Enable PIN reset from the login screen

This week I’m going for an end-user experience focused blog post. This week is all about the PIN reset option on the login screen. In other words, the **I forgot my PIN** option. Starting with Windows 10, version 1709, it’s now possible to enable the **I forgot my PIN** option from the login screen. When using Windows Hello for Business, which can be configured during the Windows enrollment, by using Microsoft Intune, the PIN is the fallback mechanism when it’s not possible to authenticate with biometrics. In other words, the PIN is really important.

In this post I’ll provide the required configuration to provide the user with the **I forgot my PIN** option from the login screen. I’ll do that by assuming that the user can use the Windows Hello for Business PIN recovery service to reset their PIN. I’ll end this post by looking at the end-user experience.

Configuration

Now let’s start by having a look at the required configuration to enable the **I forgot my PIN** option from the login screen. As the configuration of the actual settings requires the tenant ID, I divided the configuration into three steps. The first step is to find and introduce the required setting, the second step is to get the tenant ID and the third step is to use the tenant ID in the actual configuration.

Step 1: Get the required setting

The first step is to get and introduce the required setting. The PIN-related settings are part of the Windows Hello for Business settings, which can be configured by using the [PassportForWork CSP](https://docs.microsoft.com/en-us/windows/client-management/mdm/passportforwork-csp" \t "_blank). Starting with Windows 10, version 1703, that CSP contains the **EnablePinRecovery** node. With Windows 10, version 1703, this setting can be used to enable the **I forgot my PIN** option from the *Settings* panel and starting with Windows 10, version 1709, this setting can also be used to enable the **I forgot my PIN** option from the login screen.

This settings has a boolean value that enables a user to change their PIN by using the Windows Hello for Business PIN recovery service. This cloud service encrypts a recovery secret, which is stored locally on the client, and can be decrypted only by the cloud service. The default value of this setting is false. Once the administrator enables this setting, the PIN recovery secret will be stored on the device and the user can change their PIN if needed.

Step 2: Get the tenant ID

The second step is to get the tenant ID. This is super simple these days, but, as I’ve never provided the actual steps, I thought it would be smart to publish them once. To get the tenant ID, simply follow the two steps below.

|  |  |
| --- | --- |
| **1** | Open the [Azure portal](https://portal.azure.com/) and navigate to **Azure Active Directory**> **Properties**; |
| **2** | [[tenantID](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/tenantID-1.jpg?ssl=1)](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/tenantID-1.jpg?ssl=1)On the **Properties**blade, click **Copy**next to **Directory ID** to copy the tenant ID;  Note: Just to be clear, this should be used in the OMA-URI instead of *{tenantID}*. |

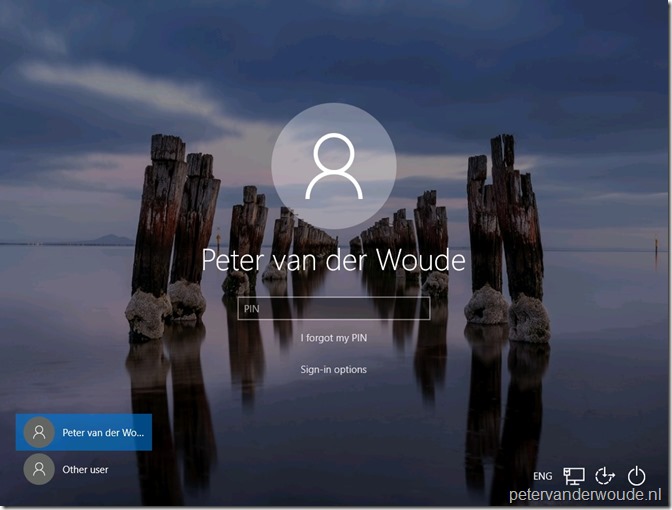
Step 3: Configure the required setting

The third step is to configure the required setting to enable the **I forgot my PIN** option from the login screen. In other words, the third 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.

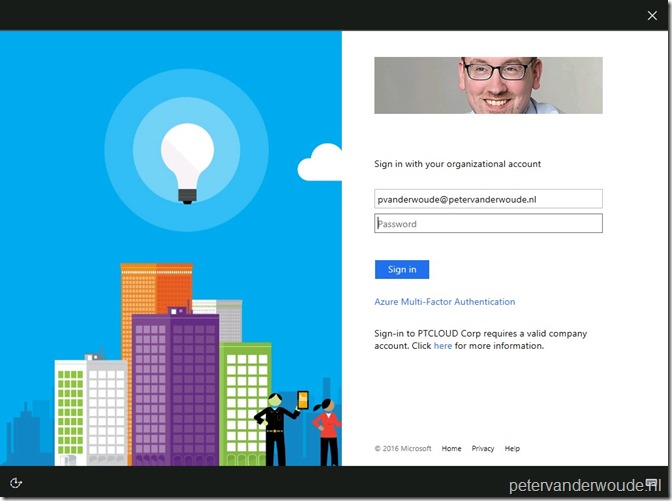
|  |  |
| --- | --- |
| **1** | Open the [Azure portal](https://portal.azure.com/) and navigate to **Intune**> **Device configuration**> **Profiles**; |
| **2** | On the **Devices configuration – Profiles**blade, click **Create profile**to open the **Create profile**blade; |
| **3a** | On the **Create 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** | [[MIS_PINReset](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MIS_PINReset-1.jpg?ssl=1)](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/MIS_PINReset-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/PassportForWork/{tenantID}/Policies/EnablePinRecovery; * **Data type**: Select *Boolean*; * **Value**: Select *True*. |

