# FIM (File Integrity Monitoring)

# FIM (File Integrity Monitoring)

## Introduction

La supervision de l'intégrité des fichiers (FIM) permet de savoir si des fichiers critiques et importants, tels que les fichiers de configuration, ont été modifiés à un moment donné dans un système.

Pandora FMS intègre cette fonctionnalité de supervision dans les Endpoints à partir de la version 784, tant pour les systèmes Linux® que pour les systèmes MS Windows®.

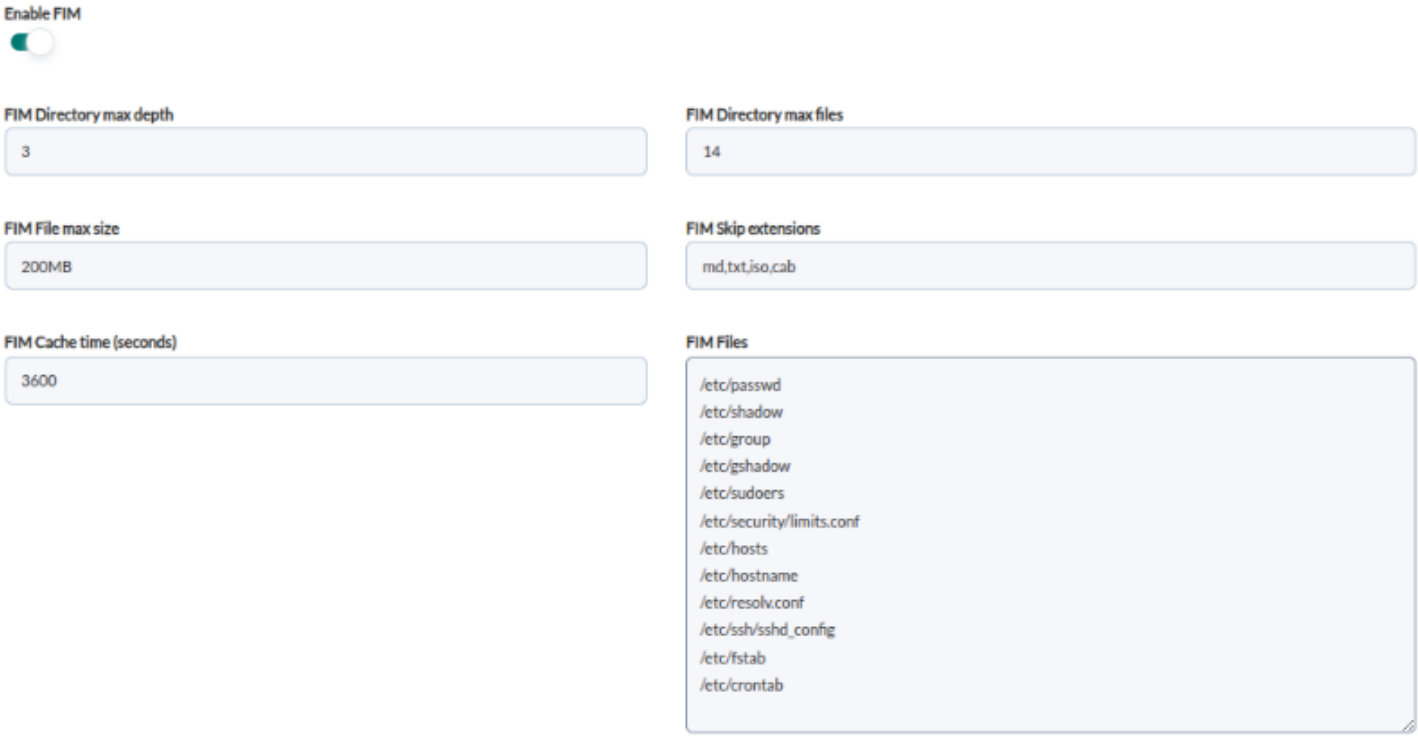
## Configuration dans un agent

Dans l'onglet Configuration de la sécurité d'un agent, vous pouvez activer ou désactiver la supervision FIM:

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

En activant cette supervision, vous pouvez indiquer les chemins d'accès aux fichiers et répertoires qui seront vérifiés à chaque intervalle de l'EndPoint.

Dans la boîte de configuration (FIM files), vous devez indiquer dans chaque ligne le chemin d'accès à un fichier ou à un répertoire. Selon chaque système d'exploitation, il existe des valeurs par défaut qui peuvent être modifiées, supprimées ou ajoutées, si nécessaire (voir également la configuration des politiques).




