MyID MFA and PSM

Version 5.2

Self Service Portal User Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: USR2055-5.2.0

July 2025

Copyright

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

The MyID MFA and PSM Self Service Portal is a website that allows end users to perform simple tasks without having to get help from the IT helpdesk.

Note: MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

You can:

- Add and manage your own mobile/cell phone, tablet or PC so that it can be used as a Multi-Factor token – you can add up to 10 devices.
- Update your Grid pattern, One Time Code, OATH and YubiKey PIN codes, answer the Phrase security questions, and manage your FIDO tokens.
- Change your Mobile / Cellular phone number.
- Reset and unlock your network (Active Directory) password.

Note: Your IT administrator may have disabled some of these features.

1.1 Language requirements

The MyID Self Service Portal is available in the following languages:

- English
- German

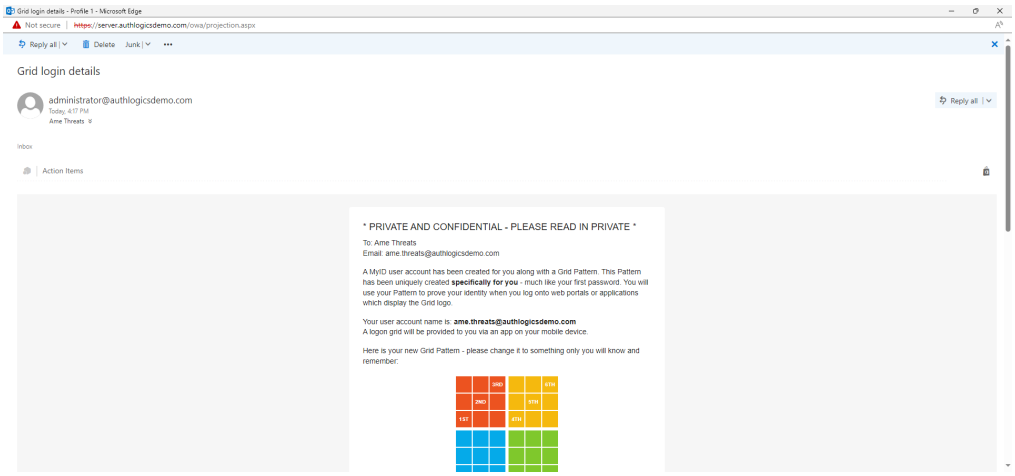
Content appears in the primary language of the browser, assuming it is supported. If the primary language of the browser is unsupported, content is shown in English.

Note: The "Self Service Portal" text strings in the window title and at the top of the page are not translated. If you want to translate this text, you must create and customize the `appsettings.Production.json` file for the Self Service Portal. See the *SSP customization* section in the ***MyID Authentication Server Installation and Configuration Guide*** for details.

Product support and documentation are available only in English.

2 Accessing the Self Service Portal

When you are first enabled to use MyID, you may receive a welcome email containing your initial logon information and a link to the Self Service Portal. If you do not have the welcome information, contact your IT team.

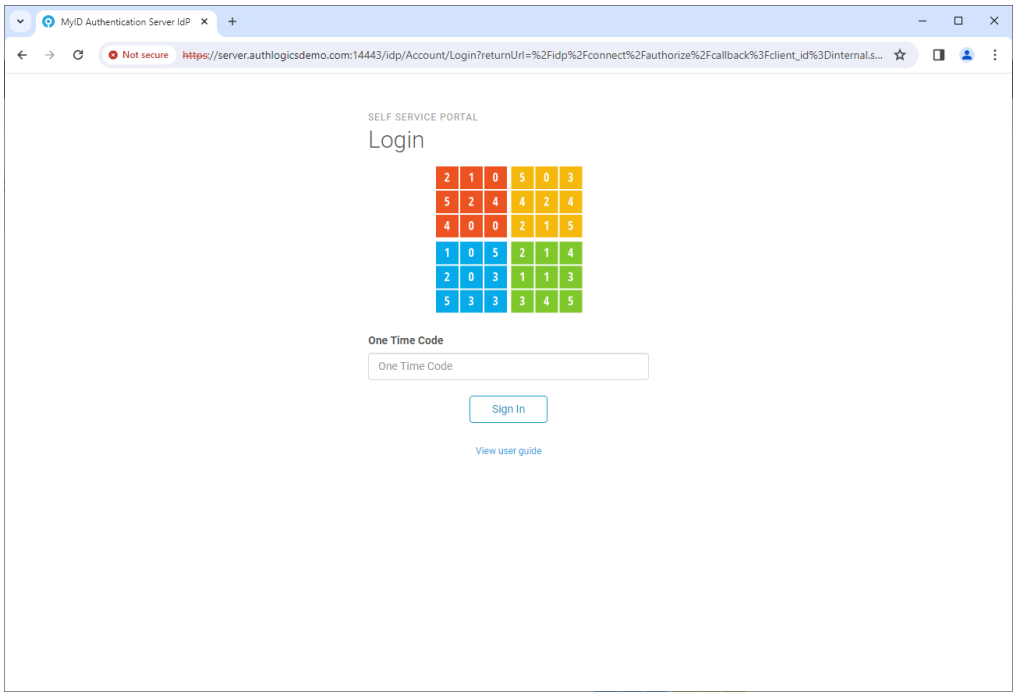


Once you have received your welcome email, you can log on. See section *2.1*, *Your first logon*.

2.1 Your first logon

To log on to the Self Service Portal for the first time:

1. Click the link in your welcome email to open the Self Service Portal in your browser.



2. Enter your **Username** and **Passcode** and click **Sign in**.

   Note: You can find your login details by using the information in the welcome email.

3 Updating your account

You can use the Self Service Portal to update the details of your account.

Using the portal, you can:

- Change the phone number on your account.

  See section *3.1*, *Changing your phone number*.
- Reset your password.

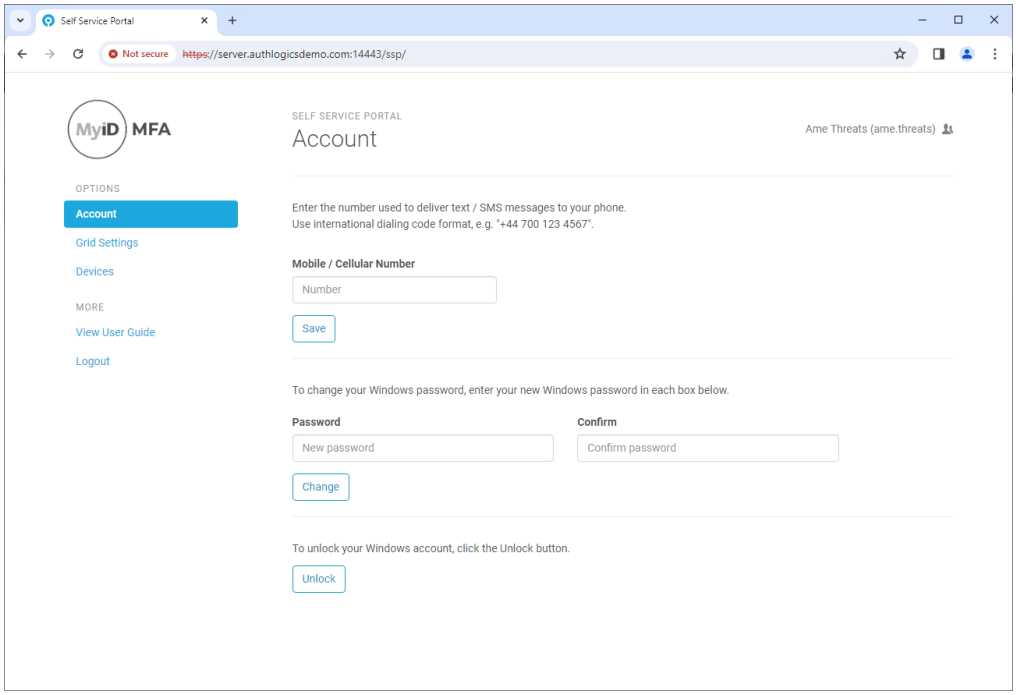
  See section *3.2*, *Resetting your password*.
- Unlock your account.

  See section *3.3*, *Unlocking your account*.

3.1 Changing your phone number

To change your phone number:

1. Select **Account** from the menu.



2. Enter your new number.
3. Click **Save** to apply the changes.

   If successful, the following message appears:

   Your Mobile / Cellular phone number was updated successfully.

   If you get the following error, you must log out and reauthenticate:

   Your account has changed. Please log out and log in again to continue.

3.2 Resetting your password

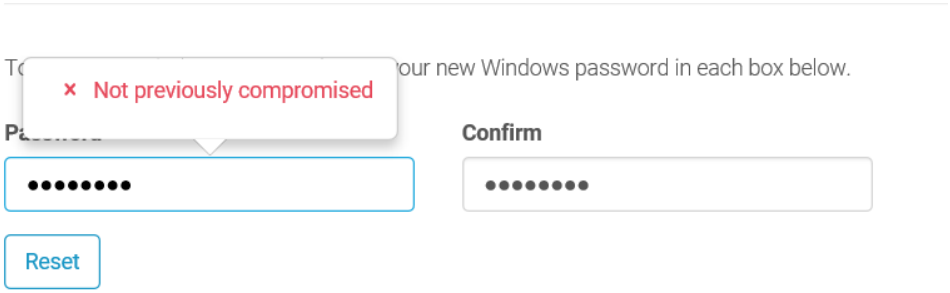
To reset your network password:

1. Select **Account** from the menu.
2. Enter your new **Password** and **Confirm** it.

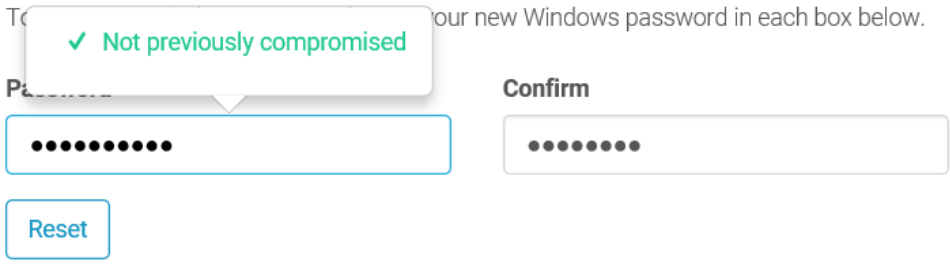
   A popup balloon may appear that helps guide you through choosing a new password that meets your company policy and is secure.

   Once all the items in the balloon have green ticks, you know your new password is safe to use.

   If you choose a bad password, the balloon is similar to:



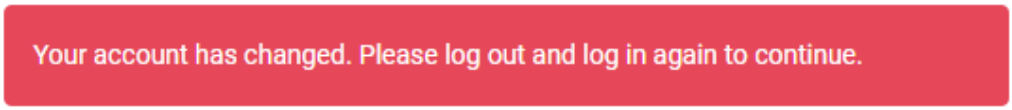
   If you choose a good password, the balloon is similar to:



3. Click **Reset** to save the new password.

   If successful, the following message appears:

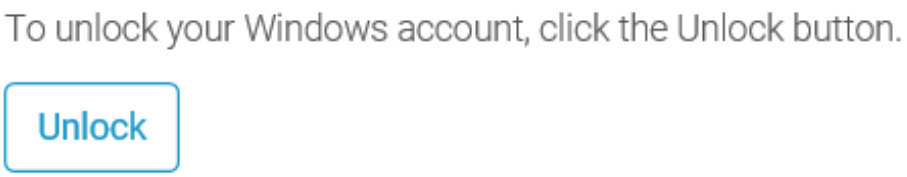
   If you get the following error, you must log out and reauthenticate:



3.3 Unlocking your account

If your network account has been locked out, you can unlock it yourself instead of waiting for your IT team to do it for you:

1. Select **Account** from the menu.



2. Click **Unlock**.

   If successful, the following message appears:

4 Changing your multi-factor authentication settings

You can use the Self Service Portal to change your multi-factor authentication settings; for example, you can change your Grid pattern, or set your Phrase answers.

Using the portal, you can:

- Change the grid pattern.

