Qualys 8.9.1 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

Provide Amazon EC2 API Proxy Information
View Platform Provider Information

Qualys Vulnerability Management (VM)

Choose CVSS Version for reports
Exclude Account ID from report filename
Set Date to Reopen Remediation Tickets
Ignored Vulnerability Scorecard Report - removed size limit

Qualys Policy Compliance (PC/SCAP)

MS IIS 10 Support
Pivotal Web Server 6.x Support
Docker Authentication support for Application Records
Support for Windows 2016 technologies

Qualys API Enhancements

See the *Qualys API Release Notes 8.9.1* for details. You can download the release notes and our user guides from your account. Just go to Help > Resources.

Qualys 8.9.1 brings you many more Improvements and updates! Learn more

Qualys Cloud Platform

Provide Amazon EC2 API Proxy Information

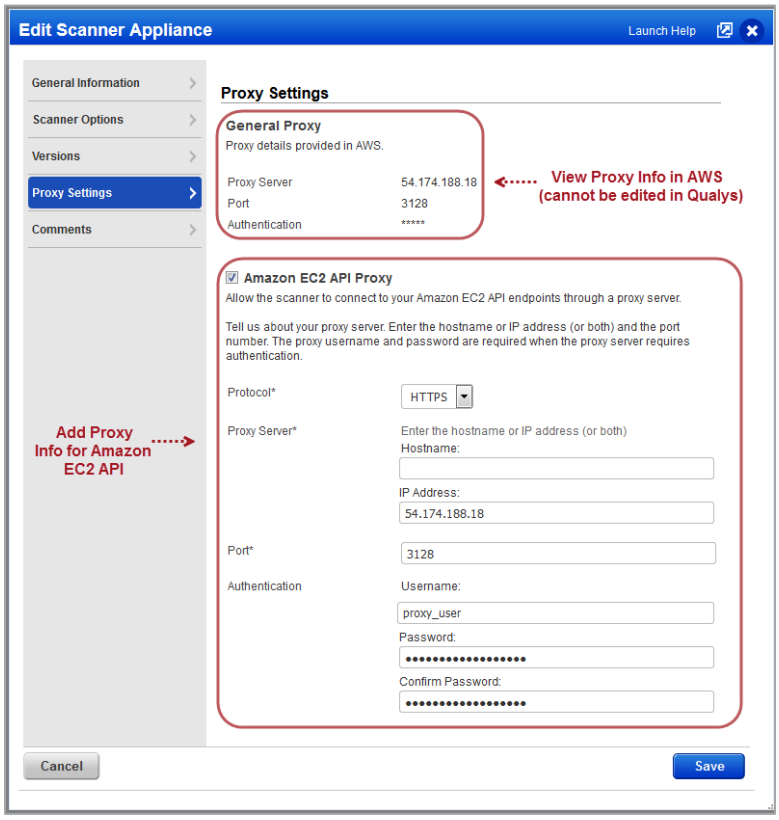
Have a proxy server for connecting to your Amazon EC2 API endpoints? If yes, you can now edit your scanner appliance in the Qualys UI to provide details about the proxy server.

Good to Know

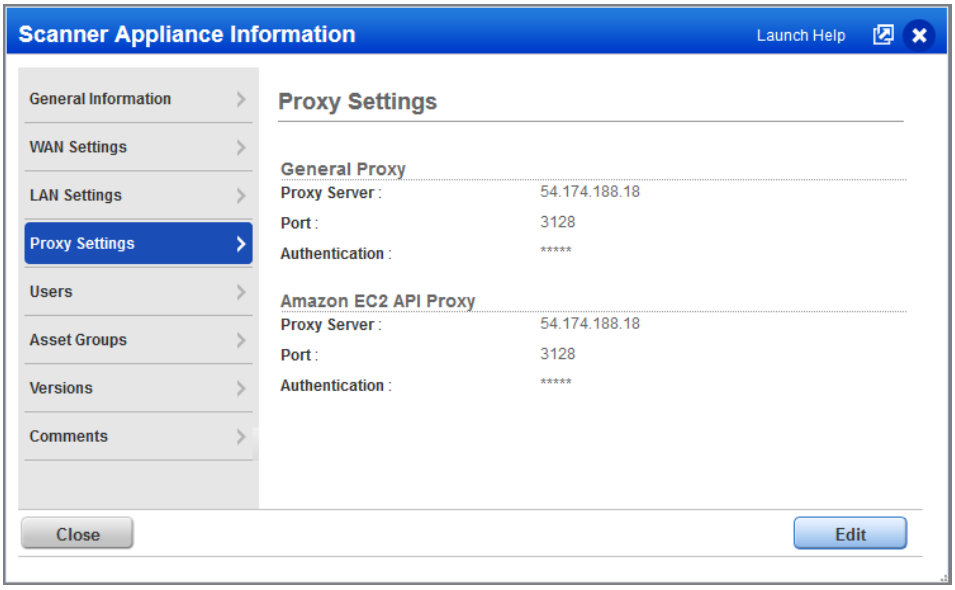
- Provide an Amazon EC2 API proxy sever to allow the scanner to connect to your Amazon EC2 API endpoints. The scanner makes API calls to the AWS Gateway through the proxy server that you specify. For example, it calls the DescribeInstance API to get the current IP address for each EC2 instance you want to scan.
- The proxy server needs to allow access to AWS region-specific endpoints. Go here to learn about regions & endpoints: http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region
- The Amazon EC2 API Proxy option only appears in the Qualys UI when general proxy settings have already been configured in Amazon AWS (as part of the instance configuration). See How to configure a virtual scanner using Amazon EC2/VPC at the Qualys Community.

