



Qualys 8.12 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

[New User Administrator Role Permissions](#)

Qualys Policy Compliance (PC/SCAP/SCA)

[Failure Summary Section in Policy Compliance Reports](#)

**Qualys 8.12 brings you many more
Improvements and updates! [Learn more](#)**

Qualys Cloud Platform

New User Administrator Role Permissions

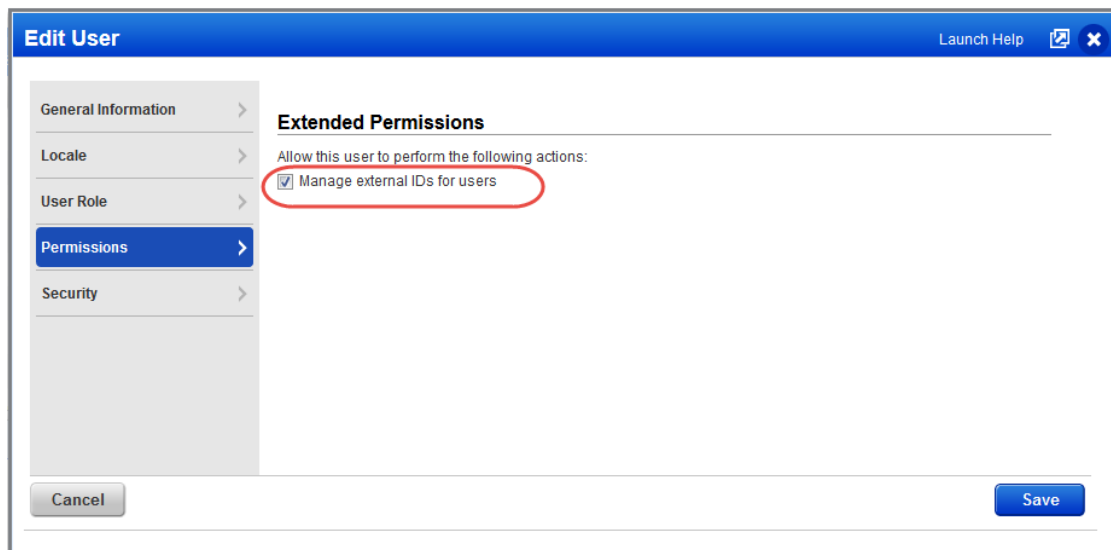
We've expanded the permissions granted to users with the User Administrator role.

They can now:

Edit and delete Manager user accounts. There must always be at least one Manager account in the subscription. A User Administrator cannot delete the last Manager account and cannot change the role for the last Manager account.

Add external IDs for users. The User Administrator must be granted the "Manage external IDs for users" permission, as shown below. This works in the same way for Managers and Unit Managers. The Manager Primary Contact for the subscription must first enable the External IDs security setting (under Users > Setup > Security) and then grant individual users this permission in their account settings.

New extended permission for User Administrators



The screenshot shows the 'Edit User' dialog box with a blue header bar containing 'Edit User', 'Launch Help', and a close button. On the left is a sidebar with menu items: 'General Information', 'Locale', 'User Role', 'Permissions' (highlighted in blue), and 'Security'. The main area is titled 'Extended Permissions' and contains the text 'Allow this user to perform the following actions:'. Below this text is a single checkbox labeled 'Manage external IDs for users', which is checked and circled in red. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Qualys Policy Compliance (PC/SCAP/SCA)

Failure Summary Section in Policy Compliance Reports

You can now add a new summary section to the PC Report which highlights required values that are missing or unexpected in failed controls. This makes it easier to identify what configuration settings caused failure of a control. This is especially useful in controls that return long lists of data such as CID's that return lists of users on a system in groups or with certain privileges. In case the failed control has multiple data points then this summary section is not displayed for that control.

Go to Reports > Templates > New > Policy Template and enable the options under Cause of Failure section.

