WHITEPAPER

Alert Logic File Integrity Monitoring

by John Pirc (JP)
Director | Product Management

ALERT LOGIC™

Table of Contents

Deploying Alert Logic File Integrity Monitoring

Alert Logic is focused on delivering unrivaled security value for our customers and partners. We continue to release new functionality while leveraging the same Alert Logic agent and one of the latest capabilities is File Integrity Monitoring (FIM). This article will focus on how the addition of FIM to the MDR platform helps customers satisfy compliance requirements.

In addition to PCI-DSS, Alert Logic FIM can satisfy requirements such as:

- PCI-DSS 10.5.5 and 11.5
- SOX - Section 404
- HIPAA - §164.312 (b), (c)(1)
- SOC 2
- HITRUST

Additionally, security best practices and frameworks such as NIST SP 800-53 are an excellent way to ensure you have the proper security controls in place. FIM is listed in Control # SI-7 (7) & (8) of NIST SP 800-53. This whitepaper will focus on the most common compliance requirement for FIM in PCI-DSS.

Use Case for Achieving PCI DSS 10.5.5 and 11.5

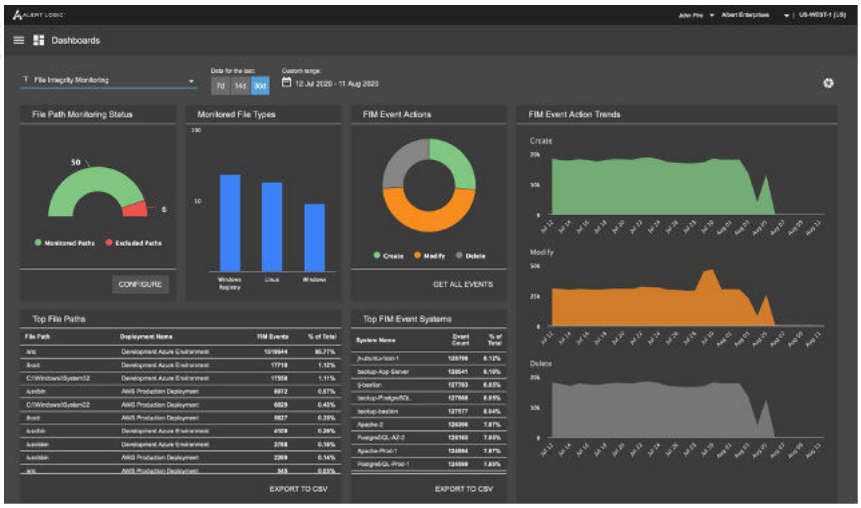
In this section, we walk through a FIM deployment that includes setting up monitoring paths and reporting to achieve PCI-DSS FIM requirements:

- PCI Requirement 10.5.5: Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.
- PCI Requirement 11.5: Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modifications (including changes, additions and deletions) of critical system files, configuration files, content files and configure the software to perform critical files comparisons at least weekly.

Requirements:

Alert Logic File Integrity Monitoring (FIM) is available to customers that are currently entitled to MDR Professional. You will need to identify what servers are in scope for PCI within the deployments you have configured in the Alert Logic Console. We also recommend that you make a list of what file paths you need to monitor and those that you want to exclude with a description. This prep work will save you a lot of time and will ensure a successful configuration experience. We provide 42 pre-populated paths to decrease time to configuration. These are recommended for monitoring but not all organizations are cookie cutter, so we provide you the ability to customize file paths down to the file type or file name. By default, when FIM is turned on, it will monitor all assets within that deployment. However, we provide you the ability to get granular by selecting only a few host/s, subnet/s, VPC/s, etc. to apply FIM within that deployment. After you have verified the Alert Logic requirements and completed your pre-deployment checklist, login into the Alert Console and select the FIM Dashboard.

Alert Logic File Integrity Monitoring (FIM) Dashboard



The Alert Logic FIM dashboard provides you an at-a-glance view of your FIM deployments. Outside of the "File Path Monitoring Status" and "Monitored File Types," the rest of the widgets are time-bound based on your selection of last 7, 14,30 day and custom date ranges up to 90 days. This will help you identify your top deployments that are generating the most file change events based on file path. Additionally, the FIM dashboard provides a snapshot on the number of files that are being created, modified and deleted based on the time ranges you selected. This dashboard is the recommended starting point regardless if you have or have not configured FIM yet.

