

MyID MFA and PSM

Version 5.3.2

Self Service Portal User Guide

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

Copyright

© 2001-2025 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

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

Self Service Portal User Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	5
1.1 Language requirements	5
2 Accessing the Self Service Portal	6
2.1 Your first logon	7
3 Updating your account	8
3.1 Changing your phone number	8
3.2 Resetting your Windows password	9
3.2.1 Resetting a basic password	9
3.2.2 Resetting your security phrase	11
3.3 Unlocking your account	12
4 Changing your multi-factor authentication settings	13
4.1 Changing your Grid pattern	14
4.2 Settings your Phrase answers	16
4.3 Changing your One Time Code settings	17
4.4 Changing your YubiKey OTP settings	18
5 Setting up your own device	19
5.1 MyID Authenticator app	20
5.1.1 Legacy Authlogics Authenticator app	20
5.1.2 Alternative Authenticator apps	20
5.1.3 Adding your MyID Authenticator device to your account	21
5.2 Other authenticator apps	25
5.2.1 Adding your standard authenticator device to your account	25
5.3 YubiKey OTP	28
5.3.1 Adding your YubiKey device to your account	28
5.4 Passkey / FIDO Token	31
5.4.1 Adding your FIDO / Security Key device to your account	31
5.4.2 Adding a Synched Passkey to your account	36
5.5 Editing devices	40
5.6 Removing devices	42

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

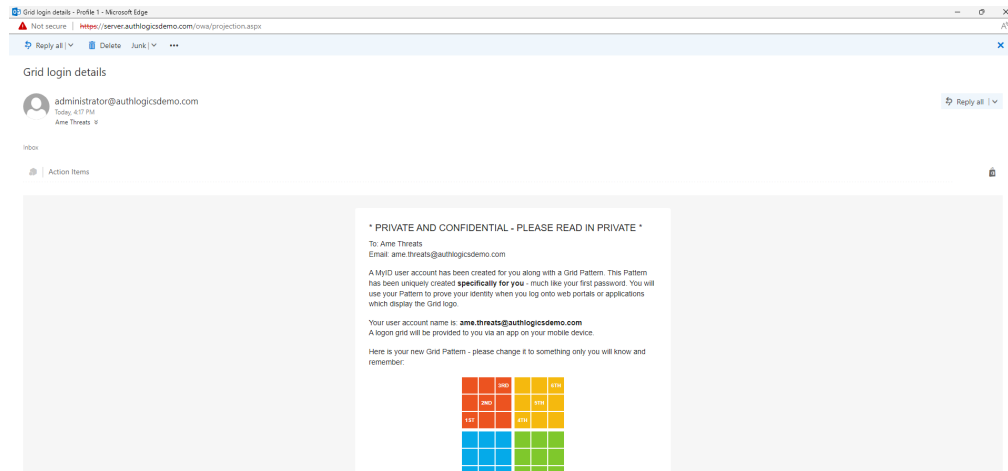
Content appears in the primary language of the browser, assuming it is supported. If the primary language of the browser is unsupported, content is shown in English.

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

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.

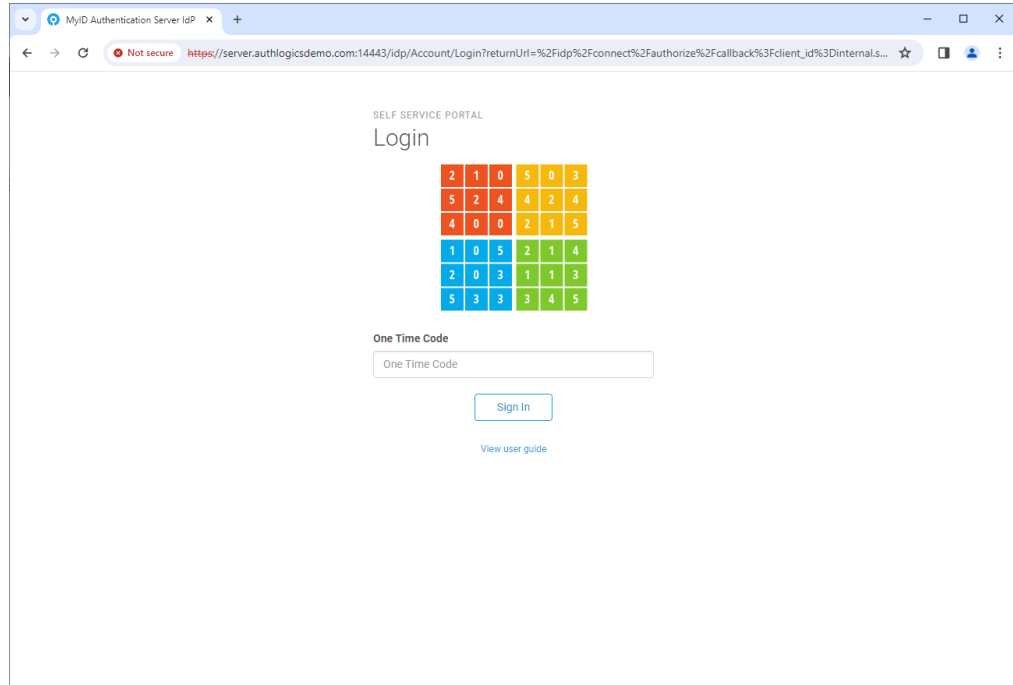


Once you have received your welcome email, you can log on. See section 2.1, *Your first logon*.

2.1 Your first login

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.

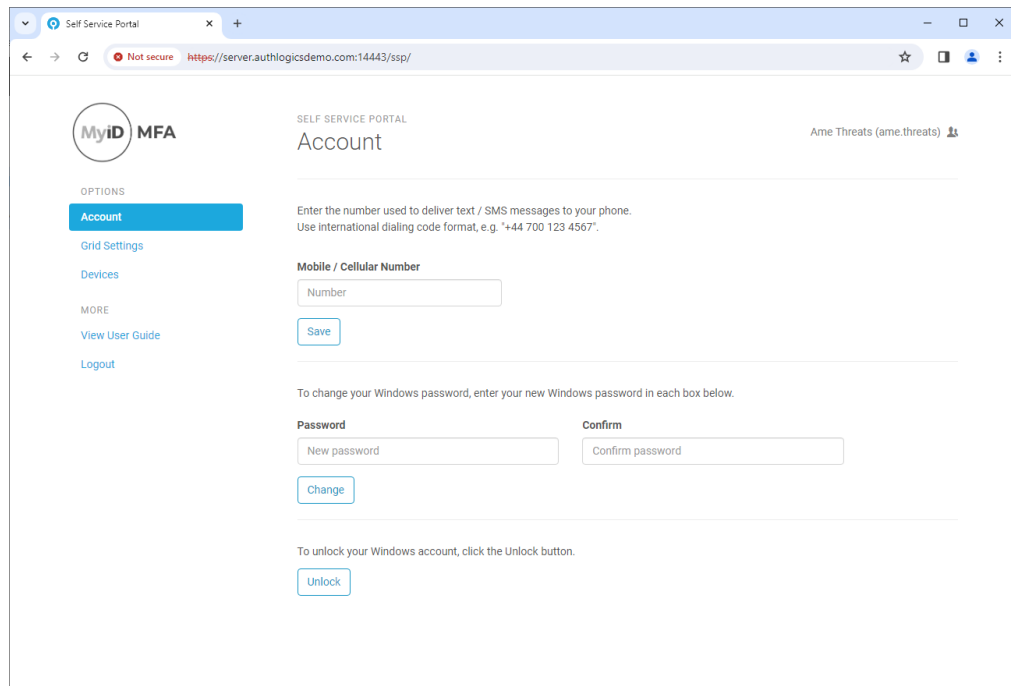
Using the portal, you can:

- Change the phone number on your account.
See section [3.1, Changing your phone number](#).
- Reset your password.
See section [3.2, Resetting your Windows 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.



The screenshot shows the 'Self Service Portal' web application. The browser address bar indicates the URL is 'https://server.authlogicsdemo.com:14443/ssp/'. The page title is 'SELF SERVICE PORTAL Account'. On the left, there is a sidebar menu with 'Account' selected. The main content area has a heading 'Account' and a sub-heading 'Mobile / Cellular Number'. Below this is a text input field labeled 'Number' and a 'Save' button. Further down, there is a section for 'Password' with 'New password' and 'Confirm' input fields, and a 'Change' button. At the bottom, there is an 'Unlock' button. The user's name 'Ame Threats (ame.threats)' is visible in the top right corner.

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 Windows password

The method to use to reset your password depends on how your system is set up. If your administrators have enabled security phrases, you do not type a new password; instead, you choose a randomly generated phrase. This phrase is used as your Windows password.

- If you do not have security phrases enabled, see section [3.2.1, Resetting a basic password](#).
- If you have security phrases enabled, see section [3.2.2, Resetting your security phrase](#).

3.2.1 Resetting a basic password

To reset your Windows 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:

At least 7 characters long

At least 1 uppercase characters

At least 2 numeric characters

Not previously breached

your new Windows password in each box below.

Confirm

Confirm password

Change

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

At least 7 characters long

At least 1 uppercase characters

At least 2 numeric characters

Not previously breached

your new Windows password in each box below.

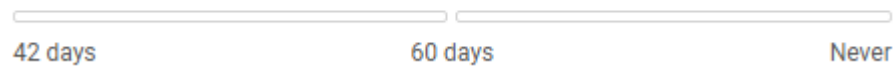
Confirm

Confirm password

Change

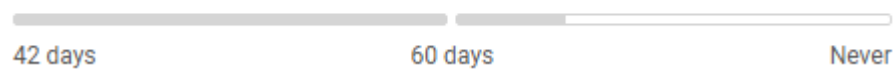
If you have dynamic password expiry enabled, a date and a bar are displayed below your password to show when you will need to reset your password. When you need to reset your password depends on the length of your password; for more information on password expiry, see the *Dynamic password expiry* section in the [MyID Authentication Server Installation and Configuration Guide](#).

Your new password will expire on **13 November**.



As you add more characters to your password, the bar fills.

Your new password will expire on **1 December**



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

If successful, the following message appears:

Your Password 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.

If you get an error similar to the following, you must change your password to align with the set password policies.

