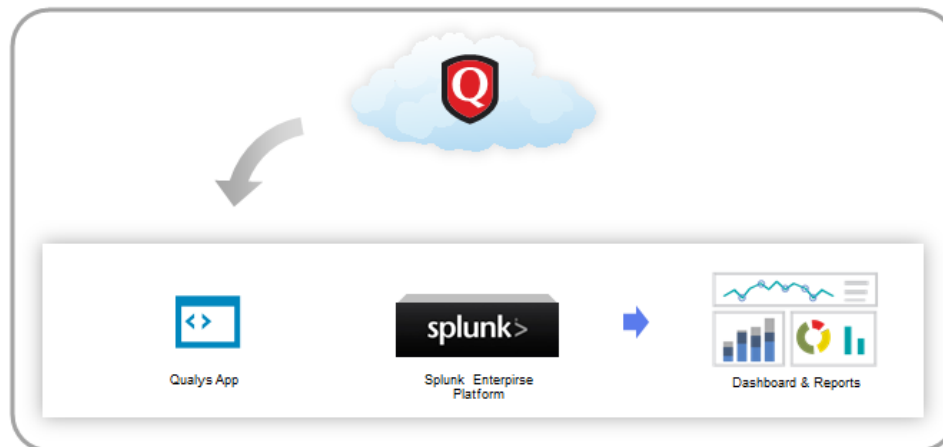


Qualys App for Splunk Enterprise with TA

We know you've been wanting to see your Qualys data in Splunk. Now you can!

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.

Qualys App for Splunk Enterprise solution



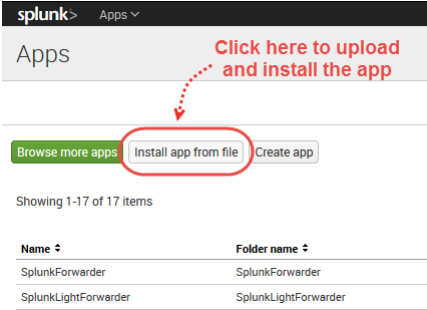
What You'll Need

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

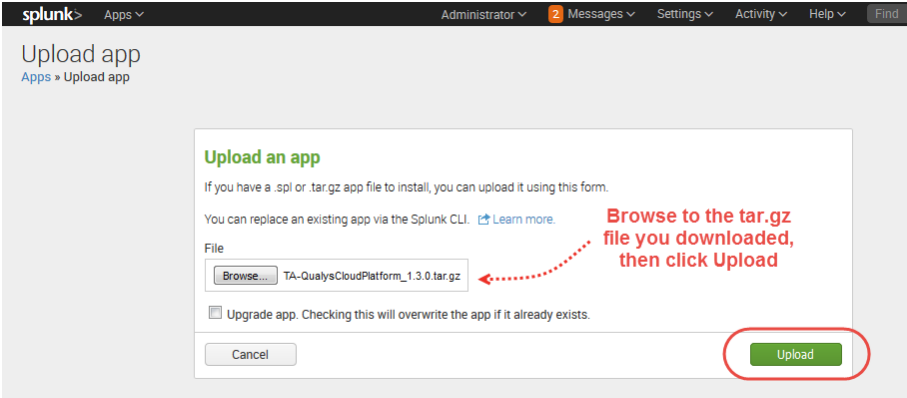
Download and Install the App

You can download the latest version of Qualys Technology Add-on (TA) for Splunk by going to: <https://splunkbase.splunk.com/app/2964/>

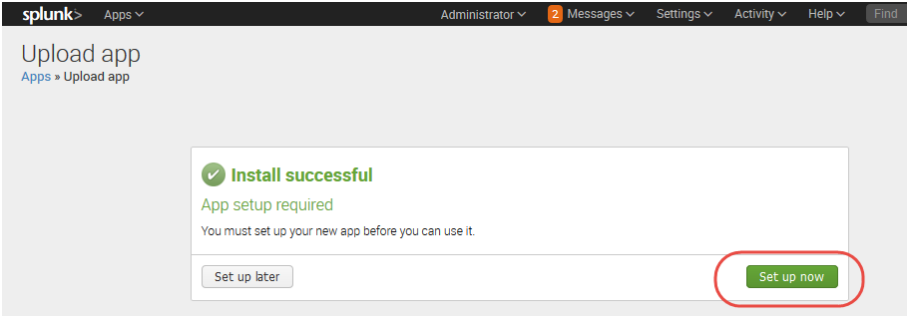
Then upload the downloaded tar.gz file using the “Install app from file” option.



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

This is where you'll provide details for connecting to the Qualys API Server and configure settings for collecting VM, WAS and PC detection data.

