Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.2

July 9, 2020 (Updated July 28, 2020)

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

Qualys 10.2 brings you more improvements and updates! Learn more

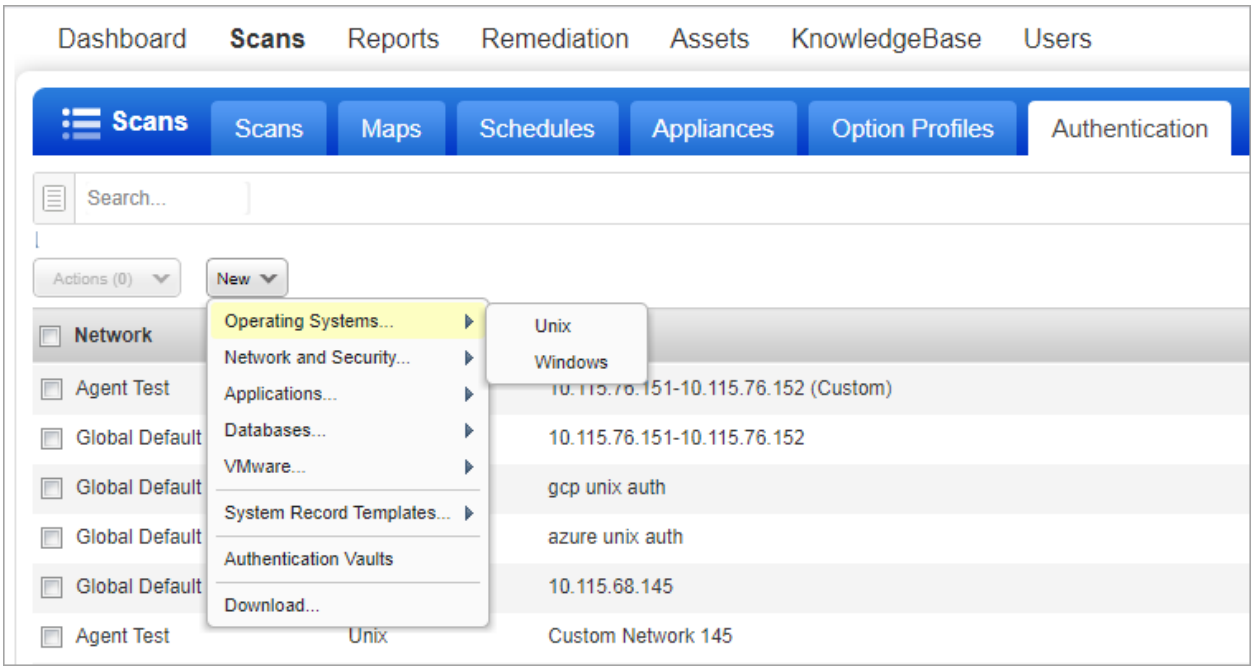
Qualys Cloud Platform

Restructured Authentication Record Menu

We have restructured the authentication record menu items to logically organize the authentication records under various categories based on the record type or family. Authentication Records that are of the same type/family are now grouped in the same category.

For example: Under Operating Systems, you will find options for creating authentication records for operating systems, such as Unix and Windows. Similarly, Applications category has options to create authentication records for applications, such as Apache Web Server, Docker and so on. The other categories are: Network and Security, Databases, VMware, System Record Templates.

To access authentication records, go to Scans > Authentication in VM and PC modules.



The table below lists the categories and the authentication records grouped under these categories according to the new structure. In the table, the authentication records that mention PC + SCA are only available in PC + SCA module. Whereas, the authentication records that mention VM only are available only in VM module. All other authentication records that do not mention (PC + SCA) or (VM only) are available in both VM and PC.

Category	Authentication Record
Operating Systems	- Unix - Windows
Network and Security	- CheckPoint Firewall (PC + SCA) - Cisco - Palo Alto Networks Firewall - SNMP

Application Records	- Apache Web Server (PC + SCA) - Docker (PC + SCA) - HTTP Record (VM only) - IBM WebSphere App Server (PC + SCA) - JBoss Server - MS Exchange Server (PC + SCA) - MS IIS (PC + SCA) - MS SharePoint (PC + SCA) - Oracle HTTP Server (PC + SCA) - Oracle WebLogic Server - Tomcat Server
Databases	- IBM DB2 - Informix DB - MariaDB (PC + SCA) - MongoDB - MS SQL (PC + SCA) - MySQL - Oracle Listener - Oracle Record - Pivotal Greenplum (PC + SCA) - PostgreSQL (PC + SCA) - Sybase
VMWare	- vCenter Mapping List - vCenter Mapping Upload - vCenter - VMware ESXi
System Record Templates	Oracle System Record Template
Authentication Vaults	No Change
Download	No Change

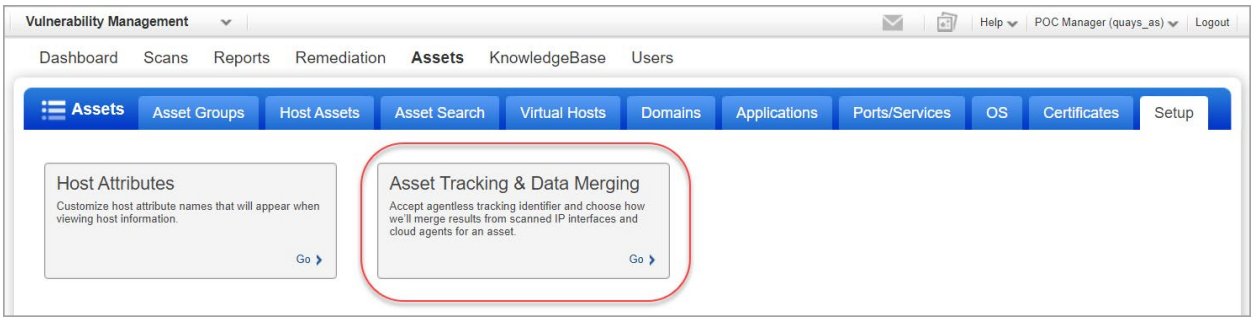
Changes in Agentless Tracking Identifier and Asset Tracking & Data Merging

A new setup option under Assets called “Asset Tracking & Data Merging” allows you to accept the Agentless Tracking Identifier feature and also choose how you want to merge results from scanned IP interfaces and cloud agents for your assets – all from the same setup window. This makes setting things up more convenient.

