

**HP MIK – Patch Assistant Updates to fix “No Data issue”**

This document is primarily focused on guiding the user to fix the issue where the HPPA dashboard shows “**No Data**”. The issue is caused when HPPA deployment reporting classes override the HP MIK Client classes during machine policy retrieval due to conflicting namespace.

The correction steps in this document are only needed for the environments with the following symptoms of the HPPA Plugin.

* **HP MIK 5.0.0.42729** is installed on the SCCM console.
* HPPA policy has been configured on at least one or more collections and successfully deployed to the clients.
* HPPA task has successfully run-on devices under the configured collections at least once.
* SCCM has completed the hardware inventory scan to pull the data from the client to the server since the last time the task ran.
* If one of the two scenarios is met:
  + The HPPA Dashboard is still showing devices as “**No Data**” even though there is a json report available under **%ProgramData%/HP/MIK/HPIAReport** on the client and the hardware inventory scan occurred after json report creation.
  + The HPPA Dashboard was showing the appropriate device reports. However, after some time, the same devices are being reported as “**No Data**”. Reinstallation of MIK Client fixes the issue temporality and the issue reappears again.

# Steps to be executed on SCCM Console

**Important note**: These steps are required to be completed on the console before the installation of the latest MIK Client on your clients. If you already have an existing MIK Client on your clients, you are still required to complete these steps before upgrading MIK Client to the latest version.

1. Install / Upgrade to **HP MIK 5.1.1.47 or later on HP FTP**.
2. As a part of the installation, a script has been added that updates the reporting classes of any existing HPPA deployment as a part of the fix for the issue. To ensure that the script has successfully updated reporting classes, please navigate to the following path **%ProgramData%\HP\HP MIK\Logs** and open the log file “**HP\_MIK.InstallScript.log**”. Ensure that there are no errors and that the log file has the following logs at the end of the script. If the logs are matching, please skip the next step.

Text

Description automatically generated

1. If the script has not run successfully in the previous step, the IT Administrator needs to manually run the script. The script can be run through PowerShell or Command Prompt as administrator. Download the following two files and follow the instructions in HP\_MIK\_InstallScript\_Instructions.txt

<https://hpia.hpcloud.hp.com/downloads/doc/hpmik/HP_MIK_InstallScript_Instructions.txt>

<https://hpia.hpcloud.hp.com/downloads/doc/hpmik/HP_MIK_InstallScript.vbs.txt>

**Step 2: Force all HPPA clients to retrieve the machine policy**

1. In the SCCM console, navigate to **Assets and Compliance > Overview > Device Collections**. Right-click each HPPA configured collection, go to **Client Notification,** and select **Download Computer Policy**. This will force all online clients to retrieve the updated machine policy as we have updated the reporting classes of the deployment.

**Important note**

This step will only trigger machine policy retrieval on online clients. The offline clients will get the latest machine policy once they are online and reconnect to SCCM.

Before moving to step 3, the IT Administrator needs to ensure that enough time is given to their clients based on their SCCM configurations so clients can retrieve the updated machine policy to correct HPPA reporting classes on clients.

Graphical user interface, text, application, email

Description automatically generated

**Track the Progress of Machine Policy and Retrieval**

The IT Administrator can also follow the steps below to track the progress of the machine policy retrieval on their clients. It is recommended to follow these steps as they will help to confirm the effectiveness of the previous step.

1. In the SCCM console, navigate to **Monitoring > Overview > Queries.** Right-click the node and select “**Create Query**”.

Graphical user interface, text, application, email

Description automatically generated

1. In the **Create Query Wizard**, name the query **Systems – HPPA – Requesting Policy after <date>** and click “**Edit Query Statement**”.

Graphical user interface, application, Word

Description automatically generated

1. In the **Properties** pop-up, click “**Show Query Language**” and paste the following query in the pop-up and click **OK**. Then, click **OK,** **Next, Next,** and **Close.**

Please update the date in this query as needed. The date should be when the new HP MIK is installed.

Format of date: YYYYMMDD

**Query:**

SELECT Client.LastPolicyRequest, R.Name, R.ResourceID from SMS\_R\_System as R INNER JOIN SMS\_G\_System\_CH\_ClientSummary Client on Client.ResourceID = R.ResourceId INNER JOIN SMS\_FullCollectionMembership collection ON collection.ResourceID = R.ResourceID WHERE collection.IsClient='1' AND collection.CollectionID IN (SELECT DISTINCT BA.TargetCollectionID FROM SMS\_BaselineAssignment BA INNER JOIN SMS\_ConfigurationItemLatest CBL ON BA.AssignedCI\_UniqueID = CBL.CI\_UniqueID INNER JOIN SMS\_ConfigurationItemLatest CIL ON CBL.LocalizedDisplayName = CIL.LocalizedDisplayName INNER JOIN SMS\_ConfigurationItemRules R ON CIL.CI\_ID = R.CI\_ID WHERE CIL.LocalizedDisplayName like 'HPPA%' AND CIL.CIType\_ID = 5 AND CBL.CIType\_ID = 2 AND CIL.RuleName = 'Task Enable') AND Client.LastPolicyRequest > '20220930'

**Important Note**

The date above needs to be updated properly to when policy retrieval is forced. The goal is to check if all HP clients managed by HPPA policies have retrieved machine policy before moving on to the next step.