To troubleshoot an issue, we recommend starting with the "Top File Paths" widget. Within this widget, you can identify what deployments you have enabled and the quantity of "FIM Events". This can help you identify a noisy file or path for tuning consideration as an "exclusion." Typically, you can correlate that noisy deployment to the "Top FIM Event Systems" to identify the exact server. In the screen shot above we have verified a one to one match on deployment to system.

Top File Paths

File Path	Deployment Name	FIM Events	% of Total
/etc	Development Azure Environment	1110927	91.33%
C:\\Windows\\System32	Development Azure Environment	44556	3.66%
/boot	Development Azure Environment	38922	3.20%
C:\\Windows\\System32	AWS Production Deployment	10051	0.83%
/usr/bin	Development Azure Environment	4773	0.39%
/boot	AWS Production Deployment	4456	0.37%
/usr/sbin	Development Azure Environment	1820	0.15%
C:\\Windows\\System32	Production Data Center	321	0.03%
/boot	Production Data Center	209	0.02%
/etc	AWS Production Deployment	130	0.01%

EXPORT TO CSV

Top FIM Event Systems

System Name	Event Count	% of Total
backup-App-Server	96395	7.93%
backup-PostgreSQL	96275	7.92%
Apache-2	95290	7.83%
PostgreSQL-AZ-2	95285	7.83%
backup-bastion	95124	7.82%
tj-bastion	95056	7.81%
Apache-Prod-1	94827	7.80%
4d-DB-7-1	94673	7.78%
jt-ubuntu-host-1	94438	7.76%
Application-Server	93600	7.70%

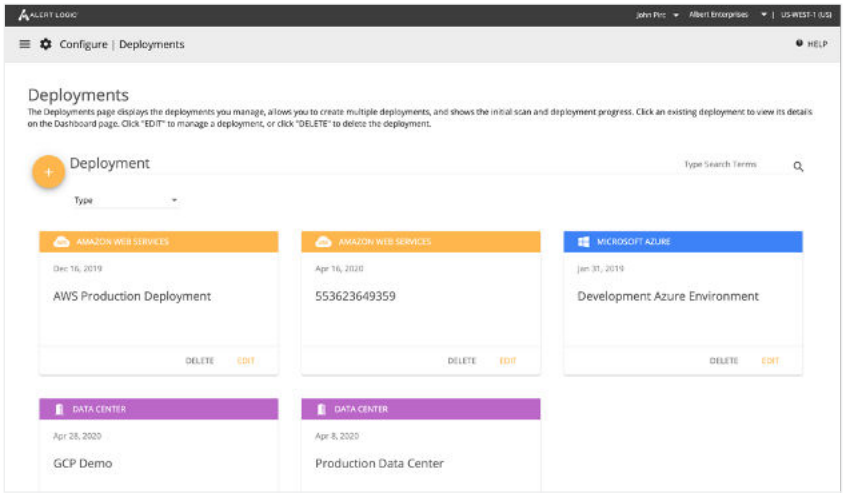
EXPORT TO CSV

If you see a spike in “Delete” under the “FIM Event Action Trends”, we recommend that you immediately triage by going to the “FIM Event Actions” and click on “GET ALL EVENTS.” This will download all FIM events from initial configuration to present day. Since this is provided in a CSV, you can determine what deployment, server and files where deleted.

Configuring FIM Monitoring

Configuring FIM is straightforward and intuitive if you are familiar with the Alert Logic Console. If this is your first week on the job, don’t worry, we have you covered in this walkthrough.

When you configure FIM, you need to select which deployment you want to apply FIM. It’s important to note that once you enable/configure FIM, it will be applied to all assets within the deployment you select. However, we do provide an option if you want to apply FIM to specific host, group of hosts, VPC, subnet, etc. For the purpose of this example we will be configuring our Azure deployment, but you could also select AWS, GCP or on-premise as you can apply FIM to any deployment that you have successfully deployed the Alert Logic Agent



Once you select your deployment you will be able to quickly start configuring your first policy. You will notice 42 pre-populated file paths across Linux, Windows and Windows Registry settings are all turned off by default.