This new setup option replaces the following:

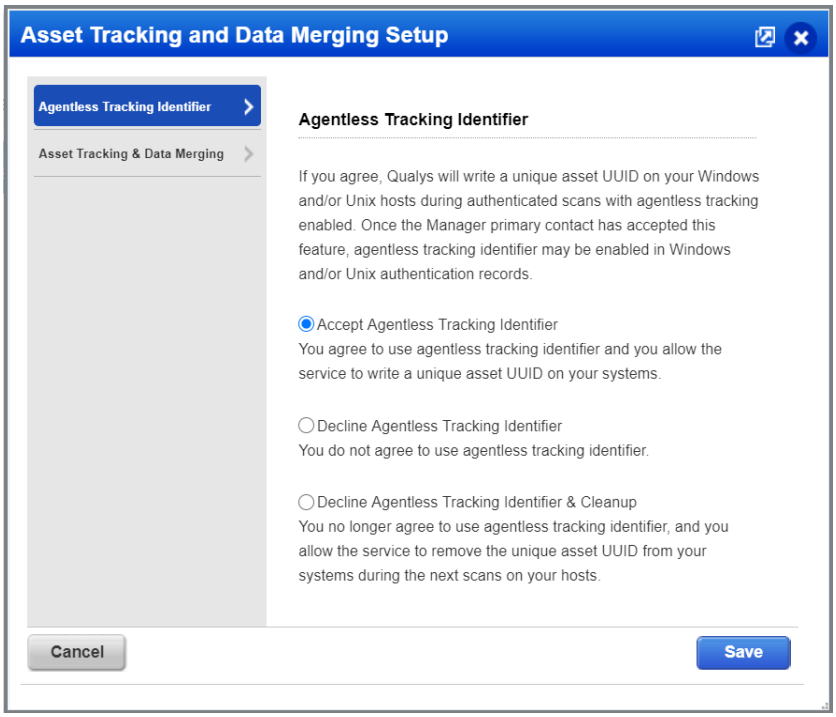
- Agentless Tracking option that was previously under Scans > Setup

- Cloud Agent Setup option that was previously under Users > Setup



Agentless Tracking Identifier

This section allows the Manager primary contact to accept or decline the agentless tracking identifier feature. Once hosts are scanned using agentless tracking identifier, they are tracked by a unique asset UUID.



What are the steps?

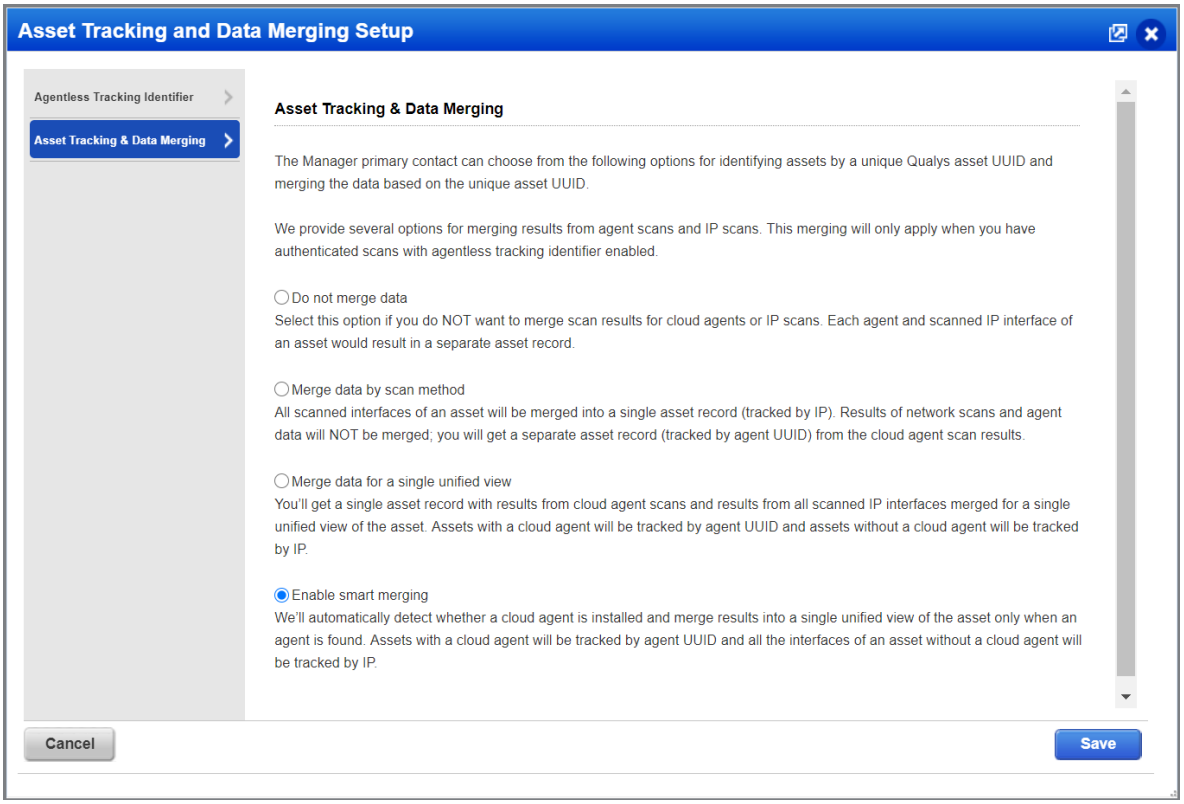
Go to Assets > Setup > Asset Tracking & Data Merging > Agentless Tracking Identifier. Select the appropriate option to accept or decline this feature. If you no longer agree to use agentless tracking identifier and want to remove the unique asset UUID from your systems during the next scan, select Decline Agentless Tracking Identifier and Cleanup option.

