Mandiant

TROUBLESHOOT MSI INTEGRATIONS

This article outlines key steps for troubleshooting Mandiant SecOps Integrations (MSI Integrations). Start with the checklist and then move onto the more specific checks, as needed, including generating logs for support. If troubleshooting steps are specific to a Security Validation environment (Mandiant Security Validation (MSV) or Mandiant Advantage Security Validation (MA-SV)), that environment is called out.

Troubleshooting checklist

1. **Run a Health Check** (https://docs.mandiant.com/home/msv-managing-integrations#healthcheck). If it returns any errors, fix them as suggested and rerun the check to ensure the status is Healthy. See **Integration Error Messages for MSI Service** (https://docs.mandiant.com/home/msv-error-messages-integrations) for more information.
2. Validate network connectivity from the Director to the integration.
    - `curl` or `nc` to hostname or IP address:port
    - If using hostname, verify the name resolution using `nslookup`.
3. Validate Director, Actor, and Integration-specific timestamps.
    - Check the NTP settings.
    - Force timestamp sync through the Director, if needed.
4. Verify that events exist in the security technology.
    - Sign in to the security technology console and query for events from select Actors and Jobs.
        - Verify that the correct Actor IP address is part of the event and not just a hostname.
    - Verify that events have accurate timestamps and fall within the window of the Job Action.
    - For SIEM integrations, verify that events are properly parsed and populating the appropriate fields:
        - Source, destination, timestamp, source port, and destination port for Network Actions
        - Hostname and timestamp for Host CLI Actions
    - For SIEM integrations, validate the fields in the query are the correct ones for the environment/implementation (and the appropriate index is being queried).
5. Validate credentials and permissions.
    - Log in to security technology console with same credentials as integration (if possible).
    - Query for events from select Actors and Jobs, and verify that they exist.
6. Validate that the last integration query executed returns results through the test query function.
    - Manipulate query parameters as needed until appropriate results are returned and update the corresponding integration query as needed.
7. Investigate integration-specific logs for error messages and other clues. See **Generated Support Logs** (https://docs.mandiant.com/home/msv-generated-support-logs) for more information.

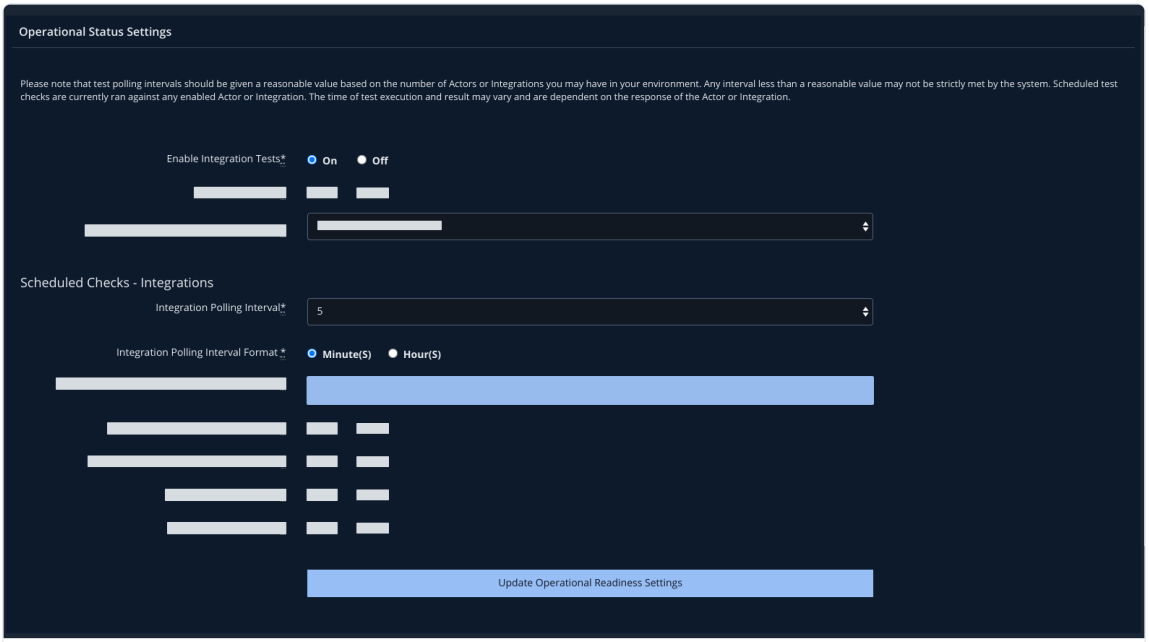
Check Operational Status

This feature verifies the overall status of the Integration on the basis of the last number of Integration query events and the Job match in a tabular form. To complete this task, perform steps in three different sections of the Director.

