Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.14

June 13, 2018

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

Qualys Vulnerability Management (VM)

Label Name changed from Cyber-Ark to CyberArk
Support for EC2 Scanning using only Instance ID
XML Format Supported for Patch Reports
Consultant Subscription: Manage Your Clients
Update to ESX/ESXi authentication mapping option

Qualys Policy Compliance (PC/SCAP/SCA)

Microsoft SQL Server 2017 Support
Support for SCA Agent on Windows and Linux
Generate STIG Based Reports to View Security Posture

Qualys Cloud Platform

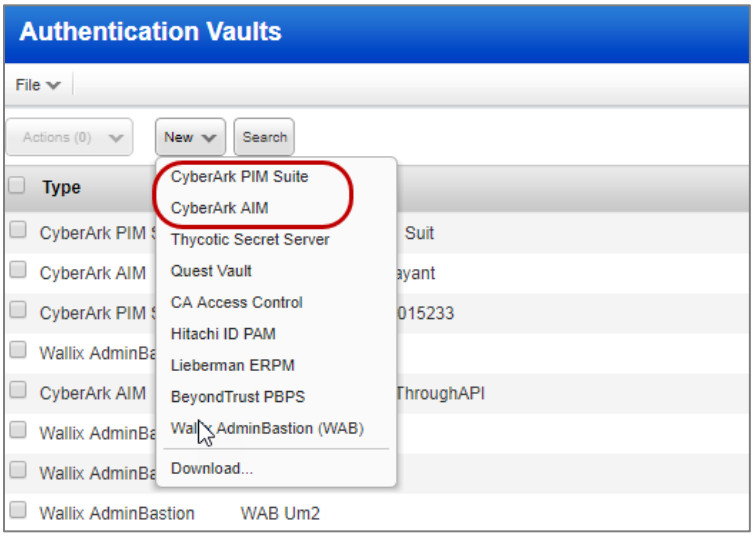
Support for Wallix AdminBastion (WAB) Vaults
Upgraded SimpleSAMLphp Library

Qualys 8.14 brings you many more Improvements and updates! Learn more

Qualys Vulnerability Management (VM)

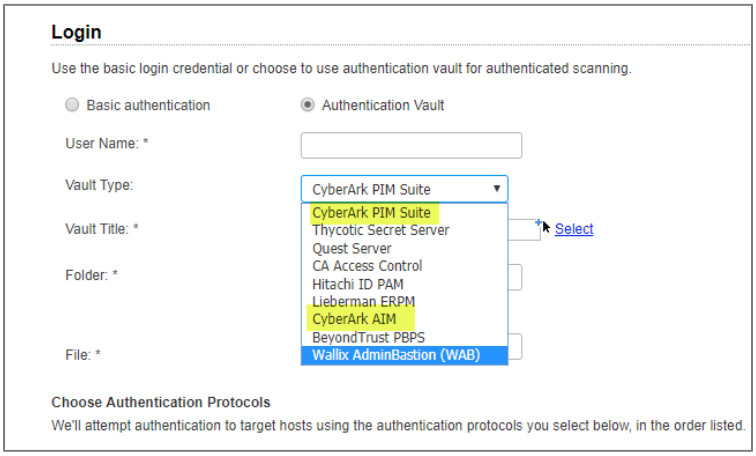
Label Name changed from Cyber-Ark to CyberArk

We have changed label name from Cyber-Ark to CyberArk (removed the hyphen) for improved integration of CyberArk vaults.



Authentication Vaults

Go to Scans > Authentication > New > Authentication Vault. When you click New, you will notice we have changed Cyber-Ark vaults to CyberArk vaults (removed the hyphen).



Authentication

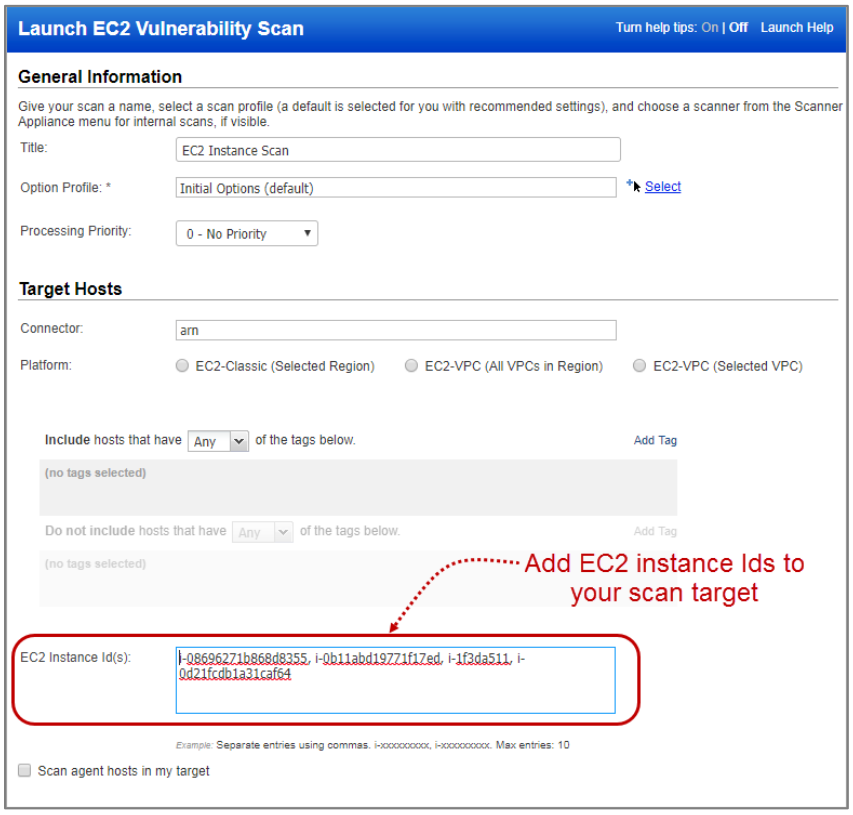
When you configure authentication vault for login credentials during authentication, you will notice that we have changed Cyber-Ark vaults to CyberArk vaults (removed the hyphen).