The screenshot displays the configuration interface for the Qualys App, organized into three columns:

- Configure This App:**
 - Qualys API Server:** A text field containing the URL `https://qualysapi.qualys.com`.
 - Qualys Credentials:** Fields for Username, Password, and Confirm password.
 - Client Certificate:** A checkbox for "Use a Client certificate for authentication". Below it are fields for Path to client CA certificate, Path to client CA certificate key, Passphrase for client CA certificate, and Confirm password.
 - API Timeout Settings:** A field for "API request timeout period in seconds" with the value `300`.
- VM Detection Settings:**
 - Checkboxes for "Log Host Summary events", "Log extra statistics in host summary (Breakdown of Vulnerability Count)", "Log Individual Host Vulnerabilities", and "Log host information with each detection (e.g. IP OS, DNS, NetBios)".
 - Text: "Extra parameters to pass to Detection API. Enter as URL Query (e.g. a=1&b=output_format,vm_scan,since,ids,suppress,duplicated_data_from,csv,m)".
 - Checkboxes for "Load detection data using multiple threads (resource intensive)" and "Number of threads to use (between 1 and 10)" with a value of `2`.
 - VM Detection - Advanced Settings:**
 - Checkbox for "Enable full data pull always? If checked, TA will always do a full data pull".
 - Checkbox for "Enable .seed file generation? If checked, TA will only generate a .seed file TA stream data into Splunk".
 - Text: "Directory path, where to generate the .seed file." followed by an empty text field.
 - WAS Findings Settings:**
 - Checkboxes for "Log Individual Findings" and "Log Web App Summary events".
 - Text: "Extra parameters to WAS Findings API. Enter as XML (e.g. <filters><Criteria".
 - Checkboxes for "Load WAS Findings data using multiple threads (resource intensive)" and "Number of threads to use (between 1 and 10)" with a value of `2`.
- Policy Compliance Settings:**
 - Note: "The PC feed does not pull the SCAP information."
 - Checkboxes for "Log individual PC Compliance Posture events" and "Log Policy Summary".
 - Checkbox for "Log 'All' details (when unchecked, logs 'Basic' details)".
 - Checkbox for "Enable multi-threading for PC Posture Information download".
 - Text: "Number of threads to use for PC Posture Information (max 10)" with a value of `2`.
 - Text: "Number of POLICY IDs to use for PC Posture Information (max 10)" with a value of `1`.
 - Text: "Extra parameters to pass to Posture Information API. Enter as URL Query (e action, output_format, details, status_changes_since, policy_id)" followed by an empty text field.
 - Proxy Configuration:**
 - Checkbox for "Use a proxy Server for Qualys API requests".
 - Text: "Proxy Server and credentials (e.g. 10.10.10.2:8080 OR username:password)" followed by an empty text field.
 - Debug:**
 - Checkbox for "Enable debug logs".

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.

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 indicate TA to do either a full data pull or an incremental pull on each run. By default, TA does incremental pull on each run. When selected, TA pulls the full host detection data from Qualys account and puts it on Splunk.

The "Enable .seed file generation?" option indicates 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 highly recommend you to get in touch with our support team before making changes to 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.

Can I filter the data indexed by Splunk?

Yes. You do this by entering API input parameters (in the Extra parameters fields) for the Host Detection API, WAS Findings API and Posture Information API. For example, only pull vulnerability data for certain hosts by specifying ips=10.10.10.2-10.10.10.10.

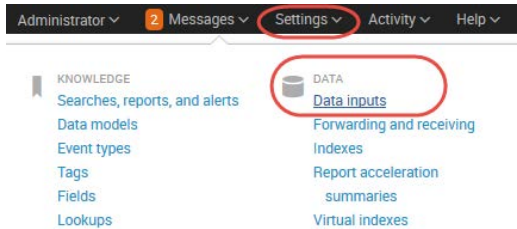
Go [here](#) to download the API Quick Reference Guide, API V2 User Guide and WAS API User Guide.

Do you support proxy?

Yes, we have proxy support! Tell us about your proxy server in the Proxy Configuration section.

