WORKING WITH MONITOR NOTIFICATION FORMATS

The Notification Format defines how you want the platform to notify you when an alert is generated by Monitor Actions or when a Monitor errors.

There are three types of notification formats available:

- **Email**: Sends the notification via email and requires you to enter a valid email address to use as the message sender. This can be any email and does not have to be associated with the platform. You can define the subject and message of the notification.
- **Syslog**: By default, the syslog messages are sent over UDP. You can define the notification's syslog severity and message, but the facility is set to Syslog automatically and cannot be changed.

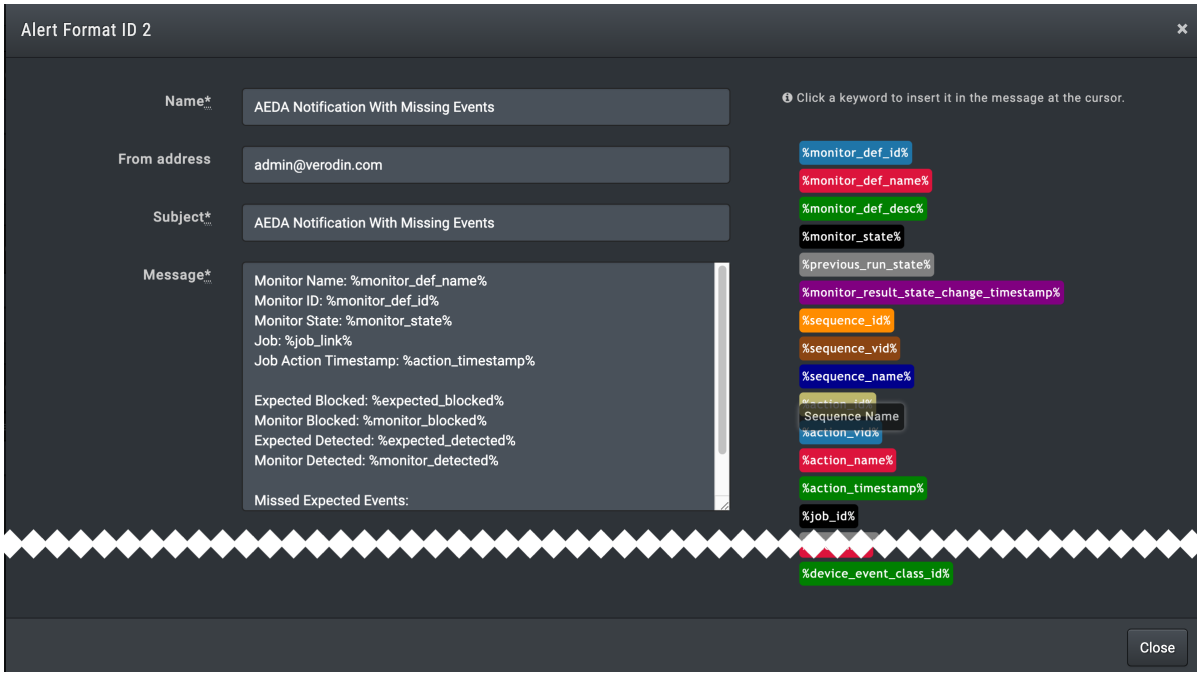
  > You must ensure that communication between the Director and destination system is permitted on the specified port or protocol.

- **Webhook**: Sends the notification as an HTTP request, so requires you to enter a valid URL. You can define the subject and message of the notification.

There are two notification formats included when you install Security Validation:

- AEDA Notification With Missing Events (email format)
- Common Event Format (syslog format)

You can clone these or use as-is.



AEDA Notification Format - Email

Monitor Notification Variables

Variables can be used to customize the subject of the email and the message field on all notification types. This table includes the variables and their meaning.

Variable	Definition	Possible Responses
monitor_def_id	Monitor ID	
monitor_def_name	Monitor Name	
monitor_def_desc	Monitor Description	
monitor_state	Did the Monitor pass or fail?	Pass/Fail
previous_run_state	Did the previous Monitor run pass or fail?	Pass/Fail
monitor_result_state_change_timestamp	Time the Monitor state changed	
sequence_id	Sequence or Evaluation ID	
sequence_vid	Sequence or Evaluation VID	
sequence_name	Sequence or Evaluation Name	
action_id	Action ID	
action_vid	Action VID	
action_name	Action Name	
action_timestamp	Time the Action was run	
job_id	Job ID	
job_link	Link to the Job	
previous_run_job_link	Link to the previously run Job	
monitor_blocked	The Monitor's Job was blocked	True/False
previous_run_blocked	The previous Monitor was blocked	True/False
expected_blocked	You expected the Monitor's Job to be blocked	Yes/No
monitor_detected	The Monitor's Job was detected	True/False
missed_expected_events	List of events, grouped by integration, that were marked as expected detected but which were not received	
missed_expected_events_with_sectech%	List of events, grouped by integration, that were marked as expected detected but which were not received, with the Security Technology listed at the end in parenthesis	