  See section *4.1*, *Changing your Grid pattern*.
- Set the answers for your security phrases.

  See section *4.2*, *Settings your Phrase answers*.
- Change the settings for your One Time Codes.

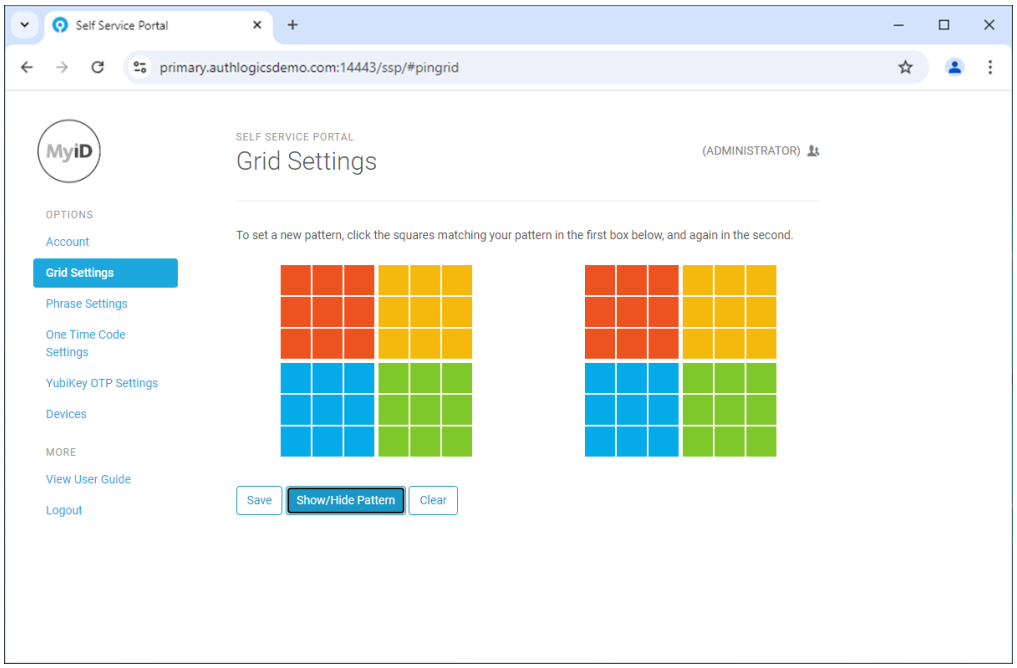
  See section *4.3*, *Changing your One Time Code settings*.
- Change the settings for your YubiKey OTP.

  See section *4.4*, *Changing your YubiKey OTP settings*.

4.1 Changing your Grid pattern

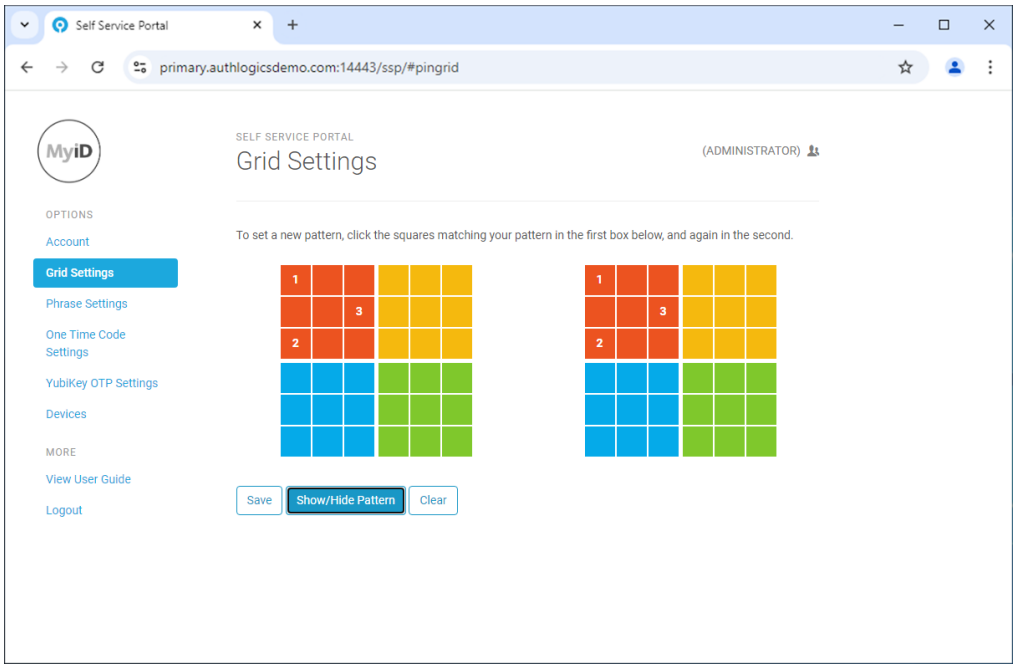
To change your Grid pattern:

1. Select **Grid Settings** from the menu.



2. On the first grid, click the squares you will use for your new pattern.

3. Click the same squares on the second grid to confirm your new pattern.



The squares that you click display the order they were clicked in the pattern.

Note: By default, the numbered indicators are not displayed. If your administrator allows it you can display the indicators – click **Show/Hide Pattern**.

You can click a single grid cell up to the number of uses of a single cell configured in group policy pin grid complexity settings.

If you mis-click squares, click **Clear** to start over.

4. Click **Save** to apply the changes.

   If successful, the following message appears:

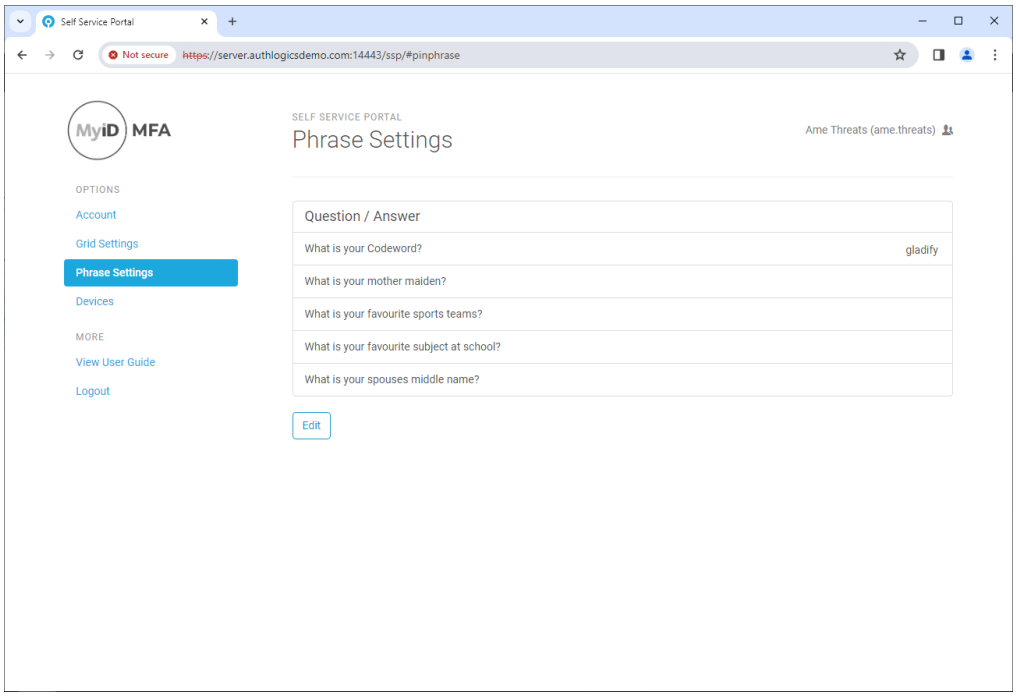
   

To configure whether or not users have the ability to display the numbered indicators, you can create and customize the `appsettings.Production.json` file for the Self Service Portal. See the *SSP customization* section in the ***MyID Authentication Server Installation and Configuration Guide*** for details.

4.2 Settings your Phrase answers

To provide answers to the Phrase questions provided by your IT team:

1. Select **Phrase Settings** from the menu.



2. To add or update your answers, click **Edit**.
3. Highlight the question you want to answer, then type your answer.

   Note: Spaces are not counted as letters, so multiple word answers are treated as a single word.
4. Click **Save** to apply the changes.

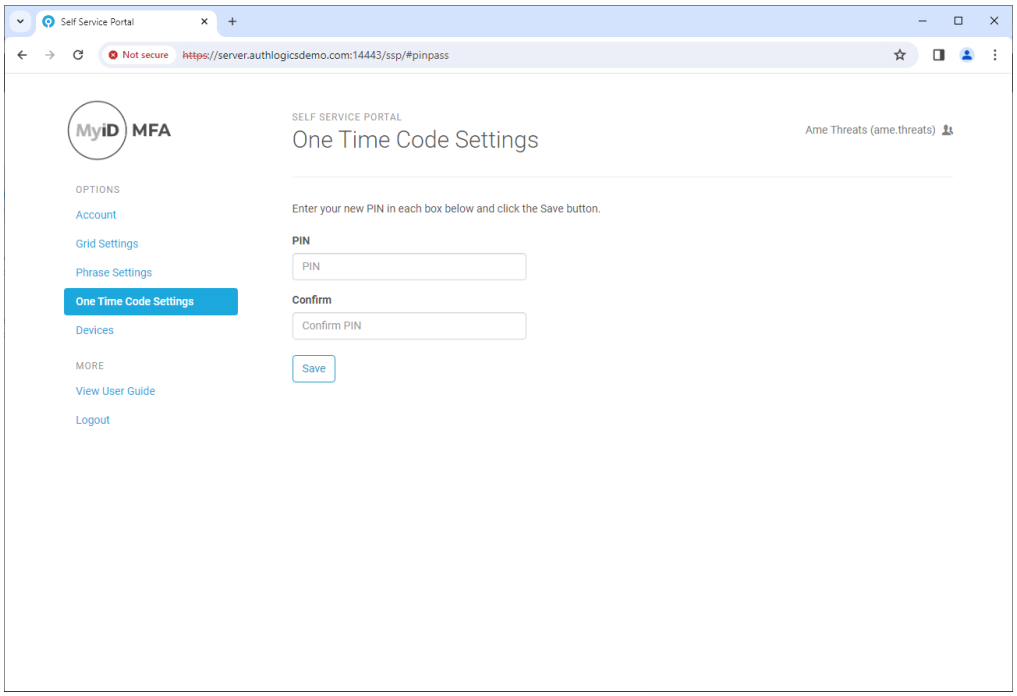
   If successful, the following message appears:

   Phrase answers have been successfully updated.

4.3 Changing your One Time Code settings

To change your One Time Code PIN:

1. Select **One Time Code Settings** from the menu.



2. Enter your new **PIN** code and **Confirm** it.
3. Click **Save** to apply the changes.

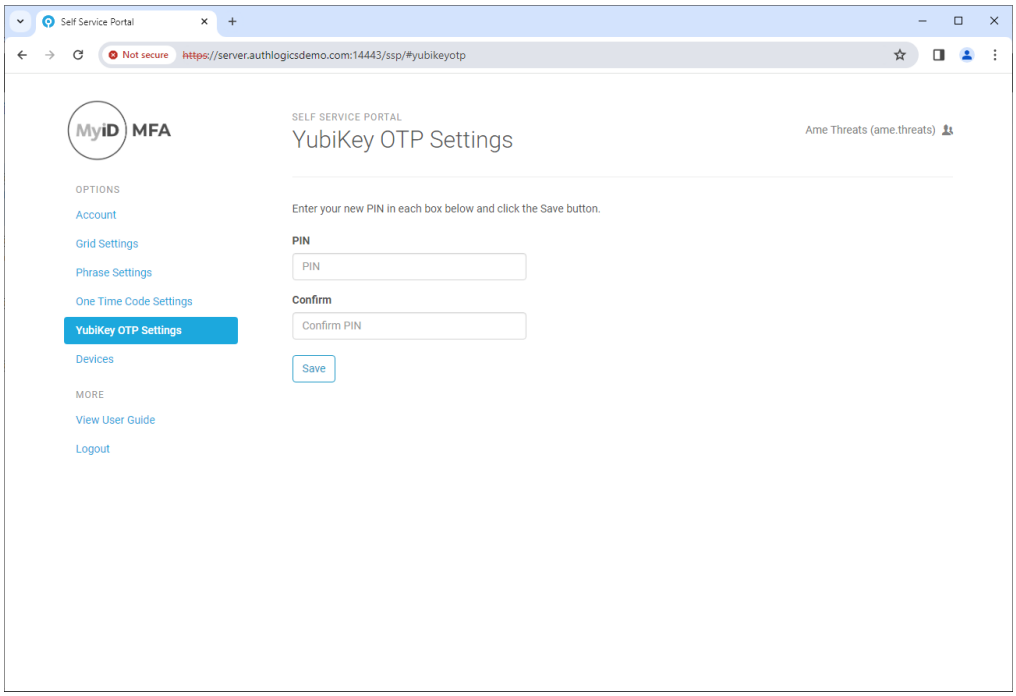
   If successful, the following message appears:

   Your PIN was updated successfully.

