Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.1

May 14, 2020 (Updated May 22, 2020)

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

Qualys Vulnerability Management (VM)

Display Host Groups Associated with Hosts in Host Based Scan Report

Qualys Policy Compliance (PC)

Oracle Instance Discovery and System Record Creation
Improvements to the Remote Security Hygiene Dashboard
Increased Character Limits for Policy Cover Page and Control Reference
PC Authentication Report - Changed Cause Text for Not Attempted Status
PC/SCA reports can now be generated on assets without OS information
Support for New OCA Technologies
Sybase Database User-Defined Control Support
User-Defined Control Support for Mac OS X 10.14 and Mac OS X 10.15
Hiding Scan Parameters in a Report
Remediation Information Available in Import or Export of UDCs

Qualys Cloud Platform

New Regions Supported for EC2 Scans
Azure Key Vault now Supported in Palo Alto Networks Firewall Record
Support for ARCON PAM (Privilege Access Management) Vaults
Microsoft Windows 2019 Active Directory Support
Report Changes to Show Instance IDs in Scan Results/Scan Status

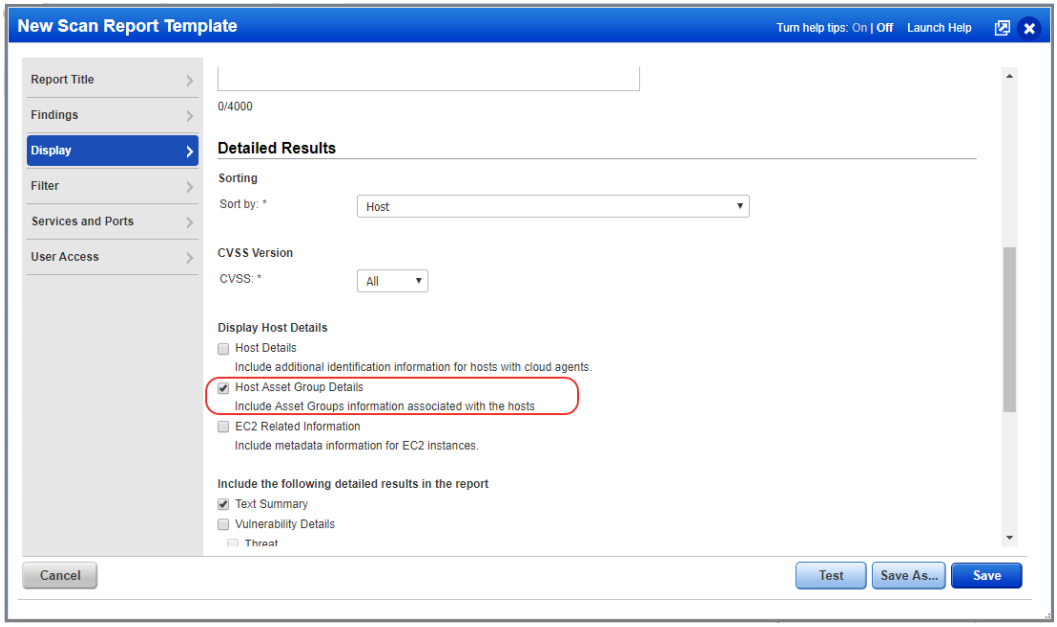
Qualys 10.1 brings you more improvements and updates! Learn more

Qualys Vulnerability Management (VM)

Display Host Groups Associated with Hosts in Host Based Scan Report

You can now see the list of asset groups associated with each host in host-based scan reports. To display the associated asset groups for the hosts in the scan report, go to Reports > Templates > New > Scan Template or PCI Template. Go to the Display tab and select the “Host Asset Group Details” check box in the New Scan Report Template screen. Optionally, edit an existing report template to select this new option.

Note - This option is only available for templates configured for Host Based Findings (on the Findings tab in the template).



Qualys Policy Compliance (PC)

Oracle Instance Discovery and System Record Creation

This release introduces instance discovery and auto record creation for Oracle authentication. This functionality is already available for other technologies like Apache Web Server, IBM WebSphere, JBoss and Tomcat. There are a few notable differences for Oracle though. When we auto discover Oracle instances, we'll discover the target configuration for each instance but not the login credentials. We've introduced a new configuration called "Oracle System Record Template" that you'll use to provide Oracle login credentials for system created records. You'll create the system record template and then select it in the option profile used for discovery scans. The template is linked automatically to the system created records created as a result of the scan.

Benefits

- We'll auto discover Oracle instances on each scanned host and create authentication records for those instances. We support auto discovery and system record creation for Oracle instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running Oracle.

- When we create Oracle authentication records for discovered instances, we'll insert the credentials from the Oracle system record template you selected in the option profile.

- You can easily rotate Oracle passwords. Simply edit the credentials in the Oracle system record template and all Oracle records linked to the template will be updated to use the new credentials with no additional scan or action by you.

- You can edit individual Oracle system created records and save them as user created. This allows you to change the credentials for individual records without changing the credentials for all records associated with a template.

How it works

Here's the basic flow for Oracle instance discovery and auto record creation.

1) Create an Oracle system record template and enter the login credentials you want to use for system created records.

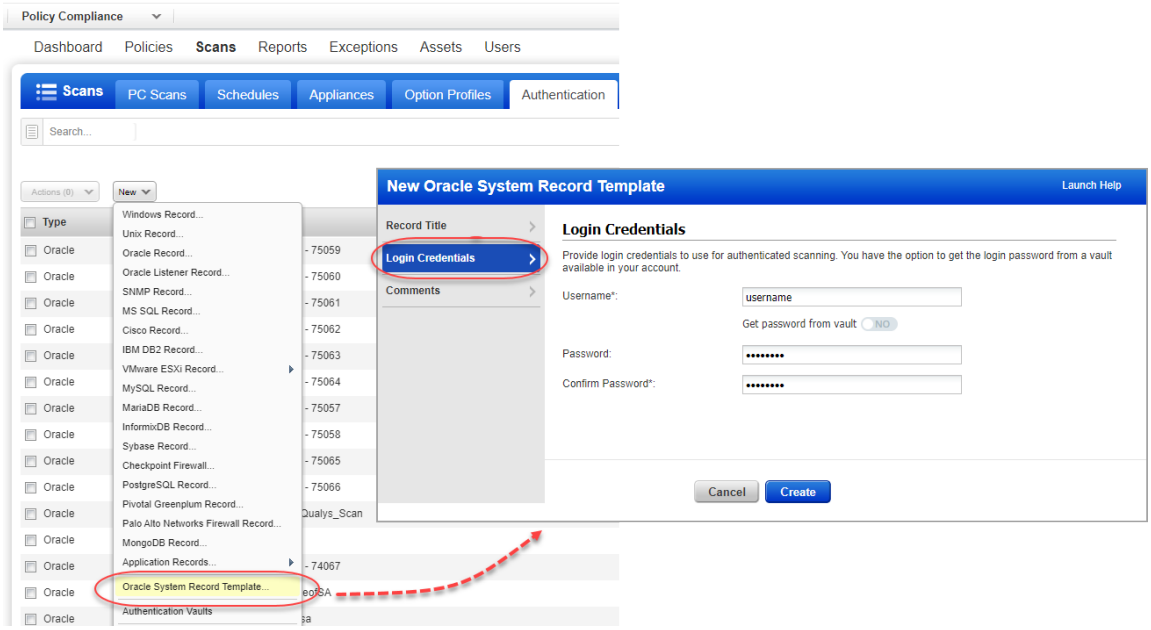
2) Select the Oracle system record template in the compliance option profile you want to use for discovery scans.

3) Launch your discovery scan. Your scan results will list the auto discovered instances.

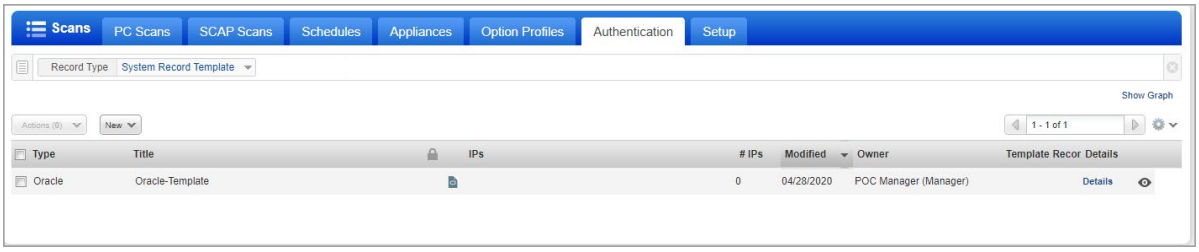
4) In the authentication list you'll see newly created Oracle records. For each system created record, you'll see the template associated with the record.

Create Oracle System Record Template

Go to Scans > Authentication > New > Oracle System Record Templates. On the Login Credentials tab, enter the username and password (or choose a password vault). These credentials will be used for all system created records that are associated with this template. Once saved, your Oracle system record template will appear on the Authentication records list with other records.

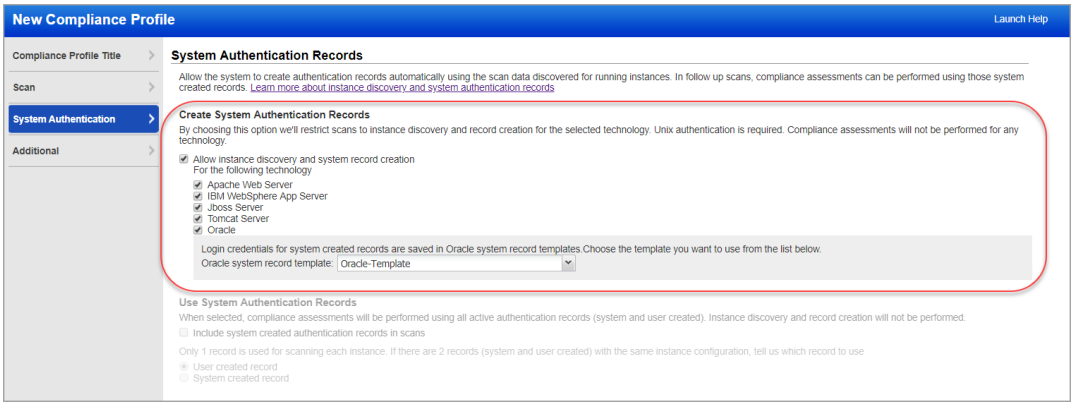


Oracle record templates are identified with in the authentication records list. You can also search for Oracle record templates by choosing Record Type: System Record Template.

