



Indication of Compromise

Getting Started Guide

Version 2.4

June 10, 2020

Copyright 2017-2020 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

About this Guide	4
About Qualys	4
Qualys Support	4
Get Started	5
Steps to start investigating IOC incidents and events.....	5
Quickly get started using our online tutorial	5
Setting up asset tags (optional).....	6
Install Cloud Agents	7
Install Agents using the CA app	7
Activate your agents for IOC	8
Enable IOC in a configuration profile.....	9
IOC Investigation and response	10
How to Search.....	10
Hunting events	11
View event tree for an event	11
Investigate incidents	13
Look into assets monitored by IOC.....	13
Narrow your results	14
Download your results.....	15
Set Up Dynamic Dashboards	16
Using pre-defined IOC templates	16
Switching dashboards	16
Adding widgets	17
Resizing and layout	17
Refresh your view	17
Configure Rule Based Alerts for Events.....	18
Create a New Action	18
Create a New Rule	19
Manage Actions	23
Manage Rules	24
Manage Alerts	25

About this Guide

Thank you for your interest in Qualys Indication of Compromise (IOC). Qualys IOC expands the capabilities of the Qualys Cloud Platform to deliver threat hunting, detect suspicious activity, and confirm the presence of known and unknown malware for devices both on and off the network.

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 founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com

Qualys Support

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

Get Started

Qualys IOC helps you continuously monitor endpoints for suspicious activity. IOC captures system activity to find indicators of compromise relating to malware and indicators of activity relating to threat actors to support investigation and response. We'll help you get started quickly!

Steps to start investigating IOC incidents and events

Install lightweight agents in minutes on your IT assets. These can be installed on your on-premise systems, dynamic cloud environments and mobile endpoints. Cloud Agents (CA) are centrally managed by the cloud agent platform and are self-updating (no reboot needed).

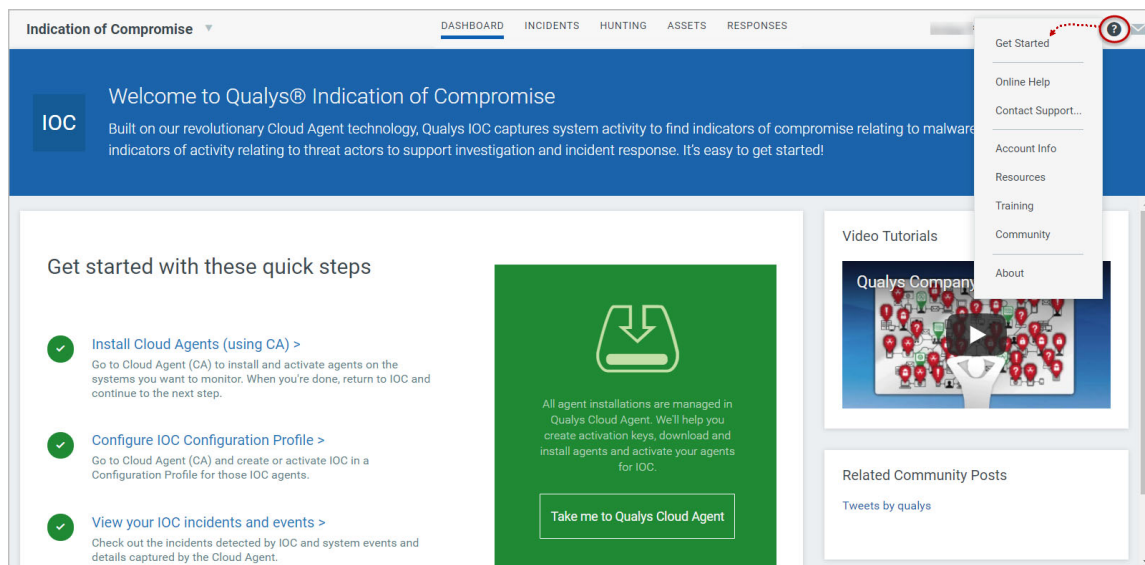
Enable IOC in a CA Configuration Profile and tell us which IOC artifacts you want to transmit to the Qualys Cloud Platform and at what interval.

View and investigate your IOC incidents and events in one central location. You'll see all incidents detected across all of your assets. Search all of your incidents and events in a matter of seconds.

We'll describe these steps in more detail in the sections that follow.

Quickly get started using our online tutorial

Just choose Get Started from the help menu and we'll walk you through the steps. Here you'll find links to helpful information.



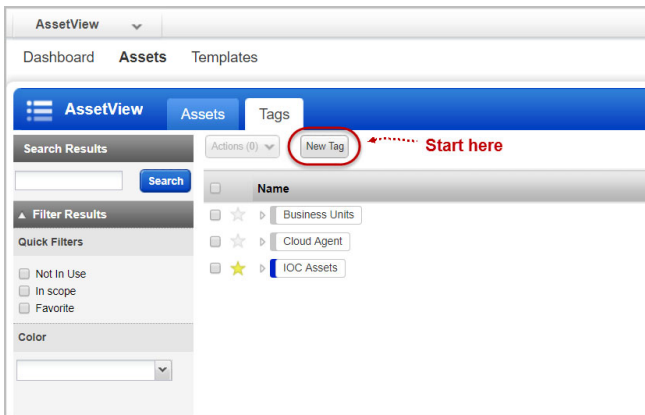
Setting up asset tags (optional)

Setting up asset tags using AssetView helps you to associate IOC assets with a CA configuration profile enabled for IOC. You can avoid assigning configurations manually to each asset by adding asset tags to the required CA configuration profiles.

How to create tags

Choose AssetView from the module picker.