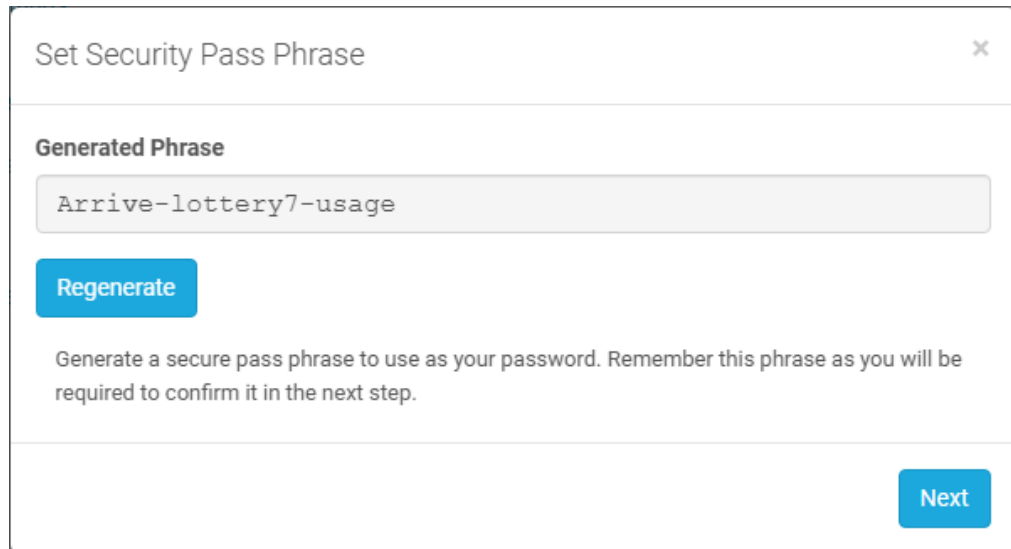
Password invalid. Choose a password with:
No more than 3 keyboard characters in a sequence (e.g. query)
At least 14 characters long

3.2.2 Resetting your security phrase

To reset your security phrase:

1. Select **Account** from the menu.
2. Click **Generate Phrase**.

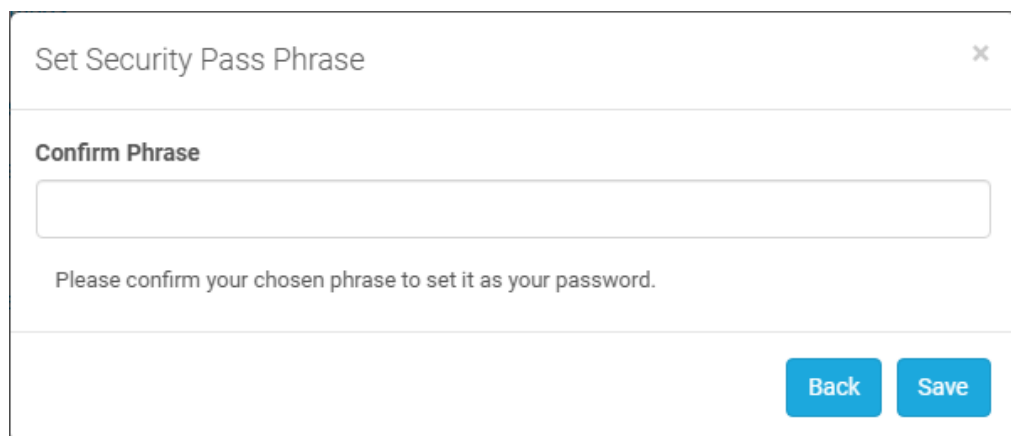
A dialog appears containing a generated phrase.



The dialog box is titled "Set Security Pass Phrase" and has a close button (X) in the top right corner. It contains a section labeled "Generated Phrase" with a text input field displaying "Arrive-lottery7-usage". Below this is a blue button labeled "Regenerate". At the bottom right is a blue button labeled "Next".

Generate a secure pass phrase to use as your password. Remember this phrase as you will be required to confirm it in the next step.

3. If you dislike the generated phrase, click **Regenerate**.
You can regenerate your security phrase as many times as you want. Choose a phrase that you are confident you can recall.
4. Once you have a generated phrase that you like, ensure that you have memorized the security phrase, including capitalization and numbers, and click **Next**.



The dialog box is titled "Set Security Pass Phrase" and has a close button (X) in the top right corner. It contains a section labeled "Confirm Phrase" with a text input field. Below this is the text "Please confirm your chosen phrase to set it as your password." At the bottom right are two blue buttons labeled "Back" and "Save".

5. Type your security phrase.

6. Click **Save**.

Your password was updated successfully.
Your new password will expire on **1 December**

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.

To unlock your Windows account, click the Unlock button.

Unlock

2. Click **Unlock**.

If successful, the following message appears:

Your account was unlocked successfully.

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.

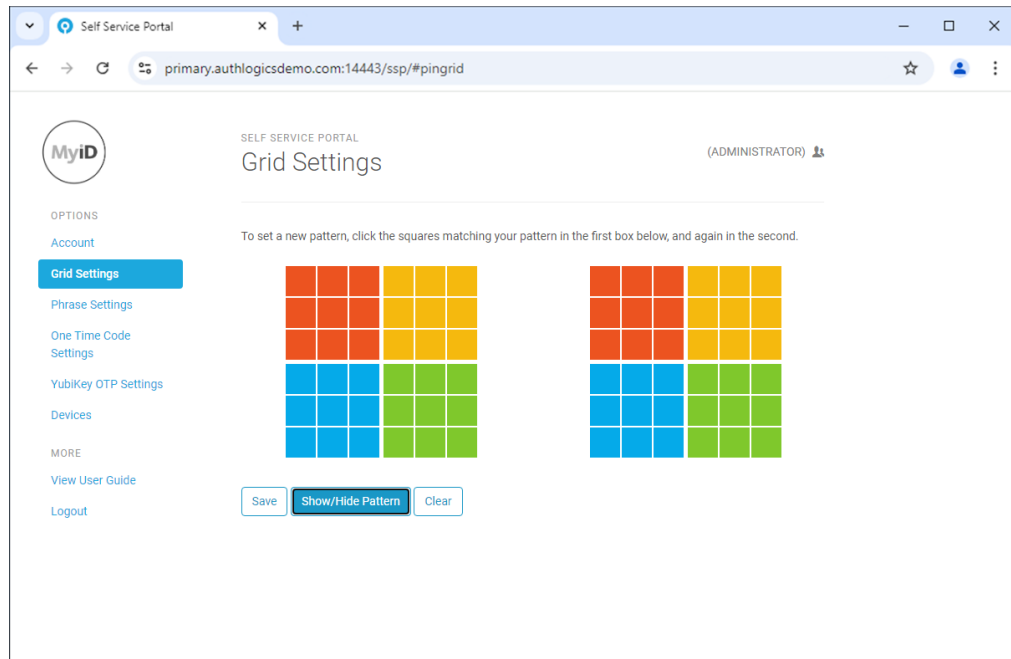
Using the portal, you can:

- 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

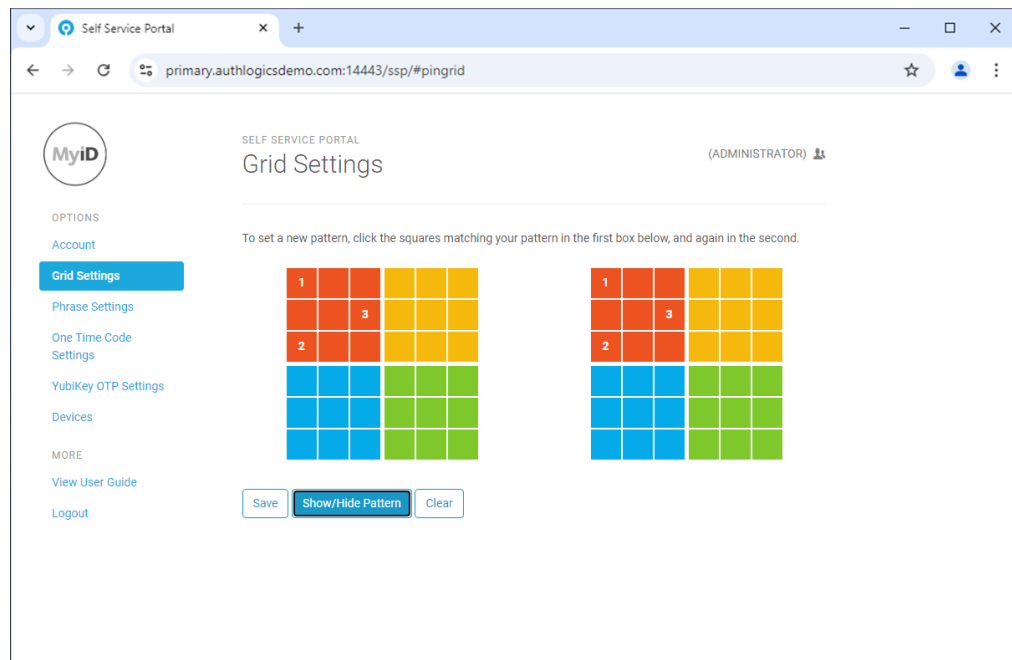
To change your Grid pattern:

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:

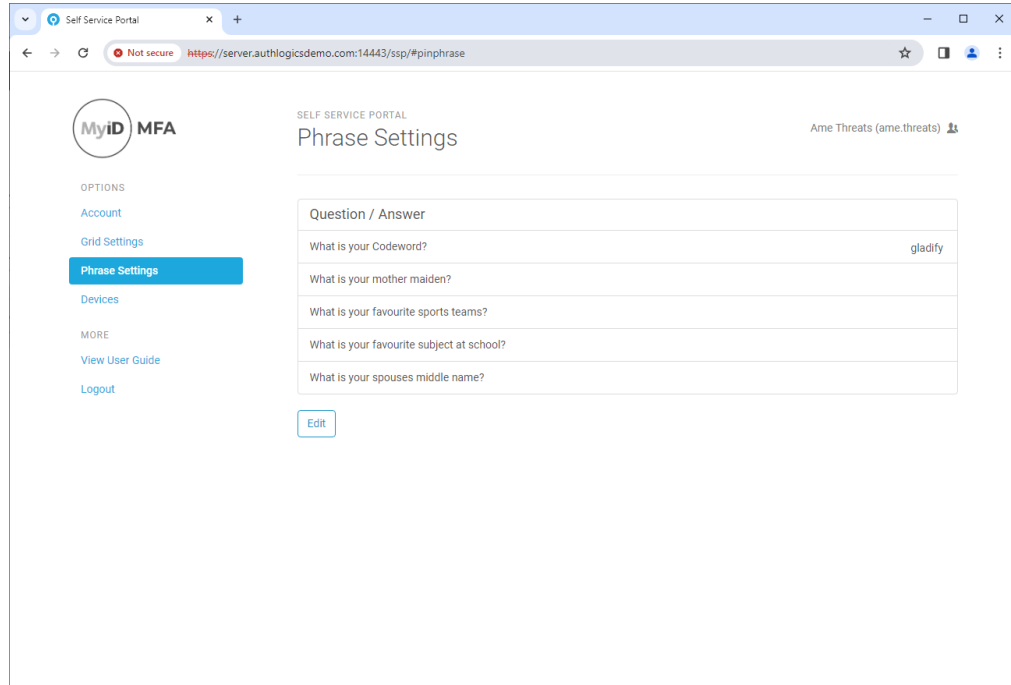
Your Pattern was updated successfully.

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.



The screenshot shows a web browser window with the URL <https://server.authlogicsdemo.com:14443/ssp/#pinphrase>. The page is titled "SELF SERVICE PORTAL" and "Phrase Settings". On the left, there is a sidebar menu with the following items: "Account", "Grid Settings", "Phrase Settings" (highlighted in blue), "Devices", "View User Guide", and "Logout". The main content area contains a table with the following questions and answers:

Question / Answer
What is your Codeword?
What is your mother maiden?
What is your favourite sports teams?
What is your favourite subject at school?
What is your spouses middle name?

Below the table, there is an "Edit" button. The user's name "Arne Threats (arne.threats)" is displayed in the top right corner.

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.

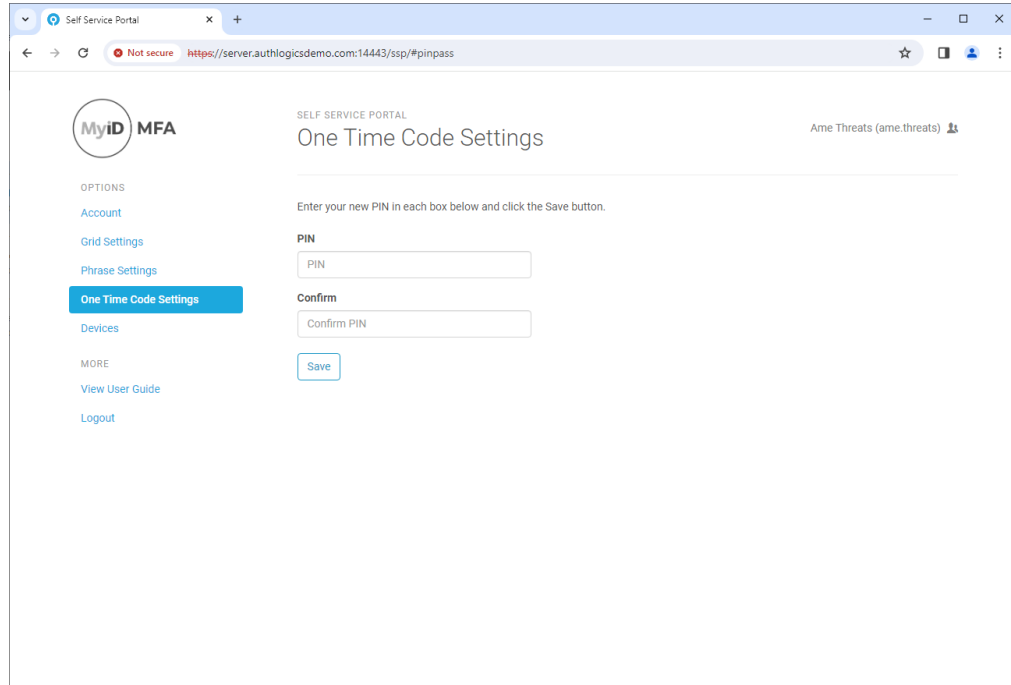
If successful, the following message appears:

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.



The screenshot shows a web browser window with the address bar displaying "Self Service Portal" and a URL starting with "https://server.authlogicsdemo.com:14443/ssp/#pinpass". The page title is "SELF SERVICE PORTAL" and the main heading is "One Time Code Settings". On the left, there is a sidebar menu with options: Account, Grid Settings, Phrase Settings, One Time Code Settings (highlighted), and Devices. Below these are links for View User Guide and Logout. The main content area has a heading "One Time Code Settings" and a subheading "Enter your new PIN in each box below and click the Save button." There are two input fields: "PIN" and "Confirm". Below the "Confirm" field is a "Save" button. The user's name "Arne Threats (arne.threats)" is visible in the top right corner.

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

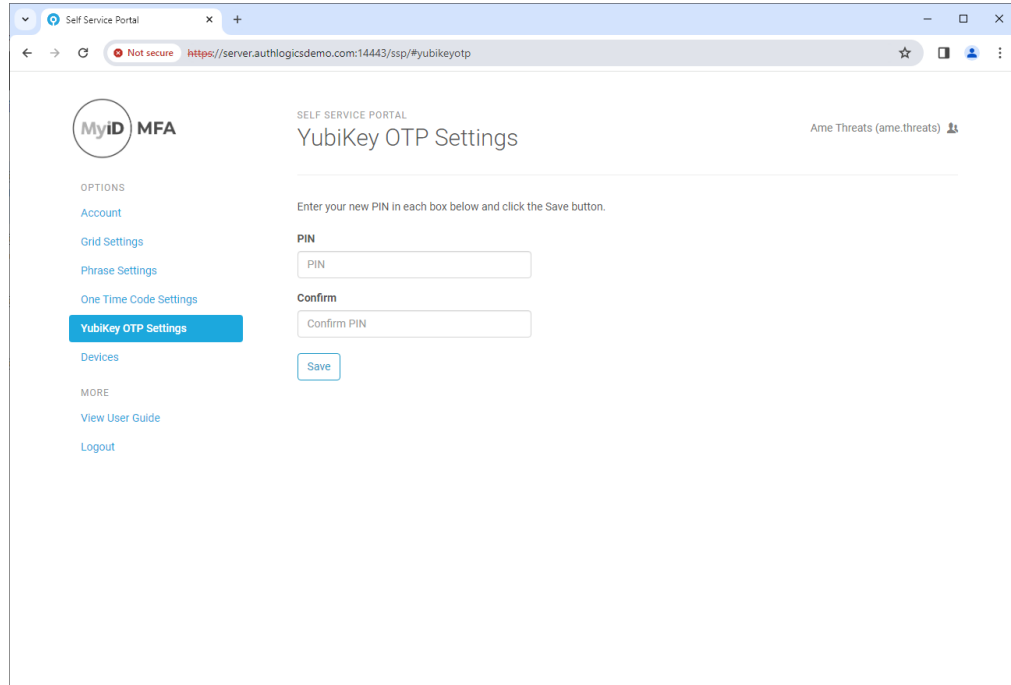
If successful, the following message appears:

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.



The screenshot shows a web browser window with the address bar displaying "Self Service Portal" and a URL starting with "https://server.authlogicsdemo.com:14443/ssp/#yubikeyotp". The page title is "SELF SERVICE PORTAL YubiKey OTP Settings". On the left, there is a sidebar menu under "OPTIONS" with links for "Account", "Grid Settings", "Phrase Settings", "One Time Code Settings", "YubiKey OTP Settings" (which is highlighted in blue), "Devices", and "MORE" (with sub-links "View User Guide" and "Logout"). The main content area has the heading "YubiKey OTP Settings" and a sub-heading "Enter your new PIN in each box below and click the Save button." Below this, there are two input fields: "PIN" and "Confirm", each with a "Confirm PIN" label. A "Save" button is located at the bottom of the form.

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 set up and manage your various authenticator technologies:

- Information on obtaining and setting up the MyID Authenticator app.
See section [5.1, MyID Authenticator app](#).
- Information on using alternative authenticator apps with MyID MFA.
See section [5.2, Other authenticator apps](#).
- Information on adding YubiKey devices to your account.
See section [5.3, YubiKey OTP](#).
- Information on adding non-YubiKey Passkey / FIDO tokens to your account.
See section [5.4, Passkey / FIDO Token](#).
- Instructions for editing your devices.
See section [5.5, Editing devices](#).
- Instructions for removing your devices.
See section [5.6, Removing devices](#).

Note: You can use the Self Service Portal to manage FIDO BIO keys, but not to register them. You can register some FIDO BIO keys through the Windows Desktop Agent; for more information, see the *FIDO considerations* and *Managing Multi-Factor options* sections of the [Windows Desktop Agent Integration Guide](#).

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

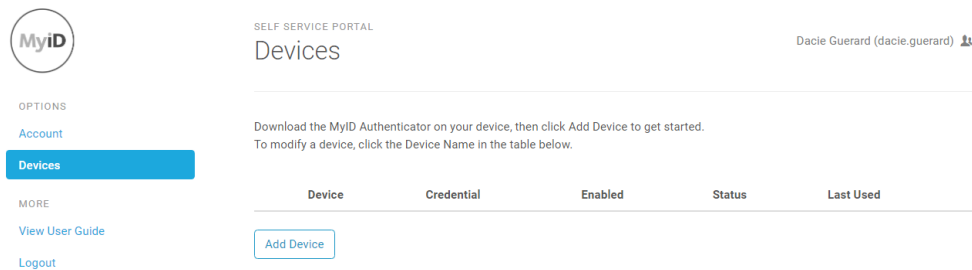
As an alternative, you can download a third-party OATH app from the relevant vendor. For example, you can use Microsoft or Google Authenticator.

5.1.3 Adding your MyID Authenticator device to your account

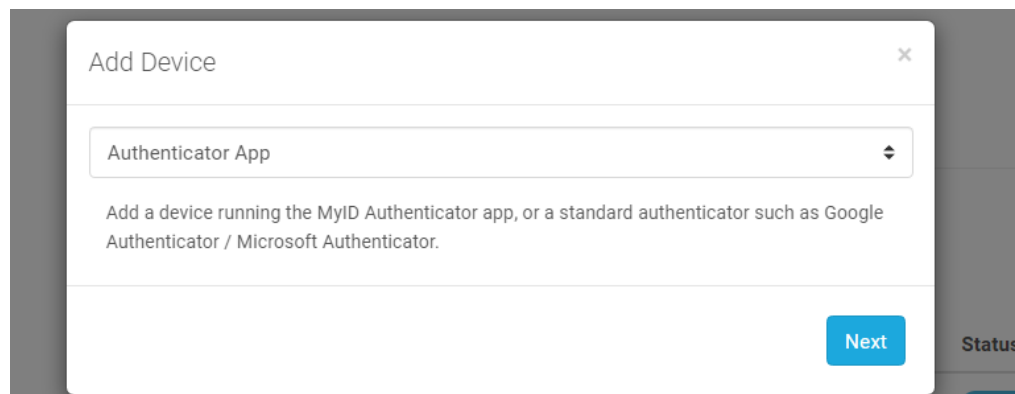
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the [MyID Authentication Server Installation and Configuration Guide](#).

To add a device to your account:

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

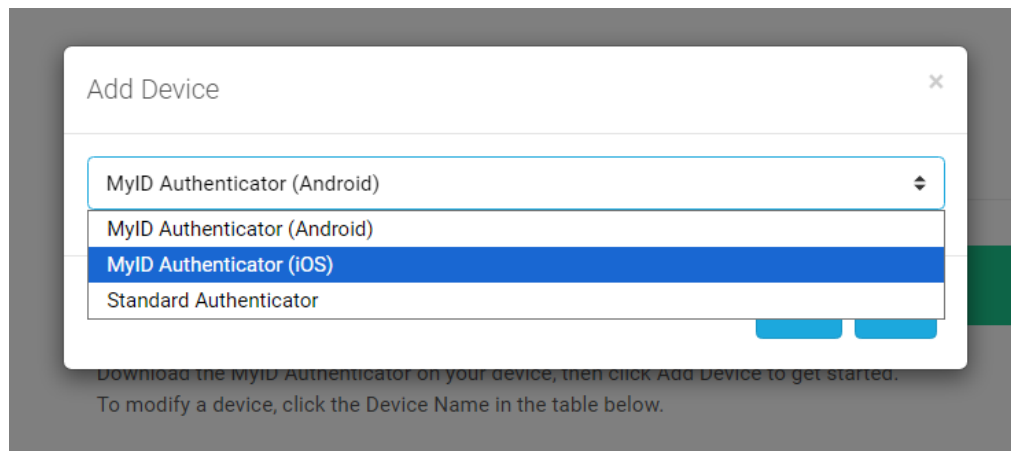


2. Install the MyID Authenticator App from the relevant App Store using the buttons on your device.
3. Click **Add Device**.



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

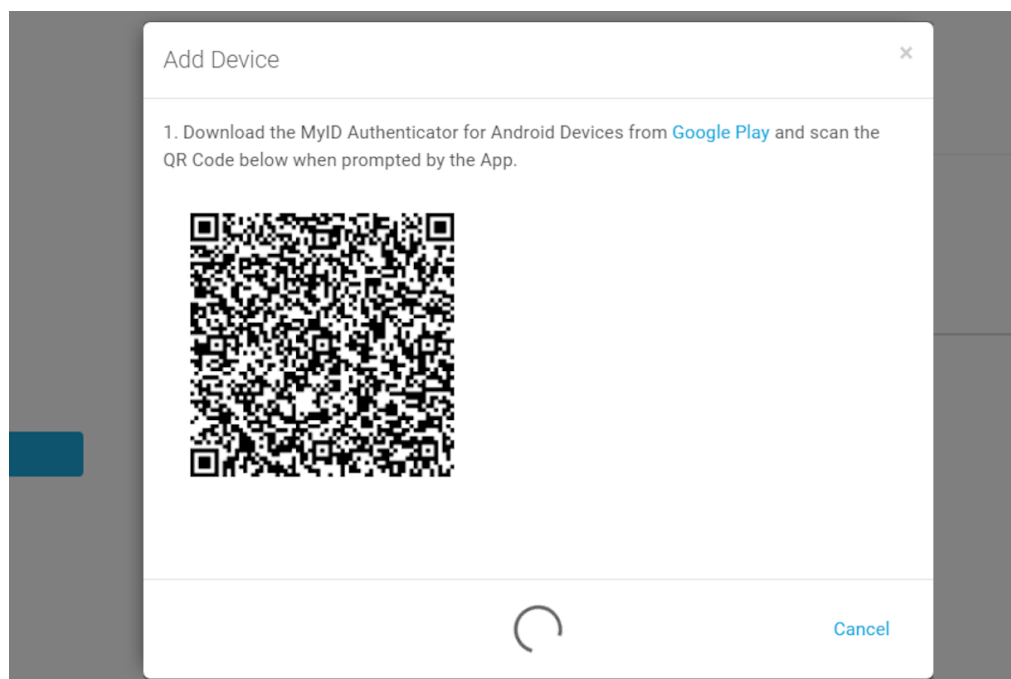
5. From the list, choose the type of device you have.



