Enable password reset from the login screen

This week is about something similar as last week. This week is all about the password reset option on the login screen. In other words, the **Reset password** option. Starting with Windows 10, version 1709, it’s possible to enable the **Reset password** option from the login screen for Azure AD joined devices. I know that a lot has been written already about this subject, but I have the feeling that this subject needs a place on my blog. My style and more details. In this post I’ll provide a short introduction about Azure AD self-service password reset (SSPR), followed by walking through the required configurations for SSPR and the **Reset password** option. I’ll end this post by looking at the end-user experience.

Introduction

Now let’s start this post with an introduction about Azure AD SSPR. With SSPR users can reset their passwords on their own when and where they need to. At the same time, administrators can control how a user’s password gets reset. That means that the user no longer needs to call a help desk just to reset their password. SSPR includes (the focus of this post is number 2):

1. **Self-service password change**: The user knows their password but wants to change it to something new;
2. **Self-service password reset**: The user is unable to sign in and wants to reset their password by using one or more of the following validated authentication methods:
   * Send a text message to a validated mobile phone;
   * Make a phone call to a validated mobile or office phone;
   * Send an email to a validated secondary email account;
   * Answer their security questions.
3. **Self-service account unlock**: The user is unable to sign in with their password and has been locked out. The user wants to unlock their account without administrator intervention by using their authentication methods.

Configuration

Let’s continue by having a look at the required configuration, to enable the **Reset password**option from the login screen. As the configuration of the actual settings requires SSPR to be enabled, I divided the configuration into two steps. The first step is to enable SSPR and the second step is to configure the **Reset password** option.

Step 1a: Enable SSPR

The first step is to enable SSPR, as it’s the starting point for enabling the **Reset password**option from the login screen. Without SSPR enabled, and still configuring the **Reset password**option, the user will receive a message that SSPR is not enabled for the user and that the user should contact the administrator. The following seven steps walk through the relatively simple configuration to enable SSPR.

|  |  |
| --- | --- |
| **1** | Open the [Azure portal](https://portal.azure.com/) and navigate to **Azure Active Directory**> **Password reset**; |
| **2** | [[AAD_PR_Properties](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Properties.jpg?ssl=1)](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Properties.jpg?ssl=1)On the **Password reset – Properties**blade, select **All** and click **Save**; |
| **3** | [[AAD_PR_Auth](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Auth.jpg?ssl=1)](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Auth.jpg?ssl=1)On the **Password reset – Authentication methods**blade, select the number of required methods to reset and the available methods to user and click **Save**;  Note: Make sure that you have at least as many methods available to users as you have required to reset. |
| **4** | [[AAD_PR_Registration](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Registration.jpg?ssl=1)](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Registration.jpg?ssl=1)On the **Password reset – Registration**blade, configure whether or not to require users to register when signing in and click **Save**; |
| **5** | [[AAD_PR_Notifications](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Notifications.jpg?ssl=1)](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Notifications.jpg?ssl=1)On the **Password reset – Notifications**blade, configure the notification settings and click **Save**; |
| **6** | [[AAD_PR_Customizations](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Customizations.jpg?ssl=1)](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_Customizations.jpg?ssl=1)On the **Password reset – Customization**blade, configure the customization settings and click **Save**; |
| **7** | [[AAD_PR_OnPrem](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_OnPrem.jpg?ssl=1)](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/AAD_PR_OnPrem.jpg?ssl=1)On the **Password reset – On-premises integration**blade, and configure the password write back configuration and click **Save**;  Note: This is required when using an on-premises directory and also requires the configuration of step 1b. |

Step 1b: (Optional) Configure password writeback

Another part of the first step is the optional configuration of password writeback. This should be configured to write the passwords from Azure AD back to the on-premises directory. To achieve this, use the following seven steps to reconfigure Azure AD Connect.

|  |  |
| --- | --- |
| **1** | On the Azure AD Connect server, start **Azure AD Connect** to open the **Microsoft Azure Active Directory Connect** wizard; |
| **2** | On the **Welcome**page, click **Configure**; |
| **3** | On the **Additional tasks** page, select **Customize synchronization options** and click **Next**; |
| **4** | On the **Connect to Azure AD** page, provide the required credentials and click **Next**; |
| **5** | On the **Connect Directories** page, click **Next**; |
| **6** | On the **Domain/OU Filtering** page, click **Next**; |
| **7** | [[MAADC_OptionalFeatures](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MAADC_OptionalFeatures.jpg?ssl=1)](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MAADC_OptionalFeatures.jpg?ssl=1)On the **Optional Features** page, select **Password writeback** and click **Next**;  Note: I’ve also got Device writeback configured, which causes the next page to appear. |
| **8** | (Optional) On the **Writeback**page, click **Next**; |
| **9** | On the **Configure**page, click **Configure** and once completed click **Exit**; |

