File Integrity Monitoring (FIM)

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

- Read FIM

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 subagent.
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 subagent, which is based on how long the FIM subagent has been offline. There are three status types: • Secured (in green) • Warning (in yellow) • Critical (in red)
Connectivity	The connection status of the subagent. There are three connection types: • Offline • Online • Unknown
Timestamp	The date and time that the FIM subagent 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.

Troubleshoot FIM Data

Armor troubleshoots servers that contain **File Integrity Monitoring** subcomponents 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**.

Review API Calls

- Get File Integrity Status
- Get File Integrity Account Statistics
- Get Overview Security Status