Asset Tracking & Data Merging

This section provides options to the Manager primary contact for identifying assets by a unique asset UUID and for merging data based on the unique asset UUID. With this release, we offer multiple new options for merging scan results from cloud agent scans and IP scans, giving you more control. Choose the option that's right for you. Note that the merging of results only applies when you have authenticated scans with agentless tracking identifier enabled.

What are the steps?

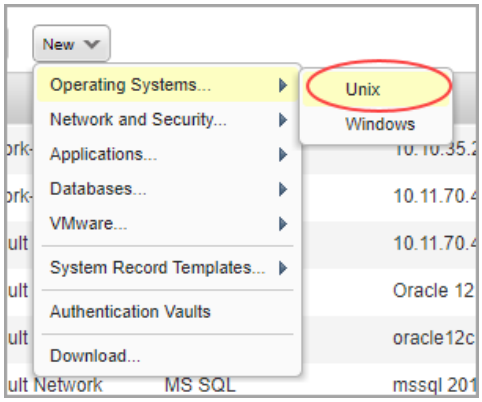
Go to Assets > Setup > Asset Tracking & Data Merging > Asset Tracking & Data Merging. Select one of the merging options on the page.



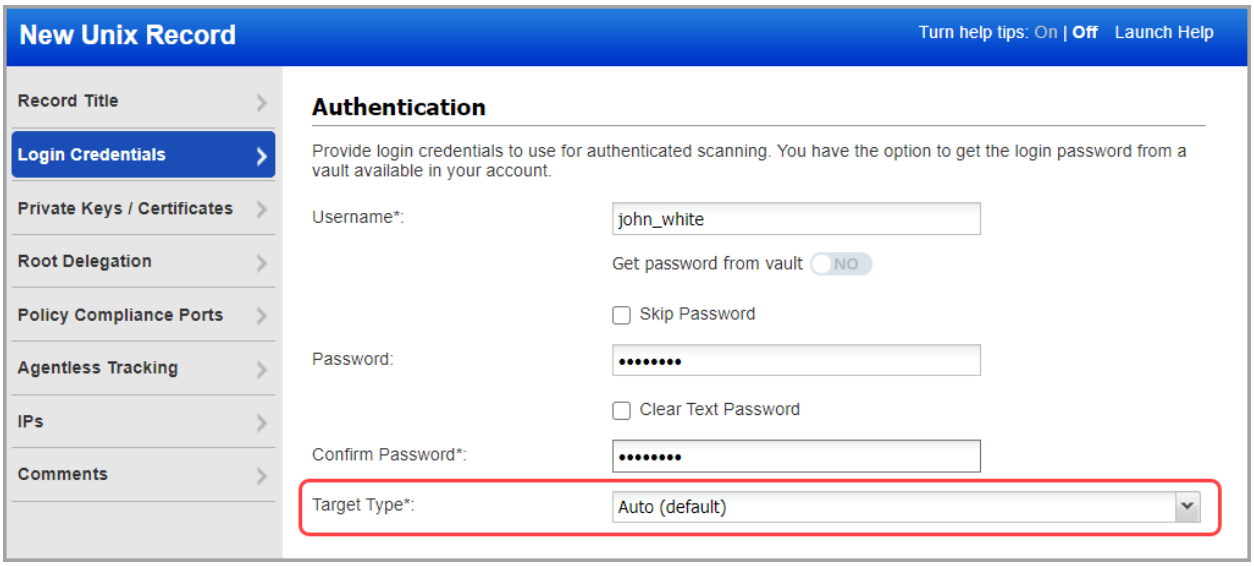
Support to Add Target Type to Unix Authentication Records

You can now provide a target type while creating or updating the Unix (SSH2) authentication record. With the addition of this field, you can define the non-shell based target types in the SSH2 authentication record. Targets with a standard Unix shell will continue to be auto-detected. With this release, Qualys offers only the single "auto (default)" option. With upcoming releases, Qualys will make other target types available.

To create a new Unix record, navigate to Scans > Authentication > New and from Operating Systems select Unix.



In the record creation wizard, navigate to the Login Credentials tab where Auto (default) value is selected for the Target Type.



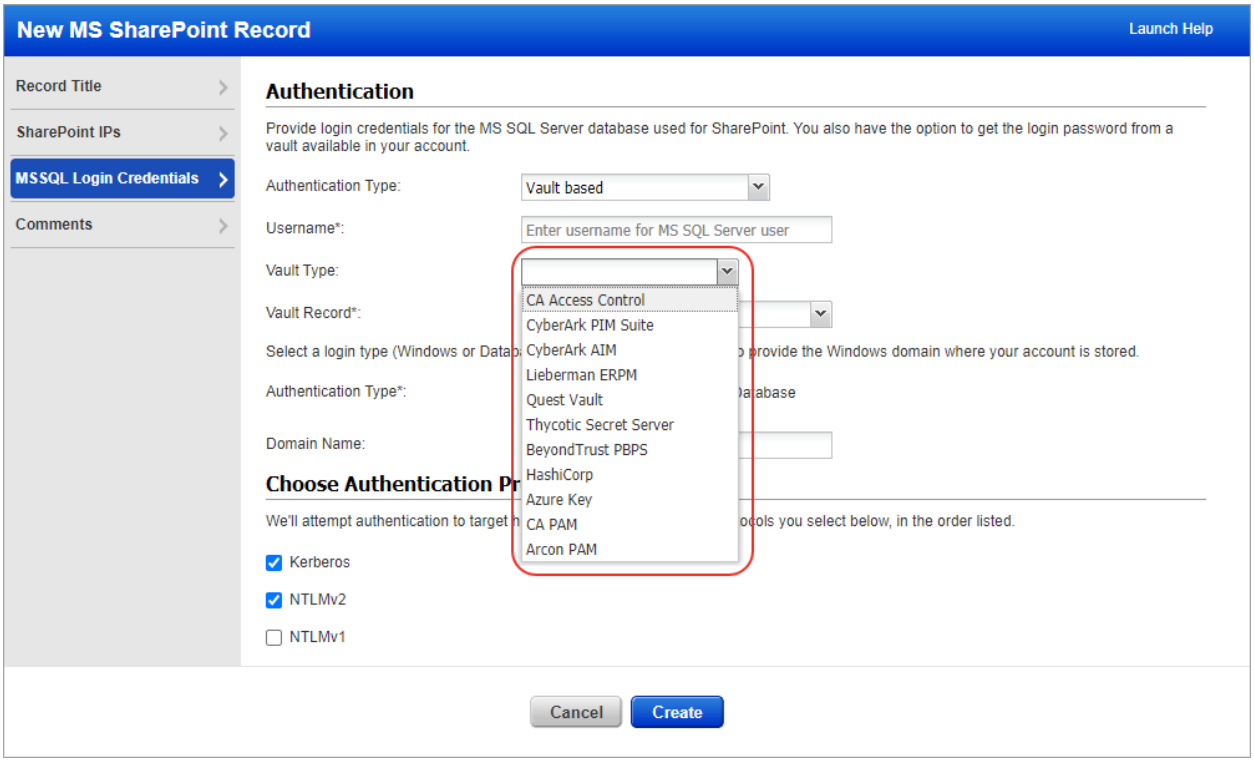
Existing auth records will start showing the Target Type field when they are opened for editing. The target types are set to "Auto (default)" for these records.

Qualys Policy Compliance (PC)

New Vaults Supported for MS SharePoint

More vaults are supported for MS SharePoint authentication, giving you more options for retrieving login credentials. You'll now see these additional vaults in the MS SharePoint authentication record: Arcon PAM, Azure Key, CA Access Control, HashiCorp, and Lieberman ERPM. The MS SharePoint record will also continue to support the following vaults: BeyondTrust PBPS, CA PAM, CyberArk AIM, CyberArk PIM Suite, Quest Vault and Thycotic Secret Server.

To create a new MS SharePoint record using a vault, go to Scans > Authentication > New > Application Records > MS SharePoint. From the MSSQL Login Credentials tab, select Vault based from the Authentication Type drop-down and select the vault type.



Support for New OCA Technologies

We now support the following new technologies on assets for which data is collected using Out-of-Band Configuration Assessment (OCA) tracking.

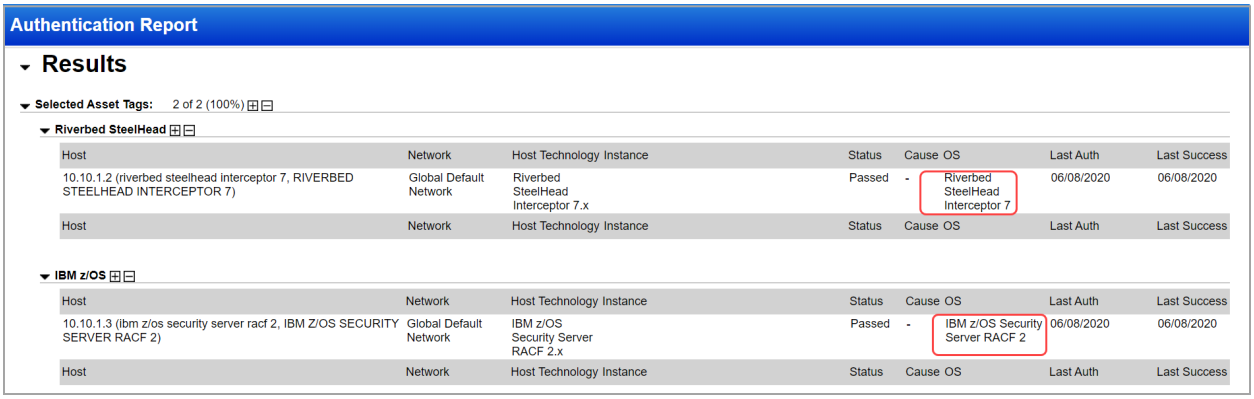
- Riverbed SteelHead Interceptor 7.x

- IBM z/OS Security Server RACF 2.x

Simply navigate to the Reports tab and run Policy Compliance Reports and Authentication Reports for these technologies to view your compliance posture.

Sample Report

Here's a sample Authentication Report with Riverbed SteelHead Interceptor 7.x and IBM z/OS Security Server RACF 2.x.



Authentication Report

Results

Selected Asset Tags: 2 of 2 (100%)

Riverbed SteelHead

Host	Network	Host Technology Instance	Status	Cause	OS	Last Auth	Last Success
10.10.1.2 (riverbed steelhead interceptor 7, RIVERBED STEELHEAD INTERCEPTOR 7)	Global Default Network	Riverbed SteelHead Interceptor 7.x	Passed	-	Riverbed SteelHead Interceptor 7	06/08/2020	06/08/2020
Host	Network	Host Technology Instance	Status	Cause	OS	Last Auth	Last Success

IBM z/OS

Host	Network	Host Technology Instance	Status	Cause	OS	Last Auth	Last Success
10.10.1.3 (ibm z/os security server racf 2, IBM Z/OS SECURITY SERVER RACF 2)	Global Default Network	IBM z/OS Security Server RACF 2.x	Passed	-	IBM z/OS Security Server RACF 2	06/08/2020	06/08/2020
Host	Network	Host Technology Instance	Status	Cause	OS	Last Auth	Last Success

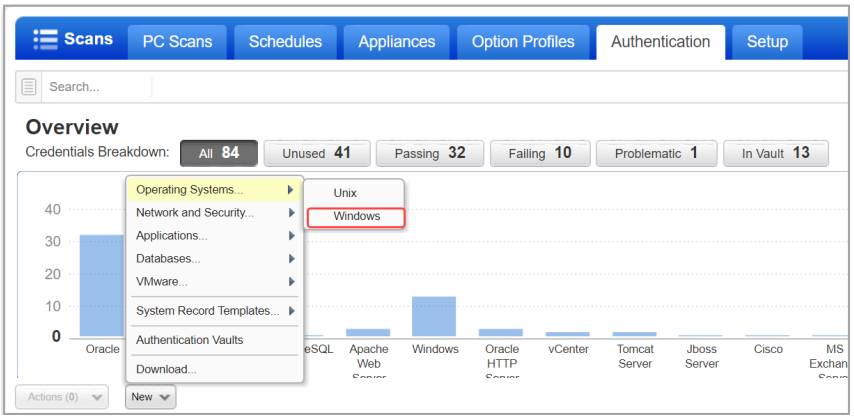
Microsoft Windows 2008, 2012, 2016 Certification Authority

We've extended our support for Windows authentication to include Windows 2008, 2012, 2016 Certification Authority.

