

intercede



MyID MFA and PSM

Version 5.0.8

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.

Apache log4net

Apache License Version 2.0, January 2004 <http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

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	6
Contents	7
1 Introduction	8
1.1 Language requirements	8
1.2 Change history	8
2 Accessing the Self Service Portal	9
2.1 Your first logon	10
3 Updating your account	11
3.1 Changing your phone number	11
3.2 Resetting your password	12
3.3 Unlocking your account	13
4 Changing your multi-factor authentication settings	14
4.1 Changing your Grid pattern	15
4.2 Settings your Phrase answers	17
4.3 Changing your One Time Code settings	18
4.4 Changing your YubiKey OTP settings	19
5 Setting up your own device	20
5.1 MyID Authenticator app	21
5.1.1 Legacy Authlogics Authenticator app	21
5.1.2 Alternative Authenticator apps	21
5.1.3 Adding your MyID Authenticator device to your account	22
5.2 Other authenticator apps	26
5.2.1 Adding your standard authenticator device to your account	26
5.3 YubiKey OTP	29
5.3.1 Adding your YubiKey device to your account	29
5.4 Passkey / FIDO Token	32
5.4.1 Adding your FIDO / Security Key device to your account	32
5.4.2 Adding a Synched Passkey to your account	37
5.5 Editing devices	41
5.6 Removing devices	43

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 customize the `appsettings.json` file for the Self Service Portal. the *SSP customization* section in the [MyID Authentication Server Installation and Configuration Guide](#) for details.

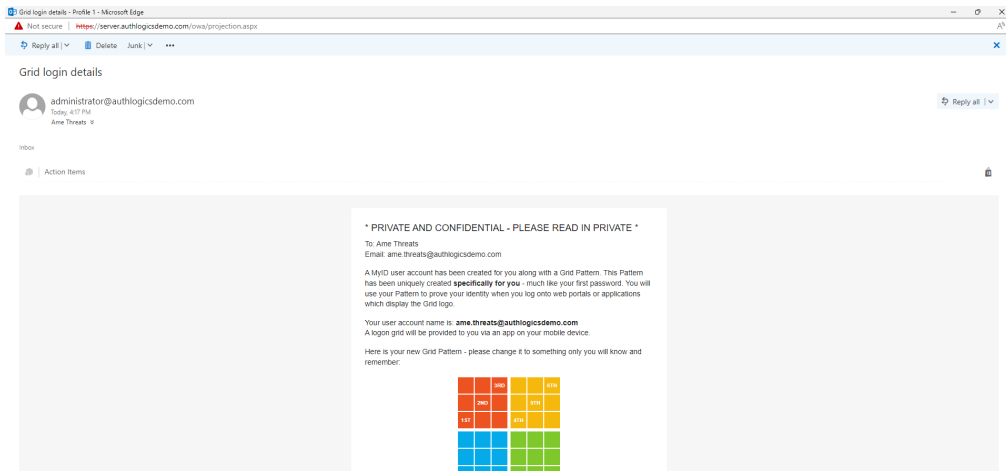
Product support and documentation are available only in English.

1.2 Change history

Version	Description
USR2055-01	Reformatted and released with MyID MFA and PSM version 5.0.7. The Authlogics Authenticator App is now the MyID Authenticator App. Added information on manual entry for keys for standard authenticators. Added information on separate add/remove token device options. Added information on multi-lingual support.
USR2055-5.0.8	Released with MyID MFA and PSM version 5.0.8.

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.

