ANYWHERE File Integrity Monitoring

Armor Knowledge Base

Topics Discussed

To fully use this screen, you must add the following permission to your account:

- Read FIM

Enable Trend Sub-Agent

As a prerequisite to installing File Integrity Monitoring, you must install the Trend sub-agent. Use the following commands to manage the Trend sub-agent.

Recommendation Scans

One of the features available in Agent 3.0 is Recommendation scans. Recommendation scans provide a good starting point for establishing a list of rules that you should implement. During a recommendation scan, the Armor Agent scans the operating system for installed applications, the Windows registry, open ports, and more. To take advantage of Recommendation scans, turn on Ongoing Recommendation scans in the Toolbox.

Recommendation Scans work in tandem with the Auto-Apply configuration for FIM. The results of the Recommendation Scan can only be applied when Auto-Apply for the FIM service is turned on.

Install Trend Sub-Agent:

```
Windows: C:\.armor\opt\armor.exe trend install
Linux: /opt/armor/armor trend install
```

Uninstall Trend Sub-Agent:

```
Windows: C:\.armor\opt\armor.exe trend uninstall
Linux: /opt/armor/armor trend uninstall
```

Trend Sub-Agent Status:

```
Windows: C:\.armor\opt\armor.exe trend status
Linux: /opt/armor/armor trend status
```

Turn On Recommended Scans:

```
Windows: C:\.armor\opt\armor.exe trend ongoing-recommendation-scan on
Linux: /opt/armor/armor trend ongoing-recommendation-scan on
```

Turn Off Recommended Scans:

```
Windows: C:\.armor\opt\armor.exe trend ongoing-recommendation-scan off
Linux: /opt/armor/armor trend ongoing-recommendation-scan off
```

Schedule a Recommended Scan (Runs on Next Trend Sub-Agent Heartbeat):

```
Windows: C:\.armor\opt\armor.exe trend recommendation-scan
Linux: /opt/armor/armor trend recommendation-scan
```

Set Recommendation Scan Interval:

```
Windows: C:\.armor\opt\armor.exe trend set-recommendation-scan-interval <interval>
Linux: /opt/armor/armor set-recommendation-scan-interval <interval>
```

Options are "24 Hours" "2 Days" "3 Days" "7 Days" "2 Weeks" "3 Weeks" "4 Weeks"

Get Recommendation Scan Interval:

```
Windows: C:\.armor\opt\armor.exe trend get-recommendation-scan-interval
Linux: /opt/armor/armor trend get-recommendation-scan-interval
```

Trend Sub-Agent Help

```
Windows: C:\.armor\opt\armor.exe trend help
Linux: /opt/armor/armor trend help
```

Restart Trend:

```
Windows: C:\.armor\opt\armor.exe trend service-restart
Linux: /opt/armor/armor trend service-restart
```

Enable File Integrity Monitoring Service

Use the following commands to manage the File Integrity Monitoring service.

Turn On File Integrity Monitoring:

```
Windows: C:\.armor\opt\armor.exe fim on
Linux: /opt/armor/armor fim on

Optional Parameters
Windows: C:\.armor\opt\armor.exe fim on auto-apply-recommendations=on
Linux: /opt/armor/armor fim on auto-apply-recommendations=on

Windows: C:\.armor\opt\armor.exe fim on auto-apply-recommendations=off
Linux: /opt/armor/armor fim on auto-apply-recommendations=off
```

The Auto-Apply configuration for FIM works in tandem with Recommendation Scans. Only after a Recommendation Scan is run will there be policies to Auto-Apply.

Turn Off File Integrity Monitoring:

```
Windows: C:\.armor\opt\armor.exe fim off
Linux: /opt/armor/armor fim off
```

List of Assigned FIM Rules on Policy:

```
Windows: C:\.armor\opt\armor.exe fim list-assigned-rules
Linux: /opt/armor/armor fim list-assigned-rules
```

Assign FIM Rules:

```
Windows: C:\.armor\opt\armor.exe fim assign-rules ID
Linux: /opt/armor/armor fim assign-rules ID
```

Un-Assign FIM Rule:

```
Windows: C:\.armor\opt\armor.exe fim unassign-rule ID
Linux: /opt/armor/armor fim unassign-rule ID
```

File Integrity Monitoring Help

```
Windows: C:\.armor\opt\armor.exe fim help
Linux: /opt/armor/armor fim help
```

Add Custom Filepath Rule

```
Windows: C:\.armor\opt\armor.exe fim add-custom-filepath-rule "<name>,<filepath>,<description>"
Linux: /opt/armor/armor fim add-custom-filepath-rule "<name>,<filepath>,<description>"
```

Update Custom Filepath Rule

```
Windows: C:\.armor\opt\armor.exe fim update-custom-filepath-rule "<id>,<name>,<filepath>,<description>"
Linux: /opt/armor/armor fim update-custom-filepath-rule "<id>,<name>,<filepath>,<description>"
```

Delete Custom Filepath Rule

```
Windows: C:\.armor\opt\armor.exe fim delete-custom-filepath-rule "<id>"
Linux: /opt/armor/armor fim delete-custom-filepath-rule "<id>"
```

Get Custom Filepath Rule

```
Windows: C:\.armor\opt\armor.exe fim get-custom-filepath-rule "<id>"
Linux: /opt/armor/armor fim get-custom-filepath-rule "<id>"
```

View FIM Data

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **File Integrity Monitoring**.

Column	Description
Name	For Armor Complete, the name of the virtual machine you created in AMP. For Armor Anywhere, the name of the instance that contains the installed Anywhere agent, which includes the FIM sub-agent.
Provider	For Armor Complete, the entry will display **Armor**. For Armor Anywhere, the name of the public cloud provider for the instance.
Status	The health status of the sub-agent, which is based on how long the FIM sub-agent has been offline. There are three status types: • Secured (in green) • Warning (in yellow) • Critical (in red)
Connectivity	The connection status of the sub-agent. There are three connection types: • **Online** indicates that the sub-agent is online. • **Offline** indicates that the sub-agent is currently offline. • **Needs Attention** indicates that the sub-agent has not communicated with Armor.
Timestamp	The date and time that the FIM sub-agent last communicated with Armor.

To learn how the overall FIM status is determined, see Understand FIM data.

Understand FIM Data

In the **File Integrity Monitoring** screen, the dashboard displays the various FIM statuses of your virtual machines (or hosts):

- **Green** indicates a virtual machine in a **Secured** FIM status.
- **Yellow** indicates a virtual machine in a **Warning** FIM status.
- **Red** indicates a virtual machine in a **Critical** FIM status.

Armor determines the status of **FIM** based on how long **FIM** has been offline.

- If **FIM** is offline for 2 to 7 days, then the **FIM** status changes from **Secured** to **Warning**.

- If **FIM** is offline for 8 days or more, then the **FIM** status changes from **Warning** to **Critical**.

Length of offline status	Security Status
2 to 7 days	Warning
8 days or more	Critical

The overall status of your virtual machine is based on the individual status of your virtual machine's subcomponents, including **FIM**.

View Detailed FIM Data

The **File Integrity Monitoring** details screen displays the changes that has been detected in certain files in your virtual machine. This screen only shows data for the last 90 days.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **File Integrity Monitoring**.
3. Locate and select the desired virtual machine.

Column	Description
Filename	The name of the file where a change was detected.
Description	A short summary of the change that took place.
Change Type	The type of change that took place in the file.
Scan Date	The date when the change was detected.

Export FIM Data

To export the data:

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **File Integrity Monitoring.**
3. (Optional) Use the filter function to customize the data displayed.
4. Below the table, click **CSV**. You have the option to export all the data (**All**) or only the data that appears on the current screen (**Current Set**).

Function	Data Displayed	Notes
CSV	VM Name, VM Provider, IP Address, OS, FIM Agent Status Fixed, FIM Agent Version, FIM Last Communication Date	A blank entry indicates that the action has never taken place.

Troubleshooting

Armor troubleshoots servers that contain **File Integrity Monitoring** sub-components in a **Warning** or **Critical** status. To troubleshoot with Armor, you must submit a support ticket.

1. In the Armor Management Portal (AMP), click **Support,** and then click **Tickets**.
2. Click **Create a Ticket**.
3. Select or search for the desired category for your ticket request type.
4. Complete the missing fields.
    a. In **Description**, enter useful details that can help Armor quickly troubleshoot the problem.
5. Click **Create**.
6. To view the status of your ticket, in the left-side navigation, click **Support**, and then click **Tickets**.

Log Search for File Integrity Monitoring

Users can search for FIM events in Log Search. For instructions on how to access and use Log Search, please see our documentation here.

An example of FIM logs can be seen below:

t	parsed.trendmicro.action	created
t	parsed.trendmicro.category	Integrity Monitor
t	parsed.trendmicro.cn1	19417
t	parsed.trendmicro.cn1_label	Host ID
t	parsed.trendmicro.description	Unix - Open Port Monitor
t	parsed.trendmicro.ds_tenant	Primary
t	parsed.trendmicro.ds_tenant_id	0
t	parsed.trendmicro.dvchost	1024__076c96be-1202-4f31-a598-27ad6812530e
t	parsed.trendmicro.file_path	udp/0.0.0.0/60709
t	parsed.trendmicro.message	When scanned the Port had the following attributes:\n\n User: postfix\n
t	parsed.trendmicro.name	Unix - Open Port Monitor
t	parsed.trendmicro.severity	8
?	parsed.trendmicro.sproc	⚠ N/A
t	parsed.trendmicro.suser	N/A

For a full list of Log Search fields and descriptions, please visit our glossary here.

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★½ 18 rates