Then go to Assets > Tags and click New Tag to add tags for your IOC assets. You can use a single tag or multiple tags to mirror your production configuration.



Not interested in tags? No problem. You can manually assign individual assets to your profiles.

Install Cloud Agents

You'll need to install a cloud agent that's been activated for IOC on each asset you want to monitor for suspicious activity.

Install Agents using the CA app

Choose Cloud Agent (CA) from the module picker.

Create an activation key. Go to Activation Keys, click the New Key button. Give it a title and provision for the IOC application and click Generate.

New Activation Key Turn help tips: On | Off

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: My activation key Select | Create

(no tags selected)

Provision Key for these applications

<input checked="" type="checkbox"/> VM Vulnerability Management 1000 Licenses Remaining	<input type="checkbox"/> PC Policy Compliance 1000 Licenses Remaining
<input type="checkbox"/> FIM File Integrity Monitoring (Beta) 99 Licenses Remaining	<input checked="" type="checkbox"/> IOC Indication of Compromise 96 Licenses Remaining

☐ Set limits

Close Unlimited Key **Generate**

As you can see you can provision the same key for any of the other applications in your account.

New Activation Key Turn help tips: On | Off

New activation key generated successfully

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

Activation Key: [Yellow Key] ✓

Key Type: Unlimited key

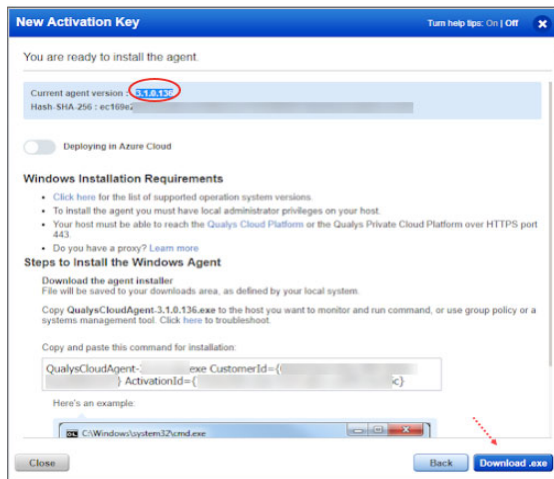
Installation Requirements

Windows (.exe)	x86-32/64	Microsoft Windows Client Microsoft Windows Server	Install instructions
Linux (.rpm)	x64	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Enterprise Linux Amazon Linux Oracle Enterprise Linux	Install instructions
Linux (.rpm)	ARM64	Red Hat Enterprise Linux CentOS Amazon Linux	Install instructions

Close

Click on Install Instructions against the Windows (exe) option.

Want to do this step later? No problem, just exit the wizard. When you're ready, return to your activation keys list, select the key you want to use, then Install Agent from the Quick Actions menu.

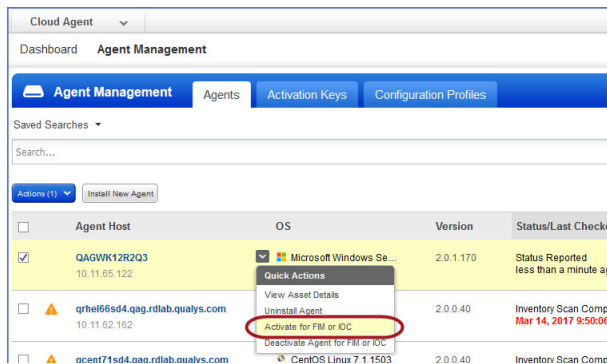


Review the installation requirements and click Download.

You'll run the installer on each host from an elevated command prompt, or use a systems management tool or Windows group policy.

Your agents should start connecting to our cloud platform.

Activate your agents for IOC



On the Agents tab choose your agent and "Activate for FIM or IOC" from the Quick Actions menu. (Bulk activation is supported using the Actions menu).

Enable IOC in a configuration profile

Go to the “Configuration Profiles” tab, create a new profile or edit an existing one. Walk through the profile creation wizard. When you get to the IOC tab:

(1) Toggle Enable IOC module for this profile to ON. This is required for IOC data collection to occur.

(2) Configure what IOC artifacts are transmitted to the Qualys Cloud Platform. Defaults are provided as shown, so this step is optional. You can configure values for process mutex, registry, and file location groups 1-3.

These settings constitute the time lapse after which the following types of IOC events are transmitted to the Qualys Cloud Platform:

Process Mutex	Events related to running processes and mutex
Registry	Events related to likely registry locations indicating the presence of malware
File Locations Group 1	Events specific to user file paths such as C:\Users*
File Locations Group 2	Events specific to system file paths such as C:\Program Files*, C:\Program Files (x86)*, or C:\Windows*
File Locations Group 3	This setting is not supported at this time

Note: Process Mutex and Registry values are available based on your subscription. Contact Qualys Support for more information.

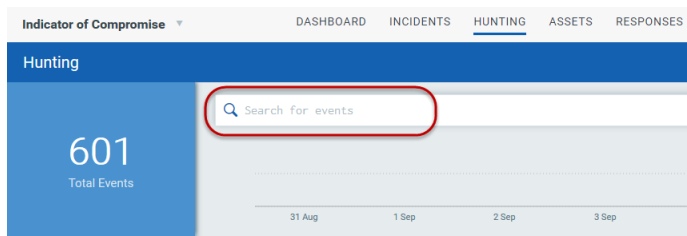
What's next?

IOC starts collecting data and analyzing your systems right away! Return to the IOC app where you can check out the incidents detected by IOC and system events and details captured by the cloud agent.

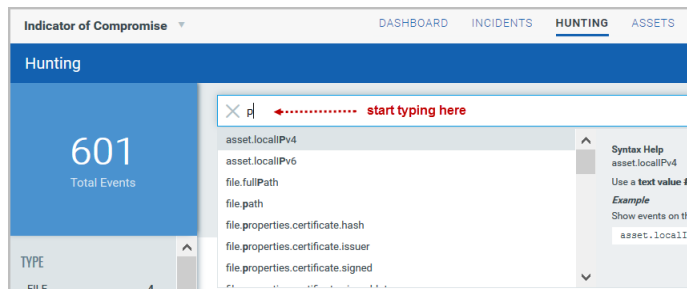
IOC Investigation and response

How to Search

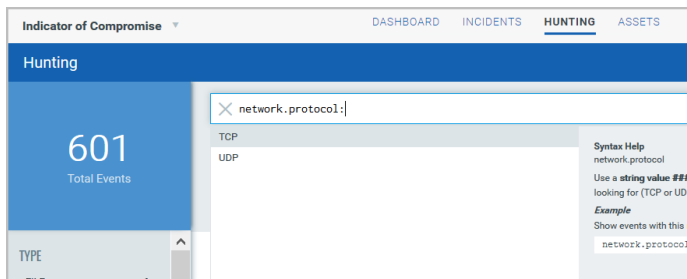
Our searching and filtering capabilities give you the ability to quickly find all about your incidents, events and assets all in one place using Qualys Advanced Search. You can search for incidents and assets in the respective tabs in the similar way.



You'll notice the Search box while viewing dynamic lists of events, incidents, and assets. This is where you'll enter your search query.



Start typing and we'll show you the asset properties (fields) you can search like `asset.localIPv4`, `file.path`, etc. and scroll down to see all the fields.

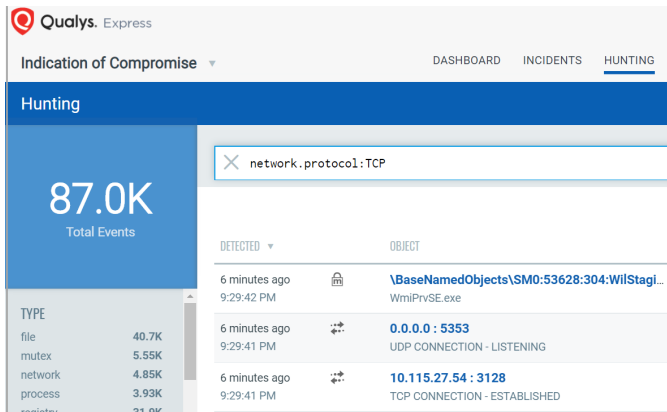


Select the one you're interested in. Check out the Syntax help for the selected field to the right to help with creating your query.

Enter the value you want to match. For this field you select from a list of predefined values.

Tip - Go to the IOC online help for details on search language and sample queries.

Then hit Enter.

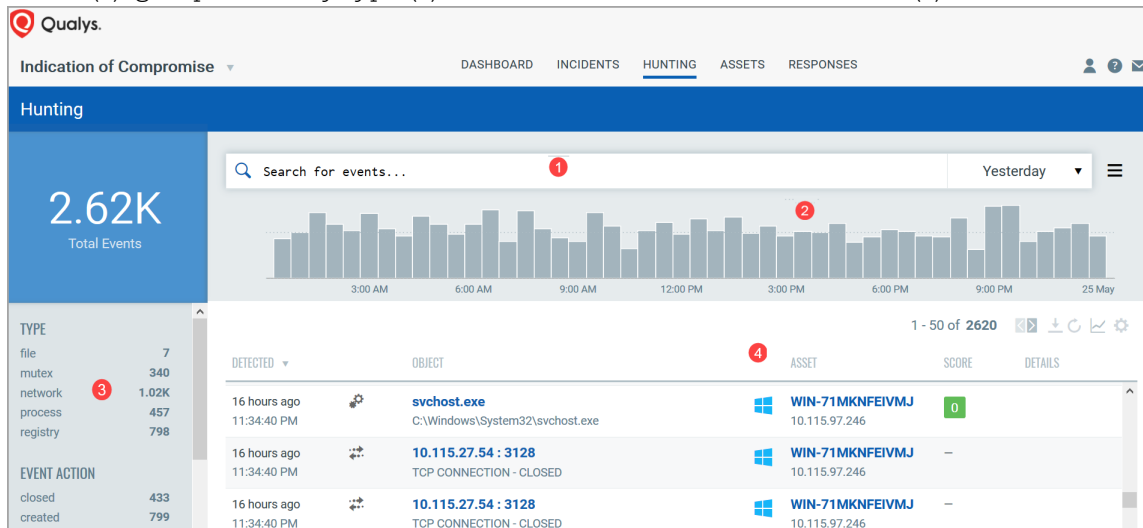


That's it! Your matches will appear in the list your viewing. Filters on the left help you drill down to objects of interest.

Tip - Use your queries to create dashboard widgets on the Dashboards tab.

Hunting events

Search for events by event properties (1), jump to events that occurred in certain time-frame (2), group events by type (3), view event details and asset details (4).



View event tree for an event

On the Event Details page, we show event tree for events that are of types Process, Mutex and Network. In the event tree, we show all the events that are related to an event. Event tree view will show maximum 3 levels of hierarchies for an event.

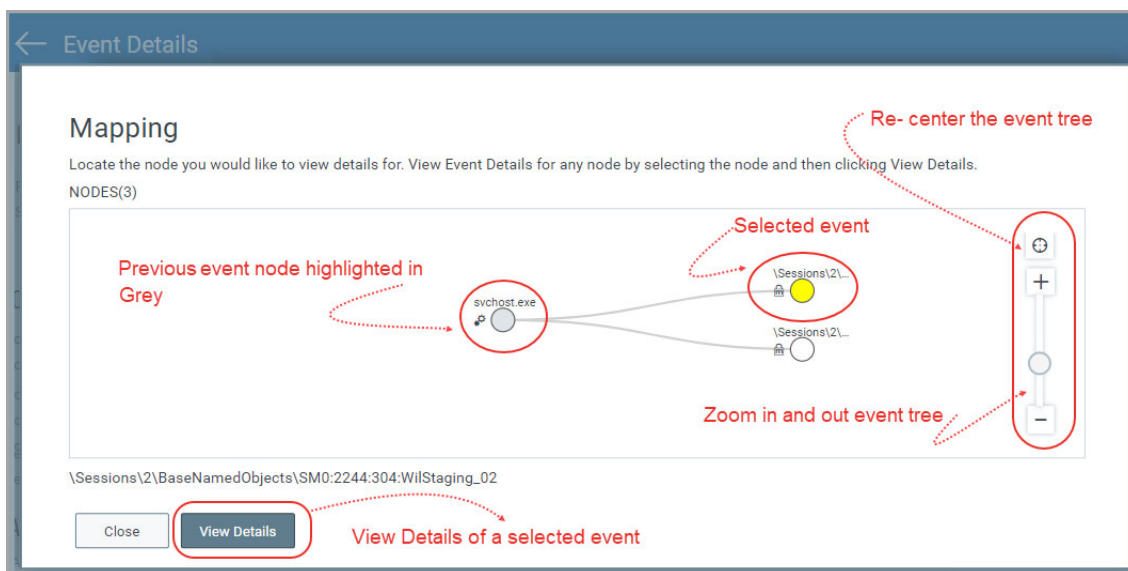
An event of "Process" type will show its parent and child processes along with the mutex and network connection of the process. For event of Network type, you see network connection of a process and for event of Mutex type, mutex connection of a process. In the event tree view, the selected event node is highlighted in yellow and child nodes are shown in white.

You can traverse between the nodes by clicking a node in the hierarchy. When you traverse from one event node to another, the selected node is shown in yellow and the node from which you traversed will be shown in Grey.

When you click on an event node in the tree view, we load the tree for the selected event and show its parent and child nodes. The Event Details page will show you the details of the selected node when you click View Details.

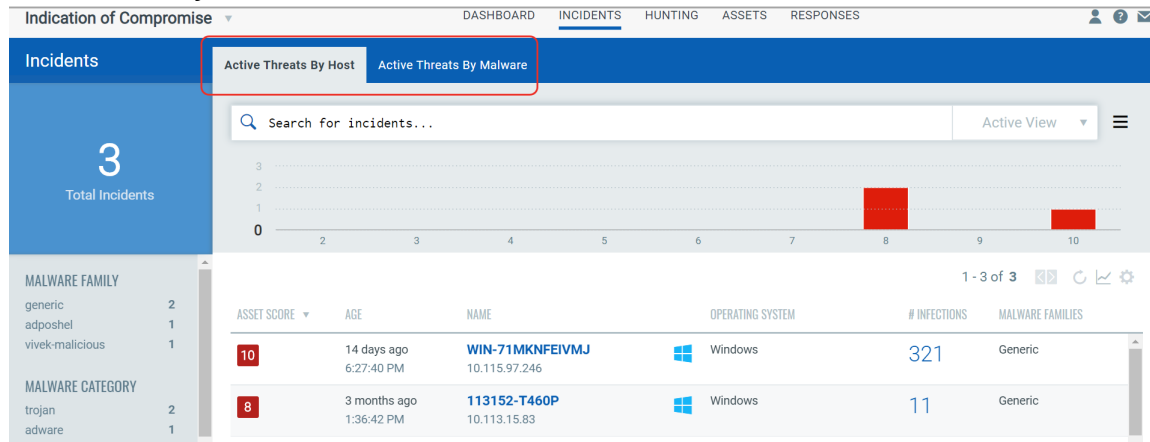
To help you identify event types of nodes in a hierarchy view, all the nodes will display the respective icons associated with that event type.

Event's tree view displays a zoom bar to zoom in and out the event's tree. Zoom bar has plus and minus button for this purpose. It has a re-center button to restore the tree to the center of the screen with its original size.



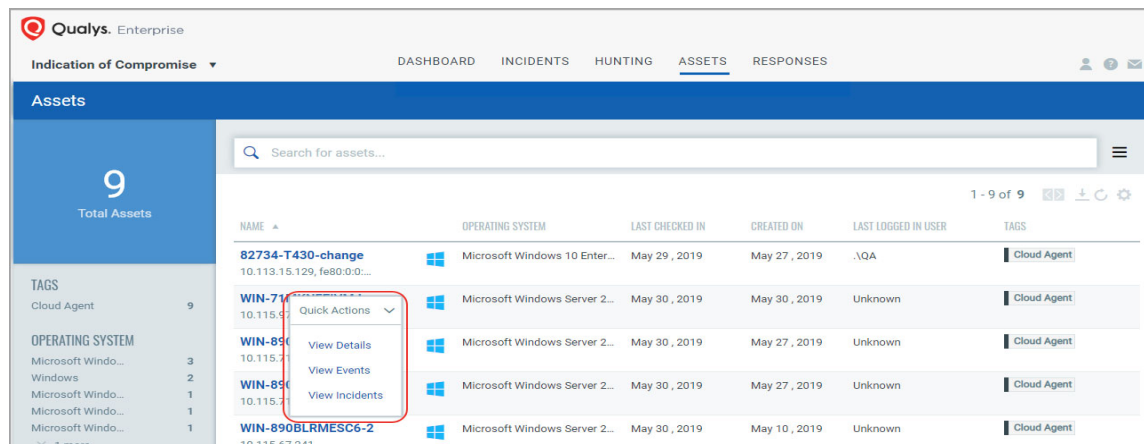
Investigate incidents

Investigate incidents by Active Threats By host, Active Threats by Malware name and malware family name.



Look into assets monitored by IOC

Get up to date views on a selected asset's details, its events and incidents.



Narrow your results

Once you have your search results you may want to organize them further into logical groupings. Choose a group by option on the left side. You'll see the number of events or assets per grouping. Click on any grouping to update the search query and view the matching incidents or events.

The screenshot shows the Qualys Enterprise Hunting interface. On the left, a sidebar displays the total number of events (168K) and two filter categories: TYPE and EVENT ACTION. A red box highlights these filters, and a red arrow points from the 'TYPE' section to the first event in the list. The main area shows a search bar and a table of detected events.

Qualys. Enterprise

Indication of Compromise ▾ DASHBOARD INCIDENTS **HUNTING** ASSETS R

Hunting

168K
Total Events

TYPE

file	18.6K
mutex	3.65K
network	841
process	1.36K
registry	143K

EVENT ACTION

created	162K
established	72
listening	770
running	5.00K

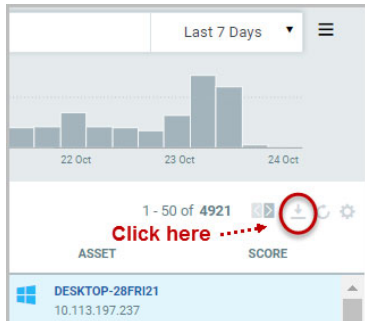
Search for events...

Select an option to narrow your results

DETECTED ▾	OBJECT
in 12 hours 5:56:54 AM	svchost.exe C:\Windows\System32\svchost.exe
in 12 hours 5:56:54 AM	QualysAgent.exe C:\Program Files\Qualys\QualysAgent\QualysAgent.exe
in 12 hours 5:56:54 AM	10.115.27.54 : 3128 TCP CONNECTION - ESTABLISHED by explorer.exe
in 12 hours 5:56:38 AM	explorer.exe C:\Windows\explorer.exe
in 12 hours 5:56:30 AM	svchost.exe C:\Windows\System32\svchost.exe
in 12 hours 5:46:52 AM	HKLM\System\CurrentControlSet\Services\W32... SecureTimeEstimated: 132036903081032425

Download your results

By downloading search results to your local system you can easily manage incidents or events outside of the Qualys platform and share them with other users. You can export results in multiple formats (CSV, XML, PDF, DOC, PPT, HTML-ZIP, HTML-Web Archive).



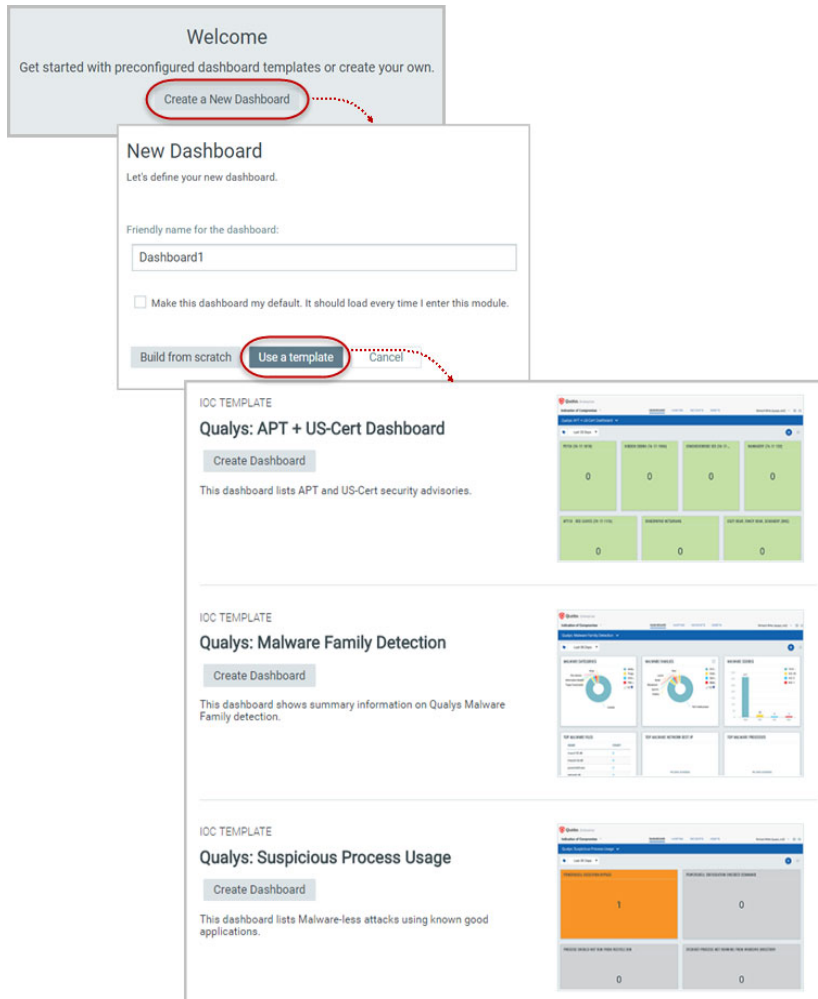
Just click the Download icon above the incidents list, choose a format and click Download.

Set Up Dynamic Dashboards

You can create multiple dashboards and switch between them. Each dashboard has a collection of widgets showing data of interest.

Using pre-defined IOC templates

The first time you create a new dashboard you are presented with an option to create the dashboard using pre-created templates for IOC.

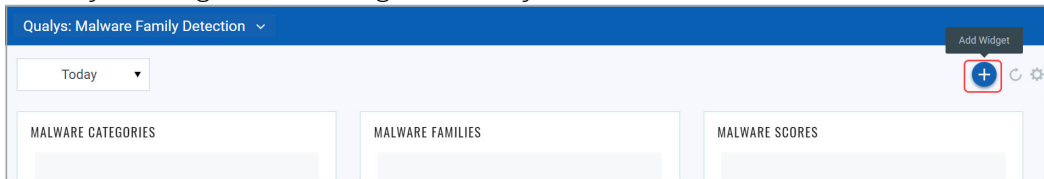


Switching dashboards

It's easy to do. Just click the down arrow next to the dashboard name and pick the one you want.

Adding widgets

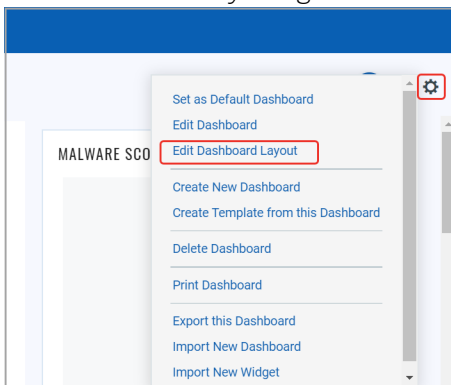
Start by clicking the Add Widget icon on your dashboard.



Pick one of our widget templates - there are many to choose from - or create your own. Each widget is unique. For some you'll select data, provide a query and choose a layout - count, table, bar graph, pie chart. Wondering how we created the widgets on the default dashboard? Choose Edit from the widget menu to see the exact settings.


Resizing and layout

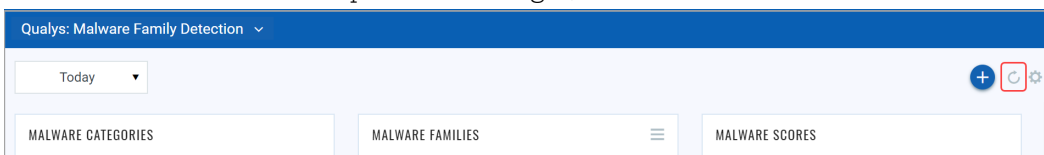
You can resize any widget horizontally, and drag & drop widgets to change the layout.



Click the Tools icon on your dashboard and then select Edit Dashboard Layout. Adjust the width for any widget or drag the widget to a new location. Click OK to save your changes.

Refresh your view

To see the latest data for a particular widget, select  icon to refresh.

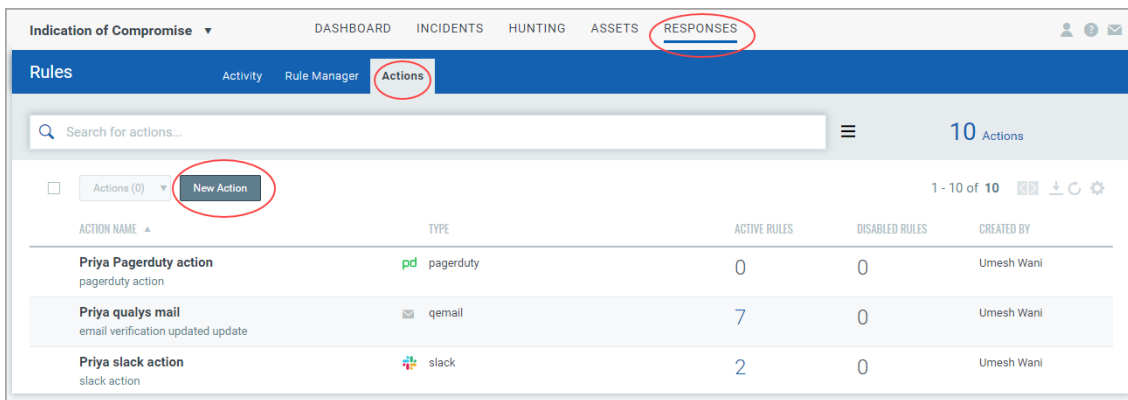


Configure Rule Based Alerts for Events

You can configure IOC to monitor events for conditions specified in a rule and send you alerts if events matching the condition is detected. For IOC to send alerts, you need to first configure a rule action to specify what action to be taken when events matching a condition is detected. IOC will use the rule action settings to send you the alerts. Finally, create a rule to specify the conditions for triggering the rule and select rule actions for sending the alert when a rule is triggered.

Create a New Action

To create an action, go to Responses > Actions > New Action..



Provide required details in the respective sections to create a new action:

- In the Basic Information section, provide name and description of the action in the Action name and Description fields respectively.
- Select an action from the Select Action drop-down and provide the settings for configuring the messaging system that IOC will use to send alerts.
- We support these three actions: Send Email (Via Qualys), Post to Stack and Send to Pager Duty for alerts.
- Select Send Email (Via Qualys) to receive email alerts and specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message.
- Select "Send to PagerDuty" to send alerts to your PagerDuty account. Provide the service key that IOC will require to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.

← Create New: Action

Basic Information

Action Name

Required

Description

Required

Add a brief description for this action

Select Action

Required

Send Email(Via Qualys)

Default Message Settings

You can add default recipients or edit the default message to be sent

Recipients

Required

Separate emails using commas (,) between addresses

Subject Line

Required


Message

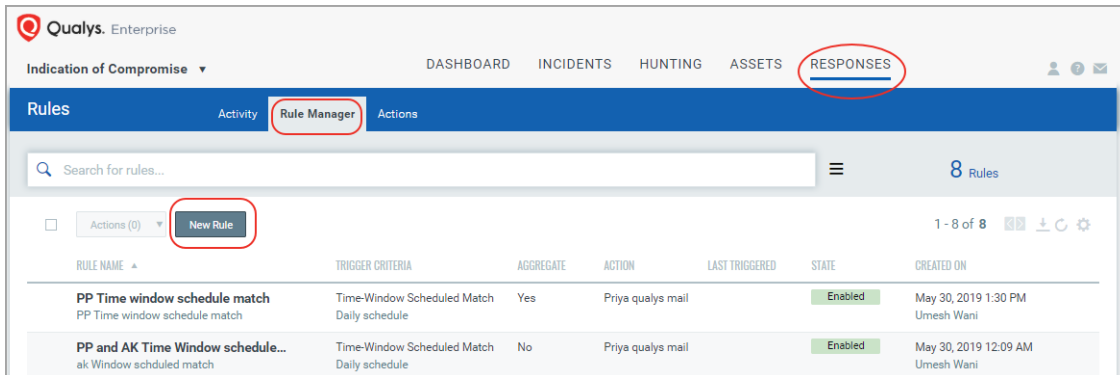
Required

7/5000

Create a New Rule

To create a rule, go to Responses > Rule Manager > New Rule. You can also create rules from the customized queries that are used for widgets on your dashboard. Select the Widget menu and choose “Create Rule from this Widget”. This option is also available on

the Hunting page. Go to the Hunting tab, select an event filter in the left pane or type a search query in the search bar. Click actions menu  on the right of the search bar and select “Create Rule from Search Query” from the menu.



Provide required details in the respective sections to create a new action:

- In the Rule Information section, provide a name and description of the new rule in the Rule Name and Description.
- In the Rule Query section, specify a query for the rule. The system uses this query to search for events. Use the Test Query button to test your query. Click Sample Queries link to select from predefined queries.
- You can choose from three trigger criteria that work in conjunction with the rule query. The trigger criteria are: Single Match, Time-Window Count Match and Time-Window Scheduled Match.
- In the Action Settings section choose the actions that you want the system to perform when an alert is triggered.

← Create New: Rule

Rule Details

Provide the following information to create the rule

Rule Information

Rule Name Required
Rule for score indicator

Description Required
Add a brief description for this rule

Rule Query

Provide a query to match particular source that will trigger the alert Required
X indicator.score: [8,9,10]

Sample Queries Test Query

Trigger Criteria

Provide the match criteria Required
Trigger Criteria
Single Match

Action Settings

Choose an appropriate alert action Required
Actions
X Priya Pagerduty action

Priya Pagerduty action

Description Required
Pagerduty Alert from POD1

Message Required
Insert token
Pager duty message body 23/5000

Cancel Save

Trigger Criteria

- Select Single Match if you want the system to generate an alert each time the system detects an event matching your search query.
- Select Time-Window Count Match when you want to generate alerts based on the number of events returned by the search query in a fixed time interval. For example, an alert will be sent when three matching events are found within 15 mins window.

← Create New: Rule

Trigger Criteria

Provide the match criteria

Trigger Criteria

Time-Window Count Match

Time-Window Count Match

No Of Matching Events

3

In

15

Mins

Aggregate Alerts

Yes

Aggregate Group

Action

Select Time-Window Scheduled Match when you want to generate alerts for matching events that occurred during a scheduled time. The rule will be triggered only when an event matching your search criteria is found during the time specified in the schedule. Choose a date and time range for creating a schedule and specify how often you want to run the schedule for example, daily, weekly and monthly. For example, send daily alerts with all matches in a scheduled window between 4 pm and 5 pm.

← Create New: Rule

Trigger Criteria

Provide the match criteria

Trigger Criteria

Time-Window Scheduled Match

Time-Window Schedule Match

Time Window Starts on

06/03/2019

Start Time

4:56pm

Time Window Ends On

06/03/2019

End Time

5:56pm

Duration

1.00Hrs

Repeats

Daily

Summary: Repeats everyday from 04:56 pm to 05:56 pm (1.00 hours)

Aggregate Alerts

Yes

Aggregate Group

Action

For the Weekly option, select the days of the week on which schedule will run. For example, send weekly alerts with all matches generated between 4.56 pm and 5.56 pm on every Monday and Wednesday.

Create New: Rule

Repeats: **Weekly**

On Day Of The Week: ☐ S ☒ M ☐ T ☒ W ☐ T ☐ F ☐ S

Summary: Repeats **monday** from **04:56 pm** to **05:56 pm** (1.00 hours)

For the Monthly option, specify the day of the month on which the schedule will run. For example, send monthly alerts on the first day of every month.

Create New: Rule

Repeats: **Monthly**

Recurring Day: **1** day of the month

Summary: Repeats every 1st day of the month from **04:56 pm** to **05:56 pm** (1.00 hours)

For “Select Time-Window Count Match” and “Select Time-Window Scheduled Match”, you have the option to aggregate the alerts by aggregate groups such as based on action, asset hostname and so on.

Manage Actions

View the newly created actions in the Actions tab with the details such as name of the action, type of the action, the number of rules for which this action is chosen are active or inactive and the user who created the rule. You can use the Actions menu or Quick Actions menu to edit, delete and rename an action. Use the search bar to search for actions using the search tokens.

Indication of Compromise ▾ DASHBOARD INCIDENTS HUNTING ASSETS **RESPONSES**

Rules Activity Rule Manager **Actions**

Search for actions... 10 Actions

ACTION NAME	TYPE	ACTIVE RULES	DISABLED RULES	CREATED BY
<input checked="" type="checkbox"/> Priya Pagerduty action pagerduty action	pd pagerduty	0	0	Umesh Wani
Priya qualys mail email verification updated update	qemail	7	0	Umesh Wani
Priya slack action slack action	slack	2	0	Umesh Wani
Qualys mail action test Qualys mail action test	qemail	0	0	Umesh Wani
Test Action test	qemail	0	0	Umesh Wani

Quick Actions menu (for Priya Pagerduty action):
 Edit
 Save As
 Delete

Manage Rules

Rule Manager tab lists all the rules that you have created with rule name, trigger criteria selected for the rule, alert message aggregating enabled or disabled for the rule, action chosen for the rule, date and time when the rule is last triggered and state of the rule, whether the rule is enabled or disabled and created date and time of the rule.

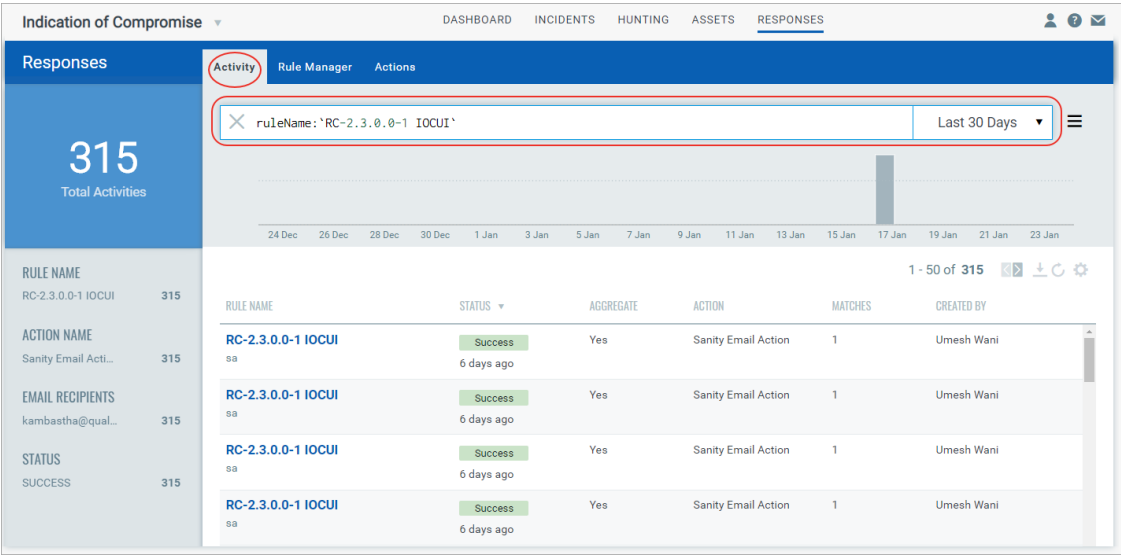
You can use the Actions menu or Quick Actions menu to edit, enable, disable, delete and rename a rule. Use the search bar to search for rules using the search tokens.

The screenshot shows the 'Rule Manager' tab in the 'Responses' section. The interface includes a search bar, a 'New Rule' button, and a table of rules. A 'Quick Actions' menu is open for the 'Antarctica/Mawson' rule, showing options: Edit, Enable, Disable, Save As, Delete, and Show Activity. The table lists 8 rules with columns for Rule Name, Trigger Criteria, Aggregate, Action, Last Triggered, State, and Created On.

RULE NAME	TRIGGER CRITERIA	AGGREGATE	ACTION	LAST TRIGGERED	STATE	CREATED ON
Action_Neha Update Action_Neha	Single Match	—	Action_Neha	January 15, 2020 3:05 PM	Enabled	January 15, 2020 3:04 PM Umesh Wani
Antarctica/Mawson Antarctica/Mawson	Time-Window Scheduled Match Daily schedule	Yes	PD sanity 8aug		Enabled	January 3, 2020 6:02 PM Umesh Wani
Demo IOC-UI_copy Demo IOC-UI Update Rule 2	Single Match	—	Demo IOC-UI	January 15, 2020 3:05 PM	Disabled	January 3, 2020 5:37 PM Umesh Wani
EST rule_copy EST rule	Time-Window Scheduled Match Daily schedule	Yes	Email Action AK		Enabled	January 3, 2020 5:37 PM Umesh Wani
Improtant Tokens Check subset of tokens are tested	Single Match	—	KA_Rule_EmailQ...	January 15, 2020 3:05 PM	Disabled	December 11, 2019 10:09 AM Umesh Wani
PP windows count match PP windows count match, I...	Time-Window Count Match Runs after every 5 matches in 1...	Yes	Priya qualys mail		Disabled	January 3, 2020 6:02 PM Umesh Wani
RC-2.3.0.0-1 IOCUI sa	Single Match	—	Sanity Email Acti...	January 16, 2020 11:03 AM	Disabled	January 16, 2020 10:40 AM Umesh Wani

View all the Alerts for a Rule

You can go to the Responses > Rule Manager tab and choose the “Show Activity” option in Quick Actions menu to view all the alerts generated for a rule. When you select “Show Activity” we will take you to the Activity tab, filter the alerts by selected rule and list them.



Manage Alerts

Activity tab lists all the alerts. Here you will see for each alert, rule name, success or failure in sending the alert message, aggregate enabled (Yes) or disabled (No) for the rule, action chosen for the rule, matches found for the rule and the user who created the rule.

Search for alerts using our search tokens (1), select a period to view the rules triggered during that time frame (2), click any bar to jump to the alerts triggered in a certain timeframe (3), use these filters to group the alerts by rule name, action name, email recipients and status (4).