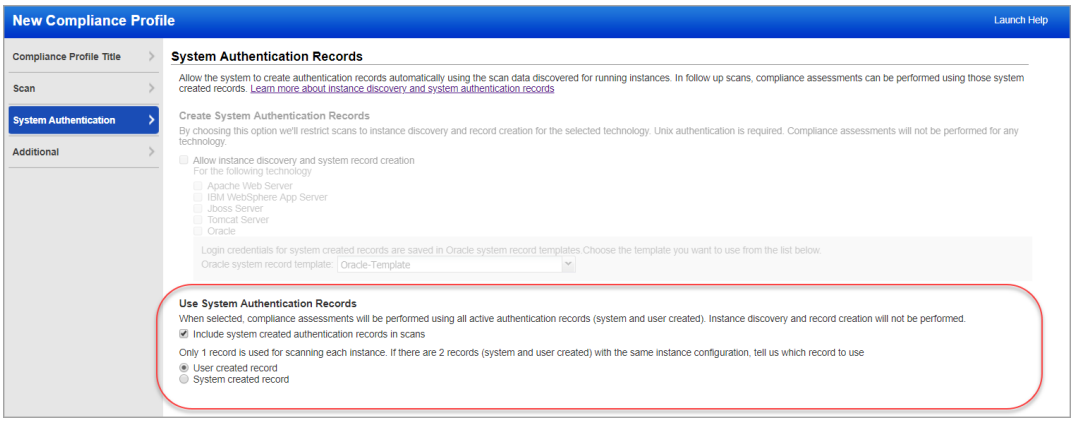


Select template in Compliance Profile

You'll select the template in a compliance profile. Under System Authentication, choose the option "Allow instance discovery and system record creation" and select the Oracle technology. Then choose one of your saved Oracle system record templates. Note - The Oracle option is disabled if you have not saved any templates. You must create templates *before* you can enable this option in the profile.

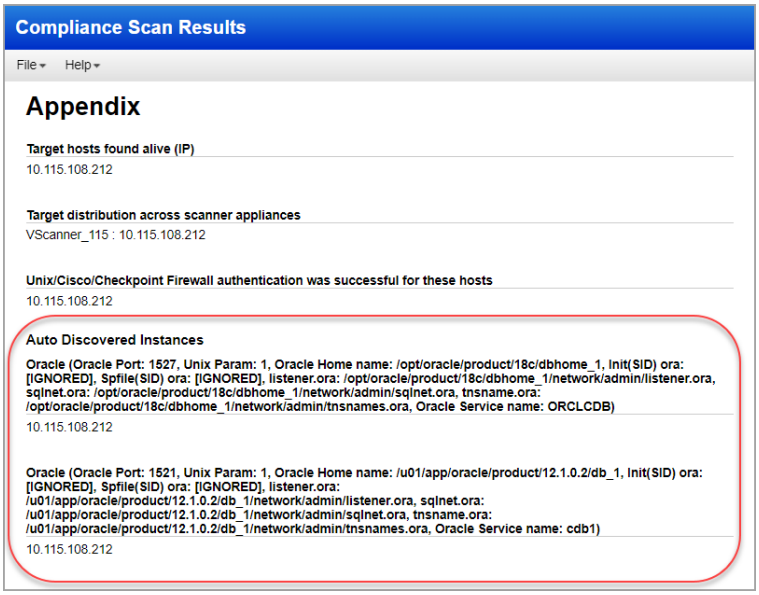


You'll need to create a separate compliance profile in order to use newly created Oracle system authentication records for compliance assessments. Under System Authentication, choose the option "Include system created authentication records in scans". System created records will be used along with user created records. If you have a user created record and a system created record for the same instance configuration we'll use the user record by default. You can change this if you prefer to use the system record.



Launch discovery scan for auto record creation

Launch a compliance scan and choose an option profile with the "Allow instance discovery and system record creation" option enabled. We recommend you schedule instance discovery scans to occur when you expect changes in your infrastructure.

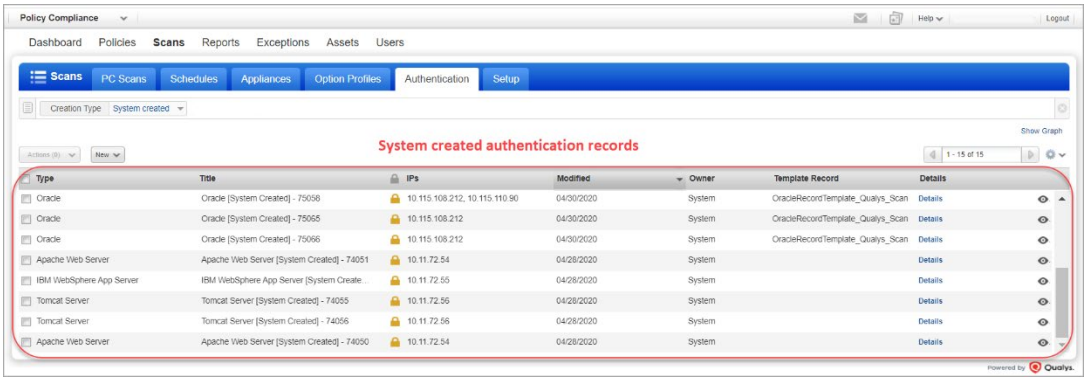


Looking for auto discovered instances? Scroll down to the Appendix section of your compliance scan results and you'll see a list of Auto Discovered Instances. For each instance you'll see the values collected about your Oracle installation on the Unix system.

Auto record creation process

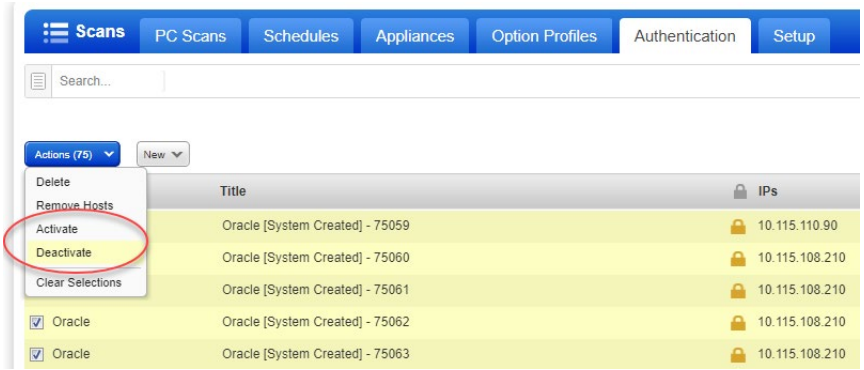
Instance scan data consolidation occurs based on authenticated scan data from the scan. Authentication records are created based on consolidated scan data. Record creation starts when the scan is Finished, during scan processing. Records may be created or updated (new IPs added, existing IPs removed).

System created authentication records are identified by a gold lock ( ) for system records and Owner “System”. For system created Oracle records you'll also see the template record name. This is the template that contains the login credentials for the Oracle instance.



Make Oracle records Active/Inactive

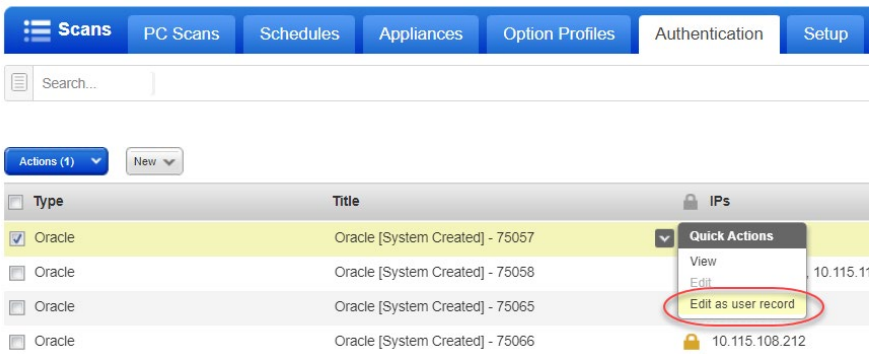
You can now change the status of system created and user created Oracle records. Inactive records are not included in scans (even if the "Include system created authentication records in scans" option is selected in the option profile).



Choose the records you want to make Inactive and pick Deactivate from the Actions menu. To activate records choose Activate. (Note that you cannot change the status of Oracle system record templates.)

Save system created Oracle records as user created

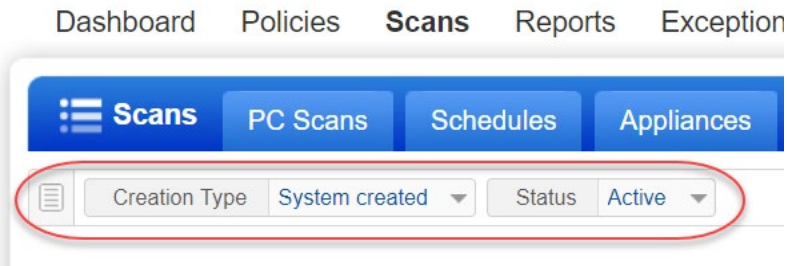
Edit individual Oracle system created records and save them as user created. This allows you to change the credentials for individual records without changing the credentials for all records associated with a template.



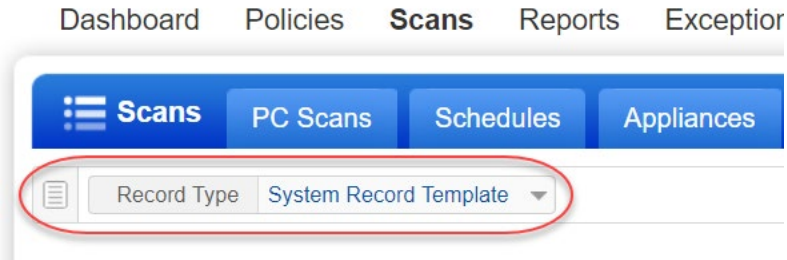
Select the option “Edit as user record” from the Quick Actions menu. Note that this option is only available for system created Oracle records.

Search Oracle records

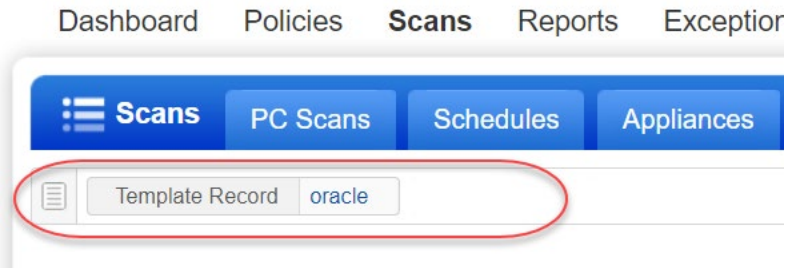
You can search records by creation type (System created or User created) and by status (Active or Inactive).



You can search for all Oracle record templates by choosing Record Type: System Record Template.



You can find all system created records that are associated with a particular Oracle record template by choosing Template Record and entering all or part of the template name.



Improvements to the Remote Security Hygiene Dashboard

We recently introduced the Remote Security Hygiene Dashboard and Library Policies. With this release we've made several improvements to the dashboard. Improvements include:

- The Trend of Security Hygiene graph now includes Pass, Fail and Error posture levels (only Fail was included previously). This graph also now includes posture data for the current day.

- Click the Info icon (ⓘ) for any asset to view Host Information for the asset.

