Enable File Integrity Monitoring with AMA

To enable File Integrity Monitoring (FIM), use the FIM recommendation to select machines to monitor:

1. From Defender for Cloud's sidebar, open the **Recommendations** page.

2. Select the recommendation File integrity monitoring should be enabled on machines. Learn more about Defender for Cloud recommendations.

3. Select the machines that you want to use File Integrity Monitoring on, select **Fix**, and select **Fix X resources**.

   The recommendation fix:

   - Installs the `ChangeTracking-Windows` or `ChangeTracking-Linux` extension on the machines.
   - Generates a data collection rule (DCR) for the subscription named `Microsoft-ChangeTracking-[subscriptionId]-default-dcr` that defines what files and registries should be monitored based on default settings. The fix attaches the DCR to all machines in the subscription that have AMA installed and FIM enabled.
   - Creates a new Log Analytics workspace with the naming convention `defaultWorkspace-[subscriptionId]-fim` and with the default workspace settings.
4. You can update the DCR and Log Analytics workspace settings later.

5. From Defender for Cloud's sidebar, go to **Workload protections** > **File integrity monitoring**, and select the banner to show the results for machines with Azure Monitor Agent.

Edit the list of tracked files and registry keys

File Integrity Monitoring (FIM) for machines with Azure Monitor Agent uses Data Collection Rules (DCRs) to define the list of files and registry keys to track. Each subscription has a DCR for the machines in that subscription.

FIM creates DCRs with a default configuration of tracked files and registry keys. You can edit the DCRs to add, remove, or update the list of files and registries that are tracked by FIM.

To edit the list of tracked files and registries:

1. In File integrity monitoring, select **Data collection rules**.

   You can see each of the rules that were created for the subscriptions that you have access to.

2. Select the DCR that you want to update for a subscription.

   Each file in the list of Windows registry keys, Windows files, and Linux files contains a definition for a file or registry key, including name, path, and other options. You can also set **Enabled** to **False** to untrack the file or registry key without removing the definition.

   Learn more about system file and registry key definitions.

3. Select a file, and then add or edit the file or registry key definition.

4. Select **Add** to save the changes.