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application, chat or text message

Description automatically generated

1. The newly created query will be shown under the “**Queries**”. Right-click the newly created query and select **Run** to run the query and see the results.

Graphical user interface, text, application, email

Description automatically generated

# Steps on managed device

**Optional Step**:

The following is an example of a client which has an existing MIK Client installed with overridden HPPA classes. This is an optional step and just additional information for the administrator who would like to confirm the state of their client before installing/upgrading the MIK Client.

1. On the windows search bar, type **wbemtest** and run the application as administrator.

Graphical user interface, text, website

Description automatically generated

1. Click the **connect** button.

Graphical user interface, table

Description automatically generated

1. Enter the following in the namespace field and click **Connect**.    
    **ROOT\HP\InstrumentedServices\v1**

Graphical user interface, application

Description automatically generated

1. Click on **Enum Classes**, then select **recursive** and click **ok**.

Graphical user interface, text, application

Description automatically generated  Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**Step 3: Installation / Upgrade of MIK Client.**

1. Install / Upgrade to **HP MIK Client 5.1.1.37 or later on HP FTP.** This step will fix the corrupted HPPA classes on the client which allows the provider to populate data from the HPIA Report.

After installation/upgrade of MIK Client, the snapshot above from the optional step should update to the following where **SW\_ManagedInstanceService** is now shown correctly compared with the previous snapshot where 0 is shown.

Graphical user interface, text, application, email

Description automatically generated

**Track progress of installation of MIK Client**

Create another new query by following the steps of **Track the Progress of Machine Policy and Retrieval** and name the query **Systems with HP MIK Client <version>** and paste the following query in the “**Show Query Language”** pop-up. This query returns all clients that have MIK Client installed with a specific version. Please update the version in this query as needed.

**Query:**

SELECT DISTINCT R.Name, SMS\_G\_System\_ADD\_REMOVE\_PROGRAMS.DisplayName, SMS\_G\_System\_ADD\_REMOVE\_PROGRAMS.Version FROM SMS\_R\_System AS R INNER JOIN SMS\_G\_System\_ADD\_REMOVE\_PROGRAMS on SMS\_G\_System\_ADD\_REMOVE\_PROGRAMS.ResourceId = R.ResourceId WHERE SMS\_G\_System\_ADD\_REMOVE\_PROGRAMS.DisplayName = 'HP MIK Client' AND SMS\_G\_System\_ADD\_REMOVE\_PROGRAMS.Version = '5.1.1.37'

**Step 4: Retrigger Machine Policy and Retrieval.**

1. Repeat **Step 2: Force all HPPA clients to retrieve the machine policy**. This step will ensure that the issue has been resolved correctly before we collect hardware inventory information from the clients in the next step.

On the next hardware inventory scan of online and connected clients, the appropriate client data will be sent to the SCCM console and the HPPA dashboard should reflect the clients’ data. Optionally, the IT Administrator can also force the hardware inventory scan (as shown in the next step) to verify the fix without waiting for the SCCM hardware inventory schedule.

**Important note:** The providers will only read the data from the json file on the client if the scheduled task has run at least once and has generated the json file. If the task has not ran at least once, then the client will still report as “**No Data**” on the HPPA dashboard because there is nothing to report back to the server from the client. This machine is expected to be under “**No Data**” category.

**Step 5: Trigger Hardware Inventory**

1. In the SCCM console, navigate to **Assets and Compliance > Overview > Device Collections**. Right-click each HPPA configured collection, go to **Client Notification** and select **Collect Hardware Inventory**. This will force a hardware inventory scan on online and connected clients.

**Import note**: This step will only trigger hardware inventory scan on online clients. The offline clients will not report any hardware inventory information back to the console.

Graphical user interface, application, email

Description automatically generated

**Track progress of installation of Hardware Inventory Scan**

Create another new query by following the steps of **Track the Progress of Machine Policy and Retrieval**, name the query as **Systems – Requesting HW Scan after <date>,** and paste the following query in the “**Show Query Language”** pop-up. This query returns all clients on which the hardware inventory scan was completed after a given date. Please update the date in this query as needed.

Format of date: YYYYMMDD

**Query:**

select s.ResourceId, s.NetBiosNamefrom SMS\_R\_SYSTEM sinner join SMS\_G\_System\_WORKSTATION\_STATUS ws on s.ResourceId = ws.ResourceId

where ws.LastHardwareScan >= '20220930'

**Important Note**

The date in the query above must be changed to when hardware inventory scan is forced to

check if expected clients have reported hardware inventory data which includes HPPA data.

**Evaluation**

After the completion of the previous step, if most of the clients still report as **“No Data”**, please ensure the following for those clients:

1. HPPA task has successfully ran on those clients and a json report is generated.
2. HPIA did not report any errors in the generated json report.
3. Hardware inventory scan was triggered and completed after the generation of json report.

If all of the prerequisites above are checked and the issue is still not resolved, please repeat the steps from **Step 2: Force all HPPA clients to retrieve the machine policy**.