Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.10

April 29, 2021

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

Qualys Policy Compliance (PC)

New Support for Azure MS SQL Authentication

New Features in Policy Editor: Remediation and Copy Control Settings

Do Not Include Criticality option in the Compliance Policy Report Template

Unix File Content Check - Evaluate Multiline Regex Scan Data as Single line

OS Authentication-based Data Collection Support for IBM WebSphere Liberty

Support for OS Authentication-based Technology Qualys Cloud Agent

Qualys Cloud Platform

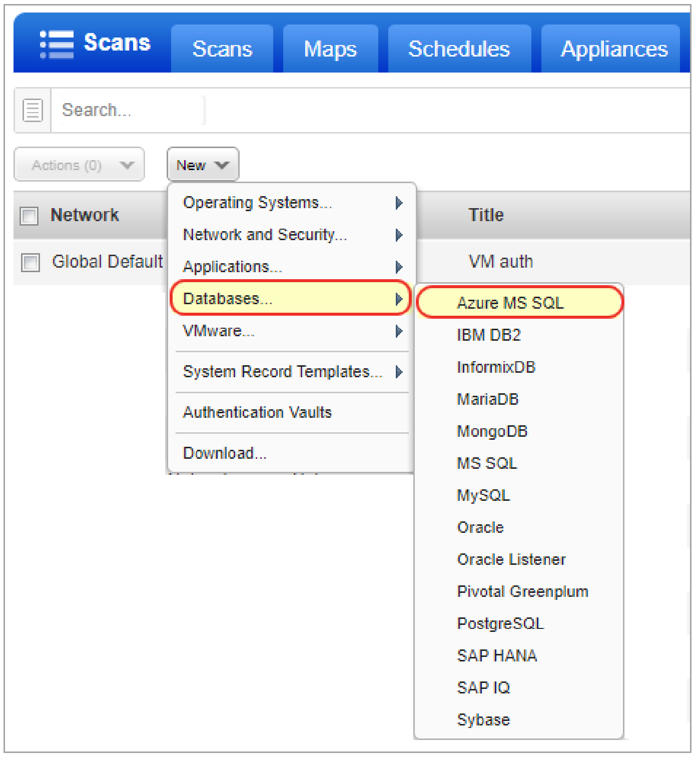
Auto adjust during Daylight Saving Time option for Schedules

Qualys 10.10 brings you more improvements and updates! Learn more

Qualys Policy Compliance (PC/SCAP/SCA)

New Support for Azure MS SQL Authentication

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

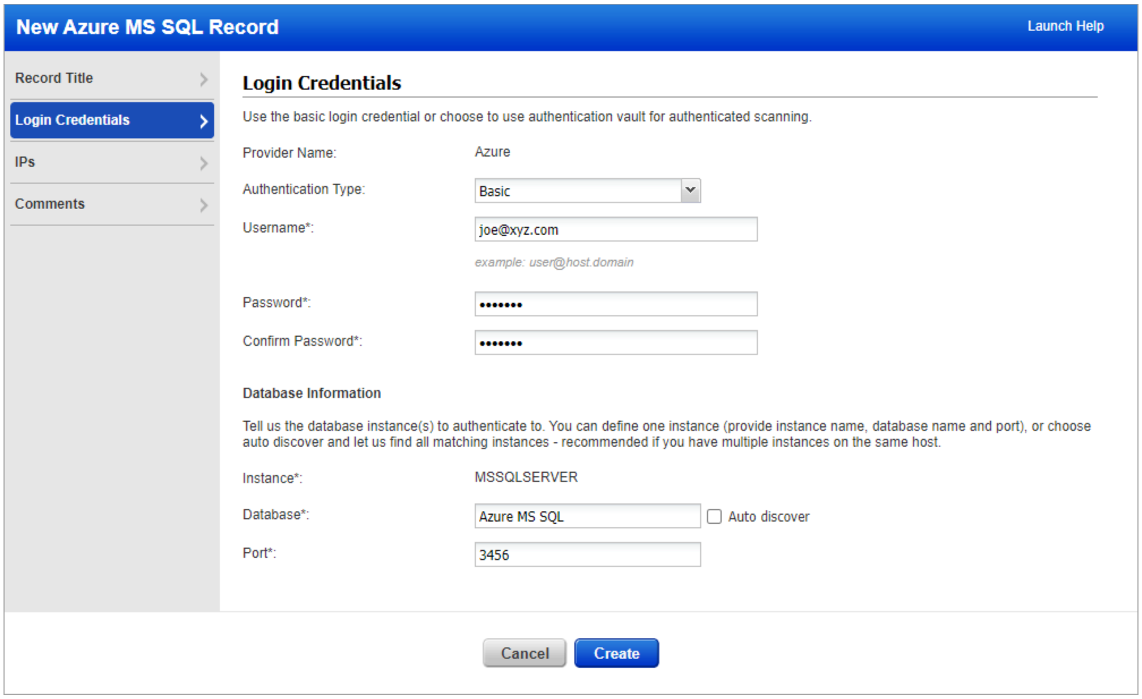


How do I get started?

Go to Scans > Authentication, and choose New > Databases > Azure MS SQL Record (as shown on the right).

Your Azure MS SQL authentication record

Each Azure MS SQL 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: Arcon PAM, Azure Key, BeyondTrust PBPS, CA Access Control, CyberArk AIM, CyberArk PIM Suite, HashiCorp, Liberman ERPM, Quest Vault, Thycotic Secret Server.



Login Credentials

Use the basic login credential or choose to use authentication vault for authenticated scanning.

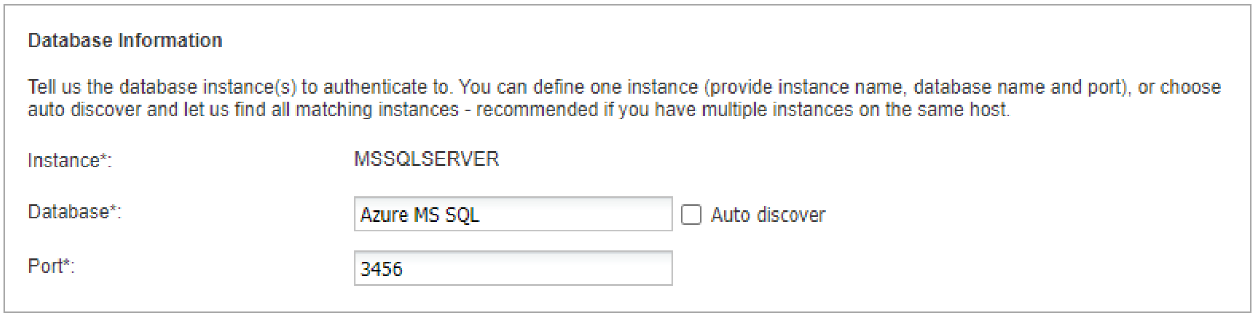
Provider Name:	Azure
Authentication Type:	Basic
Username*:	joe@xyz.com *example: user@host.domain*
Password*:	•••••••
Confirm Password*:	•••••••

Database Information

Tell us the database instance(s) to authenticate to. You can define one instance (provide instance name, database name and port), or choose auto discover and let us find all matching instances - recommended if you have multiple instances on the same host.

Instance*:	MSSQLSERVER
Database*:	Azure MS SQL ☐ Auto discover
Port*:	3456

Tell us the database name to authenticate to and the port the database is running on. You can either enter the database name or select the Auto discover option. When you select Auto discover option we'll automatically find databases on your target hosts.



