File Integrity Monitoring
Getting Started Guide

April 1, 2019
About this Guide

Thank you for your interest in Qualys File Integrity Monitoring (FIM). This new service allows you to log and centrally track file change events across your global IT assets. All you have to do is install lightweight agents on your assets and set up FIM monitoring profiles. We’ll help you get started quickly!

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

File Integrity Monitoring is a highly scalable, centralized solution that reduces the cost and complexity of detecting policy and compliance-related changes mandated by regulations such as the Payment Card Industry Data Security Standard.

Steps to start monitoring change 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. Agents are centrally managed by the cloud agent platform and are self-updating (no reboot needed).

Configure FIM monitoring profiles to tell us the files you want to monitor and the types of changes you want to know about. We provide several profiles in our Library to get you started but you can also create your own.

View your events in one central location. You’ll see all events detected across all of your assets. Search all of your 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 automate file integrity monitoring using FIM. You can avoid assigning configurations manually to each asset by adding asset tags to the required configurations - FIM monitoring profiles and CA configuration profiles.

We recommend you read these tips on configuring FIM monitoring profiles to help you with deciding how to assign tags to your assets.

How to create tags

Go to AssetView to get started.

Then go to Assets > Tags and click New Tag to add tags for your FIM 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 FIM on each asset you want to monitor for file integrity. You’ll install and manage agents using Qualys Cloud Agent (CA).

Let’s get started!

Choose CA (Cloud Agent) from the application picker.

Create an activation key

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

As you can see you can provision the same key for any of the other applications in your account.
Pick either Windows or Linux to get install instructions and download the 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 FIM

Choose “Activate for FIM or IOC” for each FIM cloud agent on the Agents tab.

Enable FIM 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 FIM tab:

1) Toggle “Enable FIM module for this profile” to On. This is required for FIM event data collection to occur.

2) Configure when events are transmitted to the Qualys Cloud Platform. Defaults are provided, so this step is optional. You can configure values for event log size, threshold time, disk usage.

(FIM settings are available only when FIM is enabled for your subscription)

Tip - We recommend you set up asset tags for your FIM assets using AssetView. This makes it easy to associate FIM assets with a CA configuration profile and a FIM monitoring profile - just apply the same FIM tags to these profiles.

Events are transmitted to the Qualys Cloud Platform when either of the following occurs:

- FIM event log reaches the maximum specified size
- Payload threshold time is hit
- Disk usage for total FIM data on the agent reaches the maximum specified size

What’s next? Your assets will appear in Qualys FIM on the Assets list. Next we’ll describe how to create FIM monitoring profiles for your assets.
Configure FIM monitoring profiles

The FIM monitoring profile is where you’ll tell us the files you want to monitor and the types of changes you want to know about. We provide several profiles in our Library to get you started but you can also create your own.

Best practices for creating profiles

Configure as many profiles as needed for different situations, and apply multiple profiles to a single device. For example, you may want to configure profiles for these objectives:

- Monitor OS critical binary and configuration data
- Monitor application data
- Monitor rights and permissions database or log files
- Monitor application critical binaries

Define Windows and Linux profiles separately. We don’t currently support defining OS version subsets to a profile. Be very granular in assignment of profiles to assets to prevent getting more events than intended. For example, let’s say you have a Linux profile for CentOS and a Linux profile for Ubuntu and assign each a tag that contains both operating systems. Both profiles will be monitored for and if there are overlapping settings you could get more events than intended.

After creating a monitoring profile you must activate it to enable change detection. You can deactivate a profile at any time to suspend monitoring for that profile.

Create a FIM monitoring profile

Choose FIM (File Integrity Monitoring) from the application picker.
We provide several profiles in our Library to help get you started. Our out of box OS based profiles include pre-defined monitoring rules.

Go to Configuration > Library, select an OS specific profile and choose the Import and Use as Active Profile from the menu provided.

Choose whether to import the profile locked or without restrictions. Tip - If you pick No Restrictions you can edit the profile once imported (on the Profiles tab).

You can also create your own profiles. Click Create New Profile on the Profiles tab.

Provide basic profile details (name, operating system, category). Keep in mind - you’ll need to create separate profiles for Windows and Linux operating systems.
Add one or more rules to the profile to tell us what you want to watch for. Go to the Rules section, click Add New Rule and provide rule details.

When defining a rule:
(1) choose a rule type (File or Directory) and provide the full path to the file/directory,
(2) select the actions that should trigger events, and
(3) click Save Rule to add the rule to the profile.

If you choose Directory as the Rule Type, you can click Advanced Options to include or exclude specific files/directories within that directory.
Add assets to the profile. You can select individual assets in your account or assign asset tags in order to monitor all matching assets automatically.

Activate your profile. New profiles are Inactive to start. Select the profile in the list and choose Activate to start using it.
Activate / Deactivate profiles

As mentioned earlier you must activate a profile to use it for monitoring. From the Profiles list, simply choose the action you want to take from the Quick Actions menu. Activate a profile to use it for monitoring; Deactivate a profile to suspend it from monitoring.

Assign a profile to an asset

Tip - If your profile has asset tags defined then there’s nothing you need to do. As long as the new asset has a tag that matches a tag in the profile it will use the profile automatically.

When you add a new asset you can quickly assign it to an existing monitoring profile. Go to the Assets list and choose Assign a Monitoring Profile from the Quick Actions menu. Then simply choose the profile you want to use.
View Your Events and Assets

FIM provides one central location for viewing all of the events detected across all of your assets. The Events tab and the Assets tab contain search capabilities, group by options, and download options. In the Assets tab you can find all assets impacted by FIM events. Use tabs in the Events section to quickly identify:

1. All events detected across all of your assets, except ignored events.
2. Events waiting to be reviewed. You can choose to ignore events or create incidents.
3. Ignored events.

View events

You can find events based on event data, file information, monitoring profile, and more.
View Your Events and Assets

View event details

Clicking Event Details in the Quick Actions for an event brings up the Event Details page. This page provides complete information about the FIM event.

Ignore events

Have an event you don’t need to track? Ignore it to move it out of your list.

Select specific events and choose Ignore Events from the Actions menu. Optionally, choose Ignore All Matching Events to ignore all events that are currently matching your query for the timeframe that you’ve selected. Ignored events are moved to the Ignored list. Note - You may get similar events in the future that will appear in your Events list and you’ll want to ignore those too.

Did you ignore an event by mistake? No worries. Easily restore any ignored event from the Ignored list.
Create and track incidents

You’ll want to review the events detected on your assets and group related changes into incidents. Review your incidents to determine if they’re valid, mark them approved or unapproved and classify them by the type of change.

On the Event Review tab, run a query to find related events, click Create Incident and give your incident a name. Your new incident will be saved on the Incidents list where you can view and add details. All events matching your query will be included.

The Incidents list is where you’ll take actions on your incidents. View details for any incident to get a break-down of the events by severity, action and user. Edit any incident to rename it or change the events associated with it by modifying the query or timeframe.

Choose Start Review to review the events associated with an incident and then mark the incident Approved or Unapproved. You’ll also classify the events by disposition category (e.g. Pre-Approved by Change Control, Patching, Data Corruption, Human Error, etc.) and indicate the type of change (e.g. Manual, Automated, etc.)
View assets

You can find assets based on tags and operating system.

Clicking View Details in Quick Actions for an asset shows complete information about the Asset impacted by FIM. Asset details can also be seen from the Events tab by clicking Asset Details for an event. This brings up details of the asset impacted by that FIM event.
How to search

Our search capabilities give you the ability to quickly find events matching certain criteria. Here are the steps to search for events. Search for incidents and assets in a similar way.

You’ll notice the Search field above the Events list. This is where you’ll enter your search query.

Start typing and we’ll show you the event properties you can search like actor process, asset hostname, profile name, etc. Select the one you’re interested in.

Now enter the value you want to match, and click Search. That’s it! Your matches will appear in your events list.

Tip - Go to the FIM online help for details on search language and sample queries.
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 events or assets.
Download your results

By downloading search results to your local system you can easily manage file change events, incidents and assets outside of the Qualys platform and share them with other users. You can export results in multiple formats (CSV, XML, PDF, DOC, HTML, etc).

Just click the Download icon above any list, choose a format and click Download.
Customize Your Dashboard

You can create multiple dashboards and switch between them. Each dashboard has a collection of widgets showing event data of interest. And your dashboards/widgets are updated in real-time.

Switching dashboards

Click the down arrow next to the dashboard name and pick the one you want.

Adding widgets

1) Start by clicking the Add Widget icon on your dashboard.

2) Pick one of our widget templates - there are many to choose from - or create your own.

3) Each widget is unique. For some you’ll select event data, a query and layout - count, table, bar graph, pie chart.

Tip - Wondering how we created the widgets on the default dashboard? Choose Edit from the widget menu to see the settings.
**Resizing and layout**

Resize any widget horizontally, drag & drop widgets to change the layout.

1) Click the Tools icon on your dashboard.

![Tools icon on dashboard]

2) Select Edit Dashboard Layout.

![Edit Dashboard Layout option]

3) Adjust the width for any widget or drag the widget to a new location.

4) Click OK to save your changes.

**Refresh your view**

You might want to see the latest data for a particular widget.

Hover over the widget, click [ ] and from the widget menu choose Refresh.

![Refresh option in widget menu]
Choose the Refresh Dashboard option from the Tools menu to refresh all the widgets.

Creating Dashboards and templates

From the Tools menu you can choose to create a new dashboard from scratch or create a template for your subscription from the current dashboard.

Import / Export options

You can import and export dashboards with corresponding widgets, and import widgets.