



Indication of Compromise

Getting Started Guide

February 12, 2018

Copyright 2017-2018 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



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
Investigate incidents	12
Look into assets monitored by IOC.....	12
Narrow your results	13
Download your results.....	14
Set Up Dynamic Dashboards	15
Using pre-defined IOC templates	15
Switching dashboards	15
Adding widgets	16
Resizing and layout	16
Refresh your view	17

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 with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations 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, Fujitsu, HCL Comnet, HPE, 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).

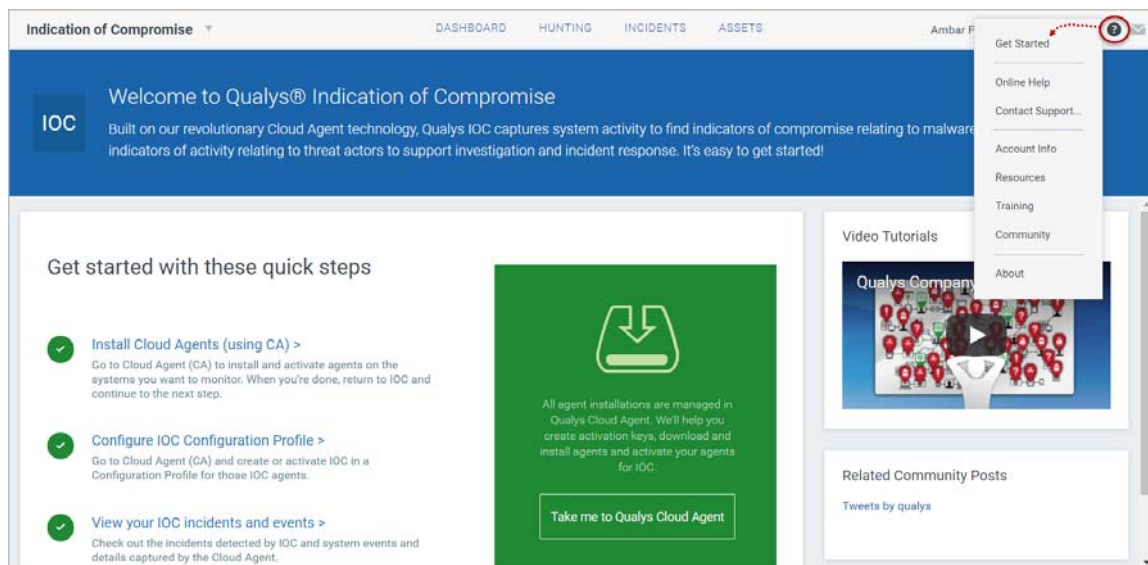
Enable IOC in a CA Configuration Profile and tell us which IOC artifacts you want to transmit to the Qualys Cloud Platform and at what interval.

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.

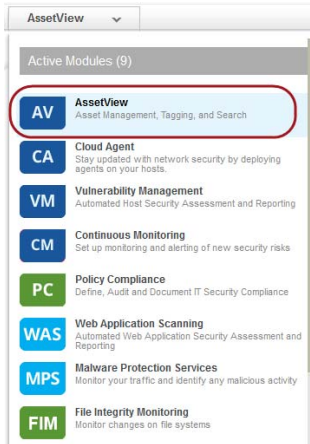


Setting up asset tags (optional)

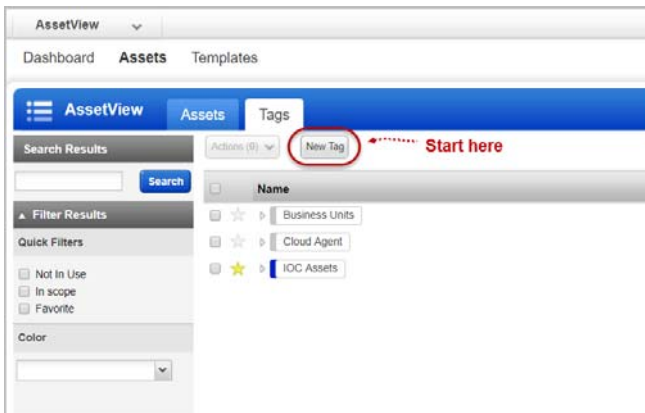
Setting up asset tags using AssetView helps you to associate IOC assets with a CA configuration profile enabled for IOC. You can avoid assigning configurations manually to each asset by adding asset tags to the required CA configuration profiles.

How to create tags

Go to AssetView to get started.



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.



