Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.21.3

October 10, 2019

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

Qualys Cloud Platform

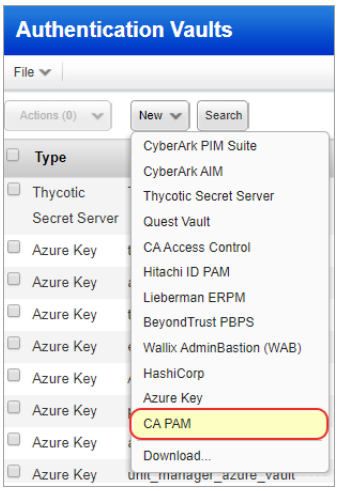
Support for CA PAM (Privileged Access Manager) Vaults

Qualys 8.21.3 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

Support for CA PAM (Privileged Access Manager) Vaults

This new vault type can be used to retrieve authentication credentials from a CA PAM vault.

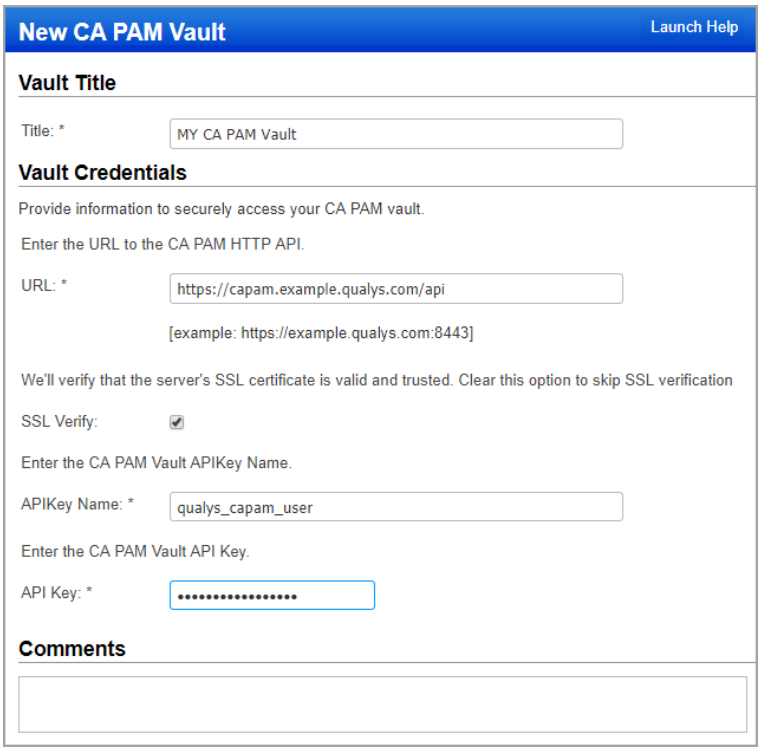


What are the steps?

You'll configure CA PAM vaults (vault credentials), configure authentication records for Windows, Unix, and/or Cisco authentication types, and start your scans.

Configure your CA PAM Vault

Go to Scans > Authentication > New > Authentication Vaults. Then choose New > CA PAM.



Provide vault credentials

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

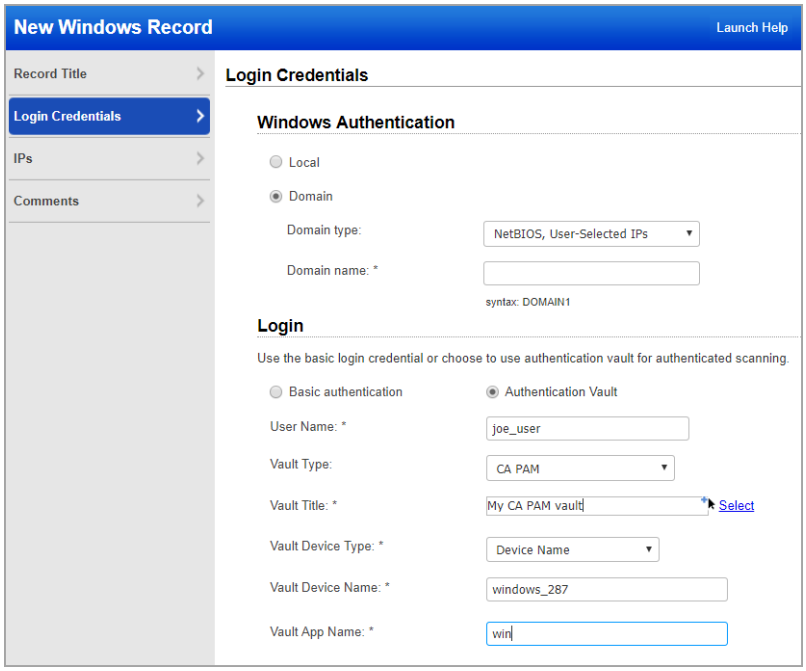
SSL Verify – Qualys scanners will verify the SSL certificate of the web server to make sure the certificate is valid and trusted, unless you clear (un-check) the SSL Verify option. You may want to clear this option to skip SSL verification if the certificate was not issued by a well-known certification authority (CA) or if the certificate is self-signed.

APIKey Name – The user account that can call the CA PAM Vault HTTP API.

API Key – The password for the user account that can call the CA PAM Vault HTTP API.

Configure authentication records

The CA PAM vault is supported in Windows, Unix and Cisco authentication records. Here's a sample Windows record with the vault selected.



Provide these settings:

Vault Type – CA PAM

Vault Title – Your vault record.

Vault Device Type

The type of device for which password is stored. Select Device Name or Device Host.

Vault Device Name

Enter the device name defined in the vault configuration.

Vault Device Host

Enter the host name defined in the vault configuration.

Note that you can use one or more variables when defining the "device name" or "device host" in order to match several targets that use the same naming convention.

Vault App Name

Application name as defined in the vault configuration for accessing a specific device.

Using Variables in the device name or device host

You can use one or more variables when defining the device name or device host in order to match several targets that use the same naming convention. During scan, we replace the variable which becomes a value when expanded to match the hosts that is already defined in the vault.

${ip} // The IP address of the target, i.e. 10.20.30.40.

${ip_dash} // The IP address of the target with dashes instead of dots, i.e. 10-20-30-40.

${dnshost} // The DNS host name of the target, i.e. host.domain.

${host} // The host name of the target, i.e. host before .domain.

${nbhost} // (Windows only) The NetBIOS host name of the target in upper-case, i.e. HOST_ABC.

For example, ${host}-${ip_dash} will match these 3 devices: host40-10-20-30-40, host80-10-50-60-70 and host12-10-30-10-12.

Issues Addressed

- The issue is now fixed and the <CRITERIA> tag will be rendered in Policy Report XML format for all technology data points.
- We have fixed an issue and now the V tag value is not enclosed in CDATA for boolean, integer, integer-list data-types when exporting a policy.
- We have fixed an issue where the Assets > Applications tab was taking longer than expected to load.
- Fixed an issue where target IPs did not appear in the VM Scan List API (/api/2.0/fo/scan/?action=list) output for running EC2 scans.
- Updated the online help for MS SQL Server Authentication to clarify requirements for VM and PC scans.
- Fixed an issue where the list of authentication status QIDs in the online help included QIDs that were not valid.
- Updated the online help to explain that for successful Unix authentication for F5 Load Balancers the user account provided for authentication must meet these requirements: 1) have Administrator or Resource Administrator role, and 2) Terminal Access must be set to "Advanced shell (bash)".