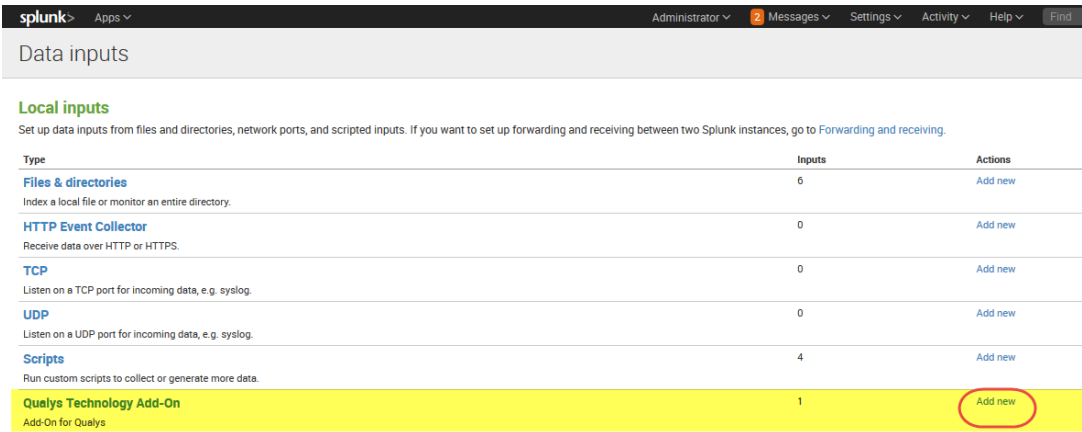
Configure Data Sync

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).

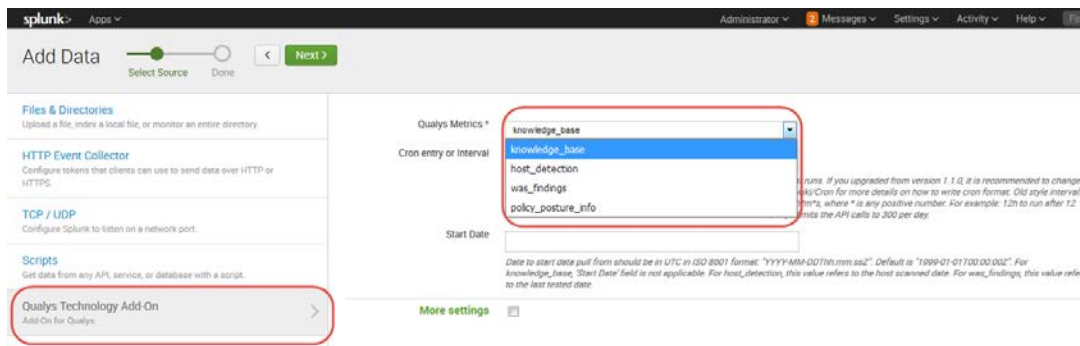


Go to Settings (on the top menu) and select Data Inputs.

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`.

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.

Qualys
Data inputs > Qualys

Showing 1-4 of 4 items

Results per page 25

Qualys Metrics	Cron entry or Interval	Start Date	Status	Actions
host_detection	48h	2017-12-09T00:00:00Z	Disabled	Enable Clone Delete
knowledge_base	12h	2017-12-09T00:00:00Z	Disabled	Enable Clone Delete
policy_posture_info	None	2017-12-09T00:00:00Z	Disabled	Enable Clone Delete
was_findings	48h	2017-12-09T00:00:00Z	Disabled	Enable Clone Delete

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.

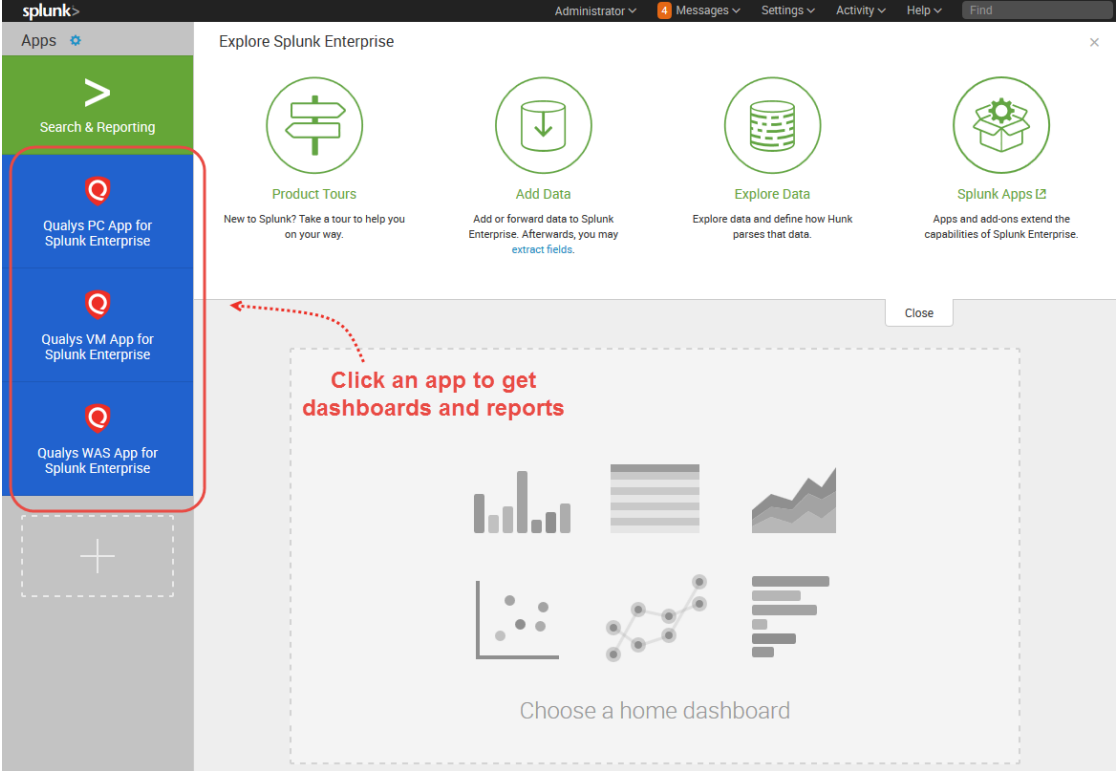
View your Qualys Data in Splunk!

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.

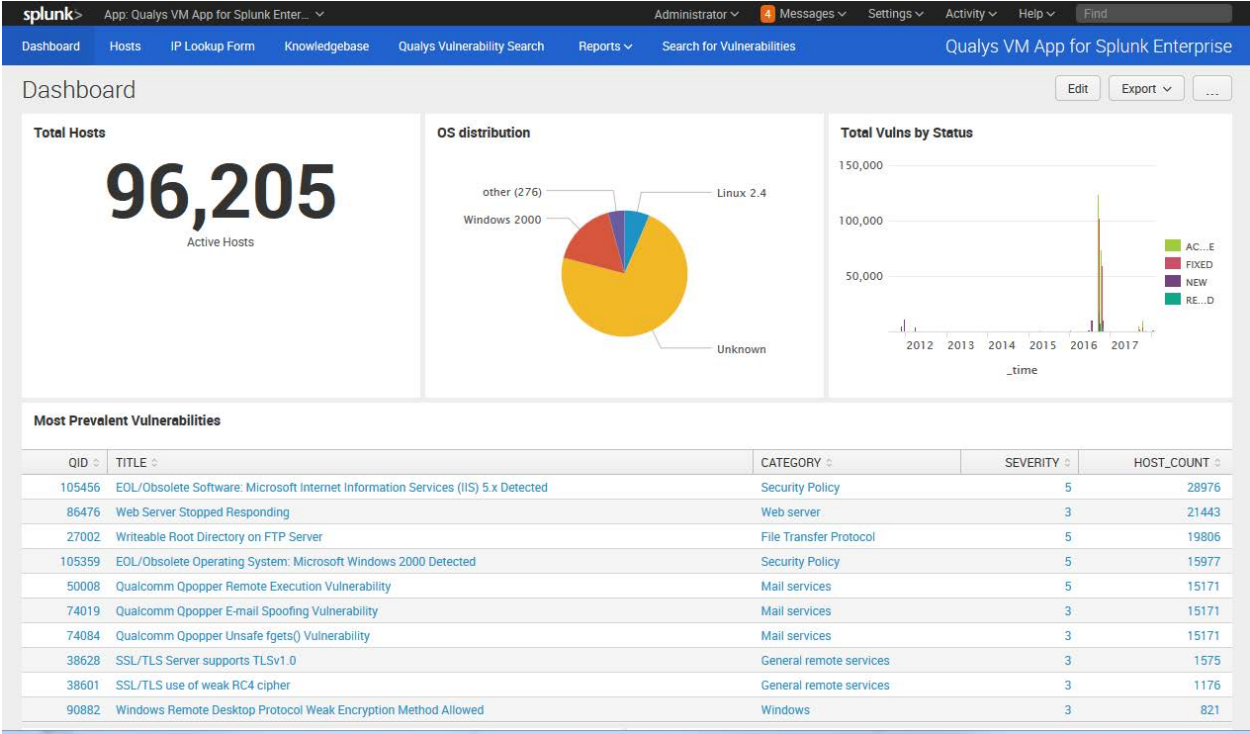
Simply download and install these apps. There is no setup needed!

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

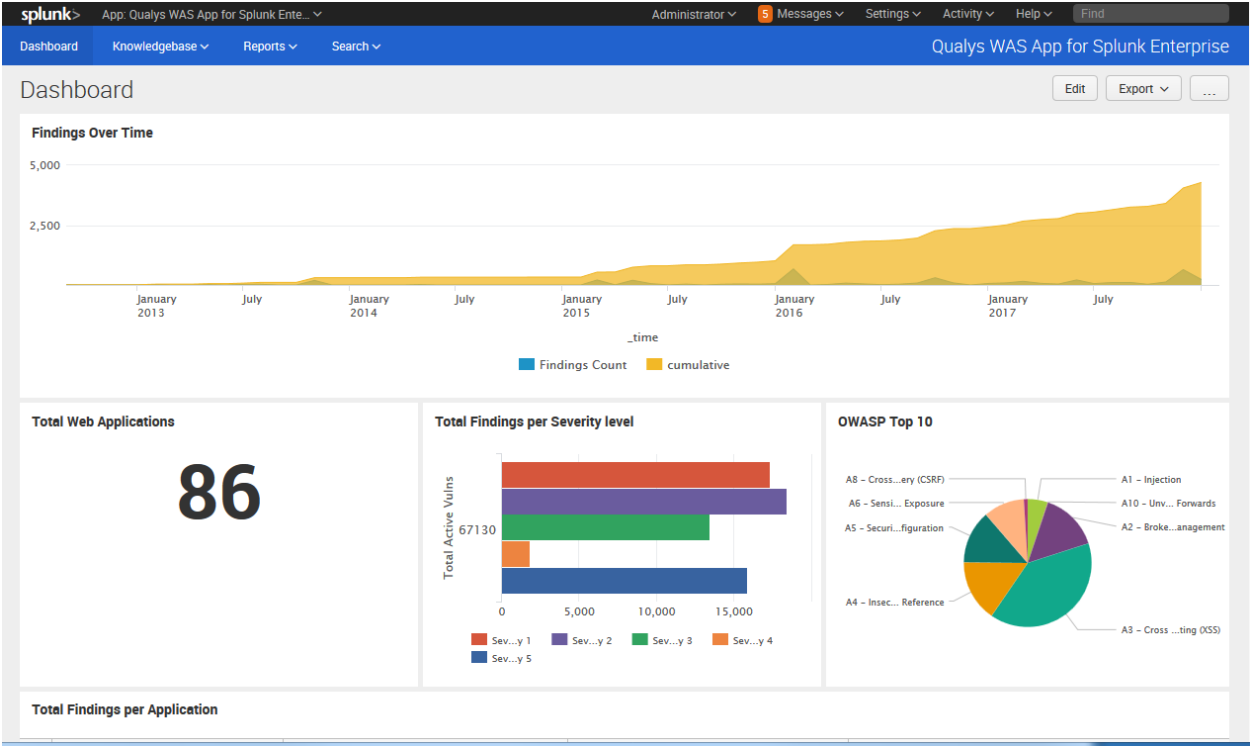
Once installed you'll see the new apps on your Splunk Home page. Click any app to view data.



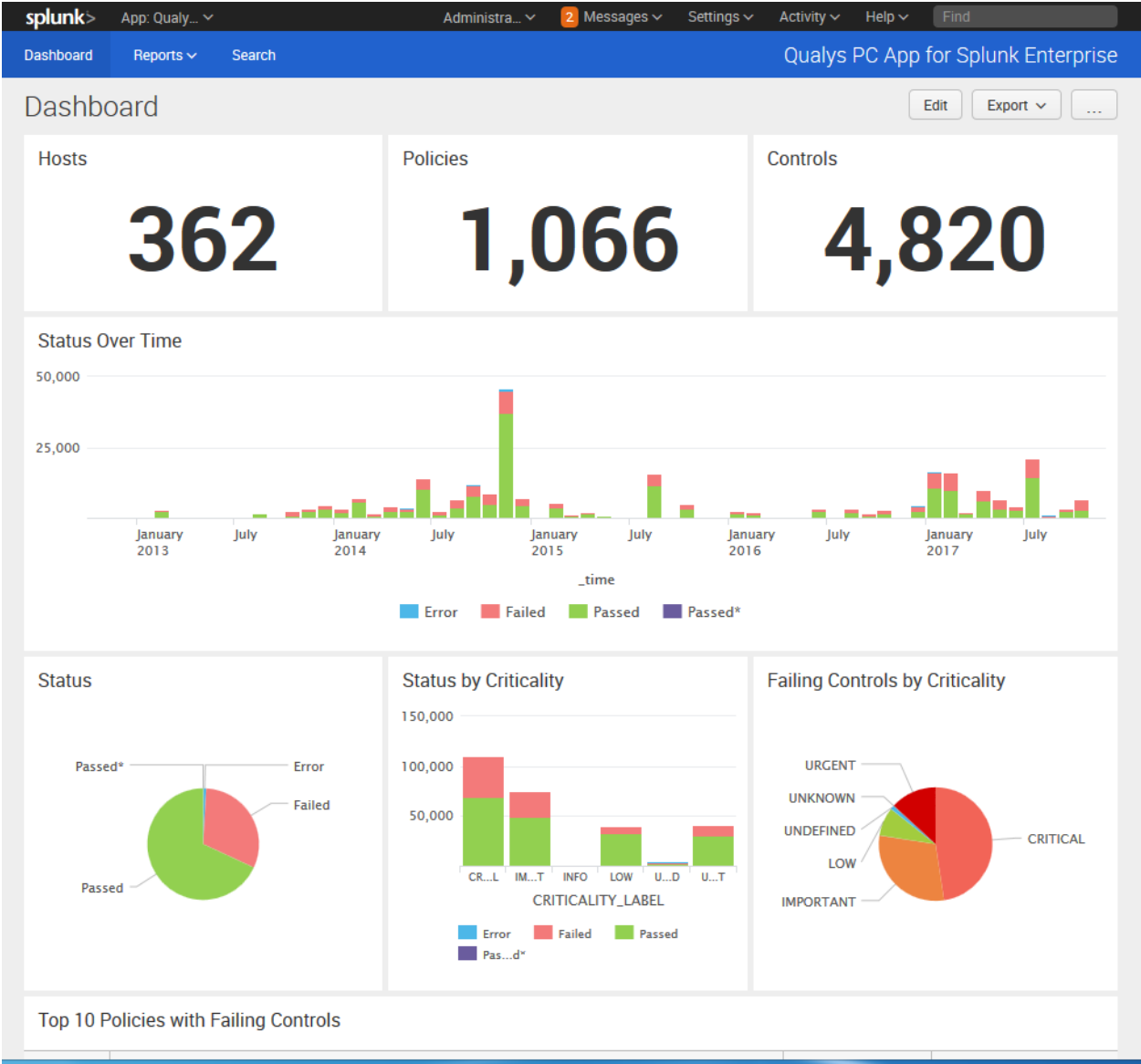
Sample VM Dashboard



Sample WAS Dashboard



Sample PC Dashboard

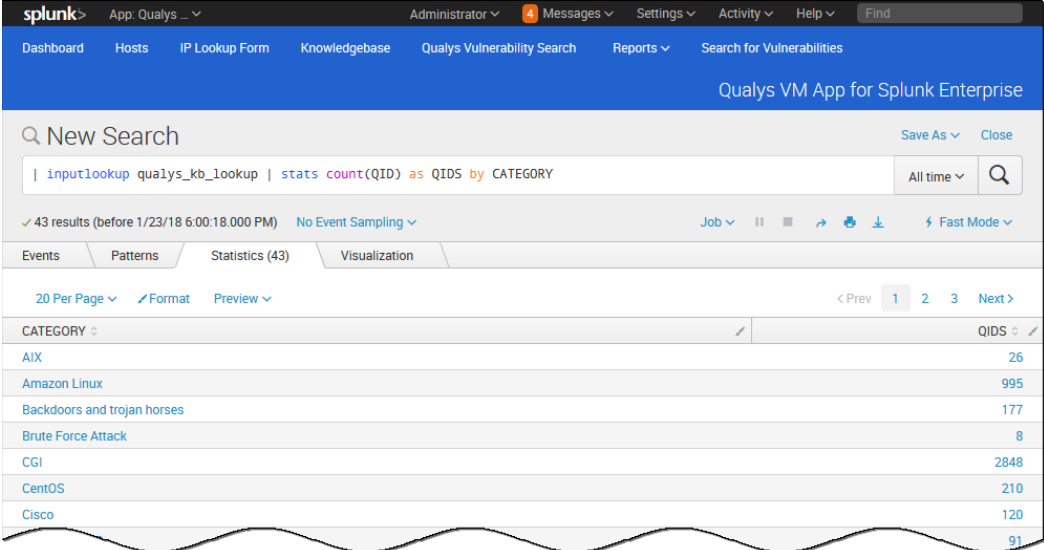


Search Your Qualys Data

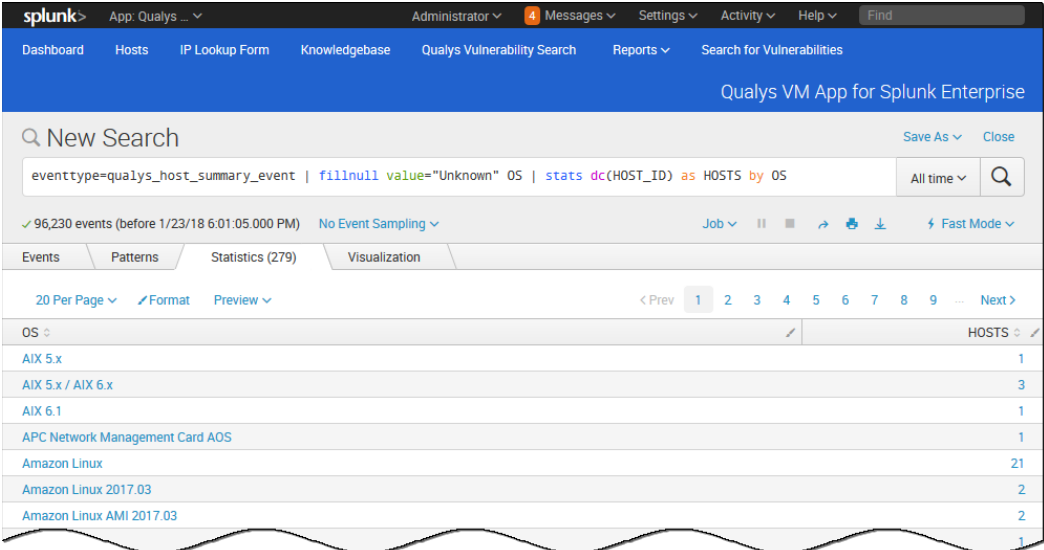
Choose Search & Reporting on the Splunk Home page. Then enter your search query in the search field.

Here are some sample search queries to get you started.

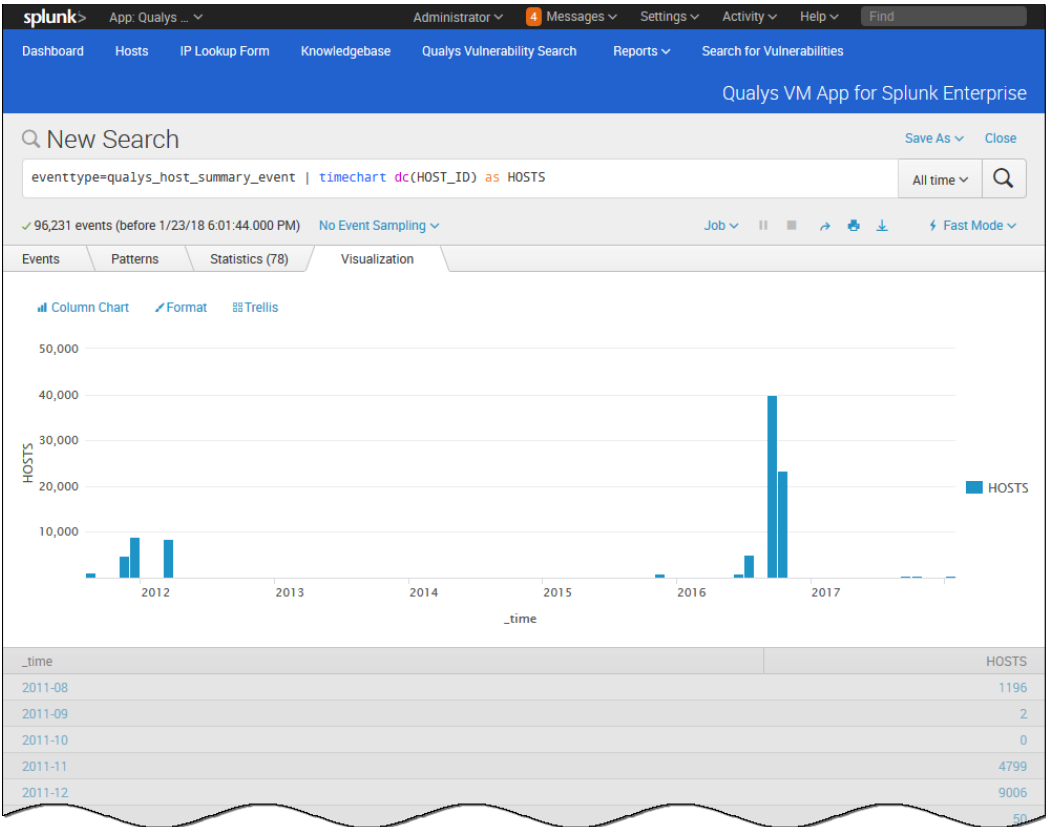
QIDs by Category



Host Distribution by OS



Scan Volume



Time since Last Scan

The figure is a Splunk dashboard titled "Time since Last Scan". It features a search bar with the query: `eventtype=qualys_host_summary_event ACTIVE_SEVERITY_5 > 0 | dedup 1 HOST_ID sortby -_time | eval epochevent =strptime(LAST_SCAN_DATETIME, "%Y=%m-%dT%H:%M:%SZ") | eval epochnow=now() | eval "Time Since Last Scan" =tostring(epochnow-epochevent, "duration") | sort 100 - "Time Since Last Scan" | table HOST_ID, IP, OS, DNS, LAST_SCAN_DATETIME, ACTIVE_SEVERITY_5, "Time Since Last Scan"`. The search results show 100 events. A table visualization displays the following data:

HOST_ID	IP	OS	DNS	LAST_SCAN_DATETIME	ACTIVE_SEVERITY_5	Time Since Last Scan
170205765	192.168.1.122	Mac OS X 10.11.6	100366mbp15.local	2018-01-23T16:55:41Z	2	
171187073	192.168.1.200	Microsoft Windows 10 Home	emily-pc	2018-01-23T12:40:36Z	9	
193503863	10.0.204.246	Microsoft Windows 10	101834-t450	2018-01-23T01:35:36Z	3	

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: /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

```
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

```
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. [Click here](#) to learn how.

- 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:
```

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".

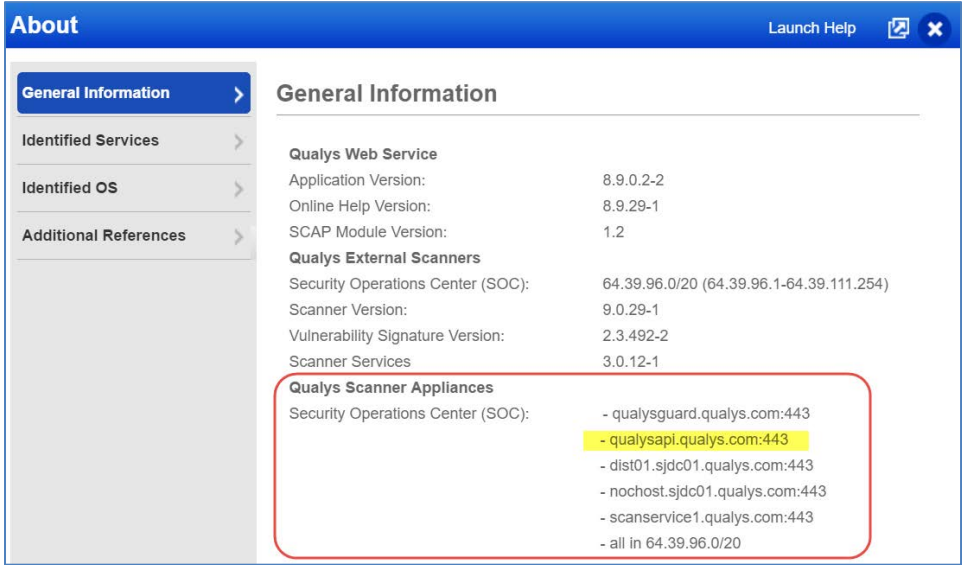
Note – RESULTS in host detection API output could be multi-line text. As we set KV_MODE = auto for hostDetection input in props.conf, we are not sure how Splunk will treat the events when RESULTS field is multi-line text. It may or may not consider the multi-line text to be the part of same single event.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

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.

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysapi.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysapi.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysapi.qg1.apps.qualys.in
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

You can easily find the API server URL for your account. Just log in to your Qualys account and go to Help > About. You'll see this information under Security Operations Center (SOC).



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.

```
HOSTSUMMARY: HOST_ID=227520646, IP="104.154.89.105", TRACKING_METHOD="IP", NETWORK_ID="0", DNS="105.89.154.104.bc.googleusercontent.com", LAST_SCAN_DATETIME="2018-09-18T12:06:35Z", LAST_VM_SCANNED_DATE="2018-09-18T11:59:44Z", LAST_VM_SCANNED_DURATION="371", SEVERITY_1=5, SEVERITY_2=3, INFO=5, CONFIRMED=3, POTENTIAL=0, NEW=0, ACTIVE=3, FIXED=0, RE-OPENED=0, _SEVERITY_1=5, ACTIVE_SEVERITY_2=3, INFO_SEVERITY_1=5, CONFIRMED_SEVERITY_2=3, TOTAL_VULNS=8
```

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

```
HOSTVULN: HOST_ID=190339320, IP="172.16.5.4", TRACKING_METHOD="AGENT", NETWORK_ID="0", OS="Ubuntu Linux 14.04.5", DNS="wordpress", LAST_SCAN_DATETIME="2018-09-19T02:47:26Z", LAST_VM_SCANNED_DATE="2018-09-19T02:43:34Z", SEVERITY=3, QID="370845", TYPE="POTENTIAL", SSL="0", STATUS="FIXED", FIRST_FOUND_DATETIME="2018-04-10T23:36:56Z", LAST_FOUND_DATETIME="2018-07-09T17:36:54Z", TIMES_FOUND="438", LAST_TEST_DATETIME="2018-09-19T02:43:34Z", LAST_UPDATE_DATETIME="2018-09-19T02:47:26Z", LAST_FIXED_DATETIME="2018-07-09T23:15:12Z", IS_IGNORED="0", IS_DISABLED="0"
```

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.

Last updated: September 26, 2018