WHITEPAPER

snare
A PROPHECY SOLUTION

How Snare helps with FIM, FAM, RIM and RAM

About this paper -
How Snare helps with FIM, FAM, RIM and RAM

This document is designed to assist a systems/security administrators with managing the File Integrity Monitoring (FIM), File Activity Monitoring (FAM), Registry Integrity Monitoring (RIM) and Registry Activity Monitoring (RAM) with Snare Enterprise Agents, Snare Central Server and the Snare Advanced Analytics dashboards.

FIM, FAM, RIM and RAM General Overview

For many years systems have used various third party software to monitor the systems files and data. Third party software features to perform a checksum on a selected group of files and directories has been one method to track file changes. This has been known as File Integrity Monitoring also known as FIM.

This software would keep a master database repository of the checksum data of the selected files and directories store and keep the log information locally or send the data to a central server. It would then run periodic checks of all the files again to compare the current state to the master copy or baseline of information. These software checks would typically be performed once a week or daily depending on the business needs. The principal behind the checksum approach was to detect a change to a file or directory, this would then trigger an alert and report to administrator to highlight the file or contents of a directory had changed from the master copy. The report would show the details of the file including the change time, file size, or owner information along with the before and after details.

The administrator would then have to determine who, how and what data had actually changed, if it was of concern and if any action was required. The Who, What and How questions are answered by using File Activity Monitoring or FAM. These events will track all the user based activity performed on the system that traditional FIM cant do.

While the traditional FIM solutions are very good for detecting that a change has occurred they are limited and don't allow the administrator to know who did the change, how many times they changed the files and what they used to make the change. This is where FAM or File Activity Monitoring compliments the traditional FIM solutions.

The Snare Enterprise agents for Windows, Linux, macOS and Solaris have the ability to monitor all file based activity and provide a much greater depth of information than traditional FIM solutions. The reporting ability of the Enterprise agents includes all read, write, change and delete activity on a file or directory. The Snare Enterprise agents can track and report on these changes in near real time. So if unauthorised activity is occurring the events are being captured and sent to the central SIEM system as they are occurring with minimal delay. These events can then be processed and real time alerts initiated to warn security staff that changes are occurring on sensitive files or data. If the SIEM system is the Snare Central Server or Snare Advanced Analytics then it can generate these alerts as the events are received or be based on specific threshold levels before being reported on. The events provide much greater detail than traditional FIM solutions in that it will show the specific userid, commands used to change or view the file (ie text editor, script, programs that was run). If they were to make multiple changes to the file, each instance of the change is recorded logged and sent to the central SIEM system and provides more detail than when, compared to only a single summary that a change occurred with traditional FIM solutions.

Additionally the Snare Enterprise agent will also report on any attempted access to files or directories that were not successful as failure events. This can also capture potential malicious activity on systems and may give early warning to a potential data breach.

For customers that also require the specific feature of FIM capability the all of our current v5 agents support the checksum (SHA512) feature for monitoring files, directories and on Windows platforms the registry keys. The agents will report on all changes, additions and deletes of files or registry keys, along with the relevant file systems permissions, file ownership changes. The full delta of the changes can be tracked with before baseline details and the after changes being reported on. This data can also be correlated with the FAM activity as detailed above to assist with any forensic investigation.

1.1. Why the need for FIM or FAM?

So why the need for file activity monitoring such as FIM and FAM? There can be many business reasons and can be a mixture of the following:

- Compliance such as PCI DSS (v4) for requirements 10.3.4, 10.4.1, 10.7, 11.5.2, 12.9, A3.3 where it is a must for compliance activity
- Tracking changes for hacker or unauthorised activity
- Malware outbreaks for system changes. This can be useful for where there is a day zero vulnerability that normal malware detection does not block and the exploit allows access to the system, now the malware or hacker starts to make changes to gain additional privilege or plant Trojans on the network.
- Intruder detection where the hacker is gaining access to systems and making changes as they move laterally around the network. Knowing what they changes and access is critical to any incident investigation and remediation activity.
- Data theft such as discriminated employees copying data, changing data, or sending internal corporate information out of the network.

1.2. Monitoring of all types of files an user data

All critical files need to be monitored. So what is critical? in general most staff can point to files that they cant lose or are very sensitive in nature that others should not see or tamper with. These can be any system files or user data such as:

- Operating system binary exe's,, DLL files, configuration files and application registry keys
- Third party application binaries, DLL files, configuration files, and application registry keys, many vendors can advise on critical parts of their applications that should be monitored and the integrity of the data is paramount to its operation.
- User data files such as spreadsheets, text files, MS Word documents, PowerPoint files etc
- Sensitive documentation and files that should be restricted to staff that have a need to know.
- Application database files are generally not a good fit for FIM and FAM monitoring as they constantly change. Unless the application data files should generally be static then they can be a candidate for monitoring.
- Log files for key systems, while some log files can be highly active, archived log files should never change as they are a record of what has occurred.

1.3. What systems should be monitored

Most systems will benefit from being monitored. The critical nature and value of the data that system contains is usually the key factor to help determine what should monitored. If management of the business, business operations or users cant live without the system or data then its often critical. System such as:

- Domain Controllers
- Application Servers
- Database Servers
- Web Servers
- Key desktops that perform critical business functions for key staff.
- POS systems, these usually have a PCI DSS requirement to be monitored.

1.4. The Snare Solution

1.5. Continuous Monitoring of Files

With the Snare file activity monitoring solution, you will collect the audit log data and can be notified when files are created or key files are viewed, deleted, modified, or when user or group ownership is changed. You can selectively monitor with granular controls and filters that can pinpoint specific files and either perform scans at desired intervals or operate in near real-time for continuous monitoring.

Correlate file-level behaviour to enhance security and audit activities. Easily pivot from a file access or change to a specific user, then view a full timeline of user activity, containing both FIM, FAM, RIM or RAM along with other user activity information. With Snare Enterprise agent policy-based FIM, FAM, RIM and RAM features, you can assign multiple policies to the same endpoint, reducing ongoing management overhead as policies are updated. Policies can also be managed from our Snare Agent Manager Console (SAMC). For example, individual policies can be created for Windows, Linux or macOS operating system files and directories.

Domain Controllers, Application Servers, File Servers, Web Application Servers, and DNS Servers. FIM and FAM multi-policy support simplifies management, ensuring that the policies are assigned to the appropriate system assets and that changes to those policies are centrally managed via the AMC and propagated across the environment.

In addition, Using our Snare Advanced Threat Intelligence suite the FIM, FAM, RIM and RAM activity can be correlated and detect changes to systems outside of authorised change control windows when linked with the customers change tracking systems. Snare detects these changes by monitoring production servers for changes that occur outside normal operating windows which can be defined using our Real time alerts/Threshold reporting feature or changes that don't precede an authorised change request from the customers change tracking system. With the addition of this file monitoring features and the data it generates, Snare can monitor for and alert on a variety of malicious behaviours, from improper user access of confidential files to botnet-related breaches and transmittal of sensitive data as detailed above.

1.6. Easy to Deploy

Snare agents are easy to deploy

- Pre-configure your agent using your custom configurations including file policies for the operating systems you need. For Windows platforms using our smart MSI packing makes deployment easy and can be deployed using GPO, Microsoft SCCM and other software deployment tools.
- Simplified policy administration with the ability to assign multiple FIM, FAM, RIM and RAM policies to the same host so you can monitor different directories, specific files, and applications as needed
- Centralised Policy Management with the Snare Agent Manager Console (SAMC) for all v5.8+ Snare agents
- Available for deployment on both desktops and servers
-

All of the Snare Enterprise agents support FAM and the latest v5.2.x agents or greater all support FIM and on Windows RIM and RAM. There are several Snare Enterprise agents for different operating systems that include:

- Snare Enterprise Agent for Windows
- Snare Enterprise Agent for Linux
- Snare Enterprise Agent for Solaris
- Snare Enterprise Agent for OS X

To see the feature set of the Enterprise Agents, go to the snaresolutions website at https://www.snaresolutions.com/products/snare-agents/

The nest section of this document instructs users of the Snare Enterprise Agent on how to use it for FIM, FAM, RIM and RAM based on your operating system platform.