You'll need a Windows record to authenticate the Windows 2008, 2012, 2016 Certification Authority, and scan it for compliance.

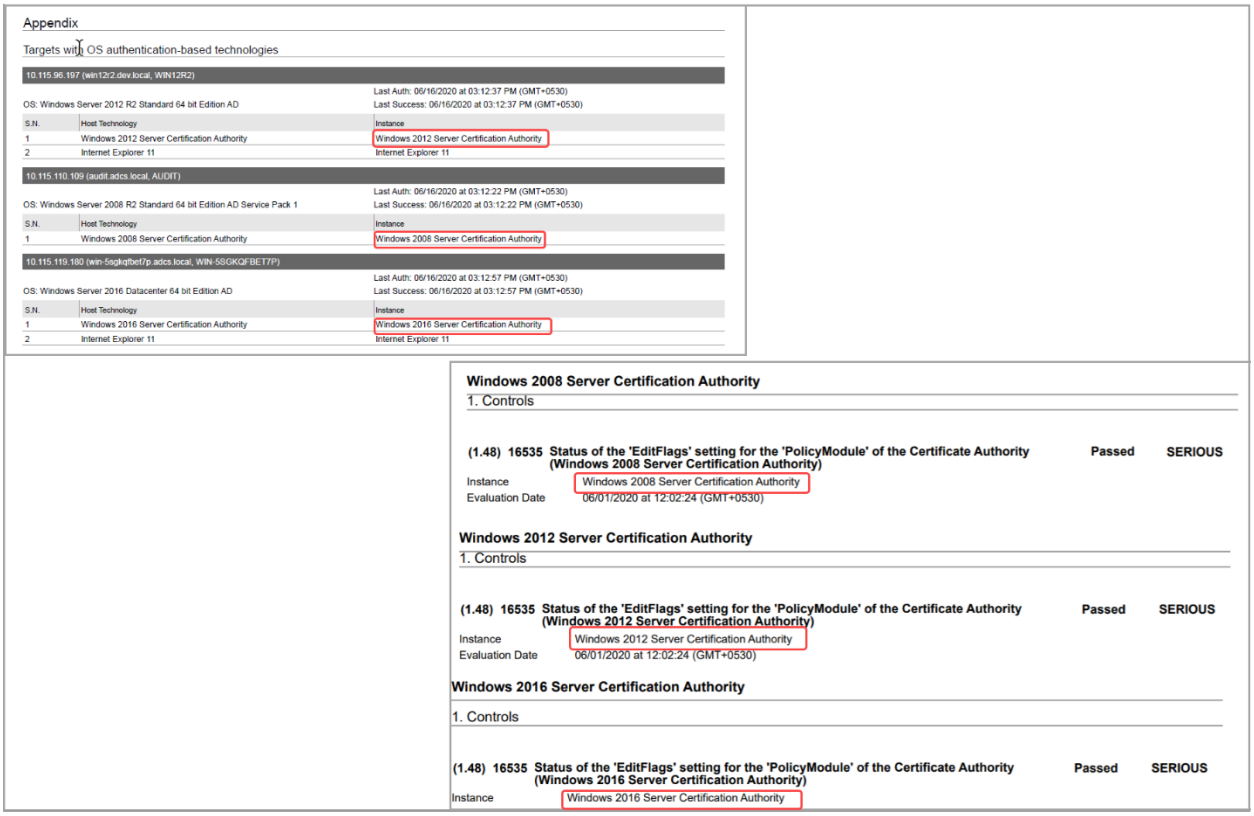
How do I get started?

Go to Scans > Authentication and choose New > Operating Systems > Windows.



Sample Reports

You'll see Windows 2008, 2012, 2016 Certification Authority instances in Authentication Reports and Policy Reports.



Appendix

Targets with OS authentication-based technologies

10.115.96.197 (win12r2.dev.local, WIN12R2)

Last Auth: 06/16/2020 at 03:12:37 PM (GMT+0530)
OS: Windows Server 2012 R2 Standard 64 bit Edition AD — Last Success: 06/16/2020 at 03:12:37 PM (GMT+0530)

S.N.	Host Technology	Instance
1	Windows 2012 Server Certification Authority	Windows 2012 Server Certification Authority
2	Internet Explorer 11	Internet Explorer 11

10.115.110.109 (audit.adcs.local, AUDIT)

Last Auth: 06/16/2020 at 03:12:22 PM (GMT+0530)
OS: Windows Server 2008 R2 Standard 64 bit Edition AD Service Pack 1 — Last Success: 06/16/2020 at 03:12:22 PM (GMT+0530)

S.N.	Host Technology	Instance
1	Windows 2008 Server Certification Authority	Windows 2008 Server Certification Authority

10.115.119.180 (win-5sgkqfbet7p.adcs.local, WIN-5SGKQFBET7P)

Last Auth: 06/16/2020 at 03:12:57 PM (GMT+0530)
OS: Windows Server 2016 Datacenter 64 bit Edition AD — Last Success: 06/16/2020 at 03:12:57 PM (GMT+0530)

S.N.	Host Technology	Instance
1	Windows 2016 Server Certification Authority	Windows 2016 Server Certification Authority
2	Internet Explorer 11	Internet Explorer 11