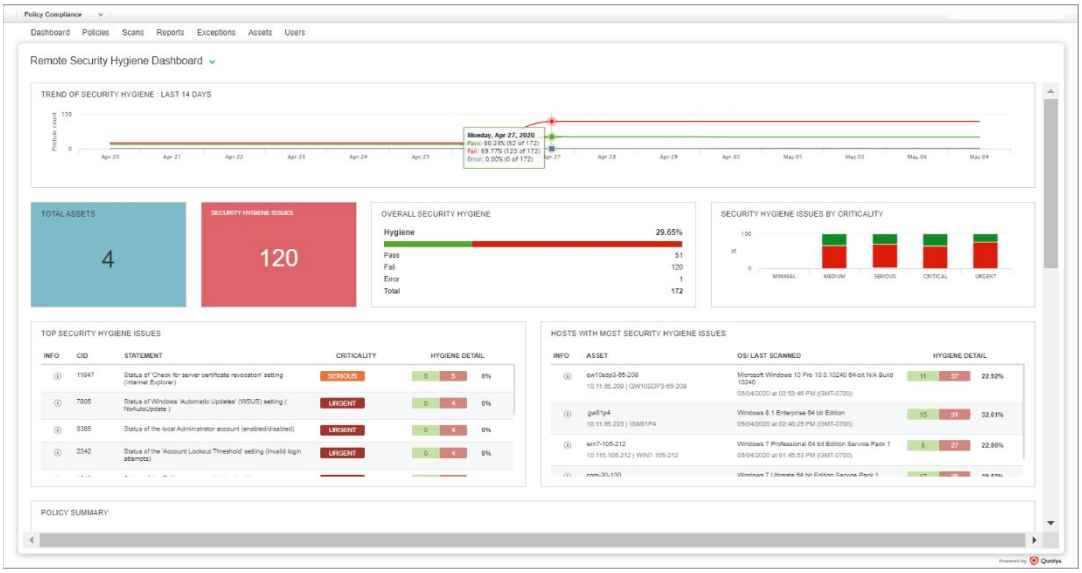
- Click the Info icon (ⓘ) for any control to view Control Information for the control.

- Click on any control ID (CID) or control statement to navigate to the Reports > Control View tab to view posture information for the control (available in accounts with PC and PC+SCA).

- Click on any asset name or IP address to navigate to the Reports > Control View tab to view posture information for the asset (available in accounts with PC and PC+SCA).

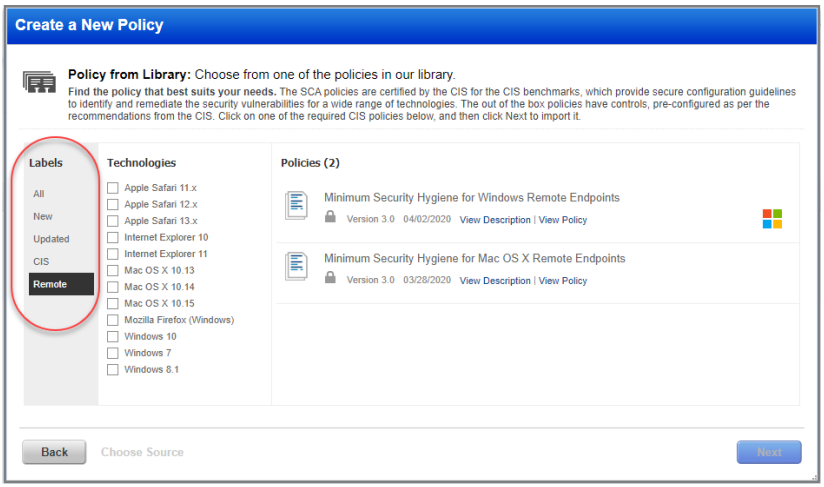
Remote Security Hygiene Dashboard

In PC or SCA, go to Dashboard and pick the "Remote Security Hygiene Dashboard".



Update to Import Policy for SCA accounts

Now accounts with SCA (and without PC) will see Labels in the Import Policy workflow, allowing these customers to filter policies by label. Go to Policies > New > Import Policy, then select the label that matches the type of policy you're interested in, such as CIS or Remote. Note that Labels are already visible to accounts with PC.

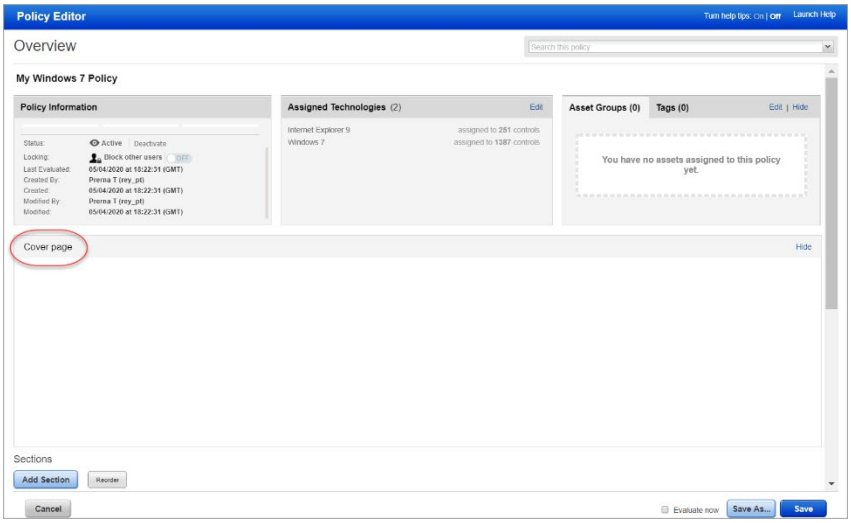


Increased Character Limits for Policy Cover Page and Control Reference

You can now enter up to 10,000 characters for the cover page of a policy and up to 1,024 characters when adding a control reference.

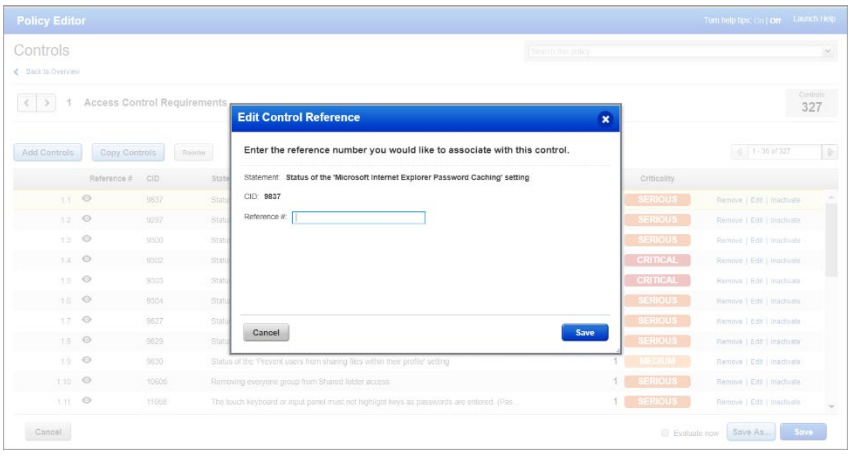
Cover Page

In the Policy Editor, click the Cover Page link to expand the section where you can add cover page content. Enter up to 10,000 characters.



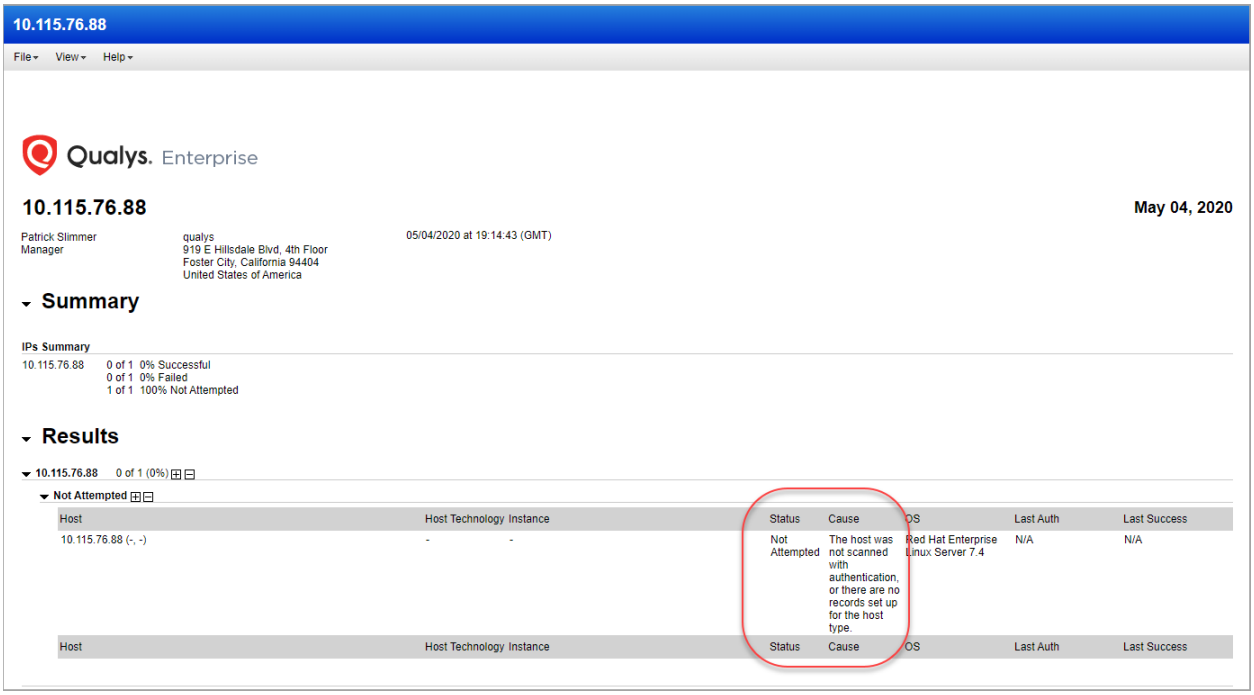
Control Reference

In the Policy Editor, you can add a reference to any control by either clicking the Add Ref # link from the list of controls or clicking Edit next to Reference # in the Control Details. The text you enter will appear in your policy reports under Control References. Enter up to 1,024 characters.



PC Authentication Report - Changed Cause Text for Not Attempted Status

In the PC authentication report when the authentication status is Not Attempted the Cause column always showed “There are no records set up for the host type.” even in cases when there were records set up. We fixed the Cause text to include the case where records are set up but authentication on the host was skipped or the host was simply not scanned with authentication. Now the Cause column shows “The host was not scanned with authentication, or there are no records set up for the host type.” This is the same text that appears in the VM authentication report for status Not Attempted.



PC/SCA reports can now be generated on assets without OS information

We made a fix in compliance reports and authentication reports so that you can now report on assets with instance based technologies that don’t have OS information, such as Relational Database Service (RDS) technologies.

Previously, customers were able to scan and process scan results for such assets but they could not report on them. This is because the reports expected an OS value for each asset and these assets did not have OS information. Now, when OS information is not present for an asset, the OS will appear as a dash (-) allowing these assets to be included in your reports.

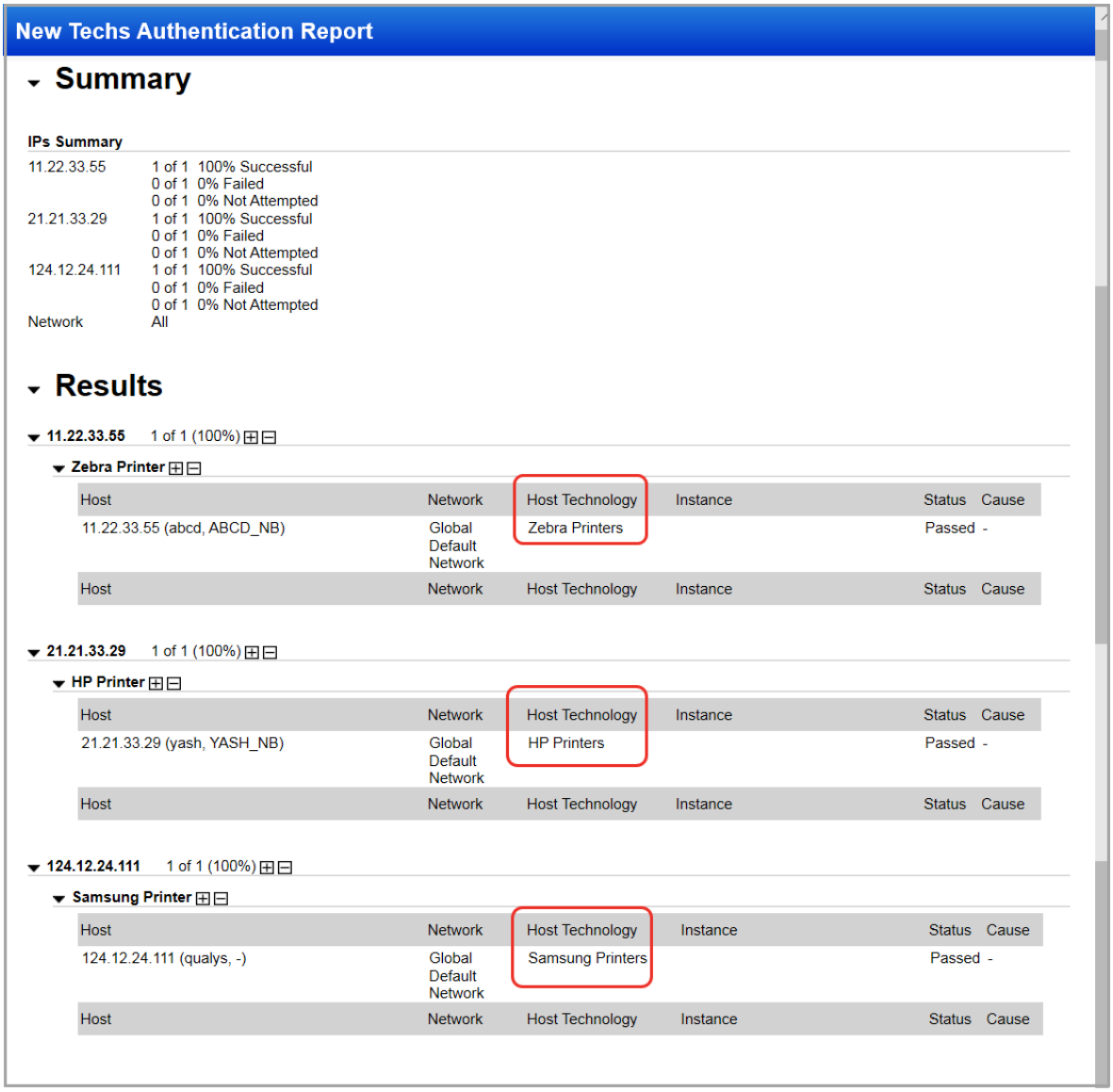
Support for New OCA Technologies

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

- HP Printers
- Samsung Printers
- Zebra Printers

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

Sample: Authentication Report



New Techs Authentication Report

Summary

IPs Summary

11.22.33.55	1 of 1 100% Successful 0 of 1 0% Failed 0 of 1 0% Not Attempted
21.21.33.29	1 of 1 100% Successful 0 of 1 0% Failed 0 of 1 0% Not Attempted
124.12.24.111	1 of 1 100% Successful 0 of 1 0% Failed 0 of 1 0% Not Attempted
Network	All

Results

11.22.33.55 1 of 1 (100%)

Zebra Printer

Host	Network	Host Technology	Instance	Status	Cause
11.22.33.55 (abcd, ABCD_NB)	Global Default Network	Zebra Printers		Passed	-
Host	Network	Host Technology	Instance	Status	Cause

21.21.33.29 1 of 1 (100%)

HP Printer

Host	Network	Host Technology	Instance	Status	Cause
21.21.33.29 (yash, YASH_NB)	Global Default Network	HP Printers		Passed	-
Host	Network	Host Technology	Instance	Status	Cause

124.12.24.111 1 of 1 (100%)

Samsung Printer

Host	Network	Host Technology	Instance	Status	Cause
124.12.24.111 (qualys, -)	Global Default Network	Samsung Printers		Passed	-
Host	Network	Host Technology	Instance	Status	Cause

Sybase Database User-Defined Control Support

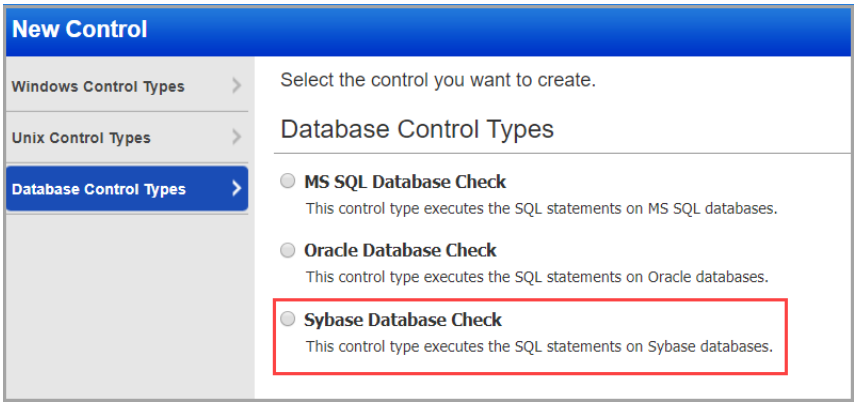
You can now use Sybase database user-defined controls to create custom checks by executing SQL statements on databases. These controls can then be used to generate policy reports on your databases. We're already supporting MS SQL and Oracle databases.

Follow these steps to create Sybase database controls and generate a report:

Step 1 - Add database controls

Go to PC > Policies > Controls > New > Control.

Select Database Control Types and then click the Sybase Database Check control type.



In each control you'll define the SQL statement that you want to execute on your database. Note - Only SELECT statements are supported for the database controls. For example, you can use the following SQL statement to list all fields from "Customers" where country is "Germany" AND city is "Berlin":

SELECT * FROM Customers WHERE Country='Germany' AND City='Berlin'

See the online help for sample queries and results.

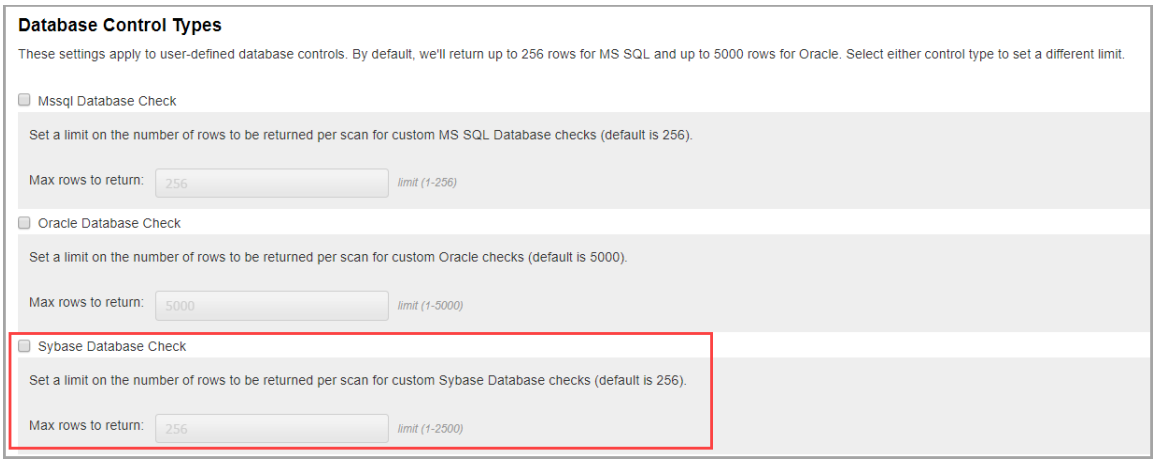
Step 2 - Add database controls to a policy

Create a new compliance policy or edit an existing policy, and add your database controls to the policy. Tip - Make sure your policy has the database technologies selected in the control.

Step 3 - Launch a compliance scan

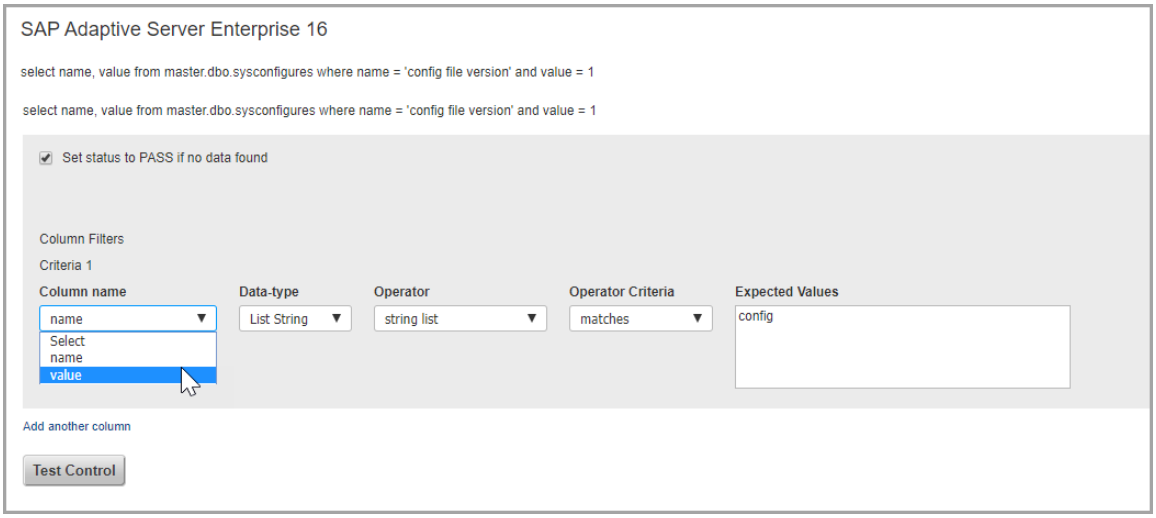
Launch a compliance scan on the host running the Sybase database.

You can edit the compliance option profile you'll use for the scan to set the max number of rows you want the check to return. By default, the max rows we'll return for a Sybase Database Check is 256 rows. To lower this limit, select the database control type in the compliance option profile and pick a new value.



Step 4 - Return to your policy to set control criteria

Edit your compliance policy using the policy editor to see the actual data returned by your scan. Select a column and define the expected value. This is how you set the criteria that will determine pass/fail status for the control.