Variable	Definition	Possible Responses
expected events	List of events, grouped by integrations, that were marked as expected	
expected events_with_sectech%	List of events, grouped by integrations, that were marked as expected, with the Security Technology listed at the end in parenthesis	
previous_run_detected	The Monitor's Job was detected the previous time it ran	True/False
expected_detected	You expected the Monitor's Job to be detected	Yes/No
source_actor	Source Actor and Zone	
destination_actor	Destination Actor and Zone	
endpoint	Endpoint Actor	
source_ip	Source IP	
destination_ip	Destination IP	
job_name	Job name	
device_event_class_id	ID that indicates the results of the Monitor; see Device Event Class ID Values and Descriptions below for the list of possible values and their definitions	numeric value

Adding a New Notification Format

1. Go to **AEDA > Notification Settings**.
   The Notification Settings page appears.
2. Click **Add Notification Format**.
   The Add Notification Format dialog appears.
3. Select a **Notification Destination** and click **Next**. Enter the required fields, based on the type of notification you are creating:
   a. If you select **Email**: Enter a name, a from address, a subject, and a message. The subject and message may contain variables (keywords).

      To configure email port, encryption, and so on, go to the Email Settings page.

   b. If you select **Syslog**: Enter a name and message, and select a syslog severity. The message may contain variables (keywords).
   c. If you select **Web Hook**: Enter a **Name**, the **Webhook URL**, **Web Hook Message Type** (**Basic JSON** or **Microsoft Teams**), and **Message**. The message may contain variables (keywords).

      The Basic message type is a standard JSON string. The Microsoft Teams option is like Basic, but adds 'title' and 'text' fields where the title is always 'Mandiant Security Validation Notification' and text is a fully-escaped JSON string.

      If you want to verify the Web Hook is configured correctly, click **Send Sample**.
4. Click **Submit**. Your Notification Format is saved and ready to used in a Notification Profile.

You can assign more than one Notification Format to a Monitor using Notification Profiles.

Editing a Notification Format

All notification formats you created can be edited to change the information. However, you can not change the Notification Formats Type - that requires creating a new Notification Format.

1. Go to **AEDA > Notification Settings**.
2. Locate the Notification Format you want to edit.
3. Click **Edit** for the format you want to edit.
4. Make edits.
5. Click **Save**.

Device Event Class ID Values and Descriptions

This table provides the definition for each code that may be included in your Monitor Notification when you include the device_event_class_id field.

Value	Description
00010001	monitor_not_passed_action_errored
00010101	monitor_passed_action_errored
00010002	monitor_not_passed_action_blocked_not_detected_not_passed
00010102	monitor_passed_action_blocked_not_detected_not_passed;
00010004	monitor_not_passed_action_not_blocked_detected_not_passed
00010104	monitor_passed_action_not_blocked_detected_not_passed
00010008	monitor_not_passed_action_not_blocked_not_detected_passed
00010108:	monitor_passed_action_not_blocked_not_detected_passed
00010003	monitor_not_passed_action_errored
00010103	monitor_passed_action_errored
00010005	monitor_not_passed_action_errored
00010105	monitor_passed_action_errored
00010009	monitor_not_passed_action_errored
00010109	monitor_passed_action_errored
00010006	monitor_not_passed_action_blocked_detected_not_passed
00010106	monitor_passed_action_blocked_detected_not_passed
0001000A	monitor_not_passed_action_blocked_not_detected_passed
0001010A	monitor_passed_action_blocked_not_detected_passed

Value	Description
0001000C	monitor_not_passed_action_not_blocked_detected_passed
0001010C	monitor_passed_action_not_blocked_detected_passed
00010007	monitor_not_passed_action_errored
00010107	monitor_passed_action_errored
0001000B	monitor_not_passed_action_errored
0001010B	monitor_passed_action_errored
0001000D	monitor_not_passed_action_errored
0001010D	monitor_passed_action_errored
0001000E	monitor_not_passed_action_blocked_detected_passed
0001010E	monitor_passed_action_blocked_detected_passed
0001000F	monitor_not_passed_action_errored
0001010F	monitor_passed_action_errored