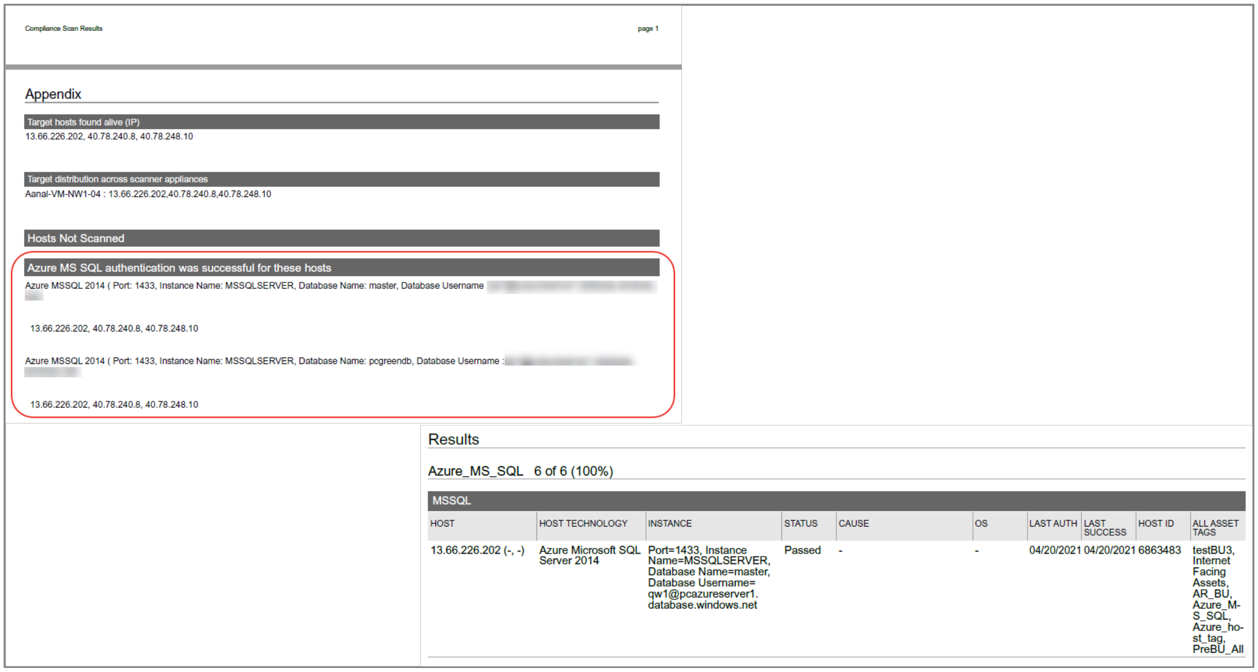
Database Information

Tell us the database instance(s) to authenticate to. You can define one instance (provide instance name, database name and port), or choose auto discover and let us find all matching instances - recommended if you have multiple instances on the same host.

Instance*:	MSSQLSERVER
Database*:	Azure MS SQL □ Auto discover
Port*:	3456

Sample Reports

You’ll see Azure Microsoft SQL Server 2014 instances in compliance scan results and reports.



Compliance Scan Results page 1

Appendix

Target hosts found alive (IP)

13.66.226.202, 40.78.240.8, 40.78.248.10

Target distribution across scanner appliances

Aanal-VM-NW1-04 : 13.66.226.202,40.78.240.8,40.78.248.10

Hosts Not Scanned

Azure MS SQL authentication was successful for these hosts

Azure MSSQL 2014 (Port: 1433, Instance Name: MSSQLSERVER, Database Name: master, Database Username [redacted]

13.66.226.202, 40.78.240.8, 40.78.248.10

Azure MSSQL 2014 (Port: 1433, Instance Name: MSSQLSERVER, Database Name: pcgreendb, Database Username : [redacted]

13.66.226.202, 40.78.240.8, 40.78.248.10

Results

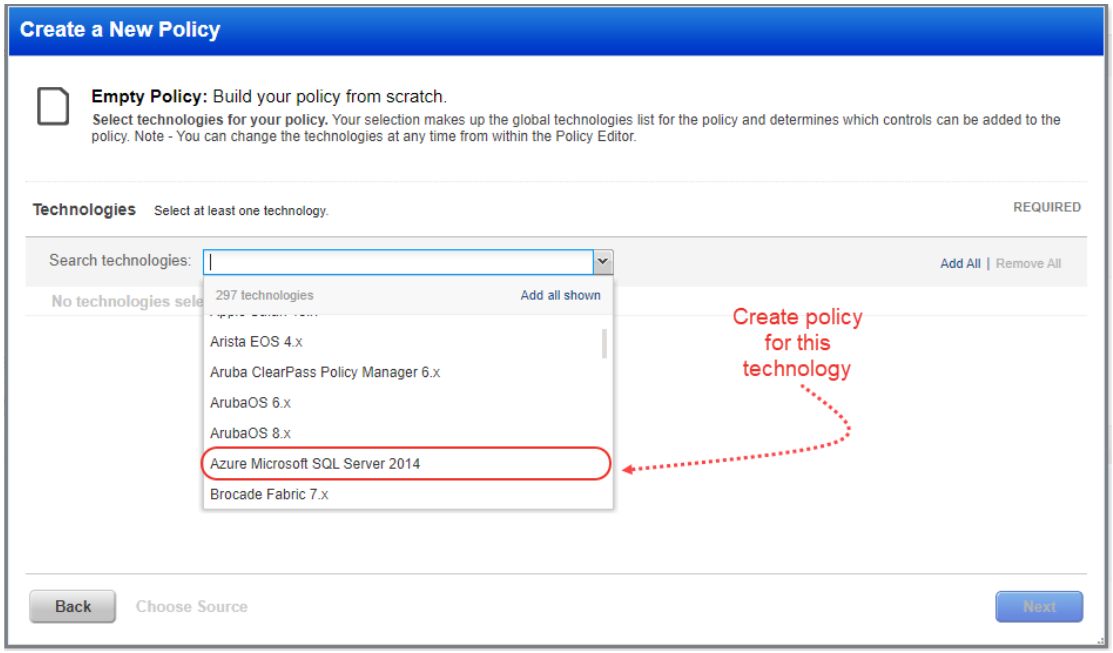
Azure_MS_SQL 6 of 6 (100%)

MSSQL

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
13.66.226.202 (-, -)	Azure Microsoft SQL Server 2014	Port=1433, Instance Name=MSSQLSERVER, Database Name=master, Database Username= qw1@pcazureserver1. database.windows.net	Passed	-	-	04/20/2021	04/20/2021	6863483	testBU3, Internet Facing Assets, AR_BU, Azure_M-S_SQL, Azure_ho-st_tag, PreBU_All

Policies and Controls

You'll see Azure Microsoft SQL Server 2014 when creating new policies and searching controls.



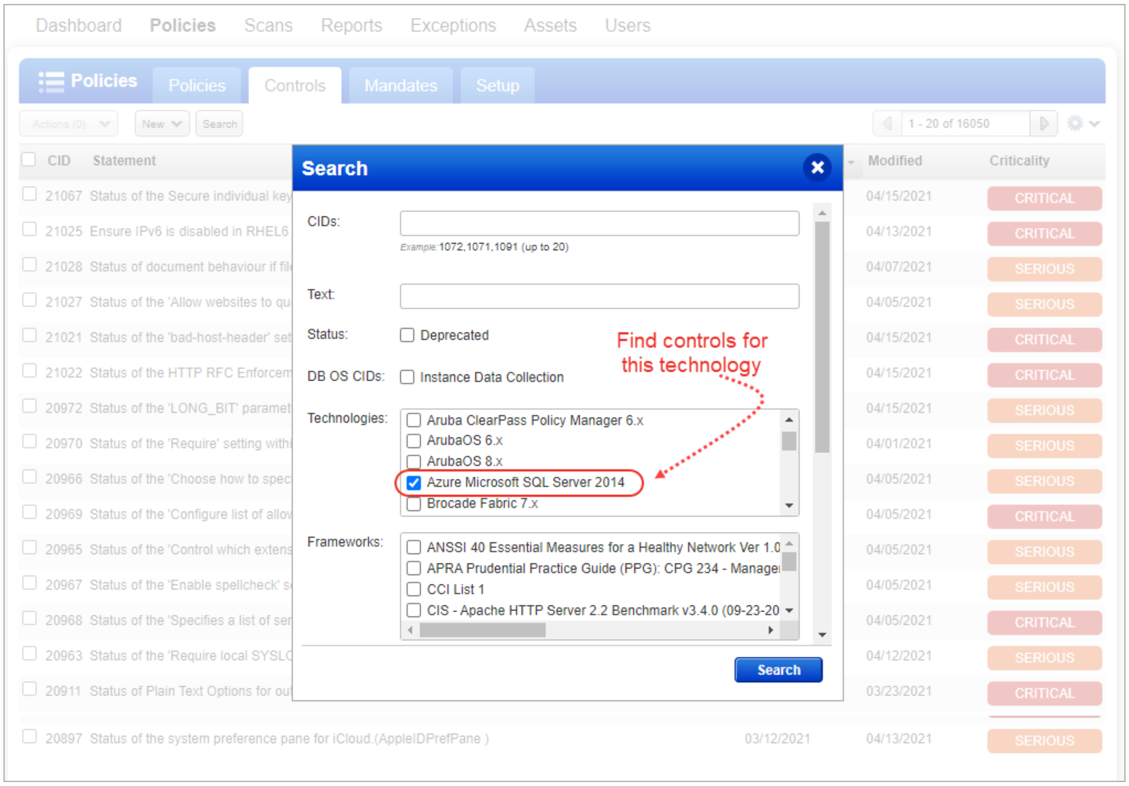
Empty Policy: Build your policy from scratch.

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.

Create policy for this technology

Search Controls

You'll see Azure Microsoft SQL Server 2014 when searching controls by technologies.