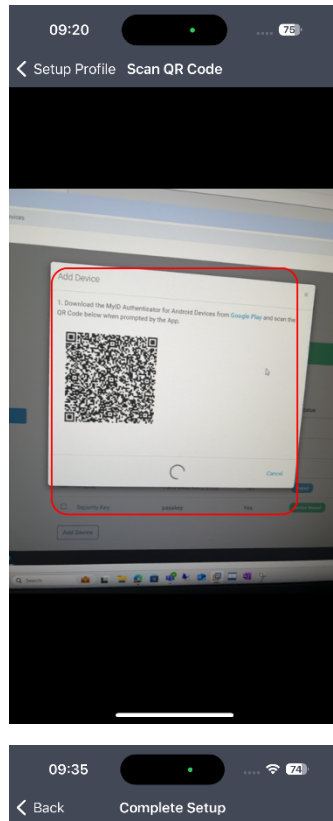
MyID Authenticator (Android) and **MyID Authenticator (iOS)** both relate to the MyID MFA app.

Standard Authenticator relates to third-party OAUTH tokens; see section [5.1.2, Alternative Authenticator apps](#) for details.

6. Click **Next**.

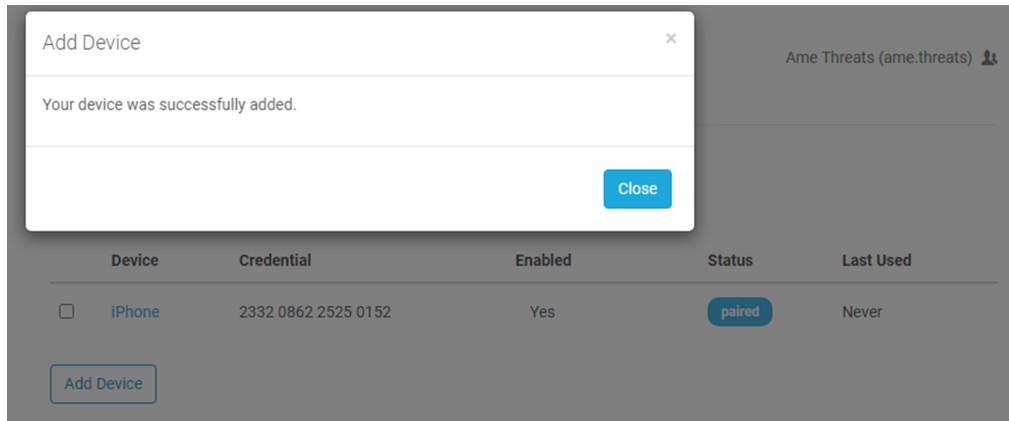


7. Scan the QR code with the MyID Authenticator App.



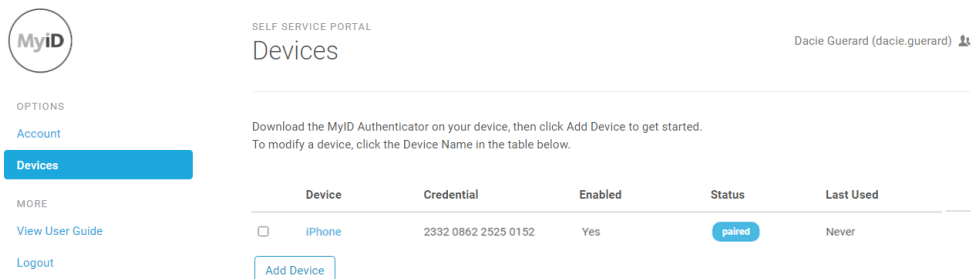
Device setup is complete.

Finish

8. Click **Finish**.

The screenshot shows a modal window titled "Add Device" with a close button (X) in the top right corner. The modal contains the message "Your device was successfully added." and a "Close" button. Below the modal, a table lists the added device. The table has columns: Device, Credential, Enabled, Status, and Last Used. The row shows an iPhone with credential 2332 0862 2525 0152, which is enabled and has a status of "paired". A "Add Device" button is visible at the bottom left of the table area.

Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/> iPhone	2332 0862 2525 0152	Yes	paired	Never

9. Click **Close**.

The screenshot shows the "MyID" Self Service Portal. On the left is a sidebar with "MyID" logo, "OPTIONS" (Account), and "MORE" (View User Guide, Logout). The main content area is titled "SELF SERVICE PORTAL Devices" and shows instructions: "Download the MyID Authenticator on your device, then click Add Device to get started. To modify a device, click the Device Name in the table below." Below the instructions is a table with columns: Device, Credential, Enabled, Status, and Last Used. The row shows an iPhone with credential 2332 0862 2525 0152, which is enabled and has a status of "paired". An "Add Device" button is at the bottom left of the table.

Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/> iPhone	2332 0862 2525 0152	Yes	paired	Never

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

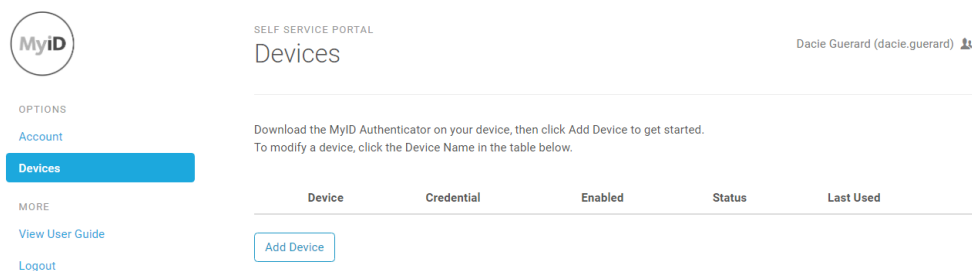
As an alternative to the MyID Authenticator app, you can download a third-party OATH app from the relevant vendor. For example, you can use Microsoft or Google Authenticator.

5.2.1 Adding your standard authenticator device to your account

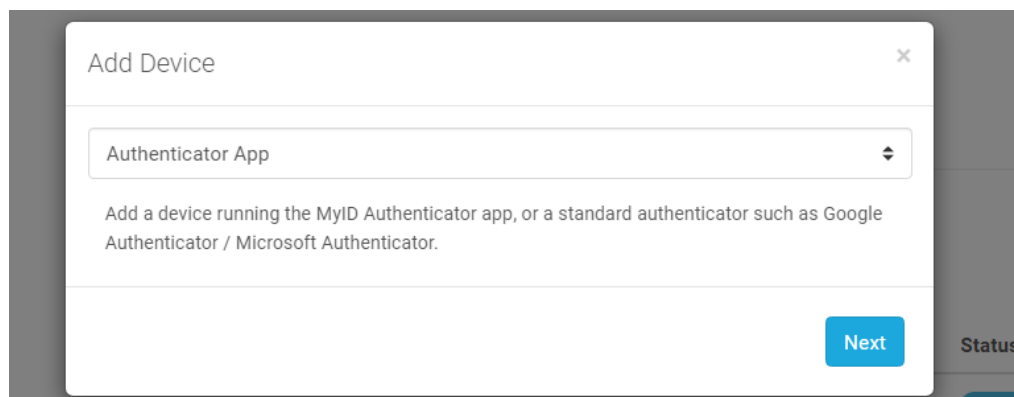
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the [MyID Authentication Server Installation and Configuration Guide](#).

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.

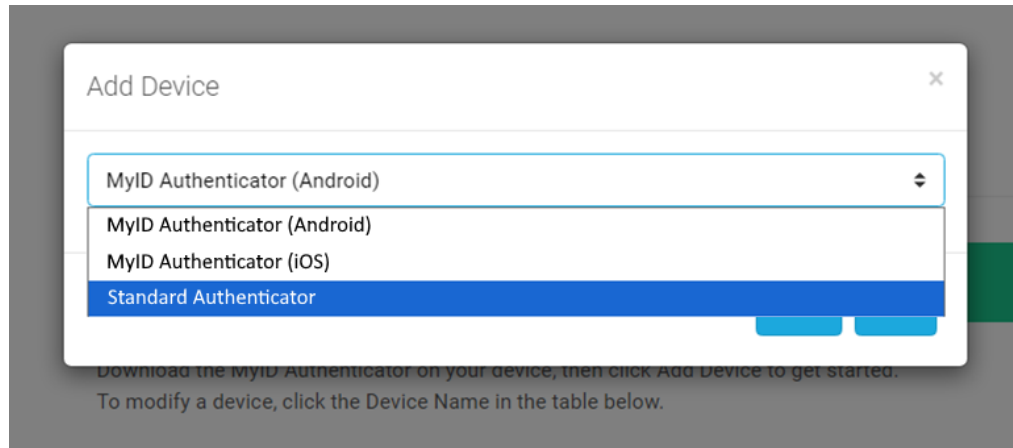


2. Install the relevant third-party app on your device.
3. Click **Add Device**.

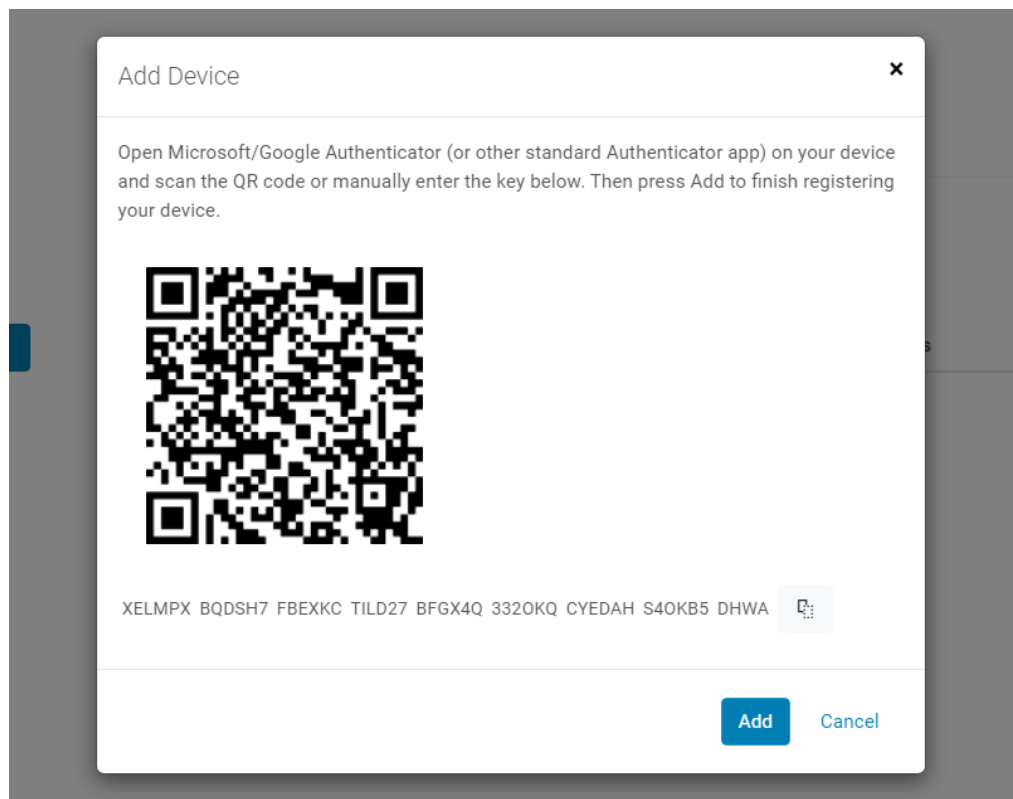


4. From the drop-down list, select **Authenticator App**.

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**.

MyID

OPTIONS

[Account](#)

[Grid Settings](#)

[Phrase Settings](#)

[One Time Code Settings](#)

[YubiKey OTP Settings](#)

Devices

MORE

[View User Guide](#)

[Logout](#)

SELF SERVICE PORTAL

Devices

(ADMINISTRATOR)

Your device has been added successfully.

Download the MyID Authenticator on your device, then click Add Device to get started.
To modify a device, click the Device Name in the table below.

Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/> Standard Authenticator	1531 6525 5196 1349	Yes		Never

Add Device

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

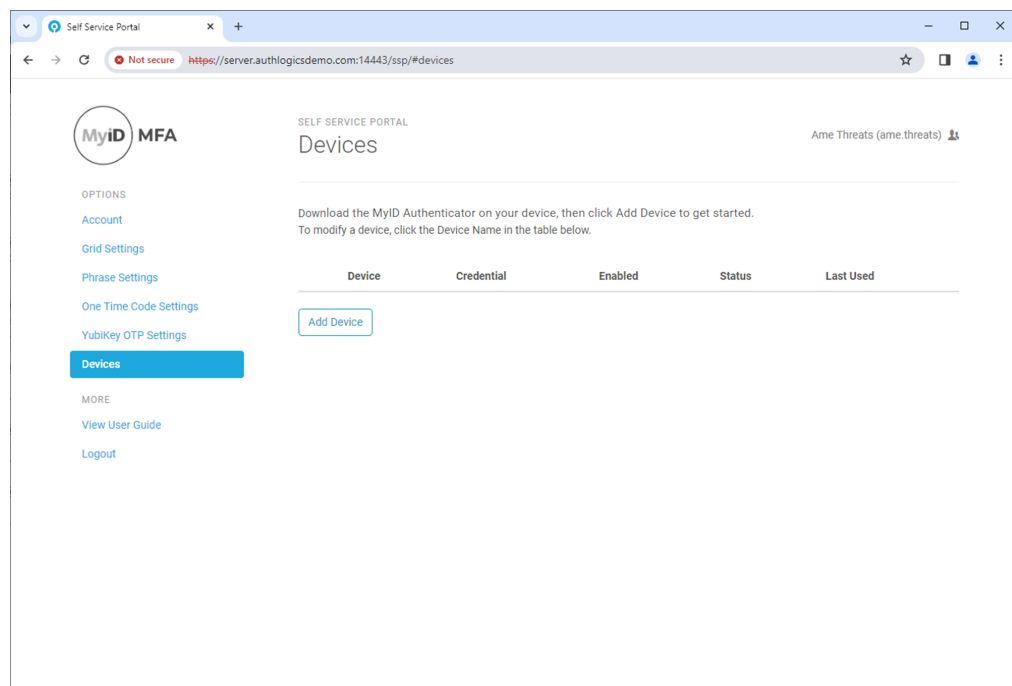
To provision your YubiKey OTP hardware device, insert the YubiKey token into your PC.

5.3.1 Adding your YubiKey device to your account

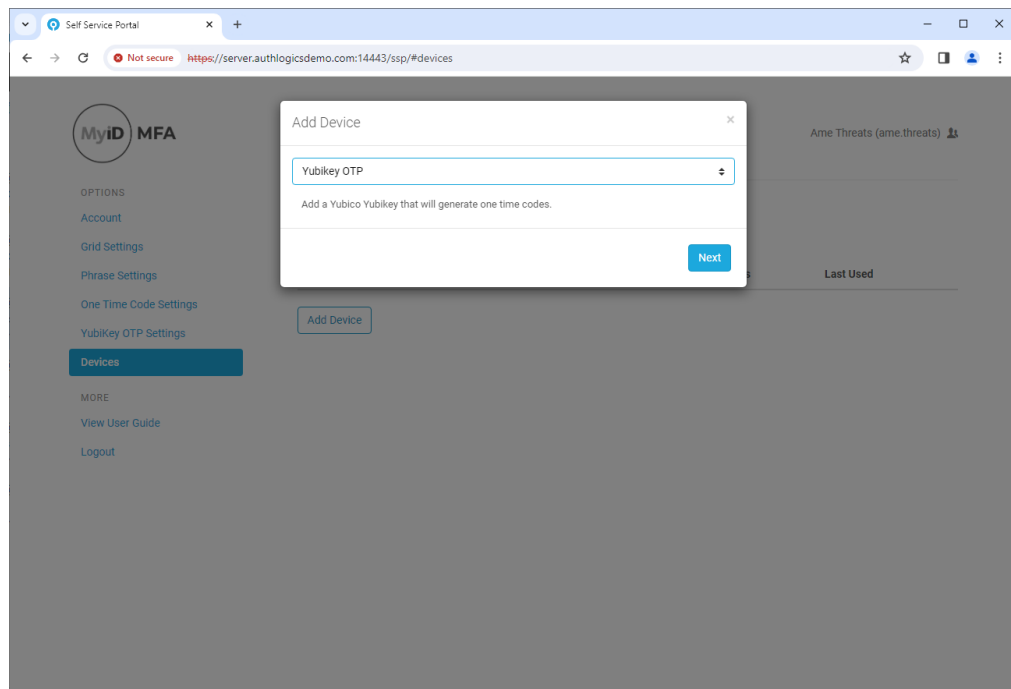
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the [MyID Authentication Server Installation and Configuration Guide](#).

To add a device to your account:

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

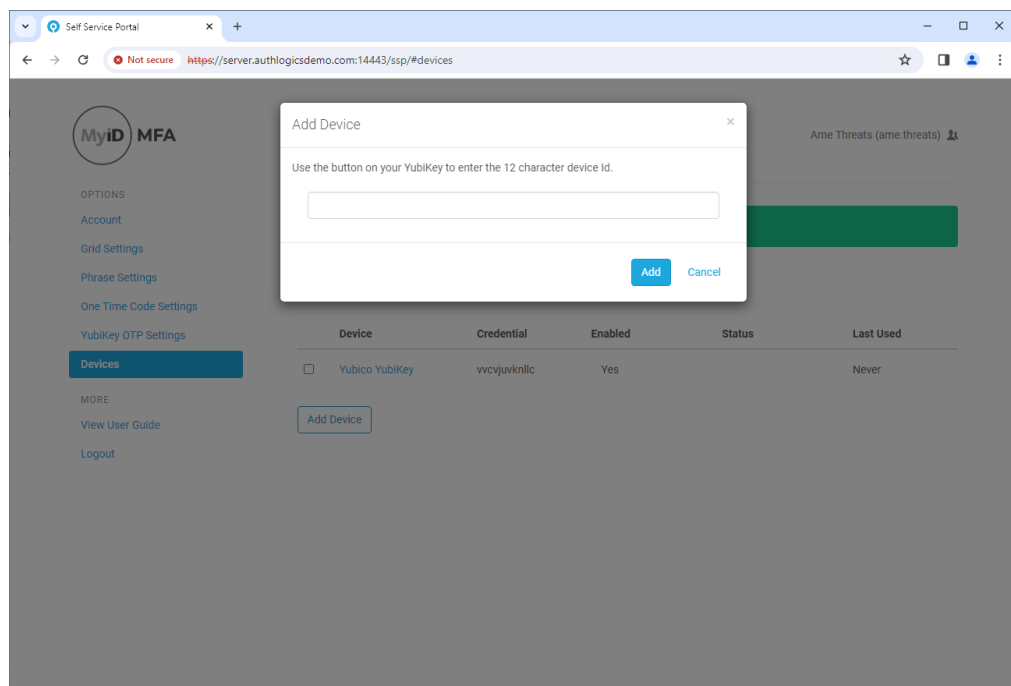


2. Click **Add Device**.

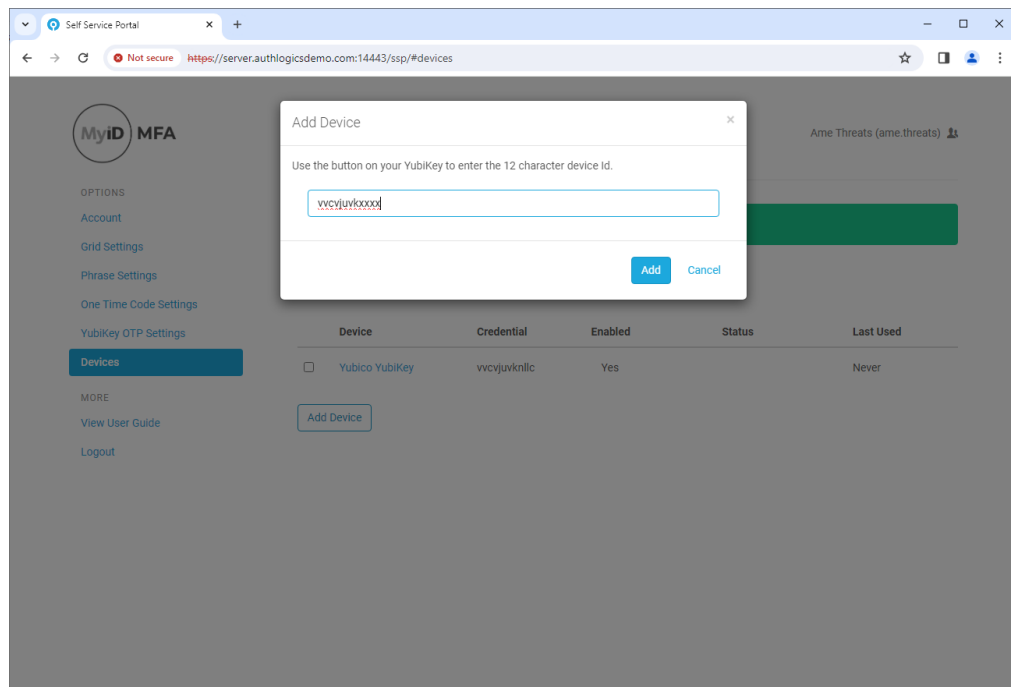


Note: If this option is not available, your user account has not been set up to use YubiKey tokens. Contact your administrator for assistance.

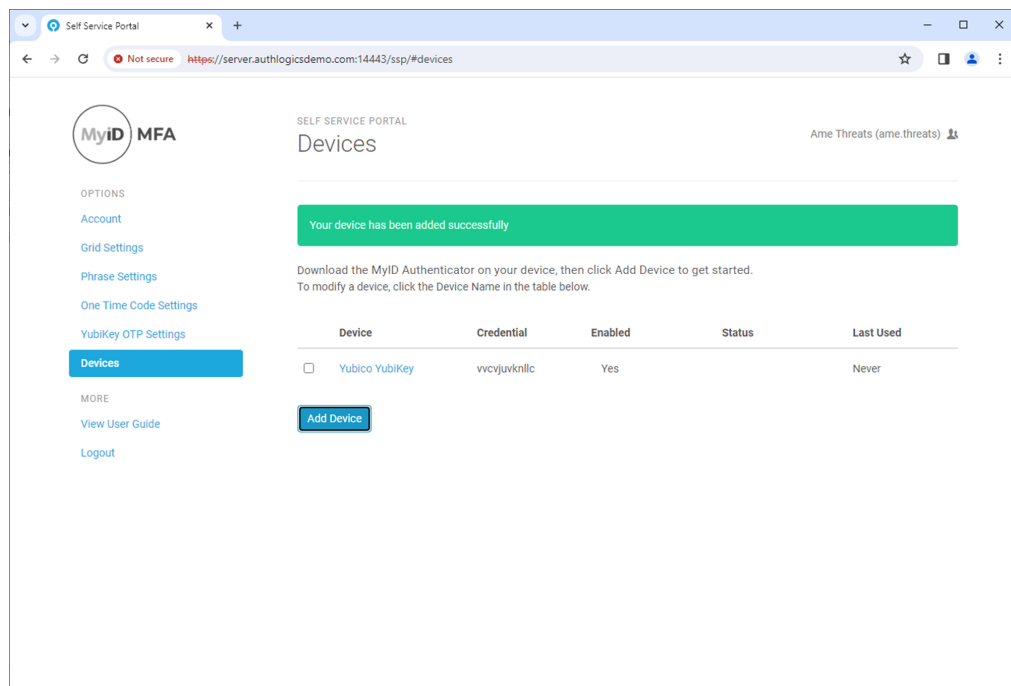
3. Select **YubiKey OTP** and click **Next**.