The screenshot shows the 'New Compliance Policy Template' dialog box. On the left is a sidebar with navigation options: General Information, Layout (selected), Display, Trending, Frameworks, and User Access. The main area is divided into several sections. The 'Cause of Failure' section is highlighted with a red circle and contains two checked checkboxes: 'Unexpected values' and 'Missing values'. Other sections include 'Extended Evidence', 'Exception', 'History', 'Remediation Info' (with 'For Failed Controls' and 'For Passed Controls' checked), 'Glossary', and 'Appendix'. At the bottom are 'Cancel', 'Save As...', and 'Save' buttons.

In your Policy Compliance report navigate to the Cause of Failure section of a failed control.

The screenshot shows a failed control report for '(1.23) 2391 Current list of Groups and User Accounts granted the 'Allow log on locally (SeInteractiveLogonRight)' right'. The report includes a description of the user right, a table of expected and actual values, and a remediation path. The 'Cause of Failure' section is highlighted with a red circle and contains two sections: 'Unexpected values' and 'Missing values'. The 'Unexpected values' section lists 'BUILTIN\Backup Operators', 'BUILTIN\Power Users', and 'BUILTIN\Users'. The 'Missing values' section lists 'guest' and 'Right not assigned'.

Expected	Actual
matches regular expression list	Last updated: 02/01/2018 at 18:50:32 (GMT+0530)
Administrators	BUILTIN\Administrators
guest	BUILTIN\Backup Operators
	BUILTIN\Power Users
	BUILTIN\Users

Remediation: To establish the recommended configuration via GP, set the following UI path to Administrators, Users: Computer

Cause of Failure:

Unexpected values	Missing values
Additional values found in failed controls:	Expected values not found in failed controls:
BUILTIN\Backup Operators	guest
BUILTIN\Power Users	Right not assigned
BUILTIN\Users	

Issues Addressed

- Fixed an issue where the Approve Hosts window for Map Results did not show IP addresses of hosts previously approved. Now newly selected IPs for approval are appended to the list of previously approved IPs.
- Host Information now appropriately displays authentication records for Cisco/Unix and Checkpoint Firewall records.
- Fixed an issue where the Scanner Appliance API was showing a negative value for MAX_CAPACITY_UNITS. This is fixed, and now a negative value is not shown.
- We fixed an issue in CSV Compliance Reports where a current value of “0” in the Evidence column was appearing blank. Now we’ll show the value.
- The Host List page now refreshes faster even after the IPv6 addon is enabled.
- Purge options are now displayed correctly to a Scanner user having appropriate permissions.
- The Tickets tab under Remediation will now be the default landing page for a user with the Remediation user role.
- Previously, the SCA agent’s data was not getting processed in spite of the agent being activated for SCA. This is fixed, and now the SCA agent’s data is processed, and the policy report gets populated for SCA enabled agents.
- Fixed an issue that resulted in task status ERROR for some customers when running vulnerability scans using the default scanner appliance option on asset groups without scanner appliances.
- We fixed an issue where some customers got an error when generating reports on asset groups that contain only DNS hostnames.
- We fixed an issue where some customers got an empty Host-based Scan Report when including search lists that only contained Potential Vulnerabilities.
- Fixed the issue where Superseded QIDs were not correctly included/excluded in a Host-based Scan Report under certain specific scenarios.
- We fixed an issue so that QIDs no longer overlap in PDF scan based reports and PCI reports.
- The fixed QID is now not displayed in the Patch report. The issue was fixed in Patch report re-design feature.
- We’ve updated the graphs and charts in the PC Policy Report and SCAP Scorecard Report to have a consistent look with other reports.
- We fixed an issue in the Mandate Report Template with selecting/clearing All Status and Criticality check boxes.
- The Mandate Report Template will now correctly show user names in the Owner menu.
- We improved the error message that is displayed when trying to add duplicate IP addresses in VMware authentication records.
- We improved the online screen text in the Remove IPs workflow for accounts that do not have Cloud Agent enabled.