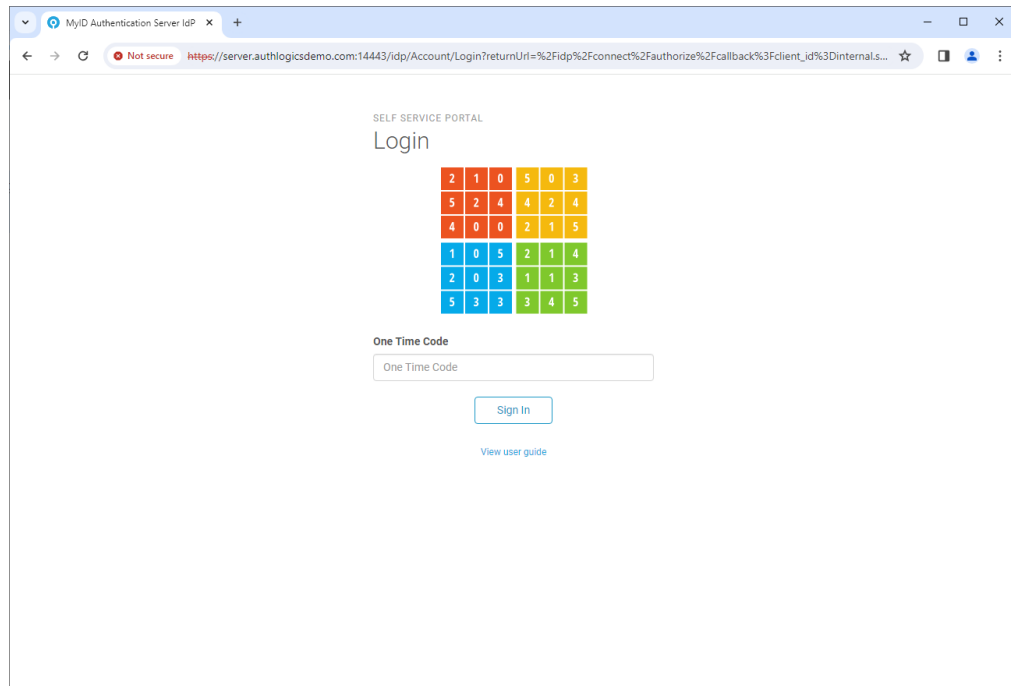


Once you have received your welcome email, you can log on. See section [2.1, Your first logon](#).

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.

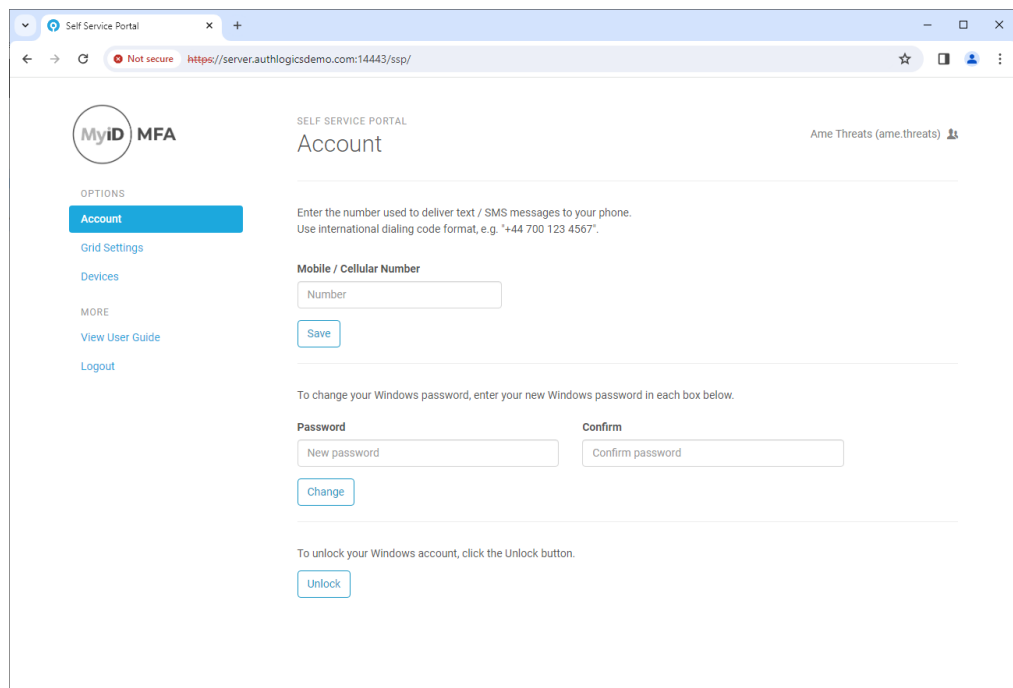
Using the portal, you can:

- 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.



The screenshot shows the 'Account' page in the Self Service Portal. The page title is 'Account' and the user is logged in as 'Ame Threats (ame.threats)'. The left sidebar contains a menu with 'Account' selected, along with 'Grid Settings', 'Devices', 'View User Guide', and 'Logout'. 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. There is also a section for changing the Windows password with 'New password' and 'Confirm password' fields and a 'Change' button. At the bottom, there is an 'Unlock' button.

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.