Enable Integration Tests and Polling Interval

1. Go to **Settings > Director Settings**.
2. Click **Operational Status** and turn on **Enable Integration Tests**.
3. Configure the following fields:
    - **Integration Polling Interval**

- **Integration Polling Interval Format**
  For example, setting them to **5** and **minute(S)**, respectively, means that the test polling interval for integrations happen every five minutes.



Operational Status Settings

> The test polling intervals should be given a reasonable value based on the number of Actors or Integrations you have in your environment. Test execution time and results may vary and depend on the response of the Actor or Integration.

4. Click **Update Operational Reading Settings** to save your changes.

Configure an Integration

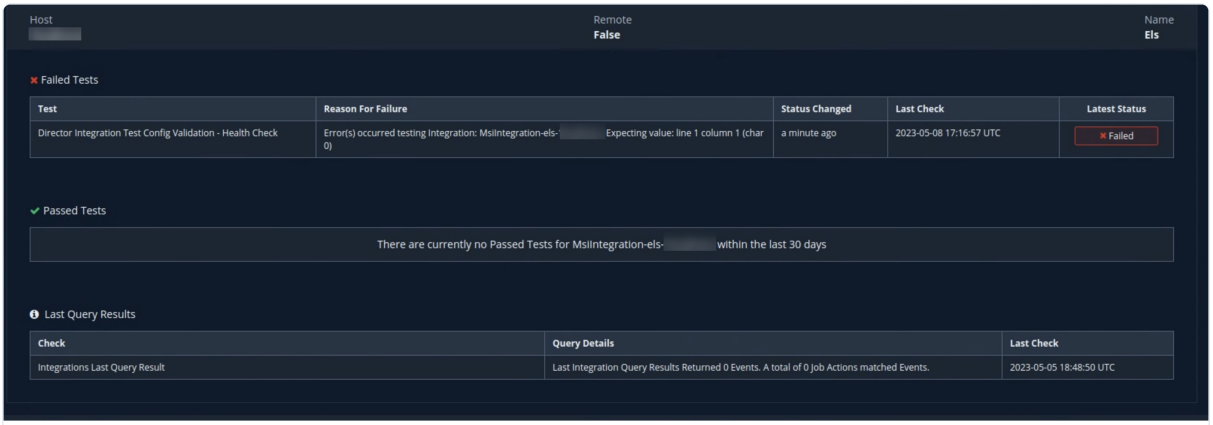
1. Go to **Settings** > **Integrations** and configure an Integration using the steps in the web interface, for example, ElasticSearch to retrieve matched events.
2. Verify that there is a Last Query configured for ElasticSearch.

Example of a Last Query for Elastic Search

Check Operational Status

1. Go to **Environment > Operational Status** and then click **Integrations**. You see the Last Query result details for the

integration. When there are events, the table displays the matched events/Job Actions that were last detected.



Last Query Results

Troubleshoot specific issues

This section provides details on specific issues with Integrations and suggestions for how to troubleshoot.

Integration not detected on Remote Actor

When you add the first MSI integration on a Remote Integrations Actor, the integration does not get detected. To fix this, reboot the Actor after the first MSI integration is selected for that Actor.

Integrations Service does not start (MSV)

Possible scenarios:

- `systemd` service configuration is corrupt.
- The device is out of space.
- Installation of integrations service during last upgrade or security patch was not successful.

Previously configured integration changed to point to local integration service

During the upgrade process, any existing integrations that have been configured to refer to `advantage.mandiant.com` are changed to the address for the Director. If you are using an Integrations Connector Client (ICC), then this could break your integration and you need to re-enable the original configuration.

Integration events not associated with Action

- One possible scenario is the matching criteria for the Action are too broad. As a result, not enough integration events are being returned because of flood prevention (a maximum of 10,000 events).
- If the Remote Integration Health Check reports no issues, but events are still not associated with Actions, the MSI integration subprocesses may not be running.
  While connected to the Remote Actor through SSH, verify whether the sub-processes are running by using the following command:

  ```
  systemctl status verodin-integrations.service
  ```

  Here is example output:

```
verodin-integrations.service - Verodin Integration Service
   Loaded: loaded (/usr/lib/systemd/system/verodin-integrations.service; static; vendor preset: disabled)
   Active: active (running) since Thu 2024-09-12 02:43:03 UTC; 4 days ago
 Main PID: 4269 (ruby)
    Tasks: 1 (limit: 61904)
   Memory: 23.1M
   CGroup: /system.slice/verodin-integrations.service
           └─4269 Verodin Integrations
```

In this case, the following subprocesses are missing:

```
           ├─335600 msi-integrations
           ├─335602 msi-integrations
           ├─335603 msi-integrations
           └─335605 msi-integrations
```

Do one of the following steps to start the subprocesses and fix the issue:

- Reboot the Actor.
- Restart the `systemd` service for `verodin.integrations-service`.

Unable to communicate with security technology even though integration configuration is valid

1. Ensure that network access is permitted between the Director (for local integrations) and the security technology.
2. Confirm that the test query works for the integration.