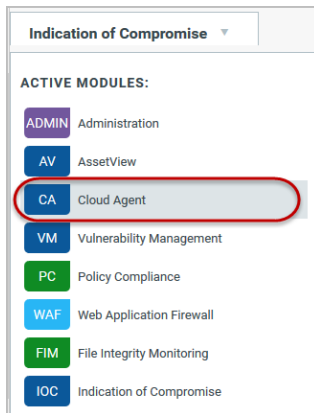
Not interested in tags? No problem. You can manually assign individual assets to your profiles.

Install Cloud Agents

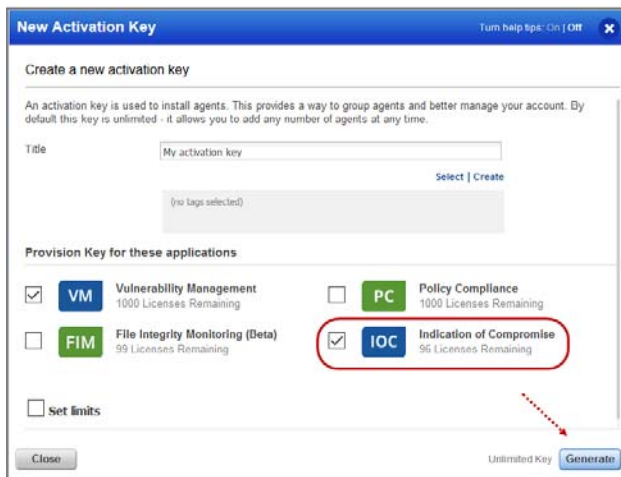
You'll need to install a cloud agent that's been activated for IOC on each asset you want to monitor for suspicious activity.

Install Agents using the CA app

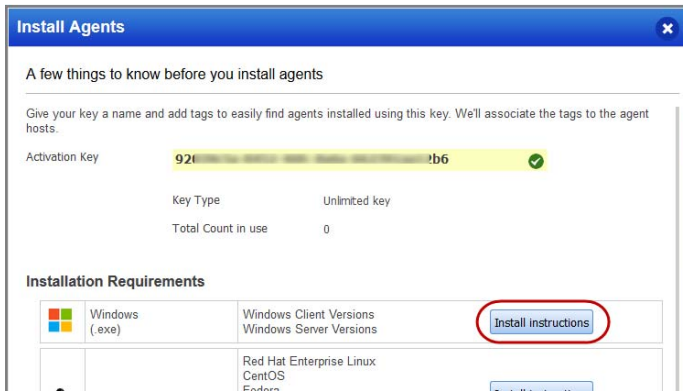
Choose CA (Cloud Agent) from the application picker.



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.

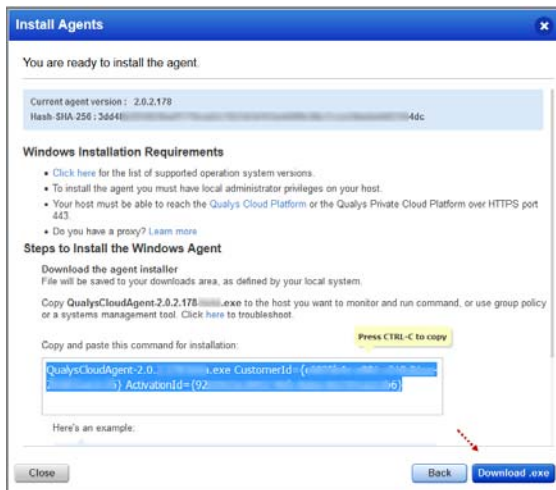


As you can see you can provision the same key for any of the other applications in your account.



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.

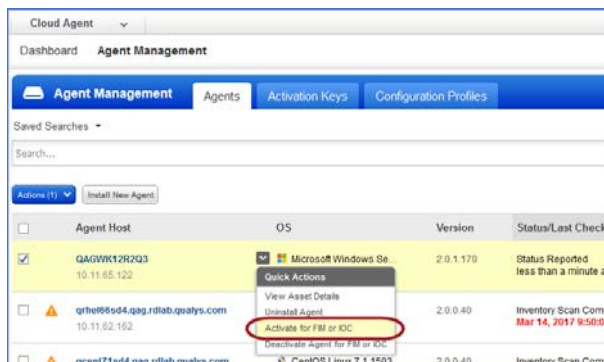


Review the installation requirements and click Download.