Find controls for this technology

Technologies: ☑ Azure Microsoft SQL Server 2014

CID	Statement	Modified	Criticality
21067	Status of the Secure individual key	04/15/2021	CRITICAL
21025	Ensure IPv6 is disabled in RHEL6	04/13/2021	CRITICAL
21028	Status of document behaviour if fil	04/07/2021	SERIOUS
21027	Status of the 'Allow websites to qu	04/05/2021	SERIOUS
21021	Status of the 'bad-host-header' set	04/15/2021	CRITICAL
21022	Status of the HTTP RFC Enforcem	04/15/2021	CRITICAL
20972	Status of the 'LONG_BIT' paramet	04/15/2021	SERIOUS
20970	Status of the 'Require' setting with	04/01/2021	SERIOUS
20966	Status of the 'Choose how to spec	04/05/2021	SERIOUS
20969	Status of the 'Configure list of allov	04/05/2021	CRITICAL
20965	Status of the 'Control which extens	04/05/2021	SERIOUS
20967	Status of the 'Enable spellcheck' s	04/05/2021	SERIOUS
20968	Status of the 'Specifies a list of ser	04/05/2021	CRITICAL
20963	Status of the 'Require local SYSLO	04/12/2021	SERIOUS
20911	Status of Plain Text Options for ou	03/23/2021	CRITICAL
20897	Status of the system preference pane for iCloud.(AppleIDPrefPane) 03/12/2021	04/13/2021	SERIOUS

Dashboard
Policies
Scans
Reports
Exceptions
Assets
Users
Policies
Policies
Controls
Mandates
Setup
Actions (0)
New
Search
1 - 20 of 16050
Search
CIDs:
Example:1072,1071,1091 (up to 20)
Text:
Status:
□ Deprecated
DB OS CIDs:
□ Instance Data Collection
Technologies:
□ Aruba ClearPass Policy Manager 6.x
□ ArubaOS 6.x
□ ArubaOS 8.x
☑ Azure Microsoft SQL Server 2014
□ Brocade Fabric 7.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
Search

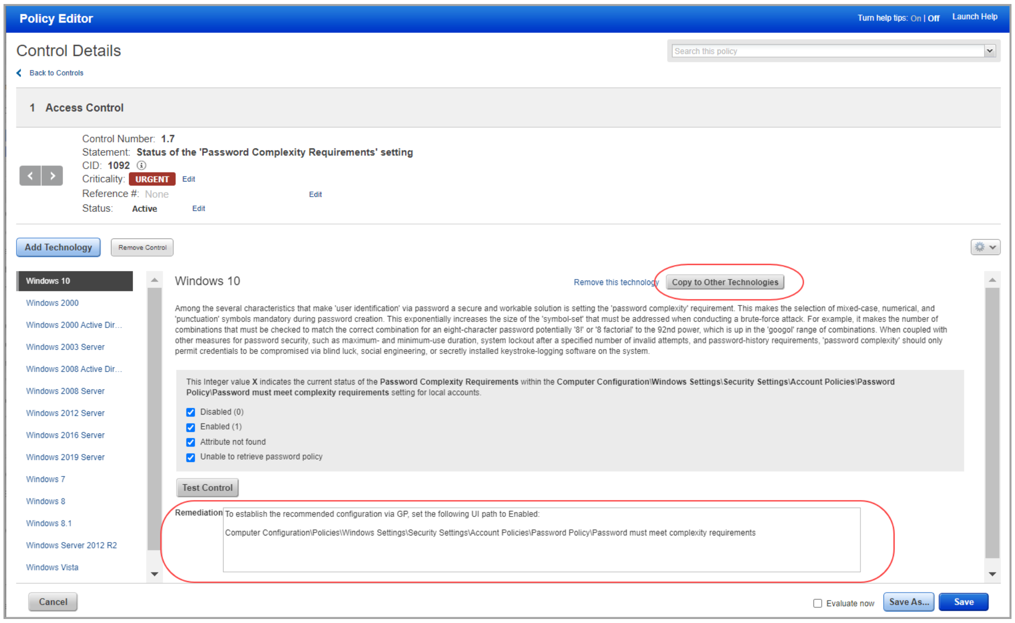
New Features in Policy Editor: Remediation and Copy Control Settings

Starting with this release, users have the ability to customize remediation information for control technologies from within the Policy Editor UI. Remediation can be defined for both Service-Defined Controls (SDCs) and User-Defined Controls (UDCs). Each technology for a control can have a different, custom remediation value. Users also now have the option to copy control settings from one technology to all the other technologies for the same control.

We'll describe these features in more detail below:

Customize Remediation Information for each Control Technology

Copy Control Settings to Other Technologies



Control Details

1 Access Control

Control Number: **1.7**
Statement: **Status of the 'Password Complexity Requirements' setting**
CID: **1092**
Criticality: **URGENT** Edit
Reference #: None Edit
Status: **Active** Edit

Windows 10

Among the several characteristics that make 'user identification' via password a secure and workable solution is setting the 'password complexity' requirement. This makes the selection of mixed-case, numerical, and 'punctuation' symbols mandatory during password creation. This exponentially increases the size of the 'symbol-set' that must be addressed when conducting a brute-force attack. For example, it makes the number of combinations that must be checked to match the correct combination for an eight-character password potentially '8!' or '8 factorial' to the 92nd power, which is up in the 'googol' range of combinations. When coupled with other measures for password security, such as maximum- and minimum-use duration, system lockout after a specified number of invalid attempts, and password-history requirements, 'password complexity' should only permit credentials to be compromised via blind luck, social engineering, or secretly installed keystroke-logging software on the system.

This Integer value **X** indicates the current status of the **Password Complexity Requirements** within the **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements** setting for local accounts.

☑ Disabled (0)
☑ Enabled (1)
☑ Attribute not found
☑ Unable to retrieve password policy

Remediation: To establish the recommended configuration via GP, set the following UI path to Enabled:

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements

Customize Remediation Information for each Control Technology

In the Policy Editor, drill-down into control details and you'll see the new **Remediation** text field as part of the control settings. Initially, this field will show remediation values defined by the service for Service-Defined Controls (SDCs) and remediation values defined by users for User-Defined Controls (UDCs). The remediation value can be changed in the policy by simply typing in the text field (up to 4000 characters). Each control technology can have a custom remediation value since the steps you take for remediation may vary by technology.

Copy Control Settings to Other Technologies

When editing control details, you can copy control settings from one technology to all other technologies for the same control, including the remediation value. Drill-down into the control details for any control in your policy and pick a technology on the left side to see the control settings for that technology. Click the **Copy to Other Technologies** button to copy the settings from the selected technology to the other technologies listed in the policy for the same control.

When settings cannot be copied

If the control criteria is different between the technology that you've selected and another technology for the control (e.g. different cardinality, operator or fixed value options), then only the remediation value will be copied. Other control settings will not be copied. You'll get a message on the screen that lets you know which technologies could not get all control settings.

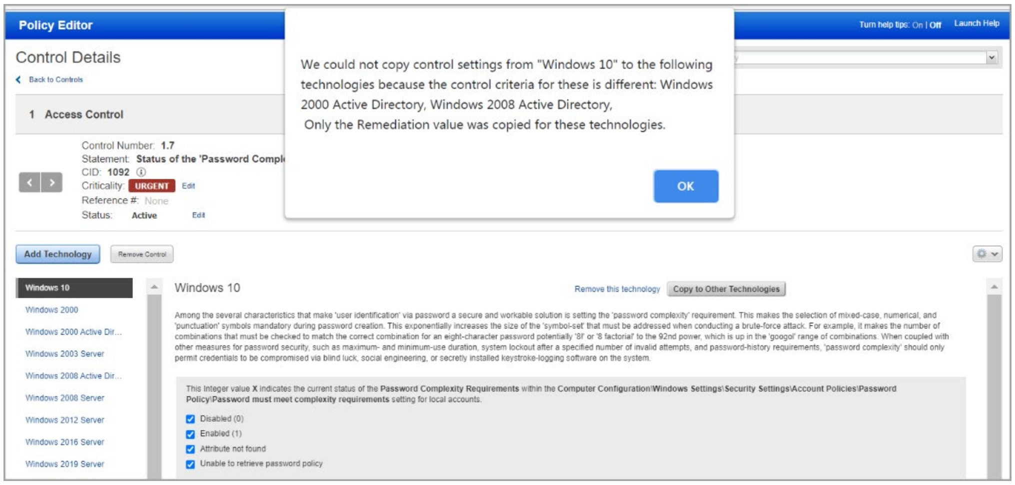
In the following example, I chose to copy control settings from Windows 10 to all other technologies for CID 1092. You'll notice that Windows 10 has these 4 check boxes selected:

- Disabled (0)
- Enabled (1)
- Attribute not found
- Unable to retrieve password policy

In this case, all control settings were copied to all other technologies, except Windows 2000 Active Directory and Windows 2008 Active Directory. Only the remediation value was copied to these technologies. The reason the other control settings were not copied is because the control criteria is different. Windows 2000 Active Directory and Windows 2008 Active Directory technologies only have 3 of the check boxes available:

- Disabled (0)
- Enabled (1)
- Attribute not found

The check box "Unable to retrieve password policy" is not listed. Since "Unable to retrieve password policy" is selected for Windows 10 but cannot be selected for the Active Directory technologies, we could not copy the settings to the Active Directory technologies. Only remediation was copied for these. When this happens, you'll see a message like the one below.



