Mandiant

VERIFYING YOUR SERVICE HEALTH

The MD service team conducts regular monitoring and testing to evaluate how well MD services are running in your environment. This section describes the validation tests your team will perform to evaluate the health of the MD service in your environment. This section also provides the guidance and tools your team needs to help identify, evaluate, and assess visibility gaps in your MD service.

Work with your MDC to conduct and establish a weekly, monthly, or quarterly system health test schedule that meets your organization's testing needs and objectives.

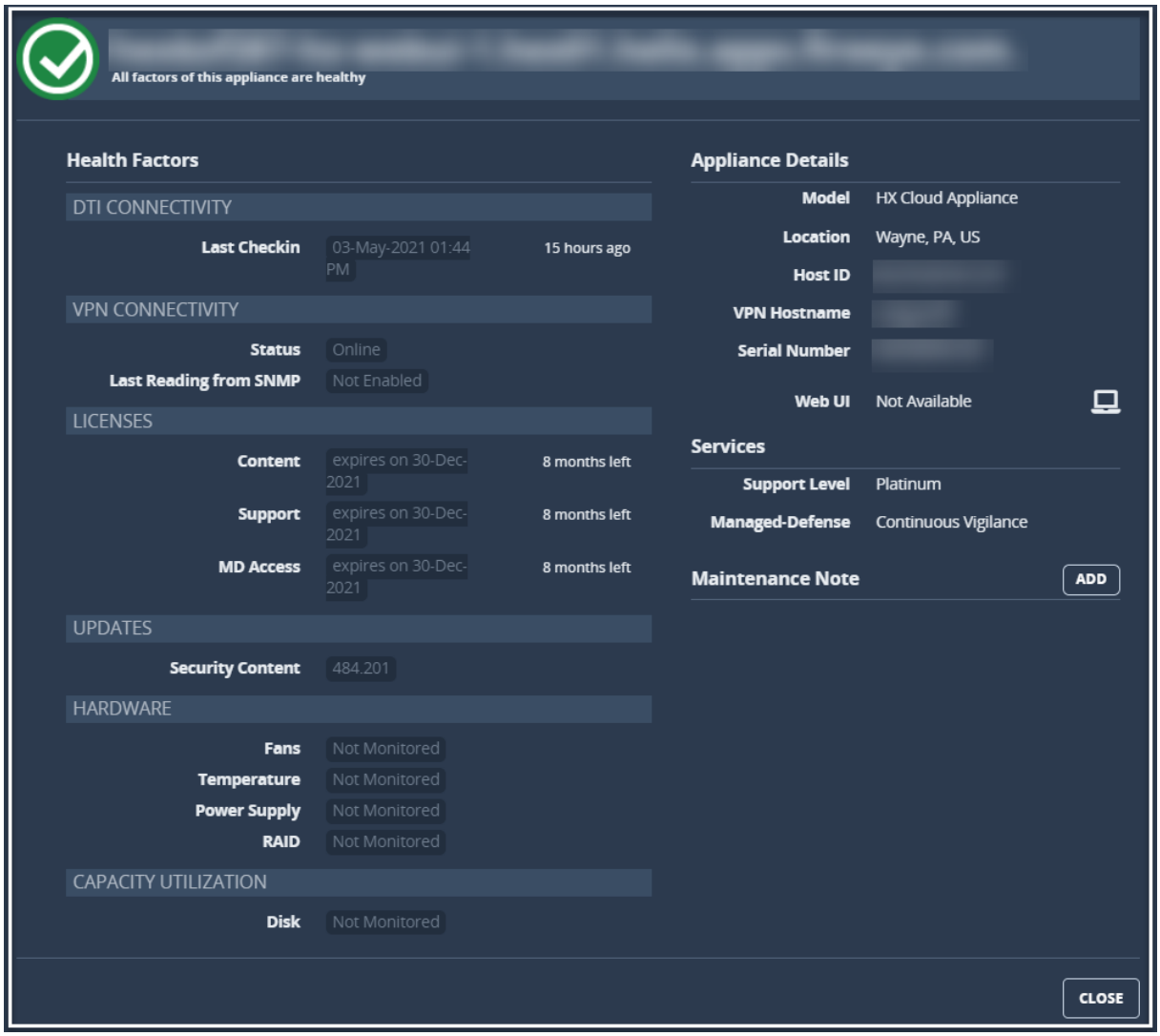
Validating Device Health

Your team will periodically conduct system testing on all of your appliances to verify that the appliances are fully operational and running optimally. The following appliance states determine what steps your team should perform next.

Appliance State	Indicator	Description	Next Steps
Good	Green	Your appliance is fully operational and running optimally.	No steps required.
Warning	Yellow	Your appliance software requires an update to the latest revision.	Contact **Support (https://docs.mandiant.com/home/customer-support)** to upgrade your appliance software to the latest software version.
		Your appliance has a network traffic issue.	Work with your internal IT team to resolve any network traffic issues.
Critical	Red	Your appliance is offline, or service delivery is impacted. For example, a product license may have expired.	Work with the Mandiant Support team and your internal IT team to bring your appliance back online.

