



Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.19

May 6, 2019

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

Qualys Vulnerability Management (VM)

[Enhanced View of Remediation Policy Deadlines](#)

Qualys Policy Compliance (PC)

[Support for Microsoft Exchange Server Authentication](#)

[Layout Options Enable by Default in Policy Report Templates](#)

Qualys Cloud Platform

[Renamed Scan Agent Hosts Option](#)

[Sybase Authentication - Password Encryption and Auto Discover Databases](#)

[Support for Microsoft Azure Key Vault](#)

Qualys 8.19 brings you many more improvements and updates! [Learn more](#)

Qualys Vulnerability Management (VM)

Enhanced View of Remediation Policy Deadlines

We have enhanced the Policies tab data list to easily understand the deadlines set for the remediation policy rules.

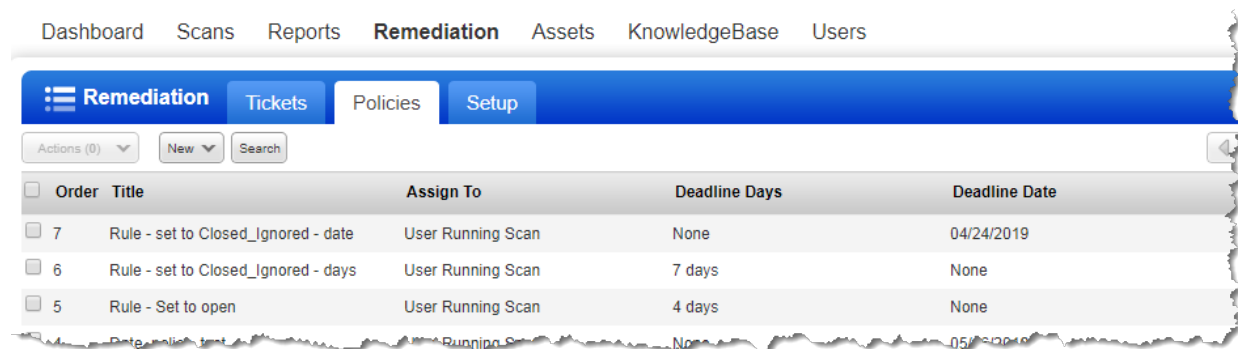
The Deadlines column is now split into two columns: Deadline Date and Deadline Days. Depending on the action you choose while creating remediation tickets the date or day column is populated and can be easily sorted.

Simply navigate to Remediation > Policies > New > Rule and provide required information to create the rule.

In the Actions tab:

If you choose the action Create tickets - set to Open, then the Deadline Days column shows the number of days in which the ticket must be closed.

If you choose the Create tickets - set to Closed/Ignored and set the reopen ticket option in days then the Deadline Days column is populated. If you choose the option to reopen the ticket after the set date then that date is shown in the Deadline Date column.



The screenshot shows the Qualys Remediation interface. At the top, there are navigation tabs: Dashboard, Scans, Reports, Remediation (selected), Assets, KnowledgeBase, and Users. Below this is a sub-navigation bar with Remediation, Tickets, Policies (selected), and Setup. There are also buttons for Actions (0), New, and Search. The main content is a table with the following data:

Order	Title	Assign To	Deadline Days	Deadline Date
7	Rule - set to Closed_Ignored - date	User Running Scan	None	04/24/2019
6	Rule - set to Closed_Ignored - days	User Running Scan	7 days	None
5	Rule - Set to open	User Running Scan	4 days	None

Qualys Policy Compliance (PC)

Support for Microsoft Exchange Server Authentication

We now support MS Exchange Server authentication for compliance scans using Qualys PC.

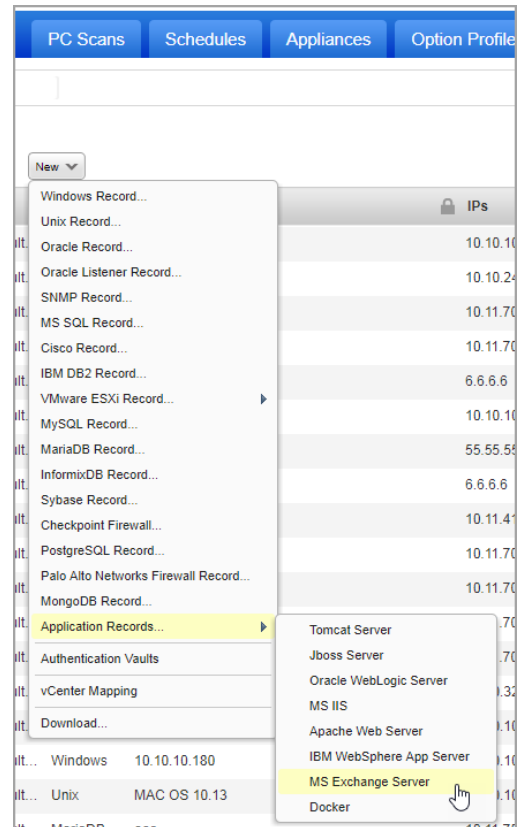
Simply create an MS Exchange Server record in order to authenticate to a Microsoft Exchange Server running on a Windows host, and scan it for compliance.

How do I get started?

Go to Scans > Authentication, and choose Application Records > MS Exchange Server Record.

We'll authenticate to each target host using the credentials provided in the Windows record.

We'll use credentials from the Windows record to authenticate to the Windows system, access the web server configuration, and scan it for compliance.



Layout Options Enable by Default in Policy Report Templates

We have now pre-enable some layout options while creating new Policy Report Templates so that additional features are enabled by default in the template to enhance reports.

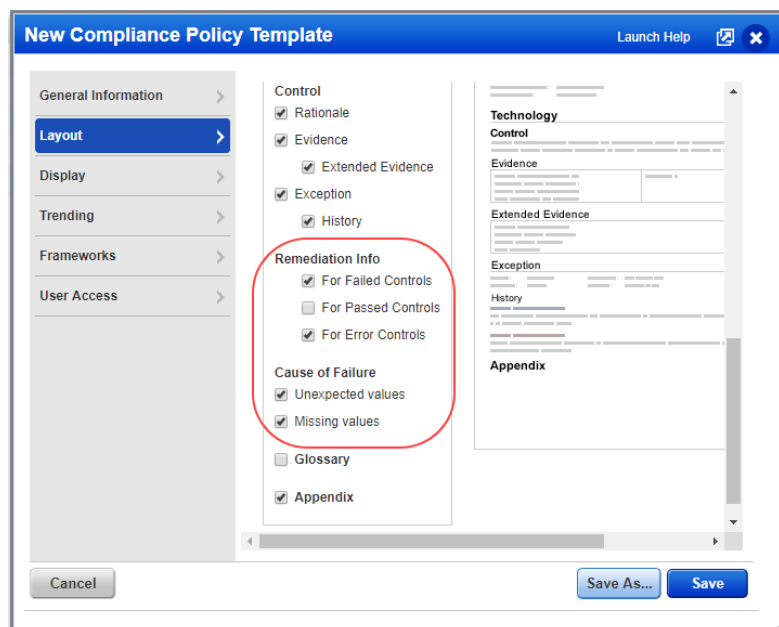
Navigate to Reports > Templates > New and go to the Layout tab. You will see these fields pre-enabled for you.

Remediation info

- For Failed Controls
- For Error Controls

Cause of Failure

- Unexpected values
- Missing Values



Qualys Cloud Platform

Renamed Scan Agent Hosts Option (VM, PC)

In the Target Hosts section of Launch/Schedule Scan pages, we have changed the label "Scan agent hosts in my target" to "Temporarily add agent addresses not currently in my subscription". This option temporarily adds the IP addresses of any agents in your target to your subscription for this scan only.

The option is visible only if Qualys Cloud Agent is enabled for your subscription.

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

Assets Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: fe80::912e:21f6:887e:fff1, fe80::912e:21f6:887e:fff2

Exclude IPs/Ranges

Example: fe80::912e:21f6:887e:fff1, fe80::912e:21f6:887e:fff2

Temporarily add agent addresses not currently in my subscription

Notification

Send notification when this scan is finished

[Launch](#) [Cancel](#)

Temporarily add agent addresses

You will need to select this option if your scan target includes agents that may have acquired IPs not in your subscription. Without this option the scan will not execute and will generate an error due to the addresses not being in your subscription. This option temporarily adds the IP addresses of any agents in your target to your subscription for this scan only. Cannot be used with the External scanner option.

Sybase Authentication - Password Encryption and Auto Discover Databases

This release introduces 2 new options for Sybase basic and vault authentication – Enable Password Encryption and Auto Discover databases.

Enable Password Encryption - Enable this option when your Sybase database instance requires an encrypted password for successful login. If password encryption is required and you do not enable this option then authentication will fail.

Auto Discover - Enable this option and we'll find all Sybase database names on each host for you. This means you no longer have to create a separate Sybase record for each database name. Create one record with Auto Discover Databases enabled to authenticate to multiple databases on the same host.

Sybase Authentication Record - Google Chrome
https://qualysguard.p04.eng.sjc01.qualys.com/fo/options/sybase_auth_edit.php?type=sybase&refresh_parent=1&text_edit=1

Record Title >
Login Credentials >
IPs >
Comments >

Login Credentials

Basic Authentication Authentication Vault

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Username *

Password *

Confirm Password *

Enable Password Encryption

Database Information

Tell us the name and port the database is running on and we'll find the database instance to authenticate to. For Unix hosts, the installation directory is also required.

Database Name: Auto discover

Installation Directory:

Required for Unix based hosts. Example: /opt/sybase

Port *

Cancel Save

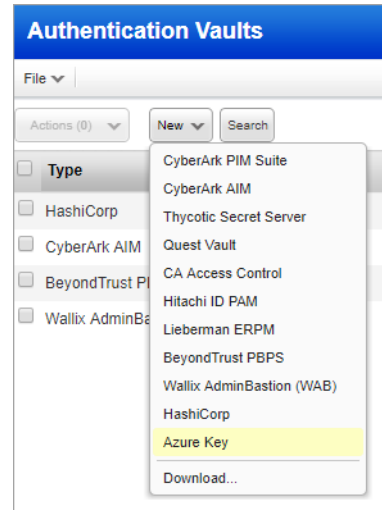
Support for Microsoft Azure Key Vault

This new vault type can be used to retrieve authentication credentials from an Azure key vault.

What are the steps?

You'll configure Azure key vaults (vault credentials), configure authentication records for Cisco, Checkpoint Firewall, Windows, Unix, MS SQL, MySQL, MariaDB, MongoDB, Oracle, PostgreSQL, authentication types, and start your scans.

Note: For PostgreSQL, we support only private keys and passphrase retrieval since the Azure key vault supports only retrieval of private keys and passphrase. Password retrieval is NOT supported for PostgreSQL.



Configure your Azure Key Vault

Go to Scans > Authentication > New > Authentication Vaults. Then choose New > Azure key.

A screenshot of the 'New Azure Key Vault' configuration form. The form has a blue header with the text 'New Azure Key Vault' and a 'Launch Help' link. Below the header, there's a 'Vault Title' section with a text input field containing 'My Azure Key Vault'. The next section is 'Vault Credentials', which includes a 'URL' field with 'https://example.vault.azure.net' and a note: '[example: https://ml-test-vault.vault.azure.net]'. Below that, there's a checkbox for 'SSL Verify' which is checked, with a note: 'We'll verify that the server's SSL certificate is valid and trusted. Clear this option to skip SSL verification'. The 'APP ID' field contains '17d4d1c3-6358-4358-b060-a2d0c6353f66'. The 'Certificate' field contains 'PEM-encoded X.509 certificate' and has a green checkmark icon. The 'Private Key' field is empty. The 'Passphrase' field is empty, with a note: 'Please provide a Passphrase if the Private Key is encrypted.' At the bottom, there's a 'Comments' section with a text area. At the very bottom, there are 'Save' and 'Cancel' buttons.

Provide vault credentials.

URL – The HTTP or HTTPS URL to access the Azure Vault HTTP API.

SSL Verify – Applies when the URL uses HTTPS. We'll verify the SSL certificate of the web server to make sure it's valid and trusted, unless you clear (un-check) this option.

API ID – The application ID associated with your vault application created in the Azure Key Vault.

Certificate – The client certificate for authentication. Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE-----and ---END CERTIFICATE-----). For a create/update request, if the cert parameter is specified, then the private_key parameter must also be specified.

Private Key – The private key for authentication. Copy the contents of private key file (id_rsa) and be sure to include the first and last line (-----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----). For a create/update request, if the private_key parameter is specified, then the cert parameter must also be specified.

Passphrase - The private key passphrase, if the private key is encrypted.

Configure authentication records

The Azure key vault is supported in Windows, Unix, MS SQL, MySQL, MariaDB, MongoDB, Oracle, PostgreSQL records. Here's a sample Windows record with the vault selected.

The screenshot shows the 'New Windows Record' configuration page. The left sidebar contains 'Record Title', 'Login Credentials', 'IPs', and 'Comments'. The main content area is titled 'Login Credentials' and 'Windows Authentication'. Under 'Windows Authentication', 'Domain' is selected. The 'Domain type' is 'NetBIOS, User-Selected IPs' and the 'Domain name' is 'my domain'. Below this is the 'Login' section, where 'Authentication Vault' is selected. The 'User Name' is 'joe'. The 'Vault Type' is 'Azure Key', 'Vault Title' is 'My Azure Key Vault', and 'Azure Key Secret Name' is 'Secret'. A red rounded rectangle highlights the 'Vault Type', 'Vault Title', and 'Azure Key Secret Name' fields. A 'Select' button is next to the 'Vault Title' field.

Provide these settings:

Vault Type – Azure Key

Vault Title – Your vault record.

Azure Key Secret Name

The secret name assigned to the secret stored in the vault.

Issues Addressed

- Now, the user will be able to update and delete Report Templates from UI that are created using API and from UI.
- Activity log is now generated when you enable or disable the "Purge old host data when OS is changed" option in an Option Profile.
- Fixed an issue where compliance policy report after scan and compliance policy report after manual re-evaluation of policy contained inconsistent data.
- Fixed an issue where the Unit Manager could not fetch host information using MSP API (/msp/get_host_info.php) in spite of having the required permission and access.
- Fixed an issue where users were getting blank scorecard reports when using asset tags with ALL filter.
- We have now fixed the issue so that the database related compliance scan data (list of policies) is retained on the host information page when you scan the asset through the scanner, has Cloud Agent installed on it and asset merging enabled for the subscription.
- Apache Web Server instances are now reported accurately in scan report for scans launched with discovery options for "Apache Web Server" enable, irrespective of the role of the user that launched the scan (previously, instances were reported only if the discovery scan is launched by user with POC-Manager role).
- For SCA only accounts, we have now enabled the Evaluate option in the Policies tab from the Actions and Quick Actions menu.
- For customers leveraging client certificates we fixed an issue where unrelated changes to the account configuration caused the certificate being used for login to get reset.
- Updated the help to explain report results when using search lists with Threat Protection RTI filters and the Exclude Superseded Patches report filter.
- Updated the help for configuring an option profile. Under "Select ports to scan" you'll see new content describing TCP ACK and SYN+ACK packets sent during host discovery and their destination ports.
- Fixed an issue where users were unable to edit a scheduled EC2 scan for subscriptions with CertView add-on.
- The Tech column in Reports > Control View tab displayed incorrect icon for MS Exchange. Now, we have removed the icons from the Tech column to prevent incorrect display of icons.
- Updated the help to clearly document that once a user is created with a "User administrator" role then the role for that user cannot be changed to any other role.
- Updated the help and Consulting Edition Getting Started Guide to explain that Scanner users in Consultant subscriptions may be granted the Add assets permission giving them the ability to add IP addresses to the subscription.
- We updated the Vulnerability Categories topic in Online help to add the missing vulnerability categories. We added the following categories: AIX, Amazon, Linux, CentOS, Cisco, Fedora, HP-UX, NFS, Oracle VM Server, QRD, RedHat, SMB\NETBIOS, Solaris, TCP\IP, VMware, Web Application and Web Application Firewall.
- Updated the help to explain that if you're using the BeyondTrust PBPS vault with Palo Alto Networks Firewall authentication, then you must directly enter the system name in

the Palo Alto Networks Firewall record because auto-discovery of the system name is not supported for this authentication type.

- Updated the help for Scheduled Scans to explain that when using pause and automatic resume, we resume the scan based on the scan start time and not when the scan was paused.
- In the Qualys API (VM, PC) User Guide, we have updated the "Limit" parameter description for the Vault API to specify that "0" is not a valid value for this parameter.
- In the Qualys API (VM, PC) User Guide, we have updated the parameter descriptions for `arf_service_filter` and `arf_config_filter`. Now setting `arf_service_filter` to 2 shows 0 in the output for each detection for exploitable vulnerabilities; when the parameter is set to 3, the output shows 1 for each detection for not exploitable vulnerabilities. Similarly, now setting `arf_config_filter` to 2 shows 0 in the output for each detection for exploitable vulnerabilities; when the parameter is set to 3, the output shows 1 for each detection for not exploitable vulnerabilities.
- Updated the Qualys API (VM, PC) User Guide to mention that Managers and Unit Managers can launch VM and compliance scans on EC2 assets.
- In the Qualys API (VM, PC) User Guide, we have fixed the endpoint from "scan" to "report" in the API URL given in the sample "Delete Saved Report" request.