4.4 Changing your YubiKey OTP settings

To change your YubiKey OTP PIN:

1. Select **YubiKey OTP Settings** from the menu.



2. Enter your new **PIN** code and **Confirm** it.
3. Click **Save** to apply the changes.

   If successful, the following message appears:

   Your PIN was updated successfully.

5 Setting up your own device

MyID MFA supports several authentication technologies. These technologies include:

- MyID MFA technologies PUSH, One Time Code, and Grid authentication.
- YubiKey OTPs
- FIDO tokens.
- Passkeys and standard OATH authenticators such as Google and Microsoft Authenticator.

The following sections detail how to enable the various technologies supported within MyID MFA:

- Information on obtaining and using the MyID Authenticator app.

  See section *5.1*, *MyID Authenticator app*.
- Information on using alternative authenticator apps.

  See section *5.2*, *Other authenticator apps*.
- Information on using YubiKey devices.

  See section *5.3*, *YubiKey OTP*.
- Information on using Passkey / FIDO tokens.

  See section *5.4*, *Passkey / FIDO Token*.
- Instructions for editing devices.

  See section *5.5*, *Editing devices*.
- Instructions for removing devices.

  See section *5.6*, *Removing devices*.

5.1 MyID Authenticator app

The first step is to install the MyID Authenticator app. The app is available on the following online stores as a free download:

Note: When installing the MyID Authenticator app, ensure that the device's clock and time zone are correct; otherwise, you may not be able to log on with the app.

5.1.1 Legacy Authlogics Authenticator app

If you are using MFA version 5.0.6 or earlier, you can continue to use the older Authlogics Authenticator app; however, if you are using MFA 5.0.7 or later, you are recommended to use the MyID Authenticator app. Credentials are not shared between the apps.

5.1.2 Alternative Authenticator apps

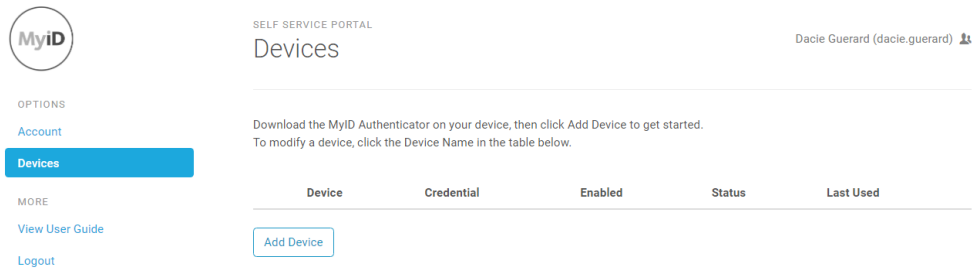
As an alternative, you can download a third-party OATH app from the relevant vendor. For example, you can use Microsoft or Google Authenticator.

5.1.3 Adding your MyID Authenticator device to your account

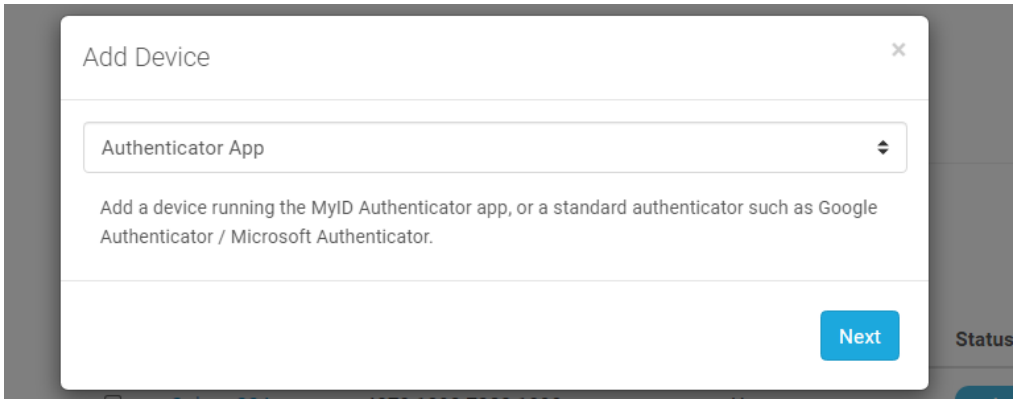
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

To add a device to your account:

1. Log on to the Self Service Portal and select **Devices** from the menu.

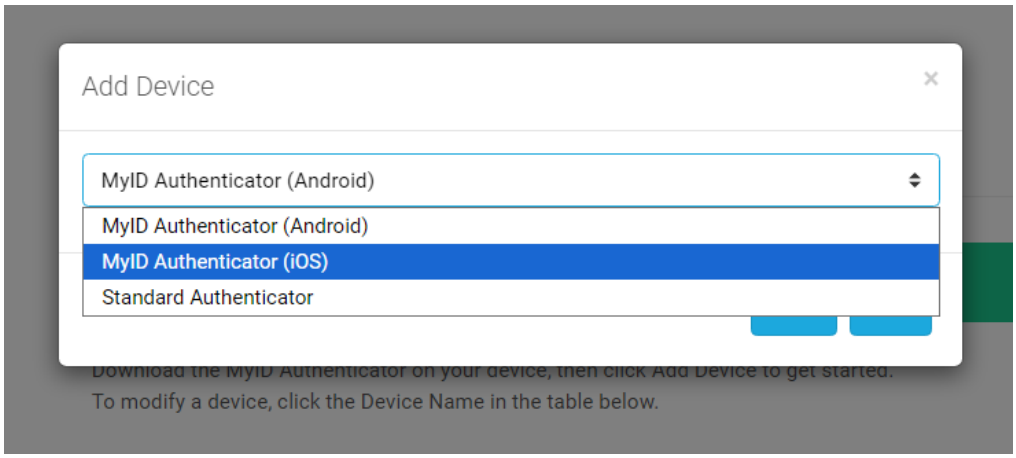


2. Install the MyID Authenticator App from the relevant App Store using the buttons on your device.
3. Click **Add Device**.



4. From the drop-down list, select **Authenticator App**.

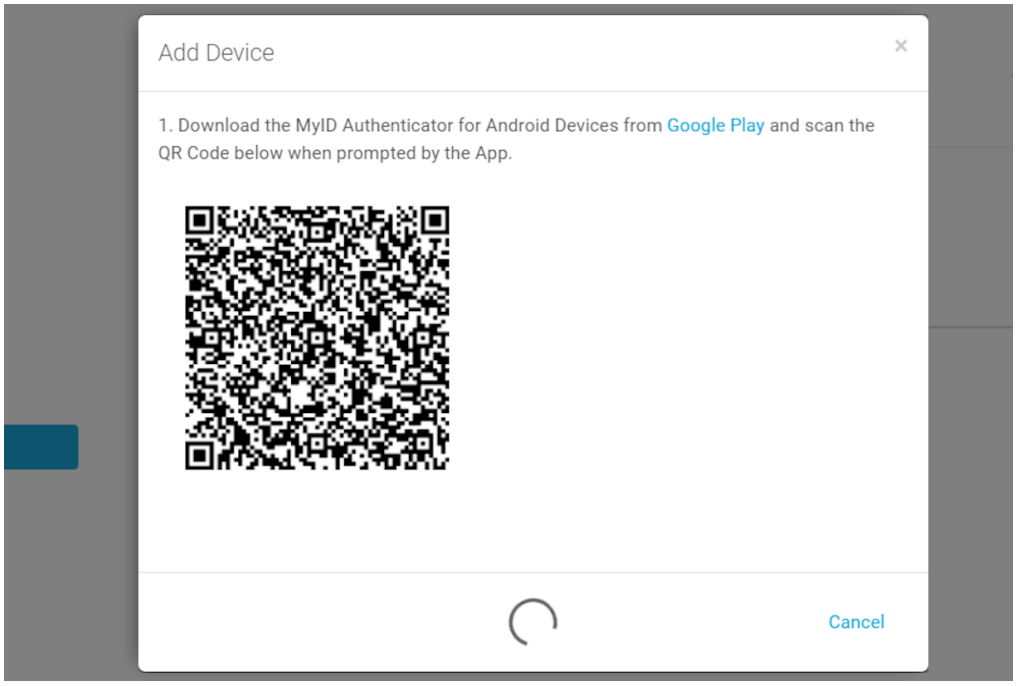
5. From the list, choose the type of device you have.



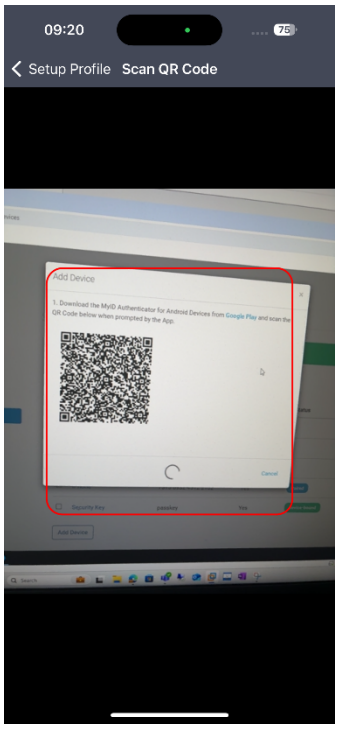
MyID Authenticator (Android) and **MyID Authenticator (iOS)** both relate to the MyID MFA app.

Standard Authenticator relates to third-party OAUTH tokens; see section *5.1.2*, *Alternative Authenticator apps* for details.

6. Click **Next**.



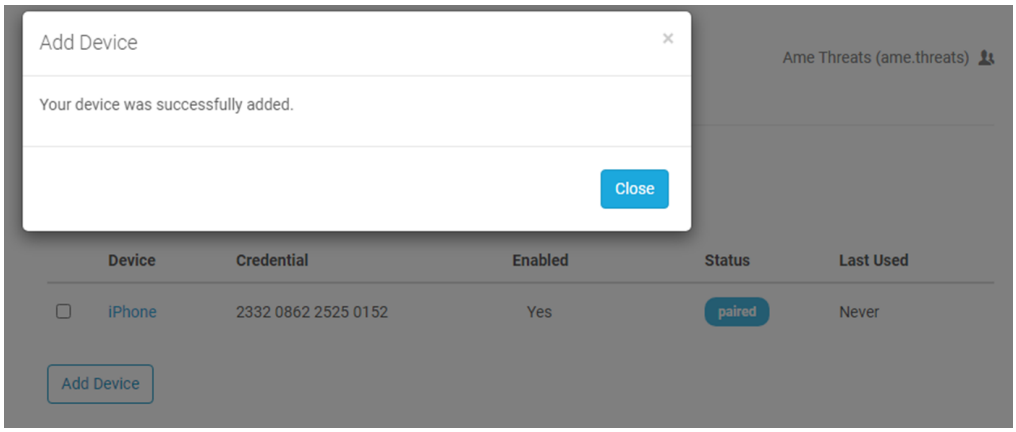
7. Scan the QR code with the MyID Authenticator App.



