Indication of Compromise

Getting Started Guide

September 6, 2018

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

Table of Contents

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).

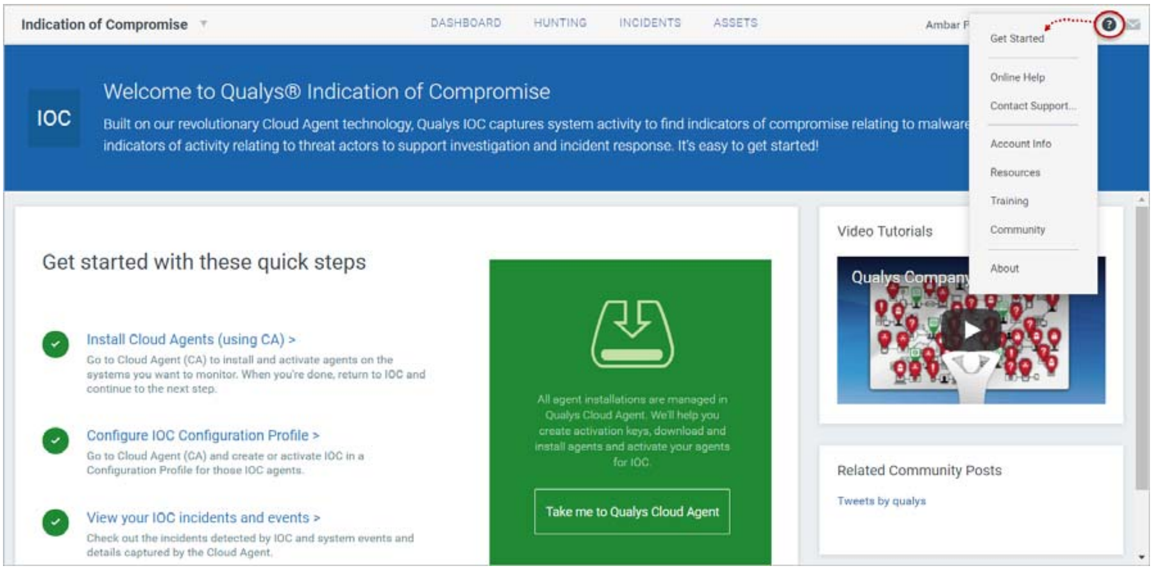
Enable IOC in a CA Configuration Profile and tell us which IOC artifacts you want to transmit to the Qualys Cloud Platform and at what interval.

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.



Welcome to Qualys® Indication of Compromise

Built on our revolutionary Cloud Agent technology, Qualys IOC captures system activity to find indicators of compromise relating to malware indicators of activity relating to threat actors to support investigation and incident response. It's easy to get started!

Get started with these quick steps

Install Cloud Agents (using CA) >
Go to Cloud Agent (CA) to install and activate agents on the systems you want to monitor. When you're done, return to IOC and continue to the next step.

Configure IOC Configuration Profile >
Go to Cloud Agent (CA) and create or activate IOC in a Configuration Profile for those IOC agents.

View your IOC incidents and events >
Check out the incidents detected by IOC and system events and details captured by the Cloud Agent.

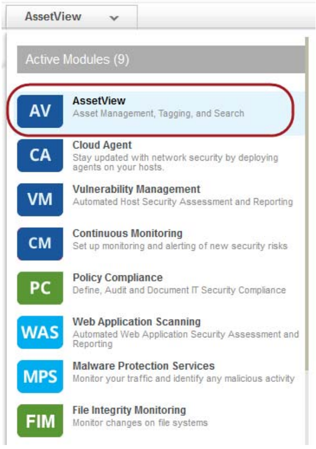
All agent installations are managed in Qualys Cloud Agent. We'll help you create activation keys, download and install agents and activate your agents for IOC.

Setting up asset tags (optional)

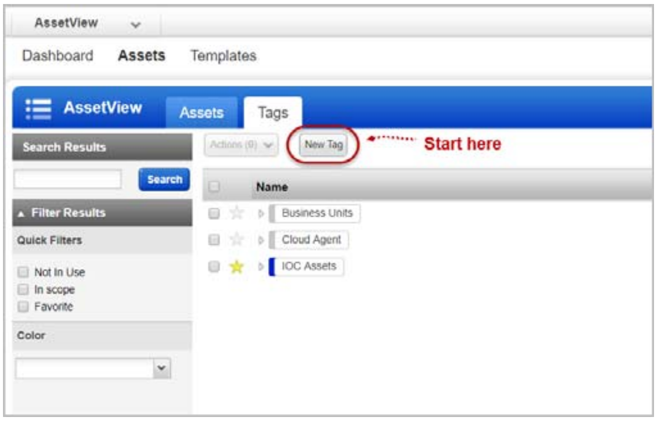
Setting up asset tags using AssetView helps you to associate IOC assets with a CA configuration profile enabled for IOC. You can avoid assigning configurations manually to each asset by adding asset tags to the required CA configuration profiles.