What are the steps?

Go to Scans > Appliances and choose Edit from the Quick Actions menu for your EC2 scanner appliance. Go to the Proxy Settings tab (only visible for EC2 scanners), select the Amazon EC2 API Proxy check box and tell us about your proxy server. You'll enter the proxy server's hostname and/or IP address, port and authentication credentials (if required by the proxy server).



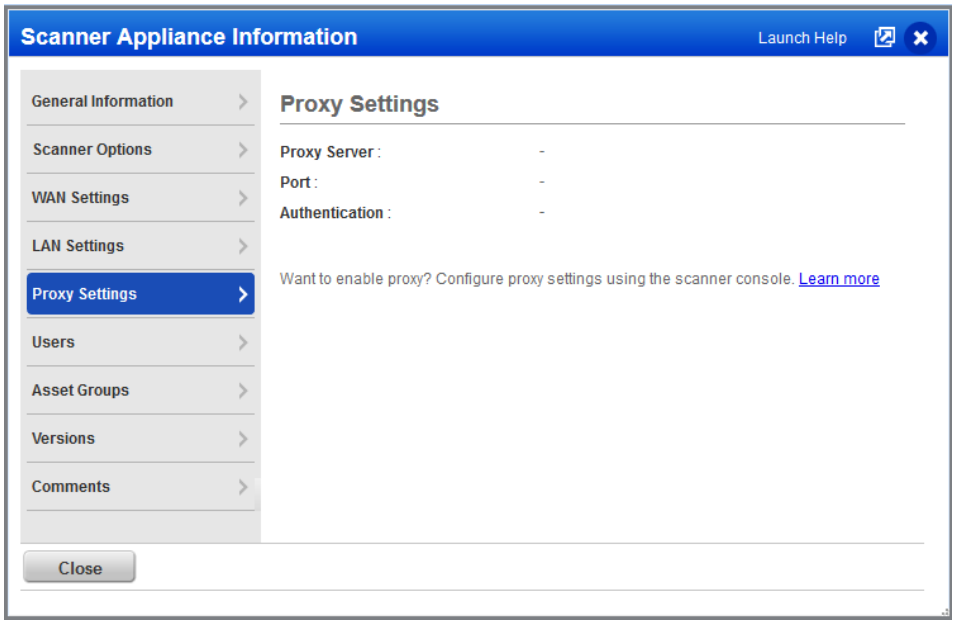
You can view all proxy settings on the Scanner Appliance Information page. Just go to Scans > Appliances and choose Info from the Quick Actions menu for your scanner.



We'll show asterisks (*****) in place of proxy authentication credentials when provided. We'll show N/A when not provided.

Have scanners that are not used for EC2 scanning?

You'll notice a change to the Proxy Settings tab on the Scanner Appliance Information page for non-EC2 scanners. When proxy settings are enabled we'll show you the proxy settings here. When not enabled, we'll show a dash for each setting and provide a link to learn more (as shown below).

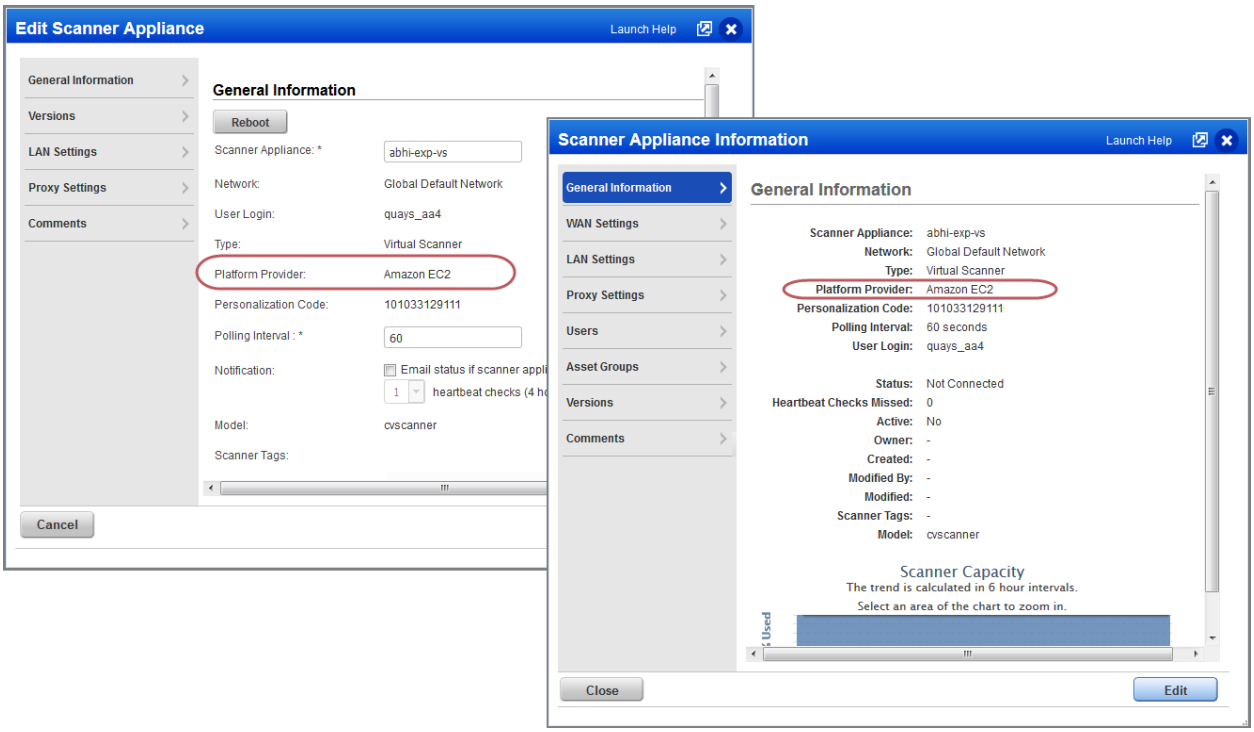


Note that you cannot edit proxy settings in the Qualys UI for non-EC2 scanners. You'll do this from the scanner console.

View Platform Provider Information

When you have a virtual scanner that's been deployed in a cloud environment, we'll now show the platform provider in the scanner appliance details. For example, we'll show platform providers like Amazon EC2, Microsoft Azure and Google Cloud Platform.

The platform provider appears under General Information when you view or edit your scanner appliance. This field applies only to virtual scanners deployed on a cloud platform.

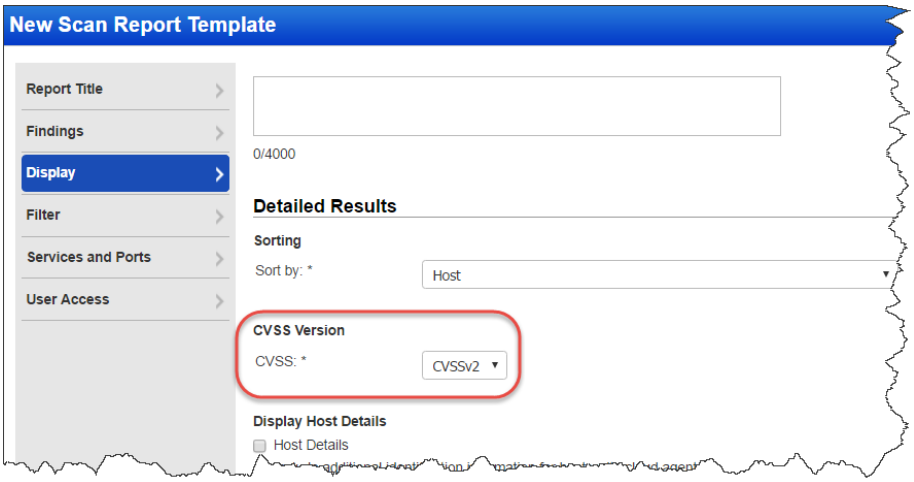


Qualys Vulnerability Management (VM)

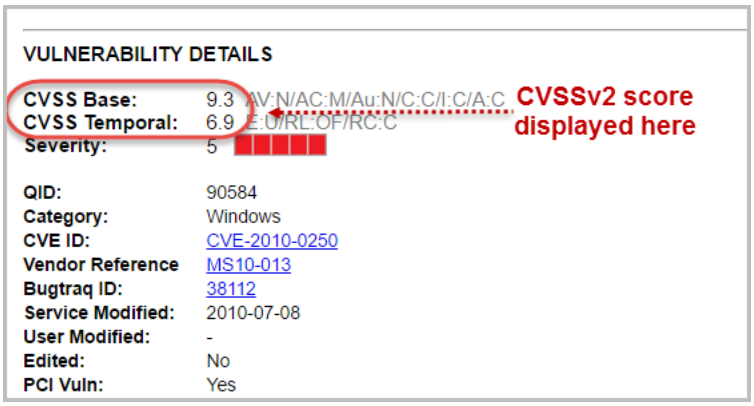
Choose CVSS Version for reports

While creating new report templates, you can choose to display the CVSS score for specific CVSS versions, such as CVSS version 2 or CVSS version 3. Selecting All (default) will display scores for both CVSS versions.