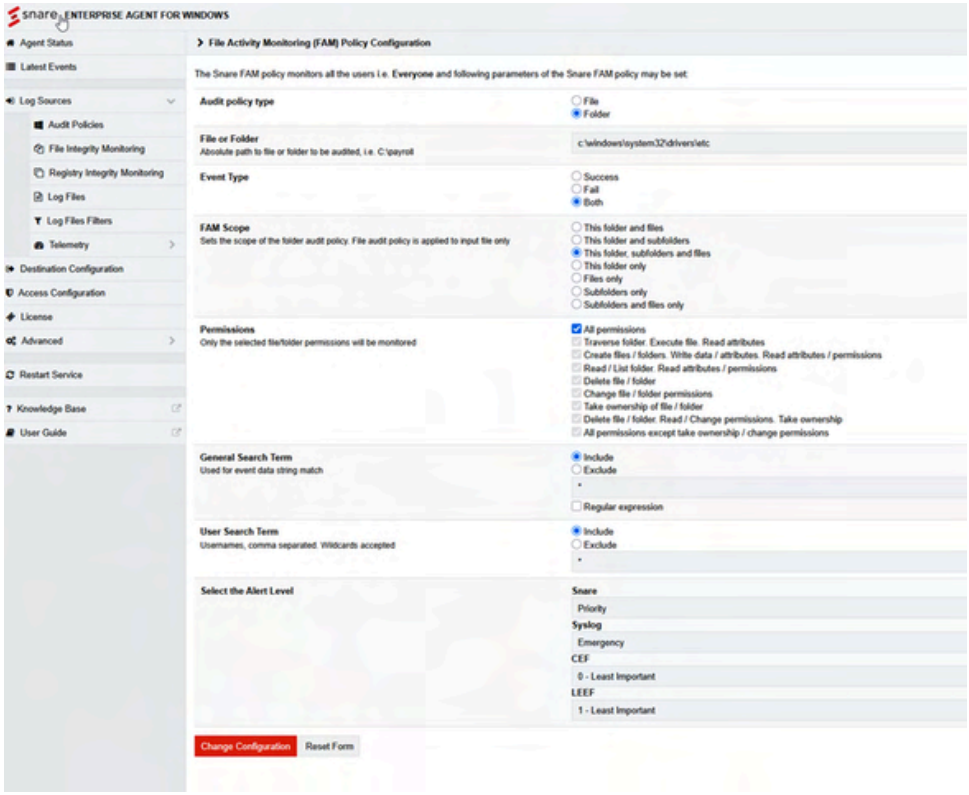
FIM, FAM, RIM and RAM Settings for Snare Enterprise Agent for Windows

To configure the Snare Enterprise Windows agent to perform File Integrity Monitoring (FIM), File Activity Monitoring (FAM), Registry Integrity Monitoring (RIM) and Registry Activity Monitoring (RAM) perform the following basic steps.

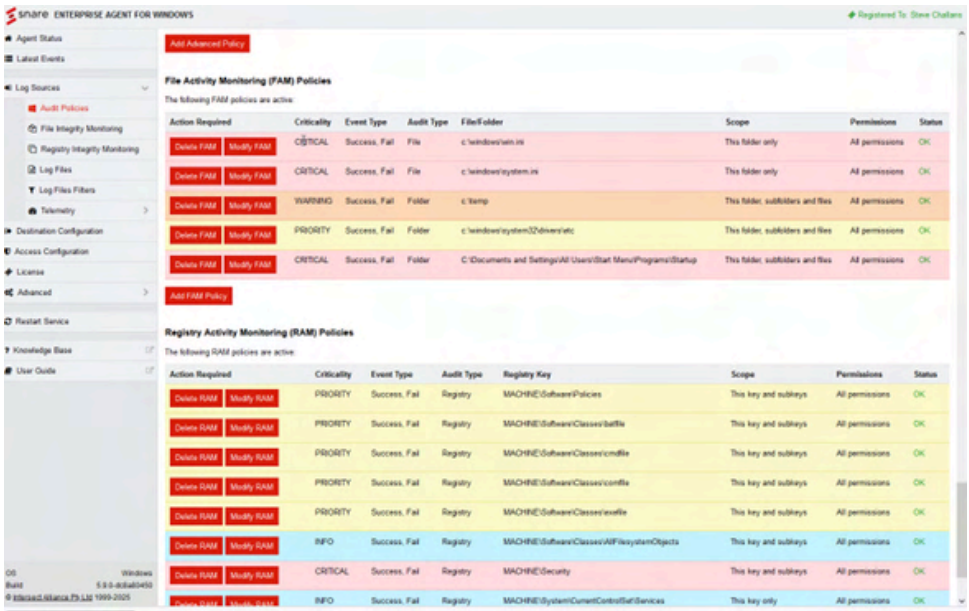
- Review the critical parts of the operating system and applications that need to be monitored.
- In general, there will be many files, directories and registry keys that need to be monitored. This should form your baseline or core monitoring
- Document the baseline of these parts of the system that need to be audited and monitored.
- Create Snare objectives in the agents to match the configuration that you documented. You may require different policies for different systems. You can use the Snare Agent Management Console to manage different polices on different systems based on operational needs.
- Ensure that all the systems have the correct date and time and are using NTP settings to keep accurate time.
- In the reporting system such as Snare Central reports ensure that the events are being monitored and alerts are configured to notify the relevant staff of the system changes.

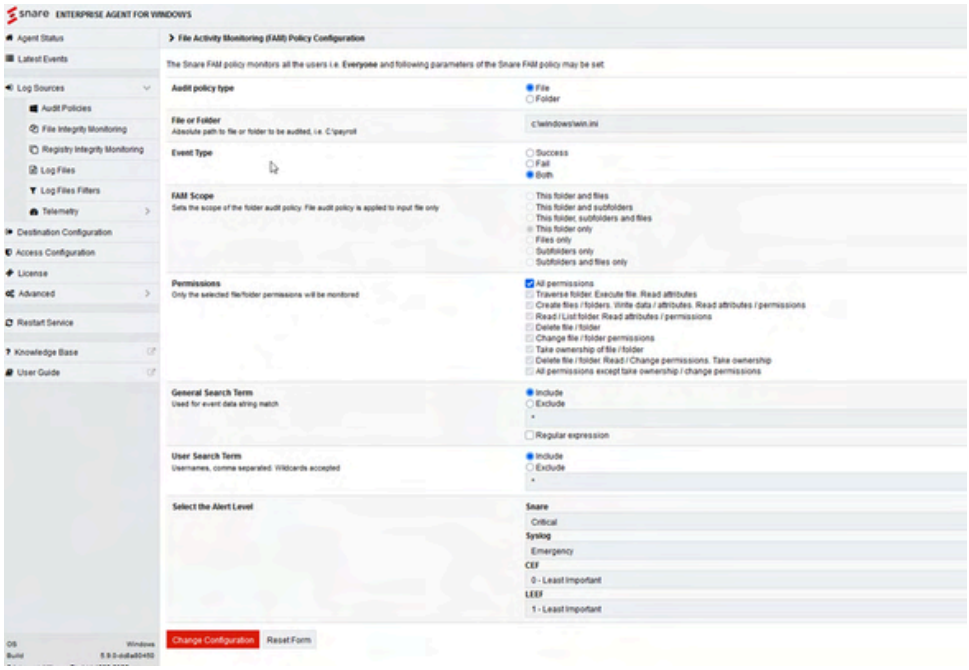
The FAM and RAM features use the host operating systems audit function. For Windows this is driven by audit policy of the system. The events produced relate to the activity being performed which can include reads, changes, adding or deletions of files or registry keys. The Windows platform can generate many events related to file changes on a system. These events will need to be correlated together to determine what the user did. The events will show what application was used for the relevant activity ie used MSWord to open the file and saved it back with some changes or deleted a file from a command prompt. For registry activity these events will show the before and after changes to any registry keys in the single event. As with other windows events the events will show the data and time of the activity, details of the user performing the operation and all the related commands the used along with any success or failure status. The basic process to configure a FAM and RAM monitoring policy is as follows:

- Allow SNARE to automatically set file audit configuration on the general configuration screen. If this is not set in the agent then all of the policy settings will need to be set manually or via local policy or AD group policy. Using this setting enables the file system auditing to be controlled by the Snare audit policy settings. In order for Windows to collect file and registry access records, not only must the correct audit category be selected, but also the correct object auditing parameters must also be set. Setting this field will automatically set these parameters, based on the agent policy which have been set. It is highly recommended that this checkbox be selected.
- Open the agent policy screen under Log Sources\Audit Policies and scroll down and select Add FAM Policy. If on 5.10 or later then select File Activity Monitoring or Registry Activity Monitoring.
- For file auditing, enter the target file or folder radio button and enter the values e.g. c:\auditme\.
- For RAM registry select Add RAM Policy for auditing and then select the Registry key value e.g. (HKEY_LOCAL_MACHINE only), enter the registry key e.g. “Software\Policies” into the field of the policy.
- Select the Event type to be collected for Success, Fail or Both
- Select the event permission types eg all, read, create, delete etc for the types to be collected.
- Filter logs using the General Search Term to either include only specific events or exclude them. You can use a Regular Expression if it requires more complex filtering.
- Then select the relative priority level of the events if the target system can understand these syslog settings.
- If applicable, set the criticality of the event so it can be tracked in Snare Central Server if events are being tracked in this way. Some events may be more critical than others, so this feature allows events to be grouped in ways to make its more applicable for reporting.
- The source of these logs will generally be from the Security event log location.



As of agent version 5.6.0 the UI has been updated and will display the following for FAM and RAM settings under audit policies. Version 5.9.0 also introduced a new menu structure in the agent to simplify navigation.



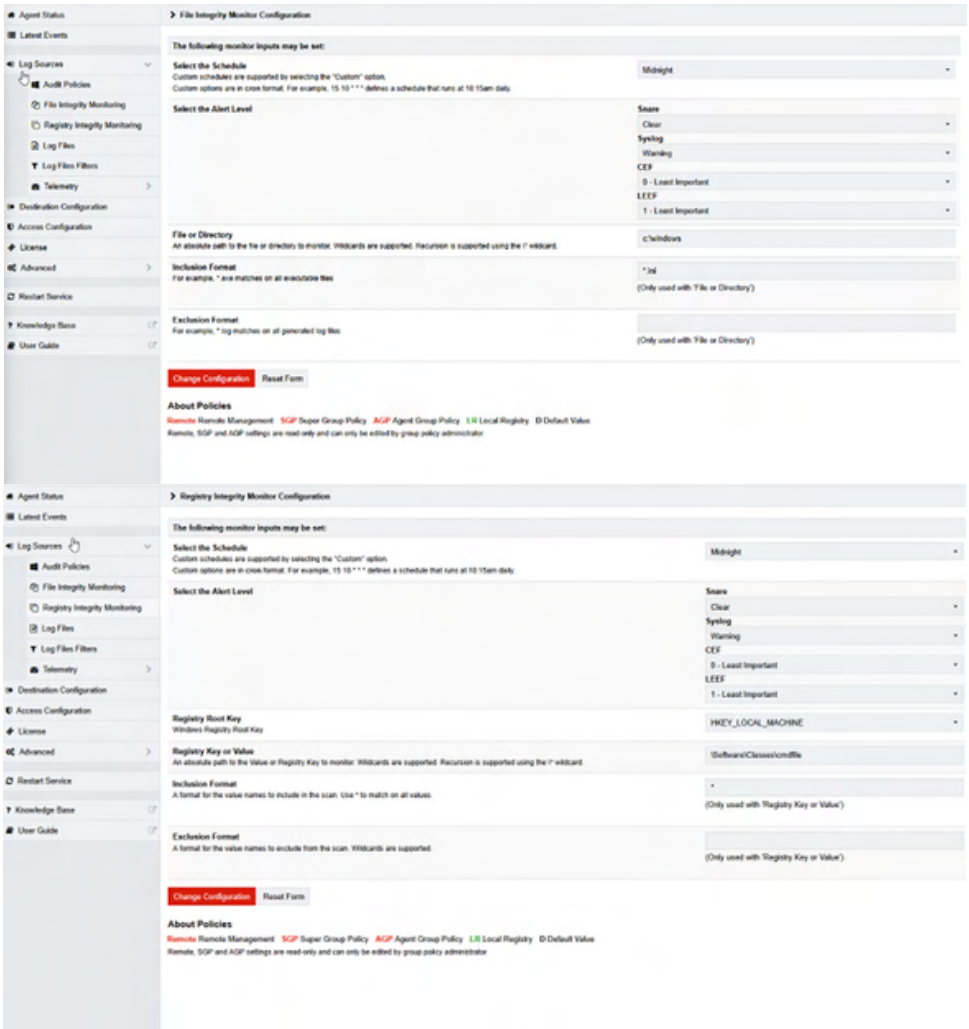


Once the all the settings are set as desired then press the Change Configuration button to save the policy. Repeat this approach for all desired files or folders that require auditing enabled. Once all the policies have been made then select “Apply the latest audit configuration” button and restart the agent. The events will show up in the latest events screen using the standard Windows Event IDs. The events can be any of the following:

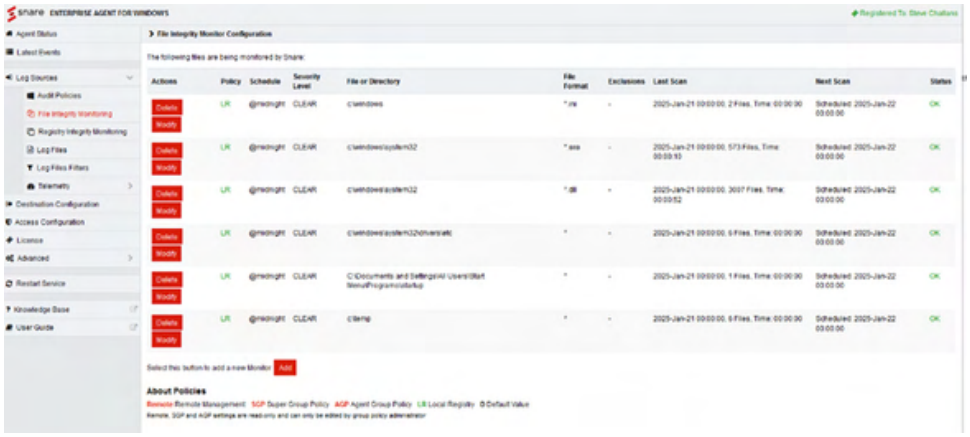
- Access a file or directory.
- for Windows 2003 and XP based systems 560, 561, 562, 563, 564, 565, 566, 567, 594, 595
- For Windows 2008, 2012, 2016, 2019, 2020, 2022, 2025 and later, windows 7,8,10,11 based systems they will use any of these event ids 4656, 4657, 4658, 4659, 4660, 4661, 4662, 4663, 4690, 4691

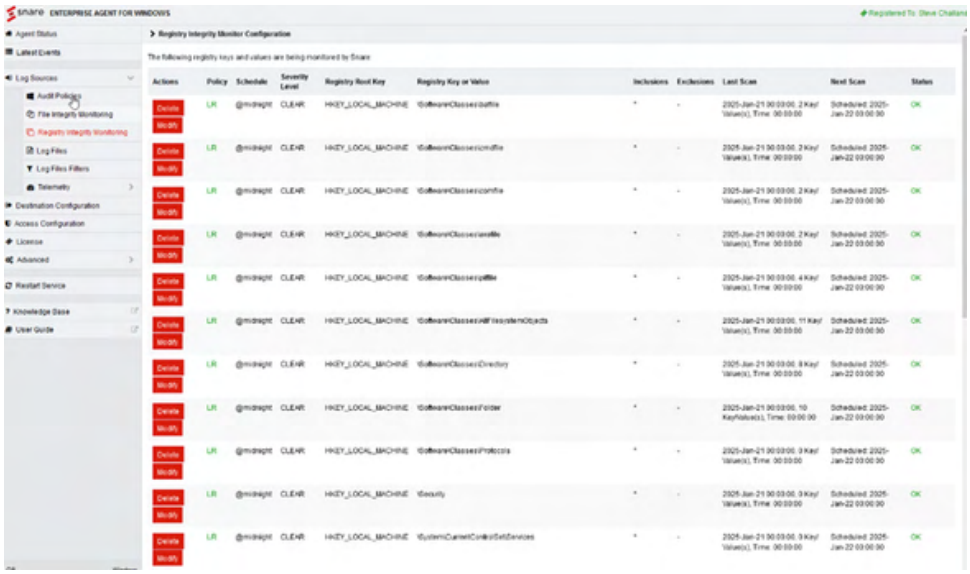
There are various standards that call for the usage of FIM and RIM such as PCI DSS. The technology compliments the FAM and RAM features with looking at some details of the file and registry changes performed on the systems. However the events will show the results of the change and not who made the change. The who activity monitoring comes as part of the FAM and RAM monitoring as detailed above. The FIM and RIM features use a checksum approach along with file system details to determine changes made to files. The Snare Enterprise agents can perform these file system checks based on a schedule of the customers choosing. In general these change detection process would be run either daily or weekly depending on the granularity required. These system checks can be system intensive as the agent has to perform a lot of disk IO to read all the files and then perform the checksum (SHA512) operations which is more CPU intensive operation, so they would generally be performed out of hours or when the system has low user activity. The basic process to configure FIM and RIM for the windows agent is as follows.

- Select the File Integrity Monitoring or Registry Integrity Monitoring menu item on the left under Log Sources
- Select the Add button
- Select the schedule the FIM/RIM checks will be performed
- Select the Alert critically levels of these events
- Enter the file or Directory path. A file will be the absolute path to that file to be monitored. For a directory its the path to that location. If you require a recursive search from that location then enter * at the end as per the agent instructions.
    - for Registry Monitoring enter the KEY path details ie HKEY_LOCAL_MACHINE from the drop down menu. Then select the registry Key or Value to be monitored. This is the absolute path of the Registry Key. As with the FIM wild card searching and recursive monitoring can also be performed.
- Enter the inclusion format ie *.exe to just select .exe files, Others such as *.dll or *.* can be used for all files in a location.
    - for Registry Monitoring enter the registry key or path that is to be monitored. The inclusion format is generally just a single * unless only specific keys are being monitored
- If there are files that you need to exclude then enter them in the exclusion section.
- Save the agent settings by selecting the Change Configuration button and then run the Apply Configuration to restart the agent
- The events will now show up in the latest events in the FIM section when the schedule kicks in showing the type of the event being New File, Change or Delete operations.



Agent 5.9.0 versions will appear as follows for FIM and RIM configuration settings once entered.





FAM and FIM Settings for Snare Enterprise Agent for Linux

The approach for enabling File Activity Monitoring for Linux is similar to Windows however the directory structure and options available are slightly different due to the operating system.
The Unix / Linux agents have a separate file watch section in the policy screen that allows policies to be created on files or directories. To configure the Snare Enterprise Linux agent to perform File Integrity Monitoring and File Activity Monitoring perform the following basic steps.

- Review the critical parts of the operating system and applications that need to be monitored. In general there will be many files, directories and registry keys that need to be monitored. This should form your baseline or core monitoring
- Document the baseline of these parts of the system that need to be audited and monitored.
- Create Snare policies in the agents to match the configuration that you documented. You may require different policies for different systems. You can use the Snare Agent Management Console to manage different polices on different systems based on operational needs.
- Ensure that all the systems have the correct date and time and are using NTP settings to keep accurate time.

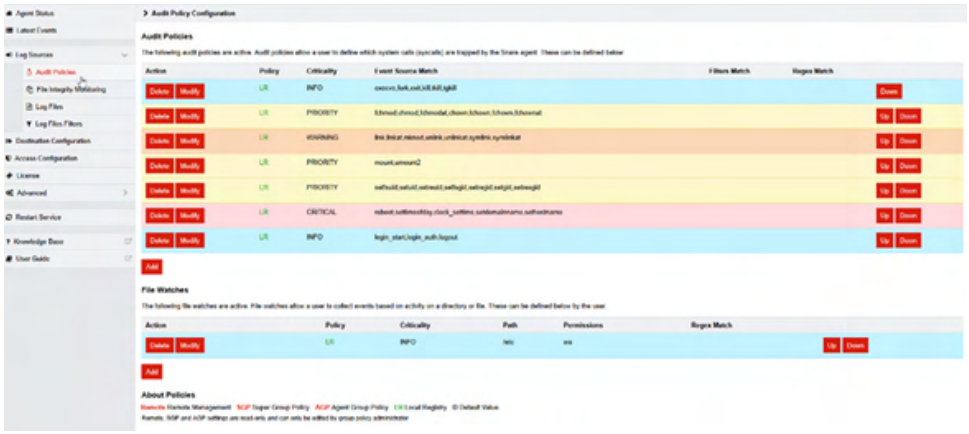
- In the reporting system such as Snare Central or Snare Advanced Analytics ensure that the events are being monitored and alerts are configured to notify the relevant staff of the system changes.

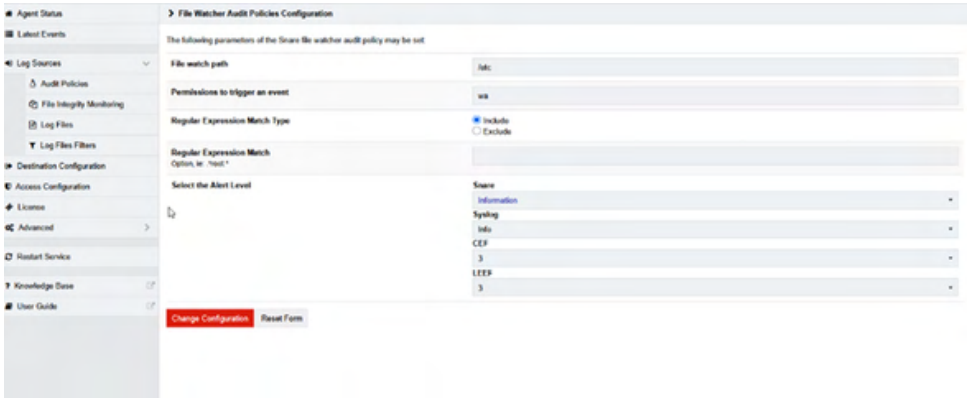
The FAM features use the host operating systems auditd function which is part of Linux. For Linux based systems this is driven by auditd policy of the system which is managed by the Snare for Linux agent. The events produced relate to the activity being performed which can include reads, changes, adding or deletions of files on the system. The Linux platform can generate many events related to file changes on a system which can come from user actions or activities performed by CRON, These events will need to be correlated together to determine what the user did. The events will show what application was used for the relevant activity ie used vi to open the file and saved it back with some changes, or deleted a file from a shell command prompt. The basic process to configure a FAM policy is as follows:

To configure a file watch policy in Linux:

1. Allow SNARE to automatically set audit configuration on the general configuration screen. If this is not set in the agent then all of the policy settings will need to be set manually or via manual updates to the audit.rules configuration file. Using this setting enables the file system auditing to be controlled by the Snare policy settings. In order for Linux to collect file and directory access logs, Not only must the correct audit category be selected, but also the correct audit rules be applied to the auditing system. Setting this field will automatically set these parameters, based on the policies which have been set. It is highly recommended that this checkbox be selected.
2. Open the policy screen and select “Add” for a new file watch radio button.
3. For file auditing, enter the target file or directory into the File watch path of the objective, e.g. /auditme/. There is a default objective that watches the /etc directory location. You can add many locations either specific directories or mount points that are in use on the Linux host.
4. Select the event permissions to watch ie “wa” for all writes and accesses to files
5. Enter a regex to match events of a specific type or user ie "".*root.*"
6. If applicable set the alert level of the event so it can be tracked in Snare Server if events are being tracked in this way. Some events may be more critical than others so this feature allows events to be grouped in ways to make its more applicable for reporting.
7. Once complete press the “Change Configuration” button and apply the latest audit configuration to restart the agent.

The figure below displays a file watch objective for the Snare Enterprise Linux agent, as of 5.9.0 the UI has been updated as per below:



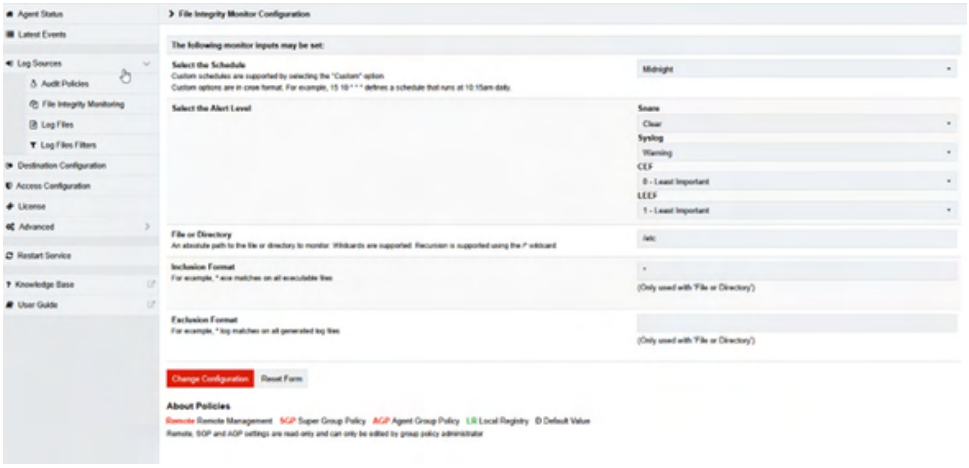


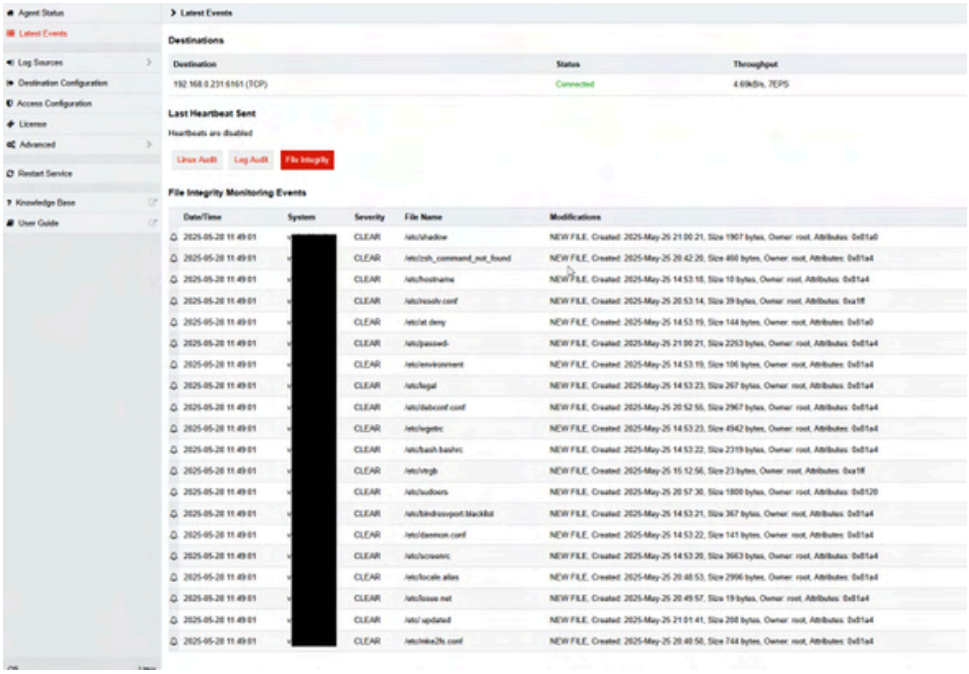
Once the all the settings are set as desired then press the Change Configuration button to save the policy. Repeat this approach for all desired files or directories that require file watch auditing enabled. Once all the policies have been made then select “Apply the latest audit configuration” button and restart the agent. The events will show up in the latest events screen using the standard Linux events. The events can be any of the following:

- Access a file or directory.
- execve calls showing the command run on the system to perform the file operation. These can be combined with other system calls for fchmod, chmod, fchmoda, chown, kchown, fchownat, link, linkat, mkmod, unlink, unlinkat, symlink, symlinkat.

There are various standards that call for the usage of FIM such as PCI DSS. The technology compliments the FAM features with looking at some details of the file and directory changes performed on the systems. However the events will show the results of the change and not who made the change. The who activity monitoring comes as part of the FAM monitoring as detailed above. The FIM features use a checksum approach along with file system details to determine changes made to files. The Snare Enterprise agents can perform these file system checks based on a schedule of the customers choosing. In general these change detection process would be run either daily or weekly depending on the granularity required. These system checks can be system intensive as the agent has to perform a lot of disk IO to read all the files and then perform the checksum (SHA512) operations so they would generally be performed out of hours or when the system has low user activity. The basic process to configure FIM for the Snare Enterprise Linux agent is as follows.

- Select the File Integrity Monitoring menu item on the left
- Select the Add button
- Select the schedule the FIM checks will be performed
- Select the critically levels of these events
- Enter the file or Directory path. A file will be the absolute path to that file to be monitored. For a directory its the path to that location. If you require a recursive search from that location then enter /* at the end as per the agent instructions. Note that this forward slash on Linux.
- Enter the inclusion format ie * to just select .all files, Others such as *.config can be used for just config files in a location.
- If there are files that you need to exclude then enter them in the exclusion section.
- Save the agent settings by selecting the Change Configuration button and then run the Apply Configuration to restart the agent
- The events will now show up in the latest events in the FIM section when the schedule kicks in showing the type of the event being New File, Change or Delete operations.


Agent Status
Latest Events
Log Sources
Audit Policies
File Integrity Monitoring
Log Files
Log Files Filters
Destination Configuration
Access Configuration
License
Advanced
Restart Service
Knowledge Base
User Guide
File Integrity Monitor Configuration
The following monitor inputs may be set:
Select the Schedule
Custom schedules are supported by selecting the "Custom" option.
Custom options are in cron format. For example, 15 10 * * * defines a schedule that runs at 10:15am daily.
Midnight
Select the Alert Level
Snare
Clear
Syslog
Warning
CEF
0 - Least Important
LEEF
1 - Least Important
File or Directory
An absolute path to the file or directory to monitor. Wildcards are supported. Recursion is supported using the /* wildcard.
/etc
Inclusion Format
For example, *.exe matches on all executable files
(Only used with 'File or Directory')
Exclusion Format
For example, *.log matches on all generated log files
(Only used with 'File or Directory')
Change Configuration
Reset Form
About Policies
Remote Remote Management SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value
Remote, SGP and AGP settings are read-only and can only be edited by group policy administrator


Agent Status
Latest Events
Log Sources
Destination Configuration
Access Configuration
License
Advanced
Restart Service
Knowledge Base
User Guide
Latest Events
Destinations
Destination
Status
Throughput
192.168.0.231:6161 (TCP)
Connected
4.69kB/s, 7EPS
Last Heartbeat Sent
Heartbeats are disabled
Linux Audit
Log Audit
File Integrity
File Integrity Monitoring Events
Date/Time
System
Severity
File Name
Modifications
2025-05-28 11:49:01
CLEAR
/etc/shadow
NEW FILE, Created: 2025-May-25 21:00:21, Size 1907 bytes, Owner: root, Attributes: 0x81a0
2025-05-28 11:49:01
CLEAR
/etc/zsh_command_not_found
NEW FILE, Created: 2025-May-25 20:42:26, Size 468 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/hostname
NEW FILE, Created: 2025-May-25 14:53:18, Size 10 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/resolv.conf
NEW FILE, Created: 2025-May-25 20:53:14, Size 39 bytes, Owner: root, Attributes: 0xa1ff
2025-05-28 11:49:01
CLEAR
/etc/at.deny
NEW FILE, Created: 2025-May-25 14:53:19, Size 144 bytes, Owner: root, Attributes: 0x81a0
2025-05-28 11:49:01
CLEAR
/etc/passwd-
NEW FILE, Created: 2025-May-25 21:00:21, Size 2253 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/environment
NEW FILE, Created: 2025-May-25 14:53:19, Size 106 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/legal
NEW FILE, Created: 2025-May-25 14:53:23, Size 267 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/debconf.conf
NEW FILE, Created: 2025-May-25 20:52:55, Size 2967 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/wgetrc
NEW FILE, Created: 2025-May-25 14:53:23, Size 4942 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/bash.bashrc
NEW FILE, Created: 2025-May-25 14:53:22, Size 2319 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/vtrgb
NEW FILE, Created: 2025-May-25 15:12:56, Size 23 bytes, Owner: root, Attributes: 0xa1ff
2025-05-28 11:49:01
CLEAR
/etc/sudoers
NEW FILE, Created: 2025-May-25 20:57:36, Size 1809 bytes, Owner: root, Attributes: 0x8120
2025-05-28 11:49:01
CLEAR
/etc/bindresvport.blacklist
NEW FILE, Created: 2025-May-25 14:53:21, Size 367 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/deemon.conf
NEW FILE, Created: 2025-May-25 14:53:22, Size 141 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/screenrc
NEW FILE, Created: 2025-May-25 14:53:20, Size 3663 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/locale.alias
NEW FILE, Created: 2025-May-25 20:48:53, Size 2996 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/issue.net
NEW FILE, Created: 2025-May-25 20:49:57, Size 19 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/.updated
NEW FILE, Created: 2025-May-25 21:01:41, Size 208 bytes, Owner: root, Attributes: 0x81a4
2025-05-28 11:49:01
CLEAR
/etc/mke2fs.conf
NEW FILE, Created: 2025-May-25 20:48:58, Size 744 bytes, Owner: root, Attributes: 0x81a4

FAM Settings for Snare Enterprise Agent for Solaris and macOS

The approach for enabling File Activity Monitoring for Solaris and Mac OSX is similar to Linux however the objective settings are slightly different due to the operating system audit differences. The Solaris and OSX agents need to use filtering options on the objectives to select the files or directories. For Sun Solaris and Mac OSX agents the operating system does not have the same facility as Linux so the events have to be selected based on the search term parameters.
To configure the Snare Enterprise Solaris and OSX agent to perform File Integrity Monitoring perform the following basic steps.

- Review the critical parts of the operating system and applications that need to be monitored. In general there will be many files, directories and registry keys that need to be monitored. This should form your baseline or core monitoring
- Document the baseline of these parts of the system that need to be audited and monitored.
- Create Snare objectives in the agents to match the configuration that you documented. You may require different policies for different systems. You can use the Snare Agent Management Console to manage different polices on different systems based on operational needs.
- Ensure that all the systems have the correct date and time and are using NTP settings to keep accurate time.
- In the reporting system such as Snare Central or Snare Advanced Analytics ensure that the events are being monitored and alerts are configured to notify the relevant staff of the system changes.

The FAM features use the host operating systems BSM audit function which is part of Solaris and macOS platforms. For these systems this is driven by BSM audit policy of the system which is managed by the Snare Enterprise agent. The events produced relate to the activity being performed which can include reads, changes, adding or deletions of files on the system. The BSM platform can generate many events related to file changes on a system which can come from user actions or activities performed by CRON, These events will need to be correlated together to determine what the user did. The events will show what application was used for the relevant activity ie used vi to open the file and saved it back with some changes, or deleted a file from a shell command prompt. The basic process to configure a FAM objective is as follows:

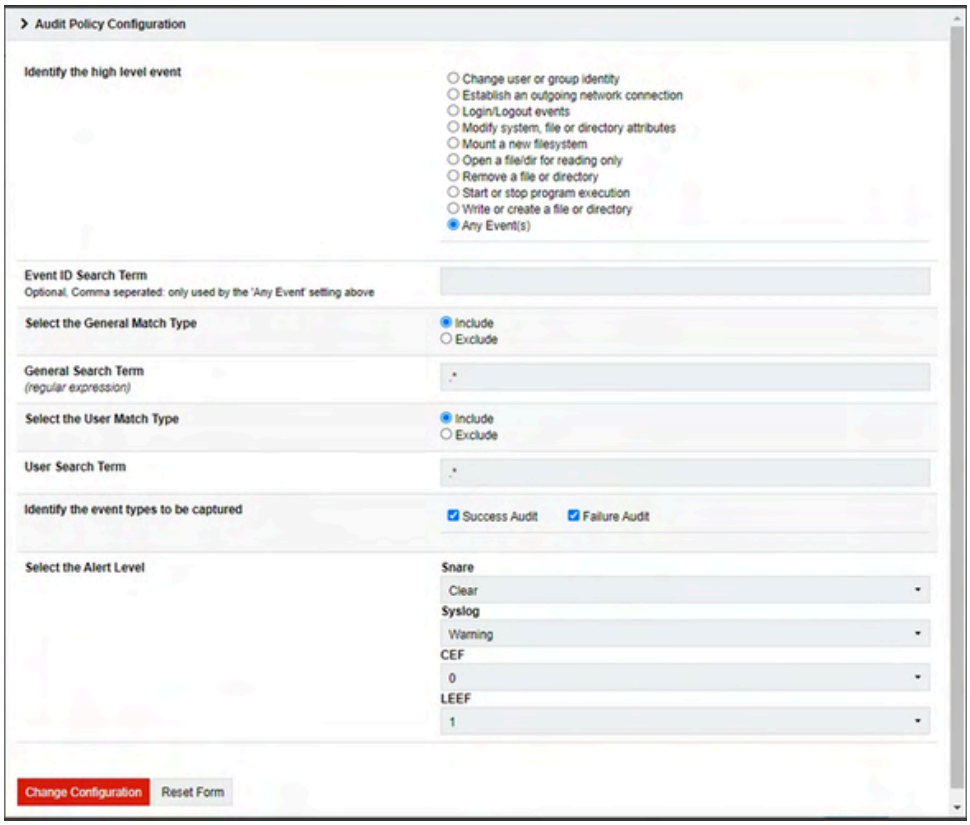
The basic process to configure an objective to capture file auditing events is as follows:

- Allow SNARE to automatically set audit configuration on the destination configuration screen. If this is not set in the agent then all of the objective settings will need to be set manually or via manual updates to the audit.rules configuration file. Using this setting enables the file system auditing to be controlled by the Snare objective settings. In order for Solaris or macOS to collect file and directory access logs, not only must the correct audit category be selected, but also the correct audit rules auditing parameters must also be set. Setting this field will automatically set these parameters, based on the objectives which have been set. It is highly recommended that this checkbox be selected.
- Open the objective screen and select “Add” for a new objective button
- Select the any event radio button
- Enter the event id to be monitored ie the following example will monitor all file opens, changes and writes to the file:
- open_rc,open_rt,open_rtc,open_rw,open_rwc,open_rwt,open_rwtc,creat,mkdir,mknod,link,symlink
- In the Search Term field enter the file(s) to be monitored. ie ^/etc/(passwd|shadow)$
- Adjust the user Search Term to match or exclude users as desired.

- Select the type of event to be collected being success or failure or both.
- If applicable set the alert level of the event so it can be tracked in Snare Central Server if events are being tracked in this way. Some events may be more critical than others so this feature allows events to be grouped in ways to make its more applicable for reporting.
- Once complete press the “Change Configuration” button and apply the latest audit configuration to restart the agent.

In the v4 Snare Enterprise Solaris agent the screen is as follows:

The v5 macOS agent has the following configuration settings.

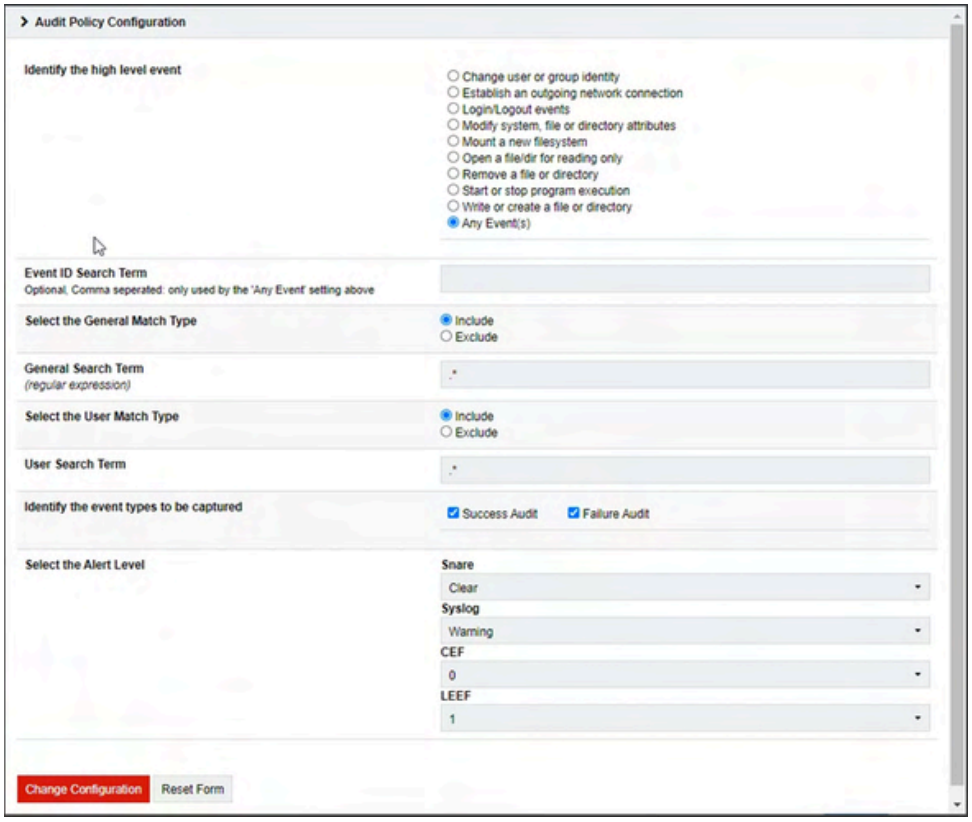


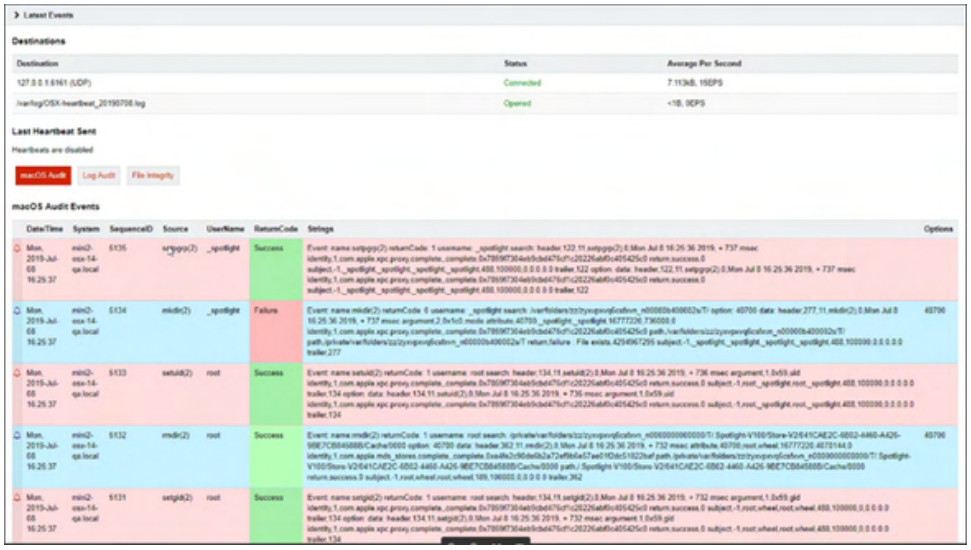
Once the all the settings are set as desired then press the Change Configuration button to save the objective. Repeat this approach for all desired files or directories that require file watch auditing enabled. Once all the objectives have been made then select “Apply the latest audit configuration” button and restart the agent. The events will show up in the latest events screen using the standard Linux events. The events can be any of the following:

- Access a file or directory.
- These can be combined with other system calls for open_rc,open_rt,open_rtc,open_w,open_wc,open_wt,open_wtc,open_rw,open_rwc,open_rwt, open_rwtc,creat,mkdir,mknod,xmknod,link,symlink,rmdir,unlink,rename,truncate,ftruncatet

There are various standards that call for the usage of FIM such as PCI DSS. The technology compliments the FAM features with looking at some details of the file and directory changes performed on the systems. However the events will show the results of the change and not who made the change. The who activity monitoring comes as part of the FAM monitoring as detailed above. The FIM features use a checksum approach along with file system details to determine changes made to files. The V5 Snare Enterprise agents can perform these file system checks based on a schedule of the customers choosing. In general these change detection process would be run either daily or weekly depending on the granularity required. These system checks can be system intensive as the agent has to perform a lot of disk IO to read all the files and then perform the checksum (SHA512) operations so they would generally be performed out of hours or when the system has low user activity. The basic process to configure FIM for the Snare Enterprise Linux agent is as follows.

- Select the File Integrity Monitoring menu item on the left
- Select the Add button
- Select the schedule the FIM checks will be performed
- Select the critically levels of these events
- Enter the file or Directory path. A file will be the absolute path to that file to be monitored. For a directory its the path to that location. If you require a recursive search from that location then enter /* at the end as per the agent instructions. Note that this forward slash on unix based sytems.
- Enter the inclusion format ie * to just select .all files, Others such as *.config can be used for just config files in a location.
- If there are files that you need to exclude then enter them in the exclusion section.
- Save the agent settings by selecting the Change Configuration button and then run the Apply Configuration to restart the agent
- The events will now show up in the latest events in the FIM section when the schedule kicks in showing the type of the event being New File, Change or Delete operations.
- As of 5.9.0 the agent UI for macOS looks like the following:

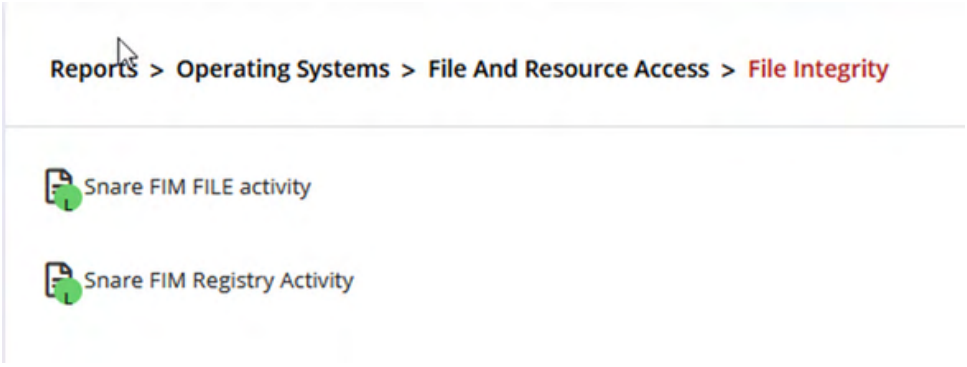

Audit Policy Configuration
Identify the high level event
Change user or group identity
Establish an outgoing network connection
Login/Logout events
Modify system, file or directory attributes
Mount a new filesystem
Open a file/dir for reading only
Remove a file or directory
Start or stop program execution
Write or create a file or directory
Any Event(s)
Event ID Search Term
Optional, Comma seperated: only used by the 'Any Event' setting above
Select the General Match Type
Include
Exclude
General Search Term
(regular expression)
.*
Select the User Match Type
Include
Exclude
User Search Term
.*
Identify the event types to be captured
Success Audit
Failure Audit
Select the Alert Level
Snare
Clear
Syslog
Warning
CEF
0
LEEF
1
Change Configuration
Reset Form

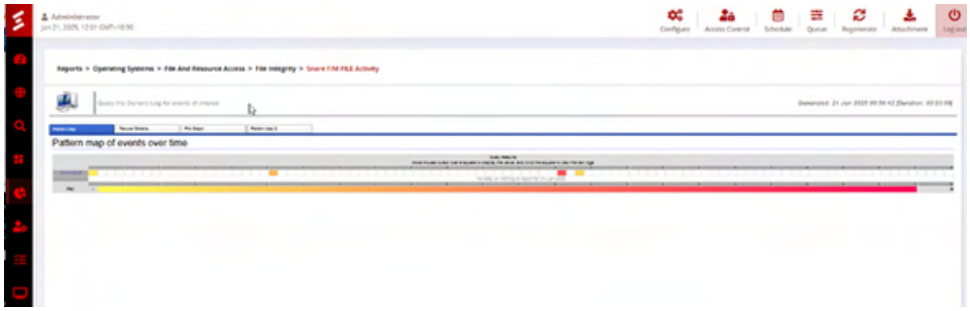

Latest Events
Destinations
Destination
Status
Average Per Second
Last Heartbeat Sent
Heartbeats are disabled
macOS Audit
Log Audit
File Integrity
macOS Audit Events
Date/Time
System
SequenceID
Source
UserName
ReturnCode
Strings
Options

Reporting on FIM, FAM, RIM and RAM Log Activity

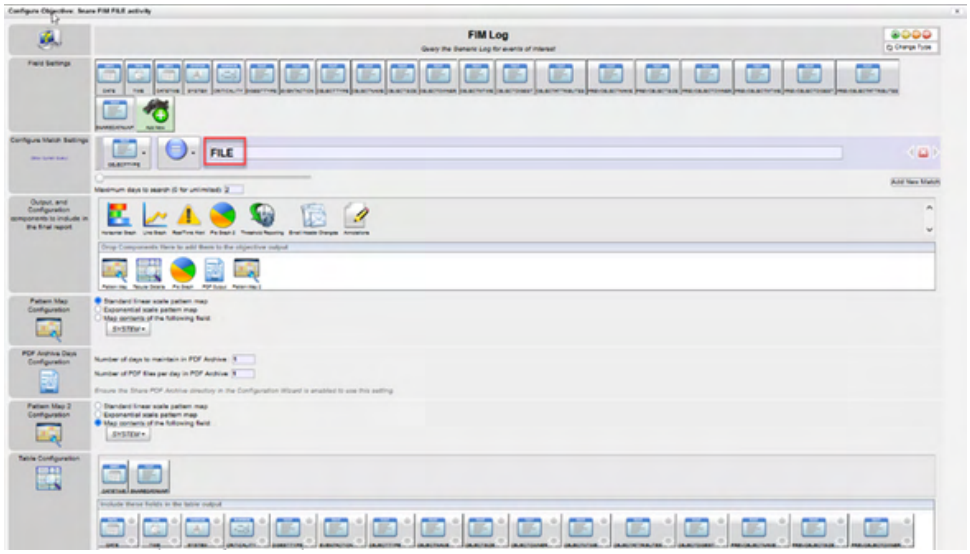
Snare has two systems that can help with reporting on FIM, FAM, RIM and RAM log activity.

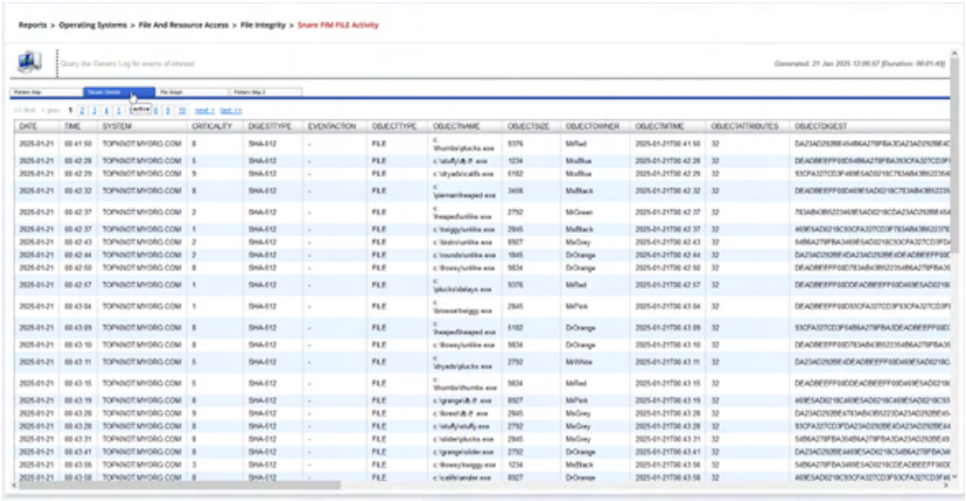
- Snare Central Server - Out of the box Snare Central contains objective for various platforms including Windows, Linux, and Solaris objective reports that can show the activity occurring on the systems. These reports can be run interactively or scheduled to run overnight to report on specific time periods.
- there are 2 types of reports one for FILE and one for REGISTRY. These report templates can be cloned and customised as needed to report on other file and registry types.



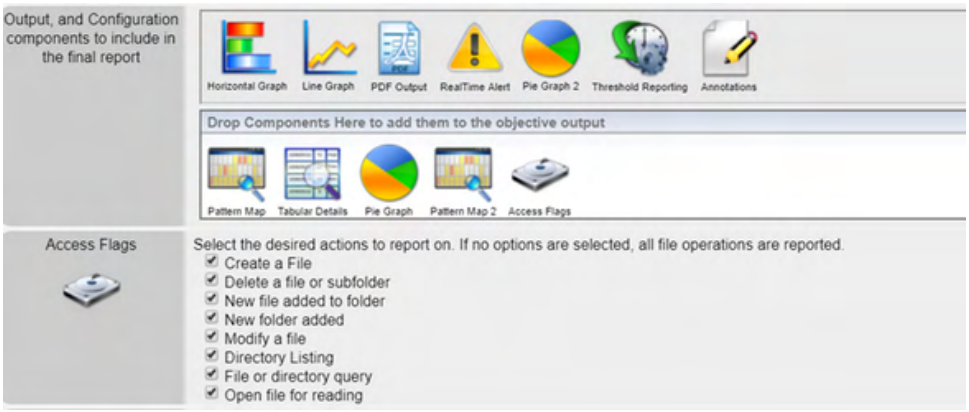


File Integrity Monitoring reports cover the following data types in the report.





File Activity Monitoring are system events generated from the operating system audit functions. The screen shots below show information related to the report output and configuration of these setting



- The integrated Snare Advanced Analytics dashboard screen shots are below. Data can be viewed in a variety of ways and customized dashboards created to link and correlate data on a single page to suit the needs of the user.