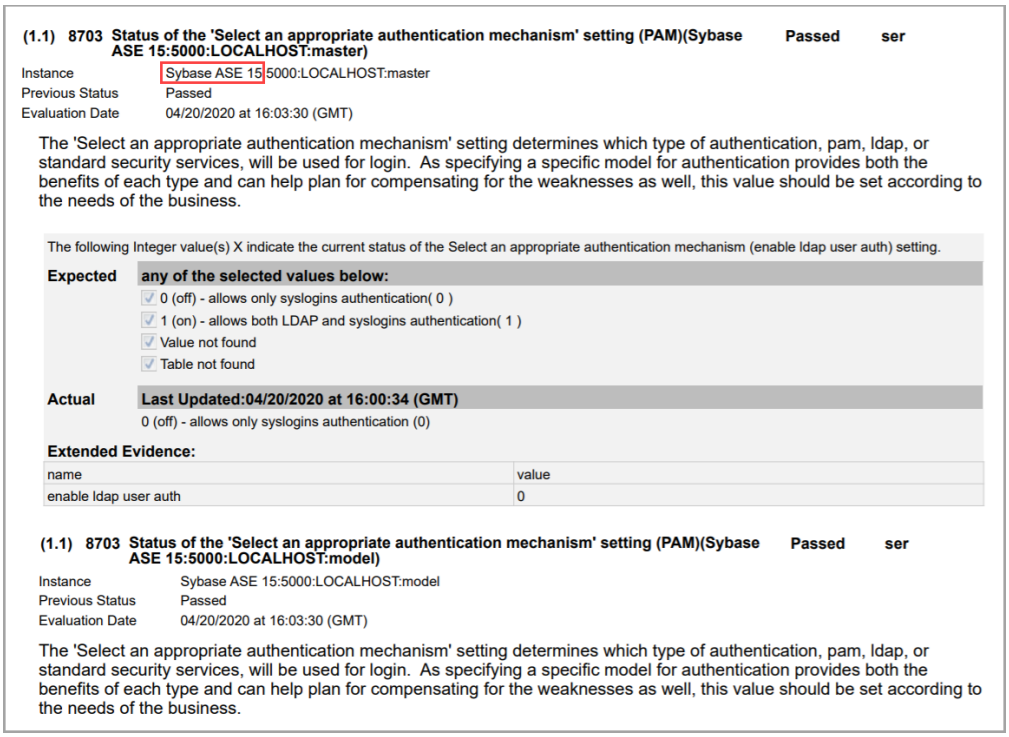
Click "Add another column" to add more criteria. You can add up to 5 criteria, i.e. Criteria 1, Criteria 2, Criteria 3 and so on.

You can choose AND or OR between each criteria. If you choose AND then both criteria must match to Pass. If you choose OR then at least one criteria must match to Pass. Click Test Control to verify the criteria you set. Then save your policy.

Step 5 - Run a report

You'll see PASS or FAIL status in your report like you do with any control. If the columns returned by the most recent scan are different than previous scans then you'll want to edit your policy to modify the criteria selected for the control.

Here's a sample report where the expected value matches the actual value, resulting in a status of Passed.



(1.1) 8703 Status of the 'Select an appropriate authentication mechanism' setting (PAM)(Sybase ASE 15:5000:LOCALHOST:master) **Passed** **ser**

Instance: Sybase ASE 15:5000:LOCALHOST:master
Previous Status: Passed
Evaluation Date: 04/20/2020 at 16:03:30 (GMT)

The 'Select an appropriate authentication mechanism' setting determines which type of authentication, pam, ldap, or standard security services, will be used for login. As specifying a specific model for authentication provides both the benefits of each type and can help plan for compensating for the weaknesses as well, this value should be set according to the needs of the business.

The following Integer value(s) X indicate the current status of the Select an appropriate authentication mechanism (enable ldap user auth) setting.

Expected **any of the selected values below:**
- 0 (off) - allows only syslogins authentication(0)
- 1 (on) - allows both LDAP and syslogins authentication(1)
- Value not found
- Table not found

Actual **Last Updated:04/20/2020 at 16:00:34 (GMT)**
0 (off) - allows only syslogins authentication (0)

Extended Evidence:

name	value
enable ldap user auth	0

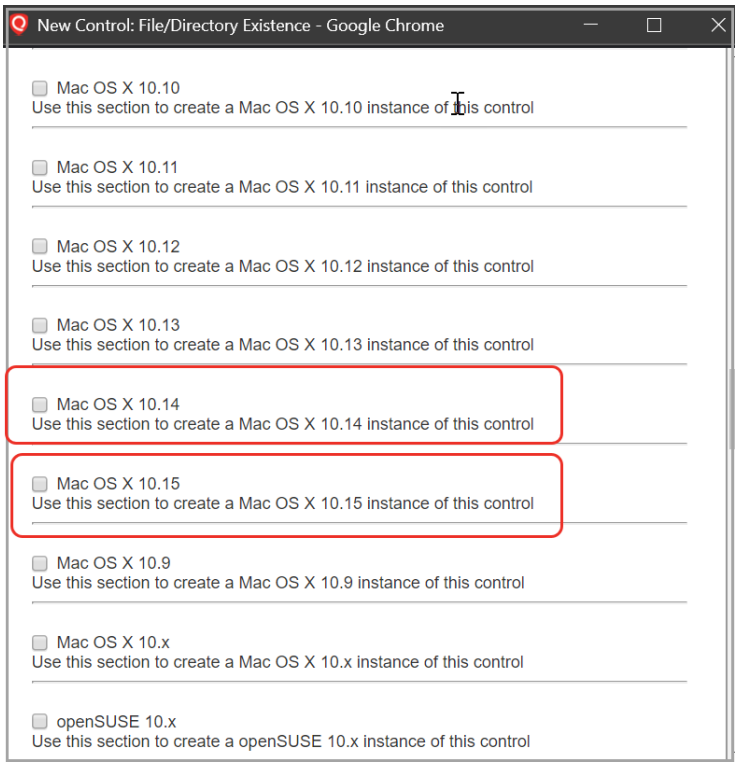
(1.1) 8703 Status of the 'Select an appropriate authentication mechanism' setting (PAM)(Sybase ASE 15:5000:LOCALHOST:model) **Passed** **ser**

Instance: Sybase ASE 15:5000:LOCALHOST:model
Previous Status: Passed
Evaluation Date: 04/20/2020 at 16:03:30 (GMT)

The 'Select an appropriate authentication mechanism' setting determines which type of authentication, pam, ldap, or standard security services, will be used for login. As specifying a specific model for authentication provides both the benefits of each type and can help plan for compensating for the weaknesses as well, this value should be set according to the needs of the business.

User-Defined Control Support for Mac OS X 10.14 and Mac OS X 10.15

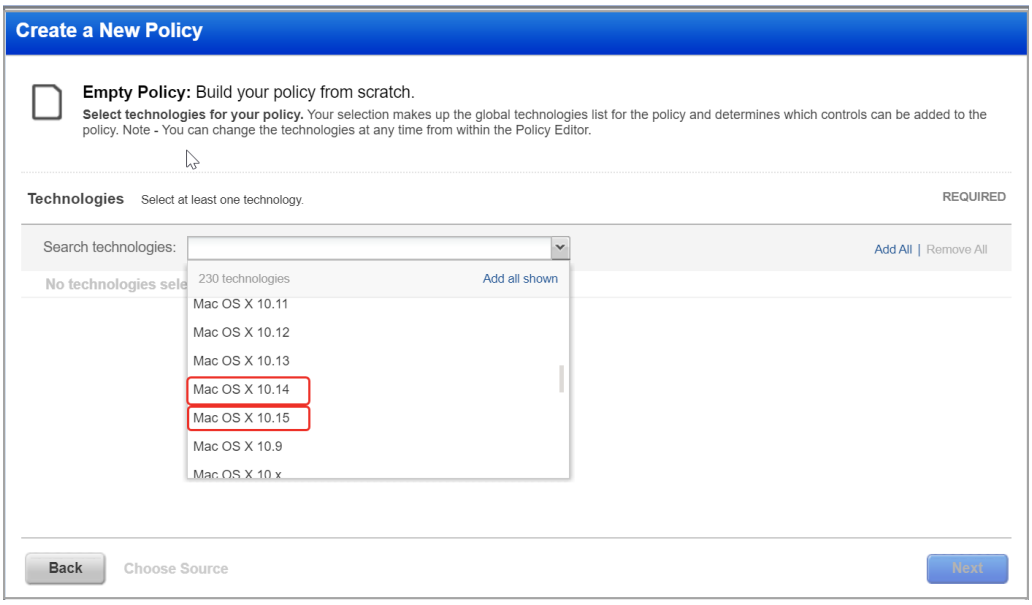
We have extended the User Defined Control (UDC) support for Mac OS X 10.14 and Mac OS X 10.15 for scanner.



Want to create a UDC for Mac OS X 10.14 and Mac OS X 10.15? Go to Policies > Controls > New > Control > Unix Control Types and select the required control types from the list. Click on the Control Technologies section to provide a rationale statement and expected value for each technology.

Note: Mac OS X 10.14 and Mac OS X 10.15 is not supported for Directory Integrity Check.

While creating a new policy, you can select Mac OS X 10.14 and Mac OS X 10.15 from the Technologies list.

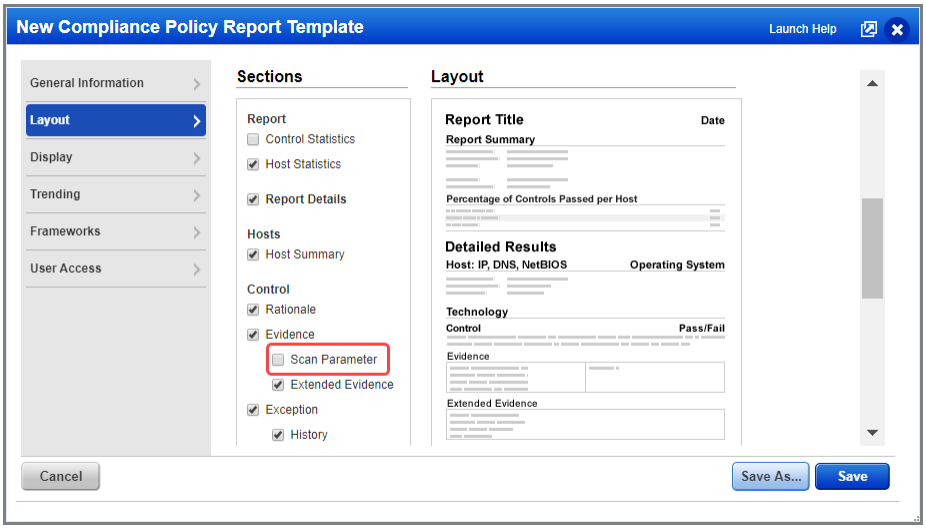


Hiding Scan Parameters in a Report

Now you'll be able to hide scan parameters in your policy report. By default, the report shows scan parameters. To hide the scan parameters from your report, uncheck the Scan Parameter check box in the Compliance Policy Report Template. You'll find it under Layout > Sections > Control while creating or editing your template.

What are the steps?

1) go to PC > Reports > Templates > New > Policy Template and click Layout from left pane.



2) Uncheck the Scan Parameter check box. You'll find it under Sections > Control.

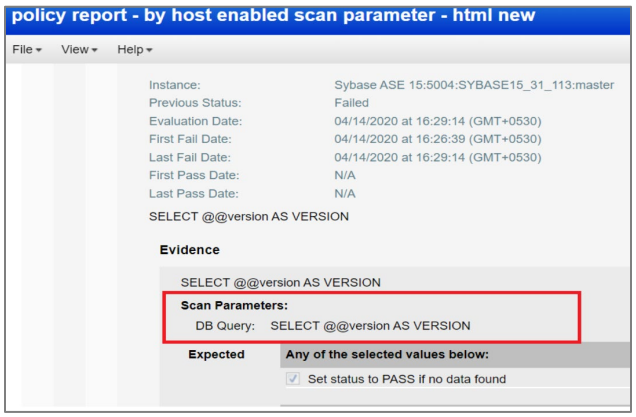
3) Click Save to create the template as per the configuration.

4) Run the policy report template you just created to generate a policy report where the scan parameter is hidden.

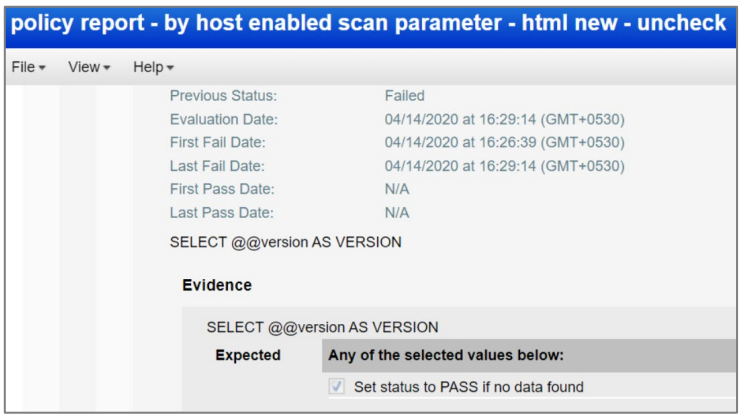
Optionally, edit an existing report template and uncheck the Scan Parameter checkbox to hide the scan parameters from the report.

Sample Reports

Report with default settings
Scan parameters are displayed in the report.



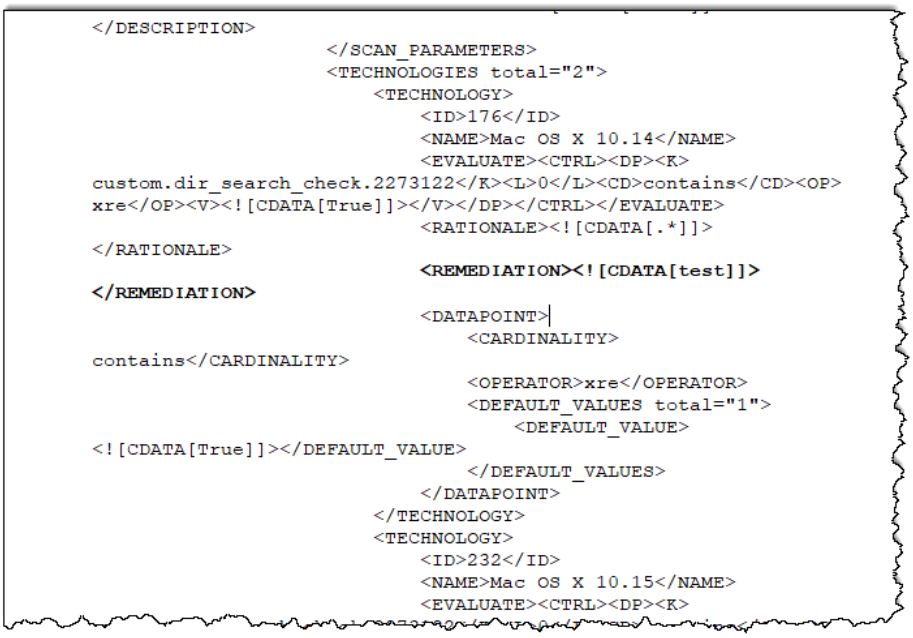
Report with the Scan Parameter checkbox unchecked
Scan parameters are hidden in the report.



Remediation Information Available in Import or Export of UDCs

You can now import or export remediation information of your User-Defined Controls (UDC) using an xml file.

Simply, navigate to Policies > Policies, choose a UDC policy from the list and from the Quick Actions menu select Export. Choose the export format as XML to view the remediation information. To import a policy with remediation information using XML file, in the Policies sub-tab go to New > Policy and select Import from XML File.



```
</DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="2">
                        <TECHNOLOGY>
                            <ID>176</ID>
                            <NAME>Mac OS X 10.14</NAME>
                            <EVALUATE><CTRL><DP><K>
custom.dir_search_check.2273122</K><L>0</L><CD>contains</CD><OP>
xre</OP><V><![CDATA[True]]></V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[.*]]>
</RATIONALE>
                            <REMEDIATION><![CDATA[test]]>
</REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>
contains</CARDINALITY>
                                <OPERATOR>xre</OPERATOR>
                                <DEFAULT_VALUES total="1">
                                    <DEFAULT_VALUE>
<![CDATA[True]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                        <TECHNOLOGY>
                            <ID>232</ID>
                            <NAME>Mac OS X 10.15</NAME>
                            <EVALUATE><CTRL><DP><K>
```

Qualys Cloud Platform

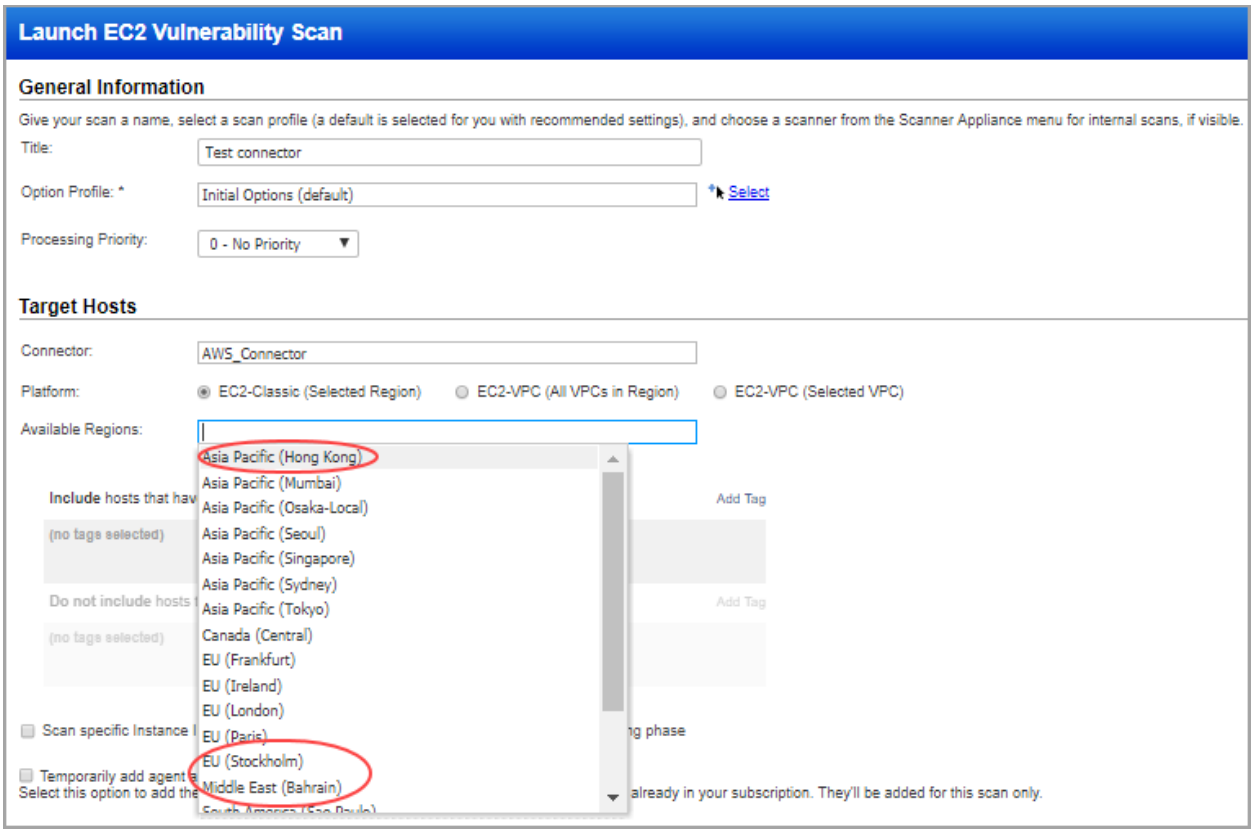
New Regions Supported for EC2 Scans

You can launch EC2 scans and scan assets in the newly supported regions. We added support for three new regions: Hong Kong (Asia Pacific), Stockholm (EU) and Bahrain (Middle East).

The newly supported regions are available when you launch any of the following scans:
- EC2 Vulnerability Scans
- Scheduled EC2 Vulnerability Scans
- EC2 Compliance Scans
- Scheduled EC2 Compliance Scans
- Cloud Perimeter Scans

Example: EC2 vulnerability scan

Go to Scans > Scans > New > EC2 Scan to launch the scan. The newly supported regions are populated in the **Available Regions** list.



Azure Key Vault now Supported in Palo Alto Networks Firewall Record

We've now extended the support for Azure Key vault to Palo Alto Networks Firewall authentication records.

Configure authentication records

Create or edit a Palo Alto Networks Firewall authentication record to retrieve password from the Azure Key vault using the specified Azure Key vault record.

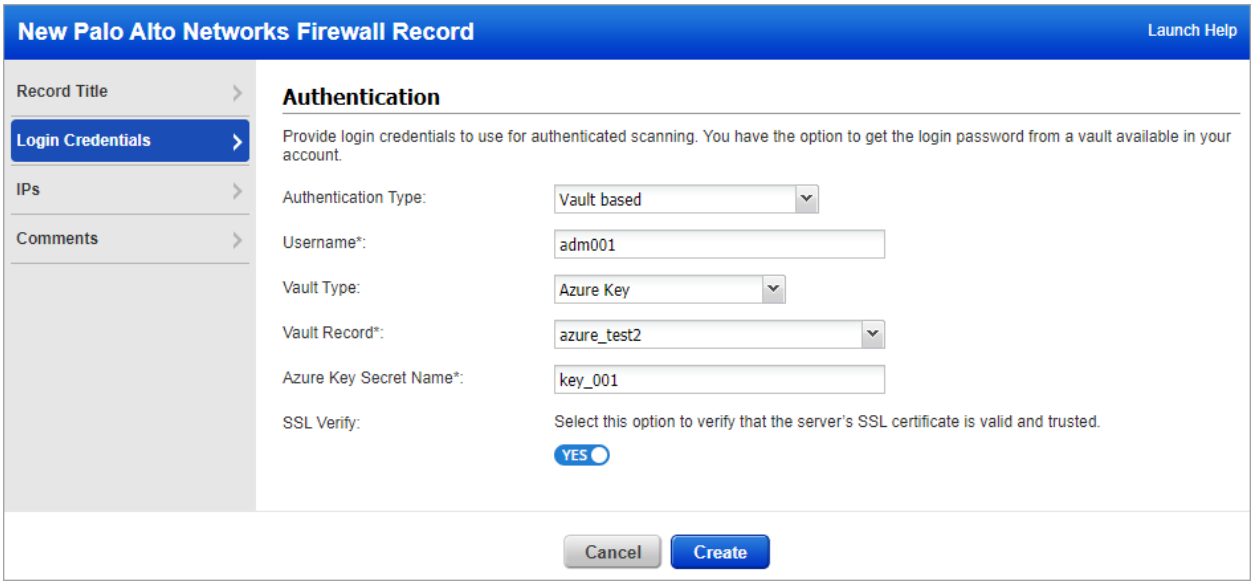
Provide these settings:

Vault Type - Azure Key

Vault Record - Your vault record.

Azure Key Secret Name - The secret name assigned to the secret stored in the vault.

SSL Verify - Toggle this button to "Yes" to verify the server's SSL certificate.



Support for ARCON PAM (Privilege Access Management) Vaults

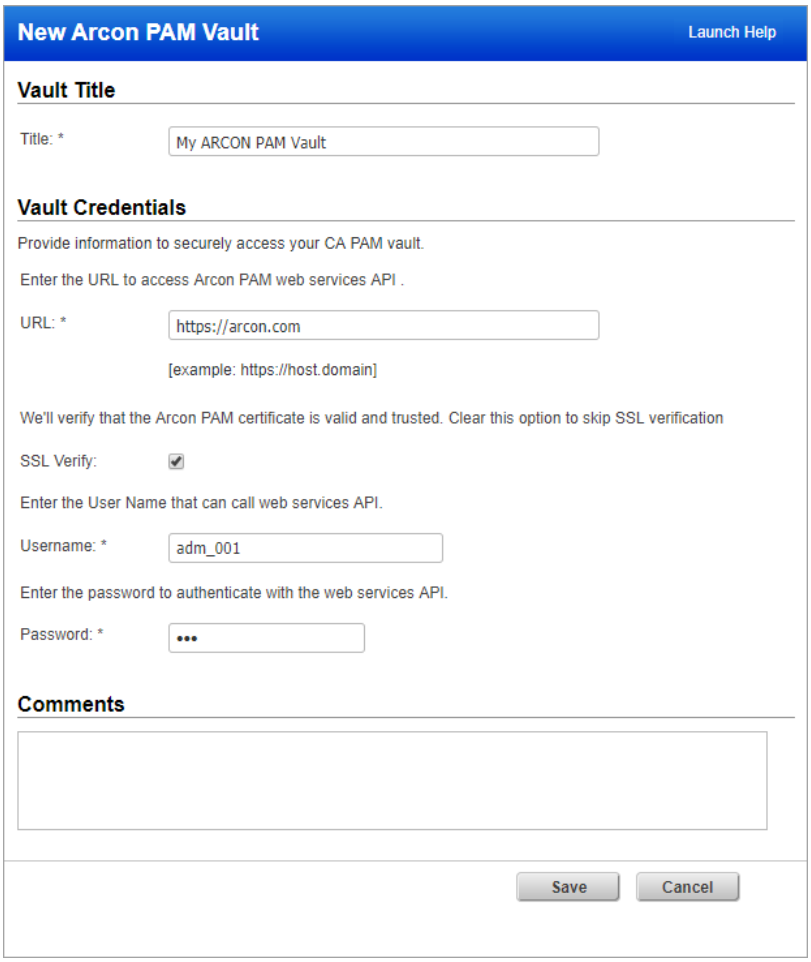
This new vault type can be used to retrieve authentication credentials from a ARCON PAM vault.

What are the steps?

You'll configure ARCON PAM vaults (vault credentials), configure the required authentication records for one or more authentication types that support the vault (Windows, Unix, Cisco, Check Point, Greenplum, MS SQL, MySQL, MariaDB, Oracle, MongoDB, PostgreSQL, Sybase and IBM DB2), and start your scans.

Configure your ARCON PAM Vault

Go to Scans > Authentication > New > Authentication Vaults. Then choose New > Arcon PAM.



Provide vault credentials

URL - The HTTP or HTTPS URL to access the ARCON PAM Vault.

SSL Verify - Qualys scanners will verify the SSL certificate of the web server to make sure the certificate is valid and trusted, unless you clear (un-check) the SSL Verify option. You may want to clear this option to skip SSL verification if the certificate was not issued by a well- known certification authority (CA) or if the certificate is self-signed.

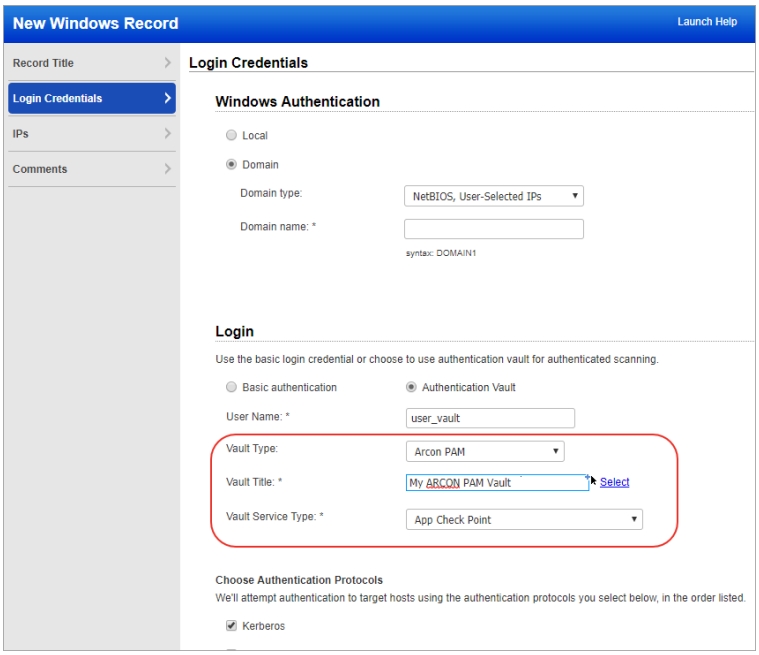
Username - A username required to access the vault.

Password - A password required to access the vault.

Configure authentication records

The ARCON PAM vault is supported in Windows, Unix, Cisco, Checkpoint Firewall, Pivotal Greenplum, MS SQL, MySQL, MariaDB, Oracle, MongoDB, PostgreSQL, Sybase and IBM DB2 authentication Windows, Unix and Cisco authentication records. Currently, ARCON PAM vault supports: 1) retrieval of password for all the authentication records that supports the vault and 2) retrieval of private key only for Unix authentication record.

Here's a sample Windows record with the vault selected.



Provide these settings:

Vault Type - Arcon PAM

Vault Title - Your vault record

Vault Service Type

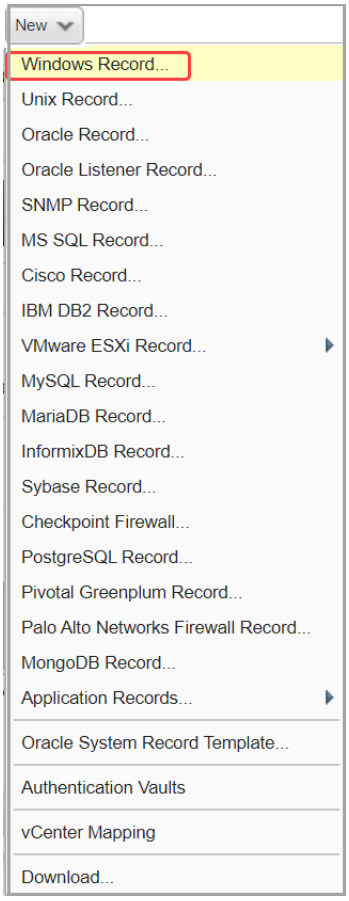
Service type that will be used for authenticating to the vault and launching the scan on the host. Select a vault service type from the drop-down.

Microsoft Windows 2019 Active Directory Support

We've extended our support for Windows authentication to include Windows 2019 Active Directory. You'll need a Windows record to authenticate to the Windows 2019 Active Directory, and scan it for compliance.

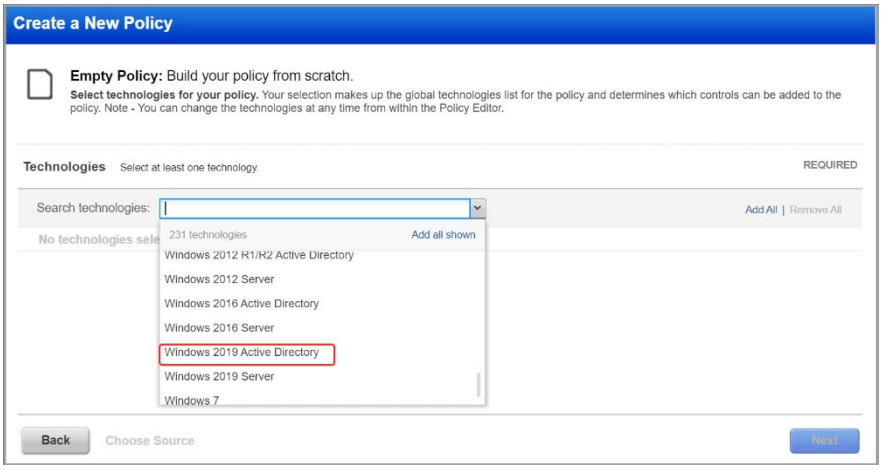
How do I get started?

Go to Scans > Authentication, and choose New > Windows Record.



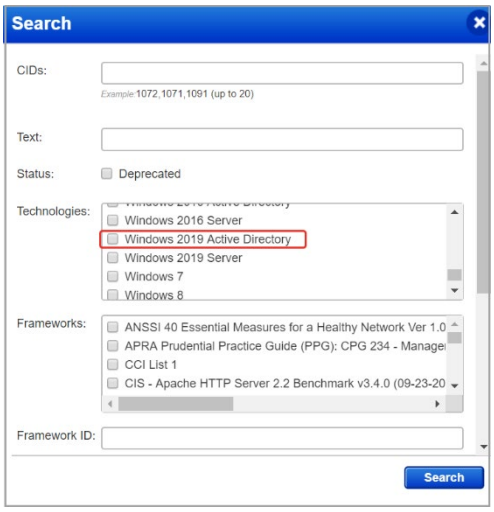
Policies and Controls

You'll see Windows 2019 Active Directory in the technologies list when creating a new policy.



