

WORKING WITH DISCONNECTED MONITORS

The **AEDA Configuration** page may contain a **Disconnected Monitors** section. This section is only displayed if a Sequence or Evaluation that is used in a Monitor has been edited and if some monitors are disconnected. The **Disconnected Monitor** section was implemented for the following reasons:

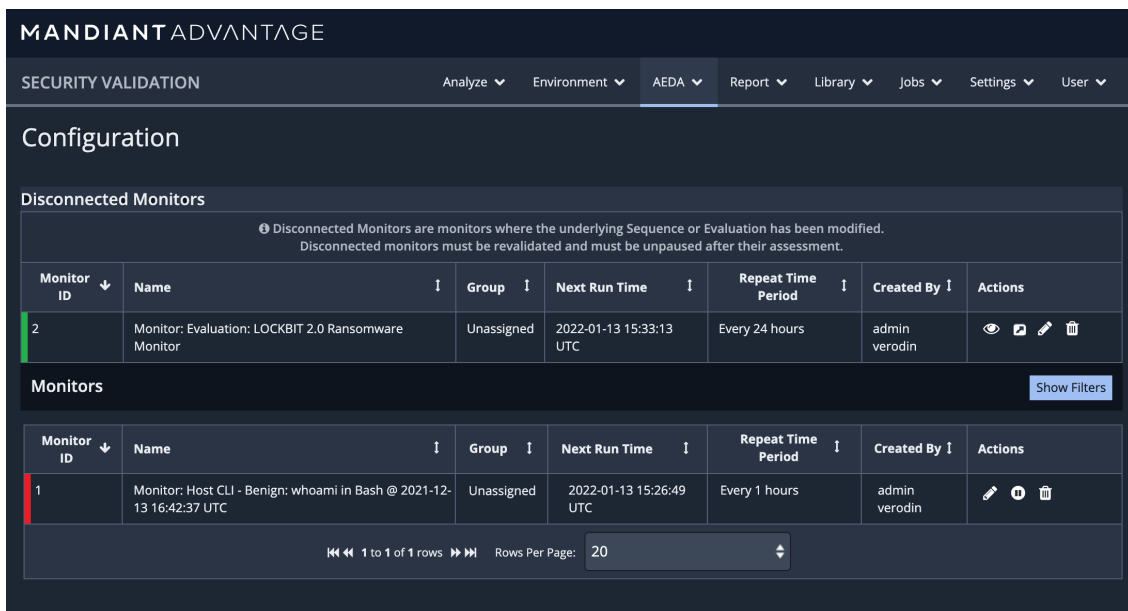
- Allows you to quickly identify Monitors that are not running due to a change to their security content
- Allows you to view the reasons why the Monitor was disconnected
- Maintains the Monitor configuration but prevents it from attempting to run, which would result in an error because it is missing information
- Allows you to review and configure the Monitor configuration to account for the change to its Sequence or Evaluation
- Allows you to acknowledge Monitor disconnections and re-enable them in a single view



All Sequences and Evaluations that include a change to the way they run (Actions added, Actions deleted, sleep Actions added or removed, Actions moved to another group, new groups created, etc.) are included in the Disconnected table.

To view the reason(s) a monitor was disconnected

1. Go to **AEDA > Configuration**.



The screenshot shows the Mandiant Advantage interface. At the top, there's a navigation bar with 'MANDIANT ADVANTAGE' and 'SECURITY VALIDATION'. Below that, there are dropdown menus for 'Analyze', 'Environment', 'AEDA', 'Report', 'Library', 'Jobs', 'Settings', and 'User'. The main content area is titled 'Configuration' and contains two sections: 'Disconnected Monitors' and 'Monitors'.

Disconnected Monitors section:

ⓘ Disconnected Monitors are monitors where the underlying Sequence or Evaluation has been modified. Disconnected monitors must be revalidated and must be unpaused after their assessment.


Monitor ID	Name	Group	Next Run Time	Repeat Time Period	Created By	Actions
2	Monitor: Evaluation: LOCKBIT 2.0 Ransomware Monitor	Unassigned	2022-01-13 15:33:13 UTC	Every 24 hours	admin verodin	View, Edit, Delete

Monitors section:

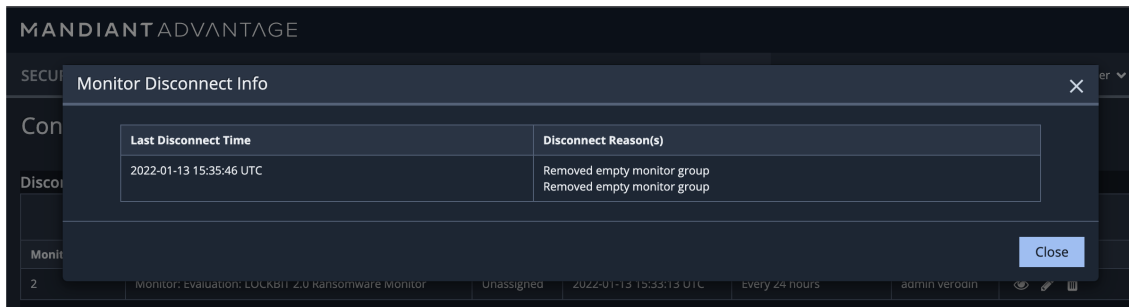
Monitor ID	Name	Group	Next Run Time	Repeat Time Period	Created By	Actions
1	Monitor: Host CLI - Benign: whoami in Bash @ 2021-12-13 16:42:37 UTC	Unassigned	2022-01-13 15:26:49 UTC	Every 1 hours	admin verodin	View, Edit, Delete

At the bottom of the Monitors table, there is a pagination control showing '1 to 1 of 1 rows' and 'Rows Per Page: 20'.

Monitor Configuration page

2. In the **Disconnected Monitors** section, locate the Monitor that you want to view the reason(s) for the disconnected status and click **View**  in the **Actions** column.



The **Monitor Disconnect Info** popup window displays, showing the last time the Monitor was disconnected and the reason(s) for the disconnect.



Reason(s) for Disconnected Monitor

3. Click **Close**.

To review and enable a disconnected Monitor

1. Go to **AEDA > Configuration**.
2. In the **Disconnected Monitors** section, click **Edit**  for the Monitor you need to review. The standard Monitor Configuration form displays.
3. Review and update the Monitor Configuration. A few methods you could use include:
 - Review each step of the Monitor and make any necessary changes.
 - Jump to the first Action of the group that contains the change you made and review each Action and update as necessary.
 - Jump directly to the Action that was added and update as necessary.
 - Only update the **Next Runtime** field.
4. Click **Update Monitor**. Unless there is an issue with the Monitor Configuration, your changes will save and the configuration will move to the Monitors section.
5. Click **Restart**  to start the Monitor.