How to create tags

Go to AssetView to get started.


AssetView
Active Modules (9)
AV AssetView
Asset Management, Tagging, and Search
CA Cloud Agent
Stay updated with network security by deploying agents on your hosts.
VM Vulnerability Management
Automated Host Security Assessment and Reporting
CM Continuous Monitoring
Set up monitoring and alerting of new security risks
PC Policy Compliance
Define, Audit and Document IT Security Compliance
WAS Web Application Scanning
Automated Web Application Security Assessment and Reporting
MPS Malware Protection Services
Monitor your traffic and identify any malicious activity
FIM File Integrity Monitoring
Monitor changes on file systems

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.



Start here

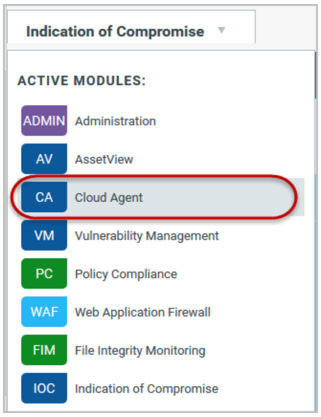
Not interested in tags? No problem. You can manually assign individual assets to your profiles.

Install Cloud Agents

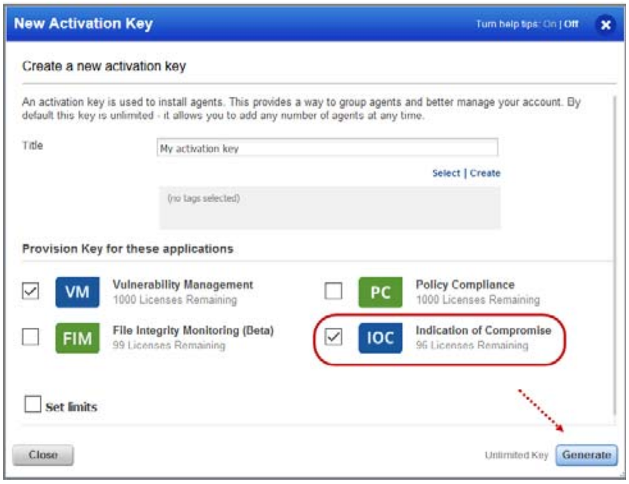
You'll need to install a cloud agent that's been activated for IOC on each asset you want to monitor for suspicious activity.

Install Agents using the CA app

Choose CA (Cloud Agent) from the application picker.


Indication of Compromise ▼
ACTIVE MODULES:
ADMIN Administration
AV AssetView
CA Cloud Agent
VM Vulnerability Management
PC Policy Compliance
WAF Web Application Firewall
FIM File Integrity Monitoring
IOC Indication of Compromise

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

☑ VM Vulnerability Management
1000 Licenses Remaining

□ PC Policy Compliance
1000 Licenses Remaining

□ FIM File Integrity Monitoring (Beta)
99 Licenses Remaining

☑ IOC Indication of Compromise
96 Licenses Remaining

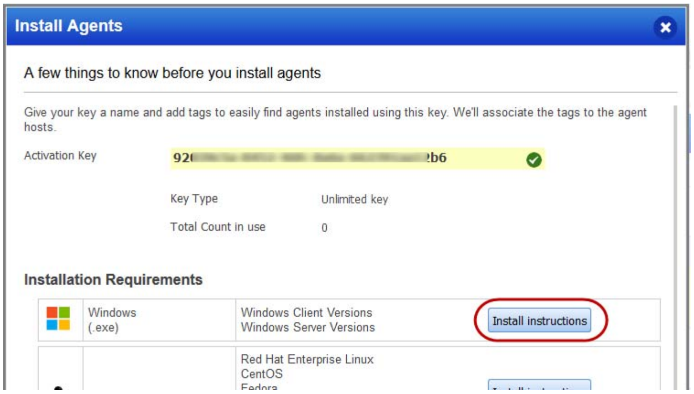
□ Set limits

Close

Unlimited Key

Generate

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



Install Agents

A few things to know before you install agents

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 92[redacted]b6 ✓

Key Type Unlimited key

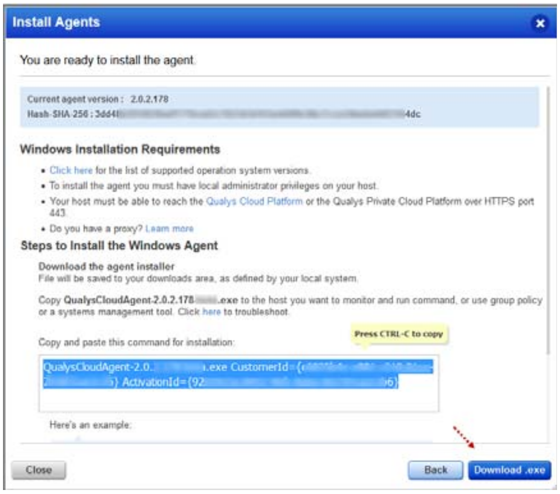
Total Count in use 0

Installation Requirements

Windows (.exe)	Windows Client Versions Windows Server Versions	Install instructions
	Red Hat Enterprise Linux CentOS Fedora	

Pick the Windows option to download the agent installer.