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

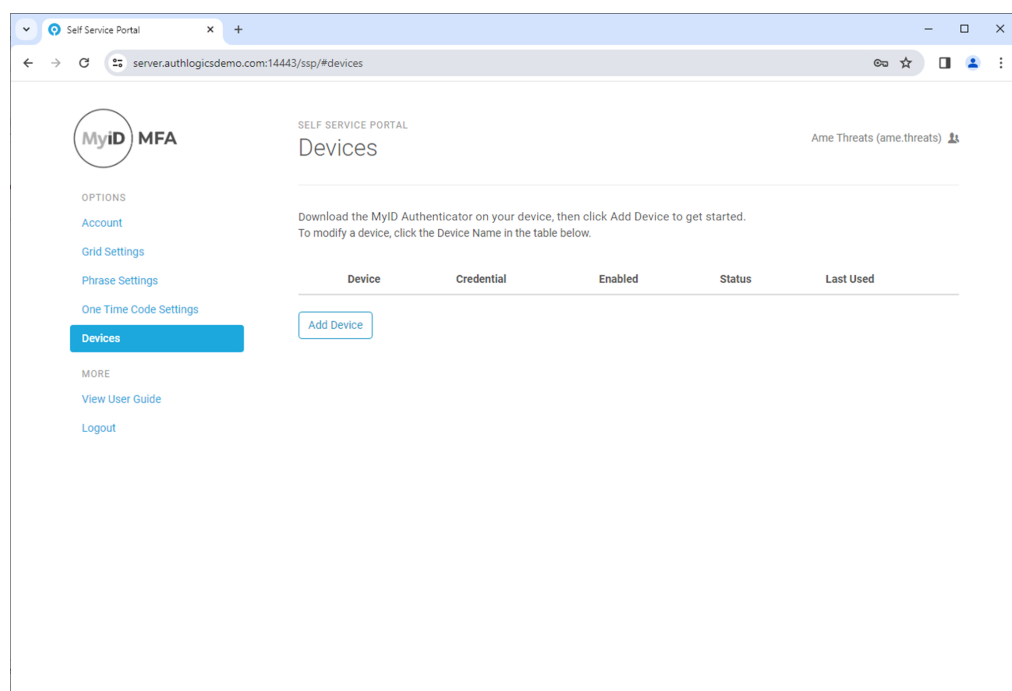
Before adding your FIDO Security Key or a Passkey to your account, ensure that no other MFA devices are attached to the workstation and that you have disconnected all Passkey / FIDO tokens from your PC.

5.4.1 Adding your FIDO / Security Key device to your account

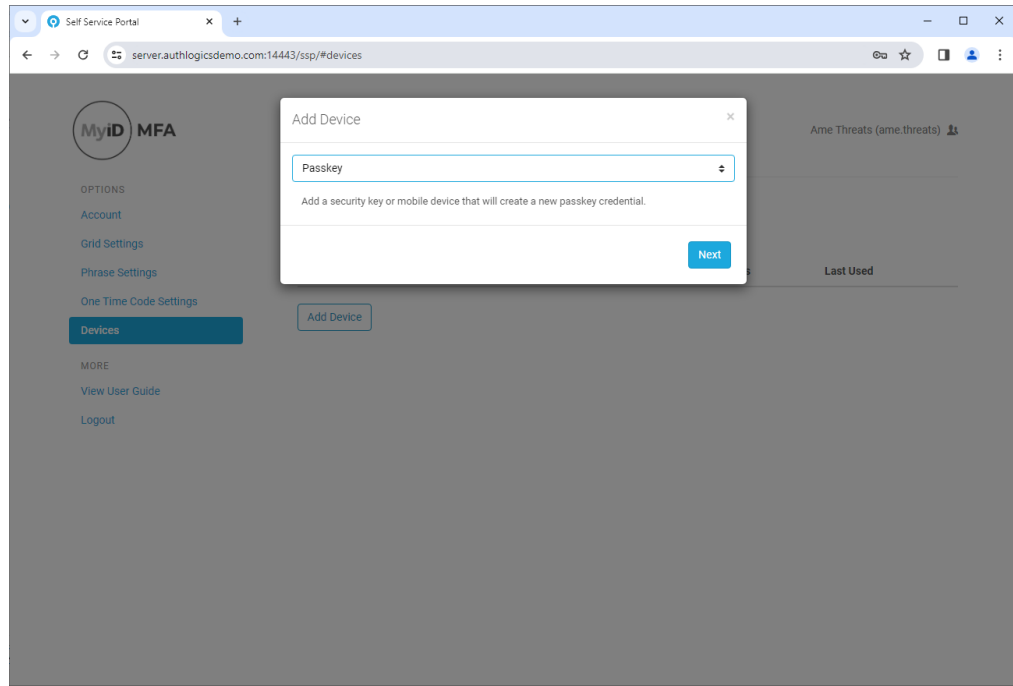
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the [MyID Authentication Server Installation and Configuration Guide](#).

To add a FIDO Passkey Security Key to your account:

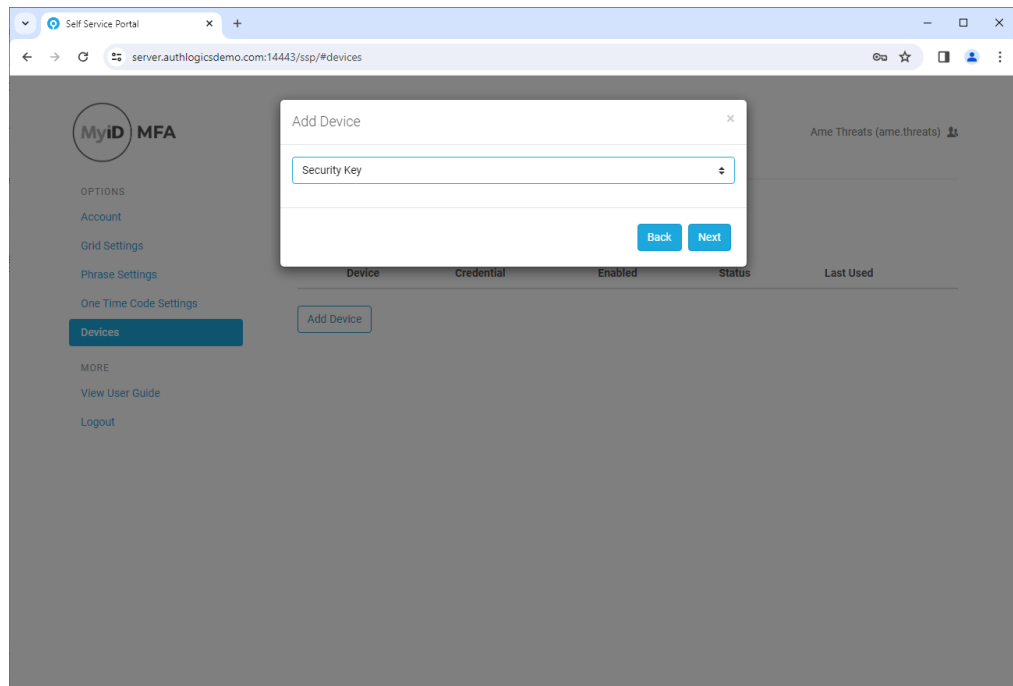
1. Log on to the Self Service Portal, and select **Devices** from the menu.



2. Click **Add Device**.



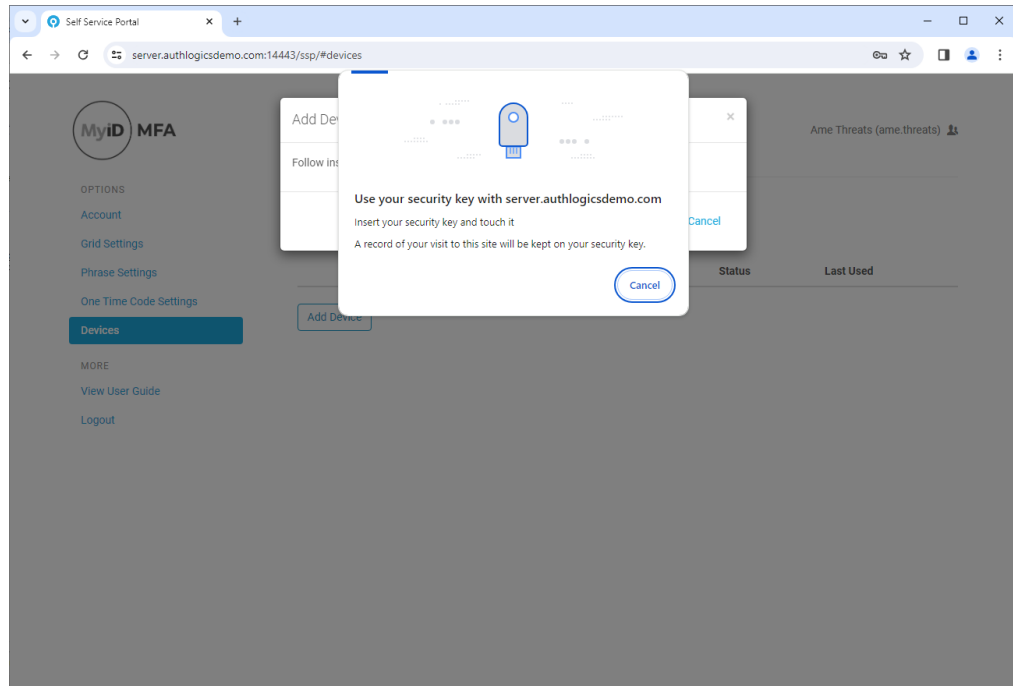
3. Select **Passkey** and click **Next**.



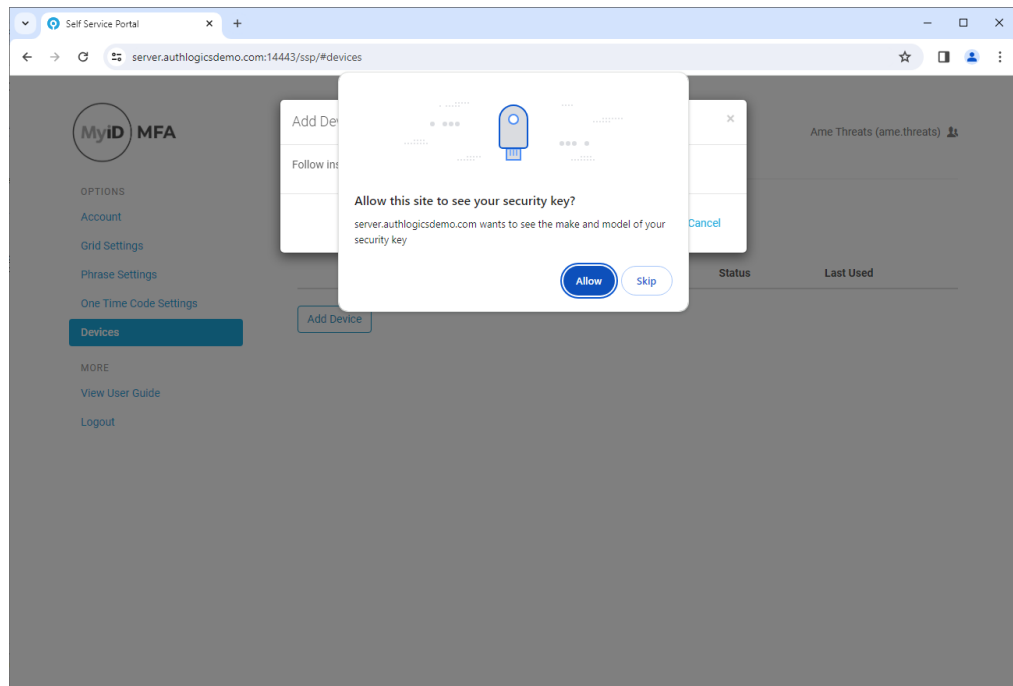
Note: If this option is not available, your user account has not been set up to use Passkeys. Contact your administrator for assistance.

