# Table of Contents

**About this guide** .......................................................................................................................... 5
  About Qualys ............................................................................................................................... 5
  Qualys Support .......................................................................................................................... 5
  Want to contact Support ........................................................................................................... 5

**Get Started** ............................................................................................................................. 6
  Pre-requisites .............................................................................................................................. 6
  Download and Install the App .................................................................................................... 6
  Configure the App ...................................................................................................................... 8
    VM Detection Data ................................................................................................................ 9
    Policy Compliance Data ........................................................................................................ 11
    WAS Findings ......................................................................................................................... 12
    Container Security Data Settings for Images ....................................................................... 13
    Container Security Data Settings for Containers .............................................................. 13
    FIM data settings for events, ignored events and incidents .................................................. 14
    Indication of Compromise (IOC) Settings .......................................................................... 15
    Activity Log Settings ............................................................................................................. 16
    KnowledgeBase Settings ....................................................................................................... 16
    Proxy Configuration ............................................................................................................... 20
    Preserve API Output ............................................................................................................. 20
  Configure Data Sync .................................................................................................................. 20
  Enable the Data Feed to Start in Splunk .................................................................................. 23
  How to setup for a Search Head Cluster .................................................................................. 23
  How to index KB data into Splunk ............................................................................................ 24
  How to get the RESULTS field indexed in host detection input ............................................. 25
  How to populate the SOLUTION section in the KB lookup file ............................................. 25

**View your Qualys Data in Splunk!** ........................................................................................ 27
  Search Your Qualys Data .......................................................................................................... 31
    Search Container Security Data ............................................................................................. 33
    Search FIM Data for Events and Incidents ........................................................................... 36
    Search IOC Data .................................................................................................................... 38
    Search Activity Log Data ....................................................................................................... 39

**Event Types for Searching your Apps Data** ........................................................................ 40
  Event types for VM Detection data .......................................................................................... 40
  Event types for WAS Findings data .......................................................................................... 40
  Event types for Policy Compliance data .................................................................................. 40
  Event types for container Security data for images ................................................................ 40
  Event types for Container Security data for containers ....................................................... 41
  Event types for FIM data for events, ignored events, and incidents ...................................... 41
Event types for Indication of Compromise (IOC) data .................................................. 41
Event types for Activity log data .................................................................................. 41

App Management & Troubleshooting ................................................................. 42
APP Management ........................................................................................................ 42
Troubleshooting ........................................................................................................... 43
URL to the Qualys API Server .................................................................................... 45

What’s New ................................................................................................................. 46
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/

Want to contact Support

Send an email to support@qualys.com with the following information:
- Qualys TA version
- Visualization App version related to the issue, if any
- Complete TA and Splunk log for the time duration you had the issue
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, FIM, IOC, CS detection data, Activity log, and KB Data. To access this page, go to Apps > Manage Apps > Qualys Technology Add-on for Splunk > Set up.

**Note**

This note is applicable to TA 1.8.0 and above versions. If you are installing TA for the first time or upgrading your TA that has no configuration, then you must restart your Splunk once configurations in TA are saved successfully. You are required to restart Splunk only when you configure TA the first time. Restarting Splunk enables TA to reload the configurations from the app.conf file, which are modified after TA configuration.
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.

Tell me about the “Host fields to log” and “Detection fields to log” fields
1) In the “Host fields to log” field, we show the default output fields that you will see for host assets on Splunk for VM events. You can add additional comma-separated host XML tag names such as “Asset_ID” returned in the Host List API response that you want to log in the event or remove any existing tag that you don’t want to log.

2) In the “Detection fields to log” field, we show the default output fields that you will see for host detection on Splunk for VM events. You can add additional comma-separated detection XML tag names such as “AFFECT_EXPLOITABLE_CONFIG” and “AFFECT_RUNNING_KERNEL” returned in the Host List Detection response that you want to log in the event or remove any existing tag that you don’t want to log.

Tell me about the “Max characters allowed in RESULTS” field
The “Max characters allowed in the RESULTS” field lets you specify how many maximum characters will appear in the Results field. This means if the number of characters exceeds the maximum allowed characters, then TA will truncate the excess characters after parsing the RESULTS field and append the message “[TRUNCATED XXX Characters]” in the Results field. The max length includes the characters in the appended message. The default value is zero which means TA won't truncate any characters while parsing and you will see the entire value in the RESULTS field in Splunk.

What values are shown in the “RESULT_TRUNCATED” field?
The “RESULT_TRUNCATED” field shows values based on whether the RESULT field is truncated by TA or Splunk.

1) The “RESULT_TRUNCATED” field is set to “0” if neither TA nor Splunk truncates the value in the Results field.

2) The “RESULT_TRUNCATED” field is set to “1” when Splunk truncates the RESULTS field. This happens if the truncation value set for the RESULTS field in the props.conf file in Splunk is greater than that set on the TA set up page. In this case, the difference between the truncation values set in the TA and Splunk is truncated by Splunk after TA truncates the RESULTS field as per the value specified in the “Max characters allowed in RESULTS” field.

3) The “RESULT_TRUNCATED” field is set to “2” if TA, after parsing the event, truncates the RESULTS field value and if the truncation value set for the RESULTS field in the props.conf file in Splunk is either the same or less than that set for the RESULTS field for VM on the TA set up page.

Note that if Splunk truncates the RESULTS field, then the message “[TRUNCATED XXX Characters]” in the Results field is not shown.
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.

