




## MANAGING NOTIFICATIONS

A Notification Profile is how you link Monitors or Monitor Groups to a specific Notification Format and how you define the notification interval. A Notification Profile is also required to receive automatic notifications if a Job for a Monitor errors.



Profile ID	Name	Type	Actions
4	My Test Profile	Monitor State Change	 

(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b81445d5e3e714b3ae8/n/notification-profile.png>)

Notification Profiles

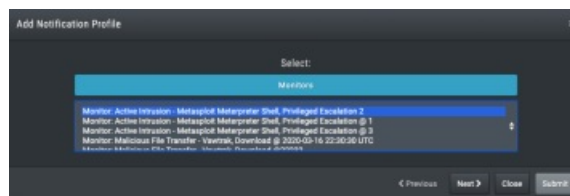
The timing of when notifications are sent is determined by how you've configured the **Expected Detected** setting for Actions in the Monitor. This allows all pertinent details about the Job to be included in the notification that is sent.

	When is the Notification sent?	
Expected Detected Value	When the Job completes	After the Monitor Event detection period has expired
Yes		True
No		True
Does not Matter	True	

For more information about the Monitor Event detection period, review the information for the **Timeout for Monitor Event Detection** field under **Advanced Settings** (<https://docs.mandiant.com/home/msv-advanced-settings>). For more information about the Monitor Event wait period, review the information for the **Timeout for Monitor Event Detection** field under **Advanced Settings** (<https://docs.mandiant.com/home/msv-advanced-settings>).

### TO ADD A NEW NOTIFICATION PROFILE

- Go to **AEDA > Notification Settings**.
- Click **Add Notification Profile**.  
The Add Notification Profile dialog appears. You can select Monitors or Monitor Groups in this dialog.
- Click **Monitor** or **Monitor Group**, as shown below, depending on which you want to add to this profile.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b67445d5e3e714b3a40/n/aeda-add-notif-profile.png>)

Create Notification Profile - Add Monitors

- Select one or more Monitors or Monitor Groups, and click **Next**.  
You can use **Ctrl+click** (Microsoft® Windows®) or **Cmd+click** (Apple® Macintosh®) to make multiple selections.



**NOTE:** If you edit a Monitor Group in the Configuration page, changes to the Monitor Group are also saved to the Notification Profile.

5. Select one or more **Notification Formats** to use.
6. Fill in the necessary information for the Notification Format, and click **Next**.
  - a. For email-based formats, configure who will receive the notification:
    - Enter email addresses (separated by commas or semi-colons)
    - Select specific Users
    - Select User Groups to send the notification to all users within that group
  - b. For syslog-based formats, configure the system information:
    - Server IP or Hostname
    - Server Port
  - c. Select whether the message will send over TCP or UDP.



**NOTE:** UDP is selected by default. Syslog messages sent over UDP will appear truncated if they are larger than 1024 bytes.

7. Enter a **Name** for the Notification Profile.
8. Select a **Notify When** value:
  - **Monitor State Changes:** Notifications occur when the Monitor's Job result changes (e.g., Pass to Fail).
  - **Monitor Runs:** Notifications occur when the Monitor's Job runs.
  - **Monitor Fails:** Notifications occur when the Monitor's criteria is not met
  - **Monitor Completes:** Notifications occur when the Monitor's Job completes.
  - **Monitor Passes:** Notifications occur when the Monitor's criteria is met.
  - **Detections Change:** Notifications occur when the events generated deviate from the prior Job.
  - **Number of Detections Changes:** Notifications occur when the events generated (e.g., SID or other event identifier) deviate from the prior Job's events.
  - **Number of Detections Increases:** Notifications occur when the total number of events generated increase.
  - **Number of Detections Decreases:** notifications occur when the total number of events generated decrease.
  - Enter a Maximum number of notifications to send and specify within what time interval.
  - For example, Maximum: 10, Notification(s) Per: Day, will limit this profile to sending 10 notifications for the selected Monitors or Monitor Groups per day.
  - Click **Submit**.

## Video Overview

### TO EDIT A NOTIFICATION PROFILE

1. Go to **AEDA > Notification Settings**.
2. Locate the Notification Profile you want to edit.
3. Click **Edit** for the format you want to edit.



**NOTE:** You cannot edit a system Notification Profile, but you can clone the profile and edit the clone.

4. Make edits.
5. Click **Save**.

## Receiving Monitor Failure Notifications

If a Monitor fails and it has a related notification profile, a notification will automatically be sent. The notification sent is based on the format and recipients included in the notification profile.

The email notification includes a subject and body in the following format:

- Subject

```
Error running Monitor : %monitor_def_name% (ID: %monitor_def_id%)
```

- Body

```
Job #%job_id% did not complete successfully, monitor results could not be determined.
```

```
Job results can be viewed here: https://%director_ip%/jobs/%job_id%
```



**NOTE:** If the %job\_link% keyword is in the message body, the link will be either the DirectorIP address or FQDN, depending on the value listed for Your Domain in the Email Settings.

The syslog notification uses the following format:

```
Error running Monitor : %monitor_def_name% (ID: %monitor_def_id%) Job ID: %job_id%
```