Support for EC2 Scanning using only Instance ID

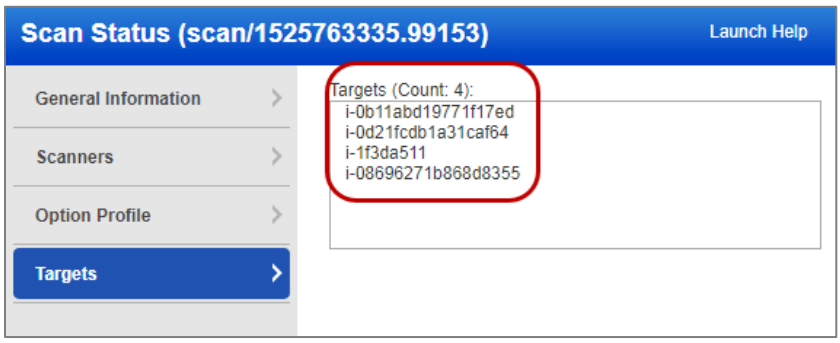
We now support launch of on demand internal EC2 scans using EC2 instance Ids. You can launch scans using only the EC2 instance Ids or only tags or both as well. Using tags for EC2 scans is now optional.

Launch VM Scan

Go to Scans > New > EC2 scans. Provide a title to the scan. You can directly add EC2 instance Id(s) to the Target Hosts. Multiple EC2 instance Ids are comma-separated. You can add up to 10 instance Ids.



Once you launch the scan, view the EC2 instances in the Target section of the scan status.

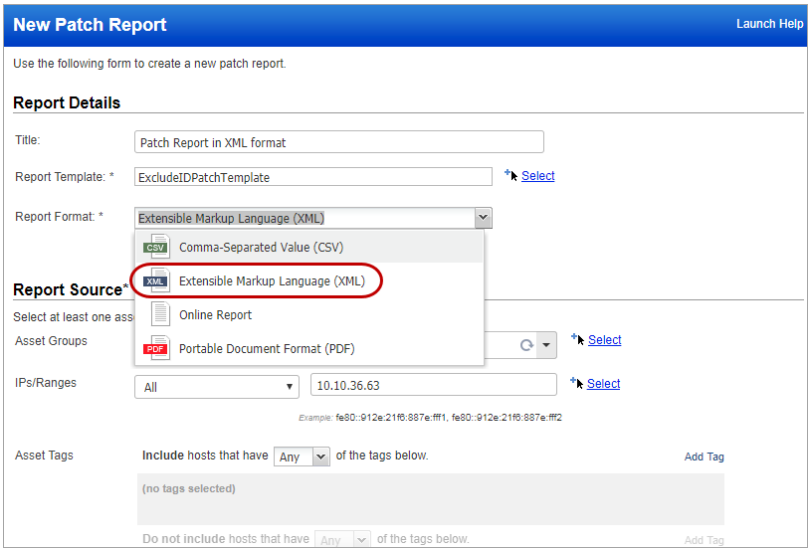


EC2 scanning using EC2 instance Id is also supported for compliance scans.

XML Format Supported for Patch Reports

You can now generate patch reports in XML format. We previously supported CSV, PDF and online reports.

Go to Reports > New > Patch Report. Provide a report title, select a patch report template and then pick Extensible Markup Language (XML) as the Report Format. Define the Report Source and click Run.



When the report is complete, click Download from the Quick Actions menu.

Here's a sample XML report:

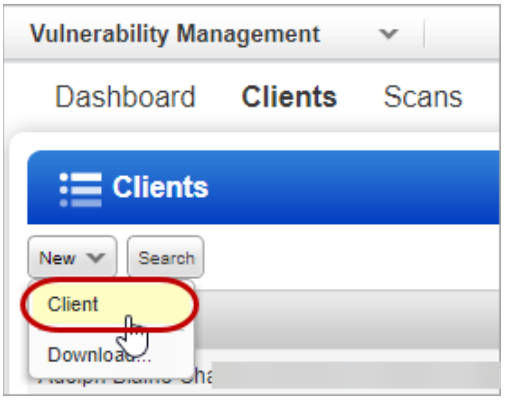
```
<!DOCTYPE PATCH_REPORT SYSTEM "https://                    .com/patch_report.dtd">
<PATCH_REPORT>
  <HEADER>
    <NAME><![CDATA[Patch Report in XML Format]]></NAME>
    <GENERATION_DATETIME>2018-05-03T12:34:49Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[User John]]></NAME>
      <ADDRESS><![CDATA[a1,a2]]></ADDRESS>
      <CITY><![CDATA[Pune]]></CITY>
      <STATE><![CDATA[]]></STATE>
      <COUNTRY><![CDATA[India]]></COUNTRY>
      <ZIP_CODE><![CDATA[411001]]></ZIP_CODE>
    </COMPANY_INFO>
    <USER_INFO>
      <NAME><![CDATA[John Doe]]></NAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
  </HEADER>
  <SUMMARY>
    <REPORT_SUMMARY>
      <TITLE><![CDATA[Patch Report in XML Format]]></TITLE>
      <GROUP_LIST><![CDATA[10.113.197.209-10.113.197.210]]></GROUP_LIST>
      <IP_LIST>N/A</IP_LIST>
      <TAG_LIST><![CDATA[N/A]]></TAG_LIST>
      <GROUP_BY><![CDATA[Patch]]></GROUP_BY>
      <CREATED_ON>05/03/2018</CREATED_ON>
      <NETWORK><![CDATA[All]]></NETWORK>
    </REPORT_SUMMARY>
    <PATCH_SUMMARY>
      <TOTAL_PATCHES>9</TOTAL_PATCHES>
      <HOST_REQUIRING_PATCHES>1</HOST_REQUIRING_PATCHES>
      <VULN_ADDRESSED><![CDATA[37]]></VULN_ADDRESSED>
    </PATCH_SUMMARY>
  </SUMMARY>
  <PATCH_LIST_BY_QID>
    <PATCH_LIST>
      <PATCH_INFO>
        <QID>38623</QID>
        <VENDOR_ID>OpenSSH 7.2p2</VENDOR_ID>
        <SEVERITY>5</SEVERITY>
        <PATCH_TITLE><![CDATA[OpenSSH Xauth Command Injection Vulnerability]]></PATCH_TITLE>
        <HOST_COUNT>1</HOST_COUNT>
        <PATCH_PUBLISHED>03/10/2016</PATCH_PUBLISHED>
```

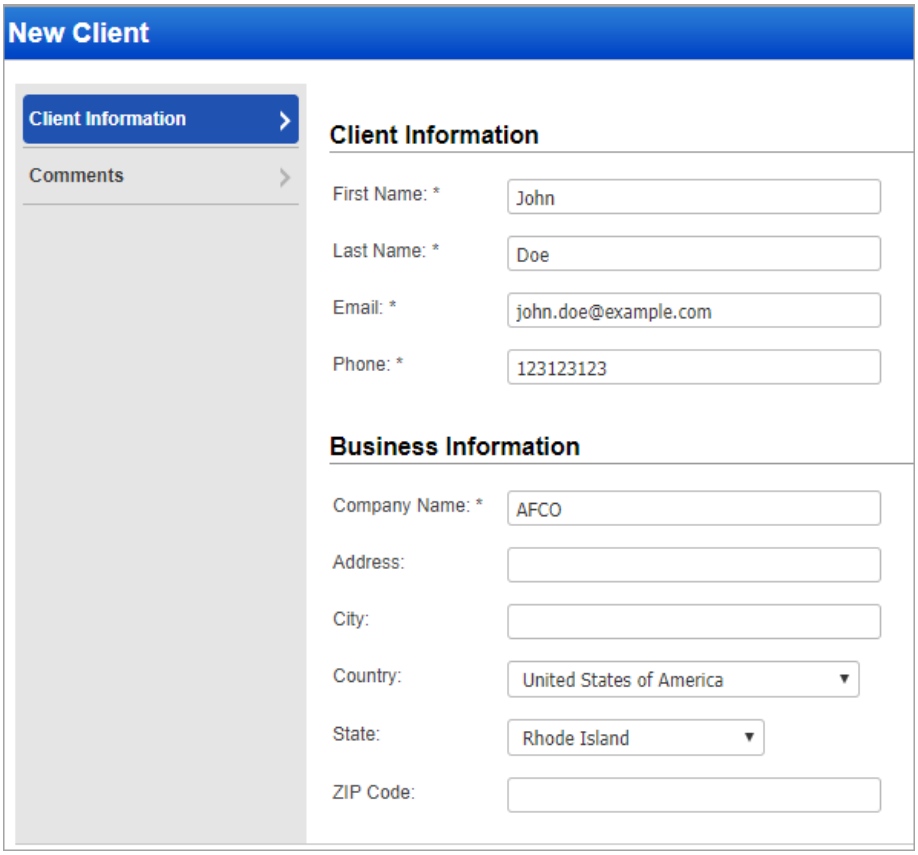
Consultant Subscription: Manage Your Clients

We have now introduced a new feature for Consultant subscribers that allows you to manage your clients – add or edit client details, launch scans, launch reports, and so on. It gives you the flexibility to separately manage your clients.

Add Clients

Go to Clients > New > Client and then you can add details about your clients.





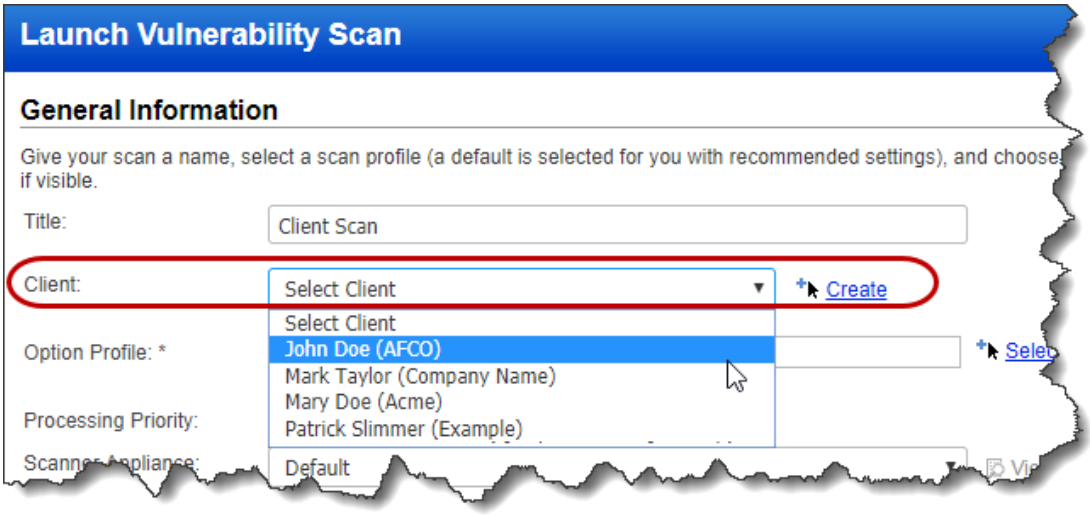
Provide the following details for your client:

- Client Information
- Business Information
- Comments

Click Save and your client gets added.

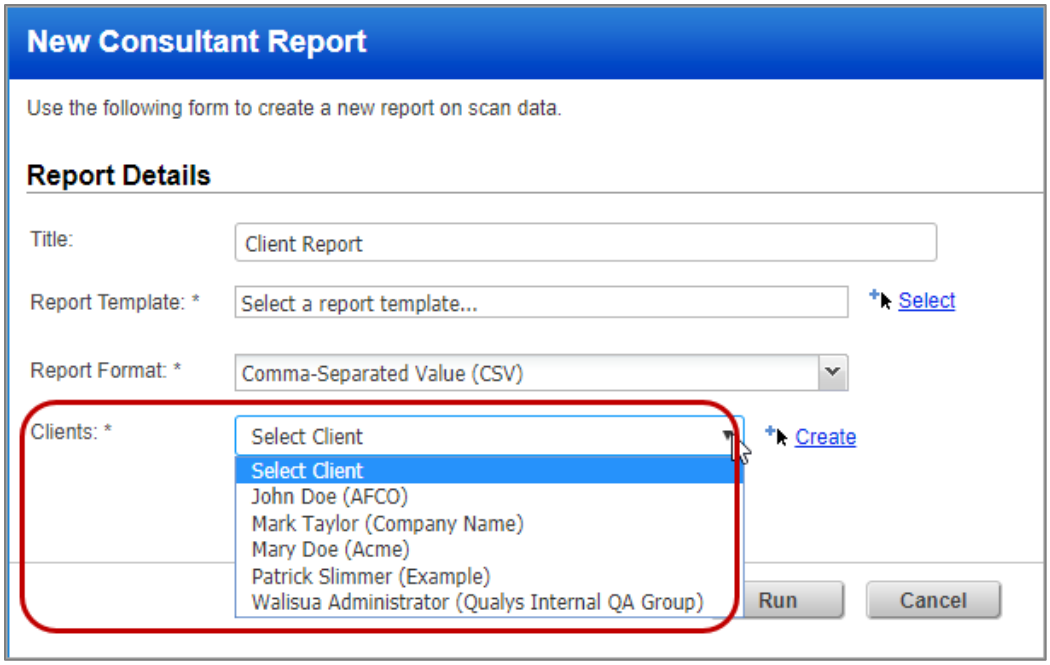
Launch Scans

Go to Scans > Scans > New Scan and then choose the client from the drop-down. All the clients that you add are auto-populated. Provide other details needed for the scan and launch the scan.



View Reports

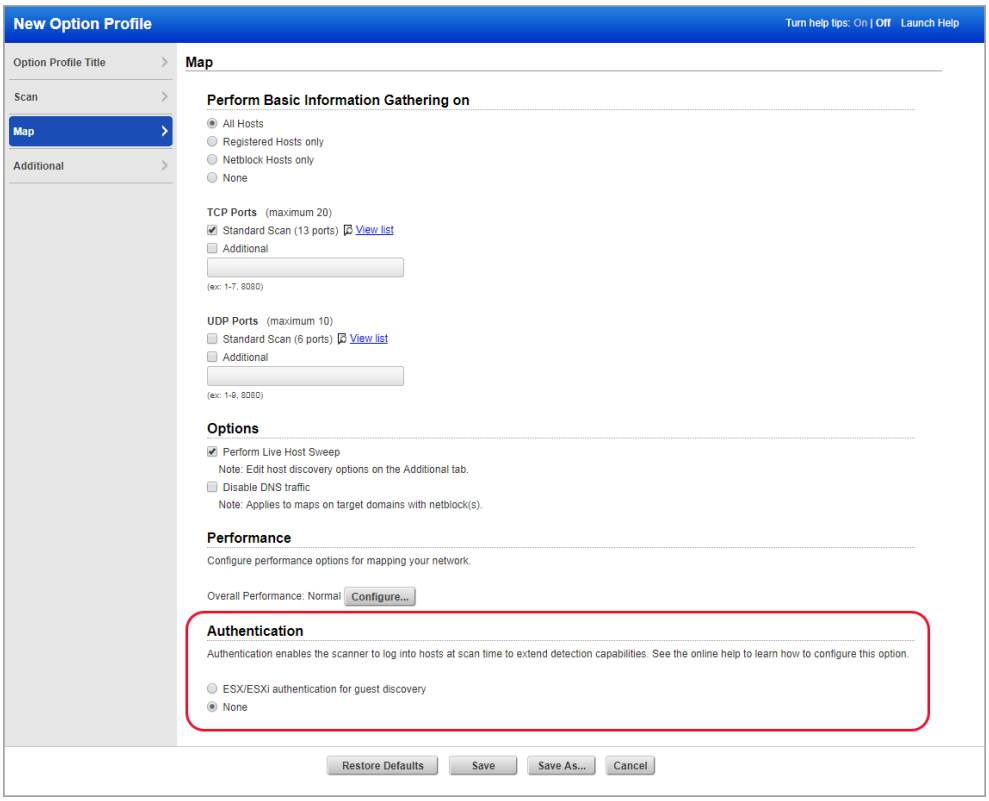
Go to Reports > Reports > New > Consultant Report and then you can choose the required client from the drop-down. All the clients that you add are auto-populated. Provide other details needed for the scan and launch the report.



Update to ESX/ESXi authentication mapping option

We have renamed the mapping option VMware to ESX/ESXi authentication for guest discovery.

In the Option Profile > Map go to Authentication section and the VMware option is now called ESX/ESXi authentication for guest discovery to support future capabilities.
Your existing option profiles will be updated automatically.

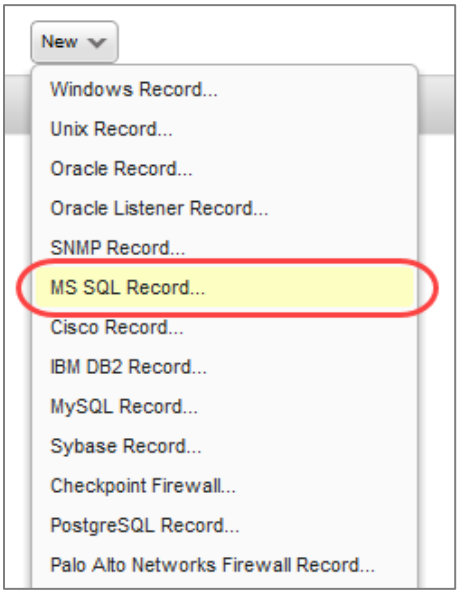


Qualys Policy Compliance (PC/SCAP/SCA)

Microsoft SQL Server 2017 Support

We've extended our support for MS SQL Server authentication to include Microsoft SQL Server 2017. These technologies are already supported: Microsoft SQL Server 2000, 2005, 2008, 2012, 2014 and 2016.

You'll need a MS SQL Server record to authenticate to your Microsoft SQL Server 2017 database, and scan it for compliance.



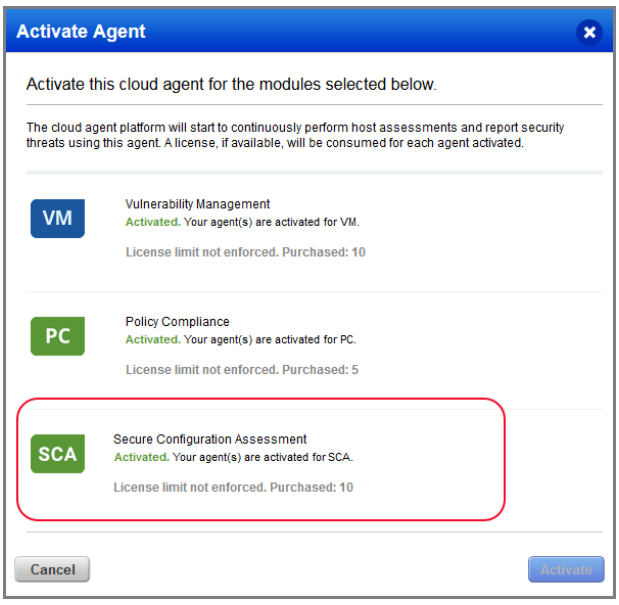
How do I get started?

Go to Scans > Authentication, and choose New > MS SQL Record. This authentication type is supported for compliance scans only.

Support for SCA Agent on Windows and Linux

We now support data collection for SCA using Cloud Agent on Windows and Linux.

Just activate agents for SCA from Cloud Agent > Agent Management > Agents.

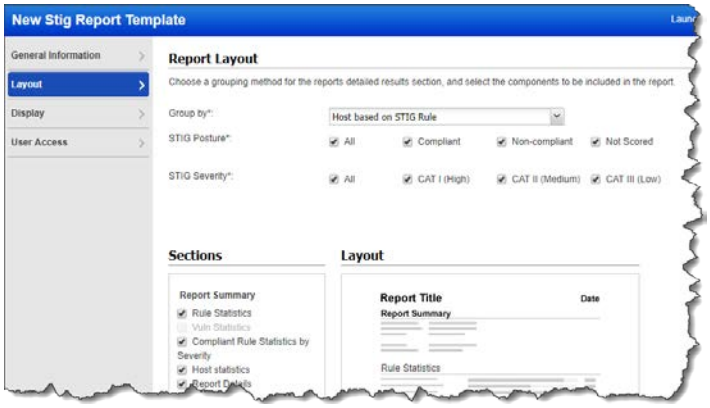


Generate STIG Based Reports to View Security Posture

Generate Security Technical Implementation Guides (STIG) Based Report to view the compliance and security posture of the organization in terms of the Defense Information Systems Agency (DISA). This report helps you to view control posture as per the Rule IDs or Vuln IDs provided in the DISA security technical implementation guides.

