



# Qualys Cloud Platform (VM, PC) v8.x

## Release Notes

Version 8.16

December 14, 2018 (revised January 17, 2019)

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

### **Qualys Cloud Platform**

New Password Security Options

Auto Delete Storage Options Cannot be Disabled

Asset Search: New Filter for Last SCAP Scan Date

Scanner Appliances List - Renamed ID Column to Personalization Code

New Search Filters Available for Searching Scanners

### **Qualys Vulnerability Management (VM)**

Virtual Host Limit Increased

Quick Start Guide UI updates

### **Qualys Policy Compliance (PC/SCAP/SCA)**

Support for Scanning ESXi Hosts on vCenter

Apache Tomcat 9.x Support

IBM HTTP Server 9.x Support

OS Authentication Based Instance Technology Discovery

New Technologies Supported for Windows UDCs

Auto Update Expected Values from Agent Scans

New Instance column in STIG Report CSV

**Qualys 8.16 brings you many more improvements and updates! [Learn more](#)**

# Qualys Cloud Platform

## New Password Security Options

We've added several new password security options to enforce a strong password policy. Go to Users > Setup > Security to set password requirements for all users in the subscription. By default, you cannot reuse any of your last 13 passwords, but this option will become configurable in a future release.

The earlier version of the Cloud Suite 8.16 Release Notes failed to mention that with this release we are also enforcing a special characters requirement, by default, but this option too will become configurable in a future release.

**Password Security**

- ☐ Password expires after 1 months
- ☐ Lock account after 3 failed login attempts
- ☒ Allow user defined passwords
- ☒ Minimum length of password is 8 characters (Range: 8 - 16)
- ☐ Password must contain alpha and numeric characters
- ☐ Force password change at initial login
- ☐ Notify user to change password 1 days before expiration
- ☐ Allow users to change expired password at login
- ☒ Password must contain at least one lowercase letter
- ☒ Password must contain at least one uppercase letter
- ☒ Password must contain at least one numeric character
- ☒ Password must not contain 3 identical characters in a row

New password security options

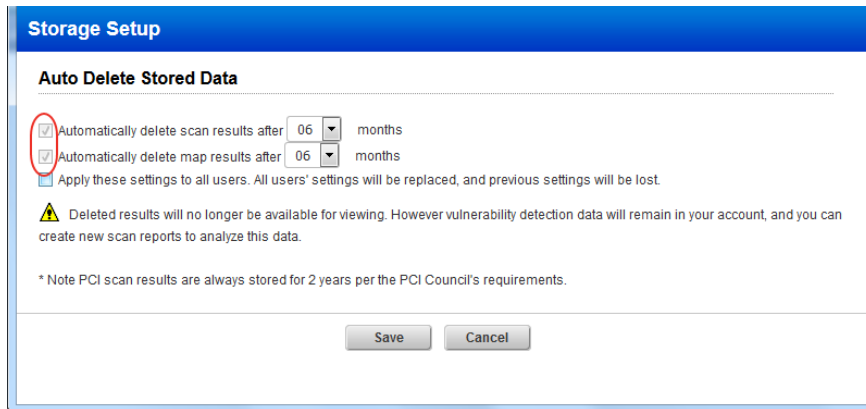
### Good to Know

For existing subscriptions, these new password security options are off by default.

For new subscriptions, these password security options are on by default.

## Auto Delete Storage Options Cannot be Disabled

You can no longer clear (un-check) the Automatically delete scan/map results options. This ensures that a retention policy for scan/map results is set. You can still change the time frame from 1-13 months (Enterprise accounts) or 1-6 months (other account types).




**Storage Setup**

**Auto Delete Stored Data**

☒ Automatically delete scan results after 06 months

☒ Automatically delete map results after 06 months

☐ Apply these settings to all users. All users' settings will be replaced, and previous settings will be lost.

 Deleted results will no longer be available for viewing. However vulnerability detection data will remain in your account, and you can create new scan reports to analyze this data.

\* Note PCI scan results are always stored for 2 years per the PCI Council's requirements.

Save Cancel

### What if I already cleared these options?

If the Automatically delete scan/map results options were cleared (un-checked) prior to this release, then you will not see a change. We recommend you select these options to set a retention policy for scan/map results.

### New users

The Automatically delete scan/map results options will be selected in new user accounts (this cannot be undone). The time frame is set to 6 months by default, except for Community Edition accounts where it's set to 3 months. You can change the time frame if you like.

## Asset Search: New Filter for Last SCAP Scan Date

Now you can search for assets based on when they were last scanned for SCAP compliance. Find assets that have been scanned within (or not within) a set number of days.

Vulnerability Management

Dashboard Scans Reports Remediation **Assets** KnowledgeBase Users

**Assets** Asset Groups Host Assets **Asset Search** Virtual Hosts Domains

**Search for**

☒ Assets ☐ Tags

Asset Groups:  [Select](#)

IPs/Ranges:  [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Include asset group titles in results

**With the following attributes**

DNS Hostname: ☐ beginning with

NetBIOS Hostname: ☐ beginning with

Tracking Method: ☐ IP address

Operating System: ☐ beginning with  [View](#)

Open Ports: ☐

Running Services: ☐  [Select](#)

QID: ☐  [Select](#)

with results: ☐ beginning with

Last Scan Date: ☐ within  the past  days

Last Scan Date (PC): ☐ within  the past  days

**Last Scan Date (SCAP): ☒ within  the past  days** **New Filter**

First Found Date: ☐ within  the past  days

Go to Assets > Asset Search, select the Last scanned date (SCAP) filter and specify the number of days. Click Search.

You'll see the last SCAP scan date in a new column in your Asset Search Report.

**Asset Search Report**

11/12/2018 at 03:39:08 PM (GMT+0530)

Manager: 123 Main St  
Bay Area, Delaware 2323  
United States of America

**Search Criteria**

Asset Groups: All

IPs/Ranges: -

DNS Hostname: -

EC2 Instance ID: -

NetBIOS Hostname: -

Tracking Method: -

Operating System: -

OS CPE: -

Open Ports: -

Running Services: -

QID: -

Last Scan Date: -

**Last Scan Date (SCAP): within 180 day(s)**

First Found Date: -

**Results ( 421 )**

<input type="checkbox"/>	IP Address	DNS Hostname	NetBIOS Hostname	OS	OS CPE	Tracking Network	First Found	Last Scan	Last Compliance Scan	Last SCAP Scan
<input type="checkbox"/>	10.10.10.10	bridge.qualys.com	WIN7-10-10	Windows 7 Ultimate Service Pack 1	[DNS]	Star Trek	03/01/2018	08/06/2018	07/27/2018	07/27/2018
<input type="checkbox"/>	10.10.10.10	win7-10-10	WIN7-10-10	Windows 7 Ultimate Service Pack 1	[DNS]	Star Trek	03/14/2018	08/28/2018	06/08/2018	06/08/2018
<input type="checkbox"/>	10.10.10.10	bridge.qualys.com			[IP]	Global Default Network		06/15/2018		06/15/2018
<input type="checkbox"/>	10.10.10.51		PAT-OSX109-P	MacOS X	[IP]	Star Trek	09/19/2017	08/28/2018	07/27/2018	07/27/2018
<input type="checkbox"/>	10.10.10.65	krb5.qualys.com		Linux 2.2-2.6	[IP]	Star Trek	10/05/2017	08/08/2018	07/27/2018	07/27/2018
<input type="checkbox"/>	10.10.10.77	com2k12dc.compliance2.qualys.com	COM2K12DC	Windows 2012	[IP]	Star Trek	10/06/2017	08/28/2018	07/27/2018	07/27/2018

## Scanner Appliances List - Renamed ID Column to Personalization Code

On the Appliances list, we renamed the ID column to Personalization Code to make it easier to identify the personalization code after adding a virtual scanner.

**Vulnerability Management** ▾

Dashboard Vulnerabilities **Scans** Reports Remediation Assets KnowledgeBase

**Scans** Scans Maps Schedules Appliances Option Profiles Authentication

New ▾ Search

Appliance	Personalization Code
My_Scanner	15409325474725
My_Scanner2	70498266513935

## New Search Filters Available for Searching Scanners

We added 2 new filters: Scanner Type and Platform Provider to improve our scanner search capability. Go to Scans > Appliances and click the Search button to find scanner appliances by scanner type or by the virtual platform on which the scanners are deployed.

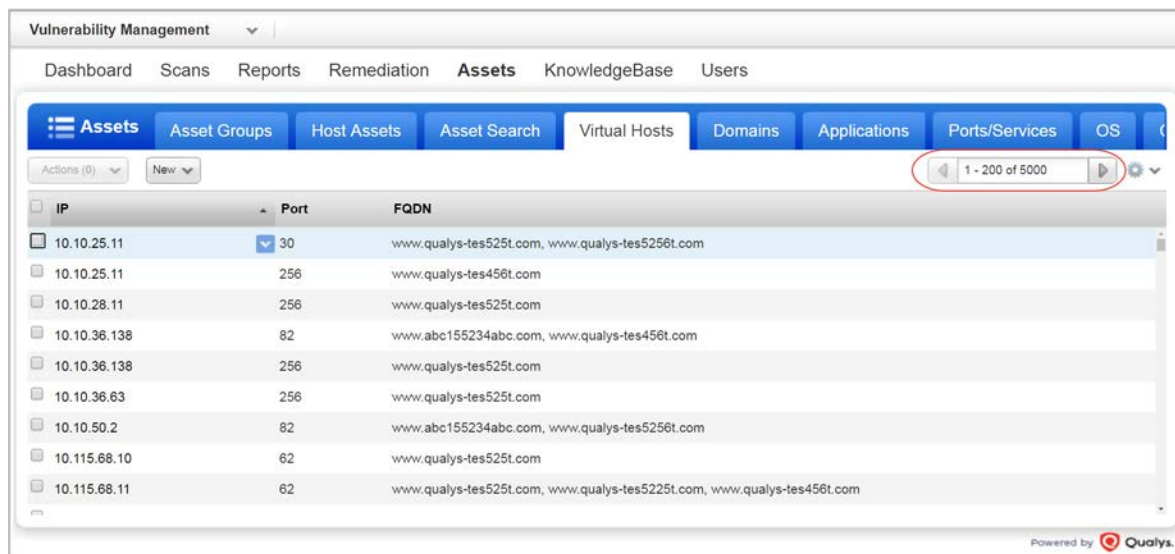
The screenshot displays the Nessus Scans page. The top navigation bar includes links for Dashboard, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. The Scans page is active, showing sub-tabs for Scans, Maps, Schedules, Appliances, Option Profiles, and Authentication. A red circle highlights the 'Search' button in the top navigation bar. A red arrow points from this button to a search modal window. The modal window has a blue header with the word 'Search' and a close button. It contains several input fields: 'Network' (with a dropdown menu showing 'All'), 'Title', 'SA S/N', 'LAN IP', 'Polling Interval', 'Scanner Version', 'Vulnerability Signatures', and 'Last Updated Since'. Below these fields are two sections: 'Scanner Type' with radio buttons for 'All', 'Offline', 'Physical', and 'Virtual', and 'Platform Provider' with a dropdown menu showing 'All' and a list of providers including Amazon EC2, Microsoft Azure Cloud Platform, Google Cloud Platform, OpenStack, and VMware vCenter. A red circle highlights the 'Scanner Type' and 'Platform Provider' sections.

## Qualys Vulnerability Management (VM)

### Virtual Host Limit Increased

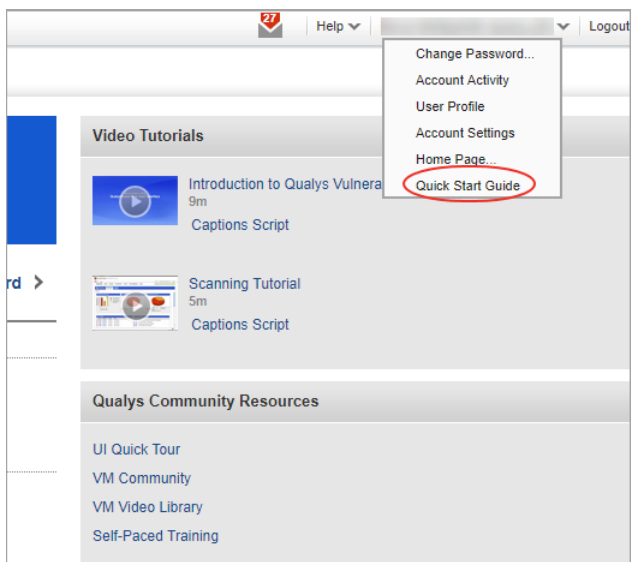
The number of virtual hosts you can add to your subscription increased from 1024 to 5000. To manage virtual hosts, go to VM > Assets > Virtual Hosts. Create a new virtual host from the New menu or edit an existing virtual host from the Quick Actions menu.

Permissions - When the VM application is enabled for the subscription, all Managers can create and edit virtual host configurations. Other users must be granted these extended permissions in their user account: Manage VM and Create/edit virtual hosts.



### Quick Start Guide UI updates

You'll notice updates to the Quick Start Guide page like new links to video transcripts, VM community and self-paced trainings.