Pour tous les chemins indiqués, un cache temporel en secondes, FIM Cache time (seconds), sera enregistré afin de déterminer si un fichier a été supprimé. En d'autres termes, si un fichier dépasse le nombre de secondes indiqué sans être détecté par le système, il sera considéré comme supprimé.

Dans le cas des chemins d'accès aux répertoires, il est également possible d'indiquer certains paramètres pour la détection des modifications dans les fichiers qu'ils contiennent:

- Il est possible d'indiquer la profondeur maximale (nombre de sous-répertoires) dans le répertoire pour rechercher des fichiers.
- Il est également possible d'indiquer le nombre maximal de fichiers à superviser dans chaque répertoire, la taille maximale des fichiers qu'il contient et les extensions de fichiers à ignorer.

Pour indiquer la taille maximale des fichiers (FIM File max size), il faut saisir la valeur et l'unité. Pour indiquer la liste des extensions à ignorer (FIM Skip extensions), il faut les séparer par des virgules.

### Fichiers à inclure dans la recherche FIM

Une liste de fichiers ou de répertoires à superviser de près est spécifiée ici afin de détecter les nouveaux fichiers dans ce répertoire, les fichiers qui disparaissent ou qui sont modifiés. Le paramètre de profondeur maximale et le paramètre de nombre maximal de fichiers à traiter dans un répertoire sont conçus pour que, si vous entrez un répertoire très générique, par exemple `c:\Windows\System32`, l'agent ne consomme pas trop de ressources système. Vous pouvez les

paramétrer selon vos besoins et également personnaliser la liste des répertoires et des fichiers à analyser.

Il existe également un moyen d'exclure certains répertoires et/ou fichiers de la recherche, par exemple:

```
exclude /opt/myapp/*.tmp
```

Ou simplement laisser des commentaires en plaçant un chiffre au début de chaque ligne, de cette manière ils ne seront pas pris en compte et pourront être activés en cas de besoin:

```
#exclude /opt/myapp/*.tmp
```

Les répertoires dynamiques (avec des *caractères génériques* tels que l'astérisque) peuvent être inclus dans la recherche de la manière suivante:

```
C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
```

## Configuration des politiques de supervision

La même configuration qui peut être effectuée sur un agent individuel peut être appliquée via des politiques de supervision.

Lorsque la supervision FIM est appliquée à partir d'une politique, il n'est pas possible de modifier cette configuration directement dans les agents.

Lors de la modification d'une politique, un onglet permettra d'activer cette option:

Menu Management → Configuration → Manage policies, cliquez sur le nom de la politique à modifier, onglet File Integrity Monitoring → Apply FIM from this policy.

En plus de cette option, il faudra également continuer à indiquer si FIM est activé ou non pour les agents de la politique (option Enable FIM). Si cette option n'est pas activée, la configuration FIM de la politique ne sera pas appliquée.

Ces deux dernières options fonctionnent conjointement pour permettre de désactiver la supervision FIM sur un ensemble d'agents à partir de la politique elle-même. Dans un tel cas, Apply FIM from this policy doit être activé et Enable FIM doit être désactivé.

Dans le cas des EndPoints installés sur des systèmes d'exploitation MS Windows®, ils devront être remplacés par les fichiers suivants dans la section FIM files:

```
%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
```

Pour le reste, la configuration est exactement la même que celle appliquée directement sur un agent.

## Résultat de la supervisionFIM

La supervision FIM génère les modules suivants dans chaque agent qui l'a activée:

- `FIM_status`: Supervise si l'intégrité des fichiers est maintenue ou non pour l'agent.
- `FIM_status_last_change`: Date du dernier changement d'état du suivi FIM.
- `FIM_changed`: Supervisez le nombre de fichiers modifiés.

- `FIM_deleted`: Supervisez le nombre de fichiers supprimés.
- `FIM_new`: Supervisez le nombre de nouveaux fichiers trouvés.

De plus, pour chaque fichier nouveau, modifié ou supprimé, des entrées *log* seront générées et pourront être visualisées si la collecte des logs est activée.

## Intégration avec SIEM

La supervision FIM s'intègre également à la supervision SIEM, car Pandora FMS intègre par défaut les *decoders* et les *rules* pour la génération d'événements SIEM (sur la base des entrées de journal générées pour la collecte des journaux).

Retour à l'index de la documentation de Pandora FMS