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.

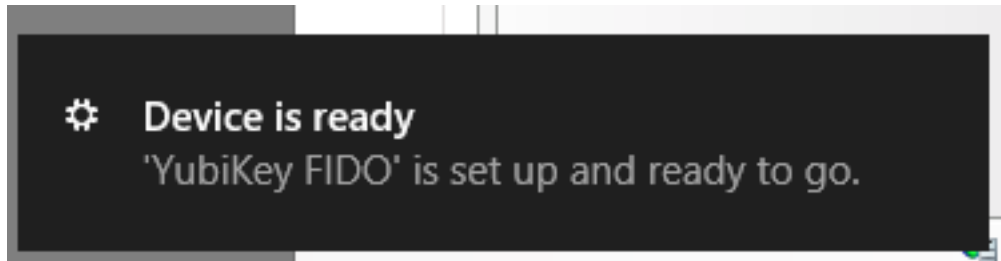
4. Select **Security Key** and click **Next**.



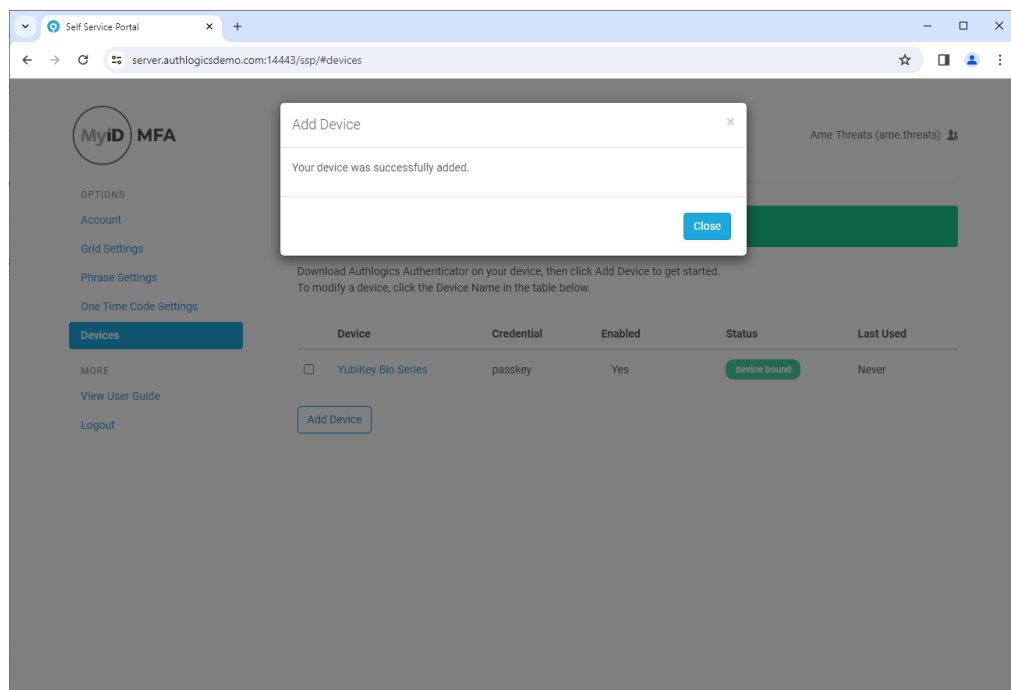
5. Insert your security key and press the FIDO token's button.



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

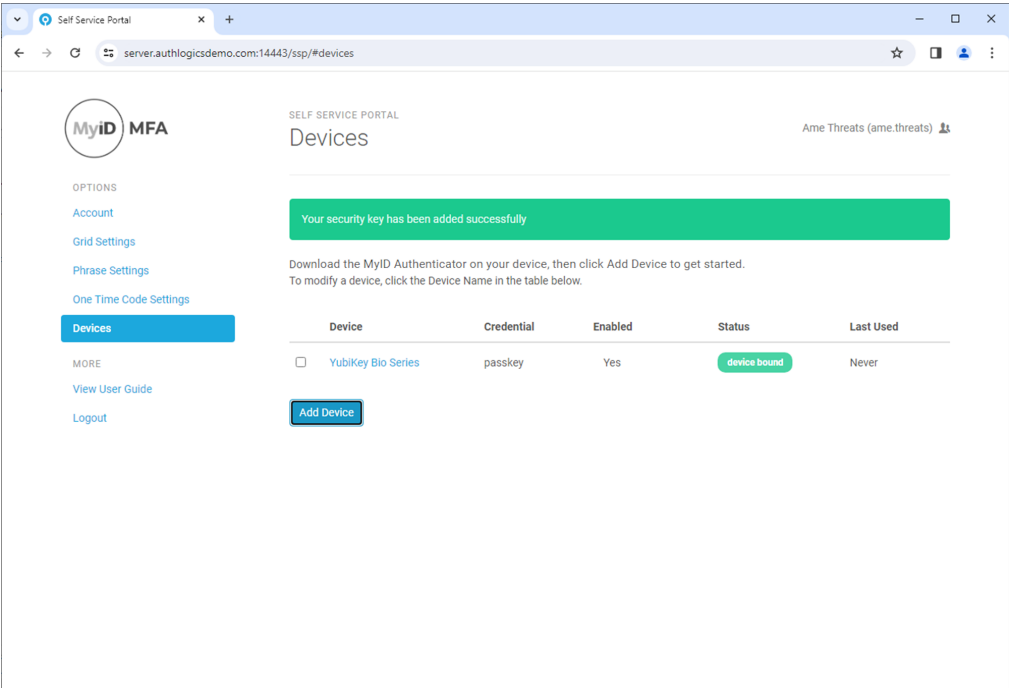


The underlying system notifies you that the FIDO token is set up and ready for use.



The device has been successfully added.

7. Click **Close**.

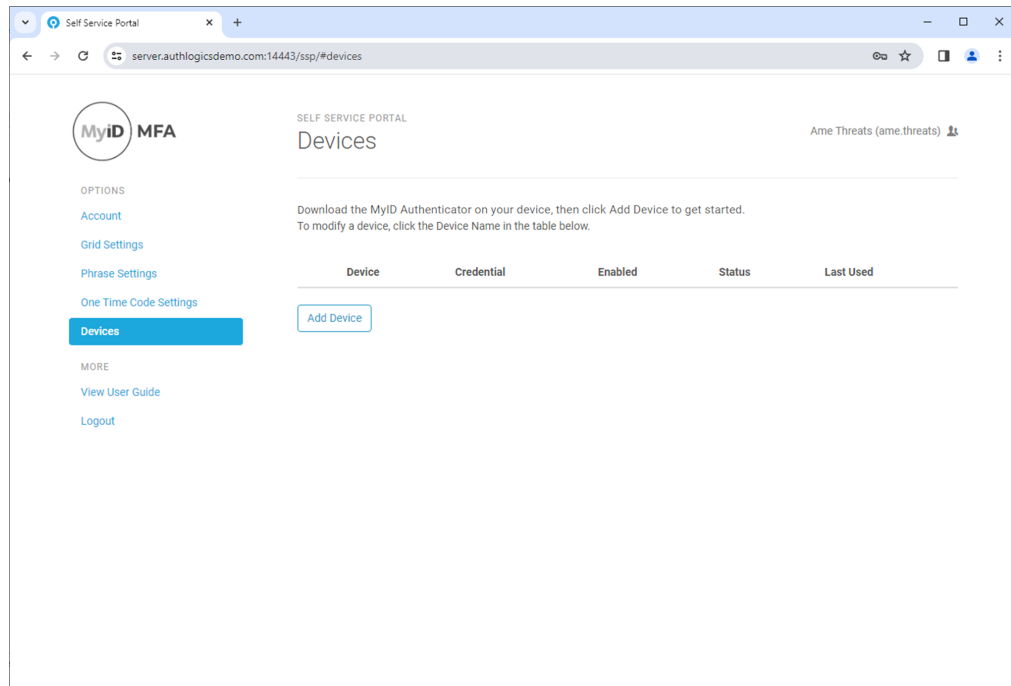


5.4.2 Adding a Synched Passkey to your account

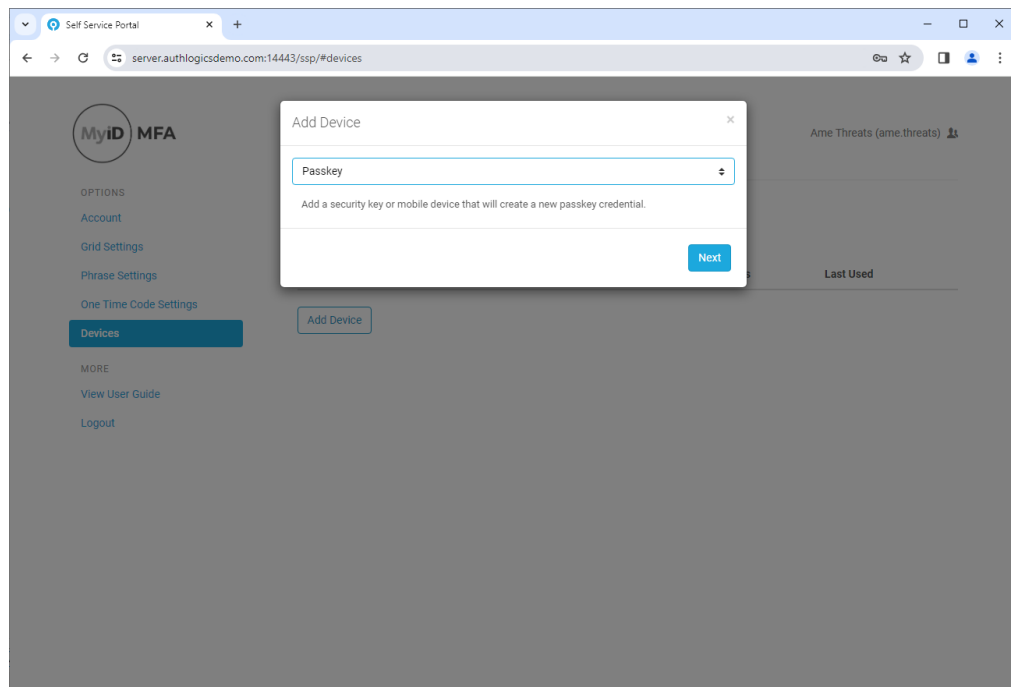
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the [MyID Authentication Server Installation and Configuration Guide](#).