We could not copy control settings from "Windows 10" to the following technologies because the control criteria for these is different: Windows 2000 Active Directory, Windows 2008 Active Directory,
Only the Remediation value was copied for these technologies.

Control Number: 1.7
Statement: Status of the 'Password Compl
CID: 1092
Criticality: URGENT Edit
Reference #: None
Status: Active Edit

Windows 10

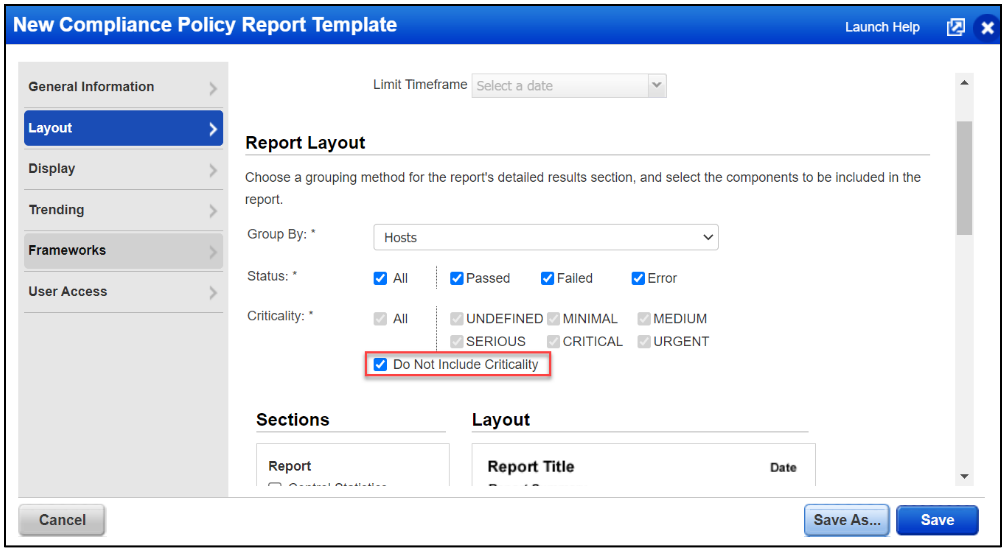
Among the several characteristics that make 'user identification' via password a secure and workable solution is setting the 'password complexity' requirement. This makes the selection of mixed-case, numerical, and 'punctuation' symbols mandatory during password creation. This exponentially increases the size of the 'symbol-set' that must be addressed when conducting a brute-force attack. For example, it makes the number of combinations that must be checked to match the correct combination for an eight-character password potentially '8!' or '8 factorial' to the 92nd power, which is up in the 'googol' range of combinations. When coupled with other measures for password security, such as maximum- and minimum-use duration, system lockout after a specified number of invalid attempts, and password-history requirements, 'password complexity' should only permit credentials to be compromised via blind luck, social engineering, or secretly installed keystroke-logging software on the system.

This integer value **X** indicates the current status of the **Password Complexity Requirements** within the **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements** setting for local accounts.

☑ Disabled (0)
☑ Enabled (1)
☑ Attribute not found
☑ Unable to retrieve password policy

Do Not Include Criticality option in the Compliance Policy Report Template

This release introduces a new option in the Policy Report Template called “Do Not Include Criticality”. When you select this option, we won’t include criticality information in the Compliance Policy Report. The Criticality column will not appear in the Control Statistics section of the report, and the 2 pie charts with the total number of passed and failed controls at each criticality level will not appear in the report.



Limit Timeframe: Select a date

Report Layout

Choose a grouping method for the report's detailed results section, and select the components to be included in the report.

Group By: * Hosts

Status: * ☑ All ☑ Passed ☑ Failed ☑ Error

Criticality: * ☑ All ☑ UNDEFINED ☑ MINIMAL ☑ MEDIUM ☑ SERIOUS ☑ CRITICAL ☑ URGENT

☑ Do Not Include Criticality

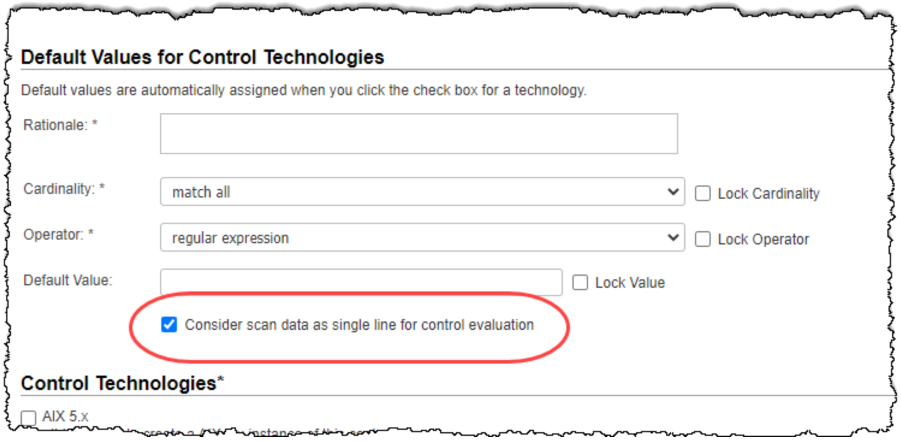
Sections — Report

Layout — Report Title, Date

Unix File Content Check - Evaluate Multiline Regex Scan Data as Single line

We have now added an option to the File Content Check UDC (Unix) so that the multiline scan data can be considered as single line for successful control evaluation.

Simply navigate to Policies > Controls and in New > Control, select File Content Check from the Unix Control Types. In the Default Values for Control Technologies section, enable the “Consider scan data as single line for control evaluation” option.



Default Values for Control Technologies

Default values are automatically assigned when you click the check box for a technology.

Rationale: *

Cardinality: * match all □ Lock Cardinality

Operator: * regular expression □ Lock Operator

Default Value: □ Lock Value

☑ Consider scan data as single line for control evaluation

Control Technologies*

□ AIX 5.x

OS Authentication-based Data Collection Support for IBM WebSphere Liberty

In the Qualys Cloud Platform 10.9 release, we added the **Instance Data Collection** tab in the compliance option profile. On this tab, you can enable data collection on the supported databases as well as OS-based applications and other technologies by using underlying OS-based authentication records.

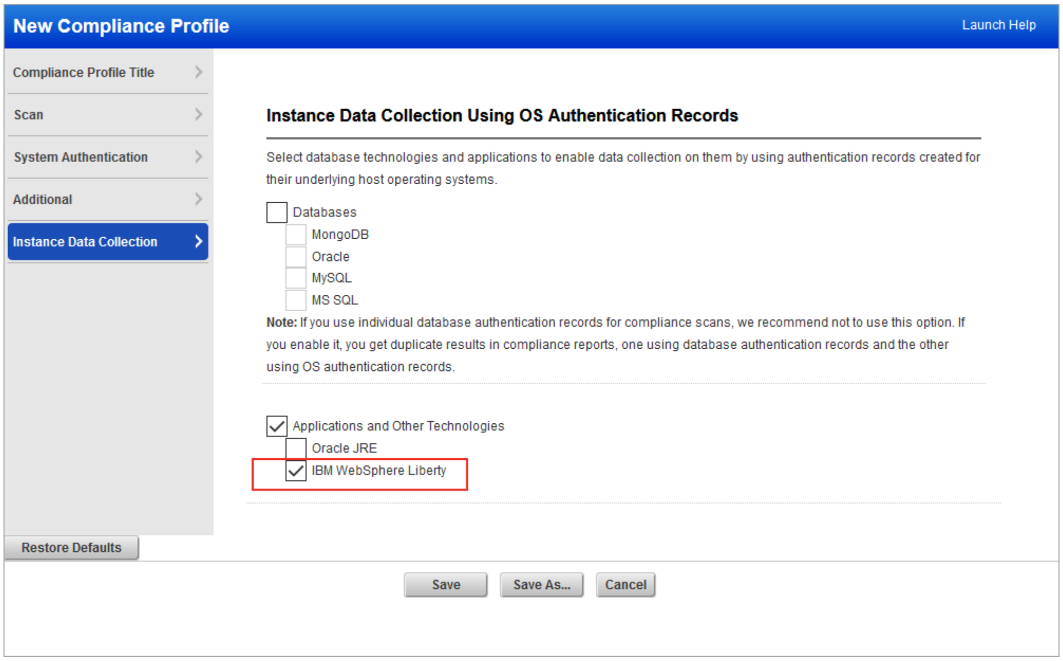
In this release, we've added the OS authentication-based data collection support for IBM WebSphere Liberty instances. You'll see the new **IBM WebSphere Liberty** check box in the **Applications and Other Technologies** section on the **Instance Data Collection** tab. To enable data collection on IBM WebSphere Liberty instances by using underlying OS authentication record, you must first select the **Applications and Other Technologies** checkbox. Only then can you select the **IBM WebSphere Liberty** checkbox.