GNU/Linux Files

- /bin
- /boot
- /etc
- /sbin
- /usr/bin
- /usr/local/bin

- /usr/local/sbin
- /usr/sbin
- /usr/my_custom_filepath
- /usr/share/keyrings
- /var/spool/cron

Windows Files

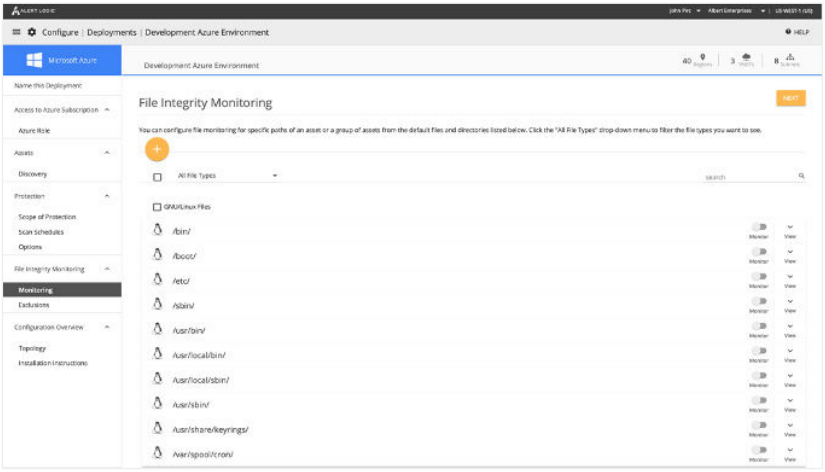
- C:\autoexec.bat
- C:\boot.ini
- C:\config.sys
- C:\Program Files\Microsoft Security Client\msseces.exe
- C:\Program Files\My Custom App\customapp.exe
- C:\Windows\explorer.exe
- C:\Windows\regedit.exe
- C:\Windows\system.ini
- C:\Windows\System32
- C:\Windows\win.ini

Windows Registry

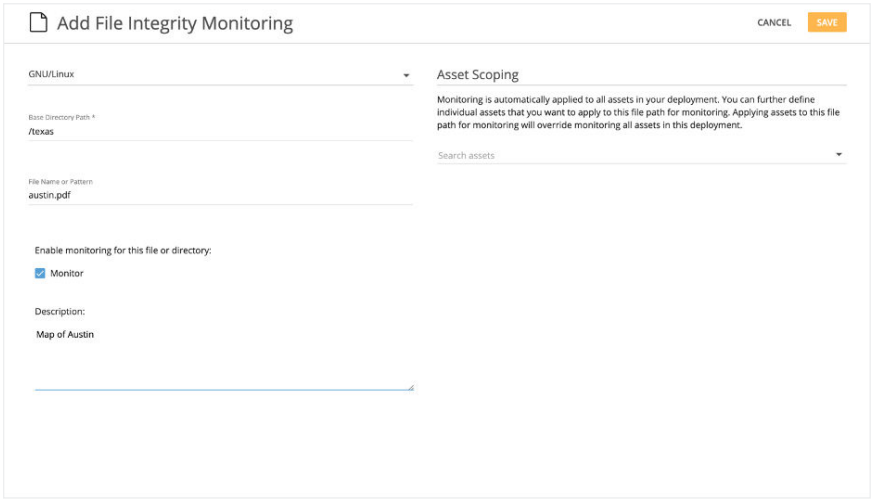
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\piffile</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemObjects</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Directory</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Folder</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Protocols</windows_registry>

- <windows_registry>HKEY_LOCAL_MACHINE\Software\Policies</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Policies\Custom</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Security</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon</windows_registry>
- <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components</windows_registry>

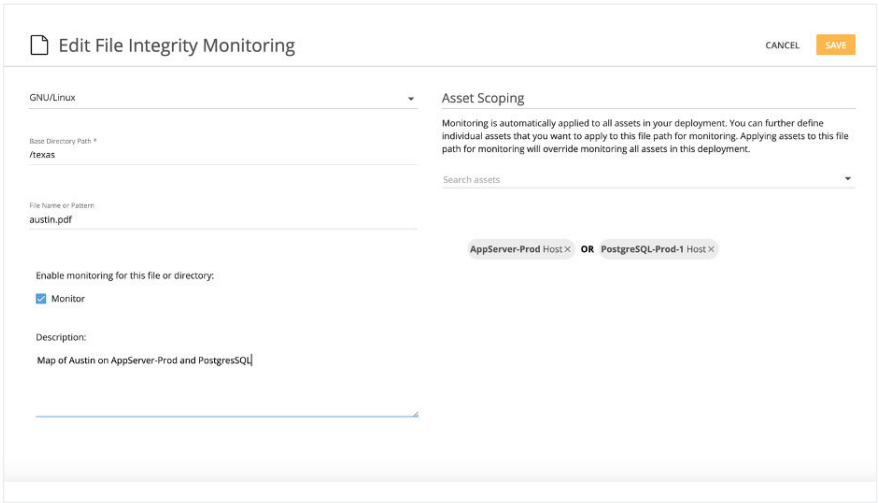
You can choose to enable all 42 directory paths or the ones that will help you achieve PCI DSS. It's recommended that you enable all the default directory paths and this can be accomplished by clicking "GNU/Linux Files" which will activate all of them. The same can be done for Windows and Windows Registry. However, we only recommend enabling FIM after you have completed your entire configuration. In addition to providing the pre-populated file paths, you have the ability to configure your own custom file paths that you have identified in the "Your Requirements" section with one click of a button.