What are the event types for searching VM Detection data in Splunk?
Note that we provide default event types that you can use to search for VM detection data pulled in Splunk. See Event Types for Searching your Apps Data.

Policy Compliance Data
Choose one or more options to specify what posture data you want to fetch and index in Splunk for your policy. 1) Select “Log individual PC Compliance Posture events” to fetch posture info for all the host assets. 2) Select “Log Policy Summary”, to fetch policy summary information. These two options are selected by default. 3) Select “Log “All” details” to fetch full posture data. If the check box is not selected, we will show only basic details for your policy. 4) Select the “Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)” check box, to fetch and index full posture data and also data for these additional fields.

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

Note that we provide default event types that you can use to search for policy compliance data pulled in Splunk. See Event Types for Searching your Apps Data.

**WAS Findings**

Configure WAS Finding settings data to collect WAS data from your Qualys WAS account. 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

Note that we provide default event types that you can use to search for WAS Findings data pulled in Splunk. See Event Types for Searching your Apps Data.
Container Security Data Settings for Images

Configure these settings to collect Container Security data for individual docker image vulnerabilities and 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 Settings for Images](image)

Note that we provide default event types that you can use to search for CS data for images data pulled in Splunk. See Event Types for Searching your Apps Data.

Container Security Data Settings for Containers

Configure these 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 to pull specific containers and their vulnerability data from your Qualys account. For example, If you want to download data only about running
containers that has 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](image1)

Note that we provide default event types that you can use to search for CS data for containers data pulled in Splunk. See Event Types for Searching your Apps Data.

**FIM data settings for events, ignored events and incidents**

Configure FIM Settings for Events, Ignored Events and Incidents to collect FIM data for events, ignored events and incidents from your Qualys FIM account.

Enter API input parameters (in the Extra filters for FIM Events API, Extra filters for FIM Ignored Events API, Extra filters for FIM Incidents API) to specify what data (events, ignored events and incidents) will be pulled from your Qualys account.

For example, specify “action: rename” to pull all the events that are generated for this action.

![FIM Settings for Events](image2)
Note that FIM UI uses the user’s local timezone while the Splunk-FIM integration uses UTC timezone by default. If you are trying to match results from UI to Splunk integration, you will need to match Qualys UI and Splunk Integration timezones.

**Note**

TA 1.6.5 works only with FIM API version 2.0.2.0 and later and not with versions earlier than 2.0.2.0.

Note that we provide default event types that you can use to search for FIM events, ignored events, and incidents pulled in Splunk. See Event Types for Searching your Apps Data.

**Indication of Compromise (IOC) Settings**

Configure IOC API settings to fetch IOC data from your Qualys IOC Account. Enter the API input parameters (in the Extra parameters to pass to Indication of Compromise API) to specify what IOC data (events) will be pulled from your Qualys account.
TA uses default parameters “type:file AND indicator.score>0) OR (type:process AND action:running)” in the API request to call IOC API. These parameters are shown in the IOC settings. You can customize the API request by adding new parameters or modifying the existing parameters.

Note that we provide default event types that you can use to search for IOC data pulled in Splunk. See Event Types for Searching your Apps Data.

Activity Log Settings

Configure Activity Log settings to fetch activities from your Qualys account. Enter the API input parameters (in the Extra parameters to pass to Activity Log API) to specify what Activity Log data (events) will be pulled from your Qualys account.

Note that we provide default event types that you can use to search for Activity log data pulled in Splunk. See Event Types for Searching your Apps Data.

KnowledgeBase Settings

Configure Knowledge Base settings to enable or disable indexing KnowledgeBase (KB) data in Splunk. The check box “Index the KnowledgeBase...”, indicates whether TA after pulling the KnowledgeBase data will index the KnowledgeBase data in Splunk or write the data into a CSV file.

When you select the check box and click Save, TA fetches the KB data and then indexes this data into Splunk. If you are in the distributed setup environment, we recommend you to select this option so that you can get the updated KnowledgeBase data on the Search Head and generate the KB CSV file from the Search Head.
If the check box is not selected, TA does not index the KB data and creates a KB CSV file. The CSV file will have KB data from 1999-01-01 till the current date. By default, this option is disabled.

After you enable the index KB data option, the KB data will be indexed in Splunk. Next, you need to generate the KB CSV lookup on the Search Head using the Splunk's scheduled saved searches feature. To generate KB CSV lookup on the Search Head, first, you need to create a schedule save searches on the Search Head, and then create the KB CSV lookup definition. Creating “scheduled saved searches on the Search Head” and “KB CSV Lookup Definition on the Search Head” are one-time activities which you need to perform when you enable KB indexing first time.

Note that we recommend these steps if you are using distributed Splunk setup & enabled the index KB data option on the TA setup page.

If you disable the KB indexing option later, then disable the scheduled save search and lookup definitions created for KB indexing. If you enable the KB indexing option after disabling, then just enable the scheduled save search and lookup definitions created for KB indexing instead of creating them again.

**Create scheduled saved searches on the Search Head**

1) Go to Settings > Searches, Reports, and Alerts.


3) On the Create Report screen, enter a title & description for the new report. For example, you can have a title: Generate KB CSV Lookup and a description: Generate KB CSV Lookup.

4) In the Search field, copy and paste this SPL and replace the {INDEX_NAME} with the actual index name which you have set for KnowledgeBase data input. The SPL will read the KB data for the specified fields from the specified index that has the Qualys KnowledgeBase source type and then write this data in KB CSV output file.
5) In the App field, select the "Search & Reporting (search)" option to generate the KB CSV file under the directory: SPLUNK_HOME/etc/apps/search/lookups/.

6) Click Save to create the report. When you click Save, you will be navigated back to the Searches, Reports, and Alerts page.

7) On the Searches, Reports, and Alerts page, select "Search & Reporting (search)" from the app drop-down field.

8) Navigate to the report title that you have created, then click Edit to schedule the report.

9) Click Edit and select the "Edit Schedule" option.

10) On the Edit Schedule screen, select the Schedule Report check box.

11) From the Schedule drop-down field, select "Run on Cron Schedule".

12) In the Cron Expression input field, enter the cron format to specify the cron schedule for running the report. For example, enter */2 * * * * to schedule the cron after every 2 minutes.

13) In the Time Range field, select the "All time" option to pull all the index data.

14) Click Save.

**Create KB CSV Lookup Definition on the Search Head**

These steps let you access the KB CSV file data using the lookup.

1) Go to Settings > Lookups and on the Lookups page, click Add New in the Lookup definitions row to create lookup for KB CSV file.

2) From the Destination app field, select the "search" option to select the destination app to be used for the lookup.

3) In the Name field, enter a name as qualys_kb_lookup.

4) From the Type field, select the "File-based" option.
5) From the Lookup file field, select the “qualys_kb.csv” option.
6) Click Save to create the KB CSV lookup.

**Why happens when you disable KB indexing option after enabling it first?**
When you disable KB indexing after enabling it first then disable the scheduled saved search otherwise user may not get updated data or see blank dashboard, as on disabling the KB indexing the lookup file generated from scheduled search will be removed from SPLUNK_HOME/etc/apps/search/lookups/ directory. So that TA shows the data of the updated lookup file that is now generated in default SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/lookups/ directory

**What happens when you enable the index KnowledgeBase data option?**
When you enable indexing, TA determines if the KB data is getting indexed for the first time into Splunk or KB data has been indexed before. If TA determines that the KB data is indexed the first time, then the entire KB data from 1999-01-01 is pulled. TA pulls the entire data so that the KB data which you could see before upgrading TA will be available to you in the new version. On the other hand, if KB data has been indexed before, then TA uses the KB checkpoint date of the last run to pull the KB data.

**How TA determines if the KB data is getting indexed the first time?**
When you upgrade Splunk TA to 1.8.4 and choose to index the KB data into Splunk, TA will check if the KB checkpoint file is empty and the KB CSV file exists to determine if the KB indexing option is enabled for the first time. Note that TA creates a KB CSV file when you upgrade Splunk TA to 1.8.4. If the condition checked by TA is true, then TA will fetch the KB data from 1999-01-01, update the KB checkpoint file with the latest date and time, and remove the KB CSV file from the lookup folder if it exists.

Later, if you delete the KB checkpoint file or clear the KB checkpoint file data, then before indexing the KB data, TA will check if the KB checkpoint file is empty and the KB CSV file doesn’t exist. If these conditions are satisfied, TA will assume that the KB indexing option is not enabled for the first time. As a result, TA will use the start date provided on the KB input data form to pull the KB data from your Qualys account and update the KB checkpoint file with the latest date and time.

Note that If the index KB check box is not selected, TA will generate the KB CSV file but TA does not update the KB checkpoint file.
Proxy Configuration

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

Preserve API Output

Select this check box to save the API output files in Splunk. By default, this check box is not selected. When checked, TA will preserve JSON/XML files of API output for all the modules for which TA is configured to pull the data from your Qualys cloud.

Configure Data Sync

TA-QualysCloudPlatform pulls Qualys data and indexes 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.
For FIM events data choose fim_events.
For FIM ignored events data choose fim_ignored_events.
For FIM incidents data choose fim_incidents.
For IOC data choose ioc_events.
For Activity Log data choose activity_log.

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.

**How to assign a custom index to an event type?**
From TA v1.7.1 onwards, we are not supporting macro definition for indexes.

Specify a custom index from UI

Go to Settings > Event types and from the App drop-down select Qualys Technology Add-On for Splunk. Navigate to the event type that you want to update. Click the event type and update the search string to specify index=<name of the custom index>.

Specify a custom index from CLI

To set custom index, copy the eventtype.conf file from $SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/default/ to $SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/local/ and update the search string of the required event type to specify index=<name of the custom index>. Then restart 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.

Note that for all FIM data inputs, choose a date equal to or greater than 2017-01-01T00:00:00.000Z.

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.

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. Do NOT add or enable any other data inputs on Search Heads.
How to index KB data into Splunk

We support indexing of the KnowledgeBase (KB) data in Splunk so that the Splunk TA users on the distributed setup environment can get the updated KnowledgeBase data on the Search Head from the Heavy Forwarder and generate the KB CSV file.

On the TA set up page, we added a KnowledgeBase Settings section that has a check box "Index the KnowledgeBox...".

The check box indicates whether to index the KnowledgeBase data in Splunk or to write the data into a CSV file. When you select the check box and click Save, TA will fetch the KB data and index the KB data in Splunk. If the check box is not selected, TA does not index the KB data into Splunk and creates a CSV file.

The CSV file will have KB data from 1999-01-01.

On the Settings > Data Inputs > Add Data page for Qualys technology add on, we added the information that for knowledge_base “Start Date” field is applicable only if “index the knowledge base” is enabled on the TA setup page.

After you enable the index KB data option, you need to generate KB CSV lookup on the Search Head. See KnowledgeBase Settings.
How to get the RESULTS field indexed in host detection input

Skip the first 4 steps if the installed version of Qualys App for Splunk Enterprise is 1.4.1 or higher.

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&show_results=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 $SPLUNK_HOME/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):

# 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):

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:
How to populate the SOLUTION section in the KB lookup file

Get Started

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:

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. 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
- Qualys FIM App for Splunk Enterprise
- Qualys IOC 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 PC Dashboard Image]

Sample CS Dashboard

![Sample CS Dashboard Image]
View your Qualys Data in Splunk!

Sample FIM 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 Diagram]

Host Distribution by OS

![Host Distribution by OS Diagram]
Scan Volume

View your Qualys Data in Splunk!

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.

Use these event types to search for different types of container data: `cs_image_info_event` to search for vulnerabilities of images, `qualys_cs_container_details`, `qualys_cs_container_vuln` to search for container data 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"`

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/17/18 9:27:06.000 AM</td>
<td></td>
</tr>
<tr>
<td>[ ] architecture: null</td>
<td></td>
</tr>
<tr>
<td>associatedContainersCount: 0</td>
<td></td>
</tr>
<tr>
<td>associatedHostsCount: 1</td>
<td></td>
</tr>
<tr>
<td>author: null</td>
<td></td>
</tr>
<tr>
<td>created: 2018-11-20T02:50:42Z</td>
<td></td>
</tr>
<tr>
<td>customerKeyId: null</td>
<td></td>
</tr>
<tr>
<td>dockerVersion: null</td>
<td></td>
</tr>
<tr>
<td>event: null</td>
<td></td>
</tr>
<tr>
<td>eventOccurred: null</td>
<td></td>
</tr>
<tr>
<td>host: null</td>
<td></td>
</tr>
<tr>
<td>imageId: 93707269bd1</td>
<td></td>
</tr>
<tr>
<td>label: null</td>
<td></td>
</tr>
<tr>
<td>lastScanned: 2018-11-22T09:27:06Z</td>
<td></td>
</tr>
<tr>
<td>layers: null</td>
<td></td>
</tr>
<tr>
<td>layersCount: null</td>
<td></td>
</tr>
<tr>
<td>operatingSystem: null</td>
<td></td>
</tr>
<tr>
<td>parentKeyId: null</td>
<td></td>
</tr>
<tr>
<td>registryUserId: null</td>
<td></td>
</tr>
<tr>
<td>repo: [ ]</td>
<td></td>
</tr>
<tr>
<td>sensorKeyId: null</td>
<td></td>
</tr>
<tr>
<td>sha: null</td>
<td></td>
</tr>
<tr>
<td>size: 88175358</td>
<td></td>
</tr>
<tr>
<td>software: null</td>
<td></td>
</tr>
</tbody>
</table>
Sample JSON query to search vulnerabilities on running containers

```json
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
Search FIM Data for Events and Incidents

FIM events, Ignored events and incidents ingested in splunk can be searched using their eventtype. Further, user can search them using SPL of desired filters.

Here are some sample queries for searching FIM data in Splunk.

**Sample query to search for FIM events**

```
eventtype="qualys_fim_event"
```

![Sample query to search for FIM events](image1)

**Sample query to search for FIM ignored events**

```
eventtype="qualys_ignored_fim_event"
```

![Sample query to search for FIM ignored events](image2)
Sample query to search for FIM incidents

`eventtype=“qualys_fim_incident”`
Search IOC Data

You can search for specific IOC events that TA has pulled in Splunk from your Qualys account. Use `eventtype="qualys_ioc_info_event"` or create your own SPL search query to filter the data.
Search Activity Log Data

You can search for specific Activity Log events that TA has pulled in Splunk from your Qualys account. Use eventtype="qualys_activity_log_event" or create your own SPL search query to filter the data.
Event Types for Searching your Apps Data

Here is the list of default event types for Qualys Apps. You can use these event types when searching your Apps data in Splunk.

Note - If the customer has used custom index then replace [INDEX_NAME] with custom index name else replace with main.

Event types for VM Detection data
1) Event Type Name - qualys_vm_detection_event
Search Query - index=[INDEX_NAME] (sourcetype="qualys:hostDetection" OR sourcetype="qualys_vm_detection") "HOSTVULN"
2) Event Type Name - qualys_host_summary_event
Search Query - index=[INDEX_NAME] (sourcetype="qualys:hostDetection" OR sourcetype="qualys_vm_detection") "HOSTSUMMARY"

Event types for WAS Findings data
1) Event Type Name - qualys_was_finding_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:wasFindings" "WAS_FINDING"
2) Event Type Name - qualys_was_summary_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:wasFindings" "WAS_SUMMARY"

Event types for Policy Compliance data
1) Event Type Name - qualys_policy_info_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:pc:policyInfo" "POLICY_INFO"
2) Event Type Name - qualys_posture_info_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:pc:postureInfo" "POSTURE_INFO"
3) Event Type Name - qualys_policy_summary_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:pc:postureInfo" "POLICY_SUMMARY"

Event types for container Security data for images
1) Event Type Name - cs_image_info_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:cs:csimageinfo" "IMAGE_INFO"
2) Event Type Name - cs_vuln_info_event
Search Query - index=[INDEX_NAME] sourcetype="qualys:cs:csimagevulninfo" "VULN_INFO"
Event types for Searching your Apps Data

3) Event Type Name - cs_vuln_summary_event
Search Query - index={INDEX_NAME} sourcetype="qualys:cs:csimagevulninfo" "VULN_SUMMARY"

Event types for Container Security data for containers

1) Event Type Name - qualys_cs_container_details
Search Query - index={INDEX_NAME} sourcetype="qualys:cs:container" "CONTAINER_DETAILS"

2) Event Type Name - qualys_cs_container_vuln
Search Query - index={INDEX_NAME} sourcetype="qualys:cs:containerVuln"
  type=CONTAINER_VULN

3) Event Type Name - qualys_cs_container_vuln_summary
Search Query - index={INDEX_NAME} sourcetype="qualys:cs:containerVuln"
  type=CONTAINER_VULN_SUMMARY

Event types for FIM data for events, ignored events, and incidents

1) Event Type Name - qualys_fim_event
Search Query - index={INDEX_NAME} sourcetype="qualys:fim:event"
  splunk_event_type=FIM_EVENT

2) Event Type Name - qualys_ignored_fim_event
Search Query - index={INDEX_NAME} sourcetype="qualys:fim:ignored_event"
  splunk_event_type=FIM_IGNORED_EVENT

3) Event Type Name - qualys_fim_incident
Search Query - index={INDEX_NAME} sourcetype="qualys:fim:incident"
  splunk_event_type=FIM_INCIDENT

Event types for Indication of Compromise (IOC) data

Event Type Name - qualys_ioc_info_event
Search Query - index={INDEX_NAME} source="qualys"
  sourcetype="qualys:ioc:ioceventinfo"

Event types for Activity log data

Event Type Name - qualys_activity_log_event
Search Query - index={INDEX_NAME} sourcetype="qualys:activityLog"
App Management & Troubleshooting

APP Management

How to remove the app
1) Stop Qualys App for Splunk Enterprise:
   `$SPLUNK_HOME/bin/splunk stop`
2) Remove Qualys App for Splunk Enterprise:
   `$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
```
my-user@my-host:$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform#$SPLUNK_HOME/bin/splunk cmd python ./bin/cleanup.py --help
```

Example 2: Delete Host Detection and WAS Findings XML
```
my-user@my-host:$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform#$SPLUNK_HOME/bin/splunk cmd python ./bin/cleanup.py --hd --was
```

Example 3: Delete XML files belonging to all data inputs
```
my-user@my-host:$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform#$SPLUNK_HOME/bin/splunk cmd python ./bin/cleanup.py --all
```

Know important file paths in Splunk

<table>
<thead>
<tr>
<th>File</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td><code>$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/default/eventtype.conf</code></td>
</tr>
<tr>
<td>KB lookup</td>
<td><code>$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/lookups/qualys_kb.csv</code></td>
</tr>
<tr>
<td>API Credential</td>
<td><code>$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/local/passwords.conf</code></td>
</tr>
<tr>
<td>Qualys TA Configuration</td>
<td><code>$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/local/qualys.conf</code></td>
</tr>
<tr>
<td>Qualys TA log</td>
<td><code>$SPLUNK_HOME/var/log/splunk/ta_QualysCloudPlatform.log</code></td>
</tr>
<tr>
<td>Check point</td>
<td><code>$SPLUNK_HOME/var/lib/splunk/modinputs/qualys</code></td>
</tr>
</tbody>
</table>
Troubleshooting

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

Delete the checkpoint file and pull the data again for a Qualys module
Navigate to $SPLUNK_HOME/var/lib/splunk/modinputs/qualys/. Delete the checkpoint file of the desired module. For example, Delete 'host_detection' file for module Host Detection and initiate the pull once again. TA will now pull the data from the date configured in Data Input Settings for the respective Qualys module.
qualys.py is running even after the data input is disabled or Splunk is restarted

This issue is seen mostly on Ubuntu OS, that has default shell set to 'dash'. To fix this issue, set the default shell from 'dash' to 'bash'.

Steps to change the Ubuntu configuration:

1) ~# debconf-show dash
   * dash/sh: true
2) ~# debconf-set-selections <<< "dash dash/sh string false"
3) ~# debconf-show dash
   * dash/sh: false
4) ~# dpkg-reconfigure -f noninteractive dash

Removing 'diversion of /bin/sh to /bin/sh.distrib by dash'
Adding 'diversion of /bin/sh to /bin/sh.distrib by bash'
Removing 'diversion of /usr/share/man/man1/sh.1.gz to /usr/share/man/man1/sh.distrib.1.gz by dash'
Adding 'diversion of /usr/share/man/man1/sh.1.gz to /usr/share/man/man1/sh.distrib.1.gz by bash'
5) ~# debconf-show dash
   * dash/sh: false

How to switch python interpreter for Python3?
1) Goto the path - $SPLUNK_HOME/etc/system/local/server.conf
2) Add the python.version=python3 under [general].

Blank dashboard for the KnowledgeBase data

Perform these steps to identify and troubleshoot the issue:

- Check whether the correct index is used in the SPL added for the scheduled saved search.
- In case you disabled indexing after enabling it earlier, then check whether the scheduled saved search is also disabled as it is running for the index in which data is not updated.
- Go to the Settings > Lookups > Lookup table files and on the Lookup table files page select “All” from the App drop-down field. Check qualys_kb.csv is generated for which app. On enabling the indexing, the file should be present for ’search' app and on disabling the
indexing, the file should be present for ‘TA-QualysCloudPlatform’ app. If qualys_kb.csv is present for any other app, then you should delete the file for that app else you may get to see blank KnowledgeBase dashboard.

**URL to the Qualys API Server**

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click [here](#) to identify your Qualys platform and get the API URL.

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

Improvements in 1.8.5

Added three new fields in the VM Detection Setting section on the TA set up page

We have added three new fields: “Host fields to log”, “Detection fields to log”, and “Max characters allowed in RESULTS field” in the VM Detection Settings section on the TA Set up page.

1) “Host fields to log” show default output values for host assets. You can add additional comma-separated host XML tag names such as “Asset_ID” returned in the Host List API response that you want to log in to the event or remove any existing tag that you don’t want to log.

2) “Detection fields to log” show default output fields for host detection. You can add additional comma-separated detection XML tag names such as “AFFECT_EXPLOITABLE_CONFIG” and “AFFECT_RUNNING_KERNEL” returned in the Host List Detection response that you want to log in the event or remove any existing tag that you don’t want to log.

3) Max characters allowed in the RESULTS field lets you specify how many maximum characters will appear in the Results field. This means if the number of characters exceeds the maximum allowed characters, then TA will truncate the excess characters after parsing the RESULTS field and append the message “[TRUNCATED XXX Characters]” in the RESULTS field.

The “RESULT_TRUNCATED” field now shows values based on whether the RESULT field is truncated by the TA or Splunk.

1) RESULT_TRUNCATED is “0” if neither TA nor Splunk truncates the RESULTS field/raw event.
2) RESULT_TRUNCATED value is “1” if the RESULTS field is truncated by Splunk. Note that if Splunk truncates the RESULTS field then the message “[TRUNCATED XXX Characters]” in the Results field is not shown.

3) RESULT_TRUNCATED value is “2” if the RESULTS field is truncated by TA. Note that if TA truncates the RESULTS field then the message “[TRUNCATED XXX Characters]” in the Results field is shown.

**Improvements in 1.8.4**

**Added option to index the KB data in Splunk**

With this release, we now support indexing of the KnowledgeBase (KB) data in Splunk so that the Splunk TA users on the distributed setup environment can get the updated KnowledgeBase data on the Search Head from the Heavy Forwarder and generate the KB CSV file.

On the TA setup page, we added a KnowledgeBase Settings section that has a check box "Index the KnowledgeBox...".

The check box indicates whether to index the KnowledgeBase data in Splunk or to write the data into a CSV file. When you select the check box and click Save, TA will fetch the KB data and index the KB data in Splunk. If the check box is not selected, TA does not index the KB data into Splunk and creates a CSV file.
The CSV file will have KB data from 1999-01-01.

On the Settings > Data Inputs > Add Data page for Qualys technology add on, we added the information that for knowledge_base “Start Date” field is applicable only if “index the knowledge base” is enabled on the TA set up page.

After you enable the index KB data option, you need to generate KB CSV lookup on the Search Head. See KnowledgeBase Settings.

**CS image label Information now available in CS events**
You will now see the CS label information along with the CS image vulnerabilities in CS events for images in Splunk. TA uses a new API "/csapi/v1.2/images/<imageId>" to fetch the CS label and image vulnerability information. TA uses the label key to fetch the label information and the "vulnerabilities" key to fetch the vulnerability information. The image vulnerabilities & label information will be available in cs_vuln_info_event event type.

The new API does not provide image vulnerability summary information in the response. TA generates vulnerability summary information with the help of severity and patch availability fields of vuln summary information. All this vulnerability summary information will be available in the cs_vuln_summary_event event type.

**Improvements in 1.8.3**
We have fixed these issues in 1.8.3.

**Issues Fixed**
- We fixed an issue where the check box selection values for “log host summary events” and “Log Individual Host Vulnerabilities” options in the TA set up > VM Detection settings section was read from the app configuration file instead of qualys.conf file.
- We fixed an issue where TA was logging “VM host summary events for host detection” in Splunk even though the user had configured to exclude the VM host summary events on the TA setup page.

- We fixed an issue where WAS summary events weren’t fetched for all the threads when the WAS data was fetched using multiple threads. Now when the WAS data is fetched in the multi-thread mode, TA logs events in Splunk from all the threads.

- We fixed an issue where TA throws an error and terminates the WAS API call when the WAS data input is fetched using multiple threads and the web application IDs are not distributed appropriately to each thread. To fix this error, we have changed the logic of distribution for web application IDs between the threads so that web application IDs are appropriately distributed.

**Improvements in 1.8.2**

**Enhancements to VM Detection Event**

With this release, we have moved the **Result** field in the VM Detection event to the end of the event. When the Result field is placed before the other event fields, Splunk, at the time of processing the VM Detection event data, truncates all the fields after the Result field if the size of the event exceeds the truncation limit. To avoid truncation of fields, we have added the Results field at the end of the event. Now only the values in the results field will be truncated, if the event size exceeds the truncation limit.

We have added a **RESULT_TRUNCATED** field before the "Results" field in the event to inform you that the event is truncated or not. RESULT_TRUNCATED = 1 means event is truncated and RESULT_TRUNCATED = 0 means event is not truncated. You can search for truncated and non truncated events using this field.

TA will also remove the leading and trailing white spaces from the Results field after TA fetches VM detection data from your Qualys account using the Host List Detection API.

Splunk reads the truncate value from the **props.conf** file in the TA in “global/local” directory. If this file is removed from the app “global/local” directory, then TA will read the truncate value from the **global props.conf** file in Splunk. TA never truncates the event data while sending it to Splunk. Splunk automatically truncates the event if the size of the event exceeds the truncate limit set in the props.conf or global props.conf file.

**Note**
The VM Detection event shows the Results field when `show_results` is set to 1 in the “Extra Parameters” fields in VM Detection Settings on the TA setup page. If this parameter is not set, then none of these changes will have any impact on the VM Detection Event data.

**Improvements in 1.8.1**

**Cleanup Script to remove API output files for Activity Log**

We added the “Activity Log” data input in the cleanup script to remove the API output files from the /tmp directory.

**Issue Fixed**

We fixed the byte string issue for the host detection data pulled in Splunk for versions above 8.x.x which uses Python 3 interpreter.

**Improvements in 1.8.0**

**Added a new data input - Activity Log**

We added a new data input “Activity Log” to TA to let you pull activity logs from your Qualys Account. To access data input page, go to Settings > Data > Data Inputs > Qualys Technology Add-On. Click Add and from Qualys Metrics drop-down, select activity_log.

**Page size field added for data inputs**

We added Page size field for these data inputs to let you specify the number of records to be fetched in single API call. The default value for page size is 1000 records, but you can change the value.

- Container Security Data Settings for Images
- Container Security Data Settings for Containers
- FIM settings for events
- FIM settings for ignored events
- FIM settings for incidents
- Indication of Compromise (IOC)
Redesigned TA setup form
We have redesigned TA setup form to make TA 1.8.0 Splunk cloud compatible as per the SplunkAppInspect tool suggestion and improve the user experience.

Issues Fixed
We have fixed the proxy server validation issue in this release.
You can now update Qualys’s password in the TA setup form without removing the password.conf file & restarting Splunk.
We now log the error in TA log if the CRON format of data input is invalid.

Improvements in 1.7.1
We made these improvements in 1.7.1
- TA is now compatible with both Python v2.7 and v3.7. See How to switch python interpreter for Python3?
- Container Security APIs now support the API gateway. Private cloud provider can use the gateway URL to connect to and fetch CS data from Qualys Cloud platform.

TA v1.7.1 no longer supports macro definition for indexes
Due to a known issue with Splunk, the user was getting a 255 error on the distributed Search Head setup. We have used macros for the ease of handling indexes and event types.
But in case of the distributed setup, macros definition was not getting expanded and as a result, the user was getting error on dashboard or while searching with event types.

To resolve this issue, the Splunk team has suggested not to use macros till further notice from them. See How to assign a custom index to an event type?

**Improvements in 1.6.7**

**Policy Compliance data to show additional fields**

You can now view REMEDIATION, RATIONALE, EVIDENCE and CAUSE_OF_FAILURE information in the compliance posture data for your policy.

To pull this data in Splunk, go to the TA setup page and in the “Policy Compliance Settings” section, select the “Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)” check box.

**Issues Fixed**

We fixed an issue where last evaluated date was not shown as the event date for the policy. Now if the policy has last evaluated date then we will show this date as the event date.
Improvements in 1.6.6

**TA to use “updated” dateTime to download Container and Images data in Splunk**

The new version of Container Security API uses a new parameter: “updated” to address the issue with mismatch count between Qualys UI and Splunk.

In TA 1.6.6, we now use the new parameter “updated” instead of “created” to ensure that all the Container and Images that were updated in particular duration gets synced in Splunk.

**Improvised Logging**

We have now improvised logging to print exception messages and avoid logging empty messages.

**Masked Passwords**

Previously, the password was in plain text. But, we now mask passwords in proxy authentication.

**Improved parsing for Host Detection RESULTS**

We have improvised Host Detection RESULTS section to address the issue of parsing RESULTS in upper case.

**Retry Interval**

We have introduced a new configuration ‘retry_interval_seconds’ to retry same API request after configured interval, in case any error occurs while calling APIs.

Steps to configure ‘retry_interval_seconds’:

- edit qualys.conf file from below location:
  
  `<Splunk_Home>/etc/apps/TA-QualysCloudPlatform/local/qualys.conf`

- add below line to qualys.conf file

  ```
  retry_interval_seconds =<time_in_seconds>
  ```

Improvements in 1.6.5

**TA to use “processedTime” for downloading FIM Data in Splunk**

The new version 2.0.2.0 of FIM API has a new parameter “processedTime” to address the time lag issues with uploading the events on the Qualys portal by FIM agents.

In TA 1.6.5, we now use the new parameter “processedTime” instead of “dateTime” to ensure that all the FIM events that are generated in a particular duration are pulled in Splunk.

Due to this change, TA 1.6.5 will work only with FIM API version 2.0.2.0 and later and not with versions earlier than 2.0.2.0.
Improvements in 1.6.4

KnowledgeBase data to show BUGTRAQ_ID field
In Splunk, we will now show a new field “BUGTRAQ_ID” in KnowledgeBase data that is pulled from Qualys. This information is shown for QIDs that has “BUGTRAQ_ID” available.

FIM events to show event generated time in search results
When you search for FIM events in Splunk, the Time column in search results will now show you the time when the FIM event occurred as reported in your Qualys account. Earlier the time shown was the time when the event is pulled in Splunk.

Improvements in 1.6.3

Error on saving proxy server credentials
Fixed an issue where the TA user was getting an error when saving proxy server credentials required for authentication to the proxy server on the Qualys App set up page. Now the credential details are getting saved.

KnowledgeBase Data not populating in the solution section of the KB lookup file
We fixed an issue where the solution section in the KB lookup file (qualys_kb.csv) was not getting populated due to a failure in parsing of KnowledgeBase data. The parsing error occurred because the parameters “Threat_INTEL_IDS” and “Threat_INTEL_VALUES” were not found in the KB lookup file. We have added these two parameters in the KB lookup file.
**Handle XML parsing error for WAS data**

We fixed an issue where TA used to parse the WAS XML response file that had XML parsing errors. Now when TA will receive WAS data that contains parsing errors, it will not parse the file and request Qualys API server to resend the response file. TA will keep on requesting the WAS data from API server till it receives the data contains no parsing errors.

**Certificate authentication failure when connecting to Qualys API server**

We fixed an issue where authentication to the Qualys API server was getting failed when the user tried to connect to the API server via the proxy server using the certificate.

**New Enhancements in 1.6.2**

We have made the following enhancements in 1.6.2 release. TA can now:

- Pull EC2 metadata in host detection events using the extra parameter. For example, "{host_metadata": "ec2", "host_metadata_fields": "region,accountId,instanceId"}.
- Pull "cwe" information in Qualys WAS events.
- Retry the request that failed due to corrupted response XML.

**New Features in 1.6.1**

You can now configure Qualys App for Splunk Enterprise to pull IOC events data in Splunk from your Qualys account. We added a new Qualys metric (data input feed) “ioc_events” that you need to configure and enable for pulling the IOC events from your Qualys account. A new event type “ioc_info_event” is added for searching pulled IOC events in Splunk.

You can now preserve API output files in Splunk using the “Enable to preserve the XML/JSON files of API output” option. This option is available on the Qualys app setup page. By default, this check box will not be selected.
Added FIM Dashboard

We have also added a FIM dashboard to give you a graphical analysis of your FIM data pulled from your Qualys Account. You will see graphical data for total number changes, events by severity, file and directory changes by change action, and top changes by OS, user and process.

Multithreading not supported for FIM

We removed multithreading support for FIM as the new APIs (FIM API Version 2.0) do not support multithreading.

New Feature in 1.5.0

Qualys App for Splunk Enterprise can now pull FIM data for events, ignored events and incidents from your Qualys Account. On the TA set up page, you will now see 3 new sections: FIM Settings for Events, Ignored Events and Incidents. Specify configuration settings in these sections for collecting FIM data. Next, enable the FIM data feeds to pull the FIM data based on the configuration settings provided on the TA set up page.

New Features and Fixed Issues in 1.4.1

View Qualys Real-time Threat Indicators (RTIs) for vulnerabilities

We are now sending the Qualys Real-time Threat Indicators (RTIs) data in the data input for the Knowledge base metric. Only, the user account with Threat Protection subscription can view this information for vulnerabilities found in the host based scans. You can set up your dashboard to monitor vulnerabilities for various threat level values. The sample search shows vulnerabilities for which threat value is High_Data_Loss.
eventtype=qualys_vm_detection_event | dedup 1 HOST_ID, QID | lookup qualys_kb_lookup QID OUTPUT THREAT_INTEL_VALUES | search THREAT_INTEL_VALUES=""High_Data_Loss"" | table HOST_ID, LAST_SCAN_DATETIME, QID, THREAT_INTEL_VALUES

Support for arf_kernel filters parameter for VM host detection
We now support “arf_kernel filters” parameter to identify vulnerabilities found on running or non-running Linux kernels. You can update the optional parameter to include the arf_kernel parameter in VM Detection Settings on the TA setup page.

Set show_results=1 to view TCP/UDP port information
We have fixed an issue where the user was unable to view the open TCP/UDP ports information in the HOSTSYMMARY events. To view the information, update optional parameters in VM Detection Settings on the TA setup page to include “show_results=1”.

Newline character removed from the port data in vulnerability data feed
We have fixed an issue where whitespace and newline characters in the port data in the Results tag in the vulnerability data feed fetched from the Qualys Server were introducing new events when imported in Splunk. Now, we have fixed this issue by removing these characters from the vulnerability data feed before importing it in Splunk.

Enable CVSS scoring in your account to view CVSS scores for vulnerabilities
We have fixed an issue where Splunk was showing an error for missing CVSS data when importing KnowledgeBase API response in Splunk TA. This issue was occurring for the user accounts that have CVSS Scoring not enabled for their subscriptions. As a result, the KnowledgeBase API response does not have CVSS data for vulnerabilities. To enable CVSS Scoring in your Qualys account, go to "Reports > Setup > CVSS > Enable CVSS" and click "save".

Now, Splunk does not show missing CVSS data error if you do not enable CVSS scoring for your subscription. In this case, Splunk will show no CVSS metrics scores for vulnerabilities in the Splunk KnowledgeBase.
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.