3.2 Resetting your password

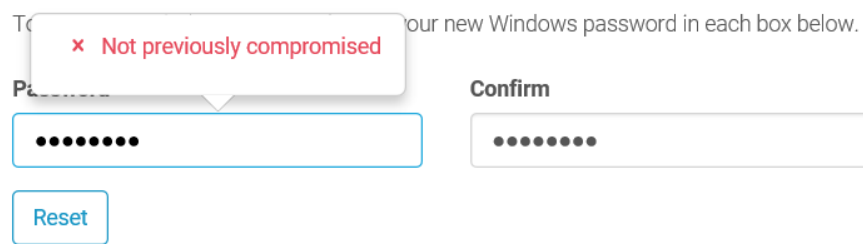
To reset your network password:

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

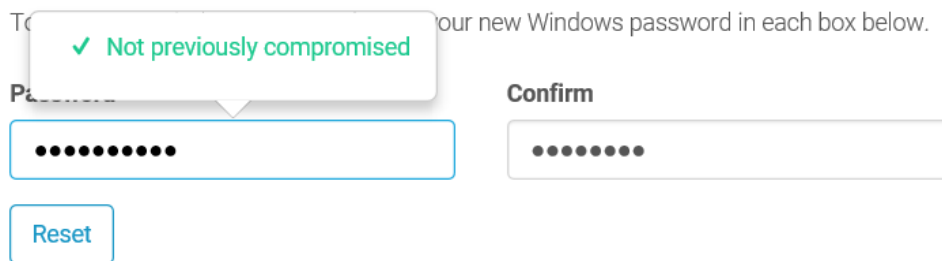
A popup balloon may appear that helps guide you through choosing a new password that meets your company policy and is secure.

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:



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.



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.

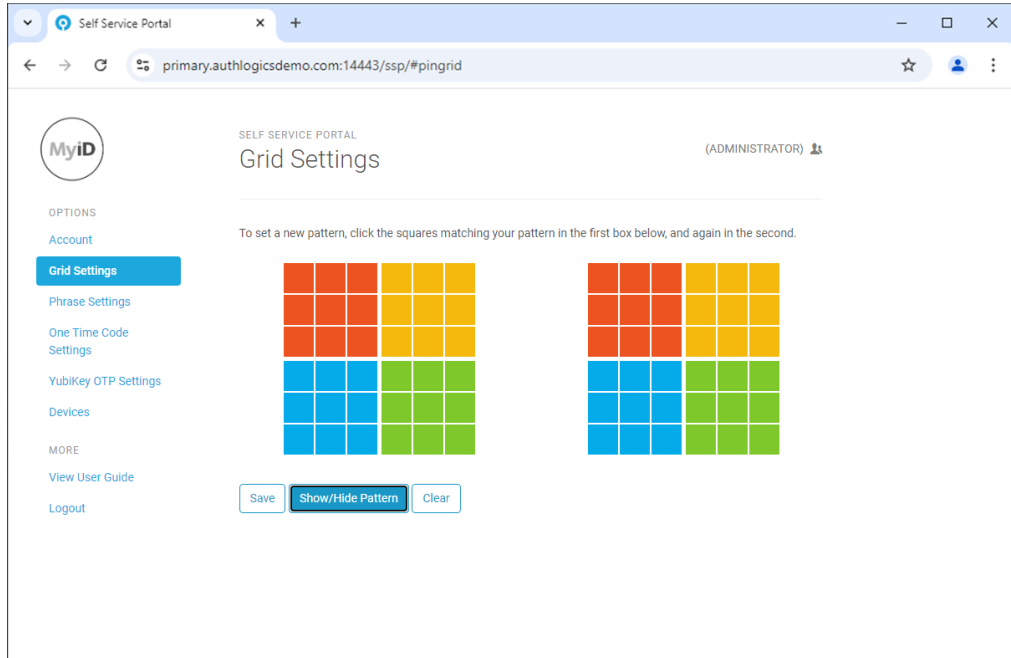
Using the portal, you can:

- 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

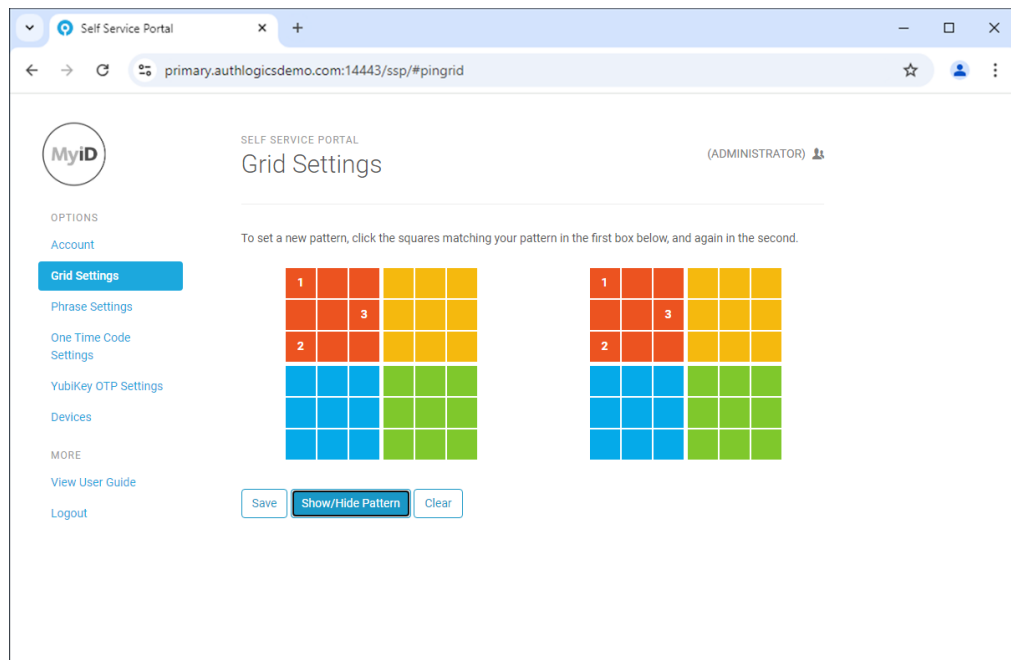
To change your Grid pattern:

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:

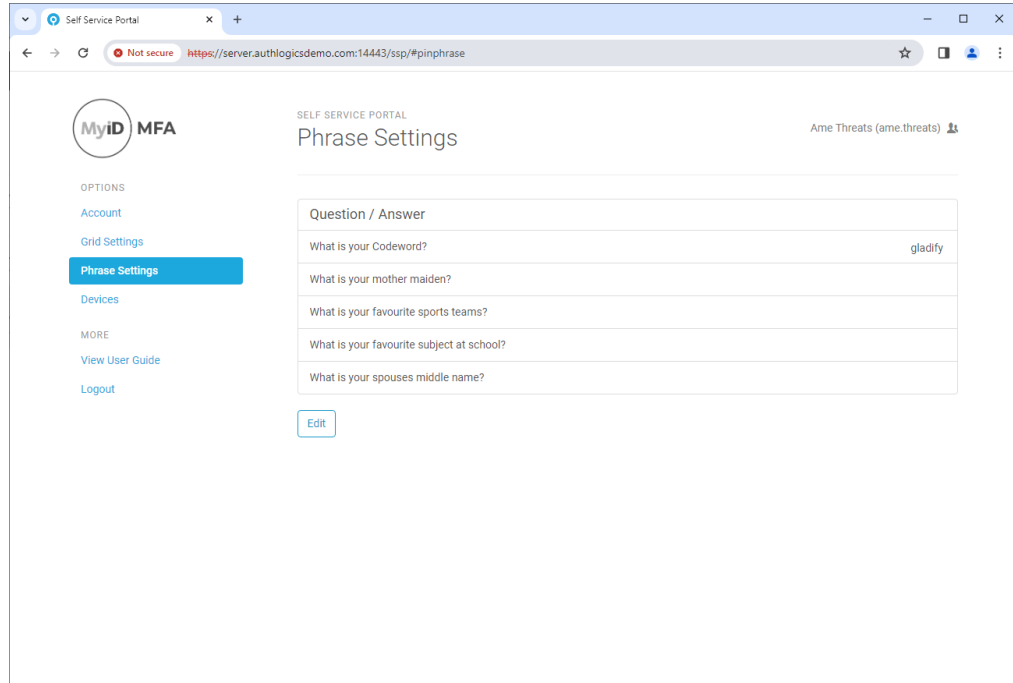


To configure whether or not users have the ability to display the numbered indicators, you can customize the `appsettings.json` file for the Self Service Portal. See the *SSP customization* section in the [MyID Authentication Server Installation and Configuration Guide](#) for details.

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.

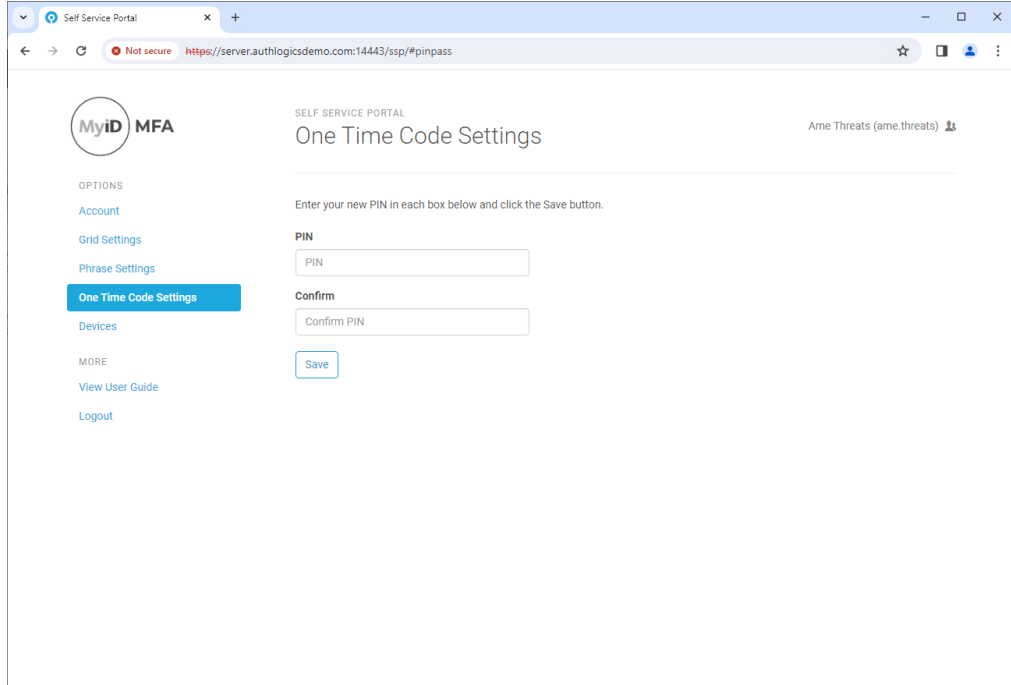
If successful, the following message appears:

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.

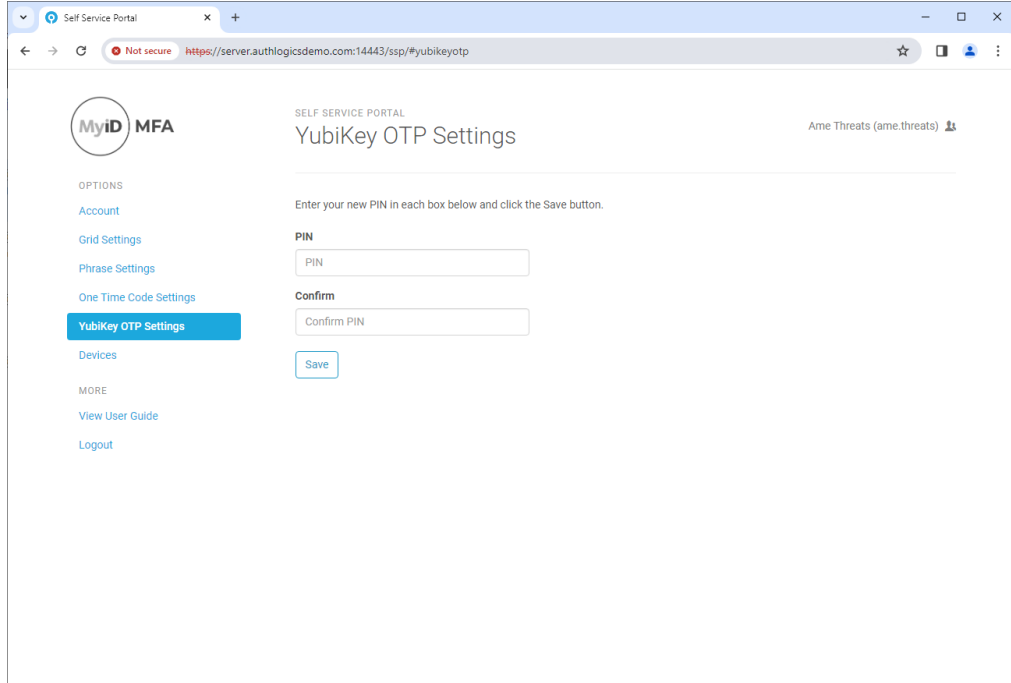
If successful, the following message appears:



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:



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

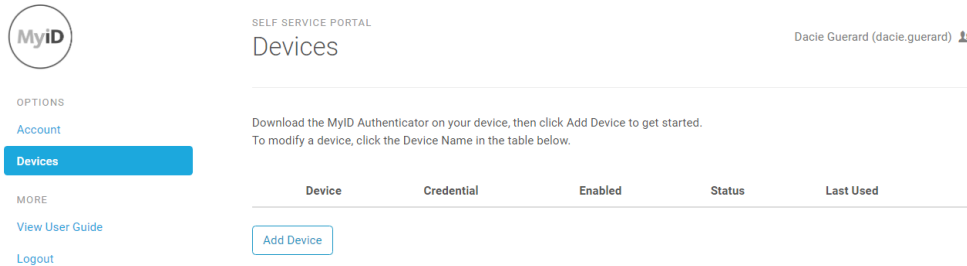
As an alternative, you can download a third-party OATH app from the relevant vendor. For example, you can use Microsoft or Google Authenticator.

5.1.3 Adding your MyID Authenticator device to your account

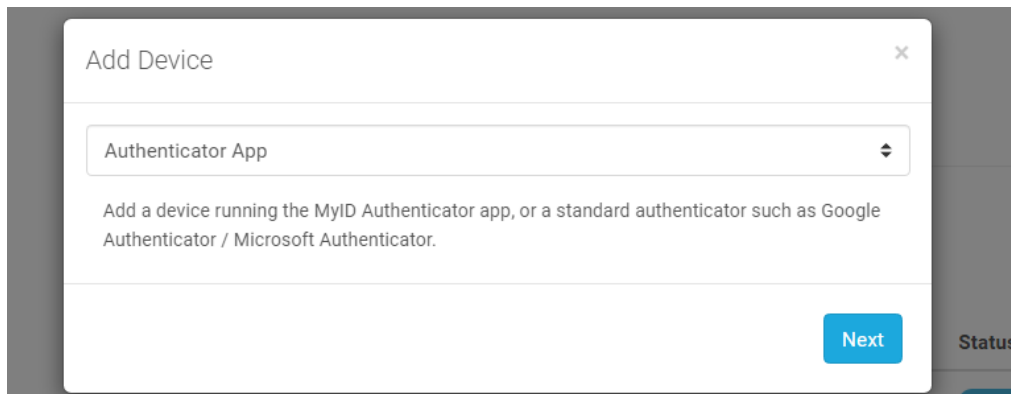
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the *MyID Authentication Server Installation and Configuration Guide*.

To add a device to your account:

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

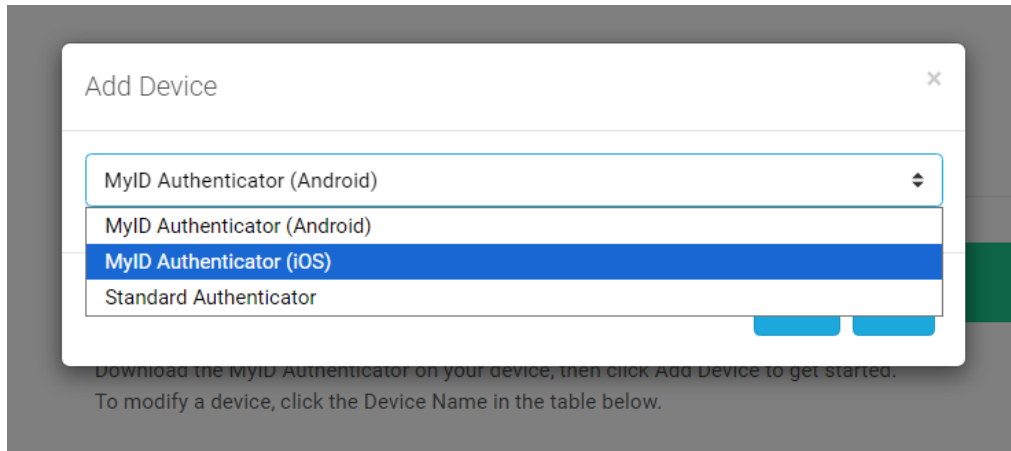


2. Install the MyID Authenticator App from the relevant App Store using the buttons on your device.
3. Click **Add Device**.



