

Apache Authentication – Auto Record Creation

Instance discovery and auto record creation is supported using Apache authentication records (UI and API). As before a single Apache record may be used when the same record configuration (Apache configuration file, Apache control command) is replicated across hosts in the record.

Modules supported - PC

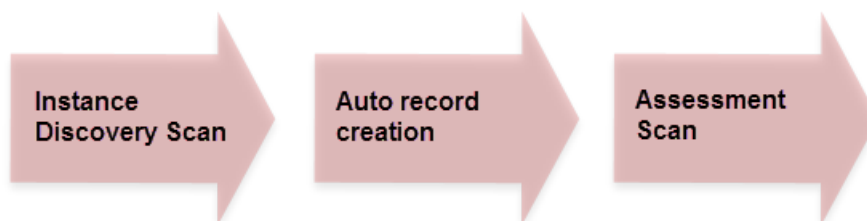
Permissions - Same permissions for Apache records as before.

Summary

These capabilities are available.

- Support for scanning multiple instances running on the same host, and when hosts have varying configurations
- 2 phased scanning process. First a discovery scan finds Apache instances, consolidates instance data, and creates/updates auth records in the user's account. Then an assessment scan uses the records saved in the user's account for control evaluations.
- Option profile settings allow you to enable instance discovery and auto record creation, include system-created records for scans, and determine whether to send system records or user records when there are 2 records for the same instance configuration.
- Compliance scan results show a list of instances discovered by the scan when the instance discovery and auto record creation feature is enabled for the scan. Compliance assessment data is not collected during instance discovery scans.
- New System created auth records. Auto created authentication records have the owner "System". These records cannot be edited by users.
- You can enable Apache records for authenticated scanning, i.e. set as Active, or disable this, i.e. set as Inactive.

Scan process for instance discovery and auto record creation



Steps to get started

1) Configure option profiles

You'll need to create 2 option profiles. These options cannot be selected in the same profile.

Option Profile 1: Choose **“Allow instance discovery and system record creation”** and select the **Apache Web Server** technology, plus any other technologies you're interested in. (Note that system record creation is supported for multiple technologies.)

Use this 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. Unix authentication is required for this option so be sure you have Unix records in your account.

New Compliance Profile Launch Help

Compliance Profile Title > **System Authentication Records**

Scan >

System Authentication >

Additional >

Create System Authentication Records

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. [Learn more about instance discovery and system authentication records](#)

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required. Compliance assessments will not be performed for any technology.

☒ Allow instance discovery and system record creation

For the following technology

☒ Apache Web Server

☒ IBM WebSphere App Server

☒ IBM WAS Installation Directory

☐ IBM WAS Server Directory

☒ Jboss Server

☒ Tomcat Server

☒ Oracle (system record template required)

Login credentials for system created records are saved in Oracle system record templates. Choose the template you want to use from the list below.

Oracle system record template:

Use System Authentication Records

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

☐ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

☒ User created record

☐ System created record

Option Profile 2: Choose **“Include system created authentication records in scans”** in the option profile you'll use for compliance assessments. 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.

New Compliance Profile Launch Help

Compliance Profile Title > **System Authentication Records**

Scan >

System Authentication >

Additional >

Create System Authentication Records

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. [Learn more about instance discovery and system authentication records](#)

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required. Compliance assessments will not be performed for any technology.

☐ Allow instance discovery and system record creation

For the following technology

☐ Apache Web Server

☐ IBM WebSphere App Server

☒ IBM WAS Installation Directory

☐ IBM WAS Server Directory

☐ Jboss Server

☐ Tomcat Server

☐ Oracle (system record template required)

Login credentials for system created records are saved in Oracle system record templates. Choose the template you want to use from the list below.

Oracle system record template:

Use System Authentication Records

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

☒ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

☒ User created record

☐ System created record

2) Launch discovery scan for auto 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 scan results.

Appendix	
Target hosts found alive (IP)	10.10.26.26, 10.10.26.46, 10.10.35.249
Target distribution across scanner appliances	External : 10.10.26.26, 10.10.26.46, 10.10.35.249
Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts	10.10.26.26, 10.10.26.46, 10.10.35.249
Auto Discovered Instances	Apache Web Server (Configuration File: /etc/httpd/conf/httpd.conf, Apache Control Command: /usr/sbin/httpd) 10.10.26.46, 10.10.35.249

We'll also tell you when we don't find running instances for scanned hosts.

Appendix	
Target hosts found alive (IP)	10.115.68.144-10.115.68.148
Target distribution across scanner appliances	VHSA : 10.115.68.144-10.115.68.148
Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts	10.115.68.145-10.115.68.147
Auto Discovered Instances	Apache Web Server instances were not found for these hosts 10.115.68.145-10.115.68.147

Seeing N/A? That means the discovery scan was launched on non-Unix hosts.

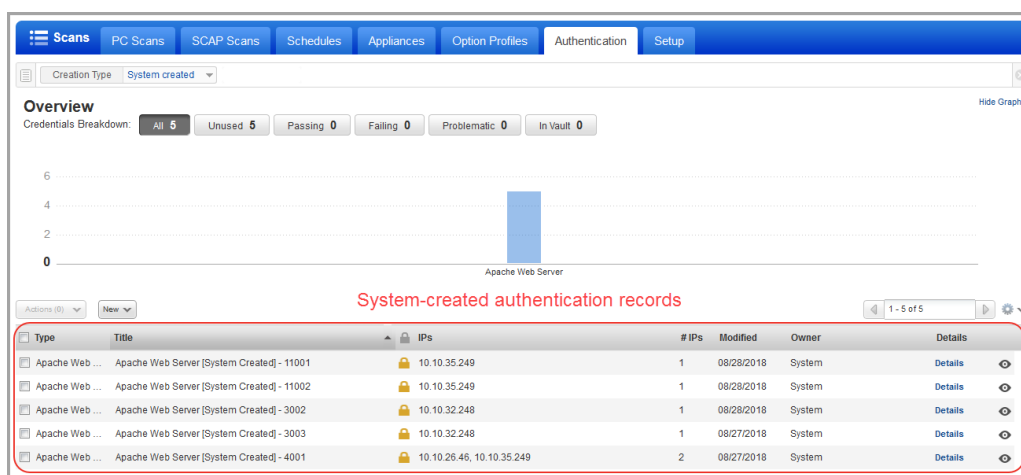
Appendix	
Target hosts found alive (IP)	10.10.36.125
Target distribution across scanner appliances	External : 10.10.36.125
Auto Discovered Instances	N/A

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  and Owner “System”.



3) Launch assessment scan for control evaluations

Launch a compliance scan (using PC or SCA) and choose an option profile with the “Include system authentication records in scans” option enabled.

How it works - auto record creation

During scan processing instance scan data is consolidated, mapping Apache record configuration to hosts:

- Single host with single instance configuration
- Single host with multiple instance configurations
- Multiple hosts with single instance configuration
- Multiple hosts with multiple instance configurations

Let's consider a sample scan with instance discovery and system record creation enabled. Sample scan data collected from the discovery scan is represented below.

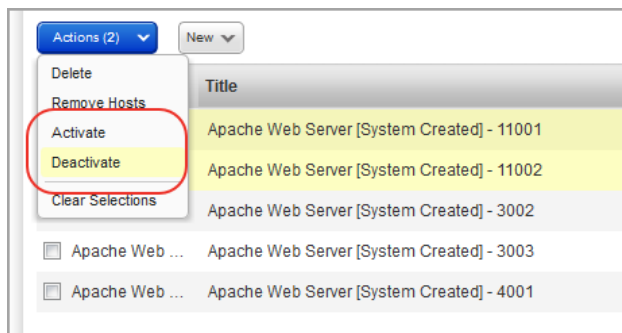
For this scan, 3 Apache authentication records are auto created:

Apache config file	Apache control command	Hosts
conf1	bin1	host1, host2
conf2	bin2	host1
conf3	bin3	host2

Make Apache records Inactive

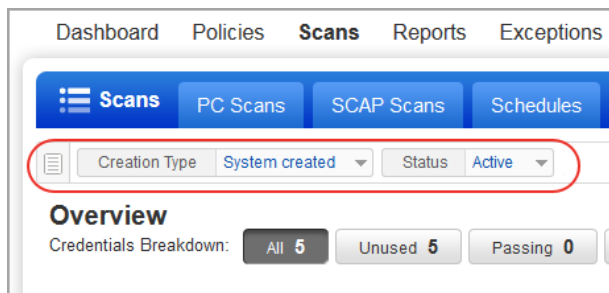
You can choose to make any Apache Web Server record Inactive, including system-created records and user-created records.

Inactive records are not included in scans (even if the “Include system created authentication records in scans” option is selected in the option profile). Simply choose the records you want to make Inactive and pick Deactivate from the Actions menu above the data list. To activate records choose Activate.



Search Apache records

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



Common questions

What is naming scheme for system created authentication records?

You'll see “Apache Web Server [System Created] – ID” for the authentication record name, where ID is a unique record ID for the instance discovered.

Changes in scan data for running instances

When new instances are discovered they are added to existing records or new records are created for them, depending on their settings (configuration file, control command, IPs, network if applicable).

What about my user created authentication records?

Your user created authentication records are not changed, and they are included in scans as long as they are Active.

Are new system created authentication records added if I already have user created records with the same settings?

Yes. New system authentication records are always created for all running instances discovered when the option profile for the scan has the “Allow instance discovery and system record creation” option enabled. If you already have a user created record with the same settings, the system makes no changes to it. The user created record is included in scans by default. Edit the option profile if you prefer to use system created records in the case of duplicates.

What happens to existing system records when instances are added and removed?

Instances are reported for the host:

For each instance reported we'll see if a system record exists with the instance configuration. If a record is found for the instance and it has the host's IP included then there is no change. If a record is found for the instance but it doesn't have the IP we'll add the IP to the record. If a record is not found for the instance we'll create a new system record for the instance and IP.

No instances are reported for the host:

The host's IP is removed from all existing system records that have the IP.

Fewer instances are reported than the previous scan (instances are brought down):

The host's IP is removed from system records for the instances that are no longer running.

More instances are reported than the previous scan (instances are brought up):

We'll look at each reported instance to see if a system record already exists. If a record exists then we'll add the host's IP to the record (if not already included). If a record does not exist then we'll create a new system record for the instance and IP.

Can I use Scan by Policy with “Include system created authentication records”?

Yes, and this is recommended. You can use Scan by Policy to perform compliance assessment on Apache assets in a policy. We recommend you include system created authentication records. This is the only way to ensure that all active authentication records (system and user created) will be used for the compliance assessment.

Can I use Scan by Policy with “Allow instance discovery and system record creation”?

No. These options cannot be used together. Compliance assessment data is not collected for instance discovery scans.

Can I edit system authentication records?

No. System authentication records cannot be edited by users. You can change the record status (Active, Inactive) from the Actions menu above the data list.

Can I delete system authentication records?

Yes. Users with permission to create/edit authentication records can also delete authentication records, including system records. Tip - You may choose to make system records Inactive. Inactive records are not included in any scans.

How do I turn off auto record creation?

Go to your option profile and clear the option “Allow instance discovery and system record creation” under System Authentication Records. When cleared, new system records will not be created.

What if I don't want to use System authentication records in scans?

No problem. Take one of these actions:

- Deactivate system records. Use the search feature above your authentication records list to find all records with creation type “System created”. Then select the records and choose Deactivate from the Actions menu.
- In your compliance profile, clear the option “Include system created authentication records in scans”. When cleared, only user created authentication records are included in scans. Keep in mind that existing compliance scan data will remain in your account. Purge hosts to remove all host information.

Download authentication records list

When you download the authentication records list in CSV format (by choosing New > Download above the list) you'll see a new column in the CSV file. The new column “Is System Created” identifies whether each record was system created or not (Yes or No).

Sample CSV:

```
"Authentication Records","08/30/2018 at 12:33:14 PM (GMT-0700)","141"
"Qualys, Inc.", "919 E Hillsdale Blvd 4th Floor, ", "Foster City", "California", "94404", "United States of America"
"Patrick Slimmer", "qualys_ps", "Manager"
"Type", "Title", "Is System Created", "IPs", "IPs", "Modified", "Owner", "Status"
"Tomcat Server", "10.10.10.10", "No", "10.10.10.10", "1", "06/21/2018 at 11:07:00 PM (GMT-0700)", "Patrick Slimmer (Manager)", "Active"
"Windows", "My Windows Record", "No", "10.10.30.9", "1", "02/25/2018 at 11:18:03 PM (GMT-0800)", "Patrick Slimmer (Manager)", "Active"
"Apache Web Server", "Apache IBM HTTP 7", "No", "10.10.26.26", "1", "08/29/2018 at 01:47:34 PM (GMT-0700)", "Patrick Slimmer (Manager)", "Active"
"Apache Web Server", "Apache Web Server [System Created] - 11000", "Yes", "10.10.35.249", "1", "08/28/2018 at 12:21:35 PM (GMT-0700)", "System", "Active"
"Apache Web Server", "Apache Web Server [System Created] - 11000", "Yes", "10.10.35.249", "1", "08/28/2018 at 12:21:35 PM (GMT-0700)", "System", "Active"
"Apache Web Server", "Apache Web Server [System Created] - 11001", "Yes", "10.10.35.249", "1", "08/28/2018 at 12:21:35 PM (GMT-0700)", "System", "Active"
...
```

Want to know more?

Search the help for System Authentication Records. For details on API changes, please see the Qualys API Release Notes.

Last updated: March 22, 2021