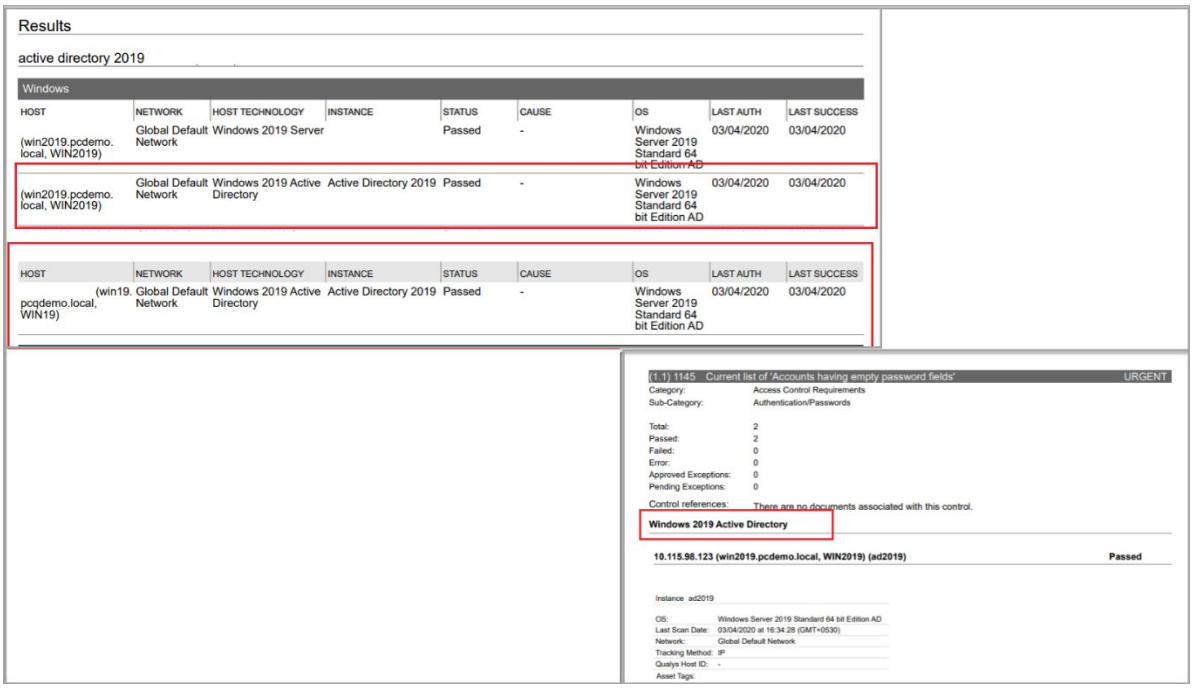
Search Controls

You'll see Windows 2019 Active Directory when searching controls by technologies.



Sample Reports

You'll see Windows 2019 Active Directory instances in Authentication reports and Policy reports.

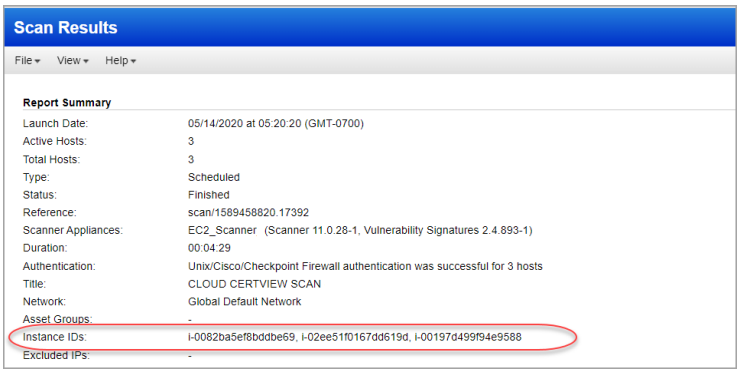


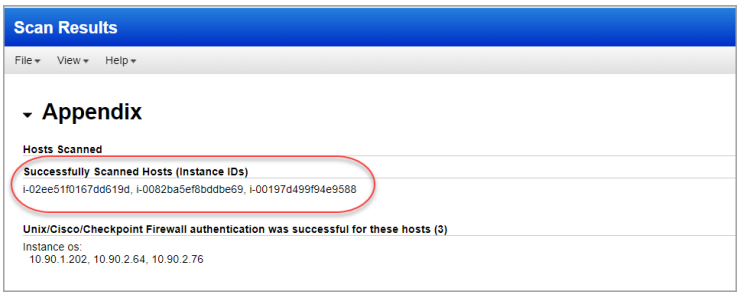
Report Changes to Show Instance IDs in Scan Results/Scan Status

We made the following changes to show scanned instance IDs, when applicable.

- We removed “FQDN” from the Report Summary section in Scan Results and Scan Status for these scan types: EC2 Scans, EC2 CertView Scans, Cloud Perimeter Scans. FQDNs are not included in the scan target for these scan types. This change applies to all report formats (HTML, PDF, CSV, etc).
- We replaced “IPs” with “Instance IDs” in the Report Summary section for EC2 CertView Scans and will show the target instance IDs for the scan.
- We replaced “DNS” with “Instance IDs” in various sections throughout Scan Results for EC2 CertView Scans, for example in the Detailed Results section and Appendix section.

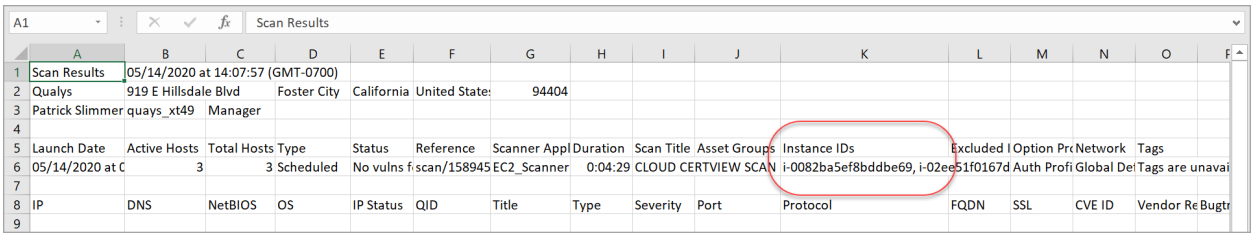
Sample Scan Results showing Instance IDs





Instance IDs in Scan Results in CSV format

You’ll notice that the IPs column has changed to Instance IDs when you download EC2 CertView Scan Results in CSV format from the UI.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Scan Results	05/14/2020 at 14:07:57 (GMT-0700)													
2	Qualys	919 E Hillsdale Blvd		Foster City	California	United State:	94404								
3	Patrick Slimmer	quays_xt49	Manager												
4															
5	Launch Date	Active Hosts	Total Hosts	Type	Status	Reference	Scanner Appl	Duration	Scan Title	Asset Groups	Instance IDs	Excluded I	Option Pr	Network	Tags
6	05/14/2020 at 0	3	3	Scheduled	No vulns f	scan/158945	EC2_Scanner	0:04:29	CLOUD CERTVIEW SCAN		i-0082ba5ef8bddbe69, i-02ee51f0167d		Auth Profi	Global Det	Tags are unavai
7															
8	IP	DNS	NetBIOS	OS	IP Status	QID	Title	Type	Severity	Port	Protocol	FQDN	SSL	CVE ID	Vendor Re
9															

Issues Addressed

- Fixed an issue where authentication record details were not loading on the Scans > Authentication tab.
- We fixed a report issue where QID 19129 “Oracle Authentication Method” only appeared in a report once even though authentication was successful on multiple Oracle database instances. This occurred when the user applied a search list to the report template.
- Fixed an issue where the Remote Discovery icon was incorrectly displayed for QID 91534 and QID 91563 in the Vulnerability KnowledgeBase even though these QIDs are detected by authenticated scans. Now you’ll see the Multiple Authentication Types Discovery icon for these QIDs.
- Fixed an issue where there was a system created authentication record for a single IP, single instance. The instance was stopped in a subsequent scan and another single instance was started. In this case we did not remove the IP from the first authentication record.
- We fixed an issue where date filters in different areas of the UI, such as Control View tab and Authentication tab, showed an invalid validation error message in the UI even though the date filter was working.
- Fixed an issue on the PC > Reports > Control View tab where pagination was not working when the Last Scan Date filter was used to filter the results.
- Fixed an issue where the Vulnerability Search List Information page was missing some report templates associated with the search list. Now this is fixed so all report templates that use the search list are listed.
- Fixed an issue where the Map Scan Canceled email notification showed the variable {friendlyName} in the email body instead of the actual scanner appliance name. The email subject line did show the correct scanner appliance name.
- Fixed an issue in the Compliance Report where the total control count shown in the Host Statistics section was incorrect because disabled controls were not filtered out. Now only active controls are counted when calculating the total control count.
- We fixed an issue where there was a discrepancy in the results from the Test Control / Evaluate option in the Policy Editor and results shown in Policy Compliance reports. Now we’ll display actual values when you evaluate controls in the Policy Editor.
- We fixed an issue where the compliance option profile in Edit mode no longer showed the restricted policies under Scan by Policy for accounts with SCA only.
- We made a fix when evaluating the actual value for a control when the value includes a single quote.
- For accounts set to Japanese language there was an issue that we fixed where the QID title and description was not appearing in Japanese after the 10.0 release.
- For accounts upgraded to VMDR you can now pick Prioritization as your home page. Just log in and choose Home Page under your account name to make your home page selection.
- We fixed an issue where PC scans were finished but the results were not processing. The issue was related to instance strings in the results that were greater than 320 characters. Now we allow for larger instance strings.
- Fixed a small UI issue where the “Confirm” tab on the left side of the confirmation screen when scheduling EC2 scans was not highlighted in blue. Now it will be highlighted.
- Fixed an issue where customers saw degraded performance for the Compliance Posture API.

- Fixed an issue where certain API calls returned the wrong HTTP status code for the API response error.
- We fixed an issue where the Host List Detection API list output was not showing EC2 instance ID for EC2 assets under EC2 metadata. Now we are showing this information in the API output for host assets that have EC2 instance ID.
- We fixed an issue where the wrong tracking method was shown for OCA tracked assets in the XML output for Host List API. Now the tracking method "OCA" is shown for these assets.
- We fixed an issue in the Activity Log API output in CSV format caused by null values. Now when there is a null value we'll show N/A in the cell so that it's not empty.
- Fixed a DTD validation issue for Dynamic Search List API when show_report_templates or show_remediation_policies were set to 0 in the API request.
- Corrected an API sample in the Qualys (VM, PC) API User Guide for "View Scanner Appliance with VLANs, Static Routes" where the API sample request was missing "X-Requested-With: Curl" -X "GET".
- Corrected an error in the Qualys (VM, PC) API User Guide for Scheduled Reports List API where the wrong values were shown for the is_active input parameter. Valid values are 0,1.
- Updated the VM option profile help to include more information on excluding QIDs and why you may still see scan traffic for QIDs that were excluded.
- Updated the VM option profile help to include a new FAQ item that explains why you may see traffic on ports that are not in your list of ports to scan.
- Added a new document for Microsoft Exchange Server Scan User Privileges and Configurations.
- Added a new document for NetScaler Authentication which outlines the privileges needed for both vulnerability scans and compliance scans.
- Updated the PC help to better explain the different dates you'll see in PC reports - Last updated date, Evaluation date and Policy last evaluated date.
- Updated the Vulnerability Information help to list the conditions that result in the Change Log section being updated.
- Updated Windows authentication help & documentation to include Windows Server 2016.
- Updated Windows authentication help to emphasize that if you select "Active Directory" or "NetBIOS, Service-Selected IPs" on the Login Credentials tab in your Windows record that the IPs tab will be disabled because you do not add IPs to records with these domain types.
- Updated the online help for HashiCorp authentication to state that you must store the secret in the KV (Key-Value) secret engine version 2 as we do not support secret engine version 1.
- Policy compliance reports will now include the current date (date the report is generated) when the template has the release timeframe filter "Within the last N days|weeks|months" enabled.