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

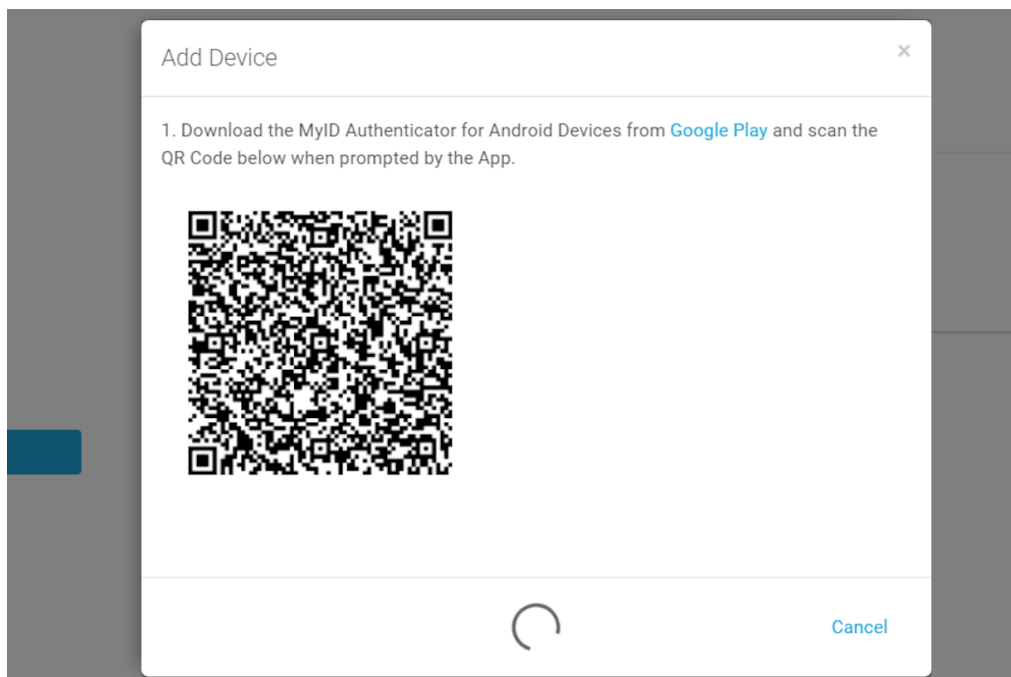
- 5. From the list, choose the type of device you have.



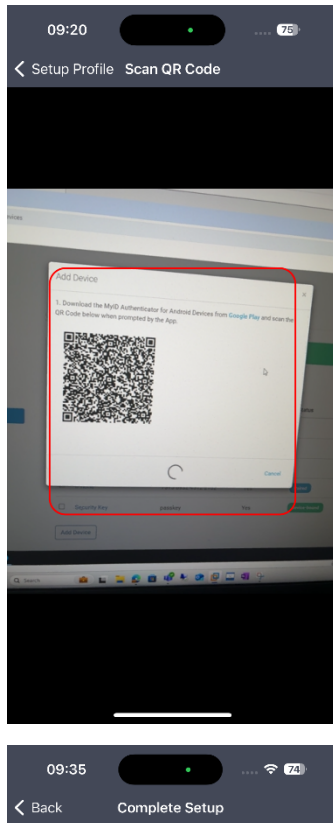
MyID Authenticator (Android) and **MyID Authenticator (iOS)** both relate to the MyID MFA app.

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

- 6. Click **Next**.



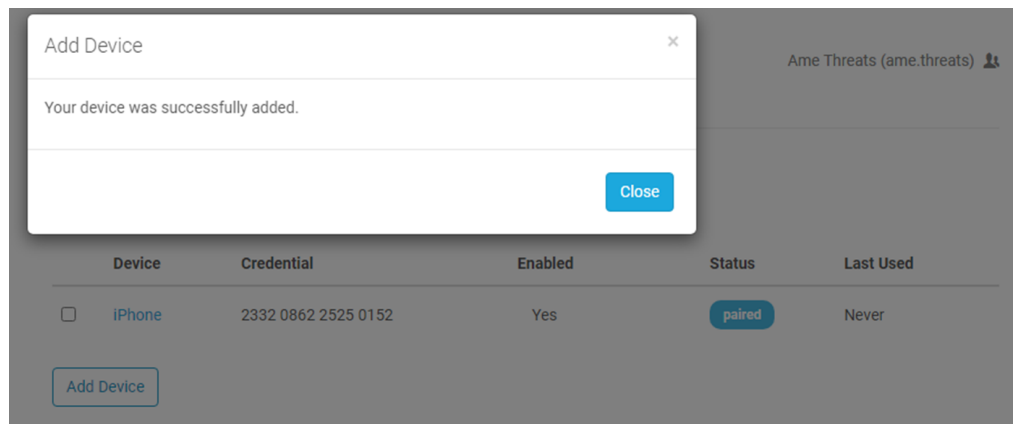
7. Scan the QR code with the MyID Authenticator App.



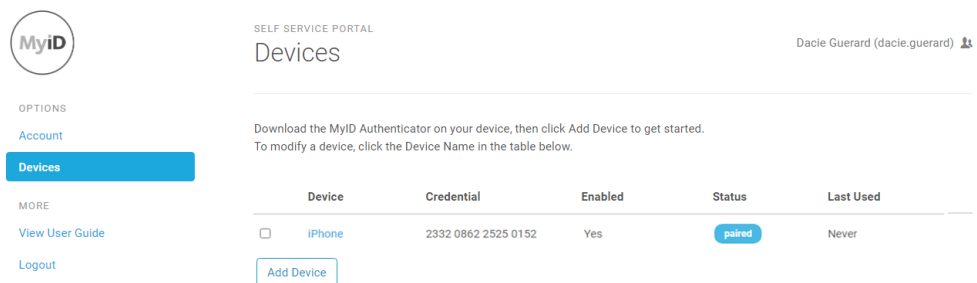
Device setup is complete.

