Table of Contents

About this guide................................................................. 4
  About Qualys ..................................................................... 4
  Qualys Support .............................................................. 4

Get Started ........................................................................ 5
  Pre-requisites .................................................................... 5
  Download and Install the App ........................................... 5
  Configure the App ........................................................... 7
    VM Detection Data .......................................................... 8
    Policy Compliance Data .................................................. 9
    WAS Findings ................................................................. 10
    Container Security Data Settings for Images .................. 10
    Container Security Data Settings for Containers ............ 11
    Proxy Configuration ...................................................... 11
  Configure Data Sync ........................................................ 12
  Enable the Data Feed to Start in Splunk .......................... 13
  How to setup for a Search Head Cluster ......................... 14
  How to get the RESULTS field indexed in host detection input ... 14
  How to populate the SOLUTION section in the KB lookup file ... 14

View your Qualys Data in Splunk! ........................................ 16
  Search Your Qualys Data .................................................. 19
  Search Container Security Data ......................................... 21

App Management & Troubleshooting ................................. 24
  APP Management ............................................................ 24
  Troubleshooting ............................................................. 25
  URL to the Qualys API Server ........................................... 26

What’s New ......................................................................... 27
About this guide

Welcome to Qualys App for Splunk Enterprise with TA! This user guide describes how to install and use the Qualys Technology Add-on (TA) to see your Qualys data in Splunk.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/
Get Started

Qualys App for Splunk Enterprise pulls (via the TA-QualysCloudPlatform) vulnerability and compliance detection data from your Qualys account and puts it in Splunk for easier searching and reporting.

The app uses Splunk’s App Development framework and leverages existing Qualys APIs.

Pre-requisites

- A valid Qualys account with API access
- A Splunk Enterprise account
- Computer with MacOS or Linux
- A couple minutes for setup

Download and Install the App

Download the latest version of Qualys Technology Add-on (TA) for Splunk by going to: https://splunkbase.splunk.com/app/2964/
Upload the downloaded tar.gz file using the “Install app from file” option.

Browse to the file and click Upload.

You’ll be prompted to restart Splunk. When you log back in, click the “Set up now” button.

Prefer to do this later? No problem. At any time go to the Apps list, find Qualys Technology Add-on for Splunk and click the “Set up” link under Actions.
Configure the App

Provide details for connecting to the Qualys API Server. Then configure settings for collecting VM, WAS, PC and CS detection data.

Which URL do I enter for the Qualys API Server?
You’ll enter the Qualys API Server URL for the Qualys Cloud Platform where your account is located. Click here if you need help finding the URL.

Which account credentials do I provide?
The username and password for the Qualys account you want to sync with Splunk. Note – If you return to this page at a later time your saved credentials won’t be visible. Do not enter credentials again as this will add another credential pair to the passwords.conf file and may cause issues when trying to pull data.
Can I authenticate using a client certificate?
Yes. Select “Use a Client certificate for authentication” and provide your PEM-encoded
X.509 certificate (.pem file). You’ll also need to provide the certificate key (.key file) if it’s
separate from the certificate, and enter a passphrase if the certificate/key file is
encrypted.

VM Detection Data
Configure settings for collecting VM detection data. Select one or more logging options to
indicate the type of data you want to view in Splunk.

Enter API input parameters (in the Extra parameters field) for the Host Detection API to
pull select vulnerability data from your Qualys account. For example, only pull data for
certain hosts by specifying ips=10.10.10.2-10.10.10.10. Download API user guides

Why choose “Log host information with each detection”?
This is recommended when you have more than 50,000 hosts in your Qualys account.

What are VM Detection-Advanced Settings?
The “Enable full data pull always?” option allows you to specify whether TA should do a
full data pull or an incremental pull on each run. By default, this is not selected and TA
does an incremental pull. Select the option to pull the full host detection data from Qualys
account and put it on Splunk.
The "Enable .seed file generation?" option indicates to TA to generate a .seed file at the location specified by you for TA to stream host detection data into Splunk. You have the option to specify either directory path or file path. If you specify a directory path, TA creates a .seed file each time TA pulls data into Splunk. TA appends data in the same .seed file if you specify a file.

We strongly recommend you to get in touch with our support team if you want to change VM Detection-Advanced Settings.

**How to configure directory path for the .seed file on Splunk Cloud?**

Directory path for the .seed file on Splunk Cloud must start with $SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/tmp. TA-QualysCloudPlatform shows an error while generating the .seed file if you configure any other path.