The CVSS version option is available in Scan, PCI Scan, and Patch templates.



Reports generated from these templates will display CVSS scores as per the selected option.

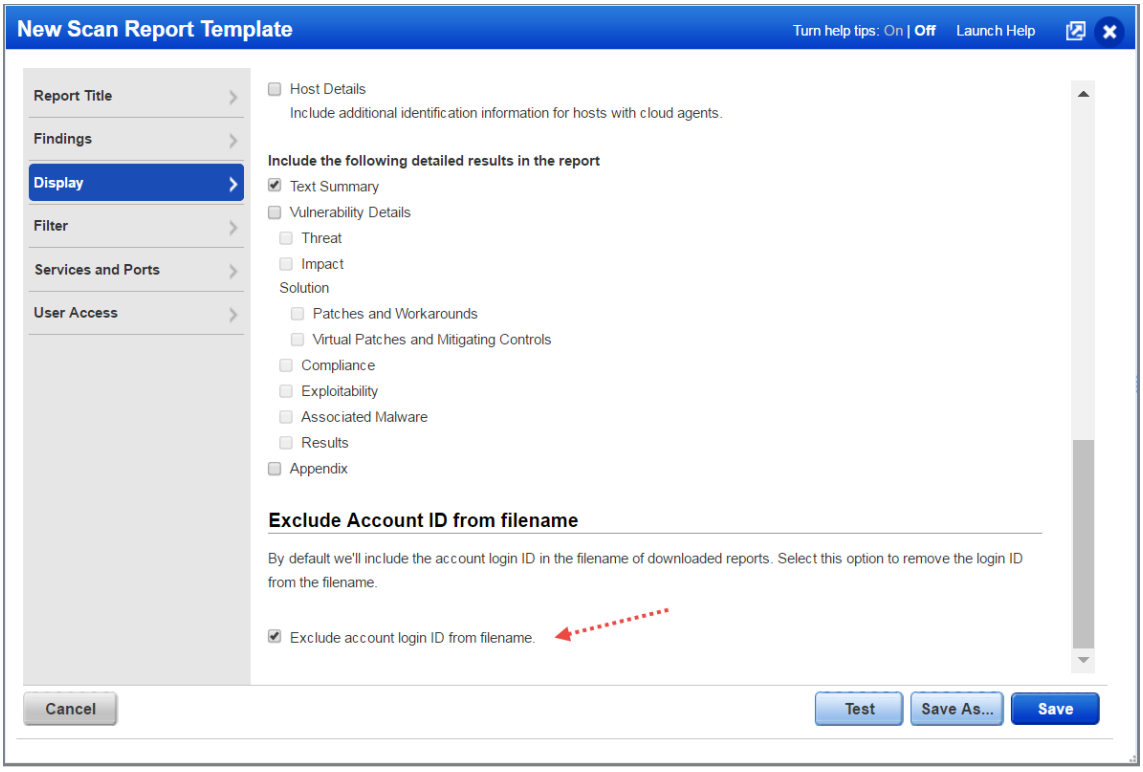


Selecting CVSSv2 will only display CVSS Base score and CVSS Temporal Score. While selecting CVSSv3, will only display CVSS3 Base score and CVSS3 Temporal Score. Whereas scores for both CVSS versions are displayed if you select All.

Exclude Account ID from report filename

By default we'll include the user's account login ID in the filename of reports you choose download. Now you have the option to exclude the account login ID from the filename. Just select the checkbox under Exclude Account ID from filename.

The Exclude Account ID from filename option is available in Scan, PCI Scan, Patch and Map templates.

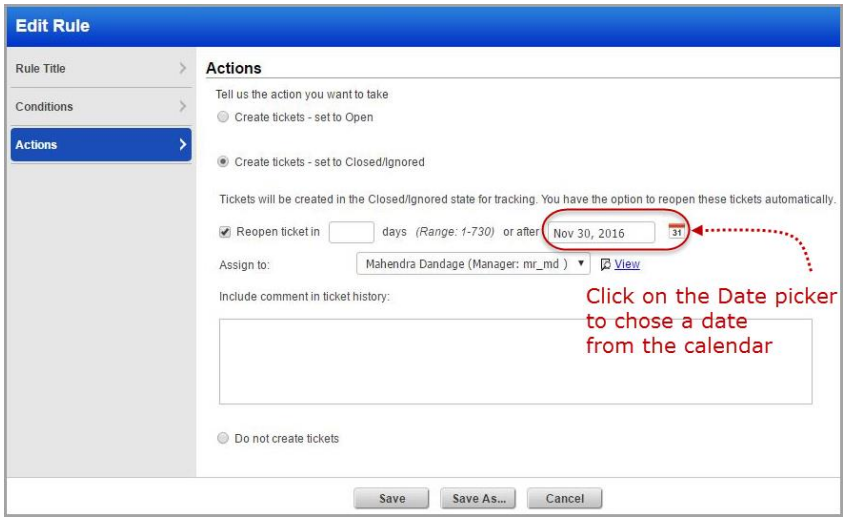


Set Date to Reopen Remediation Tickets

We now provide a date picker option to set a date for the remediation tickets to be reopened. You can preconfigure the date while you create or edit a policy rule or you could also edit an existing remediation ticket (only for closed/ignored status).

Good to know

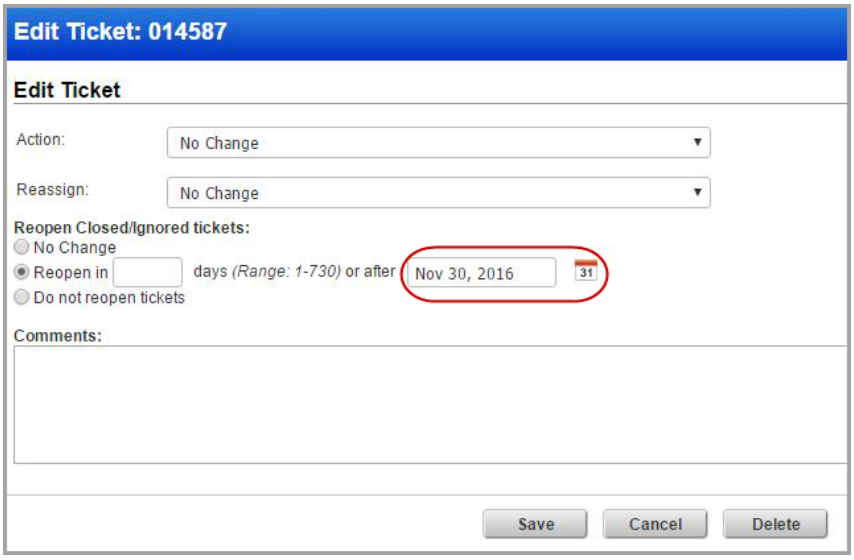
- The date picker option is available only for closed/ignored tickets.
- Select the Reopen ticket option for the date picker to be enabled.



Go to Remediation > Policies > click Edit from Quick Actions menu for an existing policy rule.

You can enable this option when you configure the Actions for the remediation ticket.

To assign a date for existing remediation tickets (in closed/ignored status), edit the ticket and select the Reopen option and then choose a date from the date picker.



Ignored Vulnerability Scorecard Report - removed size limit

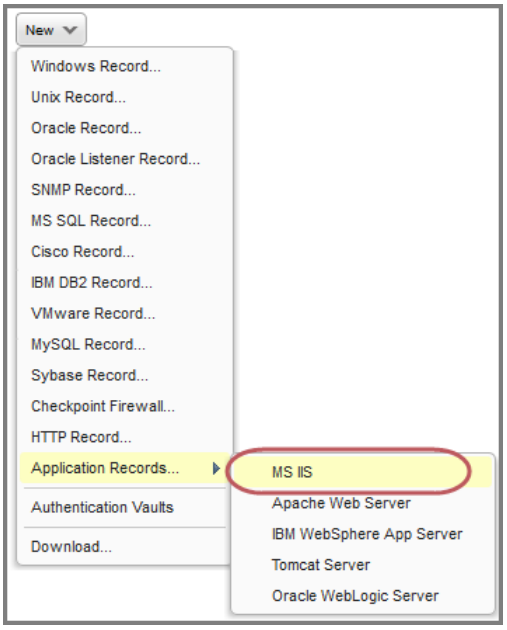
Previously the Ignored Vulnerability scorecard report showed a maximum of 10K rows. With this release this limit is removed.

Qualys Policy Compliance (PC)

MS IIS 10 Support

We've extended our support for Microsoft Internet Information Services (MS IIS) Web Server authentication to include version 10. We already support MS IIS versions 6.0, 7.x and 8.x for Windows.

You'll need an MS IIS authentication record to authenticate to your web server, and scan it for compliance. Windows authentication is required so you'll also need a Windows record for the host running the web server.



How do I get started?

- Go to Scans > Authentication.

