



# Qualys Cloud Platform

## Release Notes

Versions 3.0, 10.0

March 31, 2020 (Updated April 8, 2020)

Here's what's new in Qualys Cloud Platform 3.0 and 10.0 releases!

[Introducing Qualys VMDR](#)

[VMDR Welcome Page](#)

[VMDR Prioritization Report](#)

[Asset Details – VMDR Prioritization Information](#)

[New Real-Time Threat Indicators](#)

[New VMDR Dashboard](#)

[New Vulnerabilities Option](#)

[New Prioritization Option](#)

[Launch/Schedule Vulnerability Scans on FQDNs](#)

[Merge Agent PC Data](#)

[VMDR Customers with SCA now have access to PC APIs](#)

[Pivotal Greenplum Authentication Support](#)

[Microsoft SharePoint Authentication Support](#)

[PostgreSQL Support for Windows](#)

[PostgreSQL 12.x Support for Unix](#)

[Microsoft SQL Server 2019 Support](#)

[Thycotic Secret Server vault supported in Cisco & Checkpoint Firewall](#)

[New option on the Help menu replaces Quick Start Guide](#)

[New Remote Security Hygiene Dashboard and Library Policies](#)

**Qualys Cloud Platform 3.0 and 10.0 releases bring you many more improvements and updates! [Learn more](#)**

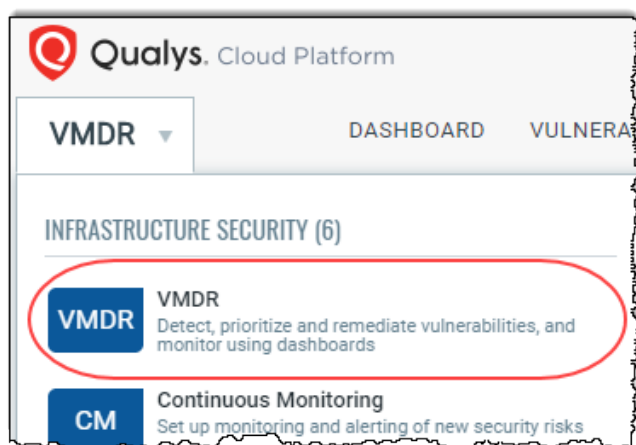
## Introducing Qualys VMDR

We have expanded our Vulnerability Management solution to establish the new game changing VMDR. Qualys VMDR is an all-in-one Vulnerability Management, Detection, and Response solution.

VMDR enables asset discovery, asset inventory, vulnerability management, threat prioritization and patch detection using one single app and an integrated workflow, to ensure comprehensive visibility and a remediation strategy that is prioritized based on context.

Once you are upgraded to VMDR, the Vulnerability Management module will be renamed to VMDR or VMDR experience depending on your subscription.

You will notice this change in the module picker for all the modules in your subscription.



If you are an existing VM customer then you are upgraded to VMDR experience by default and you can buy VMDR to get additional features.

With VMDR experience you get

- Asset inventory across environments like: Certificate, Cloud, Container, Mobile Devices
- Unlimited sensors to help you identify those assets: Virtual Passive Sensors, Cloud Agents, Mobile Agents, Container Sensors
- Search any asset in seconds using over 200+ searchable attributes
- Customizable dashboards and widgets with trending information

Once you upgrade to VMDR you'll also get

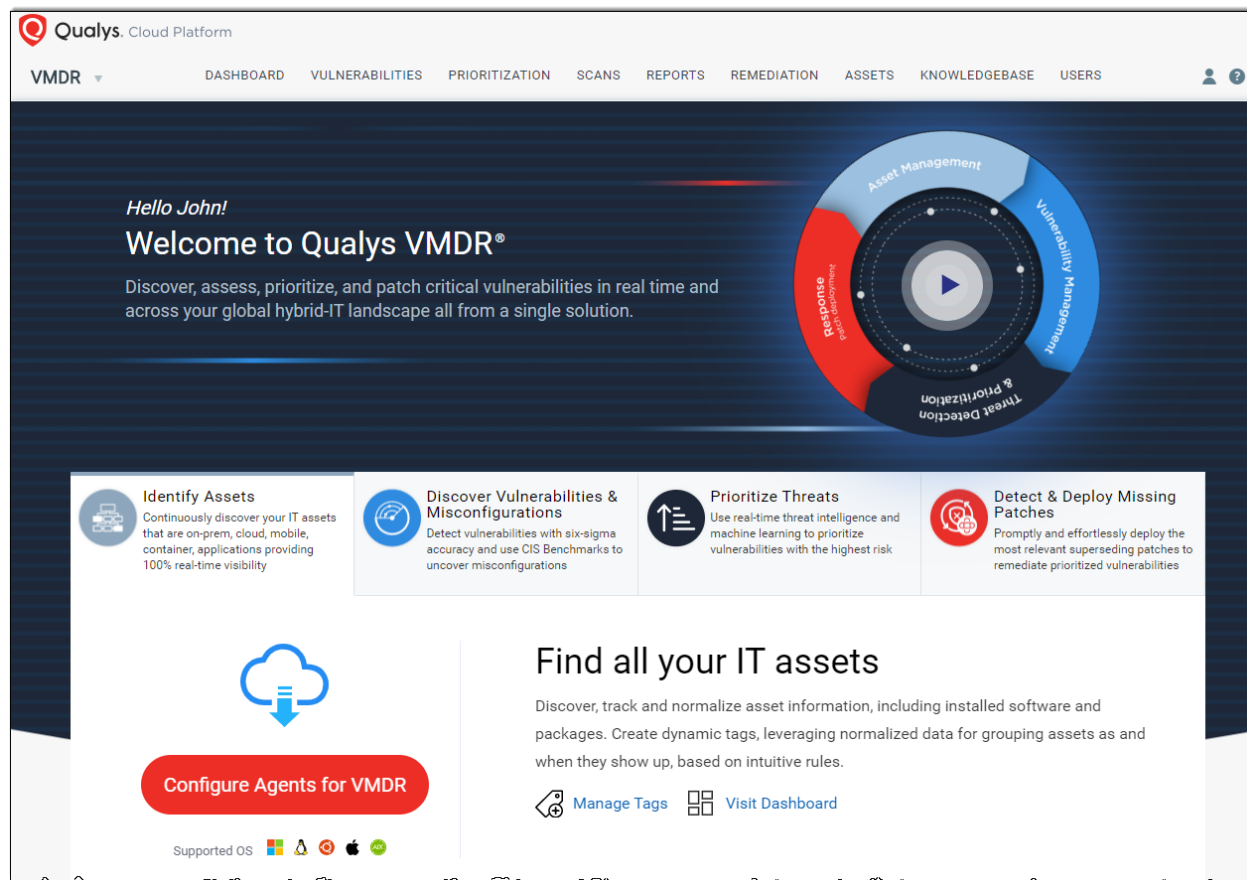
- Security Configuration Assessment to start configuration assessment and identify security misconfigurations on your assets based on CIS benchmarks
- Threat-based Prioritization based on continuously updated Real-time threat indicators
- Real-time alerting of critical vulnerabilities and changes to your external perimeter, etc.
- Detection of missing patches in context of the detected vulnerabilities
- Initiate deployment of missing patches from the Prioritization report directly

Note: Deployment of patches is available only for customers with the Patch Management add-on.

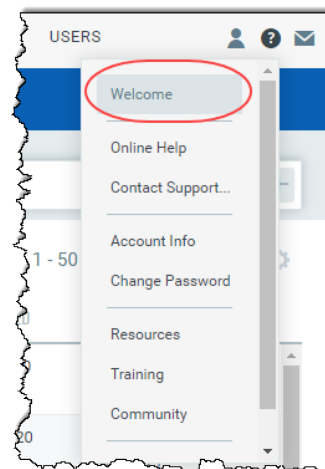
## VMDR Welcome Page

When your account is upgraded to VMDR, when you log in, you are shown the Welcome page which helps you can get started in a few quick steps.

This page gives you a quick overview of what you'll get with VMDR plus a high-level workflow of VMDR. We also give on screen guided assistance to help you get started.



To revisit this page anytime just navigate to the Welcome option in the Help menu.



## VMDR Prioritization Report

The VMDR Prioritization report allows you to automatically identify the vulnerabilities that pose risk to your organization by correlating vulnerability information with threat intelligence and asset context to zero in on only the highest risk vulnerabilities.

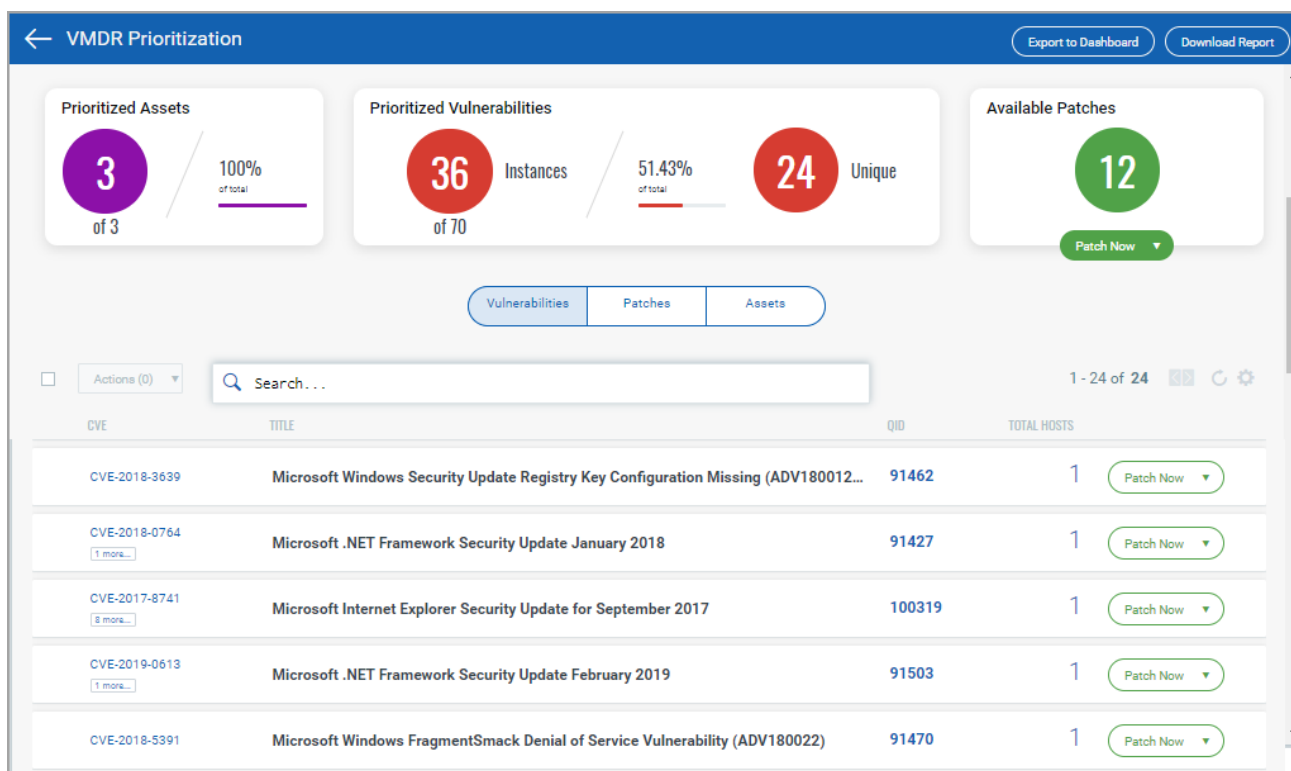
Indicators such as Exploit, Actively Attacked, and Wormable bubble up current vulnerabilities that pose risk while the “Predicted High Risk” indicator uses machine learning models to highlight vulnerabilities most likely to become material risks, providing multiple levels of prioritization.

### What does VMDR Prioritization Report do?

- Guides you to focus resources in the right area to first patch the highest risk vulnerabilities.
- Increases the security posture of your organization by identifying and remediating the vulnerabilities.
- Equips security analysts to pick and choose the relevant threat indicators.
- Helps you identify the specific patch needed to fix a particular vulnerability.
- Reduces remediation time by detecting the patch to be deployed from the same platform in an integrated workflow, at the click of a button. (if Patch Management app is enabled in your subscription).

### Sample VMDR Prioritization Report

Using real-time threat intelligence, we detect and prioritize for you which vulnerabilities to remediate first. The report also indicates the most critical threats and prioritizes patching. Refer to the online help for more information.



The report contains of two sections: Summary and Details.

The summary section of the VMDR Prioritization Report displays the findings: Prioritized Assets, Prioritized Vulnerabilities, and Available Patches.

The details section includes detailed information about prioritized vulnerabilities, patches and prioritized assets. Use the tabs to toggle between the three views. The Vulnerabilities and Assets tabs offer search capabilities using limited tokens.

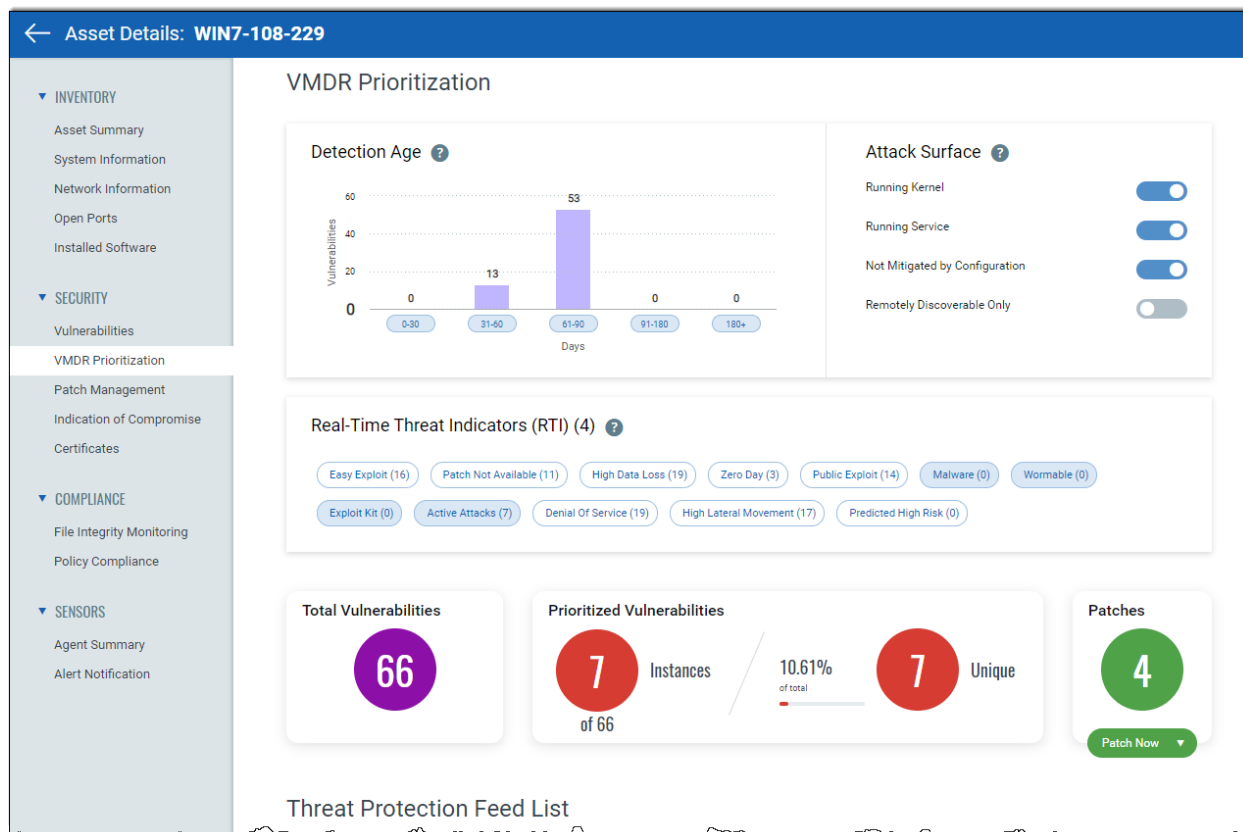
Once you generate the report, proceed with patching the vulnerabilities, export the report in the form of a widget to your dashboard or download the report in CSV format.

## Asset Details – VMDR Prioritization Information

You can now view prioritization information for individual assets in the VMDR Prioritization tab.

Simply navigate to VMDR > Vulnerabilities and choose Asset option. Then select an asset and from the Quick Action menu choose View Asset Details. You can also initiate patching the vulnerabilities for this asset using the Patch Now option.

Note: The Patch Now button is enabled only when Qualys can automatically patch the vulnerability and the Patch Management app is enabled in your subscription.



## New Real-Time Threat Indicators

We have added two new Real-Time Threat Indicators with this release:

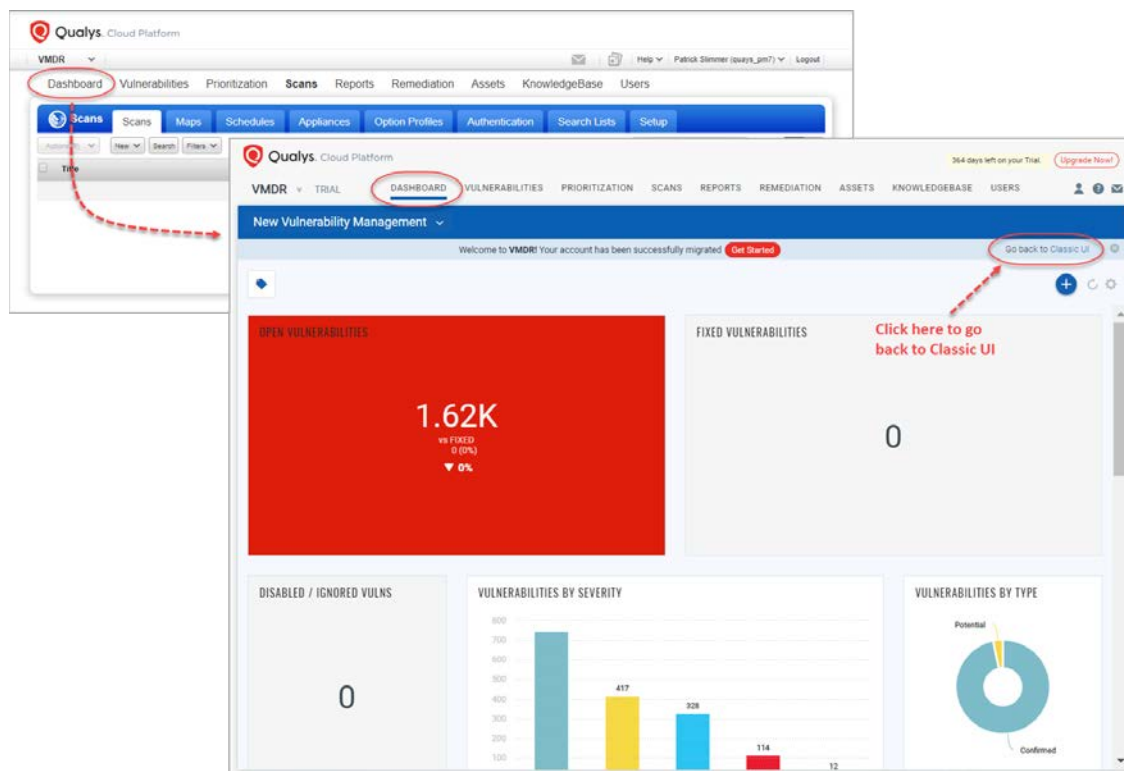
**Wormable** - Wormable has been associated with this vulnerability. The vulnerability can be used in “worms” - malware that spreads itself without user interaction.

**Predicted High Risk** - Predicted High Risk has been associated with this vulnerability. Qualys Machine Learning Model predicted this vulnerability as a High Risk based on various data sources including NVD, Social network, Dark web, Security Blogs, Code repository, Exploits etc.

## New VMDR Dashboard

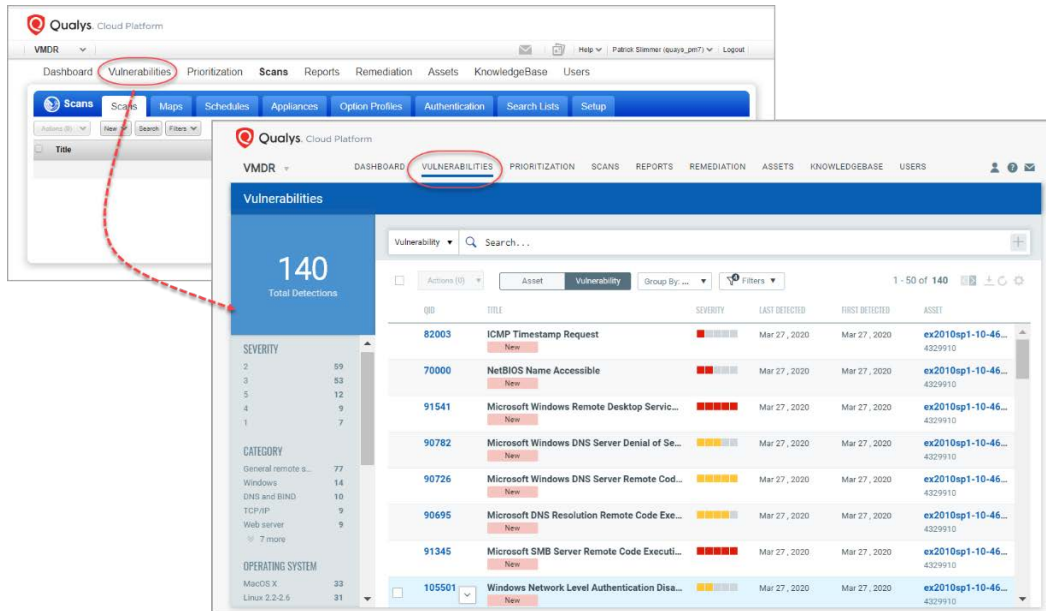
When your account is upgraded to VMDR, click the Dashboard option on the top menu and you'll get the new VMDR Dashboard. This replaces the Classic UI Dashboard in VM.

Want to go back to the Classic UI? No problem. Simply click the “Go back to Classic UI” link and you'll get your old dashboard back. This option is only available for accounts that were upgraded from VM to VMDR (not new accounts).



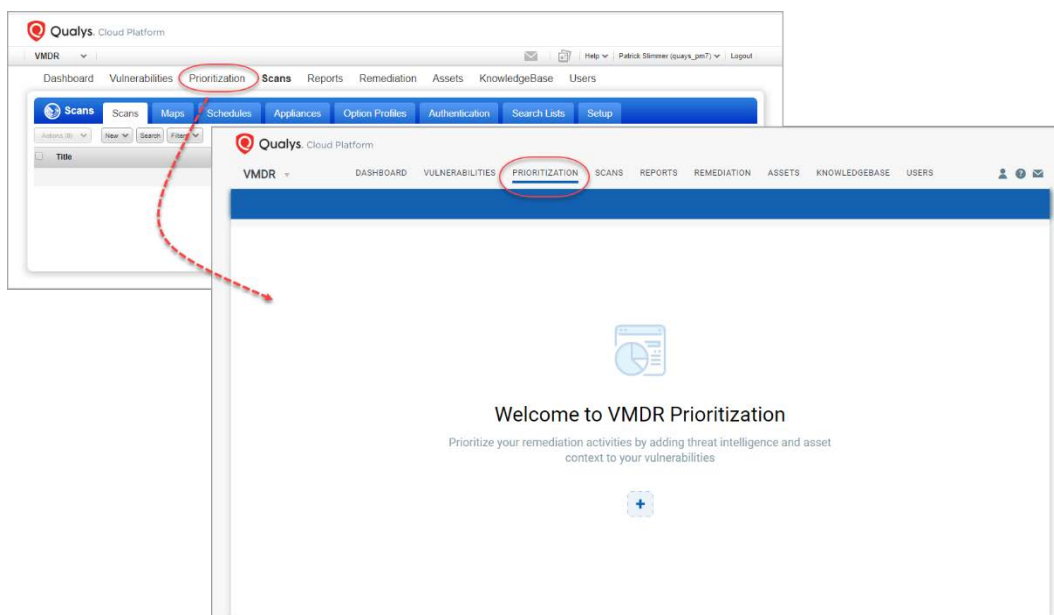
## New Vulnerabilities Option

When your account is upgraded to VMDR you'll see a new Vulnerabilities option on the top menu (after Dashboard). Choose this option and you'll get the Vulnerabilities list in VMDR where you can search vulnerabilities by vulnerability and by asset. (This option will not appear in accounts that have not yet been upgraded.)



## New Prioritization Option

When your account is upgraded to VMDR you'll see a new Prioritization option on the top menu (before Scans). Choose this option and you'll get the new VMDR Prioritization workflow where you can prioritize your remediation efforts. (This option will not appear in accounts with VMDR experience or accounts that have not yet been upgraded.)

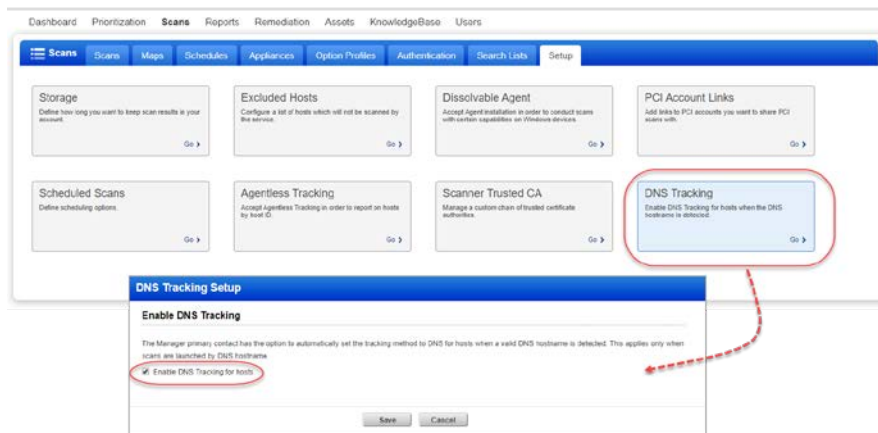


## Launch/Schedule Vulnerability Scans on FQDNs

With this release you can launch and schedule vulnerability scans on Fully Qualified Domain Names (FQDNs). When defining the scan target you'll enter FQDNs in the new FQDN input field.

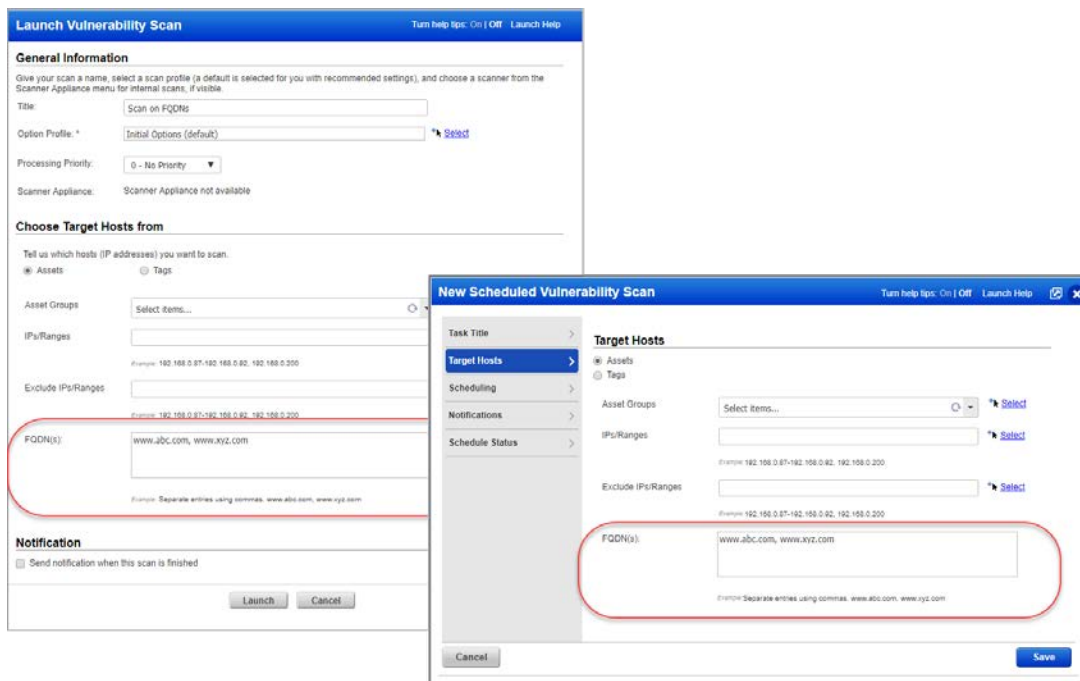
### DNS Tracking must be enabled

A Manager user can enable this feature by going to Scans > Setup > DNS Tracking and checking the "Enable DNS Tracking for hosts" option.



