Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.13.2

September 9, 2021

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

Qualys Cloud Platform

Use System Authentication Records in Vulnerability Scans

Qualys 10.13.2 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

Use System Authentication Records in Vulnerability Scans

With this release, you can start using system created authentication records from Policy Compliance in your vulnerability scans. Instance discovery and record creation will continue to be based on compliance scan data discovered for running instances when this option is selected in your compliance option profile.

Once system authentication records are created, they can be used in compliance scans (same process as before) and also in vulnerability scans. System authentication records will be used in addition to user created authentication records when authentication is enabled for your scans.

Note: Your subscription must include both PC and VM/VMDR, and the hosts being scanned must be present in both.

How to Use System Created Records in Vulnerability Scans

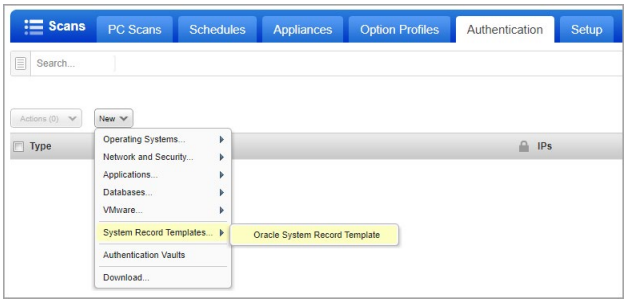
Follow the steps below to perform instance discovery and system record creation in PC, and then include those system created records in VM/VMDR.

For PC customers already using system created authentication records, you can jump directly to Step 4 to see how to use your system records for VM. The steps for instance discovery and system record creation in PC have not changed.

1) Create Oracle System Record Templates (applicable for Oracle only)

Create an Oracle system record template and enter the login credentials you want to use for Oracle system created records. In the next step you'll create a compliance option profile for instance discovery, and choose the Oracle system record template name. The template will be linked automatically to the system created records created as a result of the discovery scan.

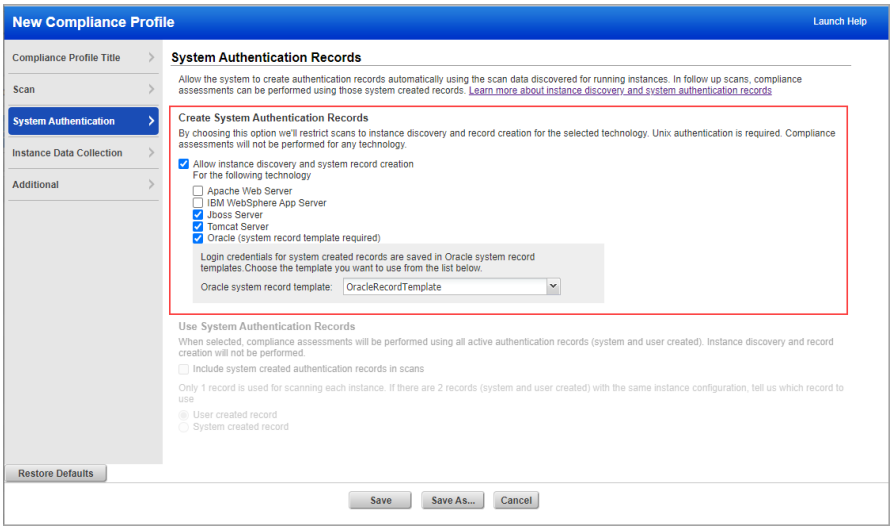
To create this template, go to **Scans** > **Authentication** > **New** > **System Record Templates** > **Oracle System Record Template**. Once saved, your Oracle system record template will be listed on the **Authentication** tab with your authentication records.



2) Create compliance profile for instance discovery and record creation

In your Compliance Profile, go to the **System Authentication** tab, choose "Allow instance discovery and system record creation" and select one or more technologies. You'll use this option profile for instance discovery scans. We'll discover running instances during the scan, and then use the information collected about your running instances to create authentication records.

For Oracle, you must also select the Oracle system record template (created in Step 1) with the login credentials you want to apply to system created records.



Note: We support auto discovery of Jboss Server instances on Unix and Windows. For the other technologies, we support auto discovery of instances running on Unix only.

Make sure you have Unix/Windows authentication records in your account.