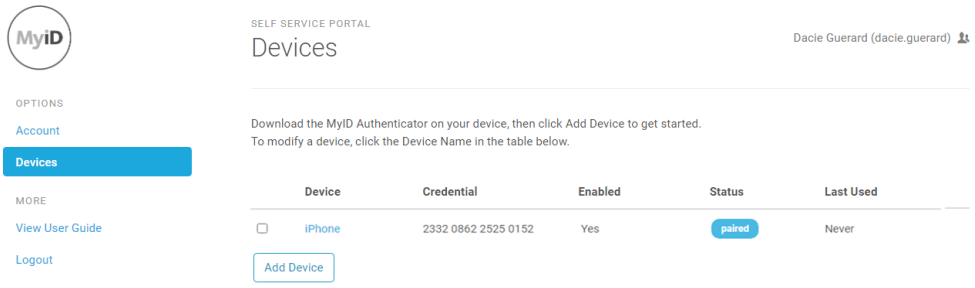
Device setup is complete.

Finish

8. Click **Finish**.



9. Click **Close**.



The new device is now visible under **Devices**. Your device is now ready for use as a multi-factor authentication token for your MyID account.

5.2 Other authenticator apps

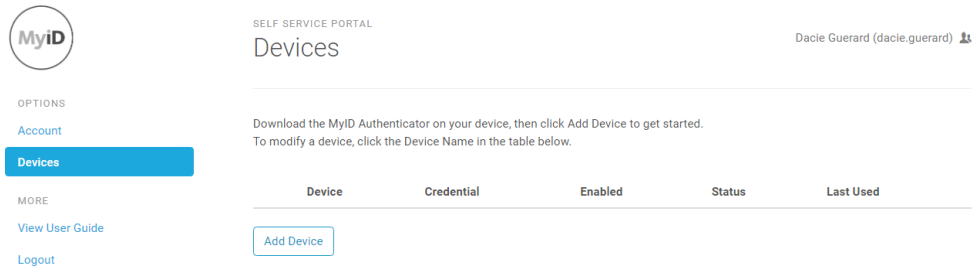
As an alternative to the MyID Authenticator app, you can download a third-party OATH app from the relevant vendor. For example, you can use Microsoft or Google Authenticator.

5.2.1 Adding your standard authenticator device to your account

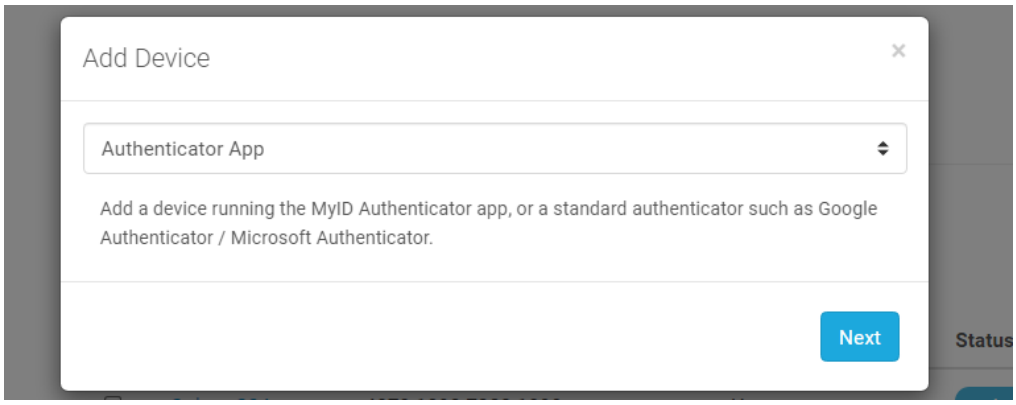
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

To add a standard authenticator device with third-party OATH tokens to your account:

1. Log on to the Self Service Portal and select **Devices** from the menu.

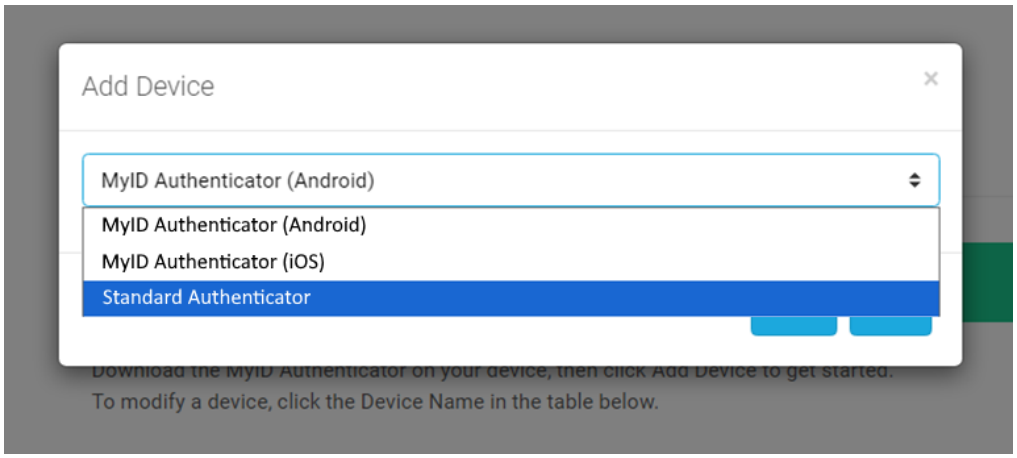


2. Install the relevant third-party app on your device.
3. Click **Add Device**.

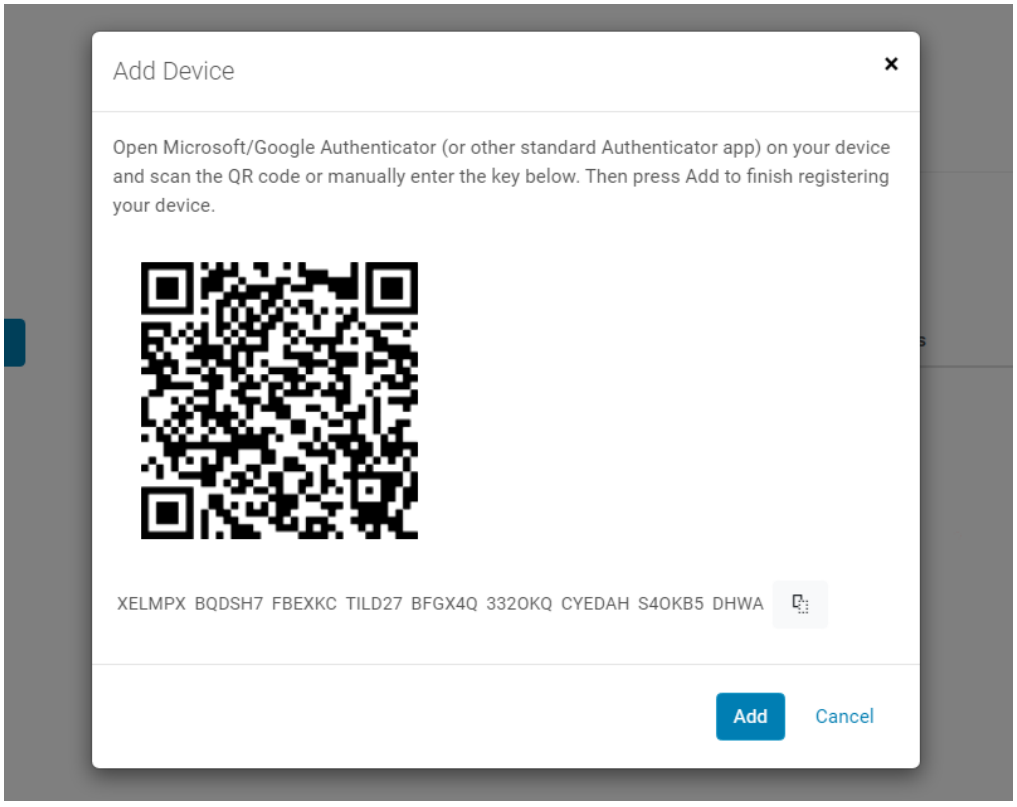


4. From the drop-down list, select **Authenticator App**.

5. From the list, choose **Standard Authenticator.**

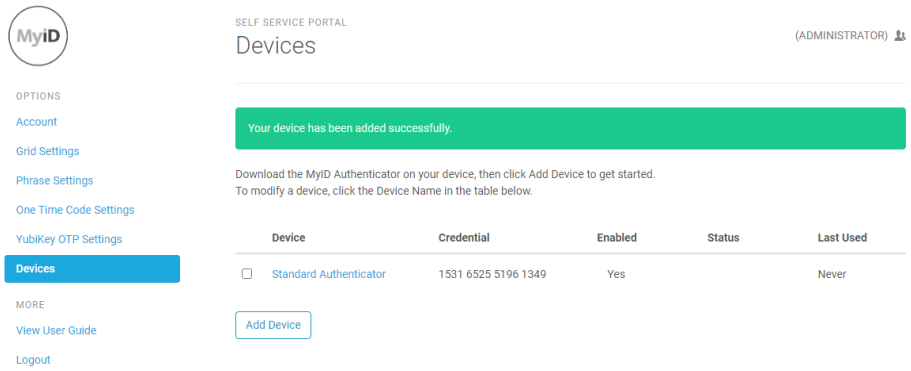


6. Click **Next**.



7. Add the code to your third-party authenticator app; you can either scan the QR code or input it manually.

8. Click **Add**.



The new device is now visible under **Devices**. Your device is now ready for use as a multi-factor authentication token for your MyID account.

5.3 YubiKey OTP

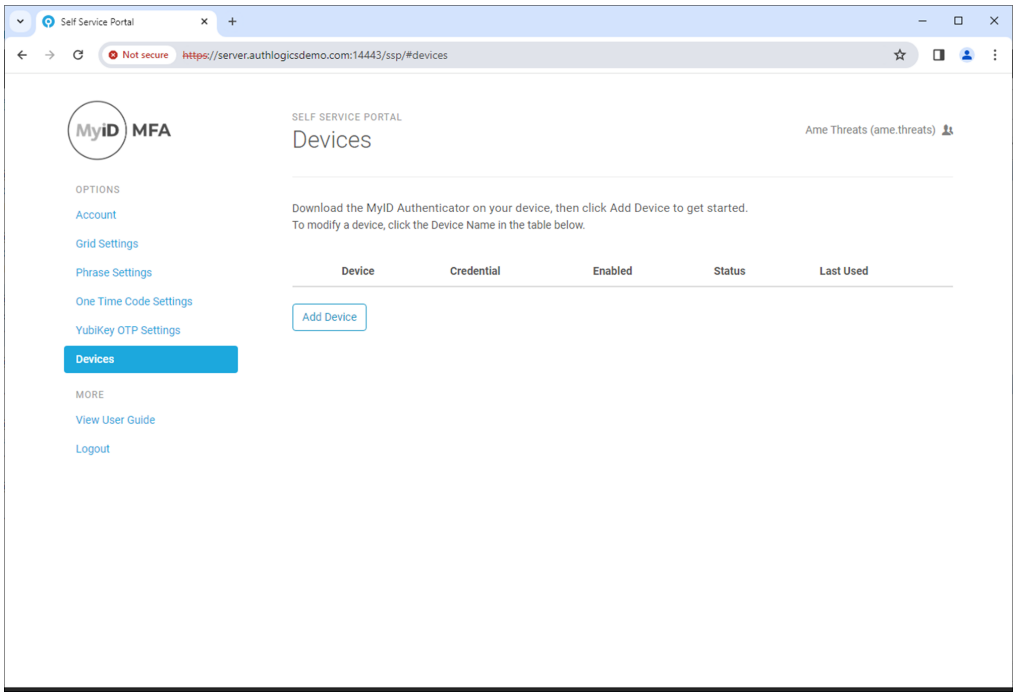
To provision your YubiKey OTP hardware device, insert the YubiKey token into your PC.

5.3.1 Adding your YubiKey device to your account

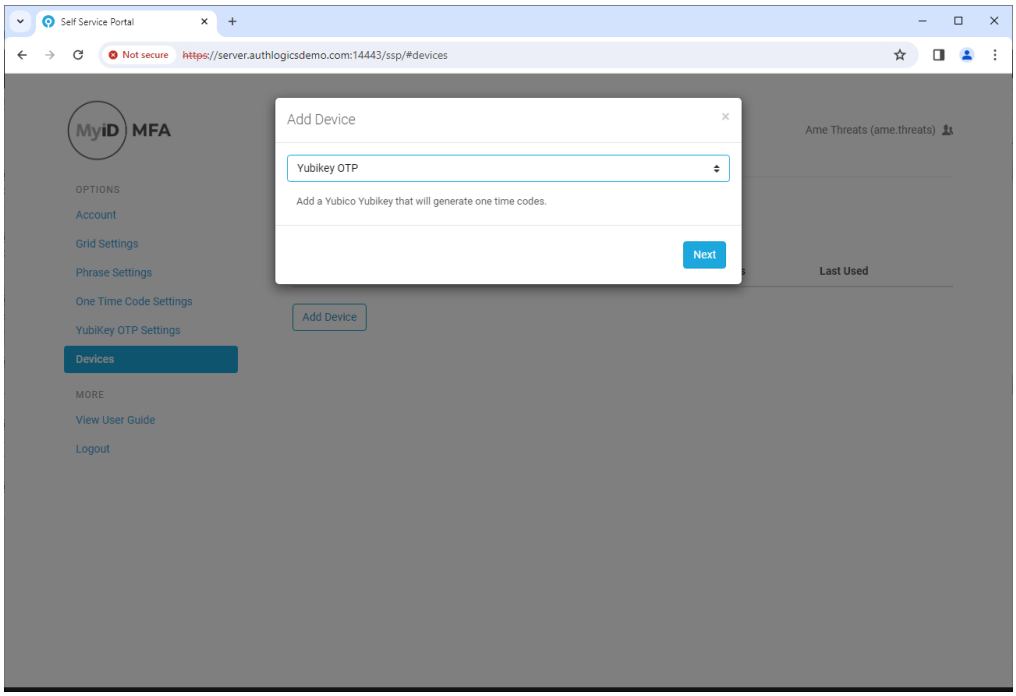
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

To add a device to your account:

1. Log on to the Self Service Portal, and select **Devices** from the menu.

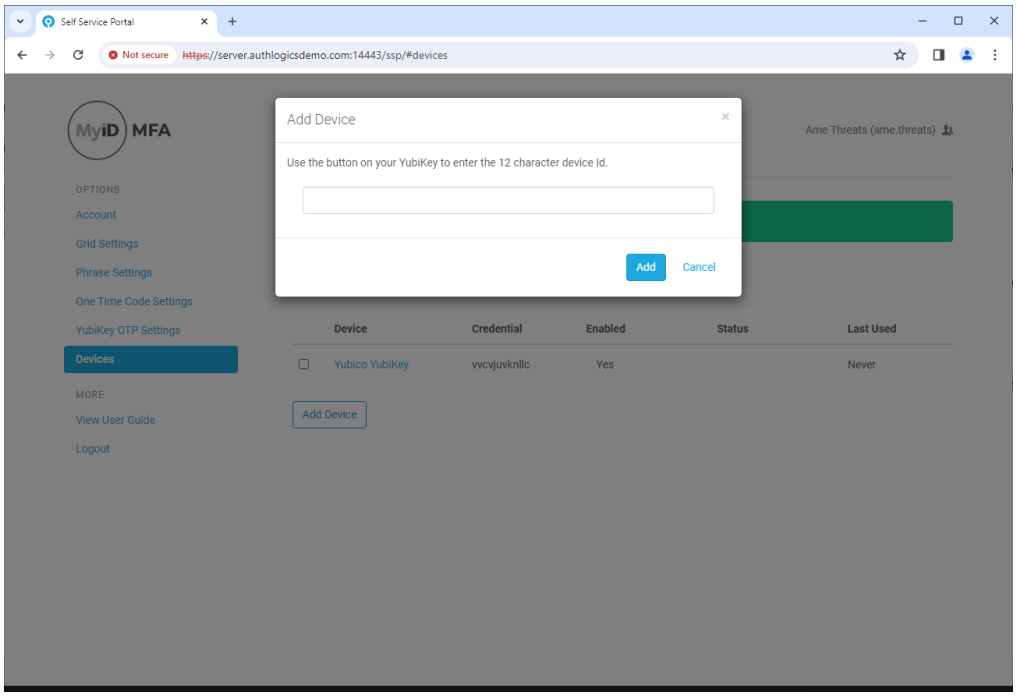


2. Click **Add Device**.

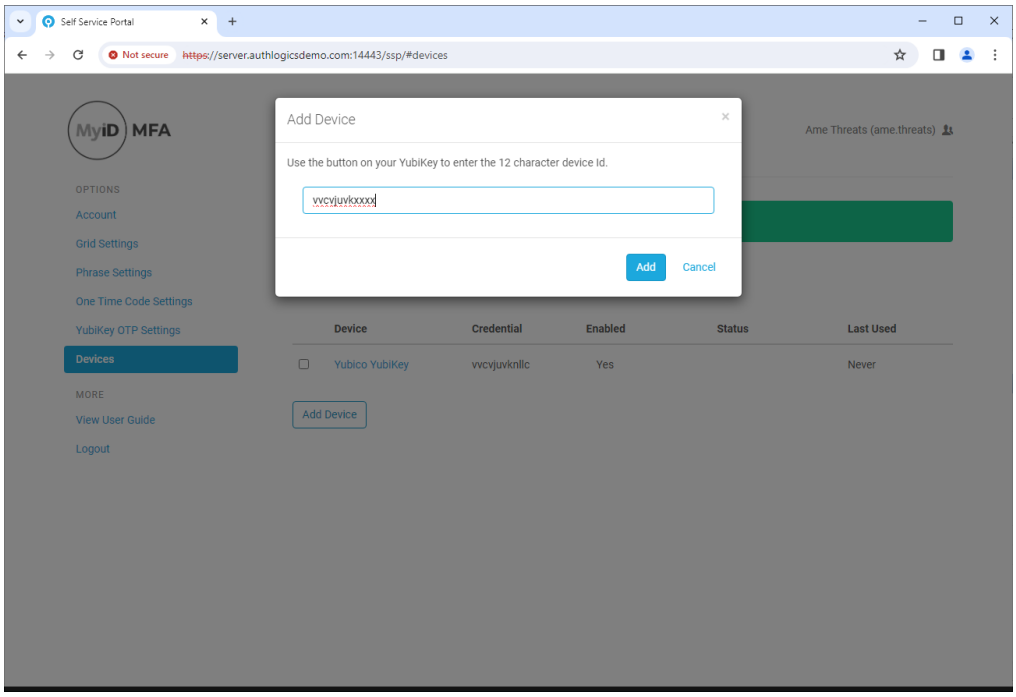


Note: If this option is not available, your user account has not been set up to use YubiKey tokens. Contact your administrator for assistance.

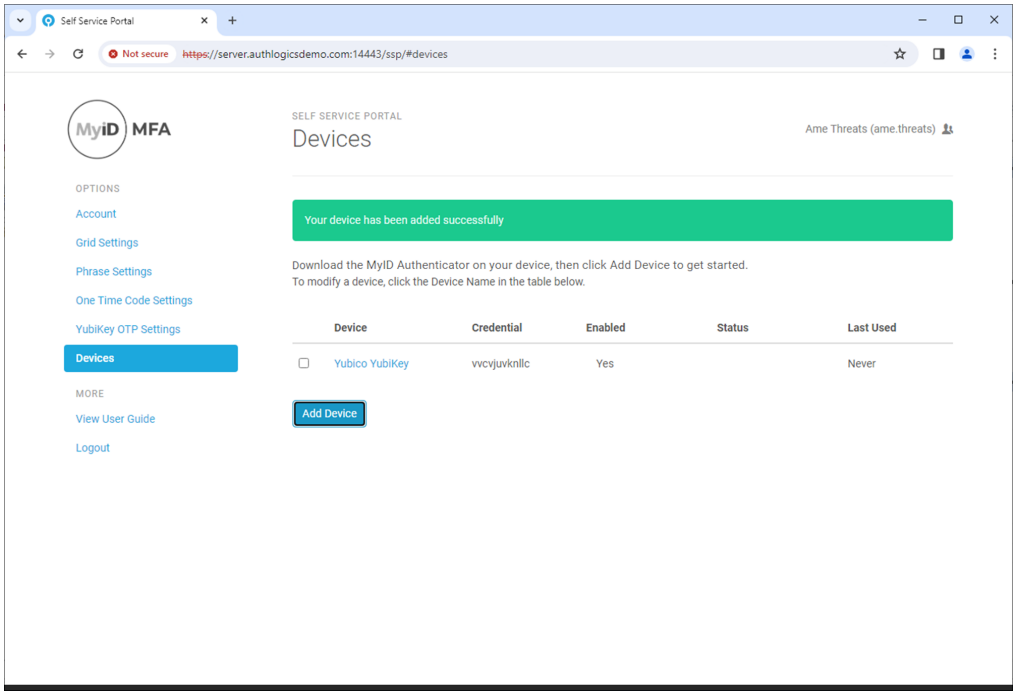
3. Select **YubiKey OTP** and click **Next**.



4. Insert your YubiKey OTP and press the YubiKey button.



5. Once the unique YubiKey ID is displayed in the edit box, click **Add**.



The new device is now visible under **Devices**.

5.4 Passkey / FIDO Token

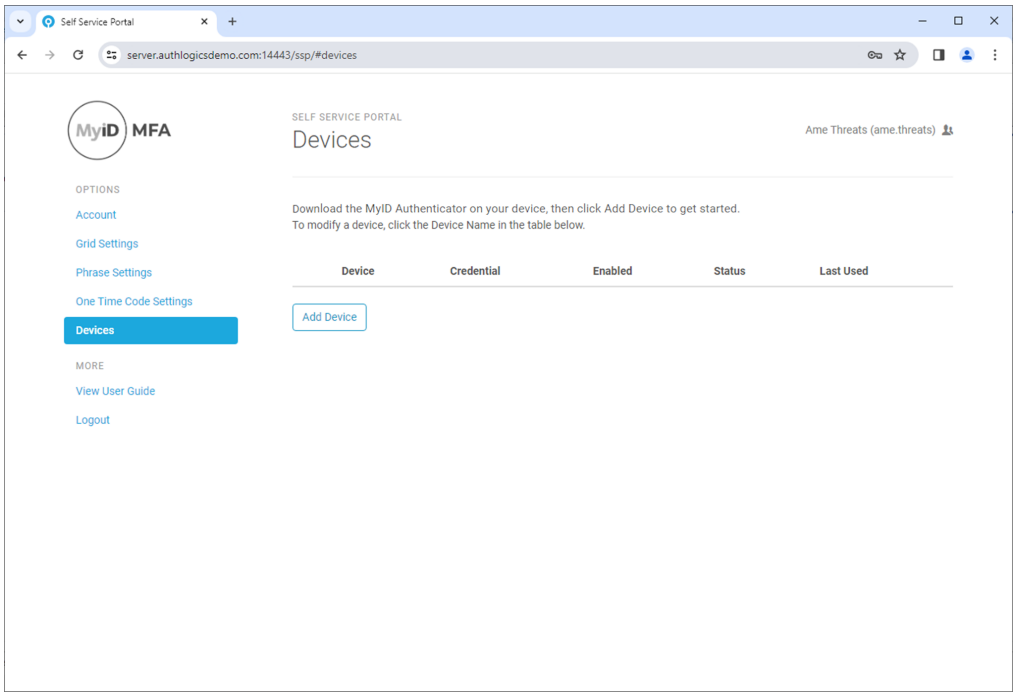
Before adding your FIDO Security Key or a Passkey to your account, ensure that no other MFA devices are attached to the workstation and that you have disconnected all Passkey / FIDO tokens from your PC.

