The different ways of enrolling devices in Windows Analytics

March 25, 2019 by Peter van der Woude

After a week of silence, due to the MVP Summit, this week another new blog post. This week is all about enrolling devices in to Windows Analytics. An updated version, with a slightly different angle, of a post of about two years ago. This time I'll summarize the different methods to achieve the same goal and the changes since Windows 10, version 1803. I'll start this post with an overview of the required settings, followed by an overview of the different configuration methods. I'll end this post by going through my preferred method, for a cloud scenario, and the administrator experience.

Settings to configure

Now let's start by looking at the settings that are required to enroll devices in to Windows Analytics. Those settings are the commercial ID, the telemetry level (and with that enabling Windows telemetry) and allowing the device name in the telemetry data (since Windows 10, version 1803). The following table describes the settings that are required, including a description, and starting point for my preferred method, for a cloud scenario, of configuring these settings.

Policy	Description
AllowTelemetry **Values**: 0 (Security), 1 (Basic), 2 (Enhanced), or 3 (Full)	This setting should be used to enable Windows telemetry. Windows Analytics requires a minimum Windows telemetry level of enhanced (optional together with the policy LimitEnhancedDiagnosticDataWindowsAnalytics

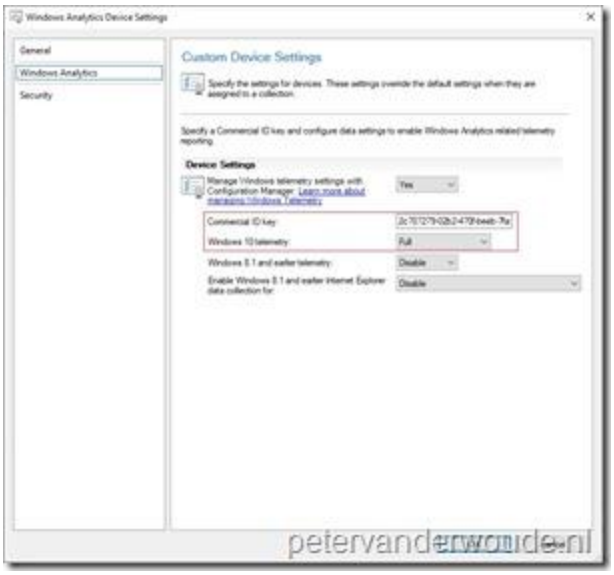
	to limit the telemetry data to the minimal required).
AllowDeviceNameInDiagnosticData **Values**: 0 (Disabled) or 1 (Enabled)	This setting should be used to allow the device name in the Windows telemetry that is sent to Windows Analytics. That will enable that the different solutions within Windows Analytics can actually be used for really tracking update compliance.
CommercialID **Values**: [YourCommercialID]	This setting should be used to specify the workspace id that should be used for Windows Analytics. The commercial ID can be found in the *Settings* of the different Windows Analytics solutions.

Note: The first two policies are available in the node ./Vendor/MSFT/Policy/Config/System and the third policy is available in the node ./Vendor/MSFT/DMClient/Provider/MS DM Server.

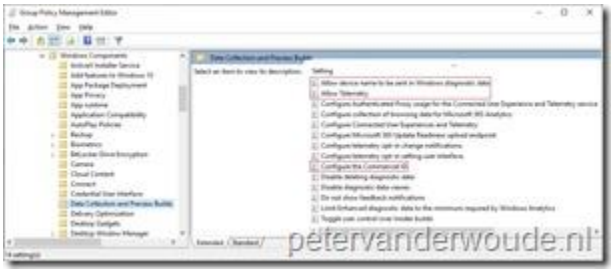
Configuration options

Let’s continue with looking at the different configuration methods. Every configuration option has pros and cons, which can differ per scenario.

1 When using Configuration Manager, the Configuration Manager client can be used to enroll a device in to Windows Analytics. This can be achieved by using the *Windows Analytics* section in the *Client Settings*. This configuration method can configure the commercial ID and the telemetry level. This can be a useful method in an on-premises, or a co-management scenario. Only allowing the device name in the telemetry data would require an additional configuration method.



2 When using Group Policy, Administrative Templates can be used to enroll a device in to Windows Analytics. This can be achieved by using the *Data Collection and Preview Builds* section in the *Windows Components* section of the *Administrative Templates*. This configuration method can configure the commercial ID, the telemetry level and the device name. This can be useful in any on-premises, or cloud scenario (by using a third-party tool like PolicyPak: MDM Edition). Only reporting on a setting-level will be limited in a cloud scenario.



3 When using Configuration Manager or Microsoft Intune, PowerShell scripts can be used to enroll a device in to Windows Analytics. This can be achieved by using the New-Item and the New-ItemProperty cmdlets to directly create the required registry keys. This configuration method can configure the commercial

ID, the telemetry level and the device name. This can be useful in any on-premises, or cloud scenario. Only reporting on a setting-level will be limited.

4 When using Microsoft Intune, Windows 10 MDM can be used to enroll a device into Windows Analytics. This can be achieved by using custom OMA-URI settings. This configuration method can configure the commercial ID, the telemetry level and the device name. This can be useful in a co-management, or cloud scenario.

Preferred configuration option

Let's continue by looking at my preferred configuration option, at least in a cloud scenario. Besides using Group Policy, this is the most reliable and complete option for configuring the required settings. It allows setting-level configuration and reporting. The following 3 steps walk through the required actions.

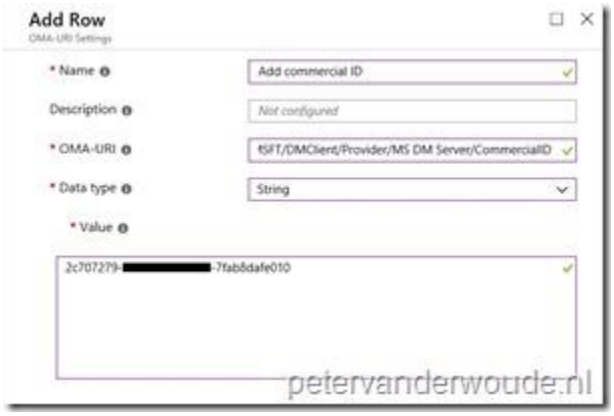
1 Open the Azure portal and navigate to **Microsoft Intune** > **Device configuration** > **Profiles** to open the **Devices configuration – Profiles** blade;
2 On the **Devices configuration – Profiles** blade, click **Create profile** to open the **Create profile** blade;

3a On the **Create profile** blade, provide the following information and click **Create**;

- **Name**: Provide a valid name;
- **Description**: (Optional) Provide a description;
- **Platform**: Select *Windows 10 and later*;
- **Profile type**: Select *Custom*;
- **Settings**: See step 3b;

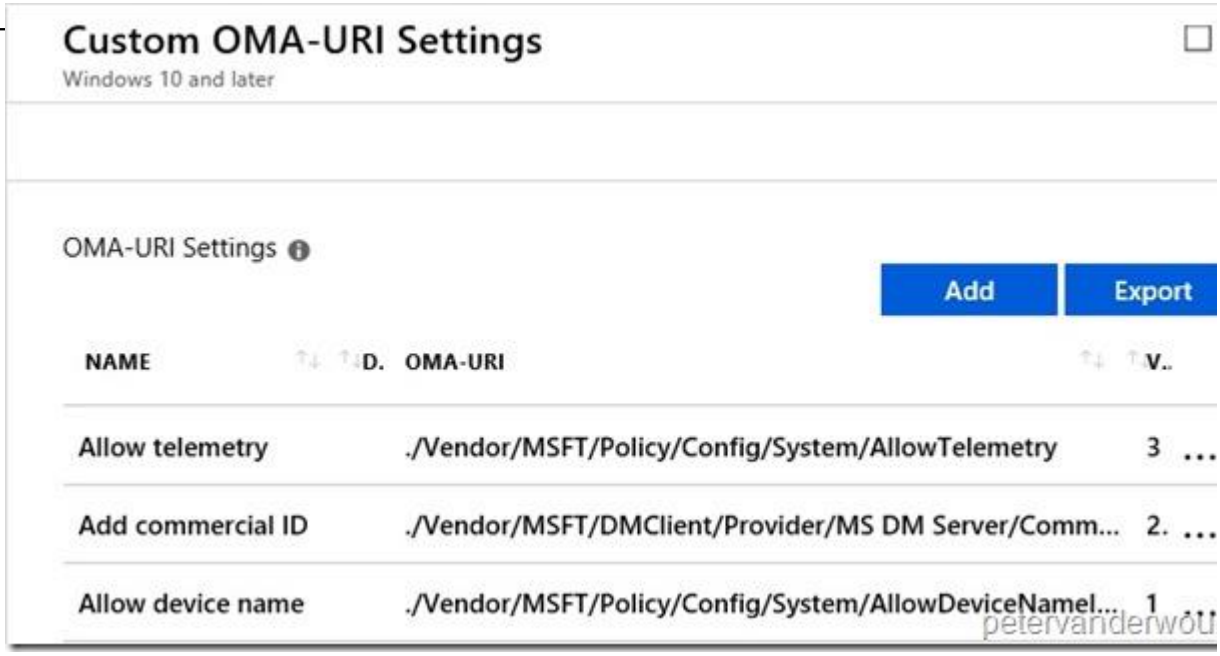
Explanation: This configuration will make sure that a custom profile is created that can be used to add the required Windows Analytics settings.

3b On the **Custom OMA-URI Settings** blade, provide the following information and click **Add** to open the **Add row** blade. On the **Add row** blade, provide the following information and click **OK** (and click **OK** in the **Custom OMA-URI** blade);



- **Name**: Provide a valid name;
- **Description**: (Optional) Provide a description;
- **OMA-URI**: Specify a the required policy setting;
- **Data type**: Select *Integer*;
- **Value**: Specify the required value;

Note: Simply repeat this step for every policy setting that should be configured.



Note: At some point in time this configuration will probably become available in the Azure portal without the requirement of creating a custom OMA-URI.

Administrator experience

Let's end this post by looking at the administrator experience. Of course I can simply show the configurations on the device, but I thought that showing a device including the device name in a solution would show the complete picture. It proofs that Windows telemetry is enabled, that it's sending data to the correct workspace and that it's sending the device name (even for devices with Windows 10, version 1803 and newer). See below for that example.

More information

For more information about Windows Analytics and Microsoft Intune, please refer to the following articles:

- Configure Windows diagnostic data in your organization: https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization
- Enrolling devices in Windows Analytics: https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-get-started
- Windows 10 enhanced diagnostic data events and fields used by Windows Analytics: https://docs.microsoft.com/en-us/windows/privacy/enhanced-diagnostic-data-windows-analytics-events-and-fields