### Enter the FQDNs you want to scan

When launching and scheduling scans enter one or more FQDNs when defining the target hosts, as shown below. FQDNs can be entered in combination with asset groups and IPs/ranges but not with asset tags. The scanned FQDN must resolve to an IP address in your VM account to successfully scan it and view the results. Not seeing the FQDN option? Make sure DNS Tracking is enabled as stated above.





## Merge Agent PC Data

Host results from scans and agents are displayed separately in reports and asset views by default. You can choose to merge host results to get unified views of your assets by taking these steps: 1) Run scans using Agentless Tracking and 2) Enable the Merge Agent Data feature.

For PC, prior to this release, there was an additional step required by Support to configure a customer's account to allow the merging of PC data. This step is no longer required. Now you can set everything up without this additional configuration by Support.

For customers with the PC agent addon, you'll see the following change when you use this feature: Previously, your VM data from scans and agents was reported on the same asset, which is agent tracked. Your PC data from scans and agents was previously reported on separate assets. Now your PC data will be merged on the same asset, which is agent tracked.

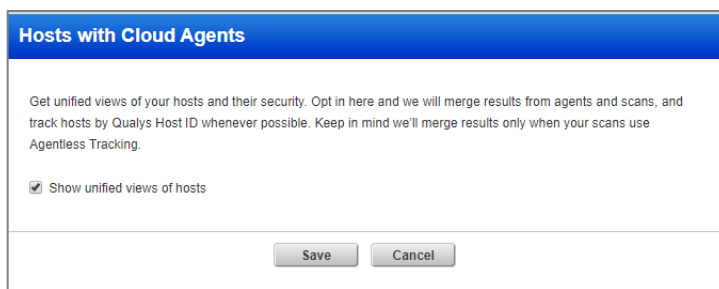
### How it works

An asset UUID is assigned to each host by the first service to reach the host - a scan with Agentless Tracking or a Cloud Agent installation. The second service discovers the asset UUID and stores data by this UUID. The combined data will appear in asset views and reports.

### Enable the Merge Agent Data feature

Host data from agents is tracked by asset UUID. Once the Merge Agent Data feature is enabled, we'll merge the host data from scans and agents.

Any Manager can go to Users > Setup > Cloud Agent Setup and select "Show unified views of hosts".

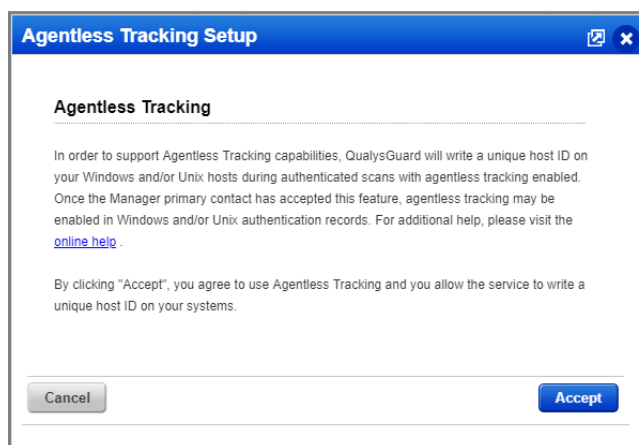


### Run scans using Agentless Tracking

1) Accept Agentless Tracking. Only the Manager primary contact for the subscription can take this step. Go to Scans > Setup > Agentless Tracking and click the Accept button.

2) Edit Authentication Records. Agentless Tracking must be enabled in the Windows and/or Unix authentication records for the hosts you want to track by host ID. Select the option "Enable agentless tracking" in your records (under Login Credentials).

3) Start a scan on the hosts you want to track by host ID. Authentication is enabled automatically for compliance scans. For vulnerability scans, you must select an option profile with Windows and/or Unix authentication enabled.



## VMDR Customers with SCA now have access to PC APIs

When upgraded to VMDR, customers with Security Configuration Assessment (SCA) can run Policy Compliance (PC) APIs even if they don't also have the PC app. This is true as long as the subscription has VMDR, SCA and the API add-on. Also, the user making the API call must have API access. (This feature is not available in accounts with VMDR experience and not available in accounts that haven't been upgraded.)

### PC APIs are available in these scenarios:

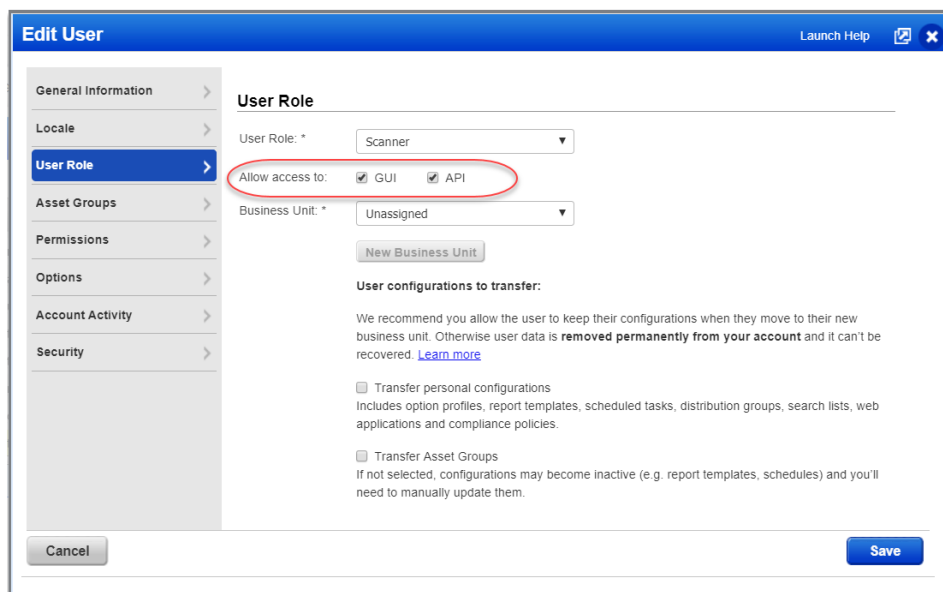
- You have PC and the API add-on.
- You have PC, SCA and the API add-on.
- You have VMDR, SCA and API add-on.

[Click here for the Qualys API \(VM/PC\) User Guide](#)

Note that the Exception API is only available in PC subscriptions and will not be available to SCA customers.

### How to grant API access to a user

The user running the API must be granted API access. Log in to your SCA subscription and go to the Users list. Edit the user's account and choose "Allow access to: API" on the User Role tab.



**Edit User** Launch Help

**General Information**

**Locale**

**User Role**

**Asset Groups**

**Permissions**

**Options**

**Account Activity**

**Security**

**User Role**

User Role: \* Scanner

Allow access to: ☒ GUI ☒ API

Business Unit: \* Unassigned

[New Business Unit](#)

**User configurations to transfer:**

We recommend you allow the user to keep their configurations when they move to their new business unit. Otherwise user data is **removed permanently from your account** and it can't be recovered. [Learn more](#)

☐ Transfer personal configurations  
Includes option profiles, report templates, scheduled tasks, distribution groups, search lists, web applications and compliance policies.

☐ Transfer Asset Groups  
If not selected, configurations may become inactive (e.g. report templates, schedules) and you'll need to manually update them.

[Cancel](#) [Save](#)

## Pivotal Greenplum Authentication Support

We now support Pivotal Greenplum authentication for compliance scans on Unix hosts. Authentication is supported for Greenplum versions 5.x and 6.x.

You'll need a Pivotal Greenplum authentication record to authenticate to a Pivotal Greenplum database instance running on a Unix host, and scan it for compliance.

### How do I get started?

Go to Scans > Authentication, then New > Pivotal Greenplum Record.

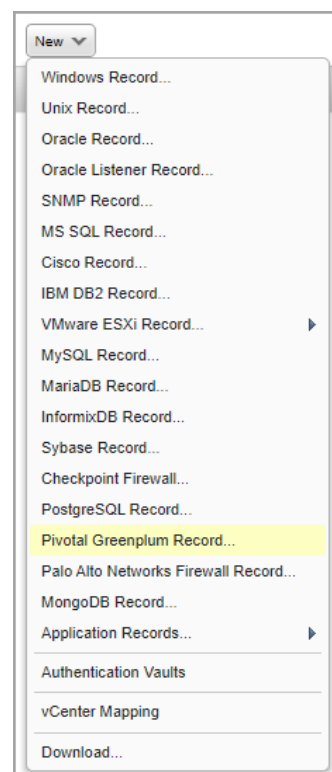
### Pivotal Greenplum Record

In the record, you'll need to tell us the user account to be used for authentication, the database instance to authenticate to, and the port where the database is installed.

The type of authentication method you use depends on your server settings and how you've configured client authentication.

You can use:

- a password (enter it on the Login Credentials tab or get it from a password vault),
- a client certificate (enter it on the Private Key / Certificate tab),
- a password AND client certificate (enter values on both tabs).



New Pivotal Greenplum Record

Launch Help

Record Title >

Login Credentials >

Private Key / Certificate >

Unix >

IPs >

Comments >

**Authentication**

Tell us the user account to use for authentication, the database instance you want to authenticate to, and the port where the database is installed.

Username:

qualys\_scan

Database Name:

my-greenplum-db

Port:

5432

(Default is 5432)

Provide a list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. This is required if you choose SSL Verify.

Hosts:

host.domain, host.domain,...