5.4.1 Adding your FIDO / Security Key device to your account

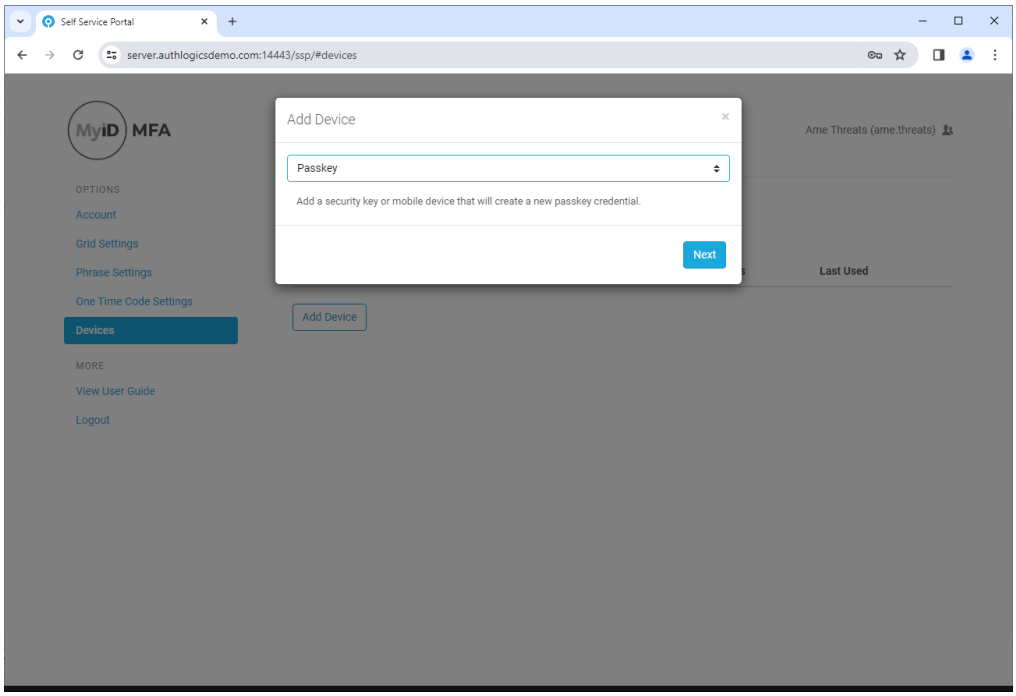
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

To add a FIDO Passkey Security Key to your account:

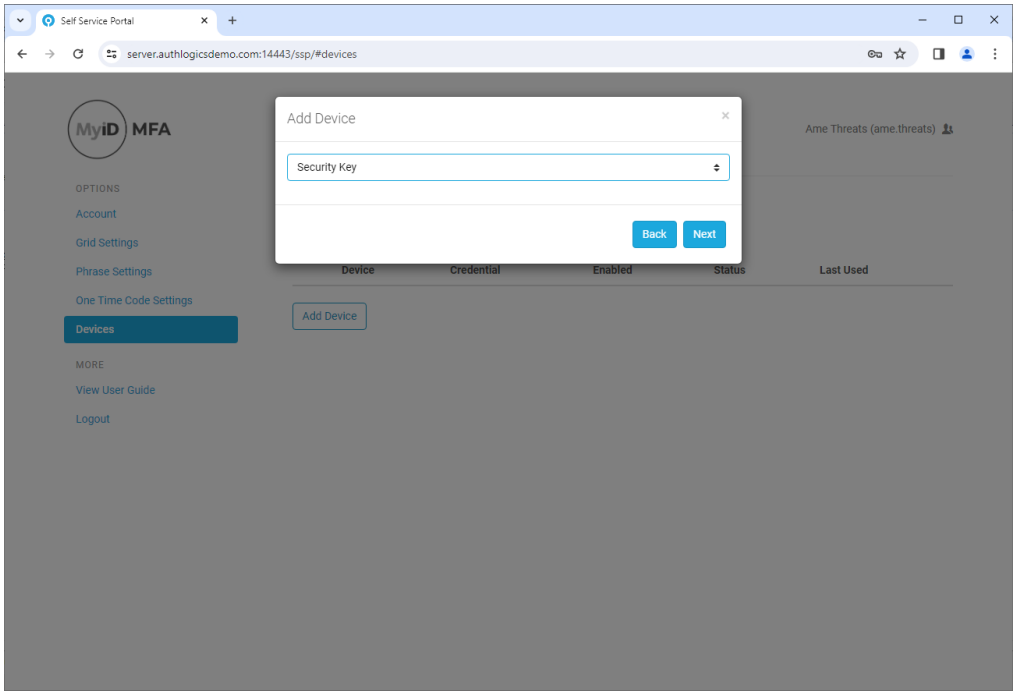
1. Log on to the Self Service Portal, and select **Devices** from the menu.



2. Click **Add Device**.



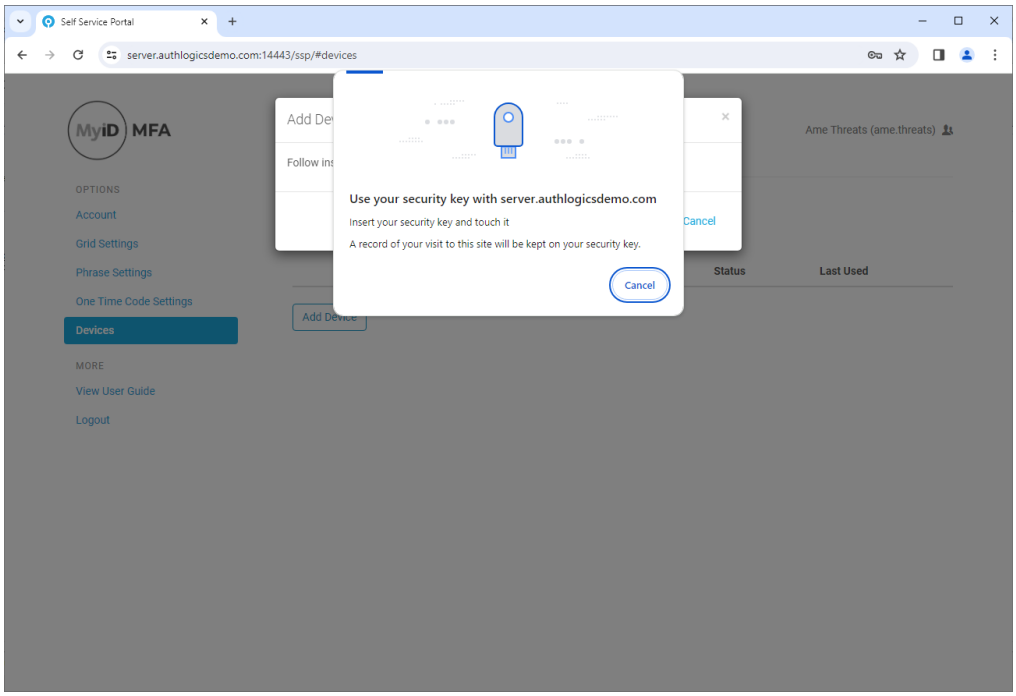
3. Select **Passkey** and click **Next**.



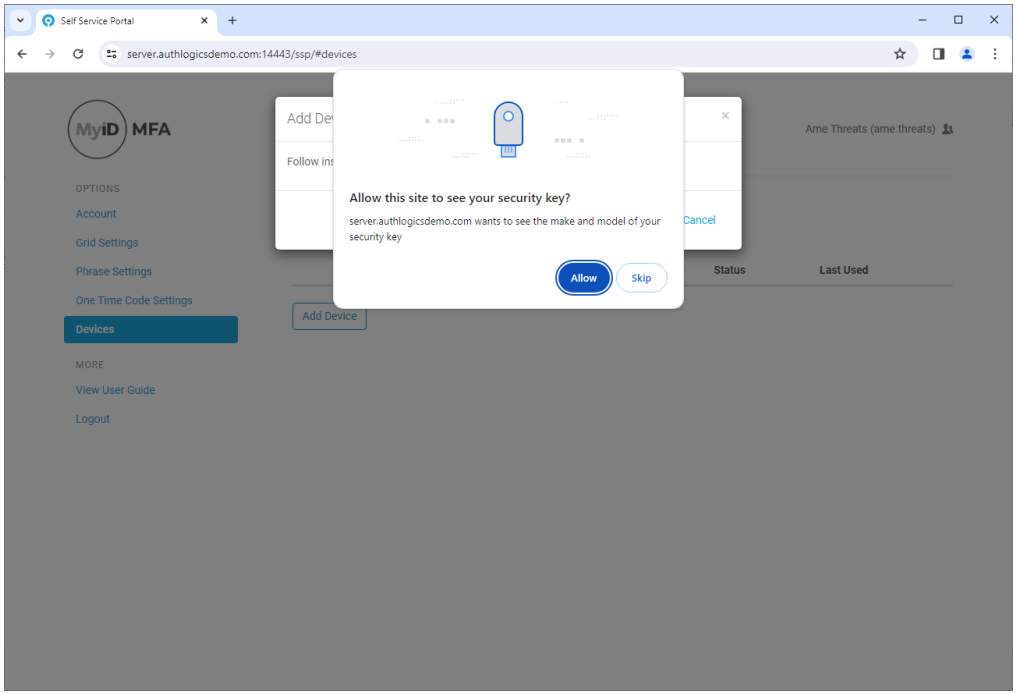
Note: If this option is not available, your user account has not been set up to use Passkeys. Contact your administrator for assistance.

You can provision a maximum of two device-bound passkeys to one account. If you have more than two device-bound passkeys already enabled, the option to add more is not available.

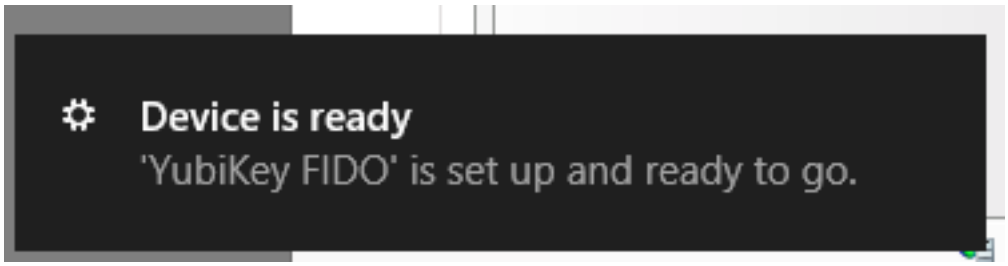
4. Select **Security Key** and click **Next**.



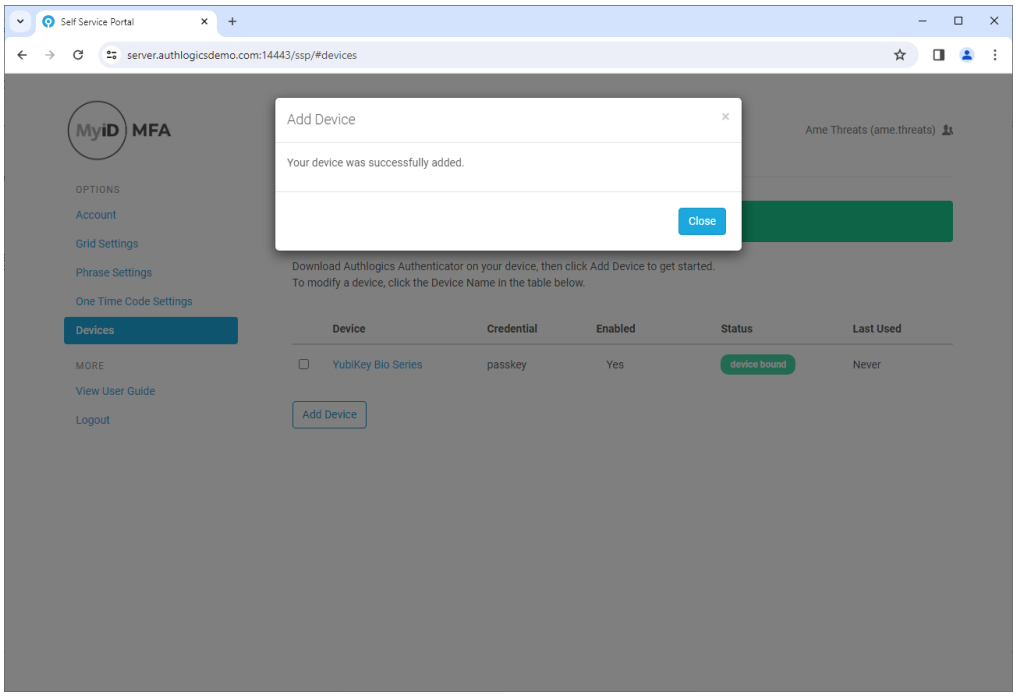
5. Insert your security key and press the FIDO token's button.