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



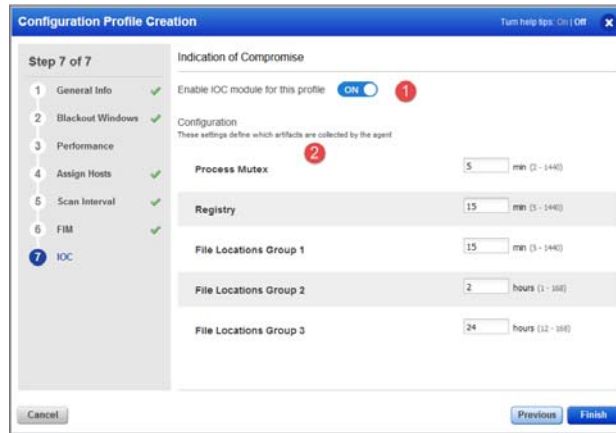
On the Agents tab choose your agent and "Activate for FIM or IOC" from the Quick Actions menu. (Bulk activation is supported using the Actions menu).

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

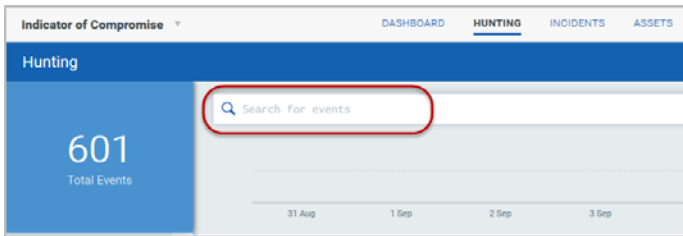
What's next?

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.

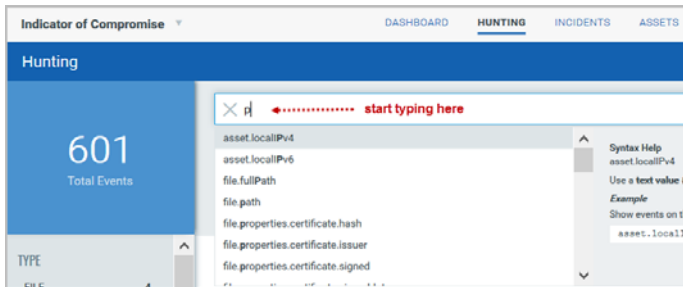
IOC Investigation and response

How to Search

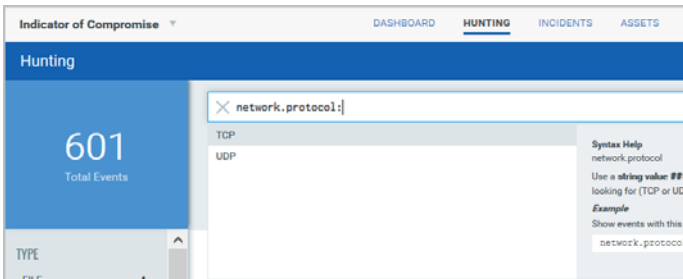
Our searching and filtering capabilities give you the ability to quickly find all about your incidents, events and assets all in one place using Qualys Advanced Search. You can search for incidents and assets in the respective tabs in the similar way.



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.

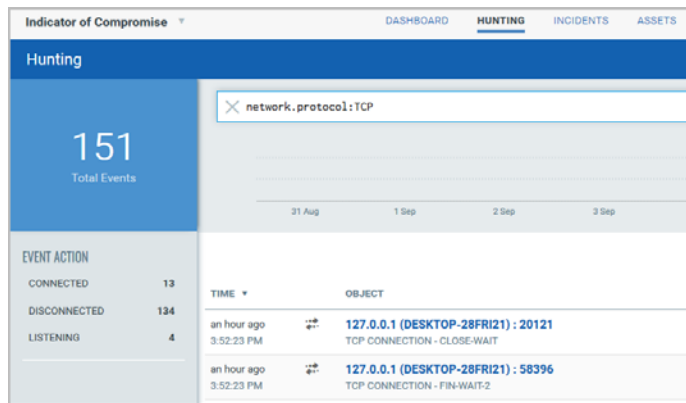


Select the one you're interested in. Check out the Syntax help for the selected field to the right to help with creating your query.

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.