Currently we support the following versions of IBM WebSphere Liberty:

- IBM WebSphere Liberty 19.x
- IBM WebSphere Liberty 20.x

This support is available for Liberty instances running on Linux machines. So, if you have a UNIX authentication record (with Sudo as root delegation), you don't need a separate authentication record for IBM WebSphere Liberty instances. The UNIX record is used for data collection.

You can use these settings while creating or editing an option profile.



Instance Data Collection Using OS Authentication Records

Select database technologies and applications to enable data collection on them by using authentication records created for their underlying host operating systems.

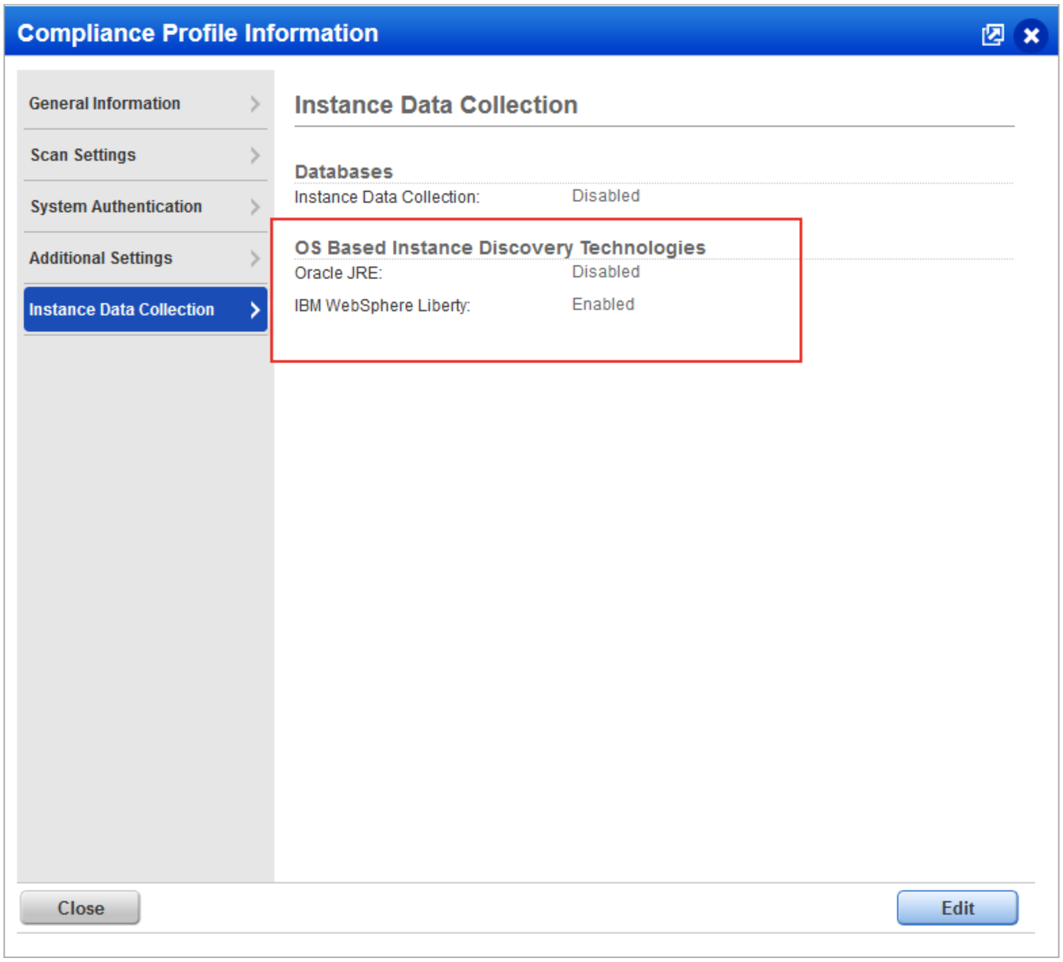
☐ Databases
☐ MongoDB
☐ Oracle
☐ MySQL
☐ MS SQL

Note: If you use individual database authentication records for compliance scans, we recommend not to use this option. If you enable it, you get duplicate results in compliance reports, one using database authentication records and the other using OS authentication records.

☑ Applications and Other Technologies
☐ Oracle JRE
☑ IBM WebSphere Liberty

If you are using Cloud Agent for Policy Compliance (PC), IBM WebSphere Liberty instances are auto-discovered by the agent. To know more, see Middleware Technologies Auto-discovered by Cloud Agents for PC.

After you save your changes, the settings in the option profile are used in the next compliance scan. You can always go back and review your compliance profile information and edit it if required.



Instance Data Collection

Databases

Instance Data Collection: Disabled

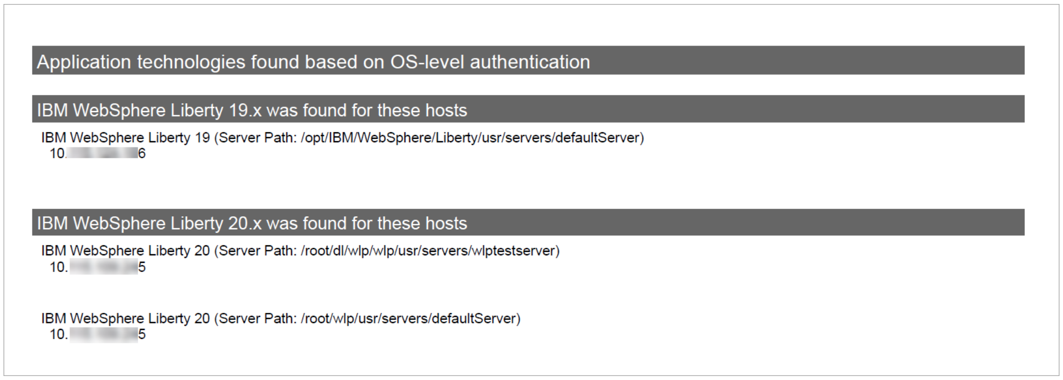
OS Based Instance Discovery Technologies

Oracle JRE: Disabled

IBM WebSphere Liberty: Enabled

Sample Compliance Scan Result

Here’s a sample compliance scan result, where, in the **Application technologies found based on OS-level authentication** section, you can see the hosts on which IBM WebSphere Liberty instances are identified.



Application technologies found based on OS-level authentication

IBM WebSphere Liberty 19.x was found for these hosts

IBM WebSphere Liberty 19 (Server Path: /opt/IBM/WebSphere/Liberty/usr/servers/defaultServer)
10.[redacted]6

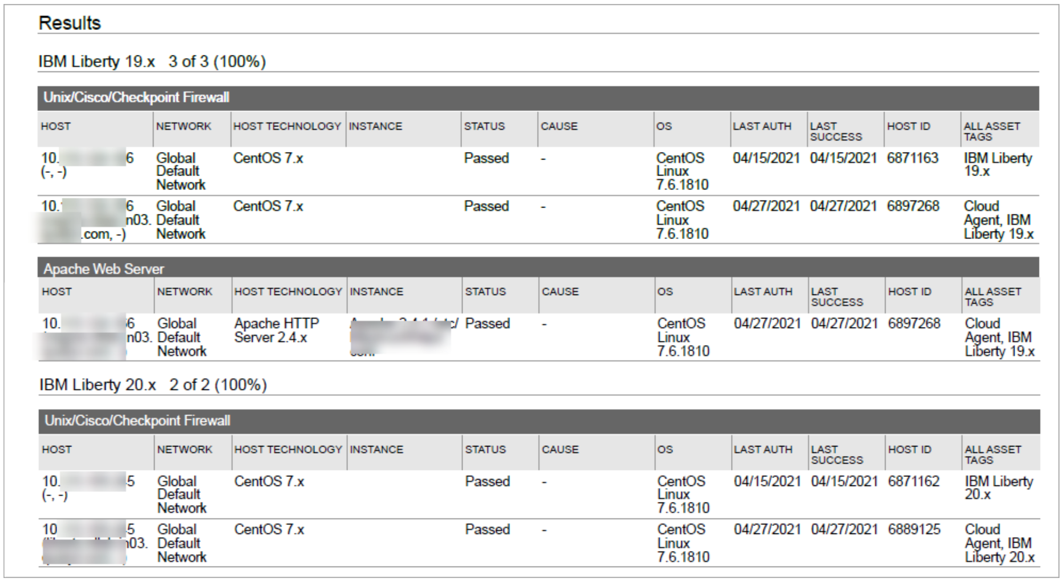
IBM WebSphere Liberty 20.x was found for these hosts

IBM WebSphere Liberty 20 (Server Path: /root/dl/wlp/wlp/usr/servers/wlptestserver)
10.[redacted]5

IBM WebSphere Liberty 20 (Server Path: /root/wlp/usr/servers/defaultServer)
10.[redacted]5

Sample Authentication Report

Here’s a sample authentication report where you can check the authentication status of the IBM WebSphere Liberty instances that are scanned by using the underlying UNIX authentication records.



Results

IBM Liberty 19.x   3 of 3 (100%)

Unix/Cisco/Checkpoint Firewall

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
10.[redacted]6 (-, -)	Global Default Network	CentOS 7.x		Passed	-	CentOS Linux 7.6.1810	04/15/2021	04/15/2021	6871163	IBM Liberty 19.x
10.[redacted]6 [redacted]n03.[redacted].com, -)	Global Default Network	CentOS 7.x		Passed	-	CentOS Linux 7.6.1810	04/27/2021	04/27/2021	6897268	Cloud Agent, IBM Liberty 19.x

Apache Web Server

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
10.[redacted]6 [redacted]n03.[redacted]	Global Default Network	Apache HTTP Server 2.4.x	[redacted]	Passed	-	CentOS Linux 7.6.1810	04/27/2021	04/27/2021	6897268	Cloud Agent, IBM Liberty 19.x

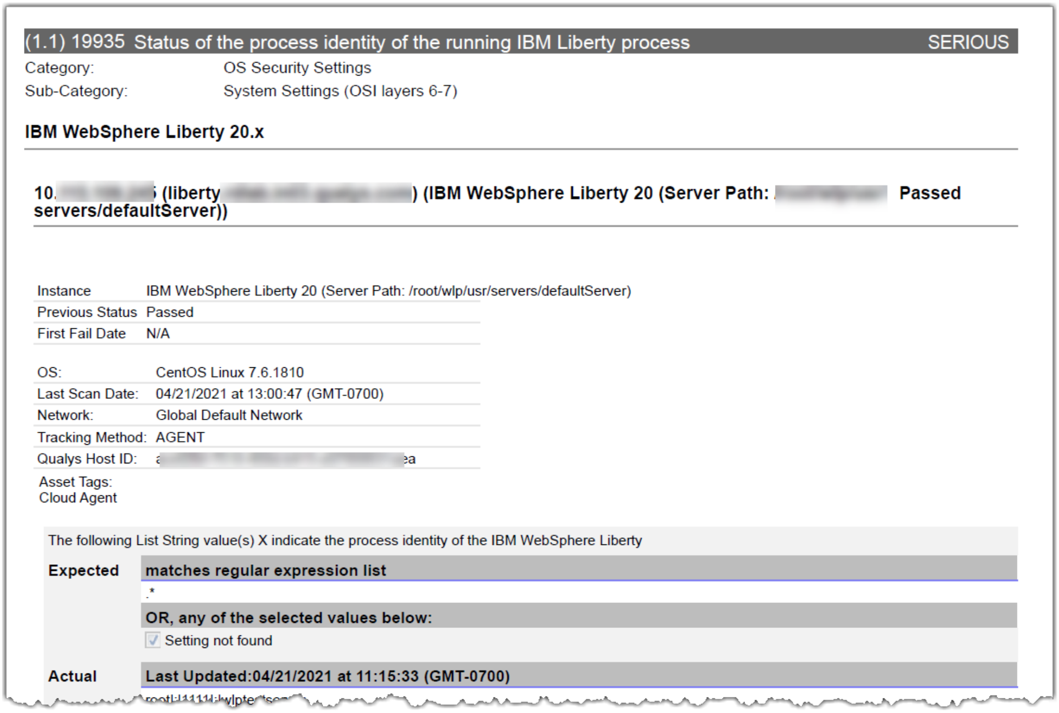
IBM Liberty 20.x   2 of 2 (100%)

Unix/Cisco/Checkpoint Firewall

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
10.[redacted]5 (-, -)	Global Default Network	CentOS 7.x		Passed	-	CentOS Linux 7.6.1810	04/15/2021	04/15/2021	6871162	IBM Liberty 20.x
10[redacted]5 [redacted]n03.[redacted]	Global Default Network	CentOS 7.x		Passed	-	CentOS Linux 7.6.1810	04/27/2021	04/27/2021	6889125	Cloud Agent, IBM Liberty 20.x

Sample Policy Report

Here’s a sample policy report where you can check the detailed results for each IBM WebShpere Liberty instance that is scanned against a policy.



(1.1) 19935 Status of the process identity of the running IBM Liberty process SERIOUS

Category: OS Security Settings

Sub-Category: System Settings (OSI layers 6-7)

IBM WebSphere Liberty 20.x

10.[redacted] (liberty[redacted]) (IBM WebSphere Liberty 20 (Server Path: [redacted] servers/defaultServer)) Passed

Instance	IBM WebSphere Liberty 20 (Server Path: /root/wlp/usr/servers/defaultServer)
Previous Status	Passed
First Fail Date	N/A
OS:	CentOS Linux 7.6.1810
Last Scan Date:	04/21/2021 at 13:00:47 (GMT-0700)
Network:	Global Default Network
Tracking Method:	AGENT
Qualys Host ID:	a[redacted]ea

Asset Tags:
Cloud Agent

The following List String value(s) X indicate the process identity of the IBM WebSphere Liberty

Expected **matches regular expression list**

.*

OR, any of the selected values below:

☑ Setting not found

Actual **Last Updated:04/21/2021 at 11:15:33 (GMT-0700)**

root|:|1111|:|wlpte

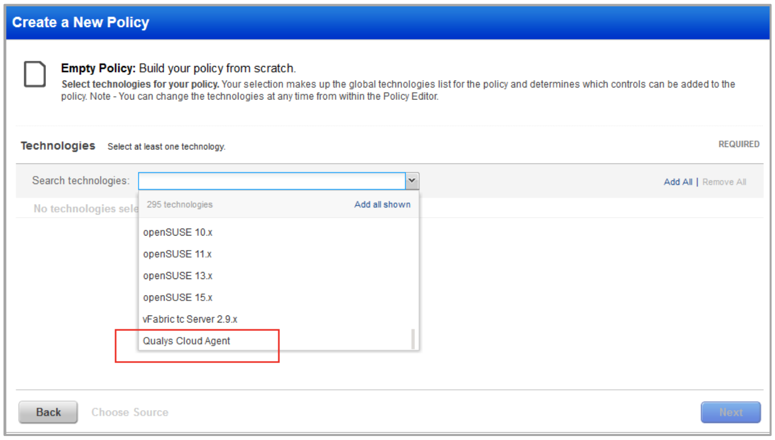
Support for OS Authentication-based Technology Qualys Cloud Agent

We've expanded our data collection and evaluation support for OS authentication-based technologies to include Qualys Cloud Agent as a new technology. For Qualys Cloud Agent, you can collect technology data and scan it for middleware compliance assessment by using the underlying OS-authentication records (Windows or Unix). You do not need to create a separate authentication record for the Qualys Cloud Agent technology.

You can now include the Qualys Cloud Agent technology in your compliance policies and when searching for controls. You'll also see the Qualys Cloud Agent host instance information in policy compliance authentication reports, scan results, and policy reports.

Qualys Cloud Agent in Policy Editor

While creating or editing a policy in Policy Editor, you can now select Qualys Cloud Agent in the **Search technologies** dropdown list.



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

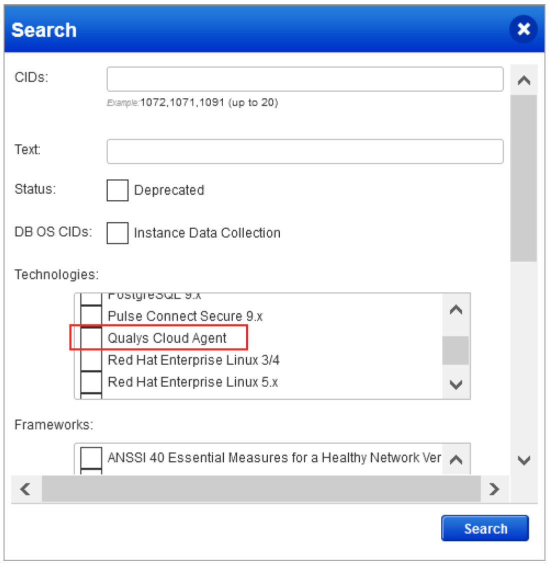
Search technologies:

No technologies sele

295 technologies

Searching Controls for Qualys Cloud Agent

You can now search for controls related to the Qualys Cloud Agent technology. Go to **Policies** > **Controls** > **Search** and select **Qualys Cloud Agent** in the **Technologies** list.



Search

CIDs:

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

Text:

Status: □ Deprecated

DB OS CIDs: □ Instance Data Collection

Technologies:

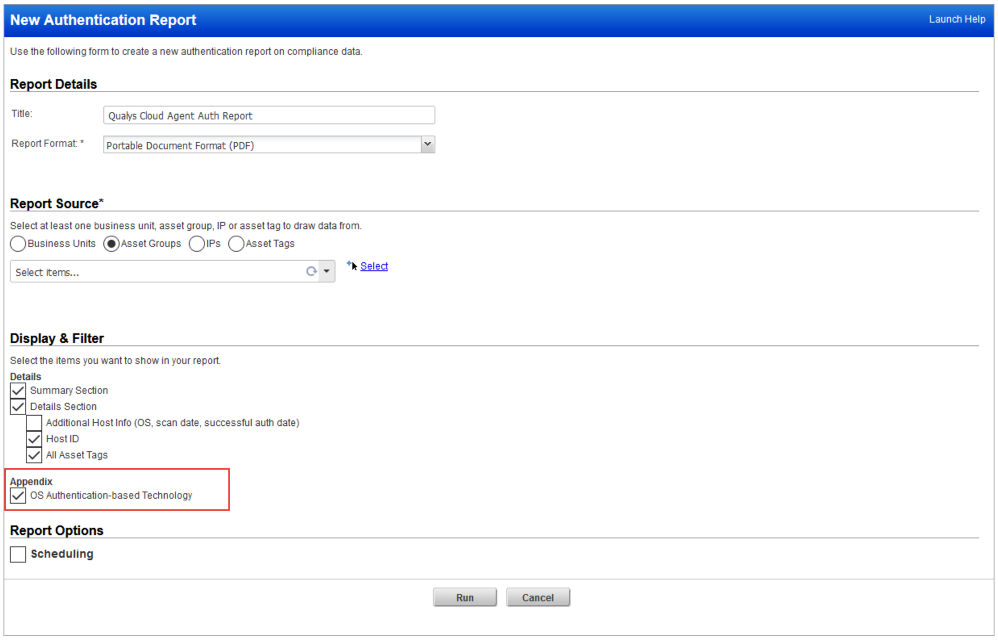
□ PostgreSQL 9.x
□ Pulse Connect Secure 9.x
□ Qualys Cloud Agent
□ Red Hat Enterprise Linux 3/4
□ Red Hat Enterprise Linux 5.x

Frameworks:

□ ANSSI 40 Essential Measures for a Healthy Network Ver

Sample Authentication Report

To display all OS auth-based instance technologies per host in your authentication report, go to **Reports** > New > Authentication Report and enable the **OS Authentication-based Technology** option in the **Appendix** section.



New Authentication Report

Use the following form to create a new authentication report on compliance data.

Report Details

Title:	Qualys Cloud Agent Auth Report
Report Format: *	Portable Document Format (PDF)

Report Source*

Select at least one business unit, asset group, IP or asset tag to draw data from.

○ Business Units ● Asset Groups ○ IPs ○ Asset Tags

Select items...

Display & Filter

Select the items you want to show in your report.

Details

☑ Summary Section

☑ Details Section

□ Additional Host Info (OS, scan date, successful auth date)

☑ Host ID

☑ All Asset Tags

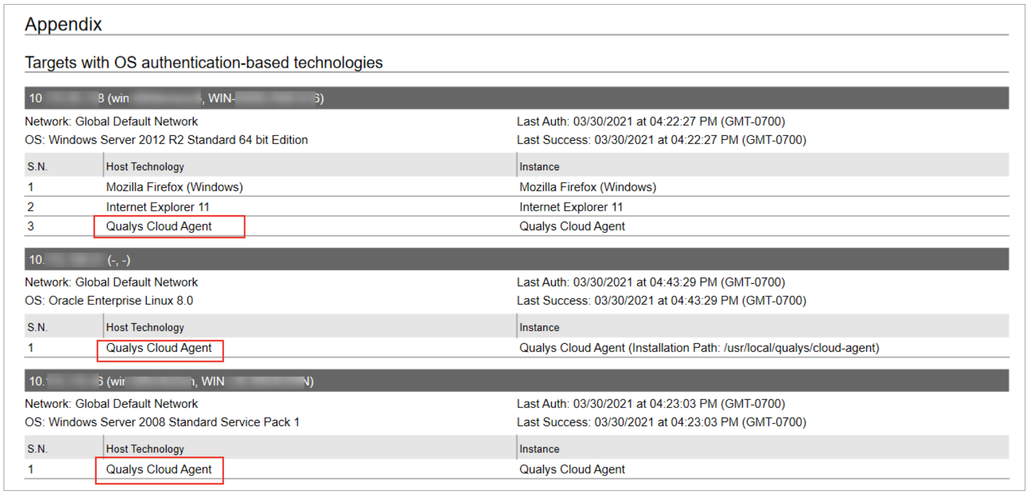
Appendix

☑ OS Authentication-based Technology

Report Options

□ **Scheduling**

Here's a sample authentication report where in the **Appendix** section, you can see the Qualys Cloud Agent instances scanned by using the underlying OS authentication records.



Appendix

Targets with OS authentication-based technologies

10 [redacted] 8 (win [redacted], WIN- [redacted] 6)

Network: Global Default Network — Last Auth: 03/30/2021 at 04:22:27 PM (GMT-0700)

OS: Windows Server 2012 R2 Standard 64 bit Edition — Last Success: 03/30/2021 at 04:22:27 PM (GMT-0700)

S.N.	Host Technology	Instance
1	Mozilla Firefox (Windows)	Mozilla Firefox (Windows)
2	Internet Explorer 11	Internet Explorer 11
3	Qualys Cloud Agent	Qualys Cloud Agent

10. [redacted] (-, -)

Network: Global Default Network — Last Auth: 03/30/2021 at 04:43:29 PM (GMT-0700)

OS: Oracle Enterprise Linux 8.0 — Last Success: 03/30/2021 at 04:43:29 PM (GMT-0700)

S.N.	Host Technology	Instance
1	Qualys Cloud Agent	Qualys Cloud Agent (Installation Path: /usr/local/qualys/cloud-agent)

10. [redacted] 6 (wi [redacted] n, WIN [redacted] N)

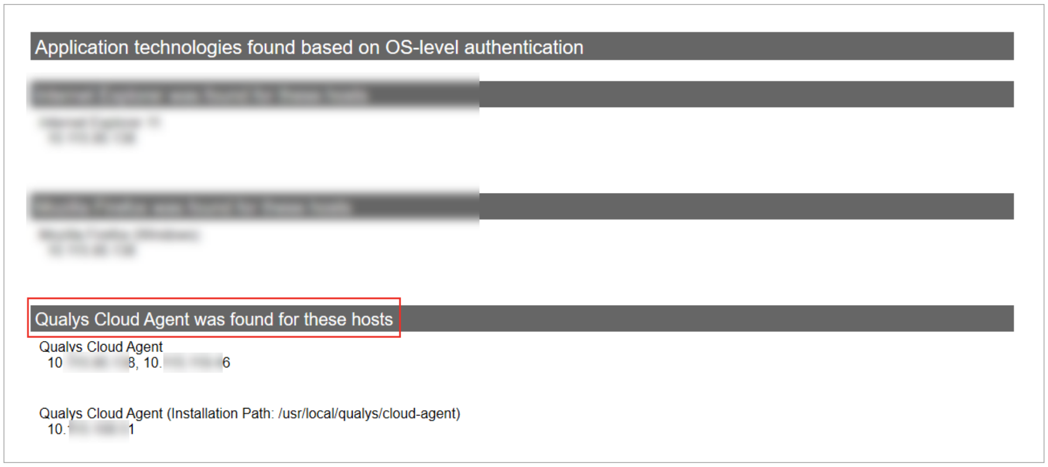
Network: Global Default Network — Last Auth: 03/30/2021 at 04:23:03 PM (GMT-0700)

OS: Windows Server 2008 Standard Service Pack 1 — Last Success: 03/30/2021 at 04:23:03 PM (GMT-0700)

S.N.	Host Technology	Instance
1	Qualys Cloud Agent	Qualys Cloud Agent

Sample Compliance Scan Result

Here’s a sample compliance scan result, where, in the **Application technologies found based on OS-level authentication** section, you can see the hosts on which Qualys Cloud Agent instances are identified.