To generate a STIG based report:

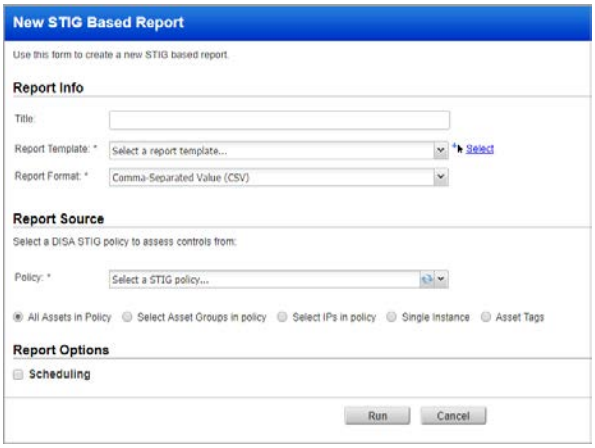
First you need to create a custom STIG based report template to create compliance report for the selected DISA STIG policy.



Just go to Reports > Templates > STIG Template and configure settings.

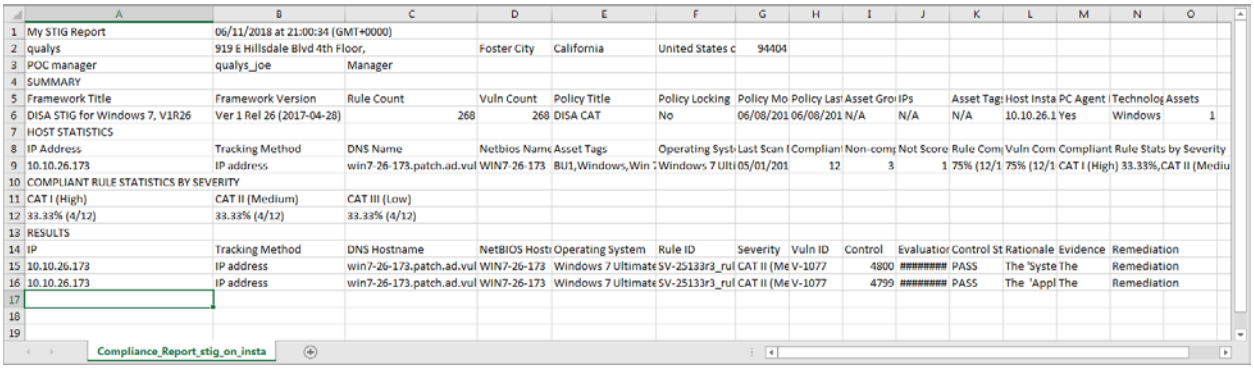
In the template define all that you want to display in your report for example which STIG postures and STIG severity. You can view results as per Rule IDs or Vuln IDs provided in the DISA benchmarks

Then, navigate to Reports > New > Compliance Report > STIG Based Report.



Select the STIG template you created, and choose a DISA STIG policy to assess controls and get a view of compliance posture against the selected policies.

Depending on what you select in the report layout while creating the custom STIG based report template, a report is generated in CSV format.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	My STIG Report	06/11/2018 at 21:00:34 (GMT+0000)													
2	qualys	919 E Hillsdale Blvd 4th Floor,		Foster City	California	United States c	94404								
3	POC manager	qualys_joe	Manager												
4	SUMMARY														
5	Framework Title	Framework Version	Rule Count	Vuln Count	Policy Title	Policy Locking	Policy Mo	Policy Las	Asset Gro	IPs	Asset Tags	Host Insta	PC Agent	Technolog	Assets
6	DISA STIG for Windows 7, V1R26	Ver 1 Rel 26 (2017-04-28)	268	268	DISA CAT	No	06/08/201	06/08/201	N/A	N/A	N/A	10.10.26.1	Yes	Windows	1
7	HOST STATISTICS														
8	IP Address	Tracking Method	DNS Name	Netbios Name	Asset Tags	Operating Syst	Last Scan I	Compliant	Non-comp	Not Score	Rule Com	Vuln Com	Compliant	Rule Stats by Severity	
9	10.10.26.173	IP address	win7-26-173.patch.ad.vul	WIN7-26-173	BU1,Windows,Win 7	Windows 7 Ulti	05/01/201	12	3	1	75% (12/1	75% (12/1	CAT I (High)	33.33%,CAT II (Mediu	
10	COMPLIANT RULE STATISTICS BY SEVERITY														
11	CAT I (High)	CAT II (Medium)	CAT III (Low)												
12	33.33% (4/12)	33.33% (4/12)	33.33% (4/12)												
13	RESULTS														
14	IP	Tracking Method	DNS Hostname	NetBIOS Host	Operating System	Rule ID	Severity	Vuln ID	Control	Evaluatior	Control St	Rationale	Evidence	Remediation	
15	10.10.26.173	IP address	win7-26-173.patch.ad.vul	WIN7-26-173	Windows 7 Ultimate	SV-25133r3_rul	CAT II (Me	V-1077	4800	########	PASS	The 'Syste	The	Remediation	
16	10.10.26.173	IP address	win7-26-173.patch.ad.vul	WIN7-26-173	Windows 7 Ultimate	SV-25133r3_rul	CAT II (Me	V-1077	4799	########	PASS	The 'Appl	The	Remediation	
17															
18															
19															

Compliance_Report_stig_on_insta

Qualys Cloud Platform

Support for Wallix AdminBastion (WAB) Vaults

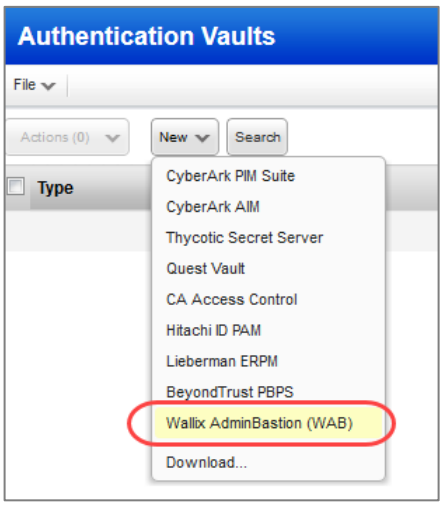
This new vault type can be used to retrieve authentication credentials from a Wallix AdminBastion (WAB) vault.