TO REVIEW APPLIANCE STATUS:

1. In the MD Portal, select **Appliance** from the **Health** menu.
2. On the **Appliance Health** page, from the summary row on top click on each appliance to get summary for the group at the bottom (see **Monitoring Appliance Health (https://docs.mandiant.com/home/md-monitoring-endpoint-network-and-appliance-health)** for more details).
3. Click on each individual appliance at the bottom to review and record the status for each appliance.



4. Work with the Mandiant Support team or your internal IT team to resolve any issues with your appliances and return them to operational state.

NOTE: As described in the table above for each 'Health Factor' you see an indicator status in the traffic light colors. For example, if there is a yellow (warning) arrow for 'DTI CONNECTIVITY' you can view the detailed guidelines on the issue and also what to do about it.

Validating Network Health

Your team will periodically test and verify that all your appliances and sensors have network connectivity, are seeing the right network traffic, and meet the standards.

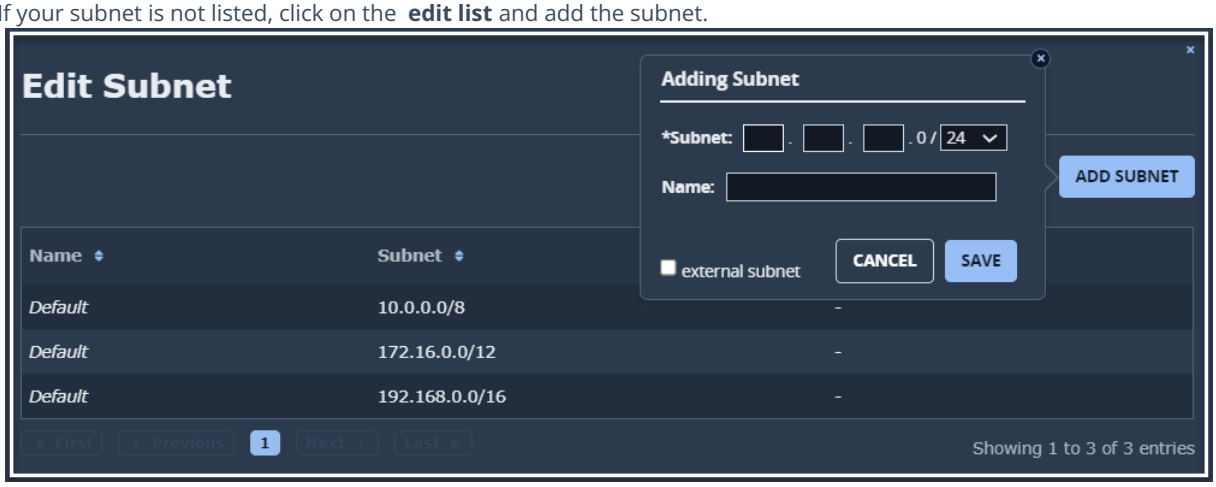
NTAP Sensors Visibility Testing

Perform the following tests to ensure that your Trellix NTAP sensors have full MD visibility for the covered subnets.

TEST 1: SUBNET VISIBILITY — TRAFFIC GRAPH

1. In the MD Portal, select **Network** from the **Health** menu.
2. Use the right or left page arrows to go to each NTAP sensor status window and view the device state.
3. Click on the gray **METRICS** bar and select **Subnet**.

4. If your subnet is not listed, click on the **edit list** and add the subnet.



5. Select your subnet from the drop-down list.
6. Repeat steps 1 - 5 for each sensor.

> **NOTE:** Filtering by subnet is no longer available for Trellix Network Forensics Sensors (PX) but remains for the legacy Mandiant NTAP Sensors.

> **NOTE:** The Traffic graph displays network traffic for subnets from the time of inclusion. Historical data is not available for newly added subnets.

TEST 2: SERVICE VISIBILITY

> **NOTE:** Managed Defense currently does not support this level of visibility. Please use the Ports graph to view traffic details.

1. In the MD Portal, select **Network** from the **Health** menu.
2. Use the right or left page arrows to go to each sensor status window.
3. If appropriate for each of your service locations and sensor types, verify the Sensor visibility checkboxes have green check marks for Web, DNS, and Email traffic.
4. Repeat steps 1-3 for each sensor.

Testing Network Security and Email Security Appliance Health

Perform the tests below to verify the health detection of your Trellix Network Security, Email Security appliances.

TEST 1: NETWORK SECURITY APPLIANCE HEALTH

1. On a device monitored by the appliance, go to the URL below to generate a test alert.
2. **http://fedeploycheck.fireeye.com/appliance-test/alert.html**

   > **NOTE:** Your appliance will send an alert email to your appliance users if it is configured to do so.

2. The following actions will occur if the test is successful:
   - You will receive a confirmation page in the web browser.
   - Mandiant Analysts will receive the test alert.
   - The timestamp is updated in Mandiant backend systems.
   - The timestamp is updated in the MD Portal under Appliance Health.

TEST 2: EMAIL SECURITY APPLIANCE HEALTH

1. Send a test email containing the URL below in the body of the email message to generate a test alert.
2. **http://fedeploycheck.fireeye.com/appliance-test/alert.html**
3. The following actions will occur if the test is successful:
    - Mandiant Analysts will receive the test alert.
    - The timestamp is updated in Mandiant backend systems.
    - The timestamp is updated in the MD Portal under Appliance Health.