Application technologies found based on OS-level authentication

[redacted]

[redacted]

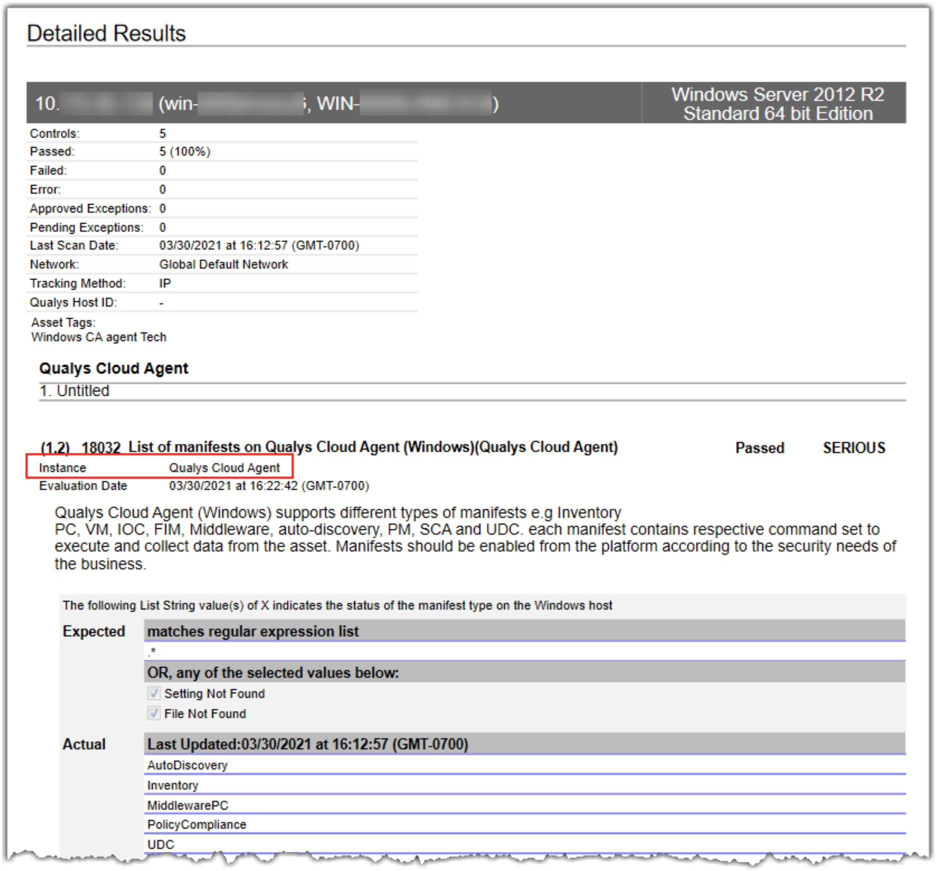
Qualys Cloud Agent was found for these hosts

Qualys Cloud Agent
10[redacted]8, 10.[redacted]6

Qualys Cloud Agent (Installation Path: /usr/local/qualys/cloud-agent)
10.[redacted]1

Sample Policy Report

And here’s a sample policy report where you can check the detailed results for each Qualys Cloud Agent instance that is scanned against a policy.



Detailed Results

10.[redacted] (win-[redacted], WIN-[redacted]) | Windows Server 2012 R2 Standard 64 bit Edition

Controls:	5
Passed:	5 (100%)
Failed:	0
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	03/30/2021 at 16:12:57 (GMT-0700)
Network:	Global Default Network
Tracking Method:	IP
Qualys Host ID:	-

Asset Tags:
Windows CA agent Tech

Qualys Cloud Agent

1. Untitled

(1.2) 18032 List of manifests on Qualys Cloud Agent (Windows)(Qualys Cloud Agent) **Passed** **SERIOUS**

Instance	Qualys Cloud Agent
Evaluation Date	03/30/2021 at 16:22:42 (GMT-0700)

Qualys Cloud Agent (Windows) supports different types of manifests e.g Inventory PC, VM, IOC, FIM, Middleware, auto-discovery, PM, SCA and UDC. each manifest contains respective command set to execute and collect data from the asset. Manifests should be enabled from the platform according to the security needs of the business.

The following List String value(s) of X indicates the status of the manifest type on the Windows host

Expected **matches regular expression list**

.*

OR, any of the selected values below:

☑ Setting Not Found
☑ File Not Found

Actual **Last Updated:03/30/2021 at 16:12:57 (GMT-0700)**

AutoDiscovery
Inventory
MiddlewarePC
PolicyCompliance
UDC

Qualys Cloud Platform

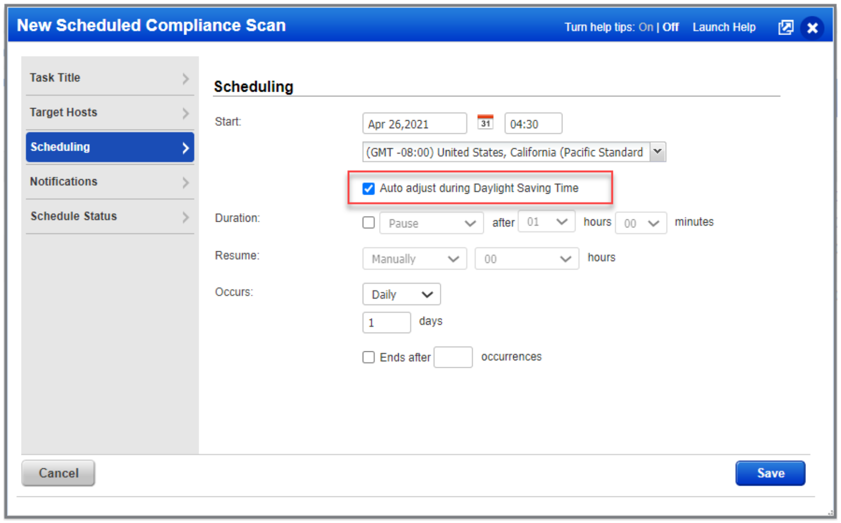
Auto adjust during Daylight Saving Time option for Schedules

You'll notice when scheduling scans and reports that we changed the "DST" option to "Auto adjust during Daylight Saving Time". We made this UI change to help users more clearly understand what to expect when using this option.

When the "Auto adjust during Daylight Saving Time" option is selected, the start time for your scheduled scan/report will be adjusted automatically during time changes so you don't have to make any edits to your schedule at these times. For example, let's say you pick the time zone "(GMT -08:00) United States, California (Pacific Standard Time)", which observes DST. When Daylight Saving Time starts in the Spring, the start time for your schedule will move forward an hour. When Daylight Saving Time ends in the Fall, the start time will be adjusted back an hour.

Note that this new option is selected by default when DST is observed for the selected time zone, and is disabled for locations that never observe DST like Arizona and Hawaii.

Sample – Scheduling Settings for Scan



New Scheduled Compliance Scan

Scheduling

Start: Apr 26,2021 | 04:30

(GMT -08:00) United States, California (Pacific Standard

☑ Auto adjust during Daylight Saving Time

Duration: □ Pause after 01 hours 00 minutes

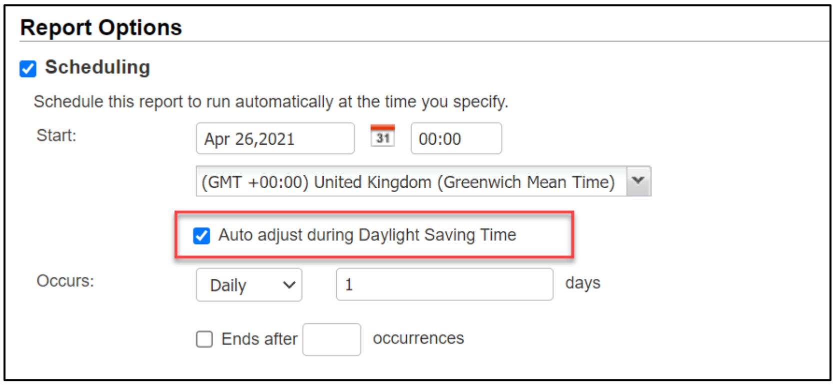
Resume: Manually 00 hours

Occurs: Daily

1 days

□ Ends after occurrences

Sample – Scheduling Settings for Report



Report Options

☑ **Scheduling**

Schedule this report to run automatically at the time you specify.

Start: Apr 26,2021 | 00:00

(GMT +00:00) United Kingdom (Greenwich Mean Time)

☑ Auto adjust during Daylight Saving Time

Occurs: Daily 1 days

□ Ends after occurrences

Issues Addressed

- We fixed a performance issue where in some cases the Scans > Schedules tab in the UI was slow to load. Now it will load faster.
- We made performance improvements to the Policy Editor page.
- We fixed an issue in the PCI Scan Report Template where the user was not able to save a search list in the template using the Search List Exception workflow on the PCI Risk Ranking tab.
- The Cause of Failure feature in the Policy Report Template was not working in some cases. Now, after this fix, we'll show correct values in the Unexpected Values section of the report.