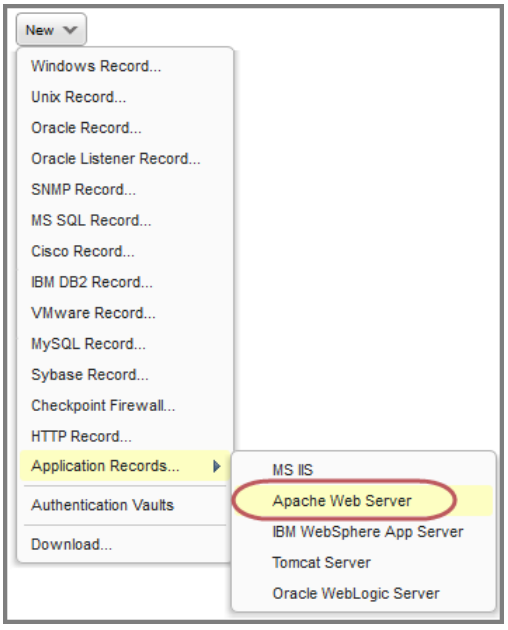
- Check that you have a Windows record already defined for the host running the web server.

- Create an MS IIS record for the same host. Go to New > Application Records > MS IIS.

Pivotal Web Server 6.x Support

We've extended our support for Apache Web Server authentication to include Pivotal Web Server 6.x. We already support these technologies: Apache HTTP Server 2.2 and 2.4, IBM HTTP Server 7.x and 8.x and VMware vFabric Web Server 5.x.

You'll need an Apache Web Server authentication record to authenticate to your web server, and scan it for compliance. Unix authentication is required so you'll also need a Unix record for the host running the web server.



How do I get started?

- Go to Scans > Authentication.

- Check that you have a Unix record already defined for the host running the web server.

- Create an Apache Web Server record for the same host. Go to New > Application Records > Apache Web Server.

Docker Authentication support for Application Records

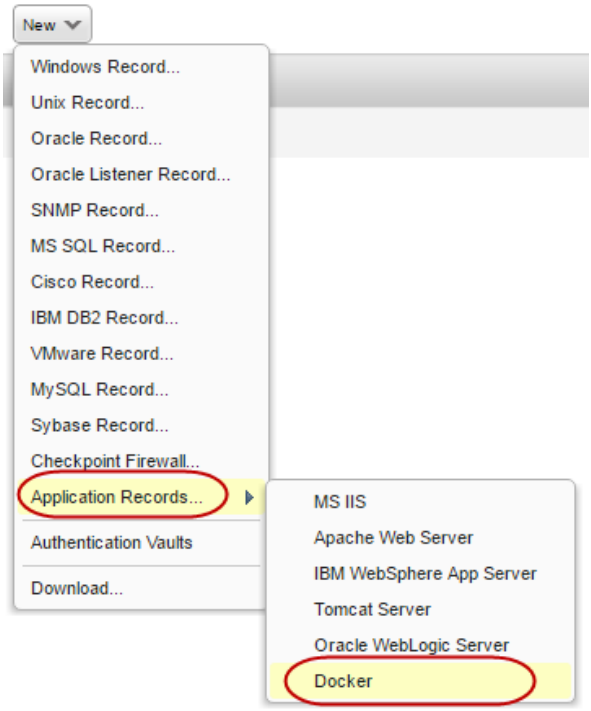
We now support compliance scans for Docker versions from 1.9 to 1.12, running on Linux hosts. Simply create a new Docker authentication record with details about your installation. Unix authentication is required so you'll also need a Unix record for the host running the docker.

Which technologies are supported?

- CentOS 7.x
- Debian 8.x
- Oracle Linux 6.x, 7.x
- RHEL 7.x
- OpenSUSE >=13.2
- SUSE 12.x
- Ubuntu >= 12.04(LTS)

How do I get started?

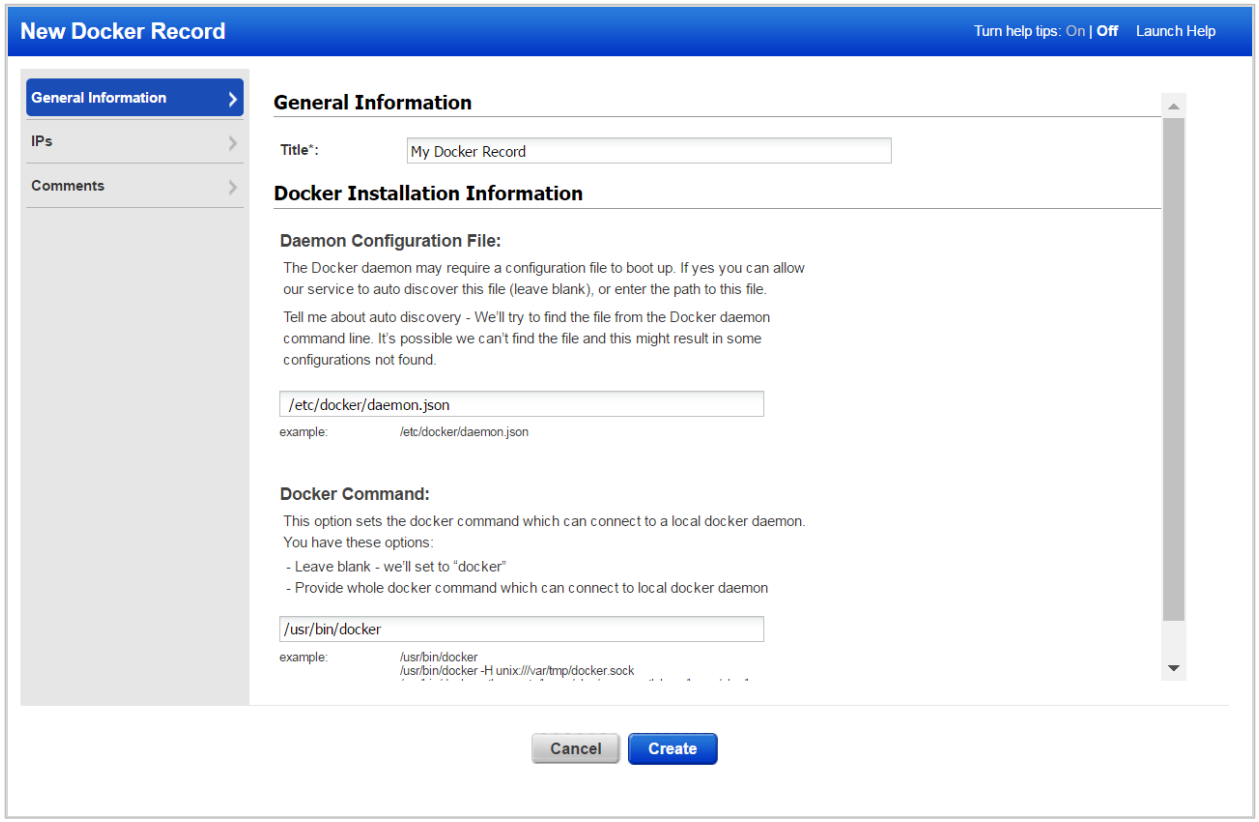
Simply navigate to Scans > Authentication and then go to New > Application Records > Docker.



Your Docker Record

For Docker installation, we need to know whether the Docker daemon requires a configuration file to boot up. If yes you can let our service auto discover this file or enter the path. Also the docker command. We have helpful information in the wizard to help you with these settings.

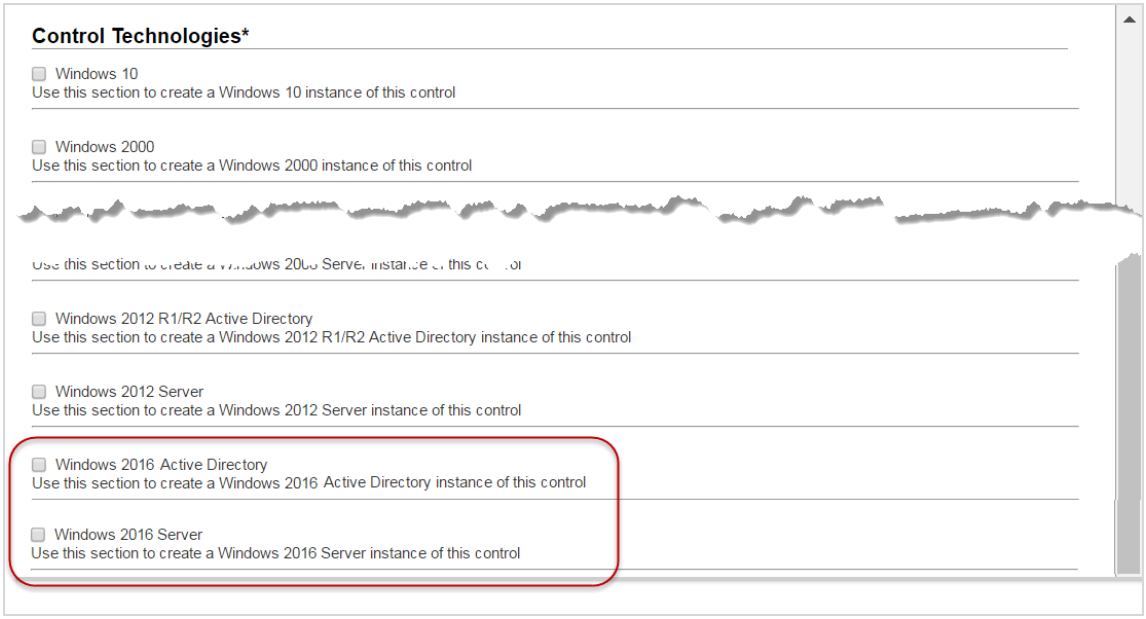
Unix authentication is required. Be sure that the IPs you assign to this record are already in a Unix record.



