Enable Windows Automatic Redeployment from the login screen

This week a short post about enabling Windows Automatic Redeployment form the login screen. It’s a follow up on [enabling password reset](https://www.petervanderwoude.nl/post/enable-password-reset-from-the-login-screen/) and [PIN reset from the login screen](https://www.petervanderwoude.nl/post/enable-pin-reset-from-the-login-screen/), as it enables another feature on the login screen, and a nice addition in combination with [Windows AutoPilot](https://www.petervanderwoude.nl/post/manage-windows-autopilot-via-microsoft-intune/). Windows Automatic Redeployment might be a familiar feature, but I couldn’t find much written information about it yet. In this post I’ll provide a brief introduction to Windows Automatic Redeployment, followed by the required configuration and the end-user experience.

Introduction

Now let’s start with a brief introduction about Windows Automatic Redeployment. Starting with Windows 10, version 1709, administrators can use Windows Automatic Redeployment to quickly remove personal files, apps, and settings, by resetting Windows 10 devices from the login screen at any time. That reset will apply the original settings and device management enrollment, so the devices are ready to use once the reset is completed. The device management enrollment is related to Azure Active Directory and Microsoft Intune (or other third-party MDM-providers).

In other words, Windows Automatic Redeployment allows administrators to reset devices to a known good managed state while preserving the management enrollment. After Windows Automatic Redeployment is triggered, the devices are ready for use by standard users.

Configuration

The configuration actually only contains one specific setting. To get that specific setting, the first step explains the location of the setting and the second step explains the usage of the setting.

Step 1: Get the required setting

The first step is to get the required setting. The [Policy CSP](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider) contains [CredentialProvider policies](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialproviders" \t "_blank). One of those policies is **[DisableAutomaticReDeploymentCredentials](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialproviders" \l "credentialproviders-disableautomaticredeploymentcredentials" \t "_blank)**. That policy is introduced in Windows 10, version 1709, and is used to enable or disable the visibility of the credential provider that triggers the reset on a device. This policy does not actually trigger the reset. This policy enables the administrator to authenticate and trigger the reset on the device. This setting supports the following values:

* **0** – Enable the visibility of the credentials for Windows Automatic Redeployment;
* **1** – Disable visibility of the credentials for Windows Automatic Redeployment.

Step 2: Configure the required setting

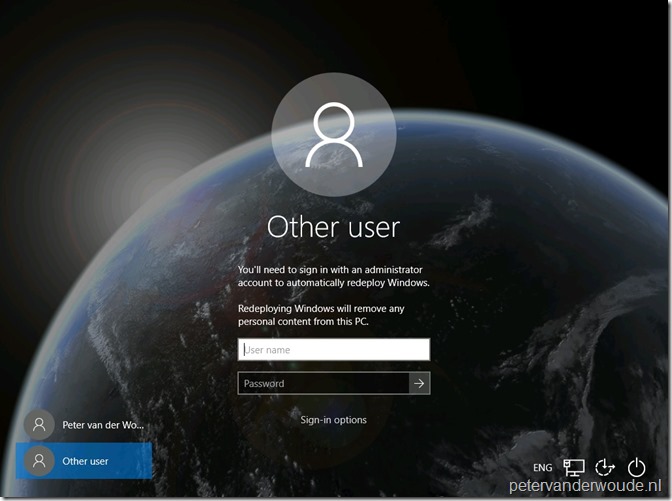
The second step is to actually configure the required setting to enable the option to automatically redeploy Windows from the login screen. In other words, the second step is to configure a device configuration profile with at least a custom OMA-URI setting. The following three steps walk through the creation of a new device configuration profile, including the required OMA-URI setting. After that simply assign the created profile to a user group.

|  |  |
| --- | --- |
| **1** | Open the [Azure portal](https://portal.azure.com/) and navigate to **Intune**> **Device configuration**> **Profiles**; |
| **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. |
| **3b** | [[MSIntune_WAR](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MSIntune_WAR.jpg?ssl=1)](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MSIntune_WAR.jpg?ssl=1)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**: ./Vendor/MSFT/Policy/Config/CredentialProviders/DisableAutomaticReDeploymentCredentials; * **Data type**: Select *Integer*; * **Value**: 0. |

End-user experience

Let’s end this post by looking at the end-user experience. I’ll do that by showing how to trigger Windows Automatic Redeployment, followed by a screenshot of the start of the process and a screenshot of the end of the process.

To trigger the Windows Automatic Redeployment, press the combination of **Ctrl +Windows key+ R** on the login screen**.** As shown below, this will provide the user with the option to provide an administrator account to automatically redeploy Windows.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/Windows_Redeploy_01.jpg?ssl=1)

Once administrator credentials are provided the redeployment process will be triggered. As shown below, when the process is finished a success message will be shown.

[](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/Windows_Redeploy_02.jpg?ssl=1)

Now the device is ready to go. Keep in mind that the device is still Azure AD joined and Microsoft Intune managed with the original account. So, the main use case for this reset is for information workers and students.