To add a FIDO Passkey Security Key to your account:

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

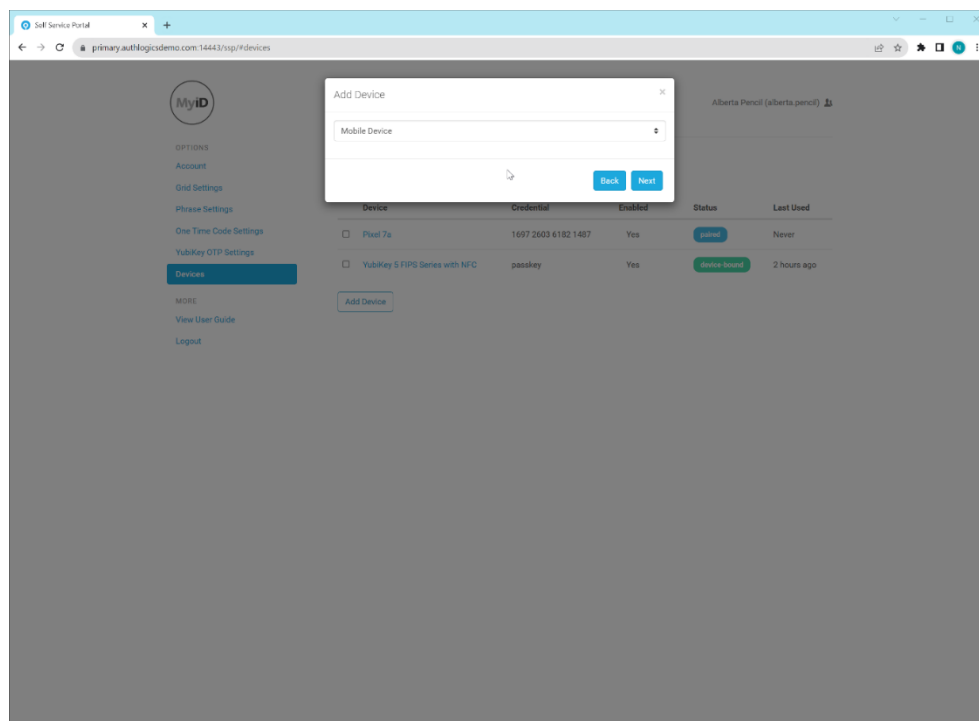


2. Click **Add Device**.

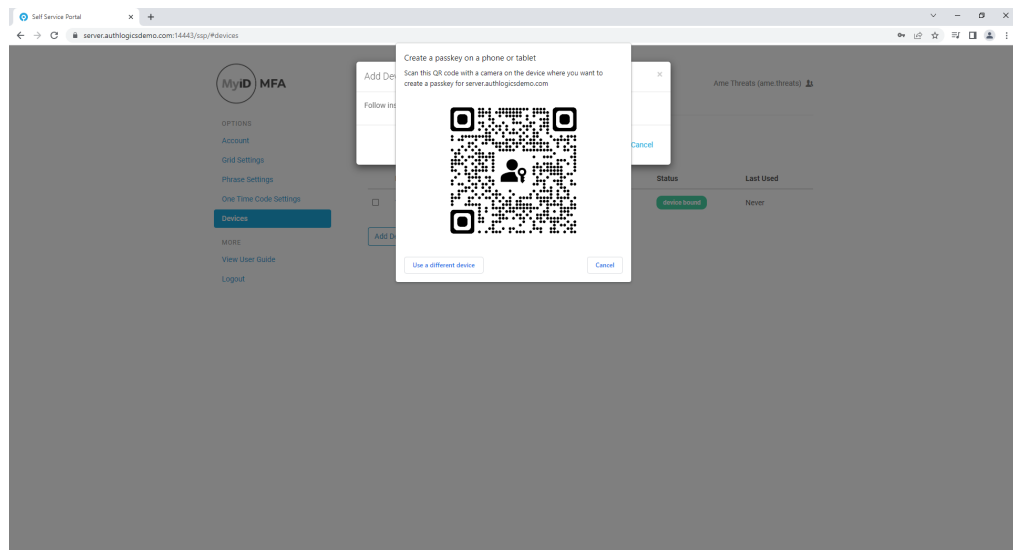


Note: If this option is not available, your user account has not been set up to use Passkeys. Contact your administrator for assistance.

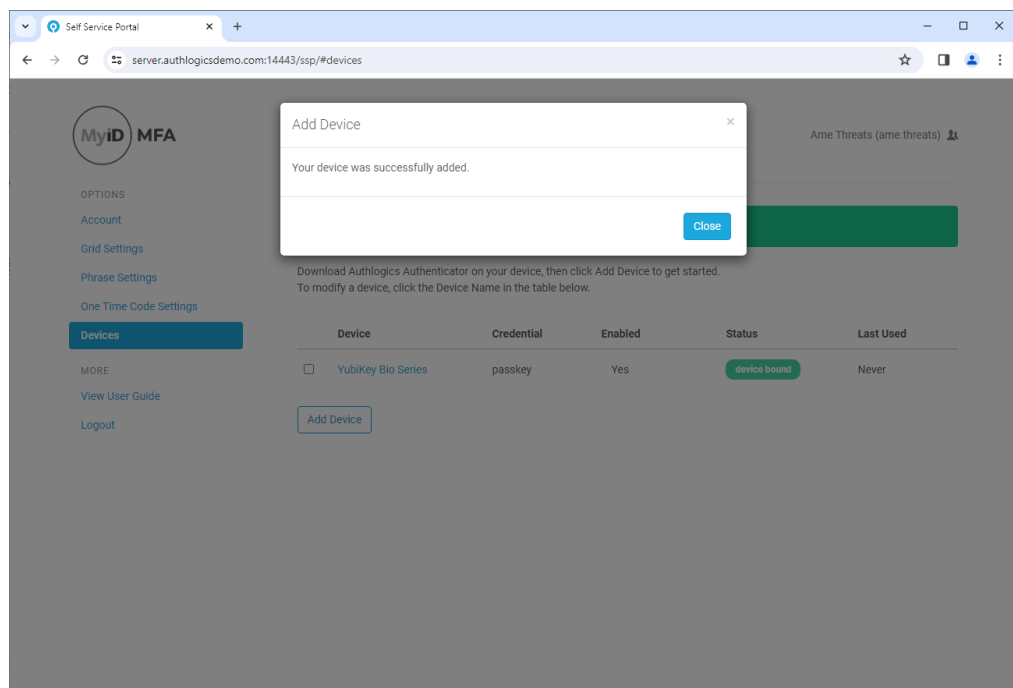
3. Select **Passkey** and click **Next**.



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

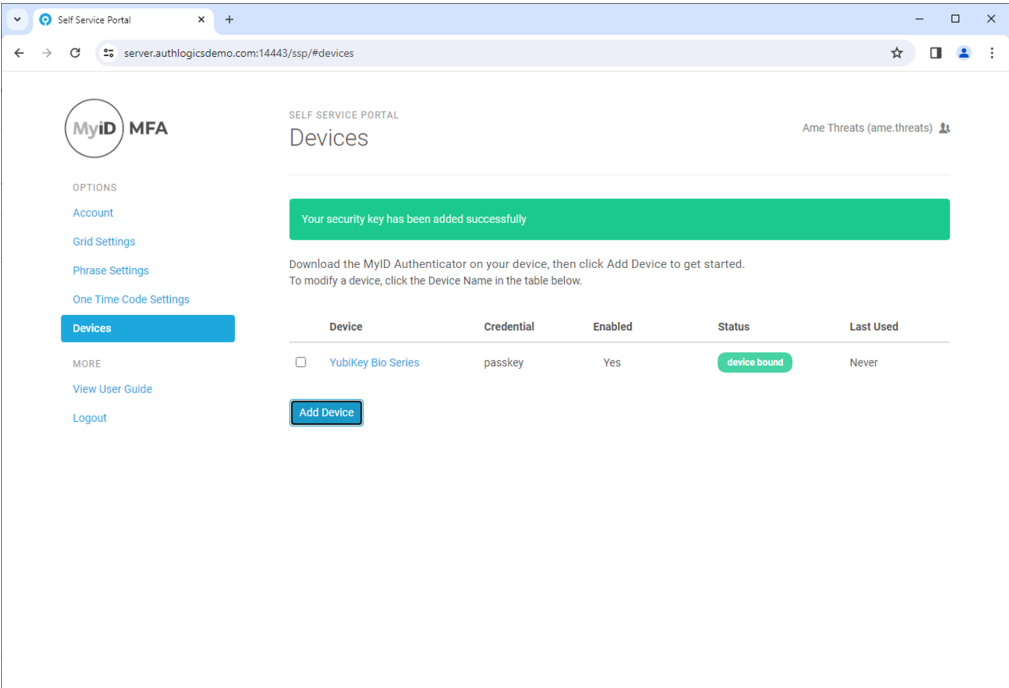


5. Ensure that Bluetooth is enabled on both the mobile device and your workstation.
If Bluetooth is *not* enabled on your workstation, the above QR Code is not displayed.
6. Open your mobile phone's camera and scan the QR Code.
7. Once you have scanned the QR Code, follow the instructions on your mobile 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.

Download the MyID Authenticator on your device, then click Add Device to get started.
To modify a device, click the Device Name in the table below.

	Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/>	Z Fold4	1031 1117 5242 0923	No	Paired	2 days ago
<input type="checkbox"/>	Yubico YubiKey	cccccbhlrtbg	Yes		3 seconds ago
<input checked="" type="checkbox"/>	YubiKey Bio Series	passkey	No	device-bound	Never

Edit DeviceRemoveDebug

3. Click **Edit Device**.

Device Name

YubiKey Bio Series

The Device Name can have a maximum length of 50 characters.

Enabled

No

Cancel Save

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.

MyID SELF SERVICE PORTAL Kayla Bue (kayla.bue)

OPTIONS

- Account
- Grid Settings
- Phrase Settings
- One Time Code Settings
- YubiKey OTP Settings
- Devices**

MORE

- View User Guide
- Logout

Download the MyID Authenticator on your device, then click Add Device to get started.
To modify a device, click the Device Name in the table below.

Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/> Yubico YubiKey	cccbccuejck	Yes		Never
<input checked="" type="checkbox"/> Standard Authenticator	1542 4267 3515 9154	Yes		Never
<input type="checkbox"/> Standard Authenticator	2478 3158 1531 0322	Yes		Never
<input type="checkbox"/> Security Key	passkey	Yes	device-bound	Never

Edit Device Remove

3. Click **Remove**.

MyID SELF SERVICE PORTAL Kayla Bue (kayla.bue)

OPTIONS

- Account
- Grid Settings
- Phrase Settings
- One Time Code Settings
- YubiKey OTP Settings
- Devices**

MORE

- View User Guide
- Logout

Remove Device

Are you sure you want to remove the device "Standard Authenticator"?

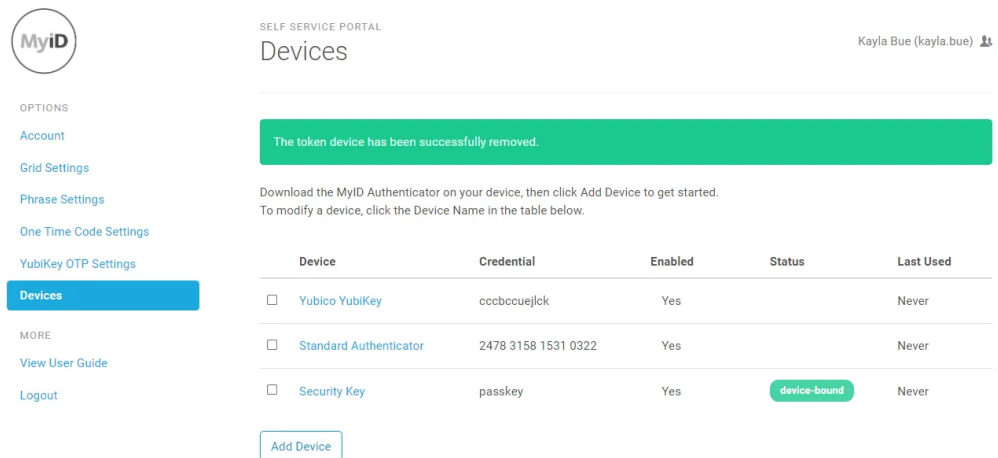
Yes No

Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/> Yubico YubiKey	cccbccuejck	Yes		Never
<input checked="" type="checkbox"/> Standard Authenticator	1542 4267 3515 9154	Yes		Never
<input type="checkbox"/> Standard Authenticator	2478 3158 1531 0322	Yes		Never
<input type="checkbox"/> Security Key	passkey	Yes	device-bound	Never

Edit Device Remove

4. Click **Yes**.


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



MyiD

SELF SERVICE PORTAL

Devices

Kayla Bue (kayla.bue) 

OPTIONS

- Account
- Grid Settings
- Phrase Settings
- One Time Code Settings
- YubiKey OTP Settings
- Devices**

MORE

- View User Guide
- Logout

The token device has been successfully removed.

Download the MyiD Authenticator on your device, then click Add Device to get started.
To modify a device, click the Device Name in the table below.

Device	Credential	Enabled	Status	Last Used
<input type="checkbox"/> Yubico YubiKey	cccbccuejck	Yes		Never
<input type="checkbox"/> Standard Authenticator	2478 3158 1531 0322	Yes		Never
<input type="checkbox"/> Security Key	passkey	Yes	device-bound	Never

Add Device