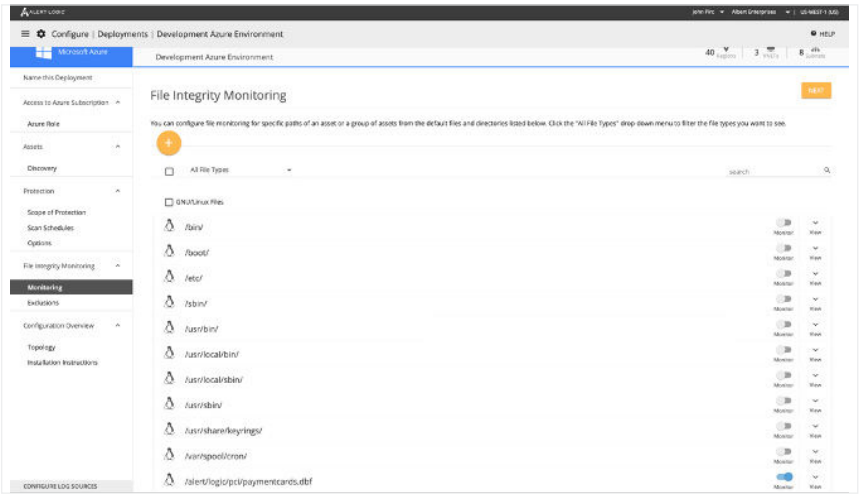
You have a couple of options when you are adding your own custom file path. You can add your own base file path that will recursively monitor anything that is created, modified or deleted in that directory path. We also support the ability to be explicit in what you are monitoring down to the exact file or file type. For example, the base path could be /texas and the file could be austin.pdf, which would only provide a filec change event for that specific file. You could also choose to configure a wildcard such as *.pdf and that would cover anything with a .pdf extension. Additionally, you can add delimiters for multiple wildcard file types in the same base path; *.tab|*.dat|*.pdf|*.tmp. It's important to note if you do nothing and click save, it will apply to every asset with the Alert Logic Agent within that deployment.



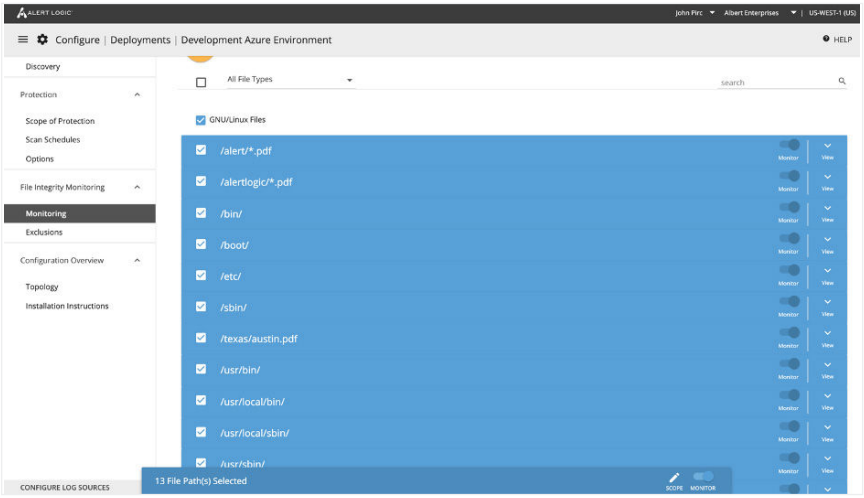
If you don't want to apply the configuration to the entire deployment, you can apply to an entire region, subnet, VPC, host or tags. In "Asset Scoping", you can customize your monitoring policy to a specific host or group of hosts within that deployment. If you choose this option, this will not apply to the entire deployment, only the assets you choose.