Windows 2008 Server Certification Authority

1. Controls

(1.48) 16535 Status of the 'EditFlags' setting for the 'PolicyModule' of the Certificate Authority (Windows 2008 Server Certification Authority) **Passed** **SERIOUS**

Instance: Windows 2008 Server Certification Authority
Evaluation Date: 06/01/2020 at 12:02:24 (GMT+0530)

Windows 2012 Server Certification Authority

1. Controls

(1.48) 16535 Status of the 'EditFlags' setting for the 'PolicyModule' of the Certificate Authority (Windows 2012 Server Certification Authority) **Passed** **SERIOUS**

Instance: Windows 2012 Server Certification Authority
Evaluation Date: 06/01/2020 at 12:02:24 (GMT+0530)

Windows 2016 Server Certification Authority

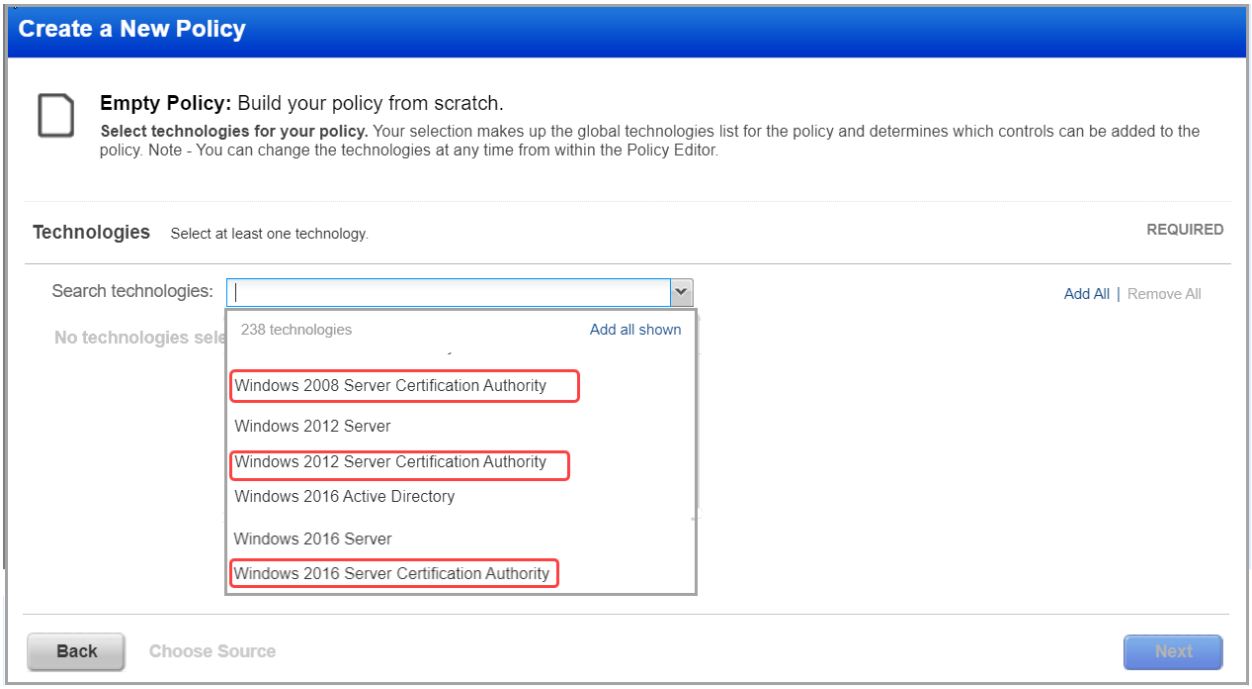
1. Controls

(1.48) 16535 Status of the 'EditFlags' setting for the 'PolicyModule' of the Certificate Authority (Windows 2016 Server Certification Authority) **Passed** **SERIOUS**

Instance: Windows 2016 Server Certification Authority

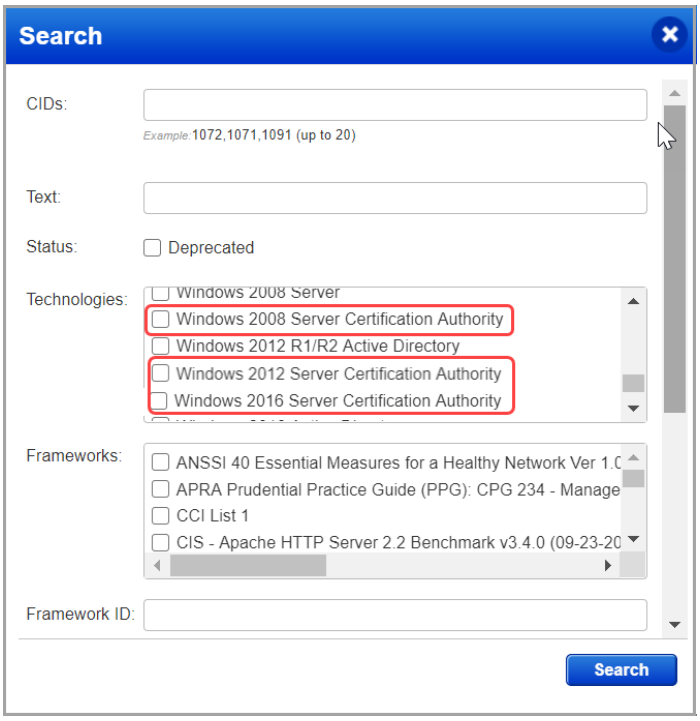
Policies and Controls

You'll also see Windows 2008, 2012, 2016 Certification Authority in the technologies list when creating a new policy.



Search Controls

You'll see Windows 2008, 2012, 2016 Certification Authority when searching controls by technologies.