6. When prompted, Click **Allow**.

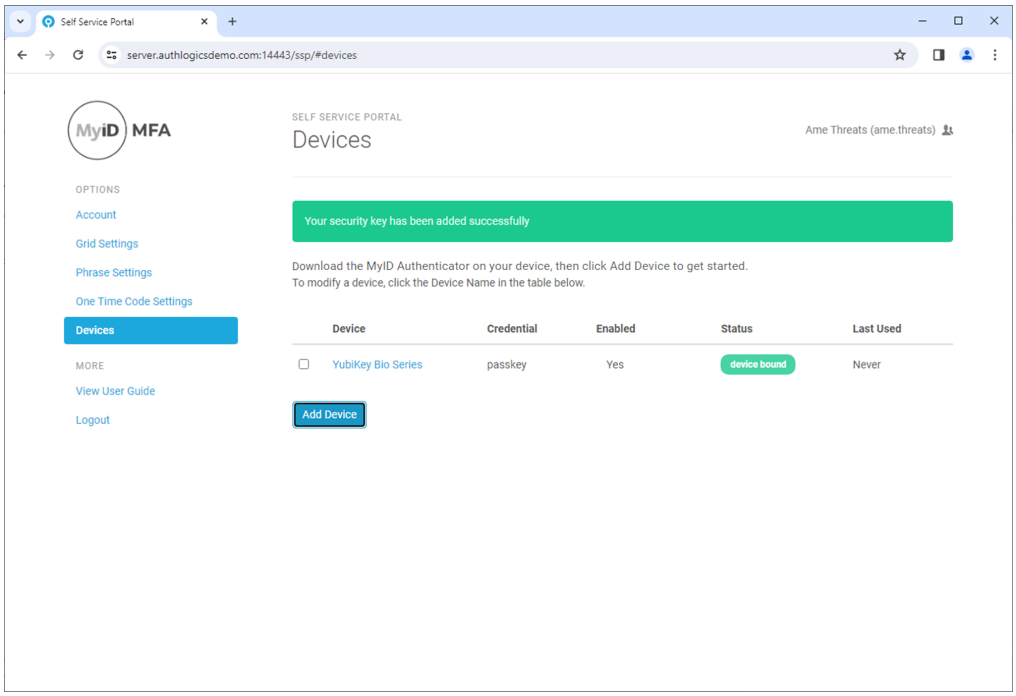


The underlying system notifies you that the FIDO token is set up and ready for use.



The device has been successfully added.

7. Click **Close**.

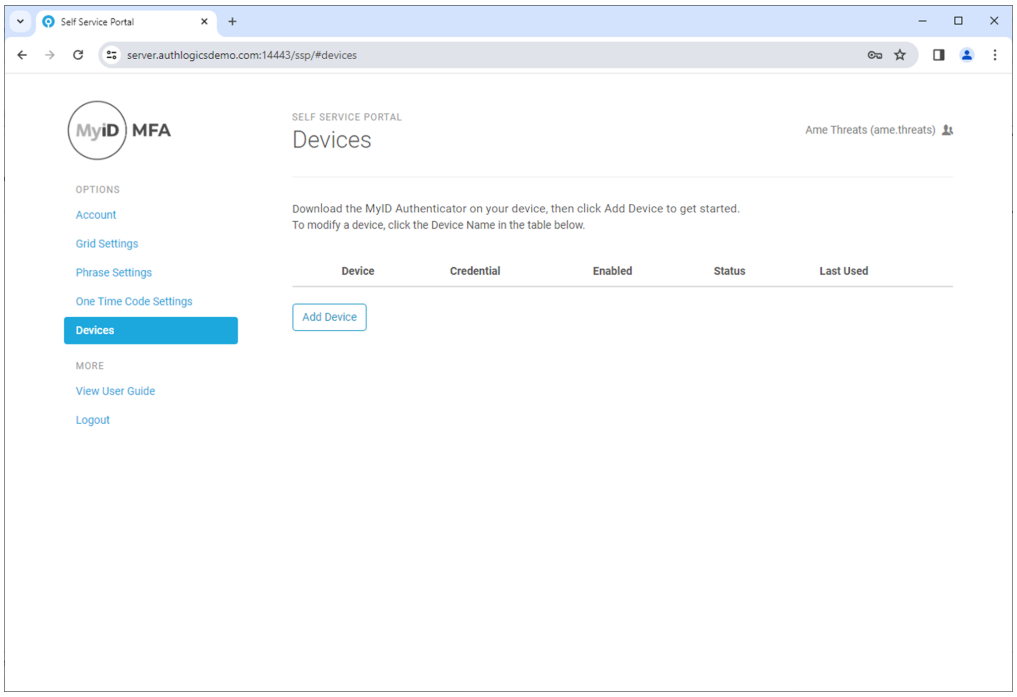


5.4.2 Adding a Synched Passkey to your account

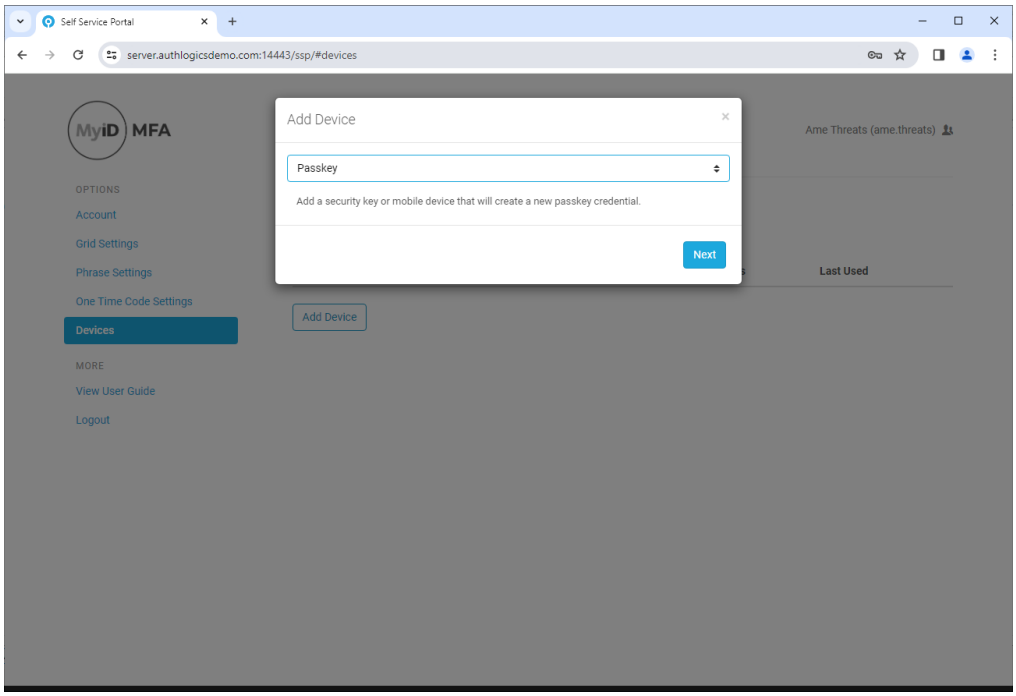
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

To add a FIDO Passkey Security Key to your account:

1. Log on to the Self Service Portal, and select **Devices** from the menu.

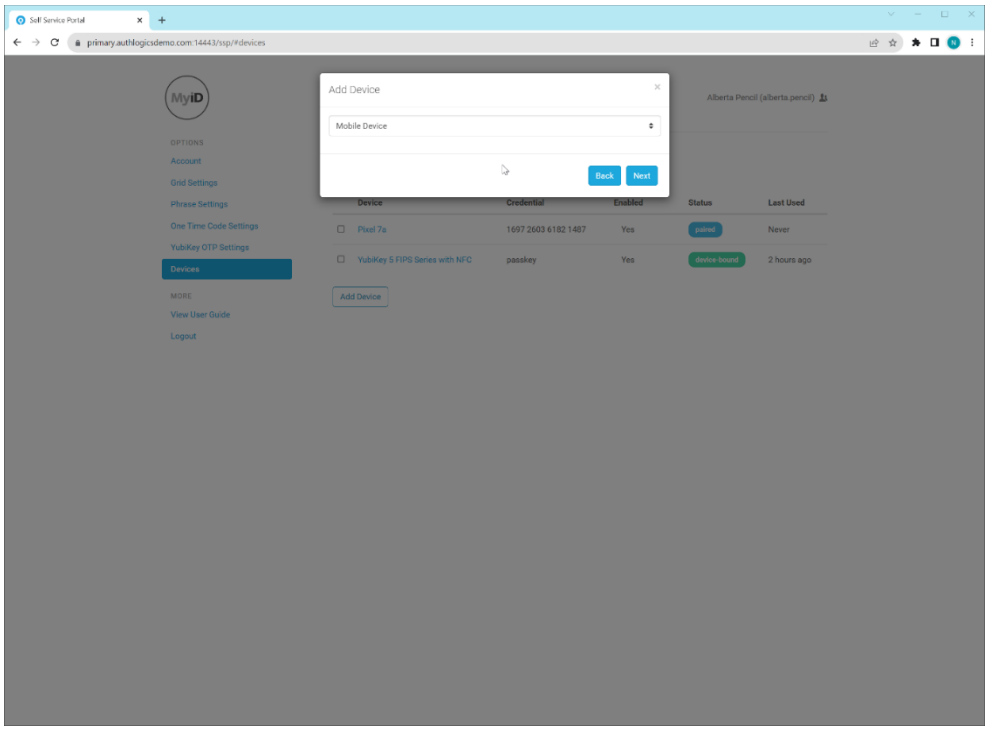


2. Click **Add Device**.

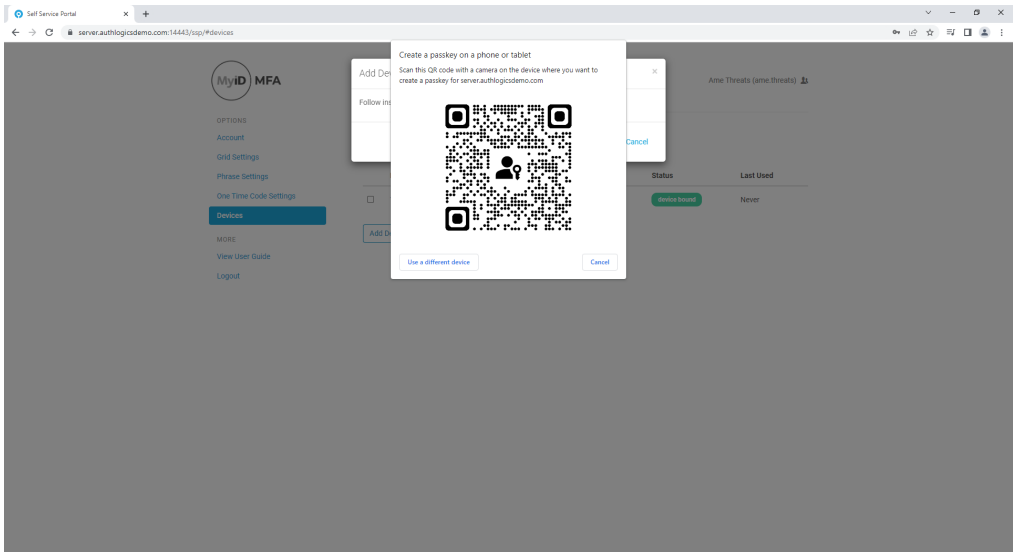


Note: If this option is not available, your user account has not been set up to use Passkeys. Contact your administrator for assistance.