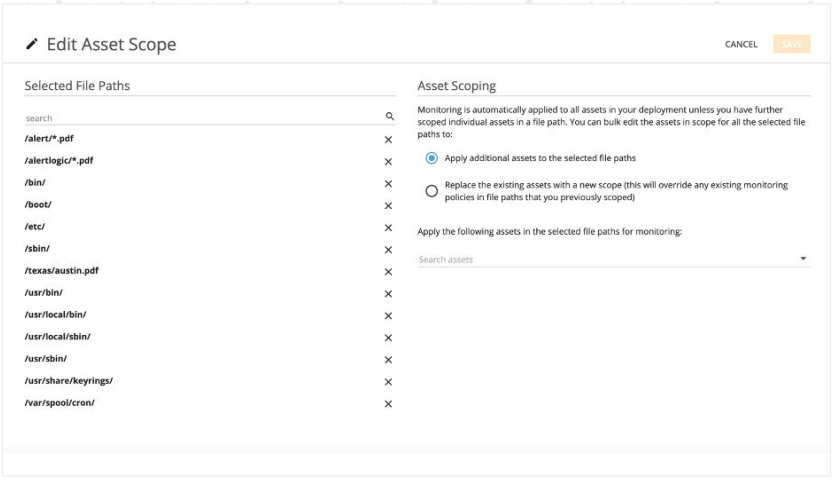
Upon saving your newly configured file path, it will automatically be enabled if you select the monitor button and will show up in the FIM configuration within the deployment you selected or assets you configured. You can choose not to select "monitor" until you have finished configuring your policy and we recommend that you not enable until you have completed configuring your FIM policy. Additionally, there is a limit of 1000 custom paths you can configure on any given deployment.



Once you have configured all your file paths for your deployment you can select all paths and click scope.



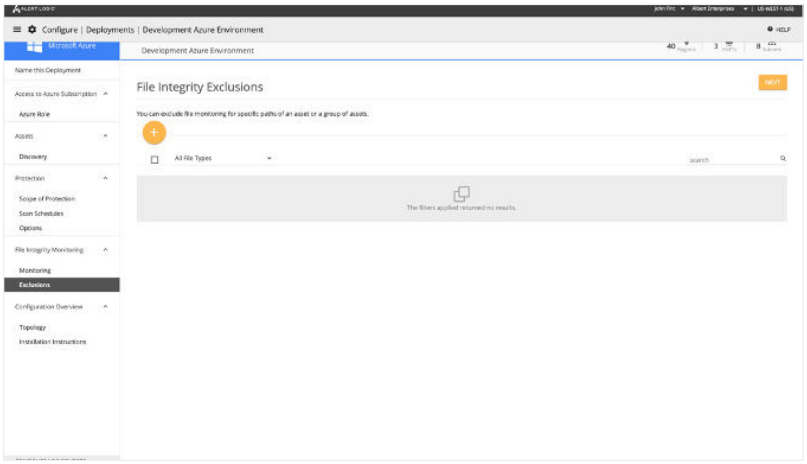
This will provide you the opportunity to edit asset scope for the entire deployment or select and option under "Asset Scoping" to add or replace assets.



Configuring FIM Exclusions

In the previous section we configured file paths, files and file types that you will monitor in order to achieve PCI compliance. However, there might be directories or other file types you don't want to see such which can be done by tuning your policy. Fortunately, we provide that same configuration experience that will provide you file paths, files or file types you don't want to see alerts from. An example could be a database file that keeps track of your pen and pencil inventory. This is probably not a critical file and you don't want to be alerted if someone modified the penandpencil.dbf file.

When you navigate to the Exclusions configuration in your current deployment, you will notice that we don't pre-populate any exclusions in your policy and should be blank.