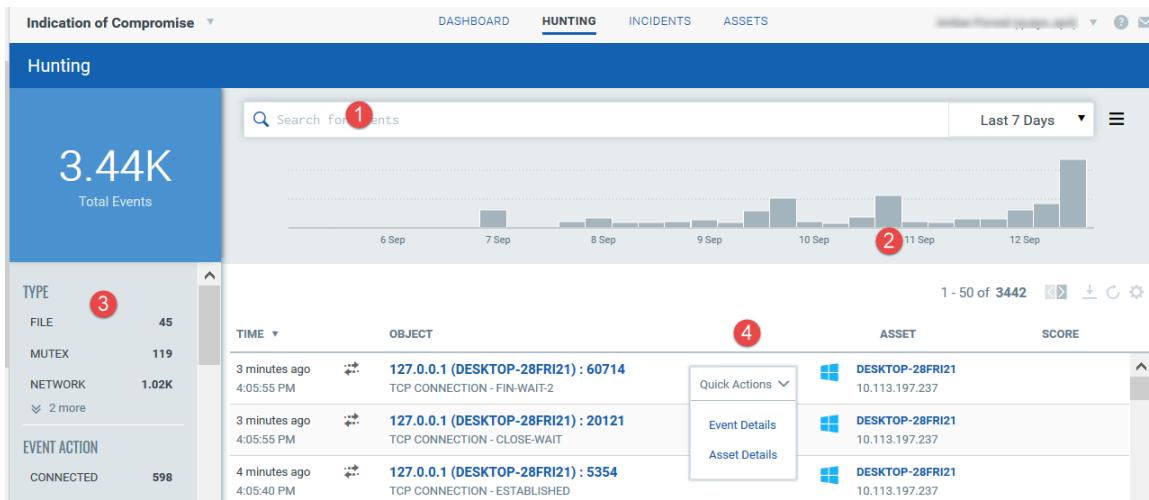


That's it! Your matches will appear in the list your viewing. Filters on the left help you drill down to objects of interest.

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



Investigate incidents

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

The screenshot shows the 'Incidents' dashboard. The 'Hosts' tab is selected and highlighted with a red box. A search bar is also highlighted with a red box. The dashboard shows 2 total incidents and a table of incident details.

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 Environ... 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 Environ... Foxit PDF Reader

Look into assets monitored by IOC

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

The screenshot shows the 'Assets' dashboard. A red box highlights the 'Quick Actions' menu for the asset 'WIN7PATCH69-2001:0:9d38:6abd', showing options for 'View Details', 'View Events', and 'View Incidents'.

NAME	SCORE	OPERATING SYSTEM	CREATED ON	LAST LOGGED IN USER	TAGS
QBC123 10.113.197.236		Microsoft Windows 7 Professiona...	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	6	Microsoft Windows 7 Professiona...	Aug 27, 2017	.Administrator	Cloud Agent

Narrow your results

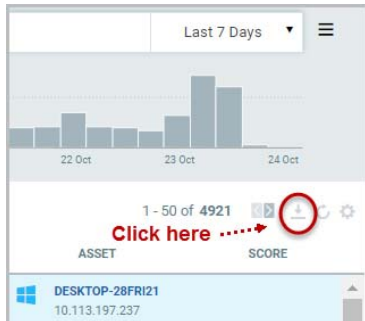
Once you have your search results you may want to organize them further into logical groupings. Choose a group by option on the left side. You'll see the number of events or assets per grouping. Click on any grouping to update the search query and view the matching incidents or events.

The screenshot shows a security dashboard interface. At the top, there are navigation tabs: DASHBOARD, HUNTING (selected), INCIDENTS, and ASSETS. Below the navigation, the main heading is 'Hunting'. On the left side, there is a summary card showing '4.92K Total Events'. Below this is a filter sidebar with several categories: TYPE, EVENT ACTION, SCORE, MALWARE FAMILY, and EXTENSION. The 'TYPE' category is highlighted with a red box and a red arrow pointing to it, with the text 'Select an option here to narrow your results' next to it. The main area of the dashboard displays a search bar and a bar chart showing event counts over time (17 Oct to 21 Oct). Below the chart is a table of events with columns for TIME and OBJECT. The table contains several rows of event data, including IP addresses and connection types.

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).