# Qualys Policy Compliance (PC/SCAP/SCA)

## Support for Scanning ESXi Hosts on vCenter

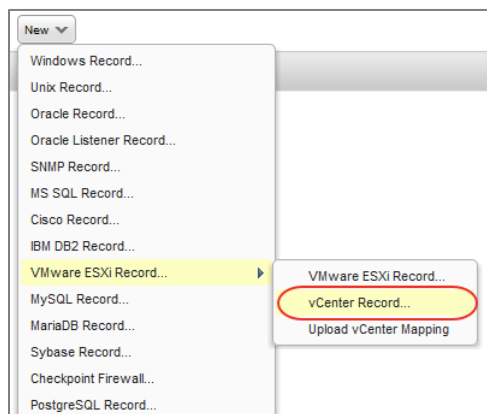
Looking for information on this feature? Our user guide will help you run Qualys Policy Compliance scans on your ESXi hosts through vCenter. [Click here](#) to download it.

We made UI changes to support this feature:

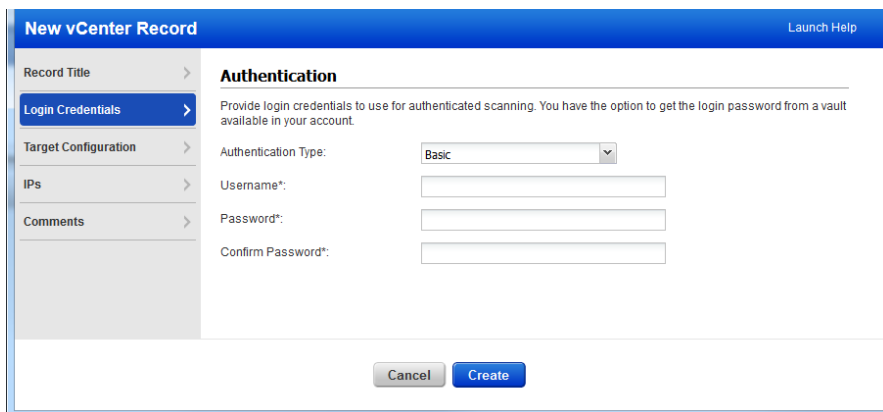
[vCenter Authentication Record](#) | [VMware Authentication Record](#) | [Upload vCenter Mapping File](#) | [Map Option for ESX/ESXi Host Discovery](#) | [View vCenter Mappings](#)

### vCenter Authentication Record

Go to Scans > Authentication > New > VMware ESXi Record > vCenter Record.

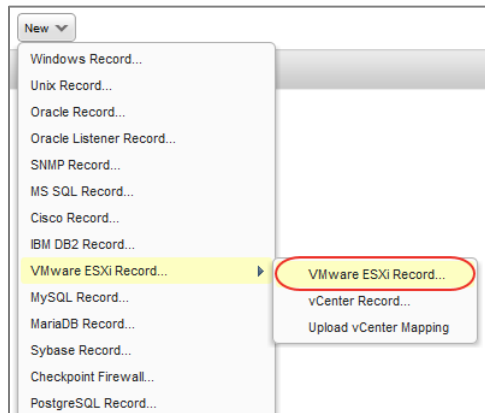


In the Login Credentials section, select the authentication type (Basic or Vault based) and enter credentials for your vCenter targets. In the Target Configuration section, update the settings to match your environment. In the IPs section, enter the target list of vCenter IPs/ranges.

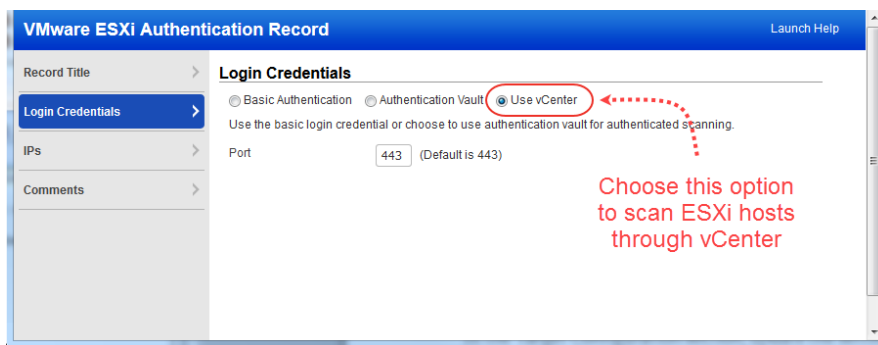


## VMware Authentication Record

Go to Scans > Authentication > New > VMware ESXi Record > VMware ESXi Record.



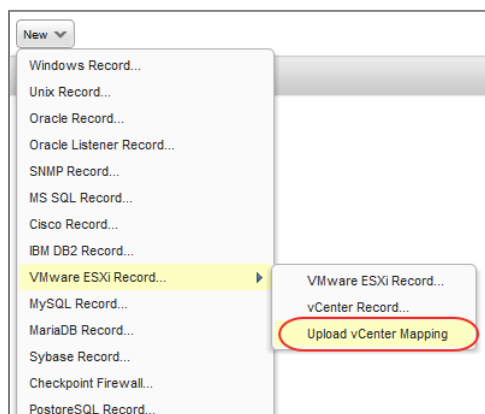
In the Login Credentials section, you'll see the new option "Use vCenter" for scanning ESXi hosts through vCenter. In the IPs section, add IP addresses/ranges for your target ESXi hosts.



## Upload vCenter Mapping File

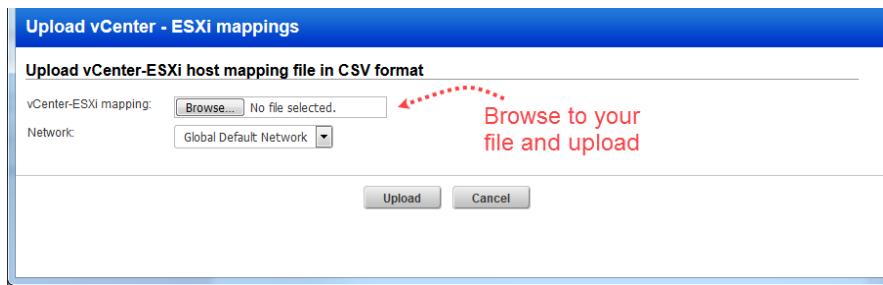
This option lets you upload a CSV file that contains mappings between a vCenter IP address and the ESXi host IP address that the vCenter manages. Any user with permission to create authentication records can upload mappings.

Go to Scans > Authentication > New > VMware ESXi Record > Upload vCenter Mapping.





Browse to your mapping file and click Upload.



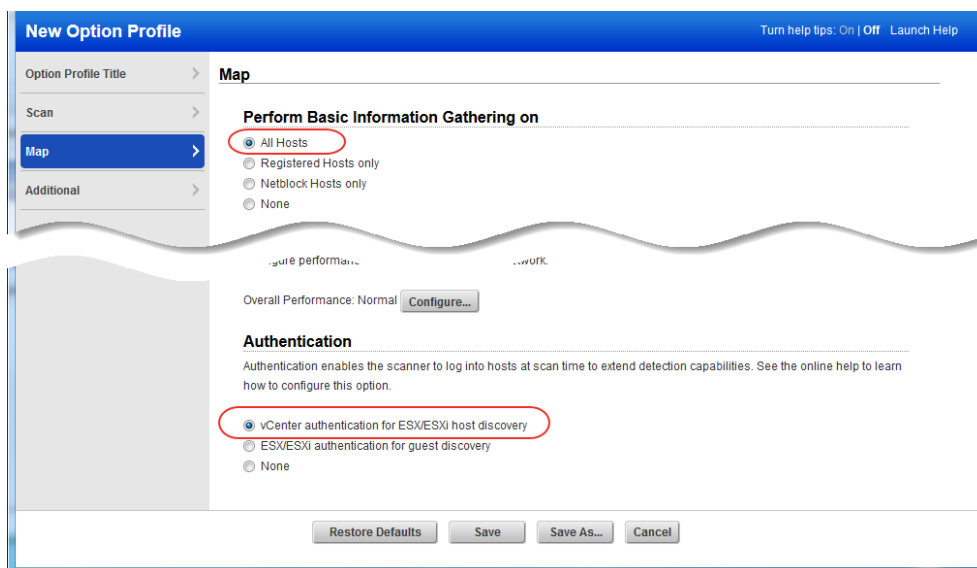
Requirements for the mapping file:

- 1) The vCenter map file has 2 required columns that can be in any order
  - Vcenter IP
  - ESXi IP
- 2) Additional columns are optional and can be in any order: Vcenter Name, ESXi System Name, Department, Location, LOB, System Type, OS Long, OS Short, Port
- 3) Column names are case sensitive

### Map Option for ESX/ESXi Host Discovery

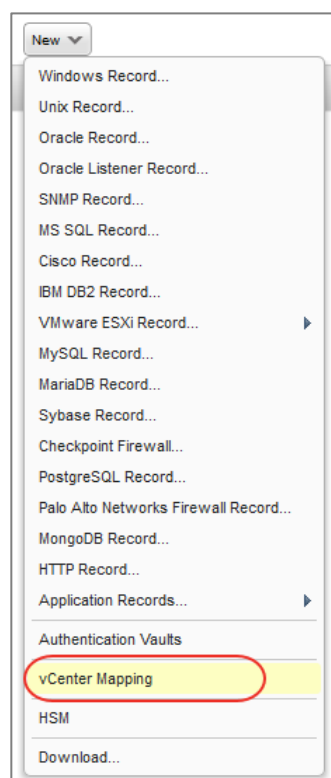
You can automatically discover ESX/ESXi hosts using the Qualys Map feature. We added a new option to the VM option profile to support this. Go to Scans > Option Profiles > New > Option Profile. Make these map settings (note that vCenter authentication is required):

- Perform Basic Information Gathering on: All Hosts
- Authentication: vCenter authentication for ESX/ESXi host discovery



[Click here](#) to download the user guide for complete information on how to run a discovery map scan and the vCenter credentials required.

## View vCenter Mappings



Go to Scans > Authentication > New > vCenter Mapping.

In the data list that appears, the Data Source column shows whether each mapping is from an uploaded file or from a discovery map scan.

vCenter ESXi Mapping Data				
Search				
1 - 16 of 16   Page 1 of 1				
VCenter IP	ESXi IP	Network	Data Source	Created Date
10.10.36.209	10.11.70.115	Network 1	Map scan	05/02/2018
10.10.34.104	10.10.34.196	Network 1	Map scan	05/02/2018
10.10.36.209	10.10.36.69	Network 1	Map scan	05/02/2018
10.10.36.209	10.10.35.107	Network 1	Map scan	05/02/2018
10.10.34.104	10.10.34.108	Network 1	Map scan	05/02/2018
10.10.36.20	10.11.70.1	Global Default Network	File	05/09/2018
10.10.38.30	10.11.70.10	Global Default Network	File	05/09/2018
10.10.36.20	10.10.36.6	Global Default Network	File	05/09/2018
10.10.36.20	10.11.70.1	Network 1	File	05/09/2018
10.10.36.20	10.10.36.6	Network 1	File	05/09/2018
10.10.38.30	10.11.70.10	Network 1	File	05/09/2018
10.10.36.209	10.10.36.69	Global Default Network	File	06/27/2018
10.10.36.209	10.11.70.115	Global Default Network	File	06/27/2018

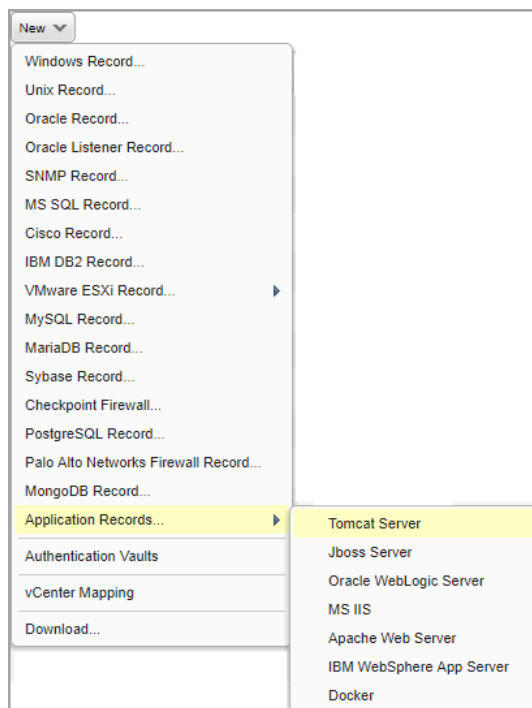
## Apache Tomcat 9.x Support

We've extended our support for Tomcat Server authentication to include Apache Tomcat 9.x for Windows and Unix. (See the help for other supported technologies.)

You'll need a Tomcat Server authentication record to authenticate to your web server, and scan it for compliance. You'll also need a Windows and/or Unix record for the host running the web server. The same record may include details for both Windows and Unix installations.

How do I get started?

- Go to Scans > Authentication.
- Check that you already have a record defined for each host running a tomcat server. For Windows hosts, a Windows record is required. For Unix hosts, a Unix record is required.
- Create a Tomcat Server record for the same host. Go to New > Application Records > Tomcat Server.



## Sample Reports

You'll see Apache Tomcat 9.x instances in compliance scan results and reports.

The screenshot displays two windows from a security tool. The left window, titled "Compliance Scan Results", shows scan details: Reference: compliance/1542088179.05213, External Scanners: vs\_qwebqa\_2 (Scanner 10.4.47-1, Vulnerability Signatures 2.1.2122-1), Duration: 00:08:35, Title: Apache TC 9 Unix, Asset Groups: Apache Tomcat 9 Unix, IPs: 10.10.32.162, Excluded IPs: -, and Compliance Profile: Initial PC Options. Below this is an "Appendix" section with "Target hosts found alive (IP)" listing 10.10.32.162, "Target distribution across scanner appliances" listing vs\_qwebqa\_2 : 10.10.32.162, and "Unix/Cisco/Checkpoint Firewall authentication was successful for these" listing 10.10.32.162. A red circle highlights the "Tomcat Server authentication was successful for these hosts" section, which lists "Apache TC 9 (Instance Path: /root/apache-tomcat-9.0.1) 10.10.32.162" and "Apache TC 9 (Instance Path: /root/apache-tomcat-9.0.1-inst2) 10.10.32.162". The right window, titled "Apache Tomcat 9 Unix", shows an "Asset Groups Summary" table with 3 of 3 Successful, 0 of 3 Failed, and 0 of 3 Not Attempted. Below is a "Results" section for "Apache Tomcat 9 Unix" (3 of 3 (100%)). It includes a table for "Unix/Cisco/Checkpoint Firewall" and a table for "Tomcat Server". The "Tomcat Server" table has two rows, both with a status of "Passed". A red circle highlights the "Tomcat Server" table.

Host	Host Technology	Instance	Status	Cause
10.10.32.162 (com-centos6.0-x86.qualys.com, -)	CentOS 6.x		Passed	-
Host	Host Technology	Instance	Status	Cause

Host	Host Technology	Instance	Status	Cause
10.10.32.162 (com-centos6.0-x86.qualys.com, -)	Apache Tomcat 9.x	Apache TC 9 9.0.1-inst2	Passed	-
10.10.32.162 (com-centos6.0-x86.qualys.com, -)	Apache Tomcat 9.x	Apache TC 9 9.0.1	Passed	-

## Policies and Controls

You'll see Apache Tomcat 9.x when creating new policies and searching controls.

The screenshot shows the "Create a New Policy" dialog. It has an "Empty Policy" section with instructions to build a policy from scratch. Below is a "Technologies" section with a search bar and a list of 164 technologies. A red circle highlights "Apache Tomcat 9.x" in the list, with a red arrow pointing to it and the text "Create policy for this technology". At the bottom are "Back", "Choose Source", and "Next" buttons.

Search technologies:  Add All | Remove All

No technologies selected

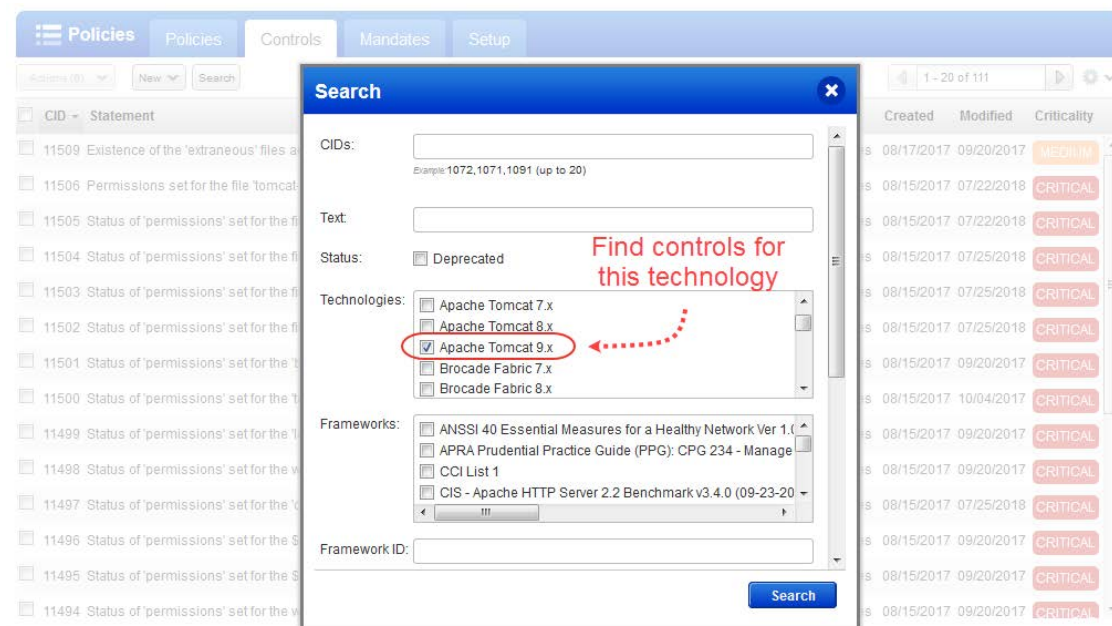
164 technologies

- Apache Tomcat 6.x
- Apache Tomcat 7.x
- Apache Tomcat 8.x
- Apache Tomcat 9.x
- Brocade Fabric 7.x
- Brocade Fabric 8.x
- CISCO ACS

Back Choose Source Next

## Search Controls

You'll see Apache Tomcat 9.x when searching controls by technologies.



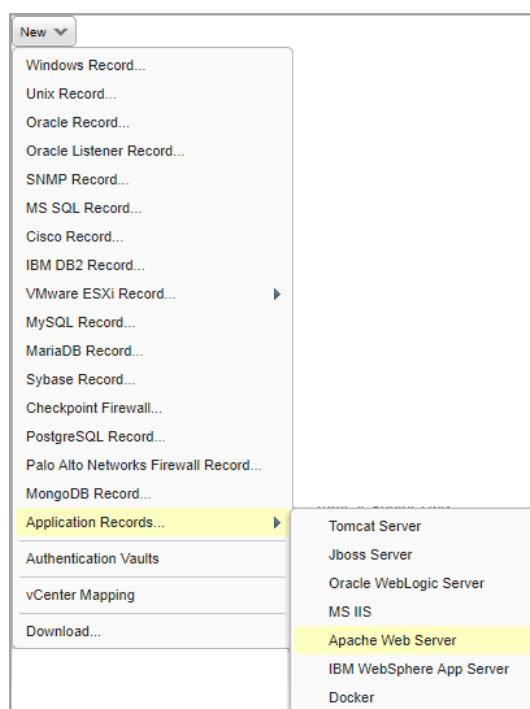
## IBM HTTP Server 9.x Support

We've extended our support for Apache Web Server authentication to include IBM HTTP Server 9.x. We already support these technologies for Unix: Apache HTTP Server 2.2 and 2.4, IBM HTTP Server 7.x and 8.x and VMware vFabric Web Server 5.x, Pivotal Web Server 6.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.



## Sample Reports

You'll see IBM HTTP Server 9.x instances in compliance scan results and reports.

The screenshot displays the 'Compliance Scan Results' interface. On the left, the 'Appendix' section lists target hosts and successful authentication results for various services. On the right, the 'IBM Http Server 9' results are shown, including an 'Asset Groups Summary' and a 'Results' table.

**Appendix**

- Target hosts found alive (IP)**  
10.10.30.38, 10.10.35.241, 10.11.70.118
- Target distribution across scanner appliances**  
vs\_qwebqa\_2 : 10.10.30.38, 10.10.35.241, 10.11.70.118
- Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts**  
10.10.30.38, 10.10.35.241, 10.11.70.118
- Apache Web Server authentication was successful for these hosts**  
Instance Name: IHS 7:1:/opt/IBM/HTTPServer/conf/httpd.conf  
10.10.30.38  
Instance Name: IHS 8:1:/opt/IBM/HTTPServer/conf/httpd.conf  
10.10.35.241  
Instance Name: IHS 9:1:/opt/IBM/HTTPServer/conf/httpd.conf  
10.11.70.118

**IBM Http Server 9**

**Asset Groups Summary**

Asset Group	Count	Success Rate
IBM Http Server 9	2 of 2	100% Successful
	0 of 2	0% Failed
	0 of 2	0% Not Attempted

**Results**

**IBM Http Server 9** 2 of 2 (100%)

**Unix/Cisco/Checkpoint Firewall**

Host	Network	Host Technology	Instance	Status	Cause
10.10.30.38 (-, -)	Gyan-Network-1	Oracle Enterprise Linux 7.x		Passed	-
10.11.70.118 (-, -)	Gyan-Network-1	Oracle Enterprise Linux 7.x		Passed	-

**Apache Web Server**

Host	Network	Host Technology	Instance	Status	Cause
10.10.30.38 (-, -)	Gyan-Network-1	IBM HTTP Server 9.x	/opt/IBM/HTTP	Passed	-
10.11.70.118 (-, -)	Gyan-Network-1	IBM HTTP Server 9.x	/opt/IBM/HTTP	Passed	-

## Policies and Controls

You'll also see IBM HTTP Server 9.x in the technologies list when creating a new policy.

The screenshot shows the 'Create a New Policy' dialog. It includes an 'Empty Policy' section and a 'Technologies' section where users can select technologies for their policy. A red circle highlights 'IBM HTTP Server 9.x' in the list, with a red arrow pointing to it and the text 'Create policy for this technology'.

**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 selected | 164 technologies | [Add all shown](#)

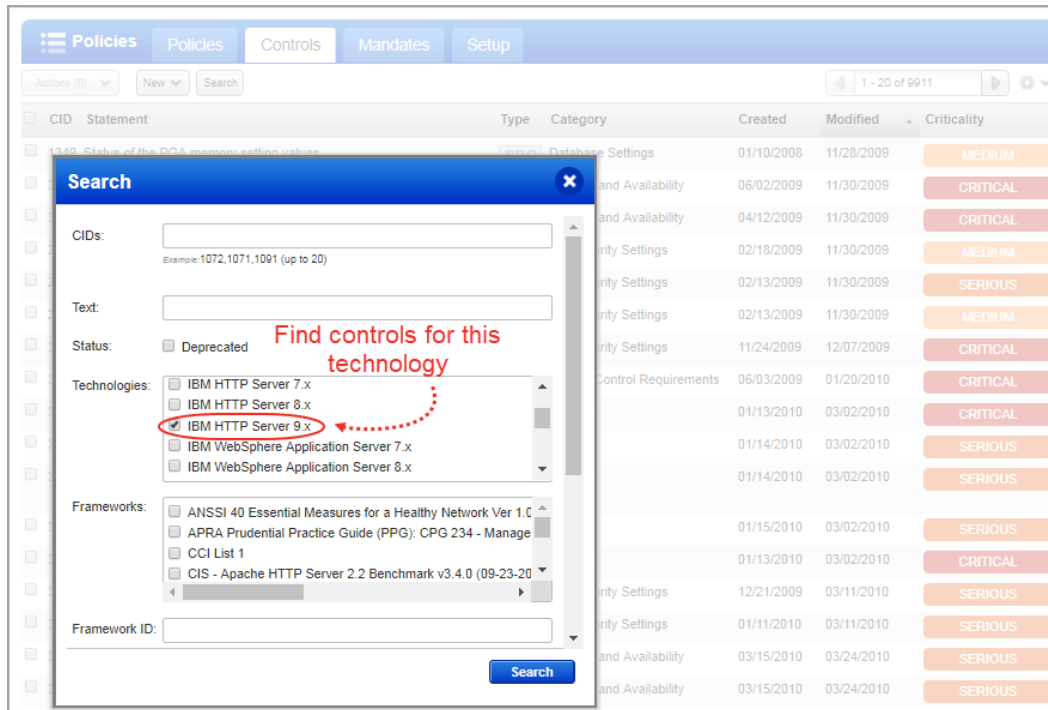
- IBM DB2 9.x
- IBM HTTP Server 7.x
- IBM HTTP Server 8.x
- IBM HTTP Server 9.x**
- IBM WebSphere Application Server 7.x
- IBM WebSphere Application Server 8.x

[Back](#) [Choose Source](#) [Next](#)

Create policy for this technology

## Search Controls

You'll see IBM HTTP Server 9.x when searching controls by technologies.



## OS Authentication Based Instance Technology Discovery

You can now collect technology data using the underlying OS technology instance without creating authentication records.

We support for the following technologies based on OS (Windows/Unix) authentication:

- Google Chrome
- Internet Explorer (9, 10, 11)
- IBM WebSphere MQ
- Microsoft Office (2013, 2016)
- Microsoft Office Access (2013, 2016)
- Microsoft Office Excel (2013, 2016)
- Microsoft Office Outlook (2013, 2016)
- Microsoft Office PowerPoint (2013, 2016)
- Microsoft Office Word (2013, 2016)
- Mozilla Firefox
- Splunk (6.x, 7.x)

You can view the information in Scan Reports and Policy Compliance Authentication Reports.

## Scan Reports

A new section "Application technologies found based on OS-level authentication", is added to the scan report. This section lists all the OS auth-based instance technologies and targets.

Application technologies found based on OS-level authentication	
Google Chrome was found for these hosts	
Google Chrome	10.10.36.126
IBM WebSphere MQ was found for these hosts	
IBM WebSphere MQ (Installation Path: /opt/mqm)	10.11.70.116
Internet Explorer was found for these hosts	
Internet Explorer 9	10.10.30.130
Internet Explorer 10	10.10.34.123
Internet Explorer 11	10.10.36.126
Microsoft Office was found for these hosts	
Microsoft Office 2013	10.10.34.123

## Policy Compliance Authentication Reports

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

**New Authentication Report** [Launch Help](#)

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

**Report Details**

Title:

Report Format: \*

**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](#)

**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)

**Appendix**

☒ OS Authentication-based Technology

**Report Options**

☐ Scheduling

The Appendix section is displayed in report as such:

▼ Appendix

▼ Targets with OS authentication-based technologies

▼ 10.10.34.123 (cw2k12sd-34-123, CW2K12SD-34-123)

OS:	Windows Server 2012 Standard 64 bit Edition	Last Auth:	10/17/2018 at 03:00:32 PM (GMT-0700)
Network:	Global Default Network	Last Success:	10/17/2018 at 03:00:32 PM (GMT-0700)
S.N.	Host Technology	Instance	
1.	Microsoft Office PowerPoint 2013	Microsoft Office PowerPoint 2013	
2.	Microsoft Office Word 2013	Microsoft Office Word 2013	
3.	Microsoft Office 2013	Microsoft Office 2013	
4.	Mozilla Firefox (Windows)	Mozilla Firefox	
5.	Internet Explorer 10	Internet Explorer 10	
6.	Microsoft Office Access 2013	Microsoft Office Access 2013	
7.	Microsoft Office Excel 2013	Microsoft Office Excel 2013	
8.	Microsoft Office Outlook 2013	Microsoft Office Outlook 2013	

▼ 10.10.35.249 (-, -)

OS:	CentOS Linux 7.0.1406	Last Auth:	10/17/2018 at 03:00:46 PM (GMT-0700)
Network:	Global Default Network	Last Success:	10/17/2018 at 03:00:46 PM (GMT-0700)
S.N.	Host Technology	Instance	
1.	Splunk 6.x (Unix)	Splunk 6.x (Installation Path: /opt/splunk6/splunk)	
2.	Splunk 7.x (Unix)	Splunk 7.x (Installation Path: /opt/splunk)	

## New Technologies Supported for Windows UDCs

Want to create a UDC for Windows Embedded 7, 8 and 8.1? Go to Policies > Controls > New > Control and select any of the Windows control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology.

**Control Technologies\***

☐ Windows 10  
Use this section to create a Windows 10 instance of this control

☐ Windows 2000  
Use this section to create a Windows 2000 instance of this control

☐ Windows 2003 Active Directory  
Use this section to create a Windows 2003 Active Directory instance of this control

☐ Windows 2003 Server  
Use this section to create a Windows 2003 Server instance of this control

☐ Windows 2008 Active Directory  
Use this section to create a Windows 2008 Active Directory instance of this control

☐ Windows 2008 Server  
Use this section to create a Windows 2008 Server instance of this control

☐ Windows 8.1  
Use this section to create a Windows 8.1 instance of this control

☐ Windows Embedded 7  
Use this section to create a Windows Embedded 7 instance of this control

☐ Windows Embedded 8  
Use this section to create a Windows Embedded 8 instance of this control

☐ Windows Embedded 8.1  
Use this section to create a Windows Embedded 8.1 instance of this control

☐ Windows Server 2012 R2  
Use this section to create a Windows Server 2012 R2 instance of this control

New technologies supported

CreateCancel



You'll see Windows Embedded 7, 8 and 8.1 in the technologies list when creating a policy.

**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:  Add All | Remove All

No technologies selected 162 technologies Add all shown

- Windows 8
- Windows 8.1
- Windows Embedded 7
- Windows Embedded 8
- Windows Embedded 8.1
- Windows Server 2012 R2

Back Choose Source Next

## Auto Update Expected Values from Agent Scans

You can now choose to update a control's expected values with the actual values collected from each cloud agent scan.

To enable this option, go to Directory Integrity Check > Agent Scan and select the Auto Update expected value option. You must also enable "Use scan data as expected value" in this control (under Control Technologies tab).

**New Control: Directory Integrity Check** Turn help tips: On | Off Launch Help

**General Information** >

**Scan Parameters** >

**Control Technologies** >

**References** >

**Agent Scan** >

**Agent Scan Options**

**Use agent scans only**  
Want to define the Base Directory using wildcards?  
This option must be selected and this control will only be evaluated using agent scan data.  
☐ Use agent scans only

**Auto Update expected value**  
When enabled, we'll update this control's expected value with the actual value collected from each cloud agent scan. You must also enable "Use scan data as expected value" in this control (under Control Technologies).  
To create reports reflecting results for each agent scan, schedule your compliance reports to run in between the scan interval defined for your agents.  
☒ Auto Update expected value

Cancel Create

You'll also see this option in File Integrity Checks in the Agent Scan Options section.

## New Instance column in STIG Report CSV

A host can have multiple instances and you can now include the host instance in the STIG report. Simply choose “Instance” in the STIG report template to include instance in the report.

The screenshot shows the 'New Stig Report Template' window. The 'Layout' tab is active. Under the 'Host' section, the 'Instance' checkbox is checked and highlighted with a red circle. Other sections include 'Control' (with 'Rationale', 'Evidence', and 'Extended Evidence' checkboxes), 'Remediation Info' (with 'For Failed Controls', 'For Passed Controls', and 'For Error Controls' checkboxes), and 'Rule' (with 'Rule Description', 'CCI', and 'Rule Posture' checkboxes). The 'Compliant Rule Statistics By Severity' and 'Host Statistics' sections are also visible.

## Sample CSV Report

Scroll down to the RESULTS section and you'll see the new Instance column at the end.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
218	HOST STATISTICS																			
219	IP Address	Tracking Me	DNS Name	Netbios N Asset Tag: Operating Last Scan   Compliant Non-com   Not Score Rule Com   Vuln Com   Compliant Rule Stats by Severity																
220	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Ag1,BU1,V	Windows 07/30/201	66	136	1	32.51%	(6)	32.51%	(6)	CAT I (High)	15.15%	CAT II (Medium)	74.24%	CAT III (Low)	10.61%		
221	COMPLIANT RULE STATISTICS BY SEVERITY																			
222	CAT I (High)	CAT II (Medi	CAT III (Low)																	
223	15.15%	(10/6)	74.24%	(49/6)	10.61%	(7/66)														
224	RESULTS																			
225	IP	Tracking Me	DNS Hostnam	NetBIOS F	Operating Rule ID	Rule Title	Severity	Rule Post	CCI	Vuln ID	Vuln Title	Vuln Post	Control	Evaluation Date	Control St	Rationale	Evidence	Remediat	Instance	
226	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-18394r	User right	CAT II (Me Non-com)	CCI-00036	V-1103	User Right Non-com	2401	10/26/2018	23:07	FAIL	The 'Sync	The	Configure	os		
227	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-18394r	User right	CAT II (Me Non-com)	CCI-00036	V-1103	User Right Non-com	2198	10/26/2018	23:07	FAIL	The 'Deny	The	To	os		
228	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-18394r	User right	CAT II (Me Non-com)	CCI-00036	V-1103	User Right Non-com	2384	10/26/2018	23:07	FAIL	The 'Force	The	To	os		
229	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-18394r	User right	CAT II (Me Non-com)	CCI-00036	V-1103	User Right Non-com	2642	10/26/2018	23:07	FAIL	The 'Impe	The	To	ad2008		
230	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-18394r	User right	CAT II (Me Non-com)	CCI-00036	V-1103	User Right Non-com	3925	10/26/2018	23:07	FAIL	The 'Chan	The	To	os		
231	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-47143r	The Deny	CAT II (Me Non-com)	CCI-00021	V-26486	Deny log c Non-com	2200	10/26/2018	23:07	FAIL	The 'Deny	The	To	os		
232	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-29493r	File Trans	CAT II (Me Complian)	CCI-00036	V-1120	Prohibit	Complian	3780	10/26/2018	23:07	PASS	The 'Micr	The	Configur	os	
233	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-83309r	The Micro	CAT II (Me Complian)	CCI-00038	V-26602	Microsoft	Complian	3780	10/26/2018	23:07	PASS	The 'Micr	The	Configur	os	
234	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-41837r	Domain C	CAT II (Me Non-com)	CCI-00241	V-4407	LDAP Sign Non-com	1432	10/26/2018	23:07	FAIL	The 'LDAP	This	Configure	os		
235	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-29392r	The Windi	CAT II (Me Complian)	CCI-00241	V-6833	SMB Serve Complian	1189	10/26/2018	23:07	PASS	The 'Micr	This	To	os		
236	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-34591r	The Windi	CAT III (Lo Non-com)	CCI-00004	V-26359	Legal Ban Non-com	1134	10/26/2018	23:07	FAIL	Login/Logi	The	To	os		
237	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-29545r	Named Pl	CAT I (Hig Complian)	CCI-00109	V-6834	Anonymo Complian	1434	10/26/2018	23:07	PASS	The 'Anon	This	To	os		
238	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-29681r	Users with	CAT I (Hig Non-com)	CCI-00036	V-1140	Users with Non-com	2521	10/26/2018	23:07	FAIL	Members	The	Configur	ad2008		
239	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-47874r	Only admi	CAT I (Hig Non-com)	CCI-00223	V-1127	Restricted Non-com	2521	10/26/2018	23:07	FAIL	Members	The	Configur	ad2008		
240	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-29437r	Internet C	CAT III (Lo Non-com)	CCI-00038	V-15673	Internet C Non-com	4095	10/26/2018	23:07	FAIL	The Windi	This	To establ	os		
241	10.10.10.46	IP address	ex2010sp1-10	EX2010SP: Windows	SV-29007r	Automati	CAT II (Me Non-com)	CCI-00036	V-1145	Disable A Non-com	1169	10/26/2018	23:07	FAIL	Automati	This	To	os		

## Issues Addressed

- We fixed an issue in Host Based Scan Reports where EC2 data was not shown in XML and CSV report outputs for certain customers.
- We fixed an issue in Host Based Scan Reports where the EC2 instance ID was missing for some EC2 assets when other EC2 metadata was shown.
- We fixed an issue in Host Based Scan Reports where no data was shown when the report was generated by non-Manager users and the report target included only asset tags.
- We fixed an issue so that the count for ignored and disabled QIDs is in sync for VM and other modules such as AssetView.
- Editing or adding tags in scorecard report template is now functioning correctly and the report also correctly displays the tags added/edited in the report template.
- When we add large IP set on an existing account with large number of existing IPs, we now observe a message saying “processing” instead of displaying a blank window.
- We now display the correct error message in case of lack of scanner appliances associated with IP range when you launch a scan.
- In the Permissions tab of Windows Directory Search UDC, the advanced permissions window is opened successfully after clicking ‘Show advanced permissions’ option.
- Fixed an issue where a patch report in CSV and XML showed discrepancies in “Published Date”. The format is now fixed to mm/dd/yyyy hh:mm:ss.
- We have fixed an issue for Consultant UI and email address is now saved successfully for the user.
- We have fixed an issue where password tips text for minimum password length on the Change Password page was not showing the length that is set in the subscription settings.
- We will now send an email notification to the user when a scan is skipped due to tag related exceptions.
- We improved the way a MongoDB instance string appears in the Policy Editor for better readability. For example, the string MongoDB 3.x:27019:admin will now appear as MongoDB 3.x (Port: 27019, Database: admin).
- The discrepancy between the count of target IPs and alive hosts in VM scan results and scan preview is fixed.
- Fixed a data discrepancy issue between VM and AssetView related to the number of vulnerabilities detected for an asset. Now, when an unauthenticated scan is run, we include all QIDs of the previous authenticated scan.
- The issue of invalid FQDN error displayed when adding a DNS hostname according to the latest RFC compliance to an asset group is fixed.
- We fixed an issue where on saving a dynamic search list as a static list, an error was displayed that no QIDs are available in the dynamic search list. Now QIDs are displayed.
- The error message displayed while trying to include the IPs already present in another Windows Auth record is now modified to mention the list of IPs you are trying to add.
- The control table in the CSV report attached to the Latest Controls email notification being sent to users is now displayed only once and not being duplicated.

- We fixed an issue where a dummy username was shown in the Modified by field in the Asset Group information. This dummy username was getting assigned when modified details were updated due to correction in asset group mapping made by the internal system. Now we are displaying a valid username.
- We now display correct tracking methods on policy report Rerun for single instance report source.
- The chosen Home Page is now displaying properly after login.
- A proper error message is now displayed when a user reaches the maximum limit of IPv4-IPv6 mappings.
- We have now fixed the overlapping text between Instance and Evaluation Date in MHT format of Policy report.
- Now when you create a File Integrity Check window control, the Hash Type scan parameter is displayed with an appropriate label name in the control information.
- Fixed an issue where an improper message was displayed when a user tries to remove VM or PC IPs which are also present in CertView.
- We have now added a new error message while removing any IP from VM / PC module: "We'll remove these IPs from your Vulnerability Management, Policy Compliance, Secure Config Assessment license based on your selection. In case you have Cloud Agent enabled, you must go to the Cloud Agent (CA) app and uninstall the agents associated with the hosts you want to remove. Once removed, IPs will no longer be available for scanning and reporting."
- The issue of policy compliance authentication error message getting truncated in the log file is now fixed.
- Various issues related to auth record functions like create, update, and list are now fixed. Also, error and success messages on UI and API are updated to be consistent.
- Now users are not allowed to reset their password through the "Forgot Password" link if the subscription has expired.
- Now Scan API displays the target list in the Activity log when multiple scanners are defined.
- We fixed an issue in the VM Detection API (/fo/asset/host/vm/detection/) where we set the wrong value for id\_min in the next URL that we provide in the output and this caused some host ids to be skipped.
- We fixed an issue where Reader users did not see any option profiles when listing option profiles from the API. This is fixed for VM, PC and PCI option profiles lists.
- We fixed an issue where non-Manager users did not see any System option profiles in the output when listing option profiles from the API. This is fixed for VM, PC and PCI option profiles lists.
- In the XML response of KnowledgeBase API, we are now showing CVSS Score for QIDs that have CVSS Base Score of 0 (zero).
- We improved UI screen text on the Vulnerability Notification tab when configuring a Distribution Group to clearly state that the notification is for new/updated vulnerabilities in the KnowledgeBase, not new/updated vulnerability detections.
- Appropriate tool tip is now displayed on mouse over for Root delegation information.
- We fixed a typo in the Delete Network confirmation message.

- For accounts with iDefense Threat Intelligence enabled - We fixed an issue where Vulnerability Details and Impacted Hosts were not loading when users viewed the threat report and the Doc ID is N/A.
- We fixed the Launch Help link for Unix Directory Search Check controls.