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.



Install Agents

You are ready to install the agent.

Current agent version : 2.0.2.178
Hash-SHA 256 : 3dd4[redacted]4dc

Windows Installation Requirements

- Click here for the list of supported operation system versions.
- To install the agent you must have local administrator privileges on your host.
- Your host must be able to reach the Qualys Cloud Platform or the Qualys Private Cloud Platform over HTTPS port 443.
- Do you have a proxy? Learn more

Steps to Install the Windows Agent

Download the agent installer
File will be saved to your downloads area, as defined by your local system.

Copy QualysCloudAgent-2.0.2.178[redacted].exe to the host you want to monitor and run command, or use group policy or a systems management tool. Click here to troubleshoot.

Copy and paste this command for installation:

```
QualysCloudAgent-2.0.[redacted].exe CustomerId={[redacted]} ActivationId={92[redacted]6}
```

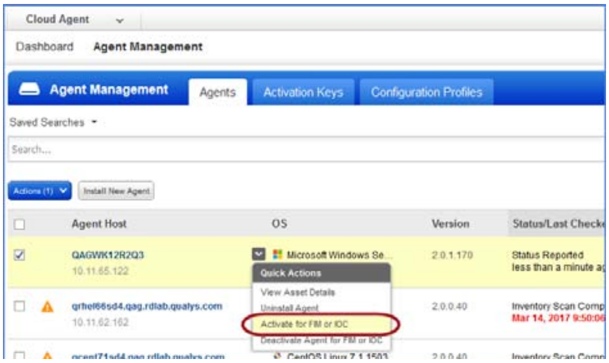
Here's an example:

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



□		Agent Host	OS	Version	Status/Last Checke
☑		QAGWK12R2Q3 10.11.65.122	Microsoft Windows Se...	2.0.1.170	Status Reported less than a minute a
□	⚠	qrhel66sd4.qag.rdlab.qualys.com 10.11.62.162		2.0.0.40	Inventory Scan Comp Mar 14, 2017 9:50:0
□	⚠	qcent71ad4.qag.rdlab.qualys.com	CentOS Linux 7.1.1503	2.0.0.40	Inventory Scan Comp

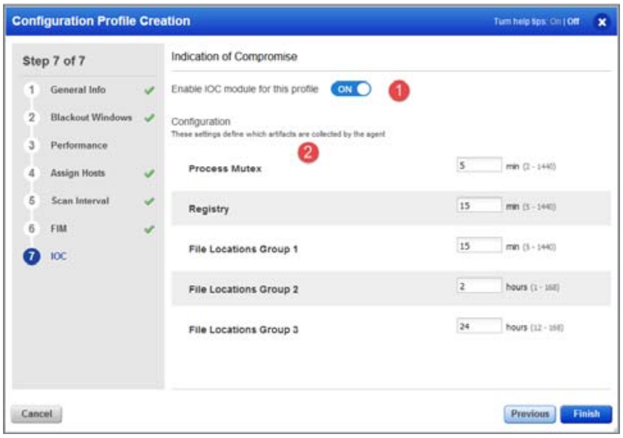
On the Agents tab choose your agent and "Activate for FIM or IOC" from the Quick Actions menu. (Bulk activation is supported using the Actions menu).

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.



Indication of Compromise

Enable IOC module for this profile ON

Configuration
These settings define which artifacts are collected by the agent

Process Mutex 5 min (2 - 1440)
Registry 15 min (5 - 1440)
File Locations Group 1 15 min (5 - 1440)
File Locations Group 2 2 hours (1 - 168)
File Locations Group 3 24 hours (12 - 168)

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	Eents 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

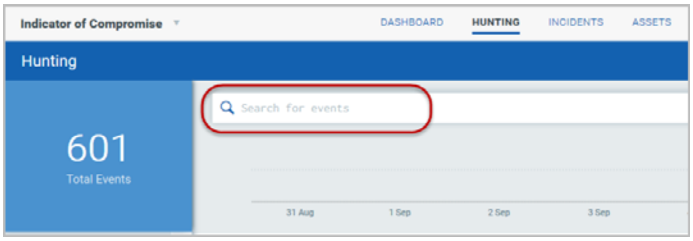
What’s next?

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.