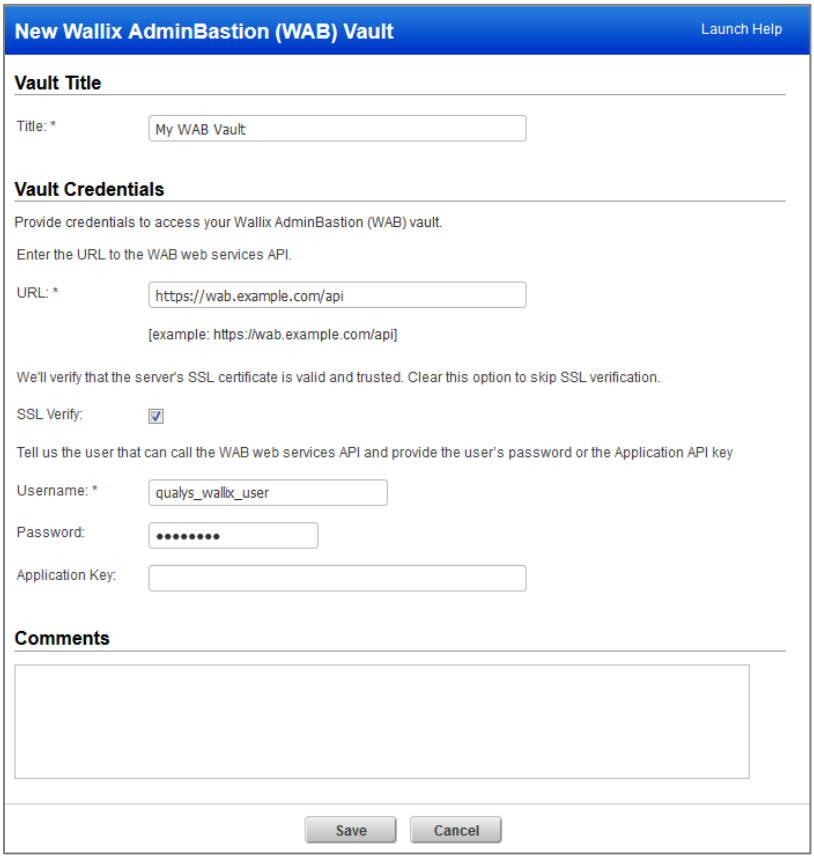
What are the steps?

You'll configure Wallix AdminBastion (WAB) vaults (vault credentials), configure authentication records for Windows and/or Unix authentication types, and start your scans.

Configure your Wallix AdminBastion (WAB) Vault

Go to Scans > Authentication > New > Authentication Vaults. Then choose New > Wallix AdminBastion (WAB).





Provide vault credentials.

URL - The HTTP or HTTPS URL to access the WAB web services 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.

Username - The user account that can call the WAB web services API (see user account requirements in the help).

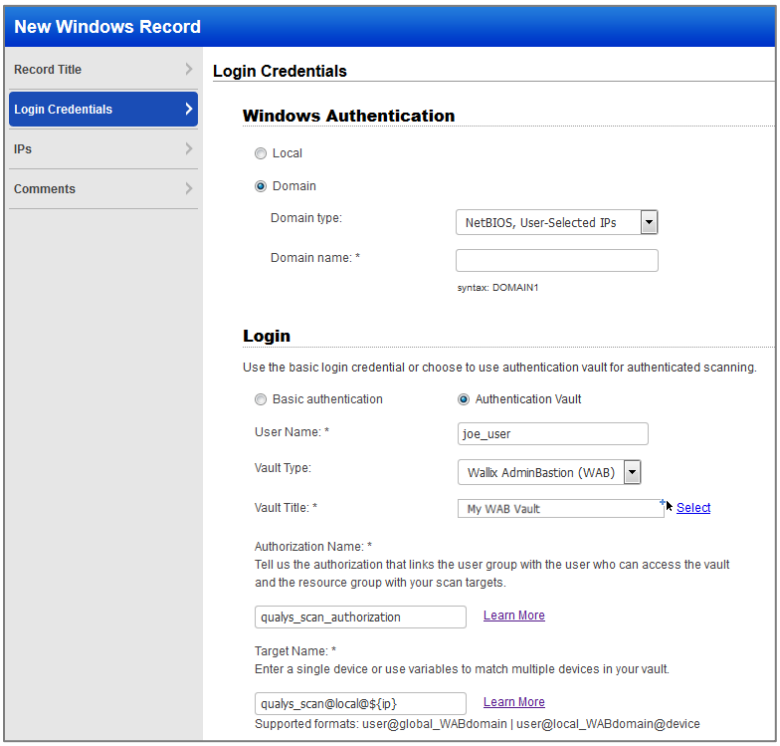
Password – The password for the user account.

Application Key – Your WAB REST API key.

Note that you cannot provide a password and a key in the same vault record.

Configure authentication records

The Wallix AdminBastion (WAB) vault is supported in Windows and Unix authentication records. Here's a sample Windows record with the vault selected.



Provide these settings:

Vault Type – Wallix AdminBastion (WAB)

Vault Title – Your vault record.

Authorization Name

Basically, you'll authorize the vault user to have access to the resource group in order to scan the targets in the group. Then you'll enter the authorization name in your record.

Target Name

You'll enter the target name using one of these formats.
user@global_WABdomain
user@local_WABdomain@device

where *user* is the user with access to the target, *global_WABdomain* is a domain name in a domain controller, *local_WABdomain* is a local domain, *device* is the device you want to scan

Using Variables in the Target Name

You can use one or more variables when defining the target name in order to match several targets that use the same naming convention.

${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, the target name user@local_WABdomain@${ip} will match these 3 devices: 10.50.60.70, 10.50.60.88 and 10.30.10.12. See the help for more examples.

Upgraded SimpleSAMLphp Library

We have now upgraded the SimpleSAMLphp library from version 1.10 to version 1.15.4 which fixes XML signature validation security issues.

Issues Addressed

- We fixed an issue where certain policies that were imported from the Policy Library failed to load in the Policy Editor when the policy included controls that were published and then unpublished.
- We have improved the performance when loading asset groups in the Policy Editor.
- We have now removed the restriction of 1000 exceptions in Policy Controls.
- We fixed an issue where Mandate Information and Mandate Reports included some controls (CIDs) that were not published.
- The Policy Report in PDF format now displays correct count and list of control statistics.
- For scheduled EC2 scans in the PC module we will only consider assets that have been activated for PC. Similarly, for scheduled EC2 scans in SCA we will only consider assets that have been activated for SCA.
- Fixed an issue on the Edit Asset Group page where scanner appliances selected for the asset group were not listed.
- The search by Asset Group option in Assets tab now displays correct output.
- We have updated the validations for adding DNS and NetBIOS in an Asset Group. The new validations require the user to enter DNS or NetBIOS names separated by a comma or newline character and not by spaces.
- You can now successfully create new asset groups using the “Add to new Asset Group” and “Add all to new Asset Group” menu option in Asset Search Report.
- You can now enter special characters in the Password/Confirm Password fields in the Palo Alto Networks Firewall authentication record.
- Fixed an issue where the “Auto Discover Instance” option in the Tomcat authentication record (Unix installation) was not being saved when checked.
- We fixed an issue where users were unable to view the login credential fields when they select the Authentication Vault option while creating a MySQL authentication record.
- We fixed an issue where users were unable to view the login credential fields when they select the Authentication Vault option while creating a Sybase authentication record.
- We fixed an issue where the Authentication tab in the Host Information window did not show IBM DB2 authentication scan details.
- The online format of Patch Report now correctly displays the consultant logo (for consultant subscriptions).
- We have fixed an issue where a wrong calculation in the non-running kernel count was displaying incorrect data for the non-running QIDs in the report.
- “Title” is being corrected to “VM Authentication Report” in XML format for authentication reports generated from the VM module.
- We fixed an issue with Remediation Reports in PDF format where we didn't show data in the Title column when the title spanned multiple lines. Now PDF reports will show all QID titles.
- We fixed an issue with Scorecard Reports in PDF format where we didn’t show data in columns when the data spanned multiple lines. Now PDF reports will show all data.

- We fixed an issue where Scan Report was displaying summary in the header of the report even if the Text Summary checkbox is not selected in the report template. Now the report summary is visible only if any one of the Text Summary checkboxes in the template is selected.
- Scan reports based on the Scan Report Template with Scan Based Findings selected will now correctly show or not show the account login ID based on the "Exclude account login ID" option in the template.
- PCI scan reports based on the PCI Scan Template with Scan Based Findings selected will now correctly show or not show the account login ID based on the "Exclude account login ID" option in the template.
- Map reports based on the Map Report Template will now correctly show or not show the account login ID based on the "Exclude account login ID" option in the template.
- Scan Results will always show the account login ID.
- Map Results will always show the account login ID.
- Payment Card Industry (PCI) Executive and Payment Card Industry (PCI) Technical reports will always show the full user name and account login ID.
- The Asset Data report when queried through API now shows correct data.
- We now display approximate time needed to process scan and report data.
- We now display correct count of Information Gathered vulnerabilities in Agent Scan.
- We fixed an issue where after using the "Purge old host data when OS is changed" feature, the OS_CPE value for the host was not getting updated for the respective hosts.
- When you schedule a scan by FQDNs, the scheduled scan list action now correctly displays FQDN in the target node of the response.
- The selection of State field in User Profile is now optional for a user.
- We have added new validations for answers to security questions. No two answers can be the same and the length of the answer is restricted between 6 to 64 characters only.
- We now display a confirmation message before you remove IPs from CertView using the Remove IPs option.
- Now we'll prevent users from editing scheduled CertView scans in accounts where the CertView module is expired.
- The filter for "CertView Hosts" is now displayed even if "IPv6" service is enabled.
- For users with IPv6 and Extend IPv6 Mappings enabled, we fixed an issue where the user is unable to save the Scan Report template that has IPv6 hosts.
- Improved the error message that appears when a user tries to save a duplicate authentication record by displaying the title of the existing authentication record.
- Improved the error message that appears when there's a validation failure while uploading SCAP content for a SCAP policy to include the error reported by the scapval tool. Also, you can now upload SCAP content and create a policy after removing the digital signature block from the content.
- Updated the online help for Docker authentication because we now support more OS platforms.
- Updated the online help to better explain what happens to scan results and user configurations when you delete a user.

- Updated the online help to clarify that PCI ASV scan results (external IPs with external scanners and PCI Option Profile) are saved for 2 years from the scan launch date even if the Auto Delete Stored Data option is enabled. PCI ASV scan results may be deleted when older than 2 years.