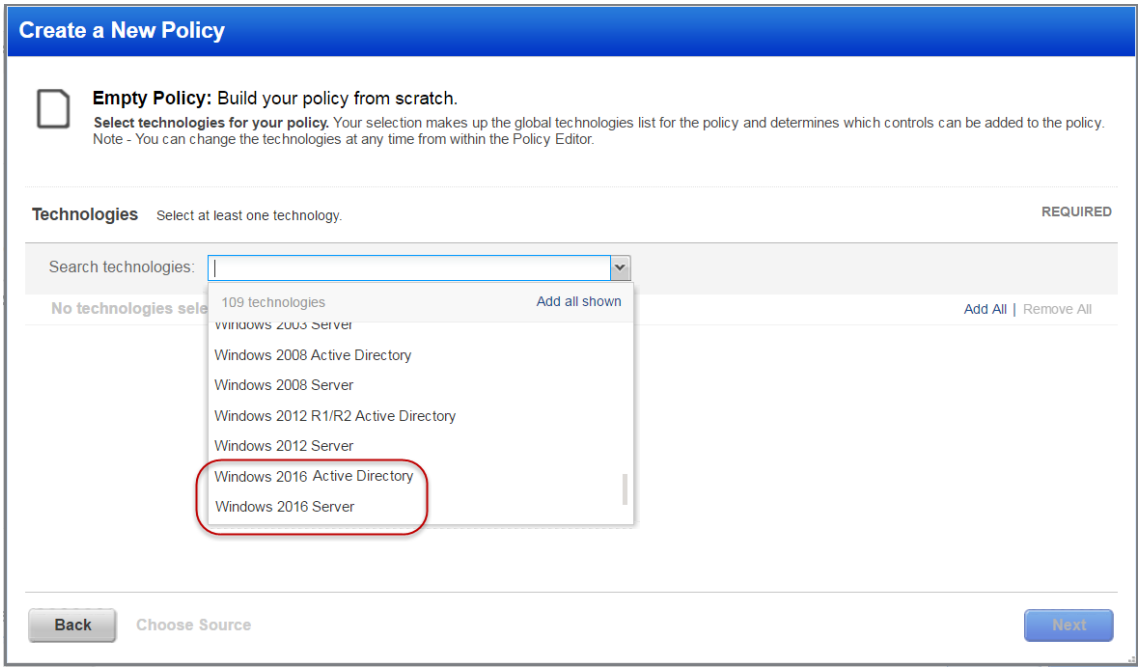
Support for Windows 2016 technologies

Windows 2016 Server and Windows 2016 Active Directory technologies are available for Windows user defined controls (UDCs).

Now you can select these technologies under Control Technologies when creating a Windows UDC.



When creating a policy these technologies are available from the Technologies list.



Issues Addressed

- Map and scan results in XML format now display the entire list of IP addresses for the Domain field.
- Remediation information for controls is now displayed in Policy report template, Policy compliance report, Policy interactive report, and UDC edit page.
- You can now successfully add QIDs for Patches & Software to the Scorecard Patch report.
- The Patch Report now runs successfully without getting stuck even for large reports.
- We added a tool tip and increased the column width to display the complete details of the cause for authentication failure.
- The Scanner Capacity graph under General Information for Scanner Appliance Information is now displayed properly.
- Netblock information is now shown correctly along with the domain name on the Asset Group Information page.
- Using the parameter asset_groups=All while launching a scan, will successfully perform the scan on all asset groups instead of throwing the error "Invalid Asset Groups (All)".
- Asset Groups are now filtered correctly based on the network selected on the Schedule Scan page.
- We've added a new "modified" date column in Scheduled Scan and Report lists. You can also search or sort the lists based on the modified date.
- We have now added "View Report" button in the deletion confirmation message for report template and option profile to tell you if the report template/option profile being deleted is linked to other scheduled tasks or not. If linked, the details of the scheduled tasks are provided.
- We fixed the vulnerability notification email to display correct text in the user-selected language.
- The list of TCP ports included in a Standard Scan is now up-to-date in the option profile. Click "View list" in the option profile to see the complete list of ports.
- We've fixed the error message that appears in Unix records when you enter one or more IP addresses that already exist in another Unix record. The message will now include the IPs and records causing the conflict.
- You can now add IPv6 addresses with "FD" hex in subscriptions with IPv6 Scanning enabled.
- Updated the online help for the Scan by Hostname feature to give users tips on how to report on IP addresses by hostname. You can perform an asset search on the "All" group and the hostname to identify the resolved IP addresses. Then it's easy to create an asset group from the asset search results in order to report on those IP addresses.