Step 2: Enable **Reset password**option

The second step is to configure the required setting to enable the **Reset password**option 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 required setting is part of the *Authentication* node of the*Policy CSP*. It’s the **[AllowAadPasswordReset](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-authentication" \l "authentication-allowaadpasswordreset" \t "_blank)** policy. That policy allows administrators to enable the self-service password reset feature on the windows logon screen. An integer value of 0 means not enabled and an integer value of 1 means enabled.

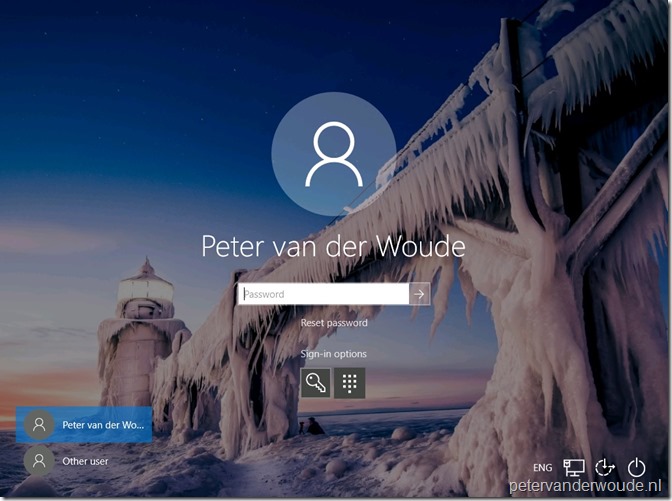
The following three steps walk through the creation of a new device configuration profile, including the required OMA-URI setting. After that simply assign the created profile to a user group.

|  |  |
| --- | --- |
| **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** | [[MSI_AllowPasswordReset](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MSI_AllowPasswordReset-1.jpg?ssl=1)](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MSI_AllowPasswordReset-1.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**: ./Device/Vendor/MSFT/Policy/Config/Authentication/AllowAadPasswordReset; * **Data type**: Select *Integer*; * **Value**: 1. |

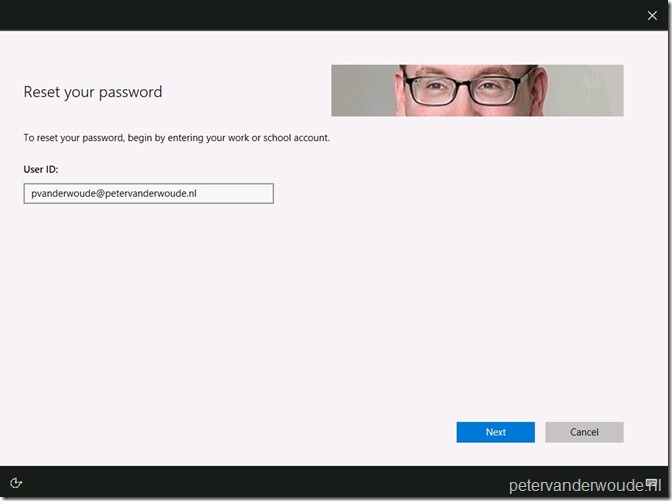
Note: For testing purposes it’s also possible to configure the**Reset password** option by using the **HKLM\SOFTWARE\Policies\Microsoft\AzureADAccount** registry key with the value, type and data of *AllowPasswordReset, REG\_DWORD and 1*.

End-user experience

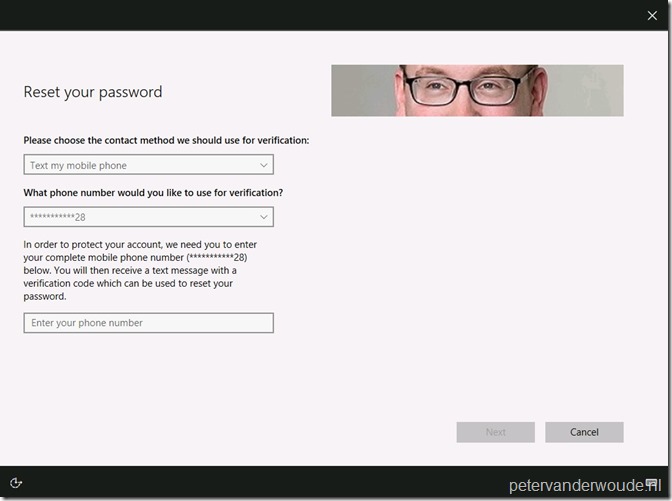
Now let’s end this post by walking through the end-user experience. On the login screen a new option is available when selecting password as the sign-in option, the **Reset password** option.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/RP_01.jpg?ssl=1)