**Policy Compliance Data**

Configure settings for collecting PC data. For example, tell us whether you want to fetch all details or only basic details. Select basic details if you have a large amount of PC data. Additionally, you can choose to fetch individual compliance posture events for all hosts and/or a policy summary. You can also configure the number of policy IDs (1-10) to be fetched by the Posture API.

Enter API input parameters (in the Extra parameters field) for the Posture Information API. For example, specify Ids for the hosts for which you want to collect compliance posture information. Download API user guides
WAS Findings
Configure settings for collecting WAS data. You can choose to log individual findings and/or web application summary events.

Enter API input parameters (in the Extra parameters field) for the WAS Findings API to pull select data from your Qualys account. For example, specify Ids of web applications for which you want to view data. Download API user guides

Container Security Data Settings for Images
Configure settings for collecting CS data. Select one or more logging options to indicate whether you want to show individual image vulnerabilities and/or a summary of events for docker images.

Enter API input parameters (in the Extra parameters field) for the Docker Image Vulnerability API. This lets you pull only select vulnerability data for docker images from your Qualys account. For example, specify Ids of docker images for which you want to view vulnerability data. Go to the Container Security online help for API information.
**Container Security Data Settings for Containers**

Configure settings for collecting CS data for containers. Select one or more logging options to indicate whether you want to log and show individual vulnerabilities on a container and/or a summary of vulnerabilities found on a container. The Summary will include the total number of vulnerabilities with a break up of potential, confirmed and patchable vulnerabilities.

Enter API input parameters (in the Extra filters for Containers field) for the Container Vulnerability API. This lets you pull specific containers and their vulnerability data from your Qualys account. For example, if you want to download data only about running containers that have severity 5 vulnerabilities, you would specify state:RUNNING and vulnerabilities.severity:5 in the Extra filters field. Go to the Container Security online help for API information.

![Container Security Settings for Containers](image)

**Proxy Configuration**

Provide the proxy server IP address and credentials for Qualys API requests.

![Proxy Configuration](image)
Configure Data Sync

TA-QualysCloudPlatform pulls Qualys data and indexes it in Splunk on a regular basis.

Scripts parse and convert the Qualys API output to Splunk friendly format (CIM-compliant in Splunk parlance).

Go to Settings (on the top menu) and select Data Inputs.

Then click the “Add new” link for the Qualys Technology Add-On, as shown below.

Choose the Qualys metric (data feed input) you’re interested in, specify when to start pulling data and how often. Then click Next. Repeat these steps for each metric you want.
For VM data, choose knowledge_base and host_detection.
For PC data, choose policy_posture_info.
For WAS data, choose knowledge_base and was_findings.
For CS image data, choose cs_image_vulns.
For CS container data, choose cs_container_vulns.

Tip – When setting the interval, keep in mind your Qualys scanning schedule. If you’re scanning weekly, you don’t need to sync data daily.

**What is the default schedule for data sync?**
Data is pulled every day, starting 24 hours after install.

**Does the script pull all data or deltas only?**
The first time a script runs it pulls all data from your Qualys account. After that it pulls only the changes.

**Qualys data is added to Splunk**
You’ll notice each scan has a separate entry in Splunk. If you purge hosts using your Qualys account the data is not removed from Splunk.

**Enable the Data Feed to Start in Splunk**
Return to Settings > Data Inputs > Qualys Technology Add-On. You’ll see each of the Qualys metrics you selected. Make sure you enable these.

Once you enable data feeds, check the `$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/tmp` directory on your search head to see the XML files begin to download. Depending on how much data there is, it can take from hours to days to download the first data set.
How to setup for a Search Head Cluster

1) Install Qualys TA on your Forwarder. Depending on the type of data you want to ingest, add and enable any of these data inputs: host_detection, was_findings, policy_posture_info. Do NOT add the knowledge_base data input.

2) Use Deployer to push Qualys TA to all Search Heads. For reporting purposes you’ll also want to push these Qualys Apps to your Search Heads: Qualys VM App, Qualys PC App and Qualys WAS App.

3) Install Qualys TA on each Search Head. Go to Settings > Show All Settings and configure TA with your Qualys API credentials. On each Search Head add and enable only the knowledge_base data input. Do NOT add or enable any other data inputs on Search Heads.

How to get the RESULTS field indexed in host detection input

1) Open <TA DIR>bin/qualysModule/splunkpopulator/detectionpopulator.py and find class HostDetectionPopulator.

2) In this class, find _process_root_element(self, elem) method.

3) In this method, add “RESULTS” to the end of the HostDetectionPopulator.detection_fields_to_log list. This is a list of fields to parse from the detection tag. This will tell the code to parse the XML tag and output it while printing the event data. As a best practice, be sure to also include a comment describing why you’re editing the list.

4) Save the file and restart Splunk.

5) Update optional parameters on the TA setup page to include “show_results=1”. Already have optional parameters listed? Simply append this with an ‘&’ sign, for example “show_tags=1&showresults=1”.

Note - RESULTS in host detection API output could be multi-line text. As we set KV_MODE = auto for hostDetection input in props.conf, we are not sure how Splunk will treat the events when RESULTS field is multi-line text. It may or may not consider the multi-line text to be the part of same single event. The newline character might confuse Splunk’s event detection.

How to populate the SOLUTION section in the KB lookup file

You’ll need to edit the kbpopulator.py script used to populate the KB lookup file. The KB lookup file is: SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/lookups/qualys_kb.csv

1) Go to SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform. Use this command: cd /opt/splunk/etc/apps/TA-QualysCloudPlatform

2) Backup this file:
SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/bin/qualysModule/splunkpopulator/kbpopulator.py
3) Open kbpopulator.py and do the following:
Find this line and remove # from the beginning of the line (uncomment it):

```python
# QID_EXTRA_FIELDS_TO_LOG = ['VULN_TYPE', 'PATCHABLE', 'PCI_FLAG', 'TITLE', 'CATEGORY', 'DIAGNOSIS', 'CONSEQUENCE', 'SOLUTION', 'PUBLISHED_DATETIME']
```
Find this line and add # to the beginning of the line (comment it out):

```python
QID_EXTRA_FIELDS_TO_LOG = ['VULN_TYPE', 'PATCHABLE', 'PCI_FLAG', 'TITLE', 'CATEGORY', 'PUBLISHED_DATETIME']
```
The 2 lines should look like this when you’re done:

```python
QID_EXTRA_FIELDS_TO_LOG = ['VULN_TYPE', 'PATCHABLE', 'PCI_FLAG', 'TITLE', 'CATEGORY', 'DIAGNOSIS', 'CONSEQUENCE', 'SOLUTION', 'PUBLISHED_DATETIME']
# QID_EXTRA_FIELDS_TO_LOG = ['VULN_TYPE', 'PATCHABLE', 'PCI_FLAG', 'TITLE', 'CATEGORY', 'PUBLISHED_DATETIME']
```
4) Save your changes to kbpopulator.py.
5) Let the knowledgebase input run according to your schedule or run it immediately using this command:

```bash
cd SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform
SPLUNK_HOME/bin/splunk cmd python ./bin/run.py -k -s <your Qualys API server> -u <your Qualys API username> -p <your Qualys API password>
```
View your Qualys Data in Splunk!

We provide additional apps that make use of the data collected by the TA app. You’ll get dashboards and reports, and you’ll be able to easily search your data.

Simply download and install these apps. There is no setup needed!

- Qualys VM App for Splunk Enterprise
- Qualys PC App for Splunk Enterprise
- Qualys WAS App for Splunk Enterprise
- Qualys CS App for Splunk Enterprise

Once installed, you’ll see new apps on your Splunk Home page. Click any app on your Home page to view data.
View your Qualys Data in Splunk!

Sample VM Dashboard

Sample WAS Dashboard
View your Qualys Data in Splunk!

Sample PC Dashboard

Sample CS Dashboard
Search Your Qualys Data

Choose Search & Reporting on the Splunk Home page. Then enter your search query in the search field. Here are some sample search queries to get you started.

**QIDs by Category**

![QIDs by Category](image)

**Host Distribution by OS**

![Host Distribution by OS](image)
Scan Volume

Time since Last Scan
Search Container Security Data

CS data is in JSON format. TA indexes CS events in a structured format. You can search the CS data in Splunk using DOT notation.

You can use event type cs_image_info_event to search for vulnerabilities of images and for container use event types: qualys_cs_container_details, qualys_cs_container_vuln and qualys_cs_container_vuln_summary to search for container vulnerabilities.

For more information on creating search queries to filter CS data, refer to the Splunk Search Reference.

Sample JSON query to filter images matching a registry object in a repo list:
sourcetype="qualys:cs:csimageinfo" | search repo{}.registry="docker.io"
Sample JSON query to search images with a specific vulnerability severity count
`eventtype="cs_image_info_event" "vulnerabilities.severity2Count"="2"`
Search Container Security Data
View your Qualys Data in Splunk!

Sample JSON query to search vulnerabilities on running containers

```
eventtype=qualys_cs_container_vuln [search eventtype=qualys_cs_container_details state=RUNNING | dedup containerId | fields + containerId]
```

You can use Debug option to view debug information for one or more data input parameters
**App Management & Troubleshooting**

**APP Management**

**How to remove the app**

1) Stop Qualys App for Splunk Enterprise:

```bash
$SPLUNK_HOME/bin/splunk stop
```

2) Remove Qualys App for Splunk Enterprise:

```bash
$SPLUNK_HOME/bin/splunk remove app TA-QualysCloudPlatform -auth username:password
```

**Utility script to clean up left-over XML and PID files**

You’ll sometimes see orphan XML files in the TA-DIR/tmp directory when TA has errors, for example while calling the API, getting the response stream or parsing the API response. While running the utility, you can provide command line options to specify data input(s) for the XML files to be cleaned up. The utility will delete all the XML files related to the chosen data input(s), except those belonging to currently running TA processes.

Example 1: Help

```bash
my-user@my-host:/opt/splunk/etc/apps/TA-QualysCloudPlatform# /opt/splunk/bin/splunk cmd python ./bin/cleanup.py --help
```

Example 2: Delete Host Detection and WAS Findings XML

```bash
my-user@my-host:/opt/splunk/etc/apps/TA-QualysCloudPlatform# /opt/splunk/bin/splunk cmd python ./bin/cleanup.py --hd --was
```

Example 3: Delete XML files belonging to all data inputs

```bash
my-user@my-host:/opt/splunk/etc/apps/TA-QualysCloudPlatform# /opt/splunk/bin/splunk cmd python ./bin/cleanup.py --all
```
Troubleshooting

Looking for logs?
Qualys logs are populated in Splunk’s index “_internal”. Use this search to find logs:
index=_internal source="/opt/splunk/var/log/splunk/ta_QualysCloudPlatform.log"

Troubleshooting the setup
- Be sure to enter the proper API Server URL for the configuration.
- Verify you can reach the API from the Splunk Search Head where you installed Qualys App for Splunk Enterprise (no firewall or other infrastructure).
- Be sure the Qualys user account you’re using to connect has API access. Edit the user account in the Qualys UI and select the API access check box in the user settings. Don’t see this option? Reach out to Qualys Support or your Technical Account Manager.

Check that API calls are being made
In the Splunk setup where failing account is used, run the following search to see if API calls are being made to Qualys APIs:
index=_internal source="/opt/splunk/var/log/splunk/ta_QualysCloudPlatform.log" 
("/api/2.0/fo/asset/host/vm/detection/" OR "/api/2.0/fo/knowledge_base/vuln/" OR "/api/2.0/fo/compliance/posture/info/" OR "/qps/rest/3.0/search/was/finding")

Check that data feed is enabled
If you don’t see any entry for the /api/2.0/fo/asset/host/vm/detection/ API call, then check that the host_detection input was added and enabled.
- If not enabled, please enable it.
- If enabled, and you still don’t see any records for the VM detection API call, please check the TA installation directory. If you find the host_detection.pid file in the installation directory, delete it.

Note that you should see entries for the /api/2.0/fo/knowledge_base/vuln/ API call.

Check error logs
If everything is fine (inputs added and enabled; API calls are made) and you still don’t have data, please check “_internal” index for errors logged for TA-QualysCloudPlatform.
Run the following search and provide error logs to Qualys Support:
index=_internal source="/opt/splunk/var/log/splunk/ta_QualysCloudPlatform.log" ERROR:
URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

<table>
<thead>
<tr>
<th>Account Location</th>
<th>API Server URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://qualysapi.qualys.com">https://qualysapi.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.com">https://qualysapi.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://qualysapi.qg3.apps.qualys.com">https://qualysapi.qg3.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://qualysapi.qualys.eu">https://qualysapi.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.eu">https://qualysapi.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://qualysapi.qg1.apps.qualys.in">https://qualysapi.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>Qualys Private Cloud Platform</td>
<td><a href="https://qualysapi">https://qualysapi</a>.&lt;customer_base_url&gt;</td>
</tr>
</tbody>
</table>

You can easily find the API server URL for your account. Log in to your Qualys account and go to Help > About. You’ll see this information under Security Operations Center (SOC).
What’s New

New Feature in 1.4.0

TA now supports ingesting Container Security data

Qualys App for Splunk Enterprise can now pull vulnerability information for docker image and container in Container Security from your Qualys account. TA pulls CS data based on the configuration information you have provided in the Container Security Settings for Images and Containers. CS data is in JSON format.

New Feature in 1.3.4

New information added in HOSTSUMMARY and HOSTVULN events

Added NETWORK_ID, LAST_VM_SCANNED_DATE and LAST_VM_SCANNED_DURATION information in HOSTSUMMARY.

Added LAST_FIXED_DATETIME, TIMES_FOUND, IS_IGNORED, IS_DISABLED information in HOSTVULN.

New Features in 1.3.3

New Basic option for fetching policy posture compliance data

You can now specify to Posture API to fetch only basic details of the policy posture compliance data for policy IDs. This option is for policy IDs with large posture compliance data. Keep the “Log All details (when unchecked, logs “Basic” details)” check box deselected in the Policy Compliance Settings for the API to get basic details.

Configure total number of policy IDs to be fetched

You can now configure in the Policy Compliance Settings the total number of policy IDs to be fetched by the Posture API. The valid number range is 1 to 10. Set this value low for policy IDs with large policy posture compliance data.
New Features in 1.3.1

Introducing new data input for Policy Compliance
TA is now able to pull and ingest Policy Compliance posture information! The TA Setup page includes new Policy Compliance configuration settings. The extra parameters option accepts API parameters for Posture Information API (/api/2.0/fo/compliance/posture/info/ with action=list). When pulling policies information, Posture API parameter policy_ids becomes the parameter ids for Policy detail API call.

Support for using client certificates to call API
Now you can specify a client certificate in TA so that TA uses it while making API calls. A new section has been added to the TA setup page for this.

New utility script to clean up left-over XML and PID files
This new script is useful for cleaning up orphan XML files in the TA-DIR/tmp directory. While running the utility, you can provide command line options to specify data inputs for the XML files to be cleaned up. The utility will delete all the XML files for the chosen data inputs, except those belonging to currently running TA processes.

Additional Improvements 1.3.1

Update to Host List Detection API
You’ll now see the parameter vm_processed_after in TA logs. With Qualys 8.9, we 1) changed the way we report host scan time so it’s based on when a scan finished, not when the scan started. 2) Introduced new parameters to filter the Host List VM Detection API by scan end dates and processed dates. The vm_processed_after parameter is used to filter the list to only show hosts with vulnerability scan results processed after a certain date and time.

Setup page save fails if there are any validation errors
TA will try to validate inputs given on the TA setup page. If validation fails, it will NOT save any details, but raise a ValueError. This results in a generic error message in the Splunk UI. You can see a more detailed error message given by TA in splunkd.log.

When installed on Search Head, do not run data inputs other than knowledge base
Checks were added to the code (with help from the Splunk team) to ensure that TA will only run the knowledgebase data input when TA is installed on a Search Head, even when other data inputs have been added and enabled. In other words, TA will not run host detection, WAS findings and PC posture information data inputs when installed on Search Head.

Log error messages given by Qualys API
If the Qualys API responds back with an error (in response body), TA will now log the error message in the TA log for troubleshooting. This way you’ll know if there’s an API reason for not getting data (e.g. Rate Limit exceeded).
**PID repeat issue resolved**
TA writes PID in .pid file for every input run. This file is deleted at the end of the run. TA uses this pid file to check if any process with the PID is running. If it finds any such process, TA will check if the process is running qualys.py then only will it terminate itself, else TA will run the qualys.py script for the scheduled input.

**Configurable API Timeout period**
By default, the API timeout period is 300 seconds. If this value is not adequate you can set a different timeout value on the TA setup page.

**Display API parameters not allowed by TA**
To avoid operational problems, API parameters that are not allowed by TA are now clearly listed for each Extra API parameter field on the TA setup page.

**Log the index name being used in each run**
To help with troubleshooting, TA will now log the name of the index where data from each run will go into. This is the same index name as selected by the user while adding/updating the data input.

**Display data input name in each log entry**
There are some common execution paths for all data inputs in TA, and they write some log entries. When multiple data inputs are running at the same time, it becomes hard to identify which log entry was written for which data input. To fix this, TA will have a mention of data input it is running for in each log entry it writes. This way, one can grep all the log entries belonging to a particular data input. This would be useful if you are troubleshooting subsequent runs of the same data input.

**Avoid unnecessary call to msp/about.php each time Splunk invokes modular input**
Splunk invokes TA’s entry point script every 60 seconds. On each invocation, the code checks for the Qualys version by making a msp/about.php API call. This call was being made irrespective of whether the current time matched the configured cron/time interval. To avoid unnecessary calls, TA will first check if now is the time for any input to run. If yes, the API call is made. If no, the API call is not made.