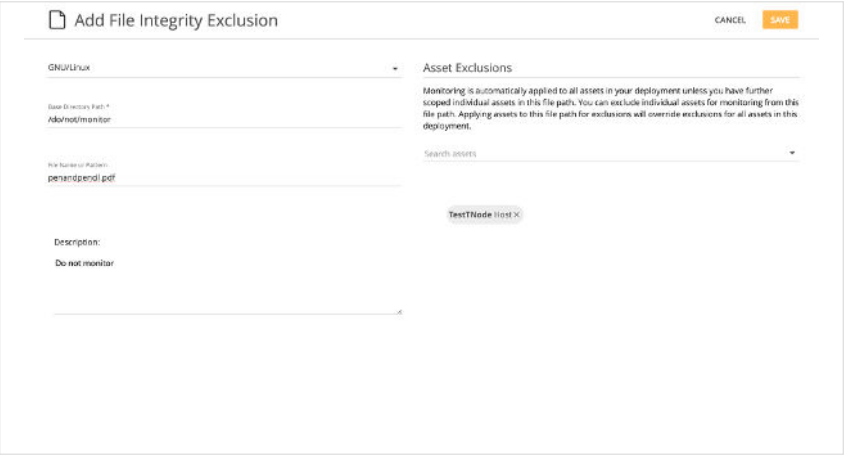


You have a couple of options when you are adding exclusions. You can add your own base file path that will recursively not monitor anything that is created, modified or deleted in that directory path. We also support the ability for you to be explicit in what you are excluding down to the exact file or file type. For example, the base path would be /do/not/monitor and the file could be penandpencil.dbf, which would not generate an alert for that specific file. You could also choose to configure a wildcard such as *.dbf and that would cover anything with a .dbf extension. Additionally, you can add delimiters for multiple wildcard file types in the same base path; *.tab|*.dat|*.pdf|*.tmp. It's important to note if you do nothing and click save, it will apply to every asset with the Alert Logic Agent within that deployment.

If you don't want to apply to the entire deployment, you can apply to an entire region, subnet, VPC, host or tags. In "Asset Exclusions" provides you more customization to a specific host or group of hosts within that deployment. If you choose this option, this will not apply to the entire deployment only to which assets you choose.

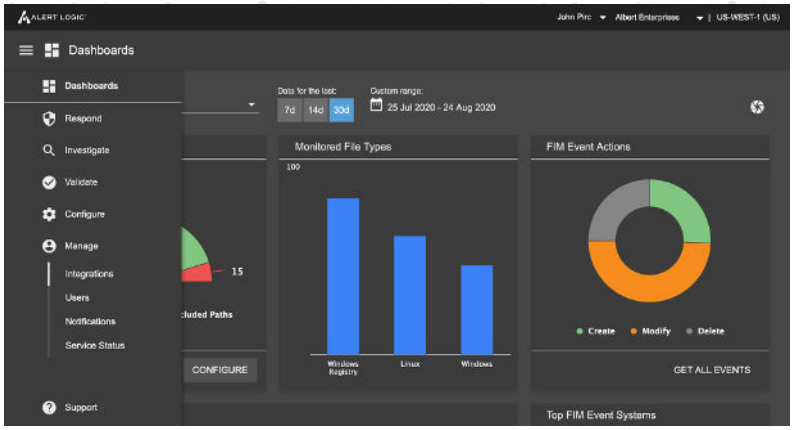
Making Last Minute Changes or Additions via Duplication

This is great for quickly adding more explicit file names that you want to monitor or exclude. This only applies if you have populated the "File Name or Pattern" field. For example, this would allow to change "austin.pdf" to "roundrock.pdf" and after hitting save, you will be monitoring "roundrock.pdf" in addition to "austin.pdf".