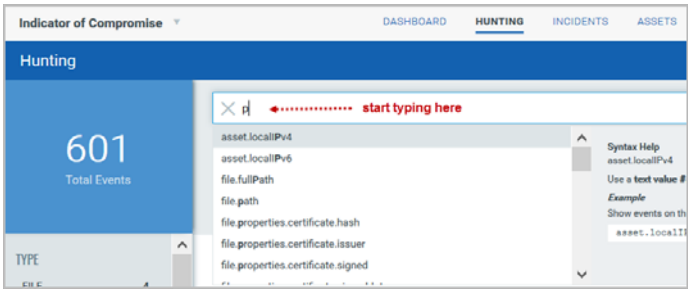
IOC Investigation and response

How to Search

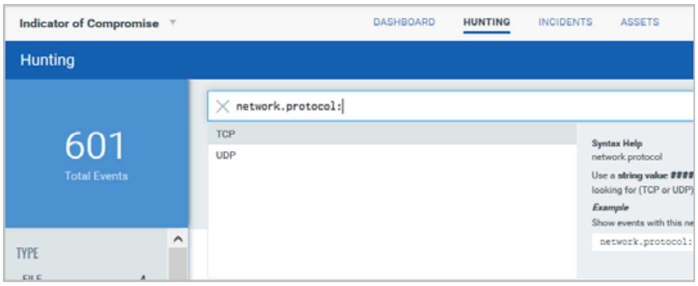
Our searching and filtering capabilities give you the ability to quickly find all about your incidents, events and assets all in one place using Qualys Advanced Search. You can search for incidents and assets in the respective tabs in the similar way.



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.

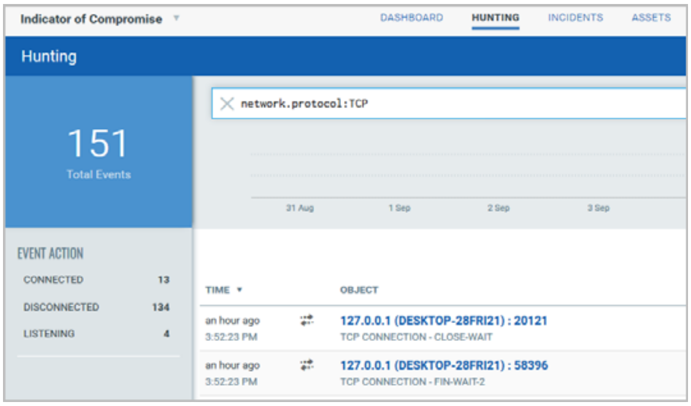


Select the one you're interested in. Check out the Syntax help for the selected field to the right to help with creating your query.

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

Then hit Enter.

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



EVENT ACTION	
CONNECTED	13
DISCONNECTED	134
LISTENING	4

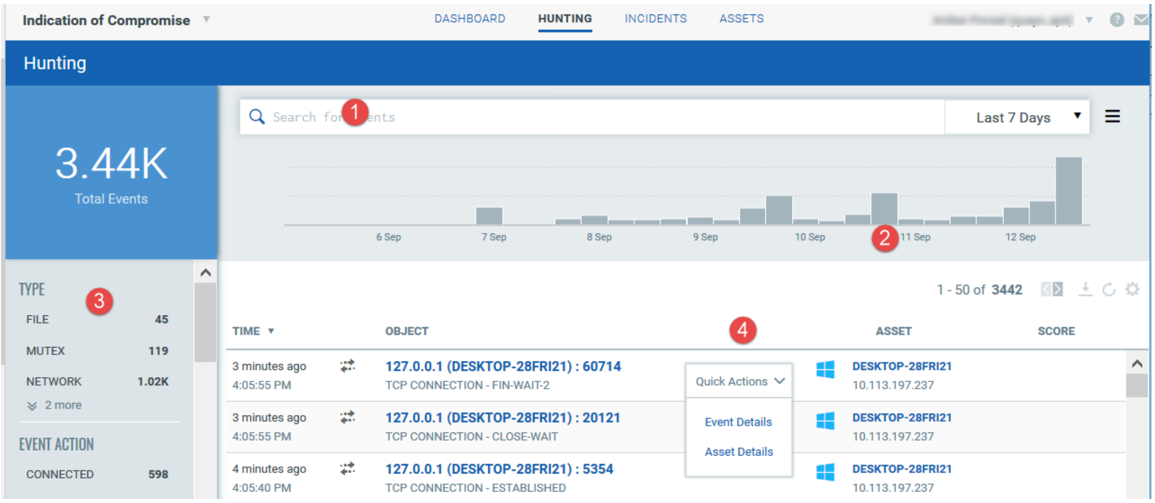
TIME	OBJECT
an hour ago 3:52:23 PM	127.0.0.1 (DESKTOP-28FRI21) : 20121 TCP CONNECTION - CLOSE-WAIT
an hour ago 3:52:23 PM	127.0.0.1 (DESKTOP-28FRI21) : 58396 TCP CONNECTION - FIN-WAIT-2

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 timeframe (2), group events by type (3), view event details and asset details (4).



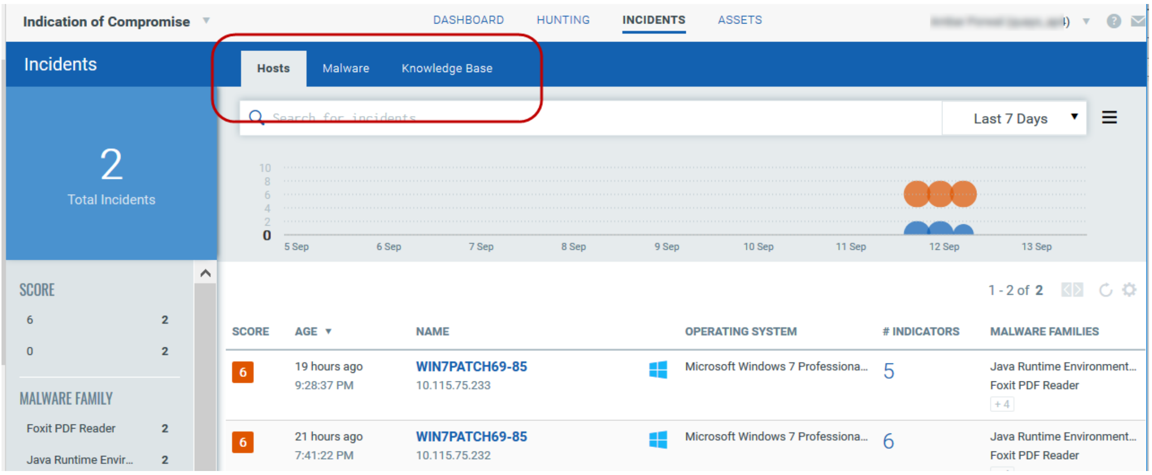
TYPE	
FILE	45
MUTEX	119
NETWORK	1.02K

EVENT ACTION	
CONNECTED	598

TIME	OBJECT	ASSET	SCORE
3 minutes ago 4:05:55 PM	127.0.0.1 (DESKTOP-28FRI21) : 60714 TCP CONNECTION - FIN-WAIT-2	DESKTOP-28FRI21 10.113.197.237	
3 minutes ago 4:05:55 PM	127.0.0.1 (DESKTOP-28FRI21) : 20121 TCP CONNECTION - CLOSE-WAIT	DESKTOP-28FRI21 10.113.197.237	
4 minutes ago 4:05:40 PM	127.0.0.1 (DESKTOP-28FRI21) : 5354 TCP CONNECTION - ESTABLISHED	DESKTOP-28FRI21 10.113.197.237	

Investigate incidents

Investigate incidents by host, malware name and malware family name.



2
Total Incidents

SCORE

6	2
0	2

MALWARE FAMILY

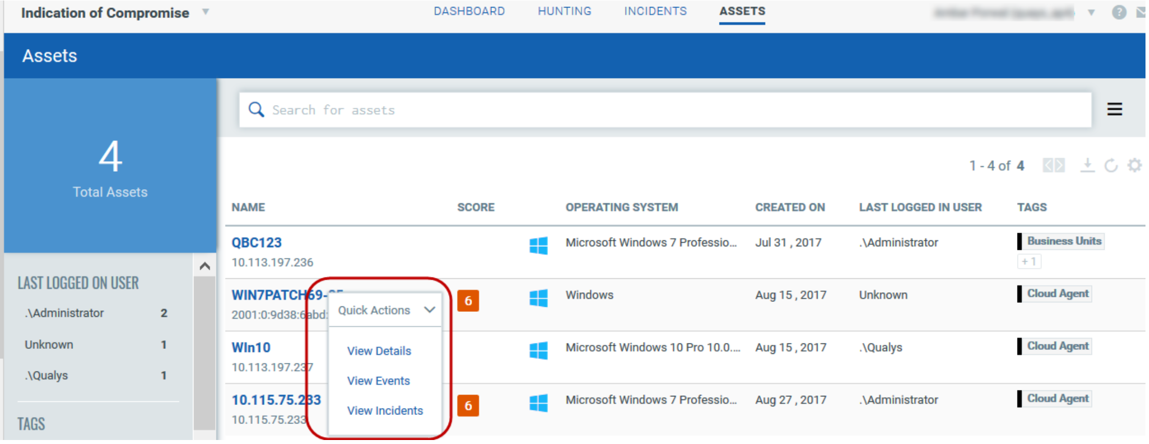
Foxit PDF Reader	2
Java Runtime Envir...	2