End-user experience

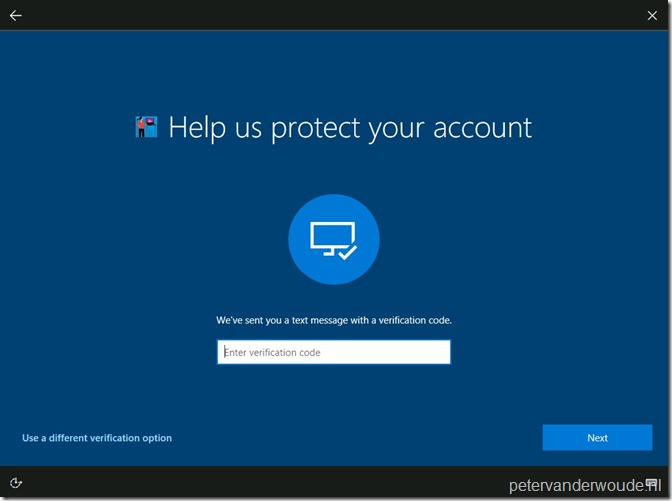
Now let’s walk through the end-user experience. On the login screen a new option is available when selecting PIN as the sign-in option, the **I forgot my PIN** option.

[](https://i0.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/IfmP_01-1.jpg?ssl=1)

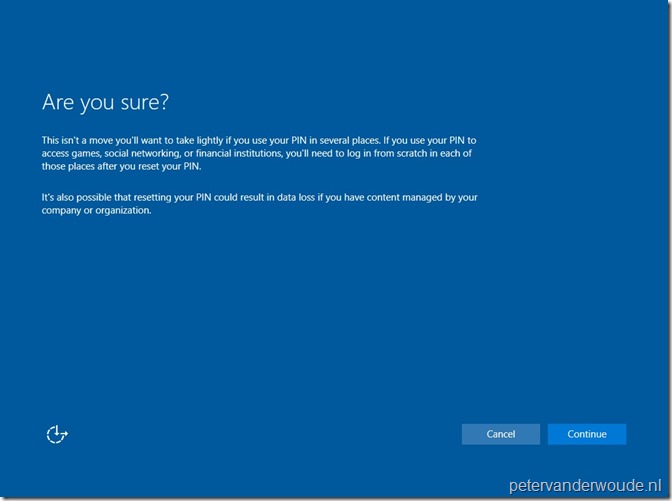
When the user selects **I forgot my PIN**, the user will be redirected to the login experience of the identity provider. In my case ADFS.

[](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/IfmP_02-1.jpg?ssl=1)

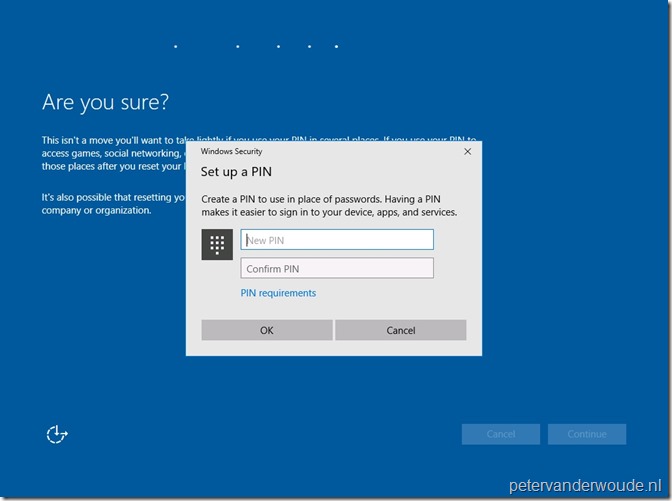
When the user provides a password and clicks on **Sign-in**, the user needs to provide an additional verification option, on an Azure AD branded page. In my case a text message.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/IfmP_03-1.jpg?ssl=1)

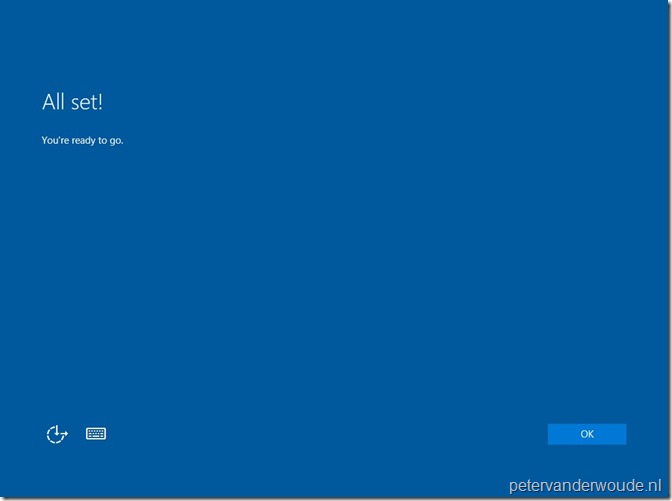
When the user provides the additional verification and clicks on **Next**, the user will be provided with an additional notification to make sure that the user is aware of the impact.

[](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/IfmP_04.jpg?ssl=1)

When the user accept the impact of resetting the PIN and clicks **Continue**, the user will be provided with a dialog box to create a new PIN. Also, the user can click on **PIN requirements** to view the requirements for the new PIN. In my case it will show the *Windows Hello for Business* settings as configured in the *Windows enrollment* section of Microsoft Intune.

[](https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/IfmP_05.jpg?ssl=1)

When the user provided a new PIN and clicks **OK**, the user will be provided with the message that it’s all set. When the user than clicks on **OK**, the user will be redirected to the login screen.

[](https://i2.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/IfmP_06.jpg?ssl=1)

More information

For more information about Windows 10 and the (remote) PIN reset functionality, please refer to the following articles: