Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.15

August 23, 2018

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

Qualys Cloud Platform

JBoss Server Authentication Now Supported for VM, PC, and SCA
Managing IPs Across Applications
Scanner Appliance: IPv6 Support for VLANs and Static Routes
IBM DB2 11.x Support

Qualys Vulnerability Management (VM)

Oracle WebLogic Server Authentication Now Supported for VM
New EC2 Information in Scan Reports
Display Full List of Hosts Not Alive in Scan Results

Qualys Policy Compliance (PC/SCAP/SCA)

Policy Compliance Report Improvements
Support for MariaDB Authentication
New Technologies Supported for Unix UDCs

Qualys 8.15 brings you many more Improvements and updates! Learn more

Qualys Cloud Platform

JBoss Server Authentication Now Supported for VM, PC, and SCA

You can now run scans on your JBoss server running on Unix and Windows for vulnerability and compliance. You'll need to create a JBoss Server record for the host running the JBoss server in a standalone or Domain Controller operating modes.

How do I get started?

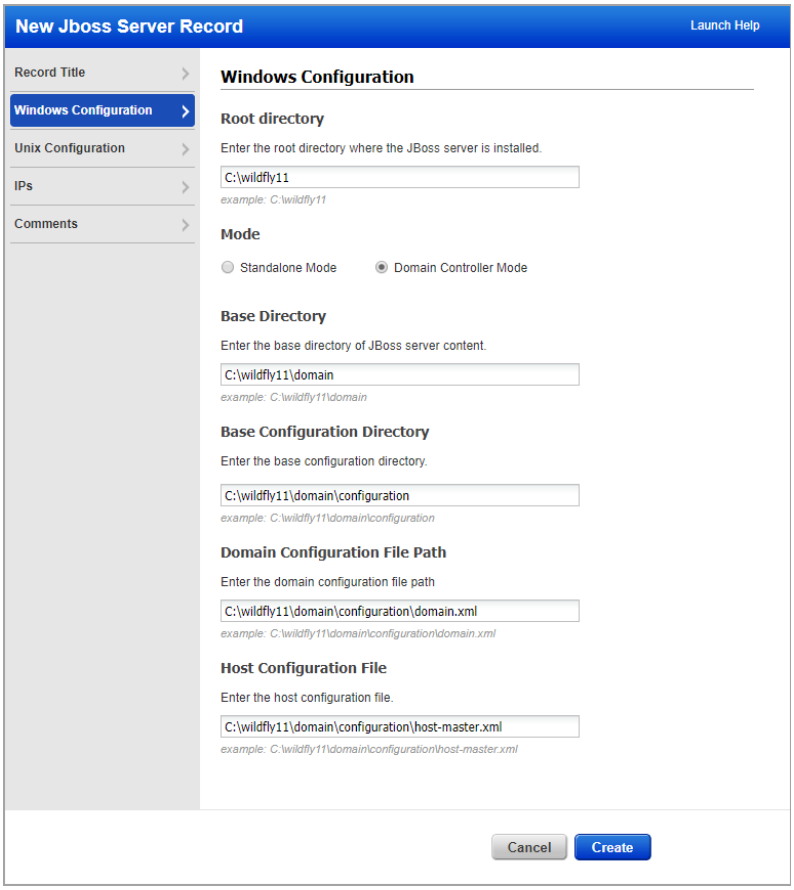
1) Go to Scans > Authentication.

2) Check that you already have a record defined for each host running a JBoss server.

3) Create a JBoss record for the same host. Go to New > Application Records > JBoss Server.

4) Provide the required root and configuration locations for the JBoss Server.

Here is an example for Windows Domain Controller mode record



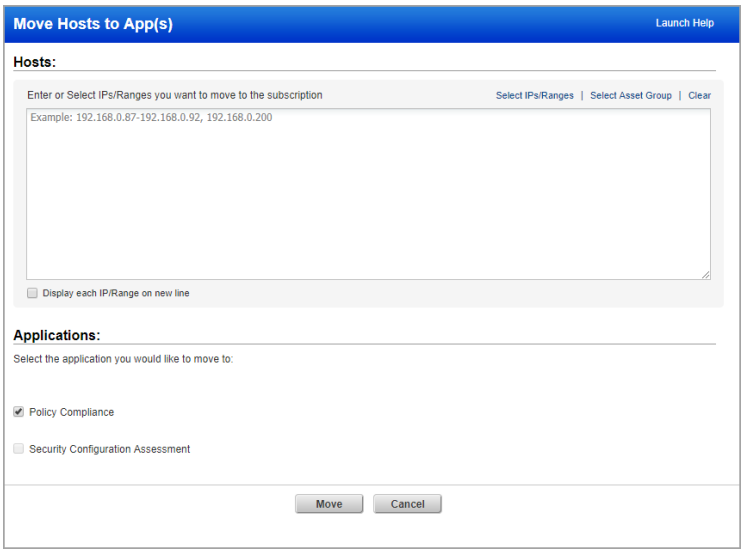
Managing IPs Across Applications

We have now enhanced our application to help you manage your hosts better.

Move Hosts

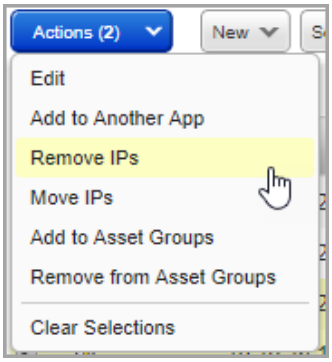
You can now move IPs from your PC module to SCA module and vice versa. This is applicable only in case you have both the PC and SCA modules enabled in your subscription.

Simply go to Assets > Host Assets > Actions and select Move IPs. Choose the IPs you want to move and the app you want to move it to and click Move.



Remove Hosts

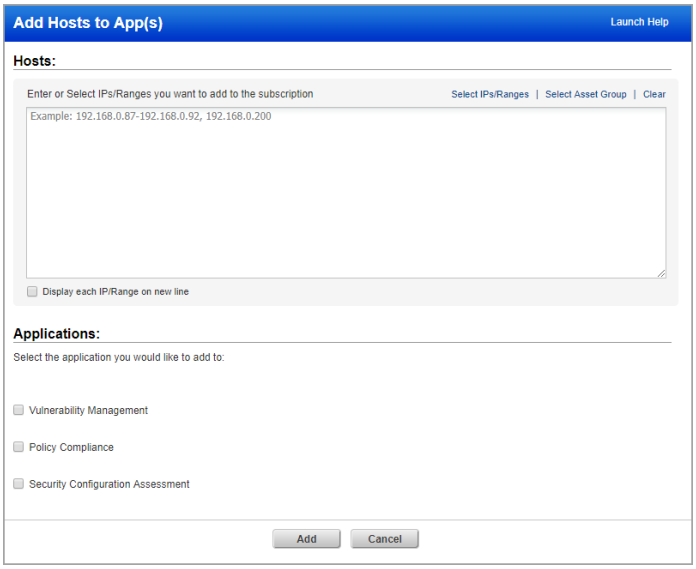
We have moved the Remove IPs option from the New menu to the Actions menu for better usability.



Add Hosts

We have also combined multiple add IPs option to a single option: Add to Another App.

Just go to Assets > Host Assets > Actions and select Add to Another App. Select IPs and choose which app you want to add them to.



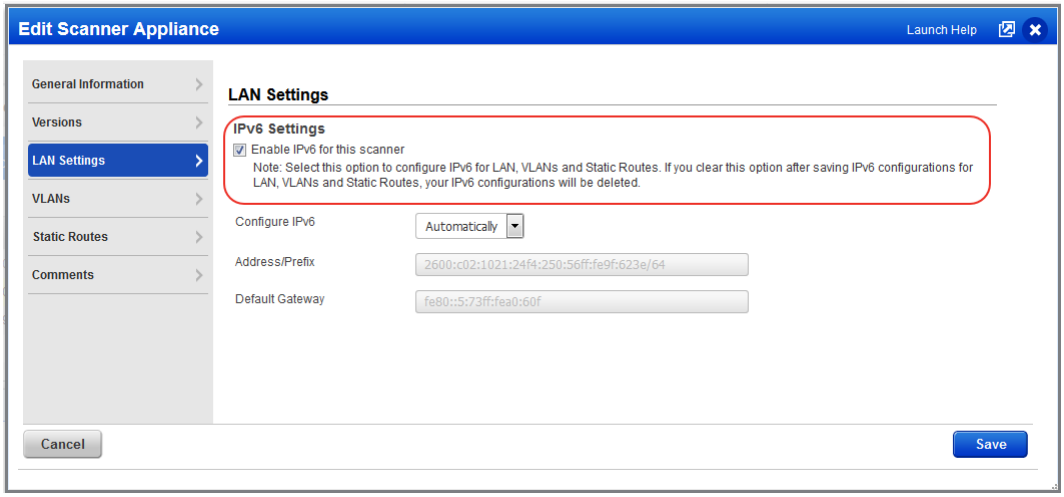
Scanner Appliance: IPv6 Support for VLANs and Static Routes

We now support IPv6 addresses when defining VLANs and static routes for virtual and physical scanner appliances. Appliances can have a mix of IPv4 configurations and IPv6 configurations.

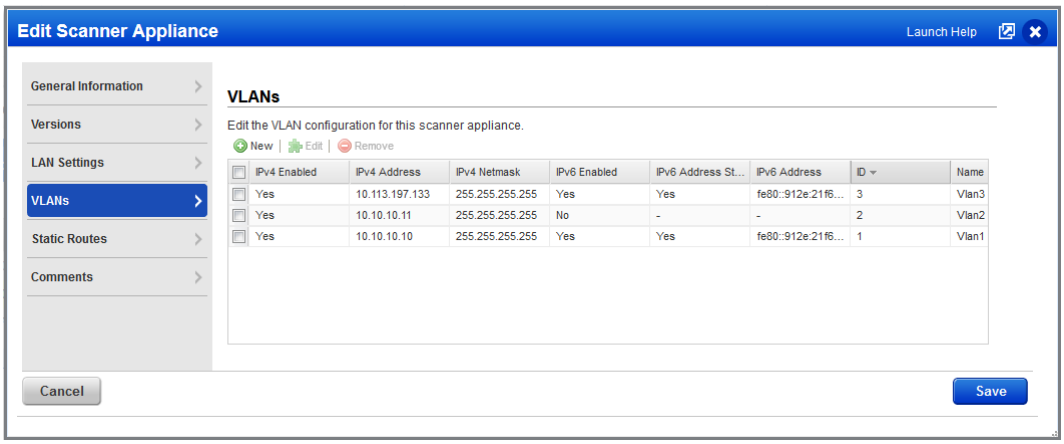
Note - The IPv6 Scanning feature must be enabled for your account. Please contact Support or your Technical Account Manager if you would like have this feature turned on.

Get Started

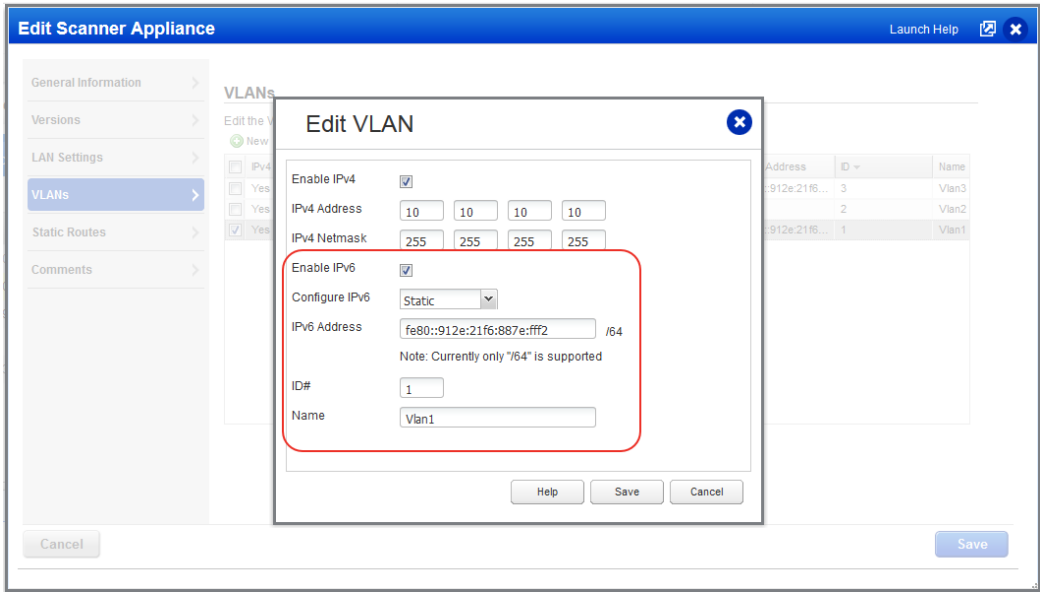
Go to Scans > Appliances and edit the appliance you're interested in. Select "Enable IPv6 for this scanner" on the LAN Settings tab. This allows you to configure IPv6 for LAN, VLANs and Static Routes. Note – If you clear this option after saving IPv6 configurations they will be deleted.



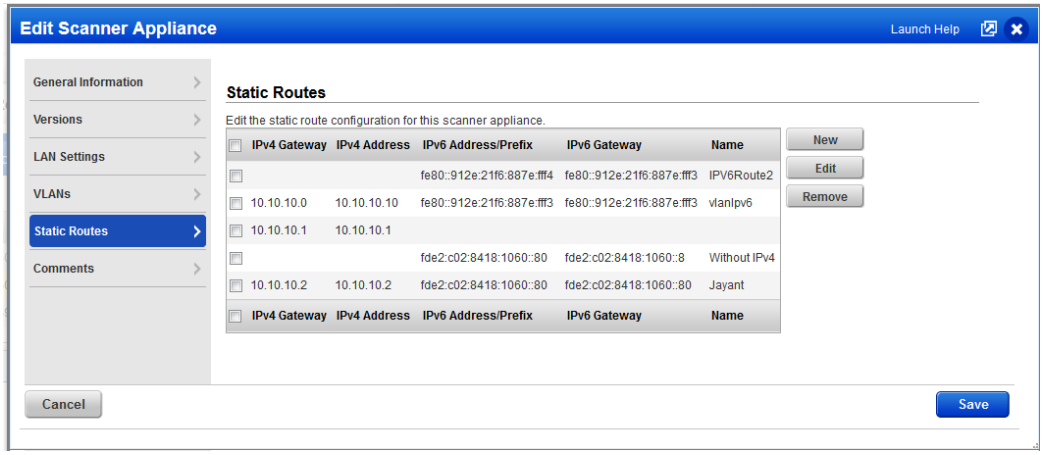
Go to the VLANs tab to view and configure VLANs for this appliance. You'll see IPv4 and IPv6 configurations for the appliance.



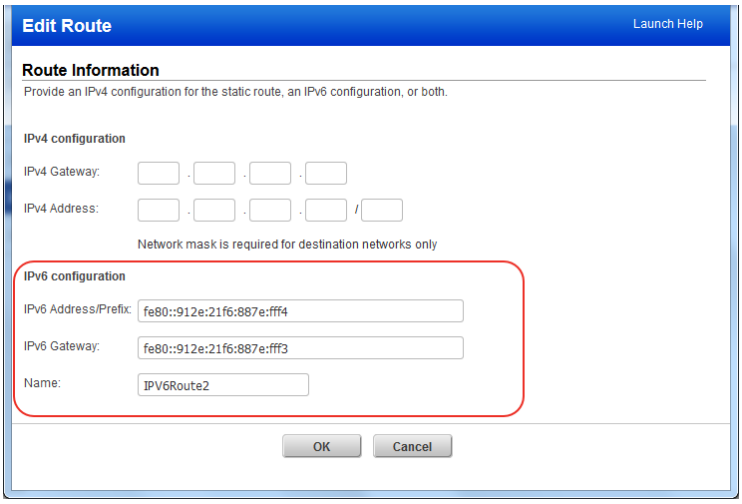
When you create or edit a VLAN, click the Enable IPv4 option to add IPv4 details and click the Enable IPv6 option to add IPv6 details. You can choose to enable IPv4 only, IPv6 only or both.



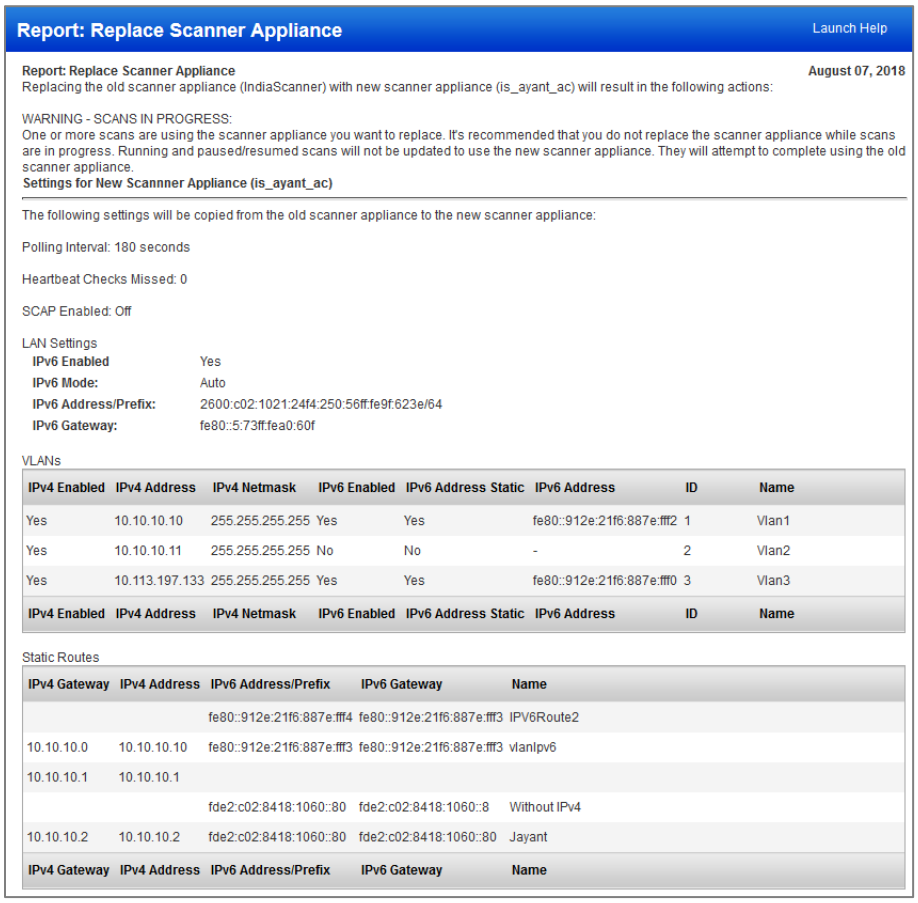
Go to the Static Routes tab to view and configure static routes for this appliance.



When you create or edit a static route, you can add IPv4 details, IPv6 details or both.



When you replace one scanner appliance with another we'll copy the IPv6 configurations (and other settings) from the old appliance to the new appliance. Click the View Report option to see the configurations that will be copied.



Report: Replace Scanner Appliance Launch Help

Report: Replace Scanner Appliance **August 07, 2018**

Replacing the old scanner appliance (IndiaScanner) with new scanner appliance (is_ayant_ac) will result in the following actions:

WARNING - SCANS IN PROGRESS:
One or more scans are using the scanner appliance you want to replace. It's recommended that you do not replace the scanner appliance while scans are in progress. Running and paused/resumed scans will not be updated to use the new scanner appliance. They will attempt to complete using the old scanner appliance.

Settings for New Scannner Appliance (is_ayant_ac)

The following settings will be copied from the old scanner appliance to the new scanner appliance:

Polling Interval: 180 seconds

Heartbeat Checks Missed: 0

SCAP Enabled: Off

LAN Settings

IPv6 Enabled	Yes
IPv6 Mode:	Auto
IPv6 Address/Prefix:	2600:c02:1021:24f4:250:56ff:fe9f:623e/64
IPv6 Gateway:	fe80::5:73ff:fea0:60f

VLANs

IPv4 Enabled	IPv4 Address	IPv4 Netmask	IPv6 Enabled	IPv6 Address Static	IPv6 Address	ID	Name
Yes	10.10.10.10	255.255.255.255	Yes	Yes	fe80::912e:21f6:887e:fff2	1	Vlan1
Yes	10.10.10.11	255.255.255.255	No	No	-	2	Vlan2
Yes	10.113.197.133	255.255.255.255	Yes	Yes	fe80::912e:21f6:887e:fff0	3	Vlan3
IPv4 Enabled	**IPv4 Address**	**IPv4 Netmask**	**IPv6 Enabled**	**IPv6 Address Static**	**IPv6 Address**	**ID**	**Name**

Static Routes

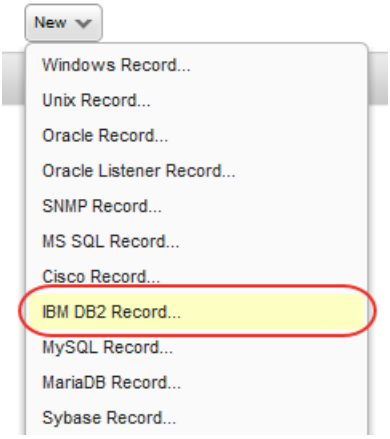
IPv4 Gateway	IPv4 Address	IPv6 Address/Prefix	IPv6 Gateway	Name
		fe80::912e:21f6:887e:fff4	fe80::912e:21f6:887e:fff3	IPV6Route2
10.10.10.0	10.10.10.10	fe80::912e:21f6:887e:fff3	fe80::912e:21f6:887e:fff3	vlanIpv6
10.10.10.1	10.10.10.1			
		fde2:c02:8418:1060::80	fde2:c02:8418:1060::8	Without IPv4
10.10.10.2	10.10.10.2	fde2:c02:8418:1060::80	fde2:c02:8418:1060::80	Jayant
IPv4 Gateway	**IPv4 Address**	**IPv6 Address/Prefix**	**IPv6 Gateway**	**Name**

IBM DB2 11.x Support

We've extended our support for IBM DB2 authentication to include DB2 11.x. You'll need an IBM DB2 record to authenticate to your DB2 11.x instance, and scan it.

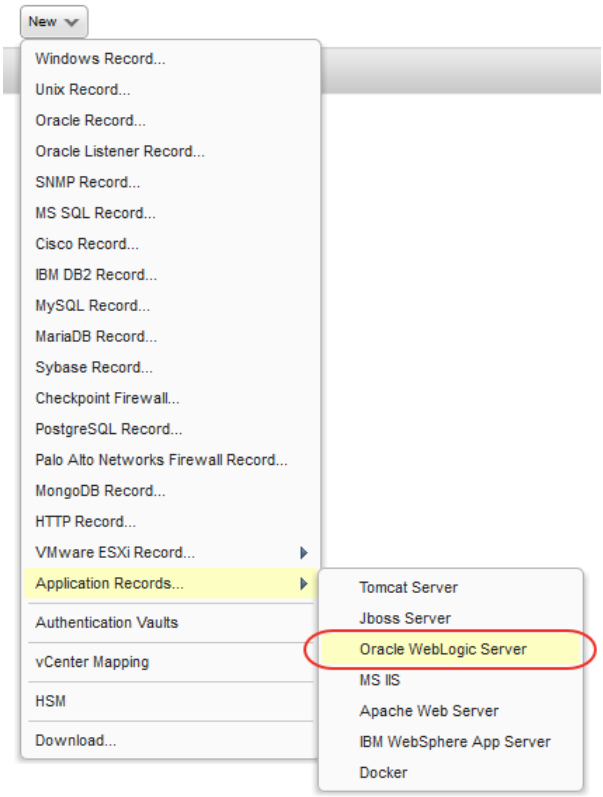
How do I get started?

Go to Scans > Authentication, and choose New > IBM DB2 Record. This authentication type is supported for vulnerability scans and compliance scans.



Qualys Vulnerability Management (VM)

Oracle WebLogic Server Authentication Now Supported for VM



You can now scan your Oracle WebLogic server running on a Unix host for vulnerabilities. You'll need an Oracle WebLogic Server record and a Unix record for the host running the web server. (Note that Oracle WebLogic Server authentication was already supported for compliance scans.)

How do I get started?

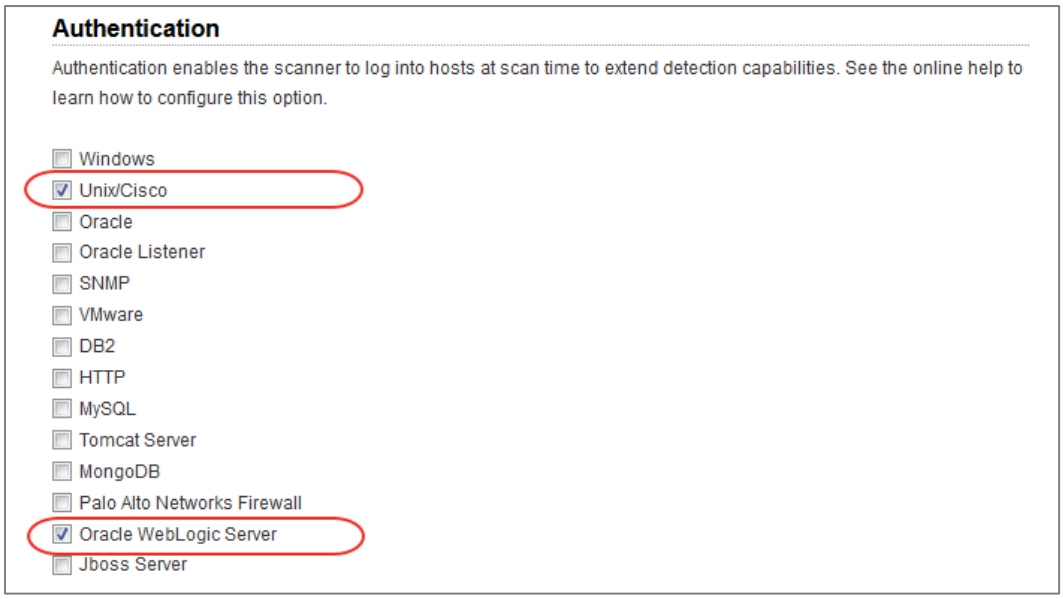
1) Go to Scans > Authentication.

2) Check that you have a Unix record already defined for the host running the web server.

3) Create an Oracle WebLogic Sever record for the same host. Go to New > Application Records > Oracle WebLogic Server.

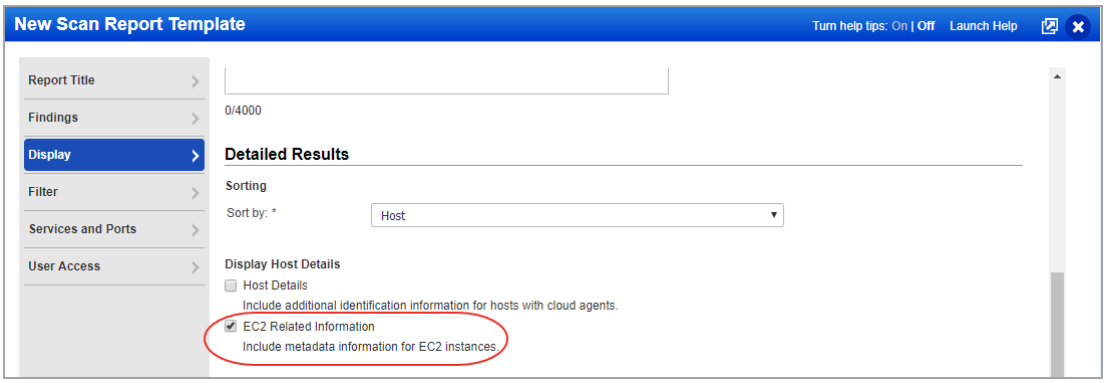
Enable authentication in your VM option profile

Before launching a vulnerability scan you'll need to enable authentication in your option profile. Create or edit an option profile and scroll down to the Authentication section on the Scans tab. Select the Unix/Cisco option and the Oracle WebLogic Server option.

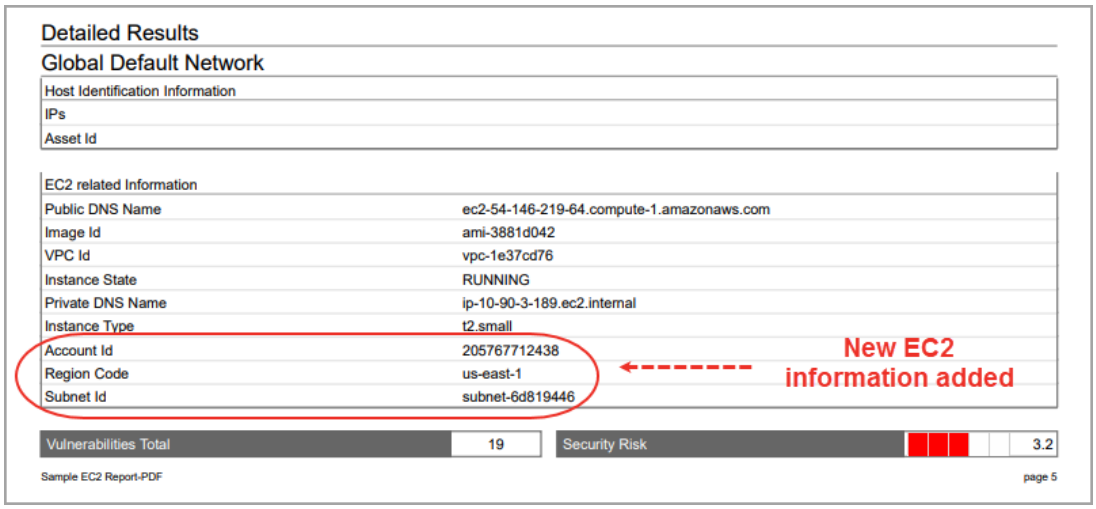


New EC2 Information in Scan Reports

We added more EC2 information to your reports. You'll now see Account ID, Region Code and Subnet ID when you pick the report template option “EC2 Related Information”. This option is available on the Display tab in Scan templates and PCI scan templates when Host Based Findings is also selected.

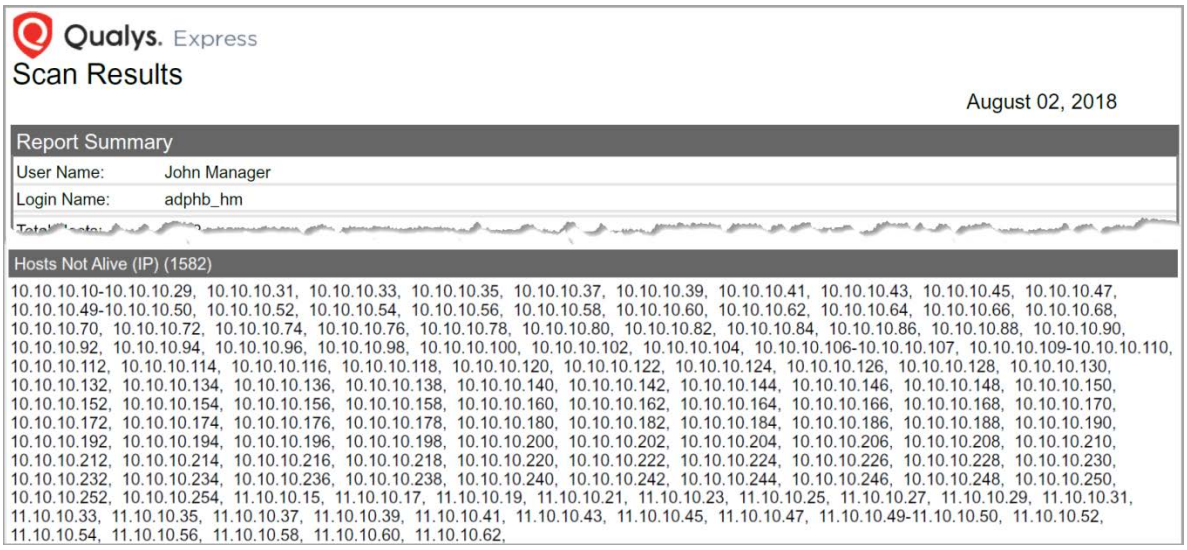


Check out this sample scan report with EC2 related information.



Display Full List of Hosts Not Alive in Scan Results

Scan reports now display all the host IPs that are not alive. Earlier, the display limit was 200.



Qualys. Express

Scan Results

August 02, 2018

Report Summary

User Name: John Manager

Login Name: adphb_hm

Hosts Not Alive (IP) (1582)

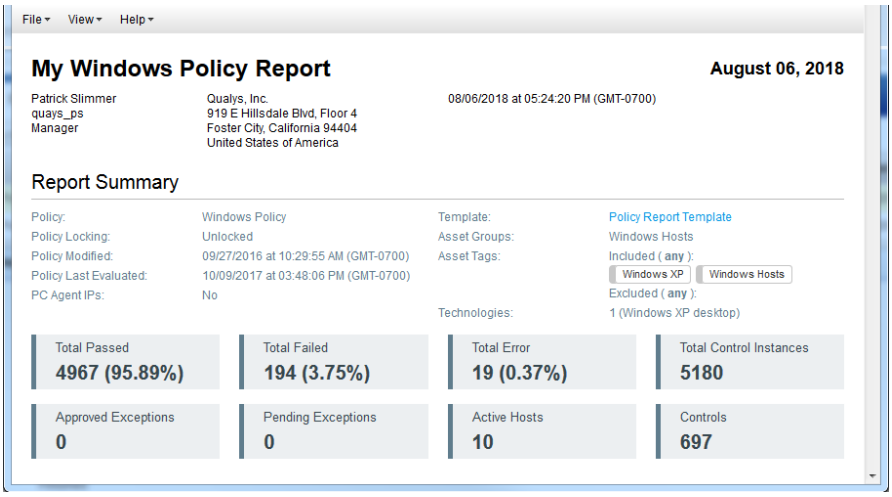
10.10.10.10-10.10.10.29, 10.10.10.31, 10.10.10.33, 10.10.10.35, 10.10.10.37, 10.10.10.39, 10.10.10.41, 10.10.10.43, 10.10.10.45, 10.10.10.47, 10.10.10.49-10.10.10.50, 10.10.10.52, 10.10.10.54, 10.10.10.56, 10.10.10.58, 10.10.10.60, 10.10.10.62, 10.10.10.64, 10.10.10.66, 10.10.10.68, 10.10.10.70, 10.10.10.72, 10.10.10.74, 10.10.10.76, 10.10.10.78, 10.10.10.80, 10.10.10.82, 10.10.10.84, 10.10.10.86, 10.10.10.88, 10.10.10.90, 10.10.10.92, 10.10.10.94, 10.10.10.96, 10.10.10.98, 10.10.10.100, 10.10.10.102, 10.10.10.104, 10.10.10.106-10.10.10.107, 10.10.10.109-10.10.10.110, 10.10.10.112, 10.10.10.114, 10.10.10.116, 10.10.10.118, 10.10.10.120, 10.10.10.122, 10.10.10.124, 10.10.10.126, 10.10.10.128, 10.10.10.130, 10.10.10.132, 10.10.10.134, 10.10.10.136, 10.10.10.138, 10.10.10.140, 10.10.10.142, 10.10.10.144, 10.10.10.146, 10.10.10.148, 10.10.10.150, 10.10.10.152, 10.10.10.154, 10.10.10.156, 10.10.10.158, 10.10.10.160, 10.10.10.162, 10.10.10.164, 10.10.10.166, 10.10.10.168, 10.10.10.170, 10.10.10.172, 10.10.10.174, 10.10.10.176, 10.10.10.178, 10.10.10.180, 10.10.10.182, 10.10.10.184, 10.10.10.186, 10.10.10.188, 10.10.10.190, 10.10.10.192, 10.10.10.194, 10.10.10.196, 10.10.10.198, 10.10.10.200, 10.10.10.202, 10.10.10.204, 10.10.10.206, 10.10.10.208, 10.10.10.210, 10.10.10.212, 10.10.10.214, 10.10.10.216, 10.10.10.218, 10.10.10.220, 10.10.10.222, 10.10.10.224, 10.10.10.226, 10.10.10.228, 10.10.10.230, 10.10.10.232, 10.10.10.234, 10.10.10.236, 10.10.10.238, 10.10.10.240, 10.10.10.242, 10.10.10.244, 10.10.10.246, 10.10.10.248, 10.10.10.250, 10.10.10.252, 10.10.10.254, 11.10.10.15, 11.10.10.17, 11.10.10.19, 11.10.10.21, 11.10.10.23, 11.10.10.25, 11.10.10.27, 11.10.10.29, 11.10.10.31, 11.10.10.33, 11.10.10.35, 11.10.10.37, 11.10.10.39, 11.10.10.41, 11.10.10.43, 11.10.10.45, 11.10.10.47, 11.10.10.49-11.10.10.50, 11.10.10.52, 11.10.10.54, 11.10.10.56, 11.10.10.58, 11.10.10.60, 11.10.10.62,

Qualys Policy Compliance (PC/SCAP/SCA)

Policy Compliance Report Improvements

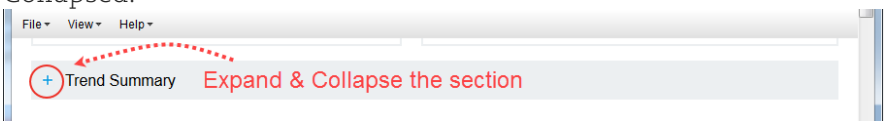
We made several improvements to Policy Compliance Reports.

The Report Summary and Trend Summary sections provide more info at-a-glance like counts for controls that passed, failed or had error, approved and pending exceptions and active hosts.

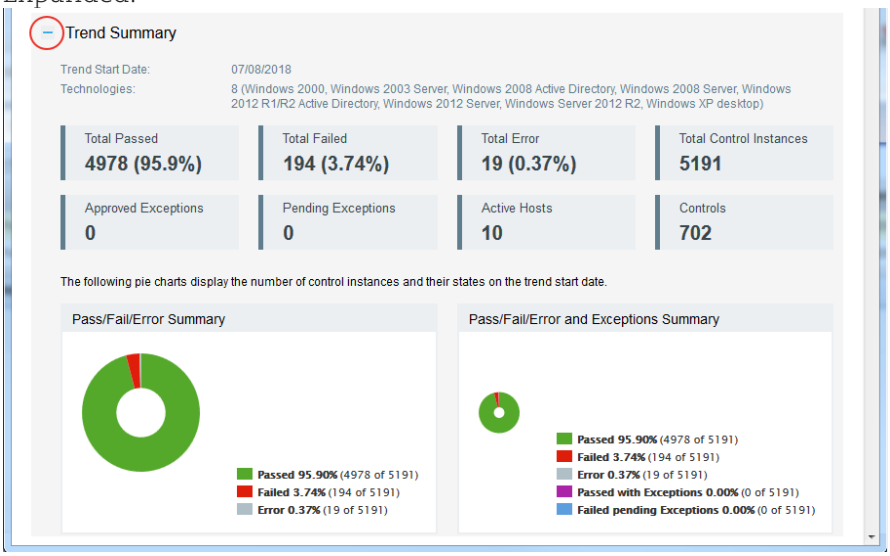


Several sections can be expanded and collapsed – just click + to expand a section and − to collapse a section. You'll see these options throughout the report like for Trend Summary, Control Statistics, Host Statistics, Control Glossary and Appendix.

Collapsed:



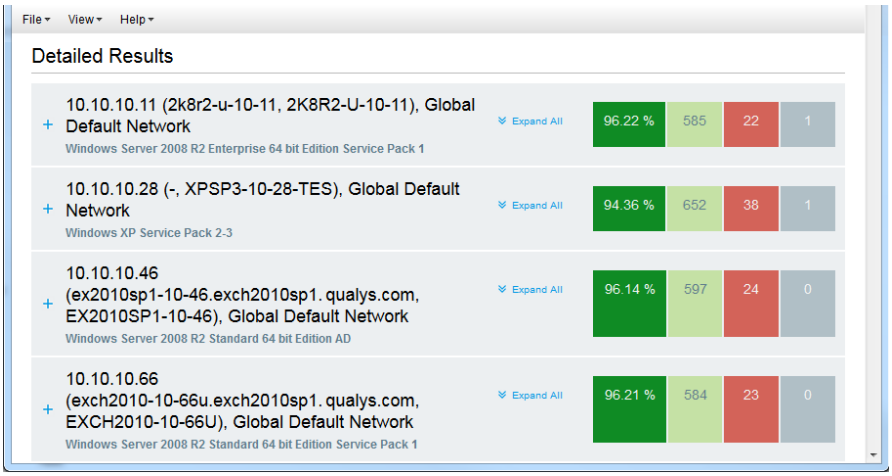
Expanded:



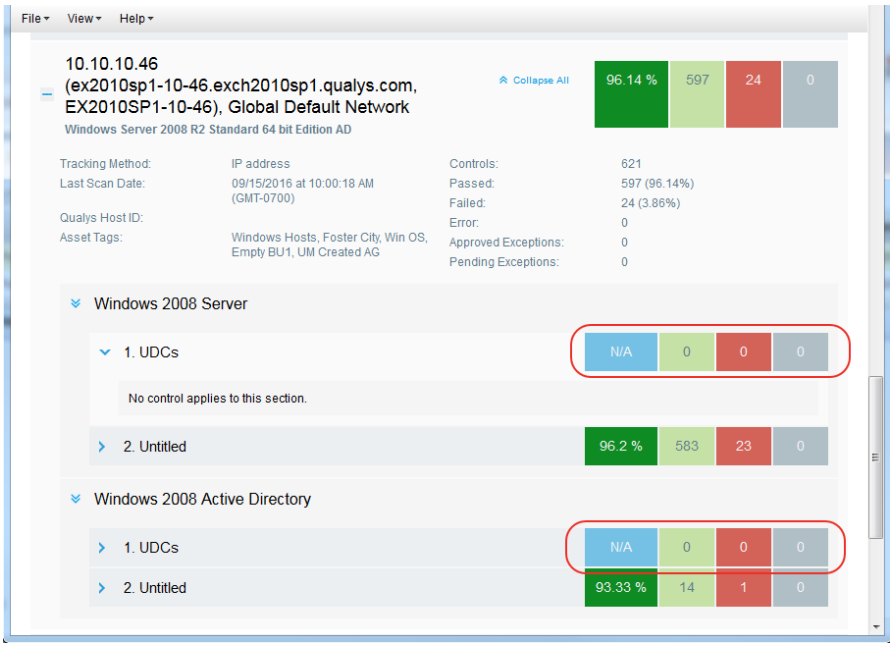
High-level Summary in Detailed Results

When you group by hosts you'll see a high-level summary for each host. Similarly, when you group by controls you'll see a high-level summary for each control.

Here's a sample report grouped by host. Host 10.10.10.11 is 96.22% compliant. This host has 585 controls that passed, 22 that failed, and 1 with error.



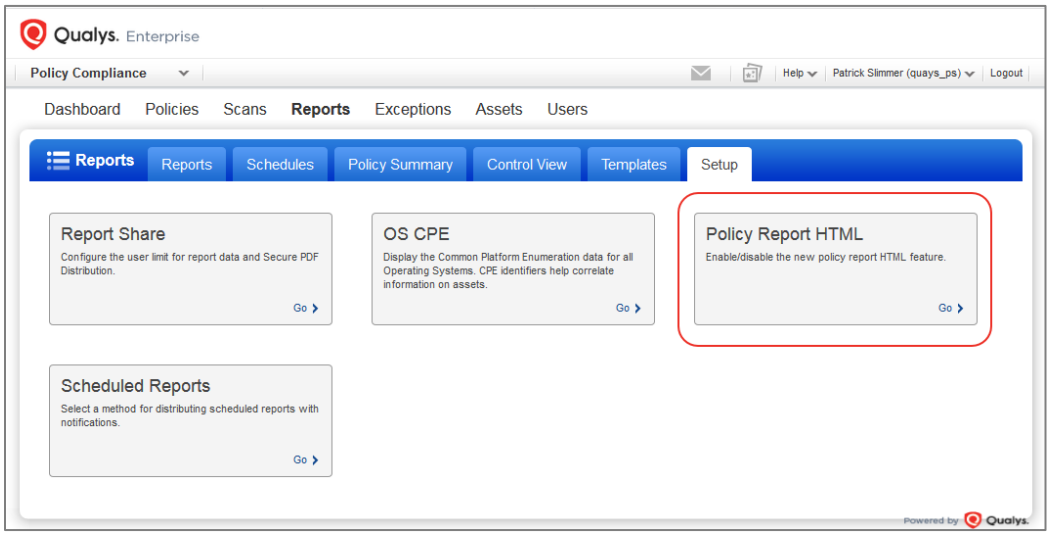
Expand any row to see complete details and a breakdown for each technology/section of the policy. When a section doesn't have any relevant controls for the technology you'll see N/A for the compliance percentage and 0 counts for passed, failed and error.



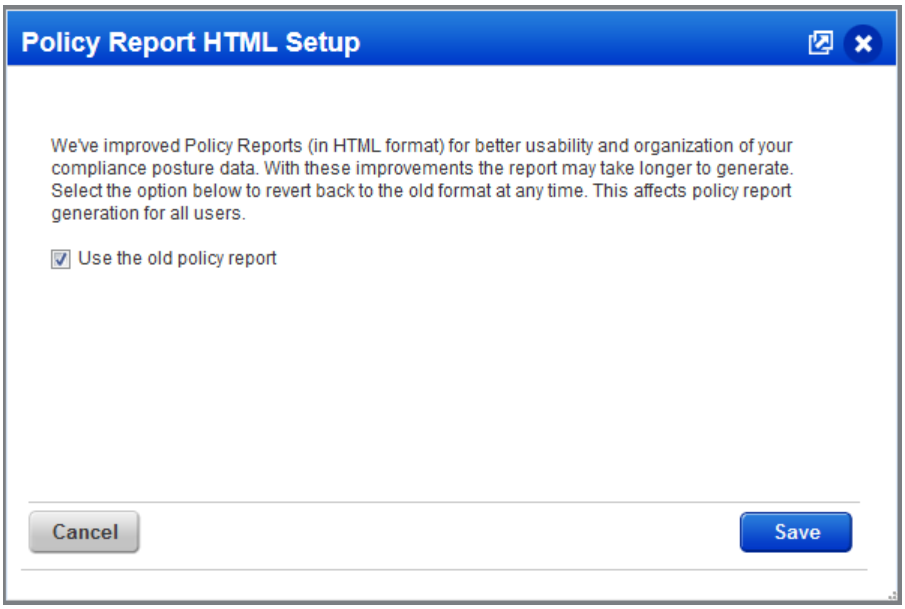
Run your own policy reports to see all the improvements!

Prefer the old policy report?

A Manager can enable/disable the new policy report HTML feature at any time. Just go to Reports > Setup > Policy Report HTML.

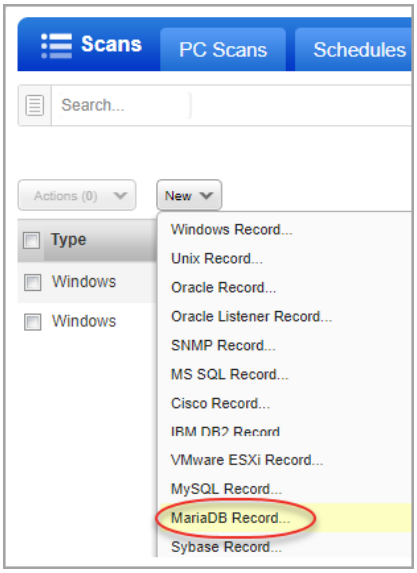


Select the option "Use the old policy report" and hit Save. Your changes will affect report generation for all users. Clear this option to use the new, improved policy report again.



Support for MariaDB Authentication

We now support MariaDB authentication for compliance scans using Qualys apps PC, SCA. Simply create a MariaDB authentication record with details about your credentials to authenticate to a MariaDB database instance running on a host, and scan it for compliance.

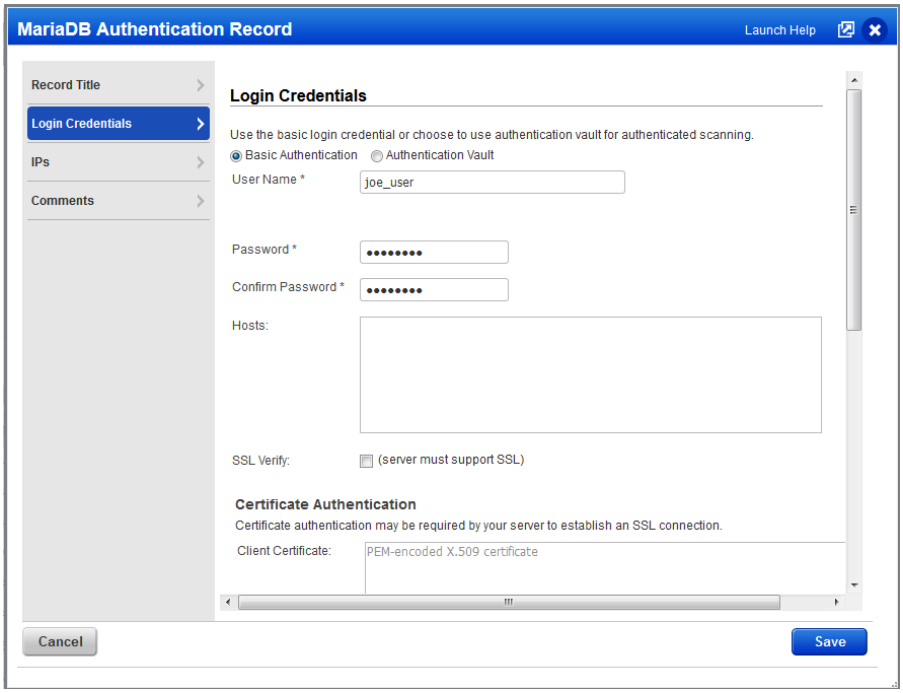


How do I get started?

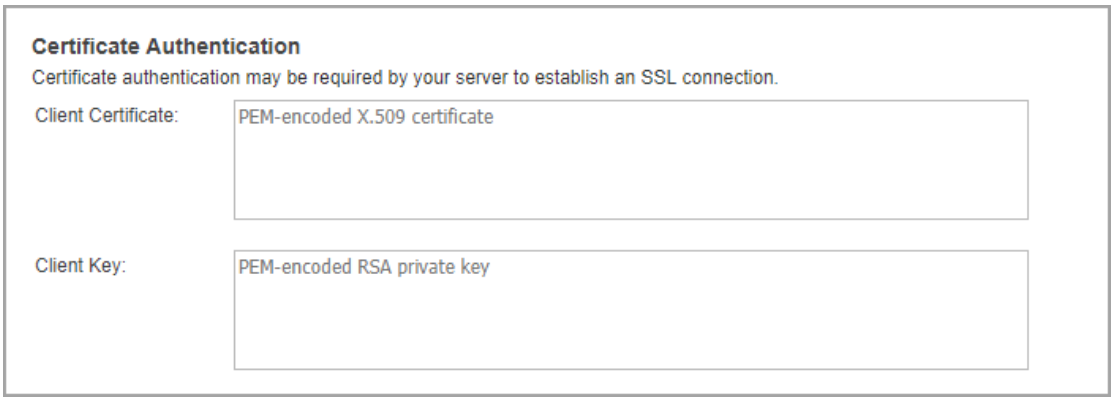
Go to Scans > Authentication, and choose New > MariaDB Record (as shown on the right).

Your MariaDB authentication record

Each MariaDB record identifies account login credentials, database information and target hosts (IPs). Provide basic login credentials (username and password) to be used for authentication or get the password from a supported password vault. Supported vaults are: BeyondTrust PBPS, CyberArk AIM, CyberArk PIM Suite, Quest Vault, Thycotic Secret Server.

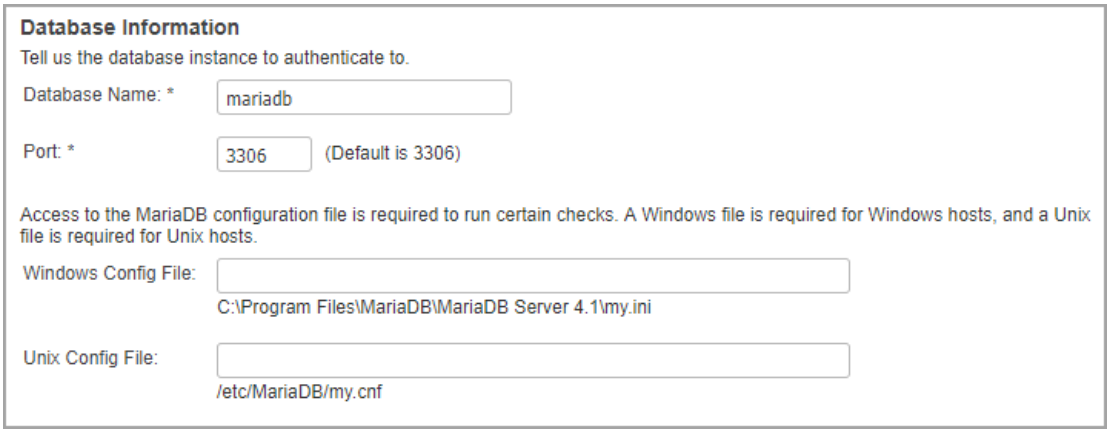


Your server may require certificate authentication in order to establish an SSL connection. In this case, enter the client certificate (PEM-encoded X.509 certificate) and client key (PEM-encoded X.509 RSA private key).



Tell us the database name to authenticate to and the port the database is running on. We provide default settings for both, but these may be customized.

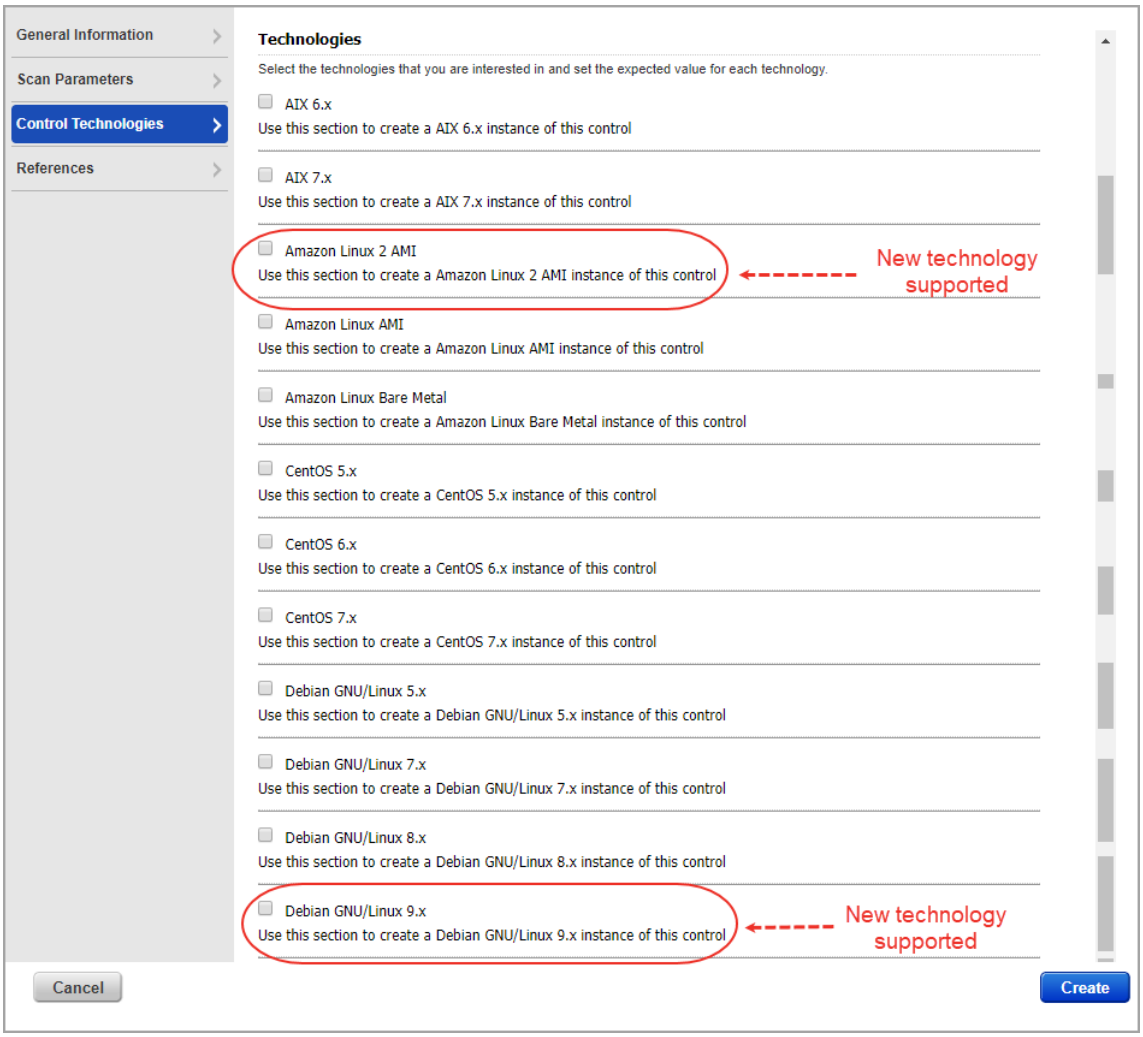
Access to the MariaDB configuration file is required to run certain checks. For authentication to Windows hosts, enter the Windows file and for Unix hosts, enter the Unix file. You may enter one or both.