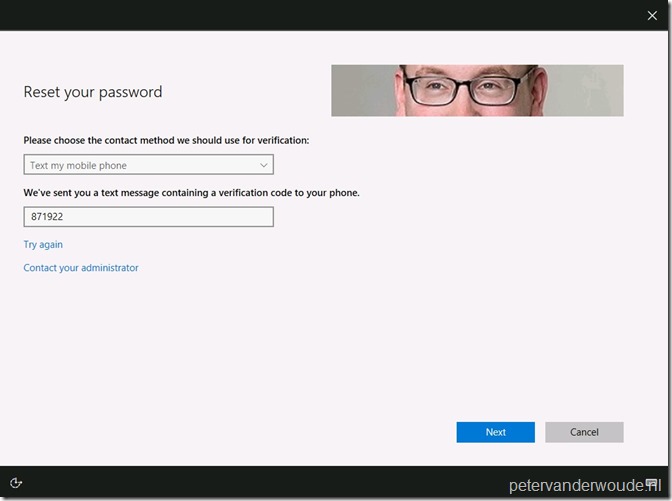
When the user selects **Reset password**, the user will be redirected to the Azure AD self-service password reset service.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/RP_02.jpg?ssl=1)

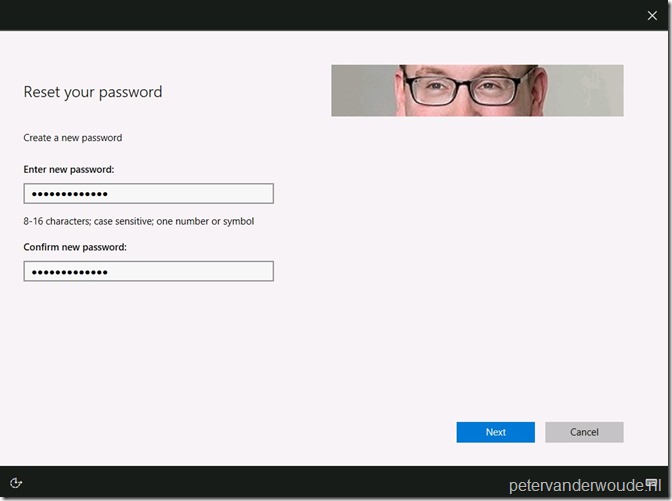
The **User ID** is already prepopulated and when the user clicks on **Next**, the user should choose a verification method. In my case a text to my mobile phone.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/RP_03.jpg?ssl=1)

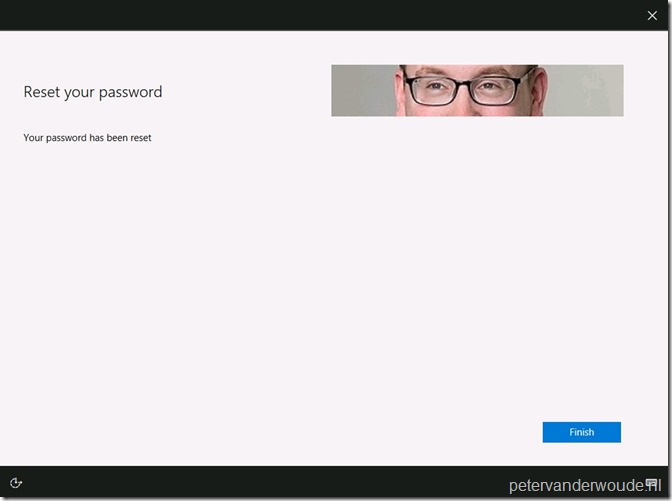
When the user provides the correct mobile phone number and clicks on **Next**, the user must provide the actual verification code of the text message.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/RP_04.jpg?ssl=1)

When the user provides the correct verification code and clicks on **Next**, the user must provide a new password.

[](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/RP_05.jpg?ssl=1)

When the user provides a new password and clicks **Next**, the user will be provided with the message that the password has been reset. When the user than clicks on **Finish**, the user will be redirected to the login screen.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/RP_06.jpg?ssl=1)

More information

For more information about SSPR, Windows 10 and the**Reset password** option, please refer to the following articles: