudAgent tag is assigned to only 500 assets. In this case, user John can view only 500 assets in Assets tab and in Dashboard. In the Certificates tab, user John can view certificates found on those 500 assets.

You can apply tags manually or configure rules to automatically classify your assets. For more details on tagging asset, refer to *Asset Tag of VM/VMDR Online help*.

You can add/remove tags to user from Administration utility. For detailed steps, refer to the section Manage User Roles from *Administration Utility Online help*.

Now, the user can view all the assets associated by this tag and certificates associated with this tag.



User Edit: John Doe [redacted]

Edit role(s) and scope

☐ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

| Assigned roles | Remove all |
|---|---|
| READER | Remove |
| Reporting Reader | Remove |
| Unified Dashboard User | Remove |
| VM User | Remove |

| Unassigned roles | Add all |
|---|---|
| ADMINISTRATOR | Add |
| AUDITOR | Add |
| CA MANAGER | Add |
| CLOUDVIEW User | Add |
| CONTACT | Add |

Edit Scope

☐ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

Define what assets the user can access by tags.

Global Scope

## Impact of Tag-Based User Scoping on Existing Users

- The manager user has access to all the assets and tags by default.

- For the existing users, if a user's **Roles and Scope** includes **Allow user full permissions and scope,** then user has full access to all the assets, same as the manager user.

If a sub user is not able to view the assets after this new release, check Roles and Scopes for the User and assign the required tags, so a user can get access to the required assets.

Now with this release a manager user can grant restricted access to all assets. For more details about assigning the tags, refer to *Asset Tag of VM/VMDR Online help*

## Impact of Tag-Based User Scoping on Public APIs

| | |
|---|---|
| APIs affected | /certview/v1/certificates<br>/certview/v2/certificates<br>/certview/v1/certificates/{certhash}/assets<br>/certview/v2/instances<br>/certview/rest/public/v1/certificates/import/leaf |
| Method | Post |
| New or Updated APIs | Updated |

Tag-Based User Scoping does not disrupt APIs.

-Going forward, users can see only those assets that have been assigned to them by their manager.

When a user sends an API request to the following Certificate APIs, they can access information about the assets and their corresponding certificates assigned to them, based on their scope.

- List CertView Certificates (v1)
- List CertView Certificates (v2)
- List Assets for a Certificate
- List Server Instances

- With this release, if the sub user with restricted access to assets requests the **Import leaf API**, the user gets HTTP response code - 403(Forbidden). It means user does not have required permissions. The API request failed because the user does not have the required permissions. Check user permissions in the Administration Utility.

- Users with access to all assets can request Import leaf API.