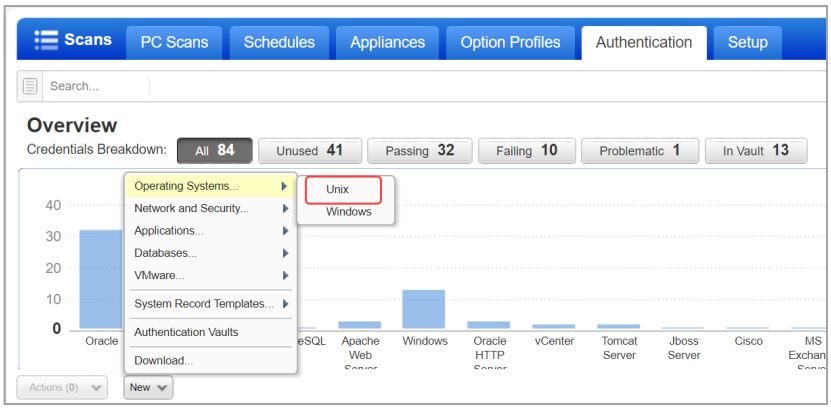
IBM Sterling Connect: Direct 4.x (Unix)

We've extended our support for Unix authentication to include IBM Sterling Connect: Direct 4.x (Unix).

You'll need a Unix record to authenticate the IBM Sterling Connect: Direct 4.x (Unix), and scan it for compliance.

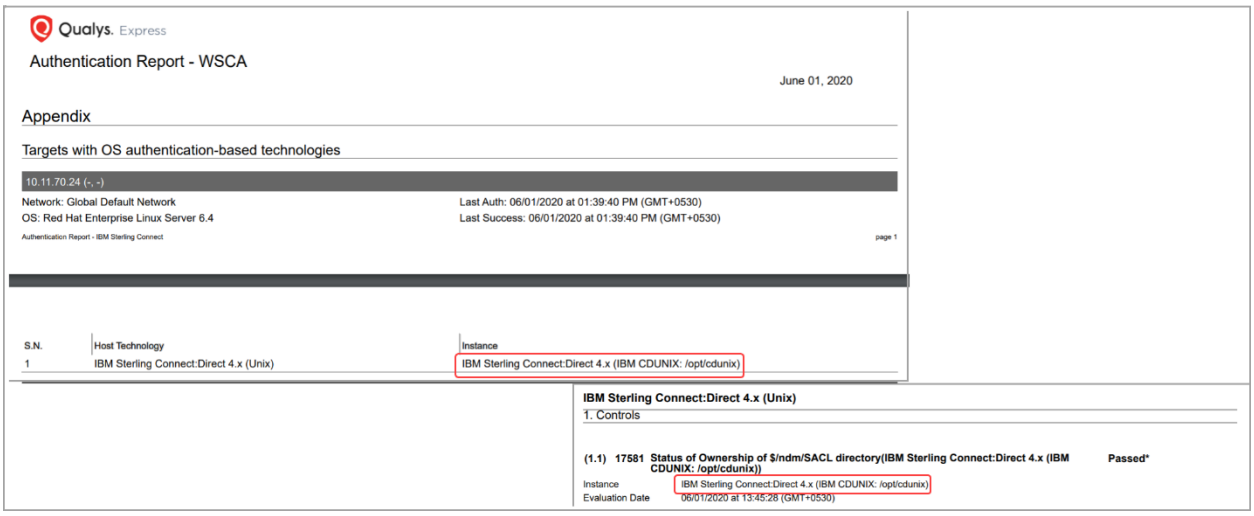
How do I get started?

Go to Scans > Authentication and choose New > Operating Systems > Unix.



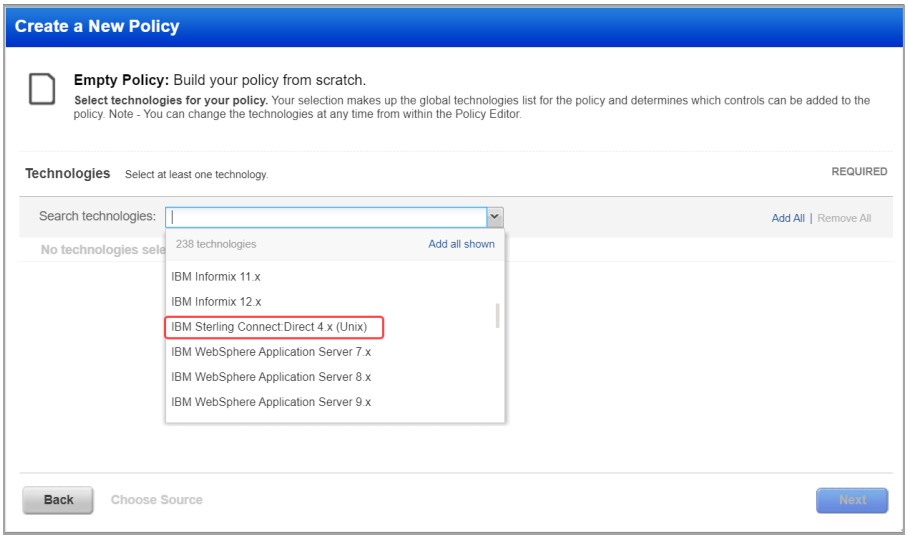
Sample Reports

You'll see IBM Sterling Connect: Direct 4.x (Unix) instance in Authentication Reports and Policy Reports.



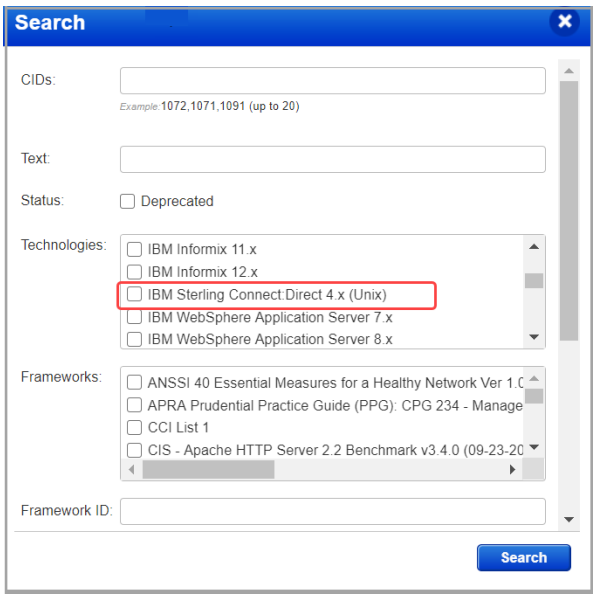
Policies and Controls

You'll also see IBM Sterling Connect: Direct 4.x (Unix) in the technologies list when creating a new policy.