1 - 2 of 2

SCORE	AGE ▼	NAME	OPERATING SYSTEM	# INDICATORS	MALWARE FAMILIES
6	19 hours ago 9:28:37 PM	WIN7PATCH69-85 10.115.75.233	Microsoft Windows 7 Professiona...	5	Java Runtime Environment... Foxit PDF Reader + 4
6	21 hours ago 7:41:22 PM	WIN7PATCH69-85 10.115.75.232	Microsoft Windows 7 Professiona...	6	Java Runtime Environment... Foxit PDF Reader

Look into assets monitored by IOC

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



4
Total Assets

LAST LOGGED ON USER

.\Administrator	2
Unknown	1
.\Qualys	1

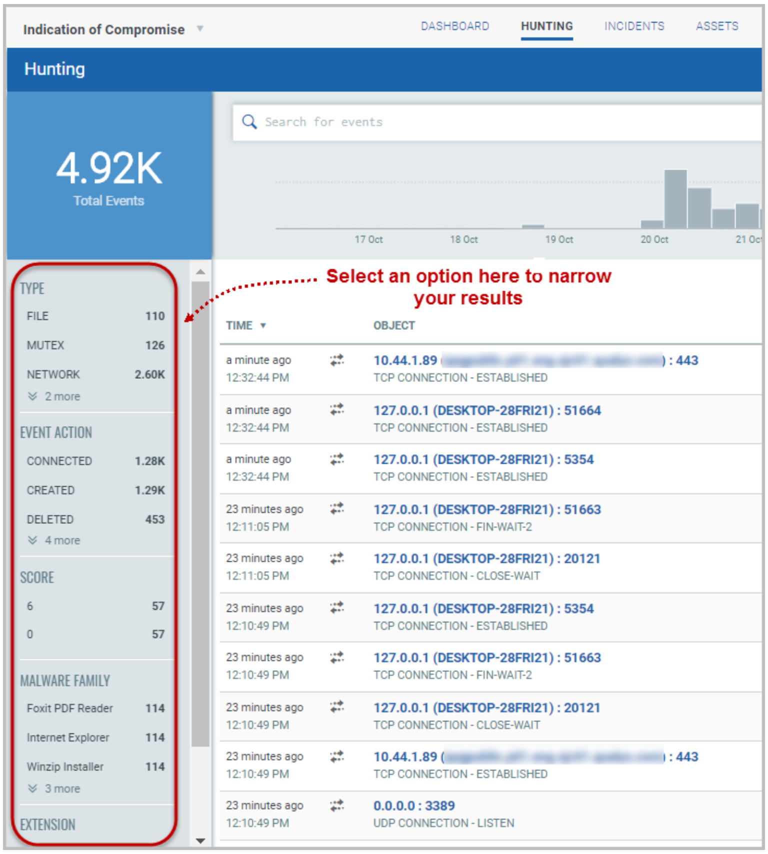
TAGS

1 - 4 of 4

NAME	SCORE	OPERATING SYSTEM	CREATED ON	LAST LOGGED IN USER	TAGS
QBC123 10.113.197.236		Microsoft Windows 7 Professio...	Jul 31 , 2017	.\Administrator	Business Units + 1
WIN7PATCH69- 2001:0:9d38:6abd:	6	Windows	Aug 15 , 2017	Unknown	Cloud Agent
WIn10 10.113.197.237		Microsoft Windows 10 Pro 10.0....	Aug 15 , 2017	.\Qualys	Cloud Agent
10.115.75.233 10.115.75.233	6	Microsoft Windows 7 Professio...	Aug 27 , 2017	.\Administrator	Cloud Agent

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.



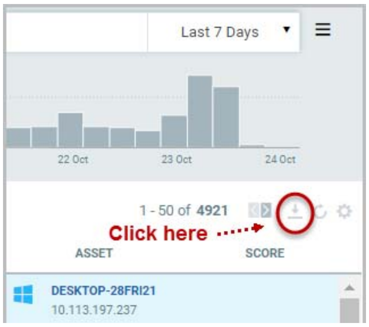
Select an option here to narrow your results

TYPE	
FILE	110
MUTEX	126
NETWORK	2.60K
2 more	
EVENT ACTION	
CONNECTED	1.28K
CREATED	1.29K
DELETED	453
4 more	
SCORE	
6	57
0	57
MALWARE FAMILY	
Foxit PDF Reader	114
Internet Explorer	114
Winzip Installer	114
3 more	
EXTENSION	