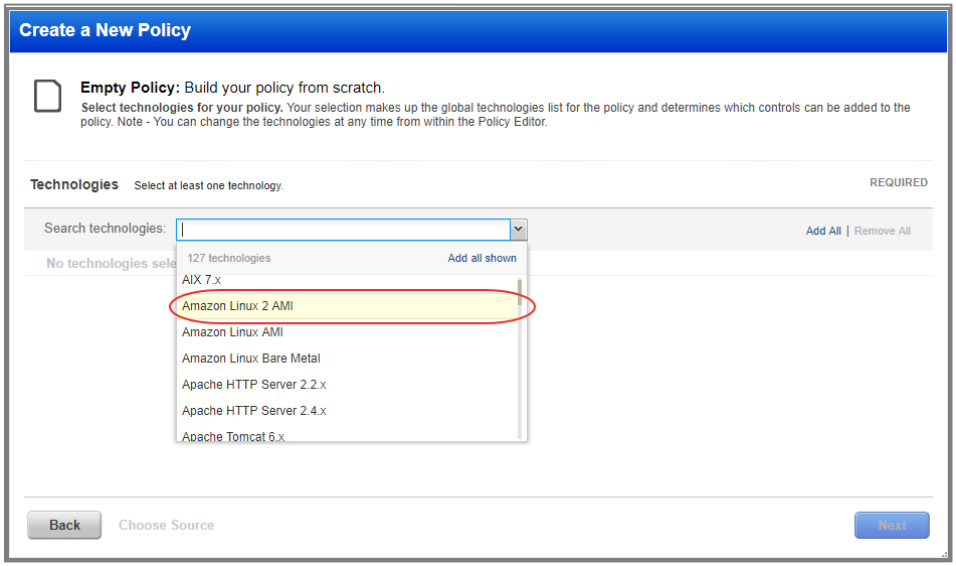
New Technologies Supported for Unix UDCs

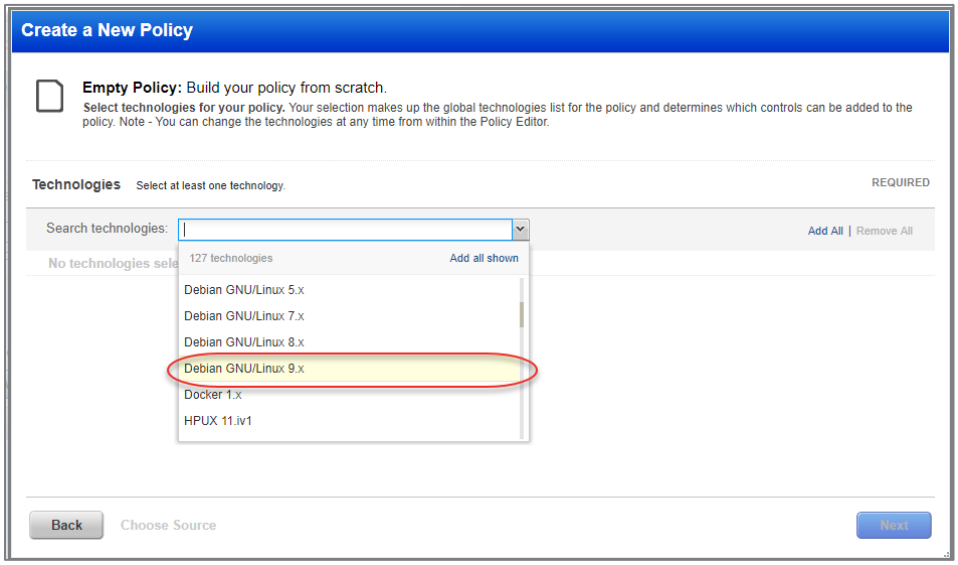
We added these two technologies: Debian GNU/Linux 9.x and Amazon Linux 2 AMI.

To create UDCs for these two new technologies, go to Policies > Controls > New > Control and select any of the Unix control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology you're interested in.



You'll also see the new technologies in the technologies list when creating a new policy.





Issues Addressed

- Now you can configure scanner appliance proxy server settings with the FQDN or IP address of the proxy server.
- We made improvements so that you can successfully add or remove scanner appliances to asset groups even if the asset group includes large number of DNS Assets.
- Fixed an issue where users were not able to create virtual scanners with certain names.
- Adhering to the IEEE new specifications, we now support alphanumeric values in Domain name for authentication records.
- DB2 Auth record password length limitation increased to 256 bytes.
- In authentication records, you can now save passwords with these characters: > < @
- Error message improvement for custom port validation in Unix authentication record.
- We fixed an issue when sorting the authentication record details list by Updated date.
- An error occurred if the user created an authentication report with custom ports selected and no custom ports were provided. Now proper validation message is displayed if the field is empty.
- The pgsql_unix_conf_path input parameter is no longer required when creating/updating PostgresSQL authentication records using the API.
- We're now showing valid API error messages when creating/updating authentication records with unsupported vaults.
- In the KnowledgeBase, only the QIDs related to Palo Alto Networks will show authentication as PANOS.
- Corrected the error the user received while downloading host assets in MHT or ZIP format from the Host Assets tab.
- The confirmation page that appears when you remove IPs from the subscription will now inform the user that IPs will also be removed from associated authentication records.
- We have now fixed a user facing error (multiple colons) in scan view summary section.
- We now display correct count of Information Gathered vulnerabilities in Agent Scan for combined manifest.
- We have fixed an issue where instead of updating the existing remediation ticket for a QID, the system was generating new tickets every time the specific QID was detected.
- We fixed a UI issue in the option profile where the Excluded QIDS checkbox was not working properly.
- Now we show the last fixed date for the vulnerability on the Host Information page.
- Fixed an issue where users were not able to save a custom list of QIDs for the Top 10 vulnerabilities widget on the VM dashboard.
- The patch report now correctly displays the target IP addresses in the report (all formats).
- When you create a report template, and if you select asset tag/IP address/range of IP addresses and Resolve DNS association of an asset group options, an appropriate error message is displayed indicating you need to choose asset group when you select Resolve DNS association of an asset group option.

- For customers with large number of IPv6 Mappings we made performance improvements that fixed an issue where the Scanners tab in the Scan Status window showed No Data Available.
- Made performance improvements to the Certificates list and download under VM > Assets.
- Made improvements to the Certificates page. You'll now see a note above the data list that explains the list only includes hosts with certificates, and hover text on graphs/charts now identifies the number of certificates and instances.
- Added Action logs for Clients creation and update.
- You can now activate or deactivate a policy irrespective of whether the policy is user-locked or locked at import (while importing library policy). You can activate or deactivate policy irrespective of locked state(Locked/Unlocked).
- Compliance reports in CSV format will not display inactive controls.
- Users will now be able to see the contents of the Results tab in the modal dialog used to display exception information.
- Fixed an issue with rendering controls including rational/statement with <IFRAME> html tag in the policy compliance report.
- We've added "Agent" and "All hosts" tracking method as options in Search window of Policy Editor.
- The Host List Detection API now returns error code 1905 with the invalid asset tag ID when searching assets by tag ID.
- Now when you filter the Host List Detection API by severity range we'll include Info Gathered QIDs in the results.
- In the subscription confirmation email, we now correctly display the Account manager name and email.
- City and State are no longer required inputs on the Terms & Conditions page for new accounts.
- Changed the title on the page that appears when enabling/disabling SAML SSO.
- We have now changed the time interval for the 'Your session is About to Expire' notification setting from 5-240 to 10-240 minutes.