FIM (File Integrity Monitoring)

FIM (File Integrity Monitoring)

Introduction

File integrity monitoring (FIM) allows you to find out whether critical and important files, such as configuration files, have been modified at any time in a system.

Pandora FMS incorporates these monitoring features in Endpoints starting from version 784, for both Linux® and MS Windows® systems.

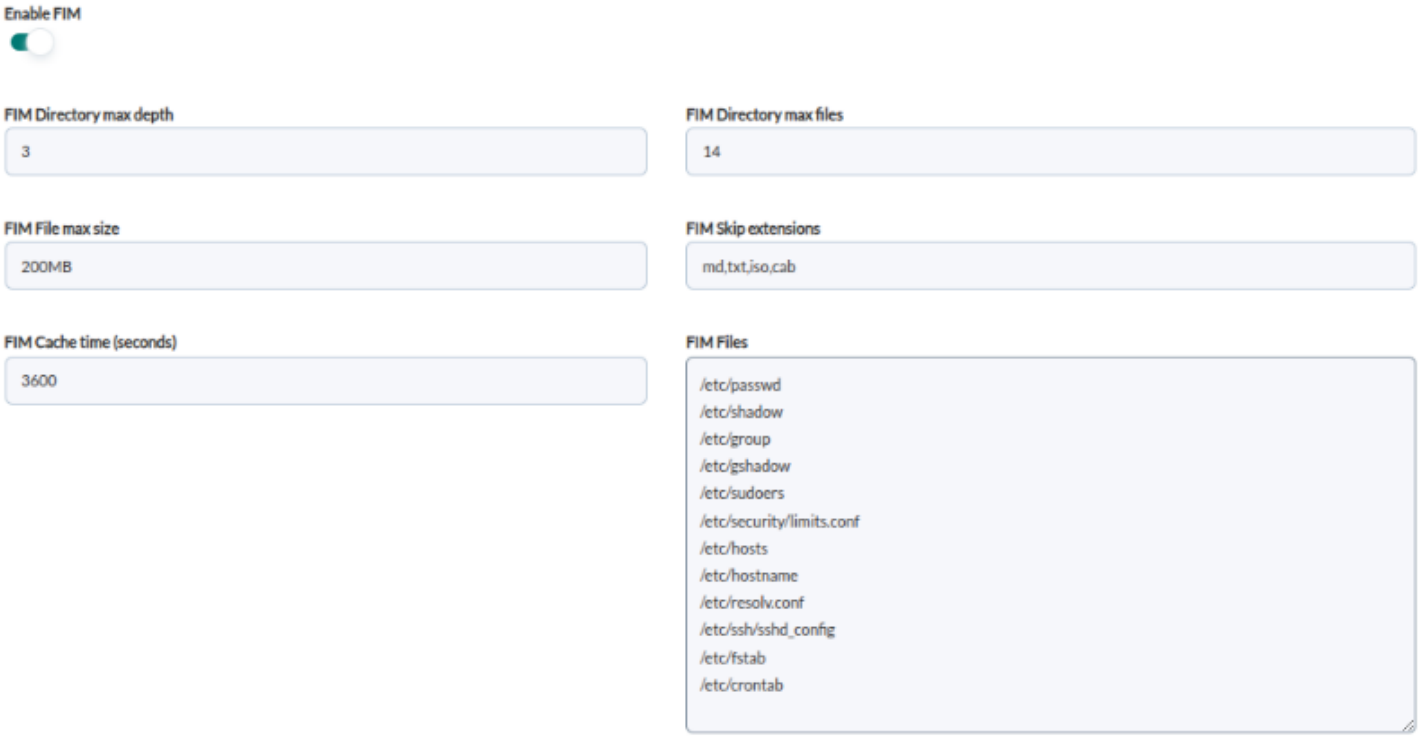
Configuration on an agent

In the security settings tab of an agent, you may enable or disable FIM monitoring:

Management → Resources → Manage agents → Edit → Security → Enable FIM

Enabling this monitoring allows you to specify the paths to files and directories that will be checked at each EndPoint interval.

Within the configuration box (FIM files), the path to a file or directory must be specified on each line. Each operating system has default values that may be edited, deleted, or added, if necessary (see also policy configuration).



For all the paths indicated, a cache time in seconds will be stored, FIM Cache time (seconds), to determine whether any files were deleted. In other words, if a file goes longer than the specified number of seconds without being detected by the system, it will be considered deleted.

In the case of paths to directories, you may also specify certain parameters for detecting changes in the files they contain:

- You may specify the maximum depth (number of subdirectories) within the directory to search for files.
- You may also specify the maximum number of files to monitor in each directory, the maximum size of the files within it, and the file extensions you wish to ignore.

To indicate the maximum file size (FIM File max size), enter the value and unit. To indicate the list of extensions to ignore (FIM Skip extensions), separate them by commas.

Monitoring policy settings

The same configuration that may be made on an individual agent may be applied through monitoring policies.

When FIM monitoring is applied from a policy, it will not be possible to modify this configuration directly in agents.

When editing a policy, there will be a tab to enable this option:

Management → Configuration → Manage policies menu, click on the name of the policy to edit, File Integrity Monitoring → Apply FIM from this policy tab.

In addition to this option, you will also need to continue to indicate whether FIM is enabled or disabled for policy agents (option Enable FIM). If this is not enabled, the FIM policy configuration will not take place.

These last two options work together to enable disabling FIM monitoring on a set of agents from the policy itself. In such a case, Apply FIM from this policy should be enabled and Enable FIM should be disabled.

For EndPoints installed on MS Windows® operating systems, they must be replaced with the following files in the FIM files section:

```
%SystemRoot%\System32\config\SAM
%SystemRoot%\System32\config\SYSTEM
%SystemRoot%\System32\config\SECURITY
%SystemRoot%\System32\config\SOFTWARE
%SystemRoot%\System32\config\DEFAULT
%SystemRoot%\System32\winlogon.exe
%SystemRoot%\System32\lsass.exe
%SystemRoot%\System32\services.exe
%SystemRoot%\System32\smss.exe
%SystemRoot%\System32\svchost.exe
%SystemRoot%\System32\csrss.exe
%SystemRoot%\System32\winload.exe
%SystemRoot%\System32\ntoskrnl.exe
%SystemRoot%\System32\drivers\etc\hosts
%SystemRoot%\explorer.exe
%SystemRoot%\System32\cmd.exe
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\System32\wscript.exe
%SystemRoot%\System32\cscript.exe
%SystemRoot%\System32\taskmgr.exe
%SystemRoot%\SysWOW64\kernel32.dll
%SystemRoot%\SysWOW64\user32.dll
%SystemRoot%\SysWOW64\advapi32.dll
%SystemRoot%\SysWOW64\gdi32.dll
%SystemRoot%\SysWOW64\ntdll.dll
%SystemRoot%\SysWOW64\ole32.dll
%SystemRoot%\SysWOW64\shell32.dll
%SystemRoot%\SysWOW64\ws2_32.dll
%SystemRoot%\SysWOW64\cmd.exe
%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```

```
%SystemRoot%\SysWOW64\wscript.exe
%SystemRoot%\SysWOW64\regsvr32.exe
%SystemRoot%\SysWOW64\mshta.exe
```

Otherwise, the configuration is exactly the same as that applied directly to an agent.

FIM monitoring results

FIM monitoring generates the following modules in each agent that has it enabled:

- `FIM_status`: Monitors whether file integrity is maintained for the agent.
- `FIM_status_last_change`: Date of the last change in FIM monitoring status.
- `FIM_changed`: Monitor the number of changed files.
- `FIM_deleted`: Monitor the number of deleted files.
- `FIM_new`: Monitor the number of new files found.

In addition, for each new, changed, or deleted file, log entries will be generated that may be viewed if log collection is enabled.

Integration with SIEM

FIM monitoring is also integrated with SIEM monitoring, as Pandora FMS incorporates decoders and rules for generating SIEM events by default (based on the log entries generated for log collection).

Back to Pandora FMS documentation index