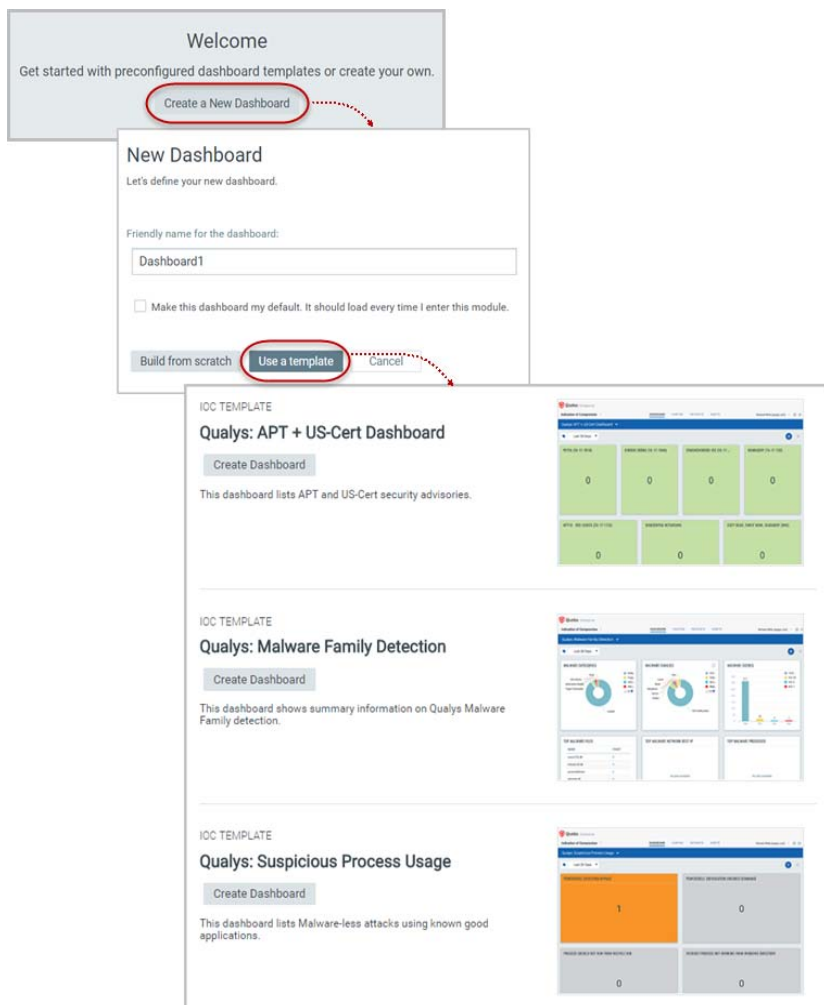
Just click the Download icon above the incidents list, choose a format and click Download.

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.

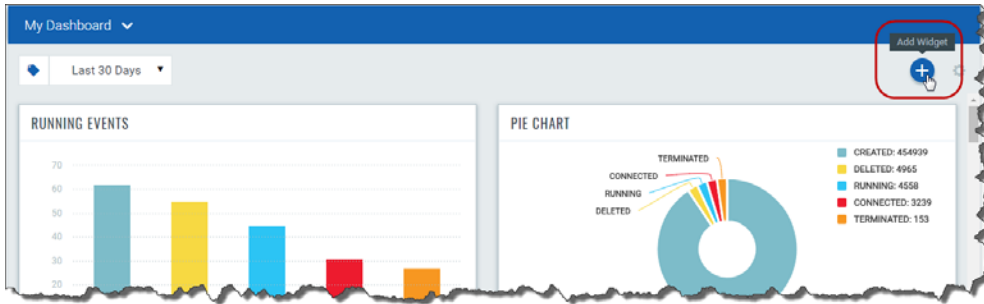


Switching dashboards

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

Adding widgets

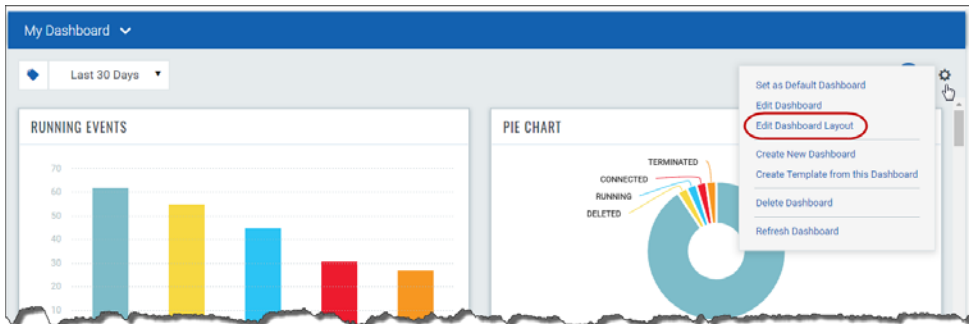
Start by clicking the Add Widget icon on your dashboard.



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

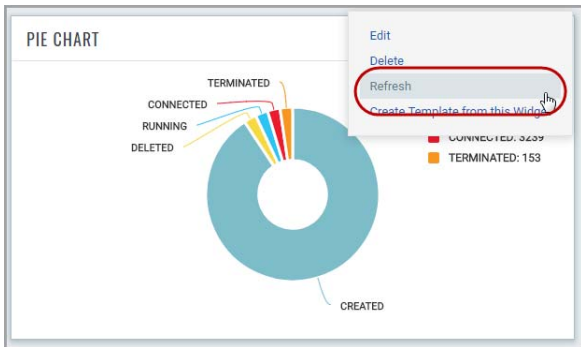
You can resize any widget horizontally, and drag & drop widgets to change the layout.



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.

