Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.14

October 1, 2021 (Updated October 6, 2021)

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

New Password Security Options

Qualys Policy Compliance (PC/SCAP/SCA)

New Scan Parameters to Exclude Users and Groups from Unix Directory Integrity and Directory Search UDCs (Agent Only)

New Unix UDC "File Content Check (Agent Only)" with Wildcard Support

New Authentication Support for Nginx

Qualys 10.14 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

New Password Security Options

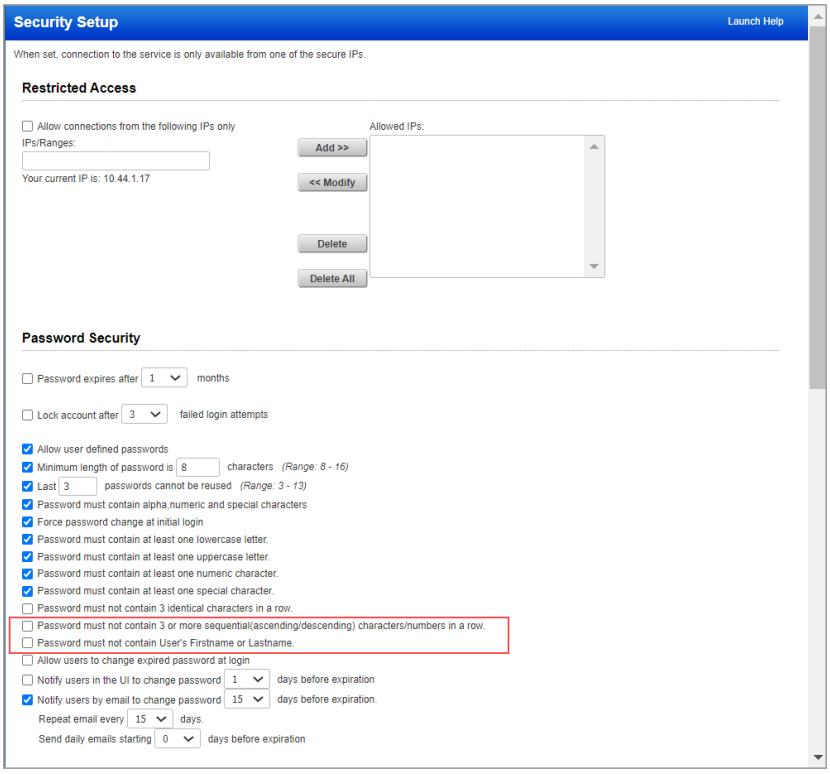
To improve password complexity for user accounts, we've added 2 new password security options. These password security options are disabled by default for new and existing subscriptions. A Manager user can choose to enable them. Once enabled, they will be enforced for all users in the subscription.

Password must not contain 3 or more sequential alpha, numeric characters in a row (ascending or descending order). When this password security option is selected, the password for a user's account cannot include 3 or more sequential alpha or numeric characters in ascending or descending order. For example, the password cannot include sequences like abc, cba, xyz, zyx, 012, 123, 321, 210, and so on.

Password must not contain user's first name or last name. When this password security option is selected, the password for a user's account cannot include the user's first or last name. For example, the user John Doe cannot have a password like 88johnab3!e or doe!6209ad# because these passwords contain the user's name.

How to enforce new password security options

The new password security options are disabled by default. Any Manager user in the subscription can enable these options for the subscription by going to **Users** > **Setup** > **Security**. In the **Password Security** section, select the password security requirements to enforce for all users, and hit **Save**. The next time any user changes their password, the password must meet the new password security requirements. This applies when creating a new password for a first time login (new account creation), or when updating a password using the Change Password or Forgot Password workflows.



Note that the new password security options are only available when "Allow user defined passwords" is selected.

Qualys Policy Compliance (PC/SCAP/SCA)

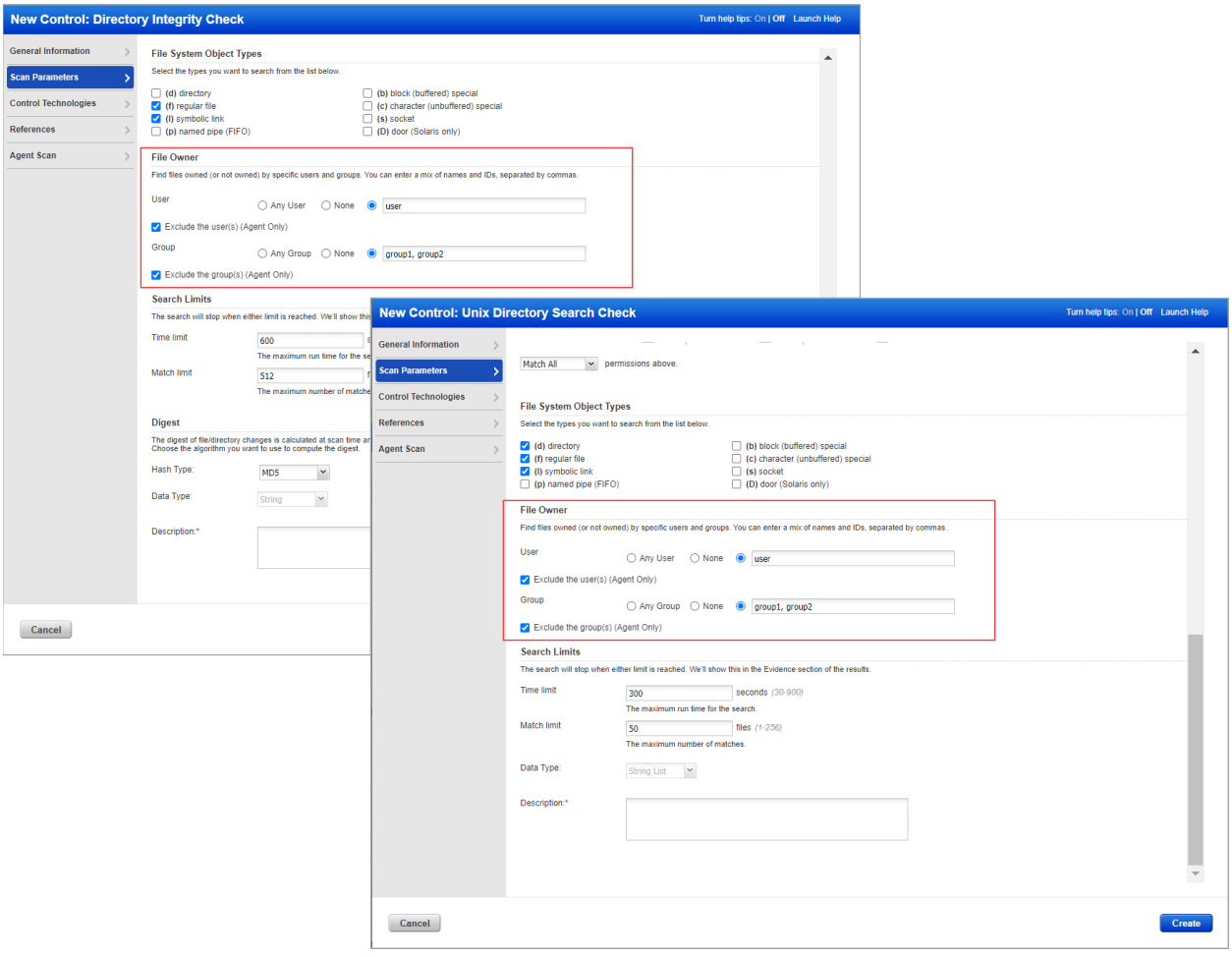
New Scan Parameters to Exclude Users and Groups from Unix Directory Integrity and Directory Search UDCs (Agent Only)

We've introduced 2 new scan parameters in the Unix Directory Integrity UDC and Unix Directory Search UDC. In previous releases, you were able to provide a list of users and groups to find files owned by those users/groups. Now you can find files owned by users/groups and exclude them.

Important - The exclude options are only supported by Cloud Agent. When selected, the scan data for the control evaluation is collected by the agent and then filtered by the agent.

What are the steps?

Go to **Policies** > **Controls**. Create or edit a Unix Directory Integrity UDC or Unix Directory Search UDC. On the **Scan Parameters** tab, scroll down to the **File Owner** section. To exclude users, enter a comma-separated list of user names and/or user IDs, and select **Exclude the user(s) (Agent Only)**. To exclude groups, enter a comma-separated list of group names and/or group IDs, and select **Exclude the group(s) (Agent Only)**. Note that the exclude options are disabled if you choose Any User, Any Group or None. They only apply if specific users and groups are listed.



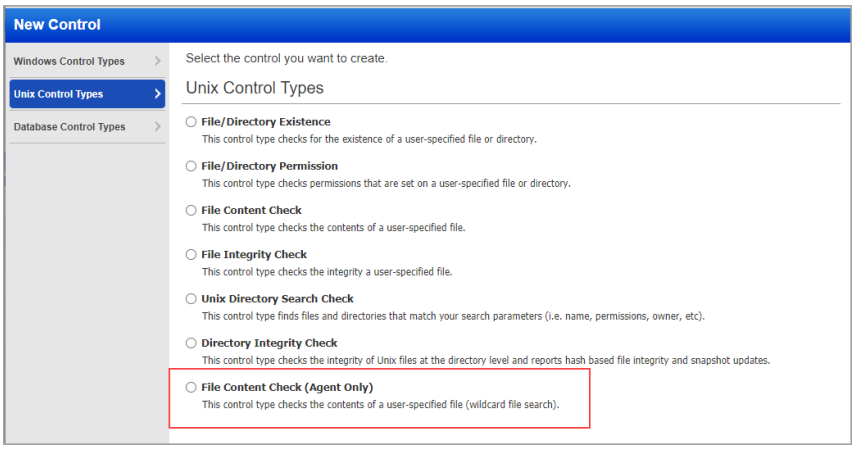
New Unix UDC “File Content Check (Agent Only)” with Wildcard Support

This release introduces a new Unix UDC called “File Content Check (Agent Only)” which supports wildcard file search and provides several additional scan parameter options than the original “File Content Check” UDC. The original “File Content Check” UDC has not changed and is still available. The new “File Content Check (Agent Only)” UDC is now available for customers with PC and Cloud Agent.

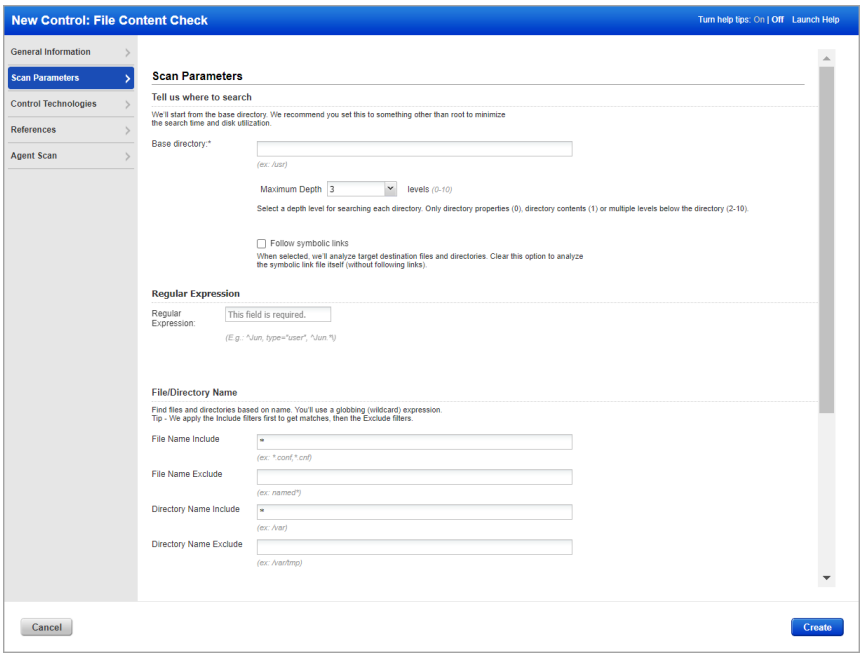
Important - The new Unix “File Content Check (Agent Only)” UDC is only supported by Linux Cloud Agent, meaning it will only be evaluated using agent scan data.

What are the steps?

Go to **Policies** > **Controls** > **New** > **Control** > **Unix Control Types**. Select **File Content Check (Agent Only)**.



Here’s a quick look at some of the options on the **Scan Parameters** tab. Log in to see all available options and click “Launch Help” for help with the options.

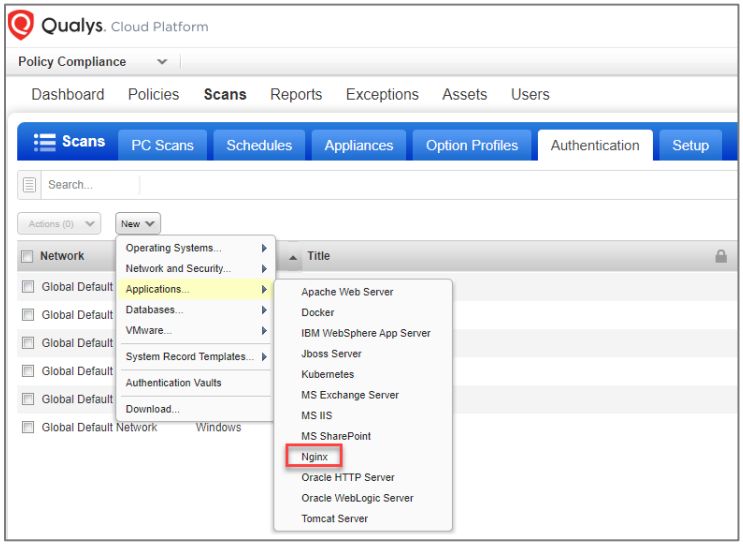


New Authentication Support for Nginx

We now support Nginx authentication for compliance scans using Qualys apps PC, SCA. Simply create an Nginx authentication record with details and scan it for compliance.

What are the steps?

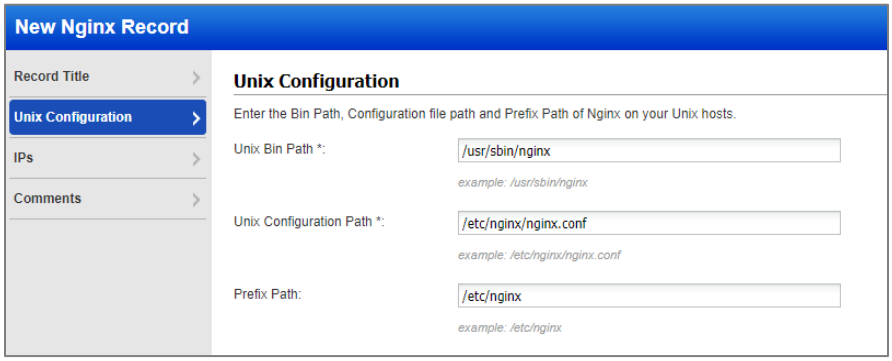
Go to **Scans** > **Authentication** > **New** > **Applications** > **Nginx**.



Your Nginx authentication record

Each Nginx record identifies account title, Unix configuration, and target hosts (IPs).

Enter the Bin path, Configuration file path, and Prefix Patch of Nginx on your Unix hosts. The configuration file must be in the same location for all hosts (IPs) in this record. If different, you must create another record.



Issues Addressed

- We fixed a logical issue in our code where we were not updating the “Modified By” field (only updating the date and time in the “Modified” field) whenever a user was modifying a business unit (BU) record. This issue led to a discrepancy where the “Modified By” field showed an incorrect user. After the fix, we show in the “Modified By” field the latest user who has updated the BU record.
- Fixed an issue where the 50th DNS record was hidden when creating or editing a DNS Hostname-based asset group with more than 50 entries.
- We have now fixed an issue where the sub-user, with asset group assigned, containing only domain names (no IP addresses), can now successfully download the map report.
- We fixed an issue where the vCenter auth record password did not accept the '<' and '>' characters. '<' and '>' characters are now accepted in the vCenter auth record as well as Unix Record password.
- We have now improved the error message to indicate that the file uploaded to vCenter includes some blank entries.
- We made a fix in the Statistics section on policy reports (PDF and CSV formats); now the error code and message are displayed if both the <V> and <E> tags are present.
- Fixed an issue where some columns in the VLANs tab for Scanner Appliance were hidden and were visible only after one of the columns was shifted.
- We fixed an issue where Oracle WebLogic could not be detected during authenticated PC scan.
- We fixed an issue where when the PC module is expired, and if the user chose SCA from the module picker, the UI showed PC in the picker title at the top instead of SCA and the PC-related tabs. The issue occurred because we were not checking the expiry of the subscription for the PC/SCA modules in our code. We now added the expiry condition to check if the PC, SCA, or both modules are enabled and not expired. Based on these conditions, we show either PC, SCA, or both the modules in the module picker and the tabs available for the corresponding modules on the UI.
- We fixed an issue where certain special characters in Model of the Asset was not being processed properly leading to Asset Data not being visible in AssetView (Legacy) or Vulnerabilities tab or Global AssetView.
- Fixed an issue where the Assets > Applications tab was not working as expected for customer with AGMS enabled. Now, behavior has been restored, where depending on how your account is configured, you may need to perform a search to see applications listed or the list would appear automatically upon page load.
- For an AGMS enabled subscription, when Netblock contains Multiple Class A IPs, we added a discrepancy check with the “Multiple Class A networks are not allowed” error message.
- We fixed an issue where the sub-user was unable to load the Remediation page. Also, fixed the request sent to AGMS to contain updated user status if the status is changed.
- We fixed an issue where the XML output of the Network List API had format issues, such as some tags repeated in the output. Now the XML output shows results in the proper format.
- We fixed an issue where customers were unable to update schedule scans via API.

- For subscriptions with AGMS enabled, we made performance improvements on the Scans list when the “Show in Scope Scan List” option is used. Now the page will load faster.