SSL verification is skipped by default. Select this option to verify that the server's SSL certificate is valid and trusted.

SSL Verify:

☐ (server must support SSL)

For authentication, you can use a password, a client certificate, or both (depending on your server settings). To use a client certificate, enter it on the Private Key/Certificate tab.

Get password from vault

NO

Password:

\*\*\*\*\*

Confirm Password:

\*\*\*\*\*

Cancel

Create

Qualys Cloud Platform Release Notes

11

## Unix installation

If you want to perform OS-dependent compliance checks, you'll need to tell us where the PostgreSQL configuration file is located on your Unix hosts. Unix authentication is required for these types of checks, so you'll need a Unix record for the same hosts in this record.

Note that the configuration file must be in the same location on all hosts (IPs) in the record. If the file is in a different location for some, then create additional Pivotal Greenplum records.

**New Pivotal Greenplum Record**Launch Help

Record Title

Login Credentials

Private Key / Certificate

**Unix**

IPs

Comments

**Unix**

To perform OS-dependent compliance checks, enter the full path to the PostgreSQL configuration file on your Unix hosts. This file must be in the same location for all Unix hosts in this record. Unix authentication is required.

Configuration File:

/var/lib/greenplum/data/postgresql.conf

example: /var/lib/greenplum/data/postgresql.conf

## Sample Reports

You'll see the Pivotal Greenplum technology in authentication reports and in compliance scan results. Check out these samples.

**Qualys Enterprise**

Summary

Results

GreenPlum 2 of 2 (100%)

GreenPlum 5 2 of 2 (100%)

Pivotal Greenplum

Host	Network	Host Technology	Instance
10.11.70.160 (-, -)	Global Default Network	Pivotal Greenplum 5.x	Port=5432, Database Name=postgres
Host	Network	Host Technology	Instance

Unix/Cisco/Checkpoint Firewall

GreenPlum 6 1 of 2 (50%)

Pivotal Greenplum

Host	Network	Host Technology	Instance
10.11.70.208 (-, -)	Global Default Network	-	Port=5432, Database Name=postgres

**Compliance Scan Results**

File Help

Report Summary

Launch Date: 02/20/2020 at 06:04:38 (GMT+0530)

Active Hosts: 1

Total Hosts: 1

Type: On demand

Status: Finished

Reference: compliance/1562158829.97084

External Scanners: vs\_rev\_pt10 (Scanner 11.9.18-1, Vulnerability Signatures 2.4.814-2)

Duration: 00:04:58

Title: 10.11.70.160 - 20200220

Network: Global Default Network

Asset Groups: -

IPs: 10.11.70.160

Excluded IPs: -

Compliance Profile: Initial\_PC\_Options

Appendix

Target hosts found alive (IP)

10.11.70.160

Pivotal Greenplum authentication was successful for these hosts

Pivotal Greenplum 5.x (Port: 5432, Database: postgres)

10.11.70.160

## Policies and Controls

You'll see Pivotal Greenplum 5.x and 6.x in the technologies list when creating a new policy.

**Create a New Policy**

**Empty Policy:** Build your policy from scratch.  
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

**Technologies** Select at least one technology. REQUIRED

Search technologies:  Add All | Remove All

No technologies selected

218 technologies Add all shown

- Oracle WebLogic Server 11g
- Oracle WebLogic Server 12c
- PaloAlto Networks PAN-OS
- Pivotal Greenplum 5.x**
- Pivotal Greenplum 6.x**
- Pivotal Web Server 6.x
- Pivotal tc Server 3.x

Back Choose Source Next

You'll see Pivotal Greenplum 5.x and 6.x when searching controls by technologies.

**Search**

CIDs:   
Example: 1072,1071,1091 (up to 20)

Text:

Status: ☐ Deprecated

Technologies:

- ☐ Oracle WebLogic Server 12c
- ☐ PaloAlto Networks PAN-OS
- ☒ Pivotal Greenplum 5.x
- ☒ Pivotal Greenplum 6.x
- ☐ Pivotal tc Server 3.x

Frameworks:

- ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
- ☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manage
- ☐ CCI List 1
- ☐ CIS - Apache HTTP Server 2.2 Benchmark v3.4.0 (09-23-20)

Framework ID:

Search

## Microsoft SharePoint Authentication Support

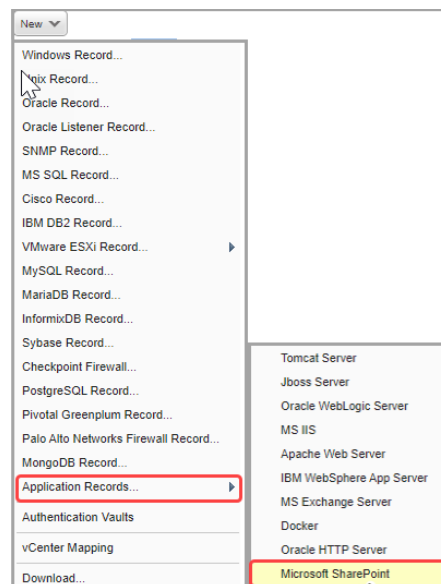
We now support Microsoft SharePoint authentication for compliance scans. Authentication is supported for SharePoint versions 2010, 2013, 2016, and 2019.

Windows authentication is required so you'll also need a Windows record for the host running Microsoft SharePoint. The Microsoft SharePoint record type is only available in accounts with PC or SCA and is only supported for compliance scans.

SharePoint instance will be auto discovered through the Windows Authentication Record. To connect to the MS SQL server, you'll need to provide information under MS SQL Login credentials in Microsoft SharePoint Record.

### Which technologies are supported?

We've added support for Microsoft SharePoint 2010, 2013, 2016, 2019 authentication for compliance scans.



### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Windows record already defined for the host running SharePoint.
- Create a Microsoft SharePoint record for the same host. Go to New > Application Records > Microsoft SharePoint.

### Sample Reports

You'll see the Microsoft SharePoint technology in authentication reports and in compliance scan results.

Check out these samples:

### Summary

#### Results

**Sharepoint 7 of 7 (100%)**

Microsoft SharePoint		
HOST	HOST TECHNOLOGY	INSTANCE
10.11.70.126 (csharepoint2016. qualys.com, CSHAREPOINT2016)	SharePoint Server 2016	SharePoint Server 2016
10.11.70.140 (csharepoint2013. qualys.com, CSHAREPOINT2013)	SharePoint Server 2013	SharePoint Server 2013
10.11.70.151 (csharepoint2019. qualys.com, CSHAREPOINT2019)	SharePoint Server 2019	SharePoint Server 2019

### Compliance Scan Results

File Help

#### Report Summary

Launch Date: 03/11/2020 at 16:48:52 (GMT)  
Active Hosts: 4  
Total Hosts: 4  
Type: On demand  
Status: Finished  
Reference: compliance/1583945274.00621  
External Scanners: vs\_rey\_pt (Scanner 11.7.45-1, Vulnerability Signatures 2.1.2823-1)  
Duration: 00:05:12  
Title: SharePointAuth  
Asset Groups: -  
IPs: 10.11.70.126, 10.11.70.140, 10.11.70.151,  
Excluded IPs: -  
Compliance Profile: [Initial PC Options](#)

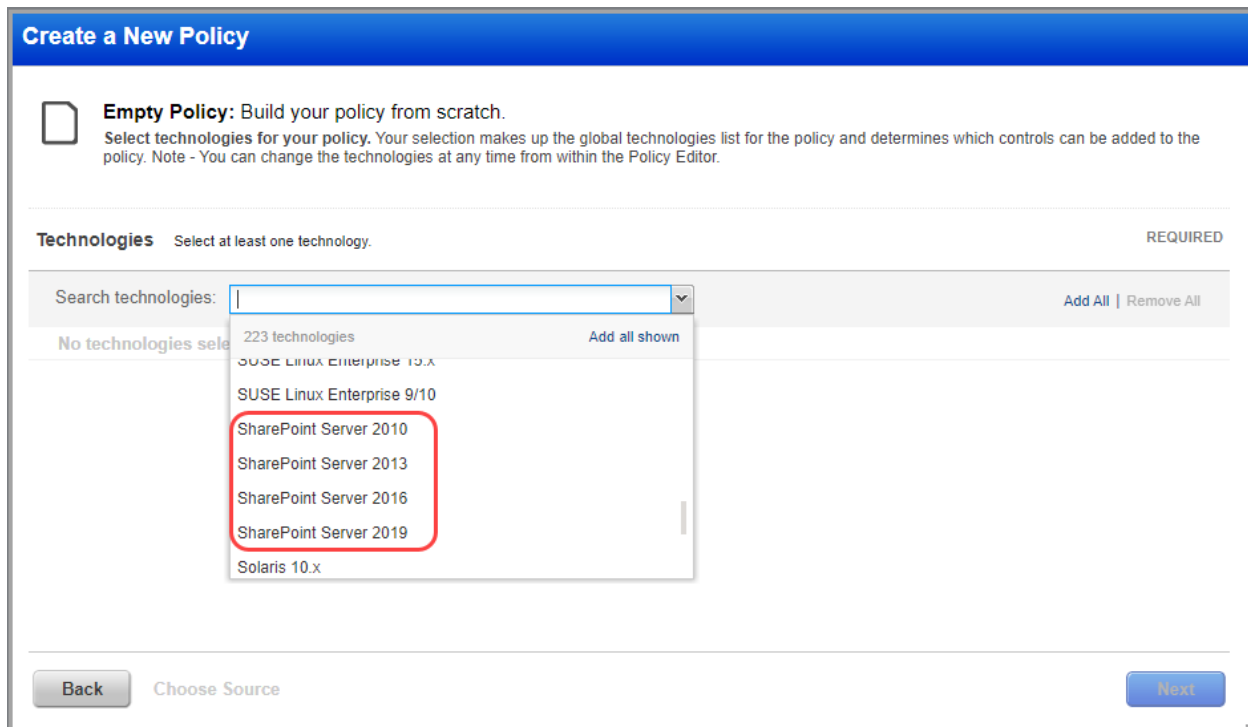
#### Appendix

**Target hosts found alive (IP)**  
10.11.70.126, 10.11.70.140, 10.11.70.151

**Microsoft SharePoint authentication was successful for these hosts**  
SharePoint Server 2013  
10.11.70.140  
SharePoint Server 2016  
10.11.70.126  
SharePoint Server 2019  
10.11.70.151