3. Select **Passkey** and click **Next**.



4. Select **Mobile Device** and click **Next**.



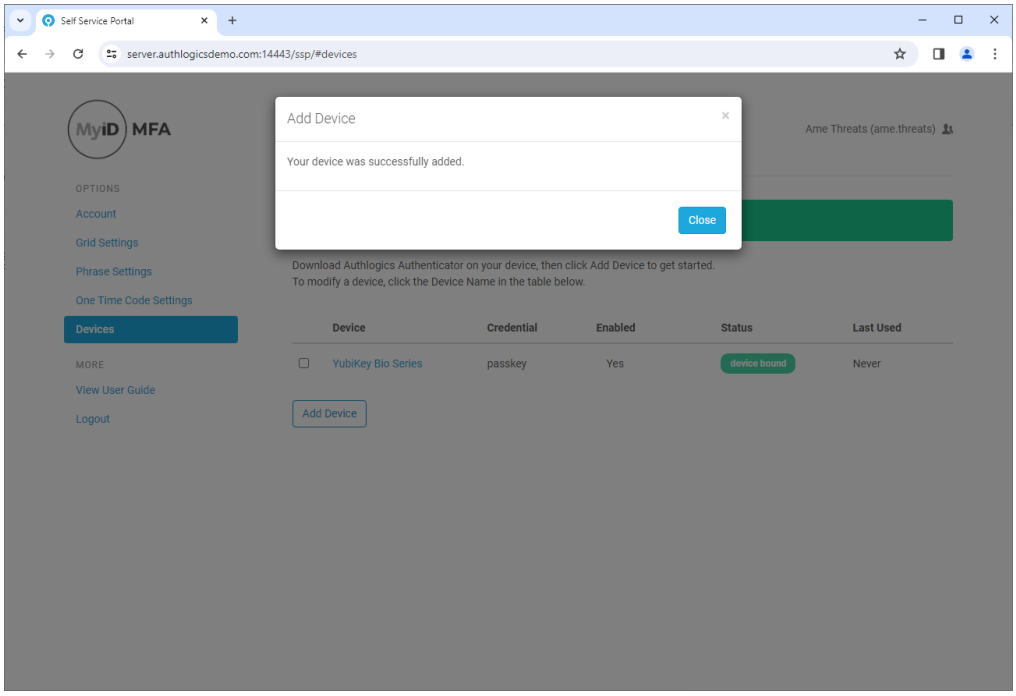
5. Ensure that Bluetooth is enabled on both the mobile device and your workstation.

   If Bluetooth is *not* enabled on your workstation, the above QR Code is not displayed.

6. Open your mobile phone's camera and scan the QR Code.

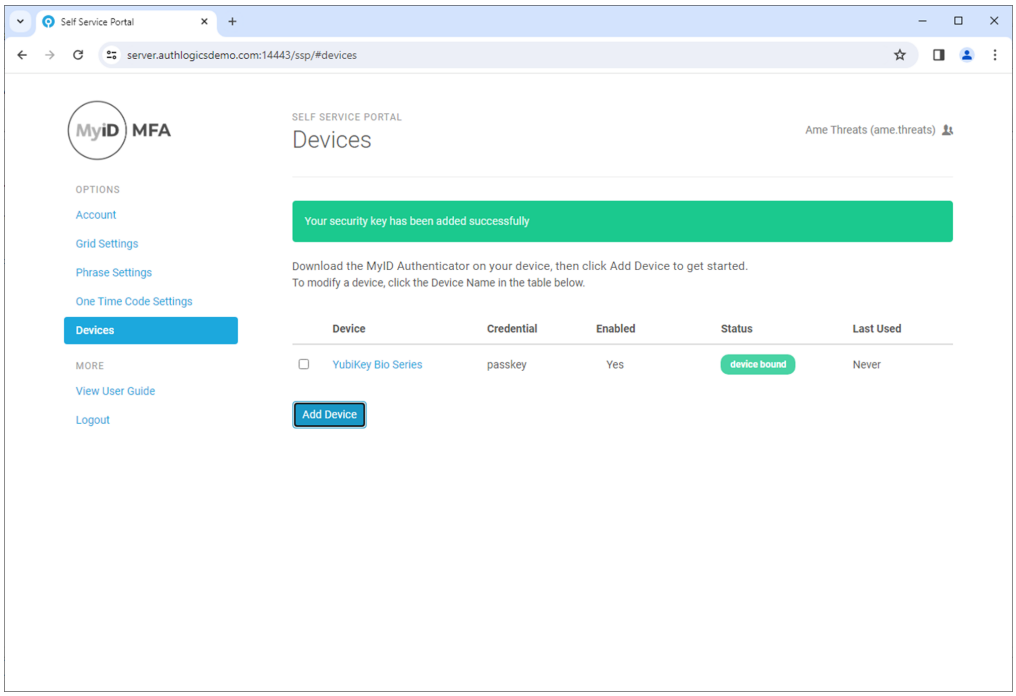
7. Once you have scanned the QR Code, follow the instructions on your mobile phone.

   The underlying system notifies you that the FIDO token is set up and ready for use.



The device has been successfully added.

8. Click **Close**.



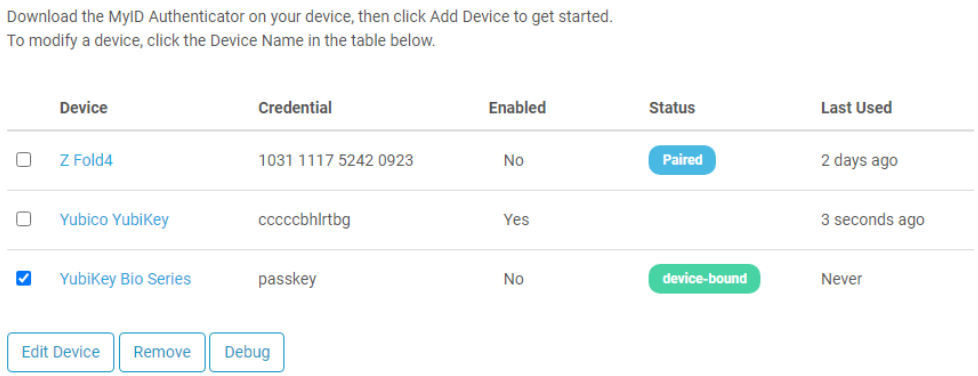
5.5 Editing devices

You can edit the name of a device, or enable or disable it using the SSP.

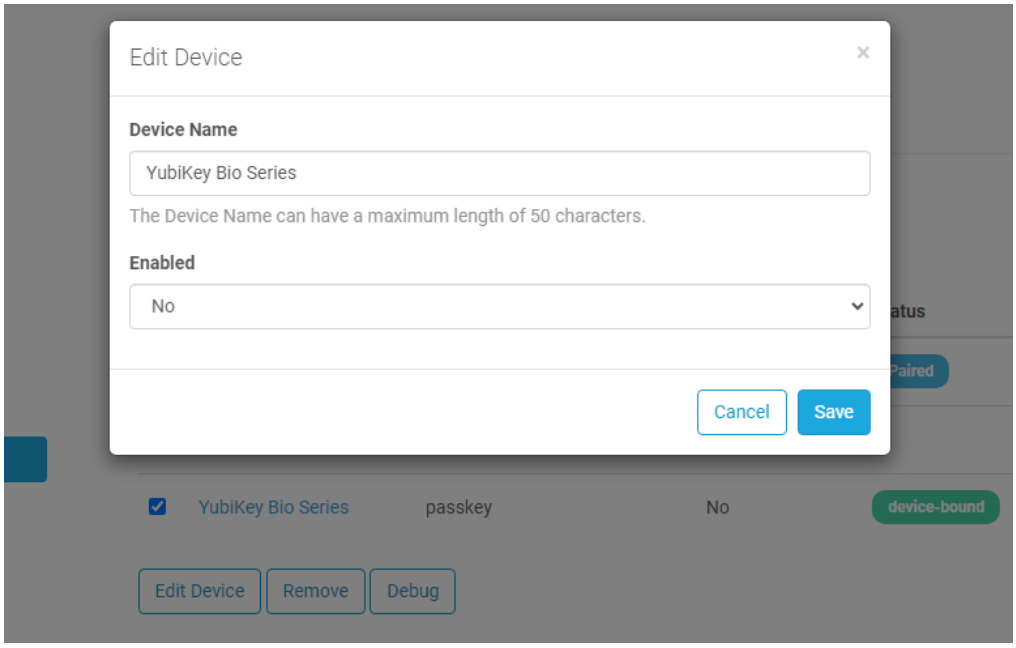
Note: To see the **Devices** menu, you must have either the **Add Token devices** option enabled, or an existing device. To be able to edit a device, you must have either the **Add Token devices** option or the **Remove Token devices** option enabled. Which options you have enabled determines what you can edit. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

To edit a device:

1. Log on to the Self Service Portal, and select **Devices** from the menu.
2. Select the device that you want to edit.



3. Click **Edit Device**.



4. To change the **Device Name**, type the new name for the device.

   Note: The device name must not be empty and can be a maximum of 50 characters long.

   Note: To change the **Device Name**, you must have either the **Add Token devices** option or the **Remove Token devices** option enabled.

5. To change the enabled status of the device, set **Enabled** to **Yes** or **No**.

   Note: To change whether the device is **Enabled**, you must have the **Remove Token devices** option enabled.

6. Click **Save**.

   The table of devices is updated with the current name and enabled status of the changed device.

5.6 Removing devices

Note: You must have the **Remove Token devices** option enabled to be able to remove a device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

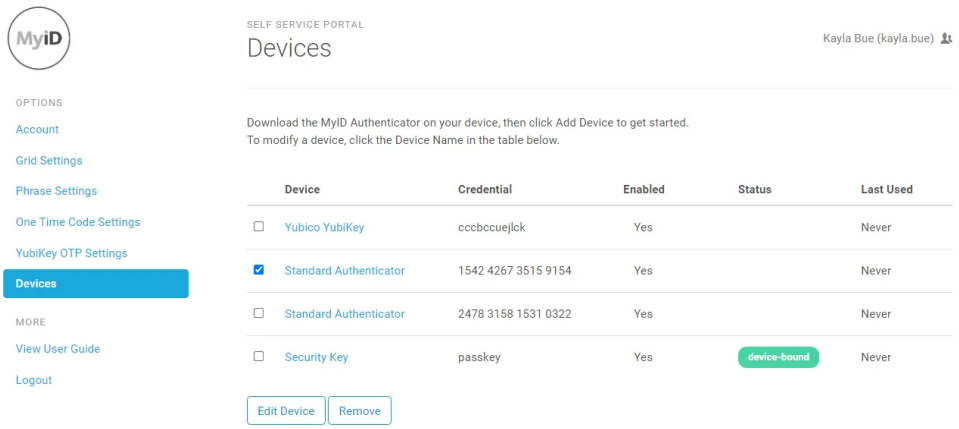
You can remove a device through the SSP.

To remove a device:

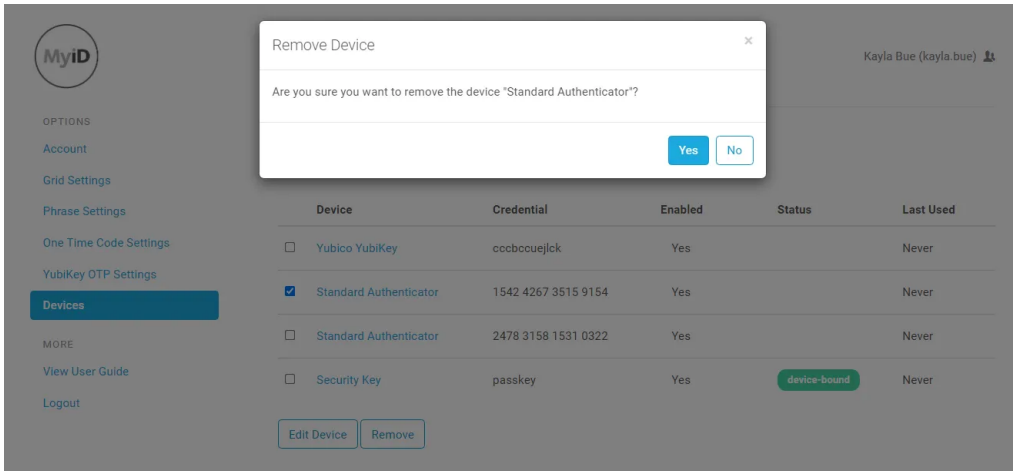
1. Log on to the Self Service Portal, and select **Devices** from the menu.

   Note: You must either have the **Add Token devices** option enabled or existing devices to see the **Devices** menu.

2. Select the device that you want to remove.



3. Click **Remove**.



4. Click **Yes**.

   The device is removed from your account. The table of devices is updated.