



Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.17.1

February 11, 2019

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

Qualys Cloud Platform

[New/Updated Password Security Options](#)

Qualys 8.17.1 brings you many more improvements and updates! [Learn more](#)

Qualys Cloud Platform

New/Updated Password Security Options

With this release, we've made certain password requirements configurable in the UI. Go to Users > Setup > Security to choose password requirements for all users in the subscription.

Last N passwords cannot be reused. (New) Select this option and enter a value from 3-13. For existing and new subscriptions, this option is off by default. When off, users cannot reuse their most recent password when changing their password.

Password must contain at least one special character. (New) Select this option to require that passwords contain at least one of these special characters: ! @ # \$ % - / _ + \ For existing subscriptions, this option is off by default. For new subscriptions, this option is on by default.

Password must contain alpha, numeric and special characters. (Updated) This option now includes special characters. Selecting this 1 option is the equivalent to selecting 3 options:

- Password must contain at least one letter (uppercase or lowercase)
- Password must contain at least one numeric character
- Password must contain at least one special character

Password Security

☐ Password expires after months

☐ Lock account after failed login attempts

☒ Allow user defined passwords

☐ Minimum length of password is characters (Range: 8 - 16)

☐ Last passwords cannot be reused (Range: 3 - 13)

☐ Password must contain alpha,numeric and special characters

☐ Force password change at initial login

☐ Notify user to change password days before expiration

☐ Allow users to change expired password at login

☐ Password must contain at least one lowercase letter.

☐ Password must contain at least one uppercase letter.

☐ Password must contain at least one numeric character.

☐ Password must contain at least one special character.

☐ Password must not contain 3 identical characters in a row.

New password security options

Issues Addressed

- When configuring a scan schedule, the calendar pop-up on the Scheduling tab would remain open even when you moved to a different tab. This is fixed and the calendar pop-up now closes when you leave the Scheduling tab.
- When a request for the Compliance Posture API (/api/2.0/fo/compliance/posture/info/) includes the asset_group_ids input parameter, the output will include the hosts that match the asset groups specified in the request.
- Improved the online help for scans to explain that when you choose the “Default” scanner appliance option with IP addresses as your scan target then we’ll use our external cloud scanners for the scan job.