## Policies and Controls

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



**Create a New Policy**

**Empty Policy:** Build your policy from scratch.  
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

**Technologies** Select at least one technology. REQUIRED

Search technologies:  Add All | Remove All

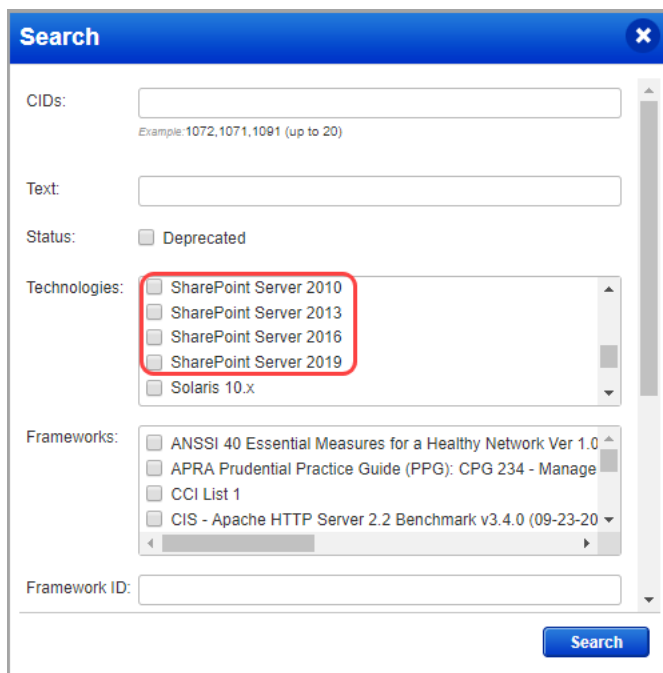
No technologies selected

223 technologies Add all shown

- SUSE Linux Enterprise 10.x
- SUSE Linux Enterprise 9/10
- SharePoint Server 2010**
- SharePoint Server 2013**
- SharePoint Server 2016**
- SharePoint Server 2019**
- Solaris 10.x

Back Choose Source Next

You'll see SharePoint Server 2010, 2013, 2016, and 2019 when searching controls by technologies.



**Search**

CIDs:   
Example: 1072,1071,1091 (up to 20)

Text:

Status: ☐ Deprecated

Technologies: ☐ SharePoint Server 2010  
☐ SharePoint Server 2013  
☐ SharePoint Server 2016  
☐ SharePoint Server 2019  
☐ Solaris 10.x

Frameworks: ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0  
☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manage  
☐ CCI List 1  
☐ CIS - Apache HTTP Server 2.2 Benchmark v3.4.0 (09-23-20)

Framework ID:

Search

## PostgreSQL Support for Windows

We've extended our support for PostgreSQL authentication to include PostgreSQL Windows hosts. We already support PostgreSQL on Unix hosts.

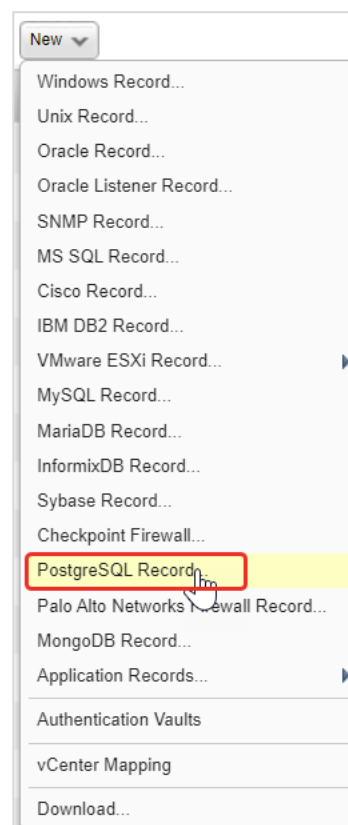
You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a Windows host, and scan it for compliance. Windows authentication is required so you'll also need a Windows record for the host running the database. This record type is only available in accounts with PC or SCA and is only supported for compliance scans.

### Which technologies are supported?

We've added support for PostgreSQL 9.x, PostgreSQL 10.x, PostgreSQL 11.x and PostgreSQL 12.x authentication for compliance scans on Windows hosts.

### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Windows record already defined for the host running the database.
- Create a PostgreSQL record for the same host. Go to New > PostgreSQL Record.



### Sample Reports

You'll see the PostgreSQL technology in compliance reports and in compliance scan results.

**Summary**

Asset Groups Summary

Asset Group	Successful	Failed	Not Attempted
PostgreSQL 9/10/11/12	8 of 8 100% Successful (4 with insufficient privileges)	0 of 8 0% Failed	0 of 8 0% Not Attempted

**Results**

PostgreSQL 9/10/11/12 8 of 8 (100%)

Host	Network	Host Technology
10.11.70.95 (ctomcatw2012r2, CTOMCATW2012R2)	Global Default Network	PostgreSQL 10.x
10.11.70.131 (cdw2016sql2017, CDW2016SQL2017)	Global Default Network	PostgreSQL 11.x
10.11.70.149 (compsql9, COMPSQL9)	Global Default Network	PostgreSQL 9.x
10.11.70.206 (cw2019data, CW2019DATA)	Global Default Network	PostgreSQL 12.x

**Compliance Scan Results**

Appendix

Target hosts found alive (IP)

10.11.70.95, 10.11.70.131, 10.11.70.149, 10.11.70.206

Target distribution across scanner appliances

External : 10.11.70.95, 10.11.70.131, 10.11.70.149, 10.11.70.206

PostgreSQL authentication was successful for these hosts

- PostgreSQL 10.x (Port: 5432, Database: postgres) 10.11.70.95
- PostgreSQL 11.x (Port: 5432, Database: postgres) 10.11.70.131
- PostgreSQL 9.x (Port: 5432, Database: postgres) 10.11.70.149
- PostgreSQL 12.x (Port: 5432, Database: postgres) 10.11.70.206



## Policies and Controls

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

**Create a New Policy**

**Empty Policy:** Build your policy from scratch.

**Select technologies for your policy.** Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

**Technologies** Select at least one technology. REQUIRED

Search technologies:  Add All | Remove All

No technologies selected 217 technologies Add all shown

- PostgreSQL 10.x
- PostgreSQL 11.x
- PostgreSQL 12.x
- PostgreSQL 9.x
- Red Hat Enterprise Linux 3/4
- Red Hat Enterprise Linux 5.x

Back Choose Source Next

You'll see PostgreSQL when searching controls by technologies.

**Search** ×

CIDs:   
*Example: 1072,1071,1091 (up to 20)*

Text:

Status: ☐ Deprecated

Technologies:

- ☐ PostgreSQL 10.x
- ☐ PostgreSQL 11.x
- ☐ PostgreSQL 12.x
- ☐ PostgreSQL 9.x
- ☐ Red Hat Enterprise Linux 3/4

Frameworks:

- ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
- ☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manage
- ☐ CCI List 1
- ☐ CIS - Apache HTTP Server 2.2 Benchmark v3.4.0 (09-23-20

Framework ID:

Search

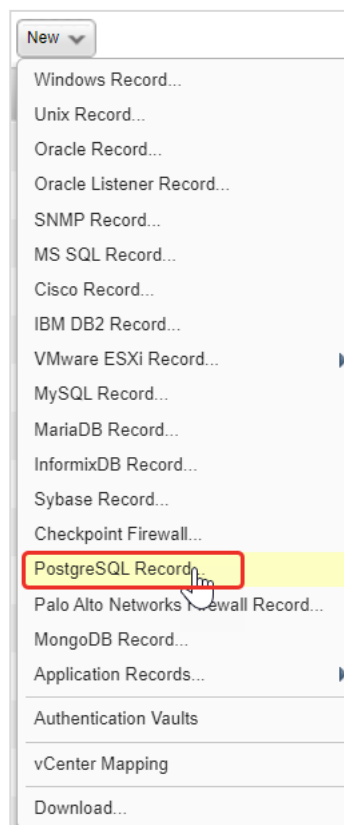
## PostgreSQL 12.x Support for Unix

We've extended our support for PostgreSQL authentication to include PostgreSQL 12.x on Unix hosts. We already support PostgreSQL 9.x, 10.x and 11.x on Unix hosts.

You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a Unix host, and scan it for compliance. Unix authentication is required so you'll also need a Unix record for the host running the database. This record type is only available in accounts with PC or SCA and is only supported for compliance scans.

### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Unix record already defined for the host running the database.
- Create a PostgreSQL record for the same host. Go to New > PostgreSQL Record.



### Sample Reports

You'll see the PostgreSQL 12.x technology in compliance reports and in compliance scan results.

#### Summary

##### IPs Summary

10.11.70.179:	2 of 3 66% Successful
	1 of 3 33% Failed
	0 of 3 0% Not Attempted

Network: All

#### Results

10.11.70.179 2 of 3 (66%)

PostgreSQL			
HOST	NETWORK	HOST TECHNOLOGY	INSTANCE
10.11.70.179 (-, -)	Global Default Network	PostgreSQL 12.x	Port=5432, Database Name=postgres

#### Compliance Scan Results

File Help

##### Report Summary

Launch Date:	01/24/2020 at 14:42:30 (GMT+0530)
Active Hosts:	2
Total Hosts:	2
Type:	On demand
Status:	Finished
Reference:	compliance/1579857052.66700
External Scanners:	new-hq-scanner (Scanner 11.8.27-1, Vulnerability Signatures 2.1.2707-1)
Duration:	00:01:12
Title:	postgres 12.x - 20200124 - 20200124
Network:	Global Default Network
Asset Groups:	postgres 12.x
IPs:	10.11.70.179, 10.115.105.243
Excluded IPs:	-
Compliance Profile:	postgres 12.x

#### Appendix

**Target hosts found alive (IP)**

10.11.70.179, 10.115.105.243

**Target distribution across scanner appliances**

new-hq-scanner : 10.11.70.179, 10.115.105.243

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts

10.11.70.179

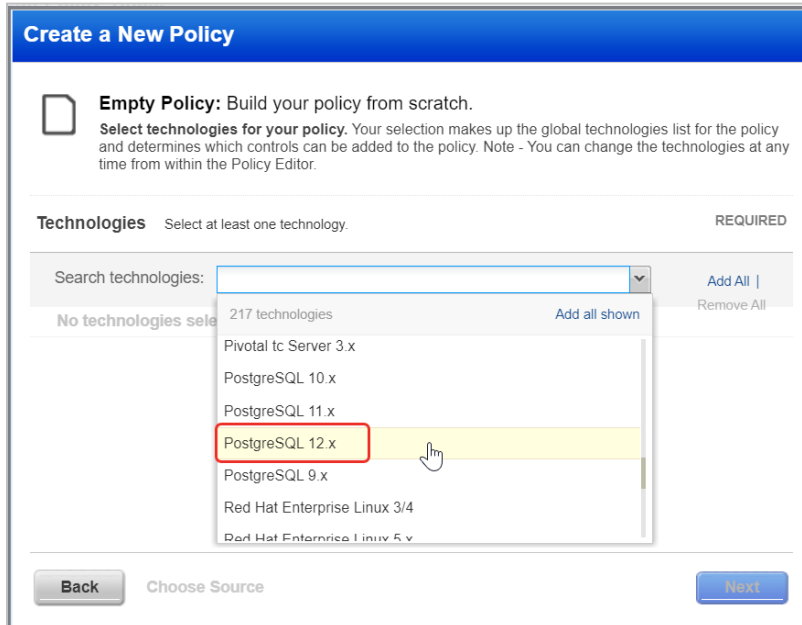
**PostgreSQL authentication was successful for these hosts**

PostgreSQL 12.x (Port: 5432, Database: postgres)

10.11.70.179

## Policies and Controls

You'll see PostgreSQL 12.x in the technologies list when creating a new policy.



**Create a New Policy**

**Empty Policy:** Build your policy from scratch.  
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

**Technologies** Select at least one technology. **REQUIRED**

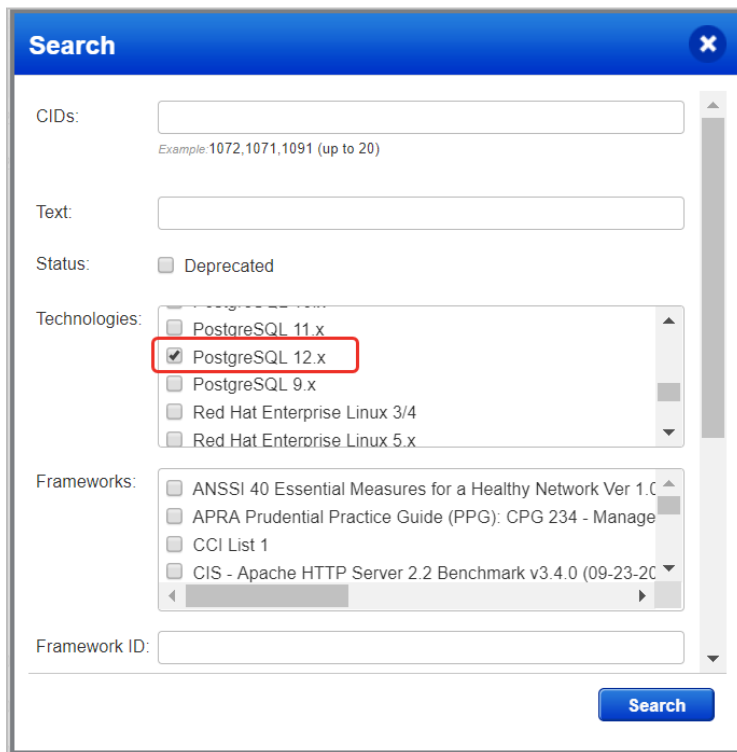
Search technologies:  **Add All** | **Remove All**

No technologies selected 217 technologies **Add all shown**

- Pivotal tc Server 3.x
- PostgreSQL 10.x
- PostgreSQL 11.x
- PostgreSQL 12.x**
- PostgreSQL 9.x
- Red Hat Enterprise Linux 3/4
- Red Hat Enterprise Linux 5.x

**Back** Choose Source **Next**

You'll see PostgreSQL 12.x when searching controls by technologies.



**Search**

CIDs:   
*Example: 1072,1071,1091 (up to 20)*

Text:

Status: ☐ Deprecated

Technologies:

- ☐ PostgreSQL 11.x
- ☒ **PostgreSQL 12.x**
- ☐ PostgreSQL 9.x
- ☐ Red Hat Enterprise Linux 3/4
- ☐ Red Hat Enterprise Linux 5.x

Frameworks:

- ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
- ☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manage
- ☐ CCI List 1
- ☐ CIS - Apache HTTP Server 2.2 Benchmark v3.4.0 (09-23-20

Framework ID:

**Search**

## Microsoft SQL Server 2019 Support

We've extended our support for MS SQL Server authentication to include Microsoft SQL Server 2019. These technologies are already supported: Microsoft SQL Server 2000, 2005, 2008, 2012, 2014, 2016 and 2017.

You'll need a MS SQL Server record to authenticate to your Microsoft SQL Server 2019 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.



## Thycotic Secret Server vault supported in Cisco & Checkpoint Firewall

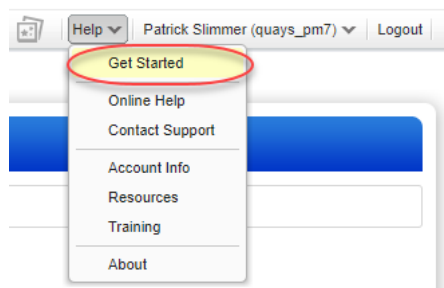
Now you can choose the Thycotic Secret Server vault type in your Cisco and Checkpoint Firewall authentication records. Go to Scans > Authentication and choose New > Cisco Record or New > Checkpoint Firewall. On the Login Credentials tab in the record choose Authentication Vault, Vault Type Thycotic Secret Server, select your vault record and enter the Secret Name that contains the password to be used for authentication.

How does it work - The scanning engine will perform a search for the secret name and then get the password from the secret returned by the search. A single exact match of the secret name must be found in order for authentication to be successful. The secret name may contain a maximum of 256 characters, and must not contain multibyte characters.

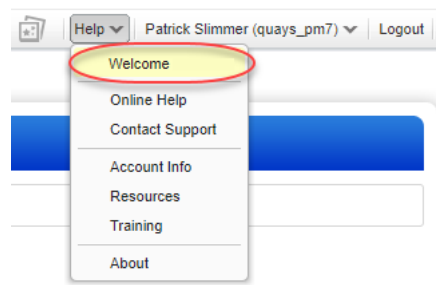
The image shows two side-by-side screenshots of the 'New Cisco Record' and 'New Checkpoint Firewall Record' forms. Both forms have a 'Login Credentials' tab selected. In the 'Login Credentials' section, 'Authentication Vault' is selected. The 'Vault Type' is set to 'Thycotic Secret Server'. The 'Vault Title' is 'My Thycotic Secret Server Vault' and the 'Secret Name' is 'secret'. A red circle highlights the 'Vault Type' dropdown and the 'Secret Name' field in both forms.

## New option on the Help menu replaces Quick Start Guide

For accounts that have been upgraded to VMDR, the Quick Start Guide has been replaced with Welcome and this option now appears on the Help menu (previously, the Quick Start Guide appeared in the menu below your username). Choose the Welcome option to go to the Welcome page in VMDR where you can get started in a few quick steps.



You'll see Get Started on the Help menu in the PC and SCA apps. You'll also see it in accounts upgraded to VMDR experience and in accounts that have not yet been upgraded. This replaces the Quick Start Guide for these apps. Choose Get Started anytime you need it for help with first steps.



## New Remote Security Hygiene Dashboard and Library Policies

Realize/visibility in device hygiene by tracking common misconfigurations that leave the endpoints exposed to exploits. It is important to monitor these remote hosts for security hygiene to minimize the asset or user downtime as well as to reduce the exposure to the breaches or exploits from malware or advanced persistent threats (APTs). This also serves as an evidence for your compliance and risk audit

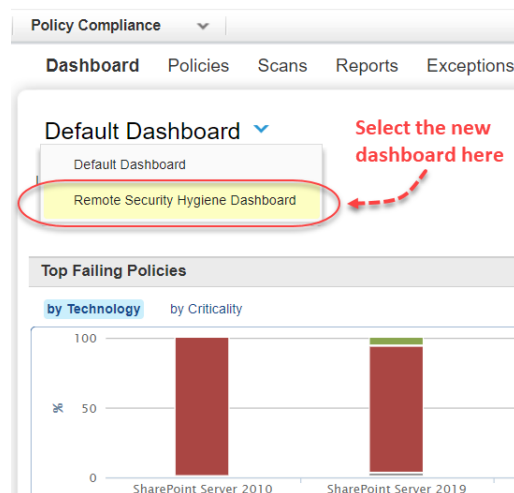
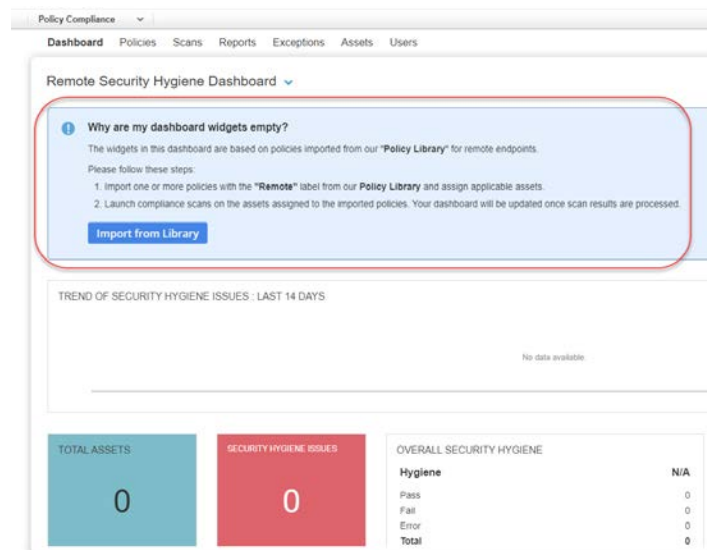
In Policy Compliance (PC) and Security Configuration Assessment (SCA) you'll see the new Remote Security Hygiene Dashboard and 2 new policies that you can import for remote endpoints – one for Windows and one for Mac. The policies are targeted for tracking critical security settings applicable for remote endpoints such as below:

- Password and account management settings
- Anti-virus settings, anti-phishing settings
- Encryption for data-at-rest
- Web browser security

### New Remote Security Hygiene Dashboard

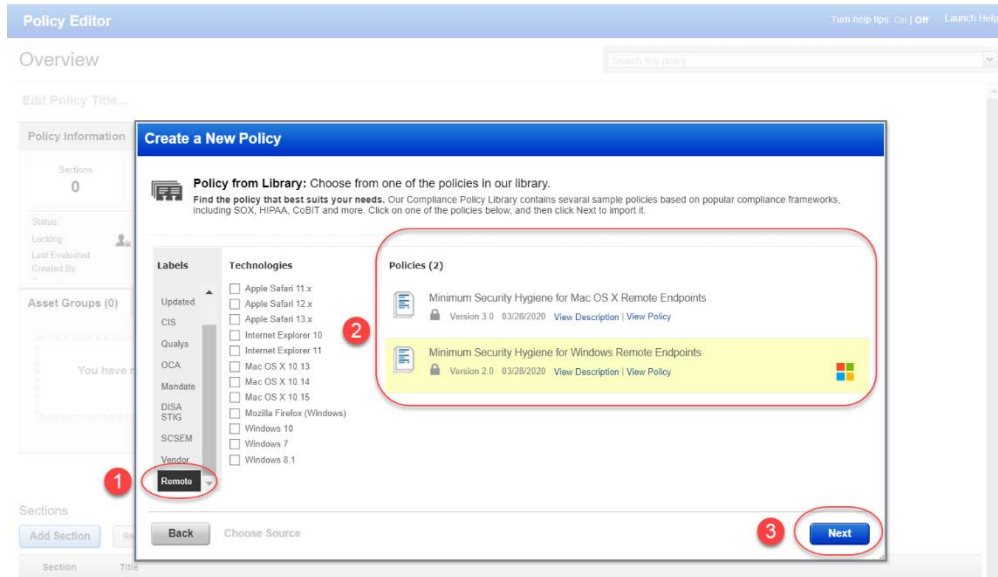
In PC or SCA, go to Dashboard and pick the “Remote Security Hygiene Dashboard”. The widgets on your dashboard will be updated automatically with scan data from your PC cloud agents.

Not using agents? Follow the steps on the screen (shown below) to import new remote endpoint policies from our Library, assign assets to the policies and scan those assets for compliance. Once scan results are processed, we'll update the widgets on your dashboard with the scan data.



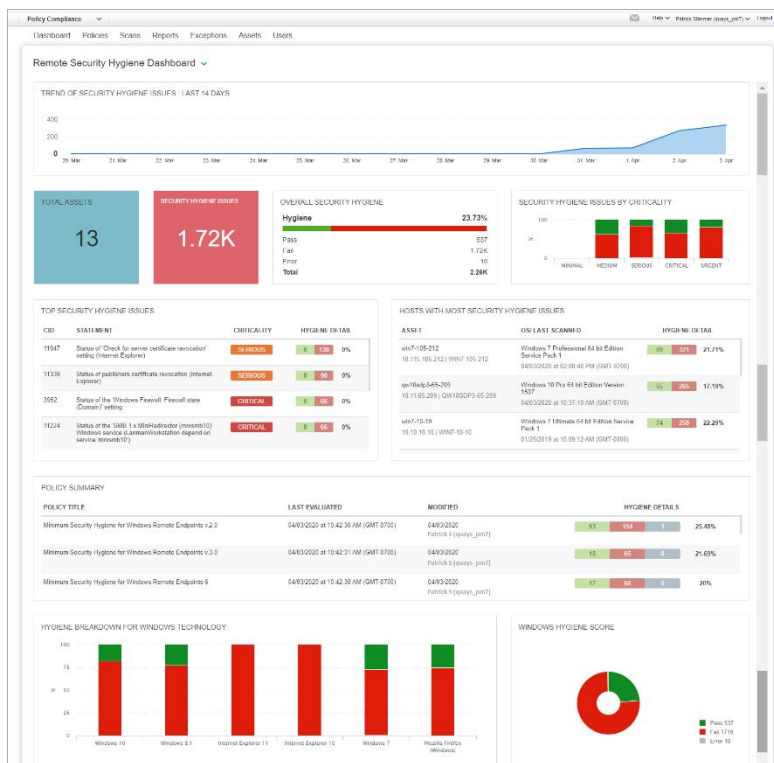
## How to import policies for remote endpoints

Click the “Import from Library” button on the Dashboard. Then (1) choose the “Remote” label to find policies for remote endpoints, (2) select the policy you want to import, and (3) click Next. Follow the prompts to give your policy a name and assign assets. The policy will be created and saved to your account.



## Sample Dashboard with Windows Policy

Check out this sample dashboard based on the Minimum Security Hygiene for Windows Remote Endpoints policy imported from the Library.



## Issues addressed in this release

- Fixed an issue where when running an interactive compliance report on a large number of hosts, the controls pop-up appeared blank.
- We now hide the Configuration tab in Threat Protect app for users who have upgraded to VMDR (FULL) and unlimited license type.
- Fixed an issue where asset and vulnerabilities report fetching were returning no results for the status: fixed query, Now the report lists accurate results.
- You can now search for a specific dashboard using the new search option in the Dashboard tab. Just start typing a dashboard name and list of matching dashboards will be listed for you to select from.
- We have fixed an issue and now the Dashboard tab is displayed properly in the Safari web browser.
- Some QID descriptions were not displayed properly in Japanese language for WAS Knowledge Base. This issue is now fixed and all descriptions are displayed properly.
- We have enhanced our search query engine and you can now use the query syntax for "exists in". It should be searchable with \*. For example:  
name: \*  
vulnerabilities.port:\*  
vulnerabilities.protocol:\*
- We have fixed an issue and you can now successfully remove tags using the REST 2.0 API call.
- We have fixed an issue and now the download of user report in the Administration module is considerably faster.
- Made updates to the Qualys API (VM, PC) User Guide to delete the section on Removing IPv6 Mappings since this is no longer supported from the API.
- Updated the online help to explain that only the Manager user has privileges to edit storage settings to auto delete scan results.
- Updated the online help for Search Lists to explain that vulnerabilities with the half red / half yellow severity icon match search lists for both confirmed and potential vulnerabilities. If you create a search list that includes all confirmed QIDs and excludes all potential QIDs, then the QIDs with half red / half yellow severity will be excluded.
- Updated the online help for CheckPoint Firewall Authentication to list supported technology versions as CheckPoint Gaia R75 and above, and CheckPoint SecurePlatform PRO R75 and above.
- Updated the System Requirements help to state that we do not support browsers on mobile devices at this time.
- Updated the online help for the VM Scan Summary Notification to clarify that this email includes vulnerability trend information based on the processed results including the total number of new, reopened, active and closed vulnerabilities. Please keep in mind that this email includes trend data, not the actual scan results.
- Updated the online help for OPatch Checks to explain that some Oracle detections use the OPatch method and others do not. In all cases database authentication is required in addition to host authentication for successful Oracle scanning.
- The remove tag functionality was not working as expected. We have fixed this issue so that users will now be able to remove parent child tag relationship without deleting the child tag.



- We fixed an issue where the user was unable to update the option profile to exclude "Timeout Error Threshold" and "Unexpected Error Threshold". You can now create or modify option profile without any issues associated with changes in Timeout Error Threshold and Unexpected Error Threshold.
- We have fixed an issue where the scans that contain SSL vulnerabilities were not getting processed and showing error during scan processing. After the fix, scans are processed successfully.
- The user can now see the payload details for the detections as before in the online report.
- We fixed an issue where payload data information in the online and downloaded reports was not matching. After the fix, both the reports show the same information for payload details.