Search Controls

You'll see IBM Sterling Connect: Direct 4.x (Unix) when searching controls by technologies.



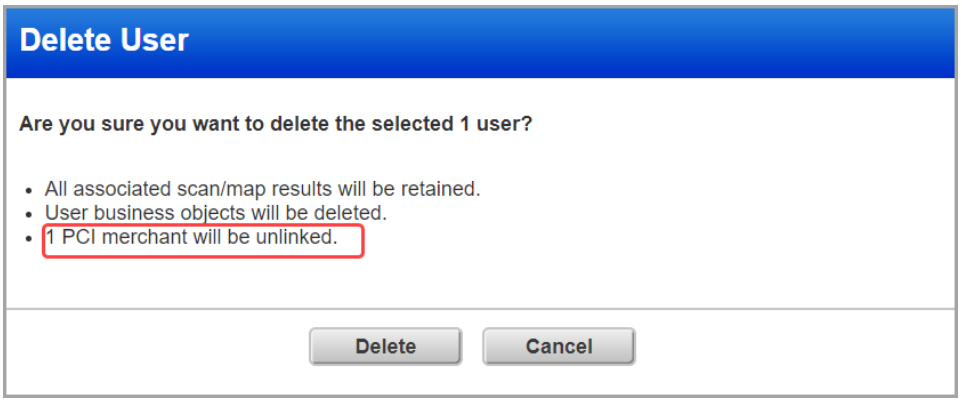
Qualys Vulnerability Management (VM)

Enhancement to the Delete User Feature

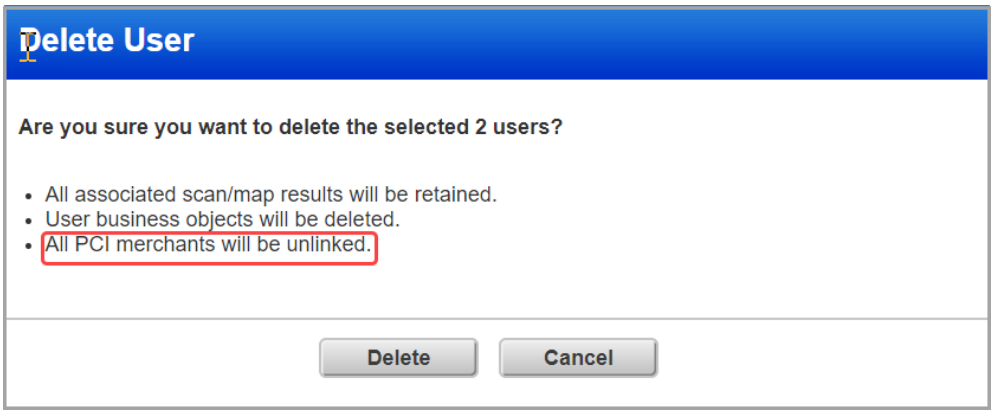
We have made the following enhancements to the Delete a user feature:

When you delete a VM user, the user is automatically unlinked from the PCI account, and you will see the following notification message.

1) If you delete one user, the following message is displayed.



If you delete more than one user, the following message is displayed:



2) After you delete a user linked to a PCI account, you can link the same PCI account to a different user.

Issues Addressed

- Fixed an issue where, when scans get delayed because of reaching the concurrency limit set for the subscription, the scan cancel time was calculated based on the actual launch time of the scan instead of the scheduled launch time.
- Fixed an issue where the Delete link was not functioning on the References page of User-defined controls.
- Fixed an issue where you could not save policies with controls that have single quotes in the expected value.
- Fixed a performance issue where the controls/hosts selection page was not loading when you tried to run an interactive report on asset groups with more than 8000 assets.
- We have now fixed an issue where purging of assets that contain data and exist in more than one module, now purge the entire data for it.
- Fixed an issue where CSV output for the Posture API was showing incorrect values for the pass and fail date columns. Now, the API call is showing correct CSV output with/without remediation info.
- We fixed an issue where the expected values set for the evaluated user defined controls in an exported policy was getting reset to original values on importing the policy in PC. After the fix, the new expected values that are set for the user defined controls are retained in the imported policy.
- We have now fixed an issue where Adding Host Assets using IP addresses caused error due to existence of hidden/special characters in the IP address.
- We have made performance improvements for processing FIM/DI UDCs when the auto-update of an expected value is selected. This will remove any delay in updating/evaluating controls for the policies.
- We fixed an issue where in the XML report for the first failed control for the first host, the 'Cause of Failure' was listing multiple criteria in the <Unexpected>/ <Unexpected> section. Now the section displays single criteria or the expected criteria for the instances.
- Fixed a performance issue related to Policy Compliance Scorecard reports.
- Fixed an issue with STIG report generation using IP asset selection for non-network account.
- Fixed an issue where you were not able to save a policy if the reference field of the control contained single quotes.
- Fixed an issue where Host List API Response was not showing EC2_INSTANCE_ID parameter.
- Fixed an issue to update MariaDB Auth record without Unix/Windows config parameters through API.
- We have now fixed an issue where an extra space was getting added in the DNS hostname of the assets in the Posture API data.
- We have updated the description for "password" input parameter for Session Login in the API User Guide to clarify how curl request should be formed using -d and -u.
- We have updated the online help to describe how appliance indicators are represented using icons.
- The online help is now updated to describe how to create a Palo Alto Networks Firewall record in order to authenticate to a firewall instance.

- We have updated the API User Guide to add information regarding API details for /msp/ignore_vuln.php.
- The online help for MongoDB authentication is now updated to accurately list the type of authentications supported.