TIME	OBJECT
a minute ago 12:32:44 PM	10.44.1.89 ([redacted]) : 443 TCP CONNECTION - ESTABLISHED
a minute ago 12:32:44 PM	127.0.0.1 (DESKTOP-28FRI21) : 51664 TCP CONNECTION - ESTABLISHED
a minute ago 12:32:44 PM	127.0.0.1 (DESKTOP-28FRI21) : 5354 TCP CONNECTION - ESTABLISHED
23 minutes ago 12:11:05 PM	127.0.0.1 (DESKTOP-28FRI21) : 51663 TCP CONNECTION - FIN-WAIT-2
23 minutes ago 12:11:05 PM	127.0.0.1 (DESKTOP-28FRI21) : 20121 TCP CONNECTION - CLOSE-WAIT
23 minutes ago 12:10:49 PM	127.0.0.1 (DESKTOP-28FRI21) : 5354 TCP CONNECTION - ESTABLISHED
23 minutes ago 12:10:49 PM	127.0.0.1 (DESKTOP-28FRI21) : 51663 TCP CONNECTION - FIN-WAIT-2
23 minutes ago 12:10:49 PM	127.0.0.1 (DESKTOP-28FRI21) : 20121 TCP CONNECTION - CLOSE-WAIT
23 minutes ago 12:10:49 PM	10.44.1.89 ([redacted]) : 443 TCP CONNECTION - ESTABLISHED
23 minutes ago 12:10:49 PM	0.0.0.0 : 3389 UDP CONNECTION - LISTEN

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).



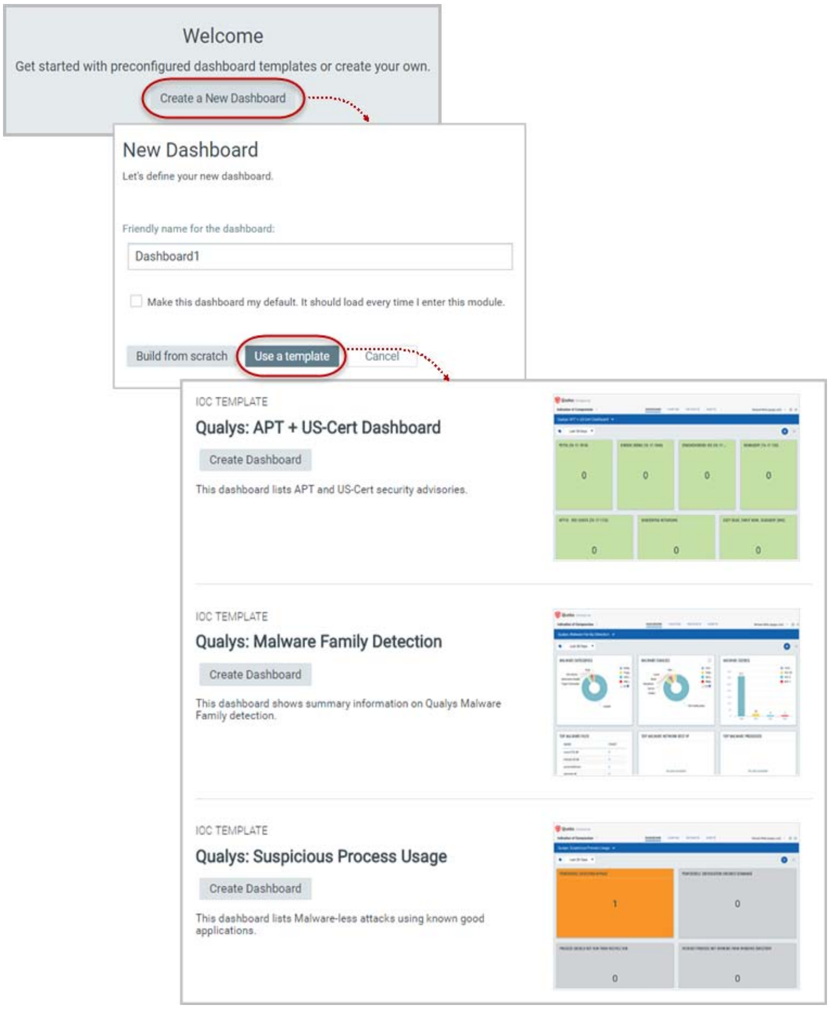
Just click the Download icon above the incidents list, choose a format and click Download.

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.



Welcome

Get started with preconfigured dashboard templates or create your own.

Create a New Dashboard

New Dashboard

Let's define your new dashboard.

Friendly name for the dashboard:

Dashboard1

□ Make this dashboard my default. It should load every time I enter this module.

Build from scratch | Use a template | Cancel

IOC TEMPLATE

Qualys: APT + US-Cert Dashboard

Create Dashboard

This dashboard lists APT and US-Cert security advisories.

IOC TEMPLATE

Qualys: Malware Family Detection

Create Dashboard

This dashboard shows summary information on Qualys Malware Family detection.

IOC TEMPLATE

Qualys: Suspicious Process Usage

Create Dashboard

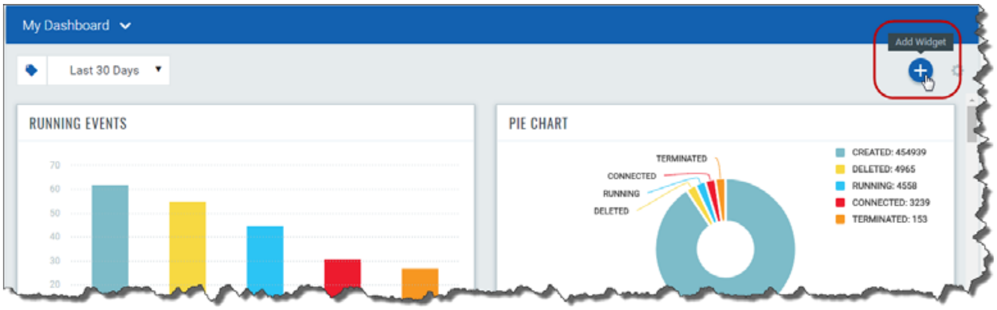
This dashboard lists Malware-less attacks using known good applications.

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

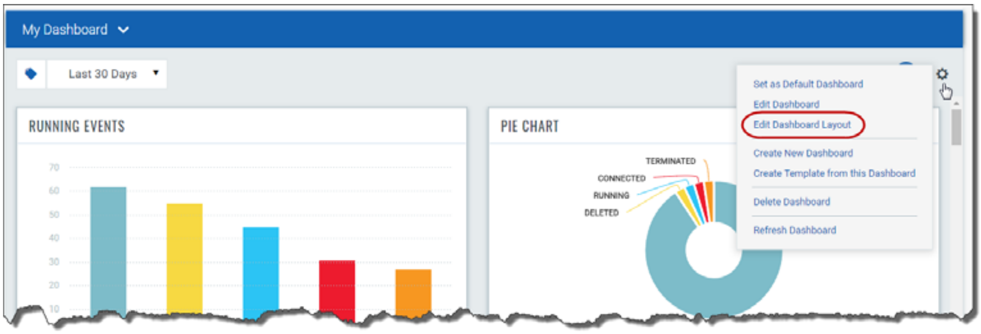
Start by clicking the Add Widget icon on your dashboard.



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

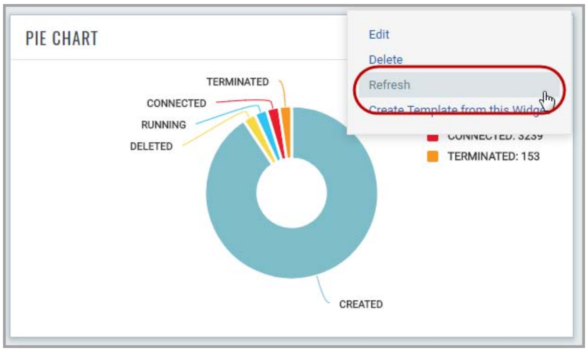
You can resize any widget horizontally, and drag & drop widgets to change the layout.



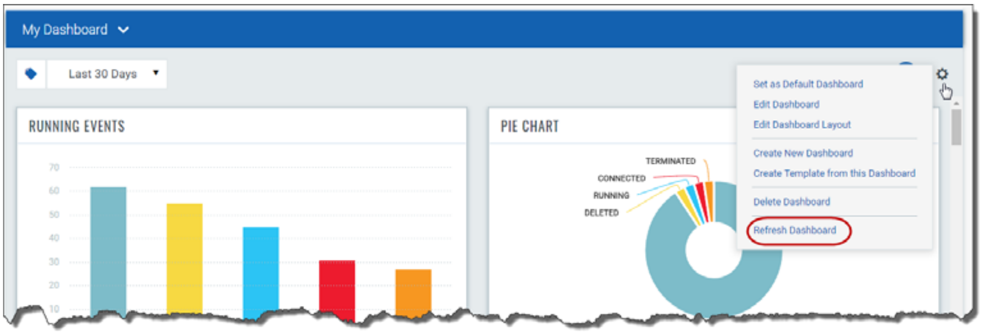
Click the Tools icon on your dashboard and then select Edit Dashboard Layout. Adjust the width for any widget or drag the widget to a new location. Click OK to save your changes.

Refresh your view

To see the latest data for a particular widget, select the widget menu and choose Refresh.



Optionally, choose the Refresh Dashboard option from the Tools menu to refresh all widgets on the dashboard with one click.


My Dashboard
Last 30 Days
RUNNING EVENTS
70
60
50
40
30
20
10
PIE CHART
TERMINATED
CONNECTED
RUNNING
DELETED
Set as Default Dashboard
Edit Dashboard
Edit Dashboard Layout
Create New Dashboard
Create Template from this Dashboard
Delete Dashboard
Refresh Dashboard