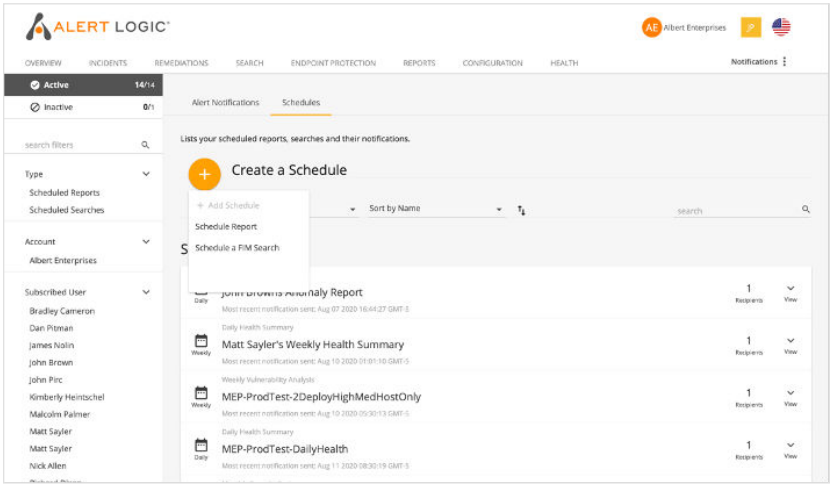


Configuring Reporting

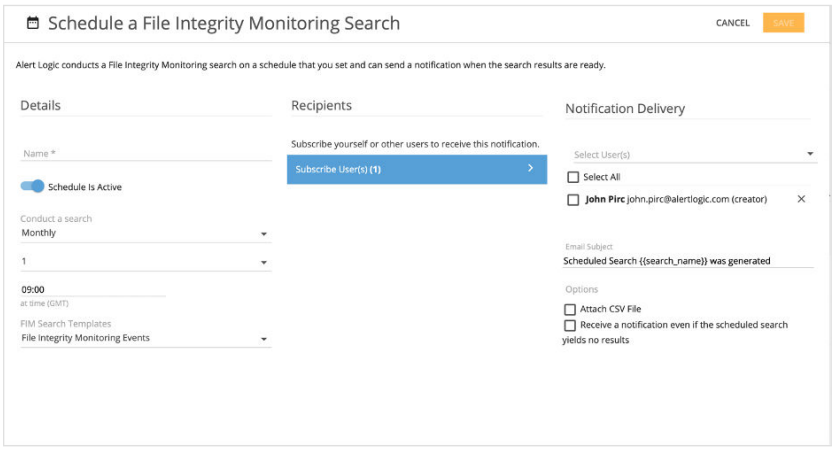
After you set up File Integrity Monitoring, you can schedule reports that will be emailed to you or a group of individuals within your organization to review. The reports can be scheduled daily, weekly or monthly. The reports will provide all file changes to your File Integrity Monitoring deployment policy. This will help you keep records of changes to your assets for compliance requirements. This is important regardless if you are working with a QSA or doing a self-assessment for PCI-DSS. To configure reporting, navigate to Manage and select Notifications.



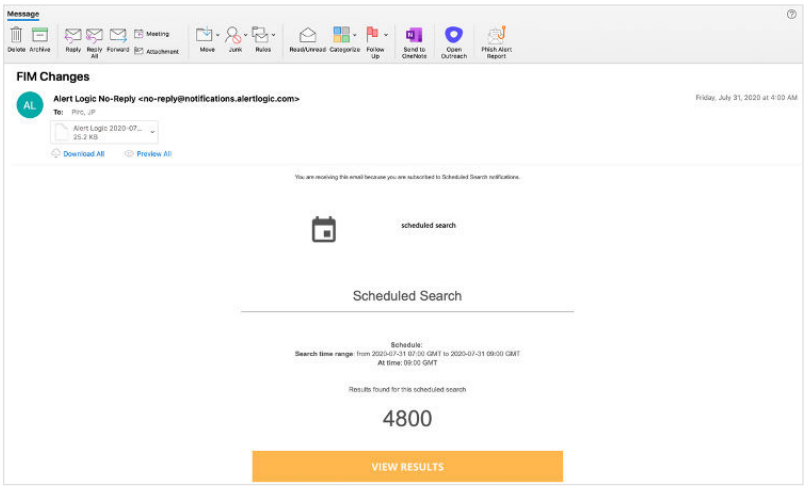
Under “Schedules,” you will select “Schedule a FIM Search.”



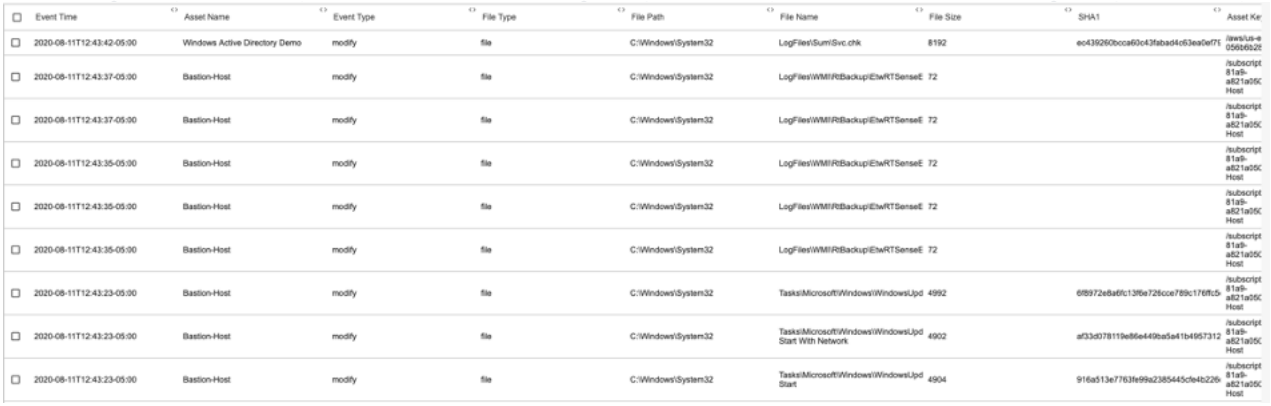
Here you will be able to name your report, the frequency with which you will receive the report, and the recipients who should receive the report. Although PCI recommends that you receive reports weekly, we suggest that you receive the reports daily so that you can react more quickly to any malicious or unauthorized activity and so that you have less to review at any one time. We also suggested that you select both CSV attachments to be delivered in the report.



Once we generate the report, you will receive the following email I containing the CSV attachment that you can open in a spreadsheet or if you choose, you can click on "View Results" and that will take you directly to the Alert Logic console to download the report in the event you didn't select to receive the CSV attachment. It's important to note that if the CSV attachment is greater than 10 MB, we will only provide a link. Depending on the size of your environment and the report frequency, it is easy to exceed 10 MB of file changes. .



Lastly, the CSV output will provide you the information of any file changes including, but not limited to, time stamp, host name, file path, event type, SHA1 hash and deployment.



Event Time	Asset Name	Event Type	File Type	File Path	File Name	File Size	SHA1	Asset Ke
2020-08-11T12:43:42-05:00	Windows Active Directory Demo	modify	file	C:\Windows\System32	LogFiles\Sum\Svc.chk	8192	ec439260bcca60c43fabad4c63ea0ef7f	/aws/us-e 058b6b2f
2020-08-11T12:43:37-05:00	Bastion-Host	modify	file	C:\Windows\System32	LogFiles\WMI\RtBackup\EtwRTSenseE	72		/subscript 81a9- a821a05(Host
2020-08-11T12:43:37-05:00	Bastion-Host	modify	file	C:\Windows\System32	LogFiles\WMI\RtBackup\EtwRTSenseE	72		/subscript 81a9- a821a05(Host
2020-08-11T12:43:35-05:00	Bastion-Host	modify	file	C:\Windows\System32	LogFiles\WMI\RtBackup\EtwRTSenseE	72		/subscript 81a9- a821a05(Host
2020-08-11T12:43:35-05:00	Bastion-Host	modify	file	C:\Windows\System32	LogFiles\WMI\RtBackup\EtwRTSenseE	72		/subscript 81a9- a821a05(Host
2020-08-11T12:43:35-05:00	Bastion-Host	modify	file	C:\Windows\System32	LogFiles\WMI\RtBackup\EtwRTSenseE	72		/subscript 81a9- a821a05(Host
2020-08-11T12:43:23-05:00	Bastion-Host	modify	file	C:\Windows\System32	Tasks\Microsoft\Windows\WindowsUpd	4992	6f8972e8a6fc13f6e726cce789c176ffc5	/subscript 81a9- a821a05(Host
2020-08-11T12:43:23-05:00	Bastion-Host	modify	file	C:\Windows\System32	Tasks\Microsoft\Windows\WindowsUpd Start With Network	4902	af33d078119e86e449ba5a41b4957312	/subscript 81a9- a821a05(Host
2020-08-11T12:43:23-05:00	Bastion-Host	modify	file	C:\Windows\System32	Tasks\Microsoft\Windows\WindowsUpd Start	4904	916a513e7763fe99a2385445cfe4b226	/subscript 81a9- a821a05(Host

Conclusion

In this document, you learned how to navigate the dashboard and that you can use it as a triage tool to identify noisy file paths and possible malicious behavior. We demonstrated how you can quickly take advantage of the 42 pre-populated file paths to reduce configuration time and the ability to create custom monitoring or exclusion paths, file types, bulk scope edits, duplicating single pre-configured scopes to ease configuration burden. Additionally, we provided you guidance on schedule searches to achieve PCI-DSS 10.5.5 and 11.5 compliance. For more technical information on configuring File Integrity Monitoring, please click here.