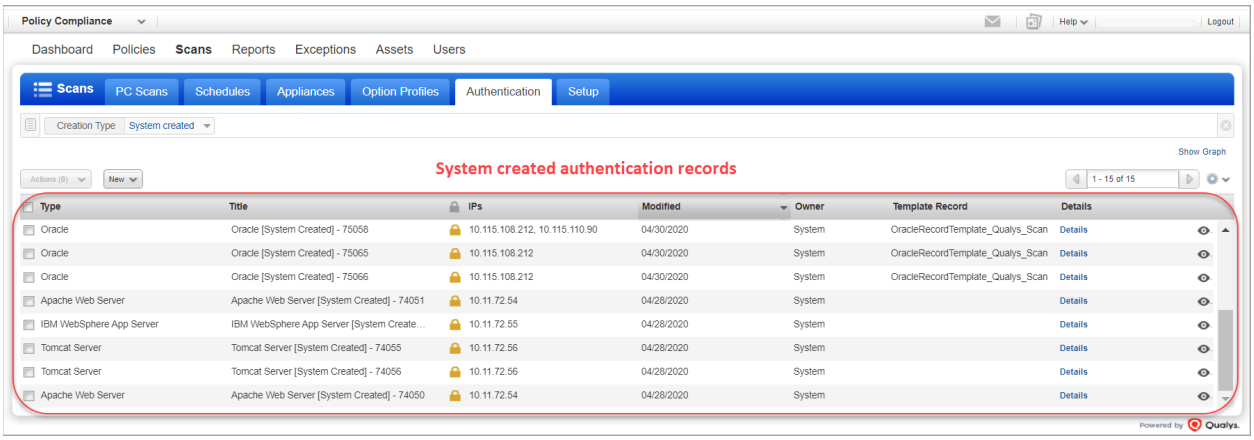
3) Launch compliance scan for instance discovery and record creation

Launch a compliance scan (using PC or SCA) 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.

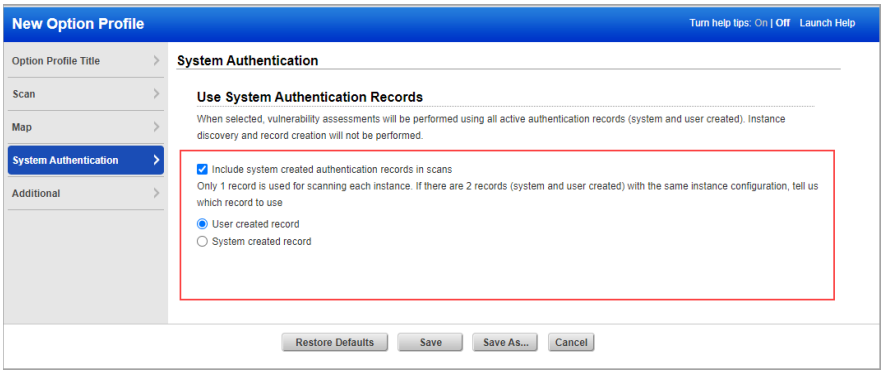
Auto record creation process – Instance scan data consolidation occurs based on authenticated scan data from the scan. Authentication records are created based on consolidated scan data. Record creation starts when the scan is Finished, during scan processing. Records may be created or updated (new IPs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

How to identify system created authentication records – Go to **Scans** > **Authentication**. System records are identified in the list by a gold lock (🔒) 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.

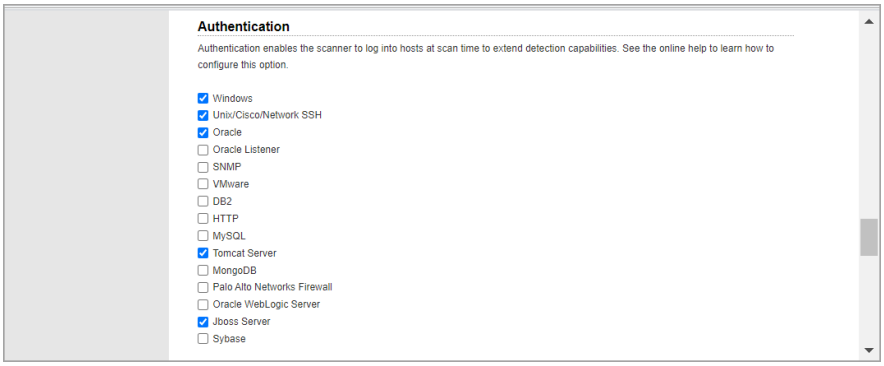


4) Create VM option profile to include system authentication records in scans

In your VM Option Profile, you'll see the new **System Authentication** tab. On this tab, select "Include system created authentication records in scans". When selected, system created records (for technologies supported in VM) will be used along with user created records at scan time. 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.



Authentication must also be enabled in the option profile. Go to the **Scan** tab and scroll down to the **Authentication** section. Select each authentication type you're interested in. Note that only system records for technologies supported in VM will be included in vulnerability scans.



5) Launch vulnerability scan and include system records

Launch a vulnerability scan and choose an option profile with the "Include system created authentication records in scans" option selected. That's it! Your vulnerability scan will use system created records and user created records at scan time.

Learn more

See the online help to learn more about system created authentication records, including how to make system records Inactive so they won't be included in scans, how to search for system records, and you'll also find answers to common questions.

Issues Addressed

- We fixed an issue where customers were unable to schedule vulnerability scans on asset groups that only contain DNS names.
- We fixed an issue where Policy Compliance reports appeared blank for customers when the report was generated using asset tags.