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

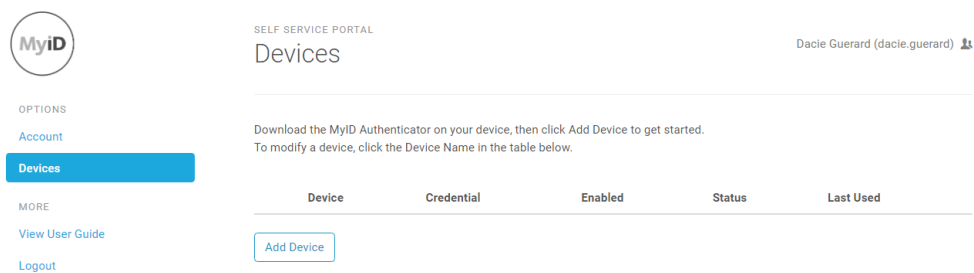
As an alternative to the MyID Authenticator app, you can download a third-party OATH app from the relevant vendor. For example, you can use Microsoft or Google Authenticator.

5.2.1 Adding your standard authenticator device to your account

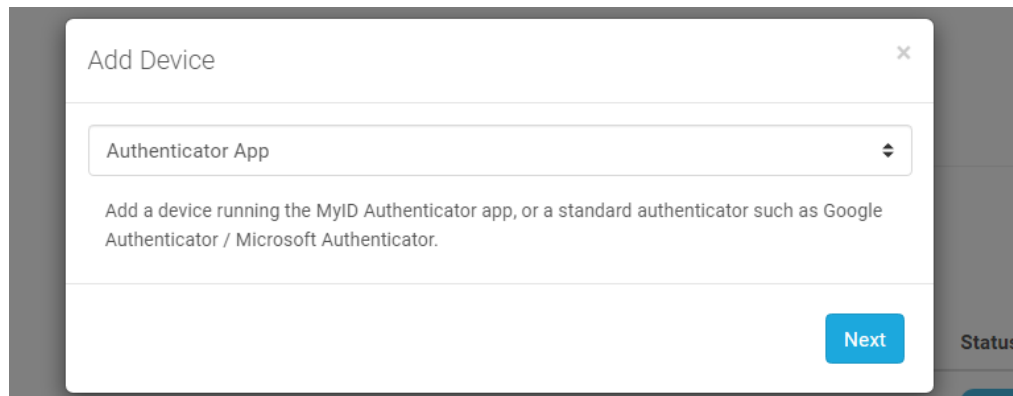
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the [MyID Authentication Server Installation and Configuration Guide](#).

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.

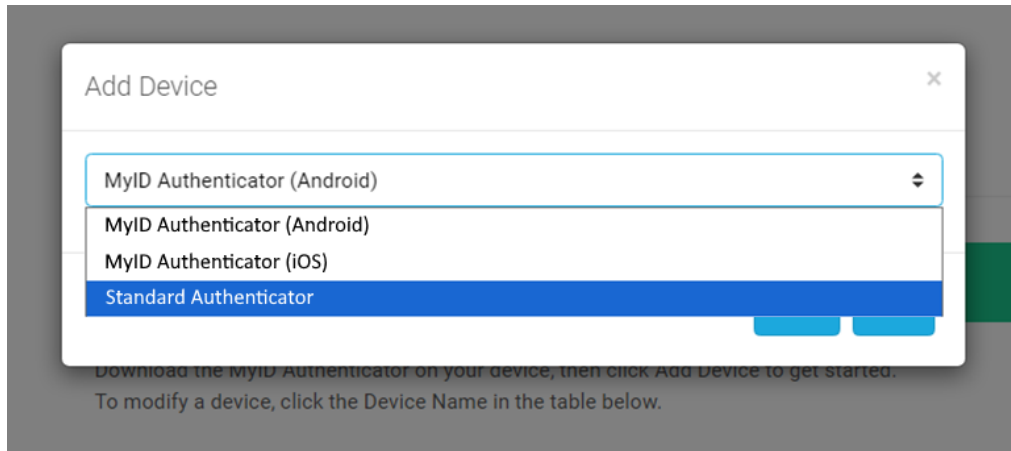


2. Install the relevant third-party app on your device.
3. Click **Add Device**.

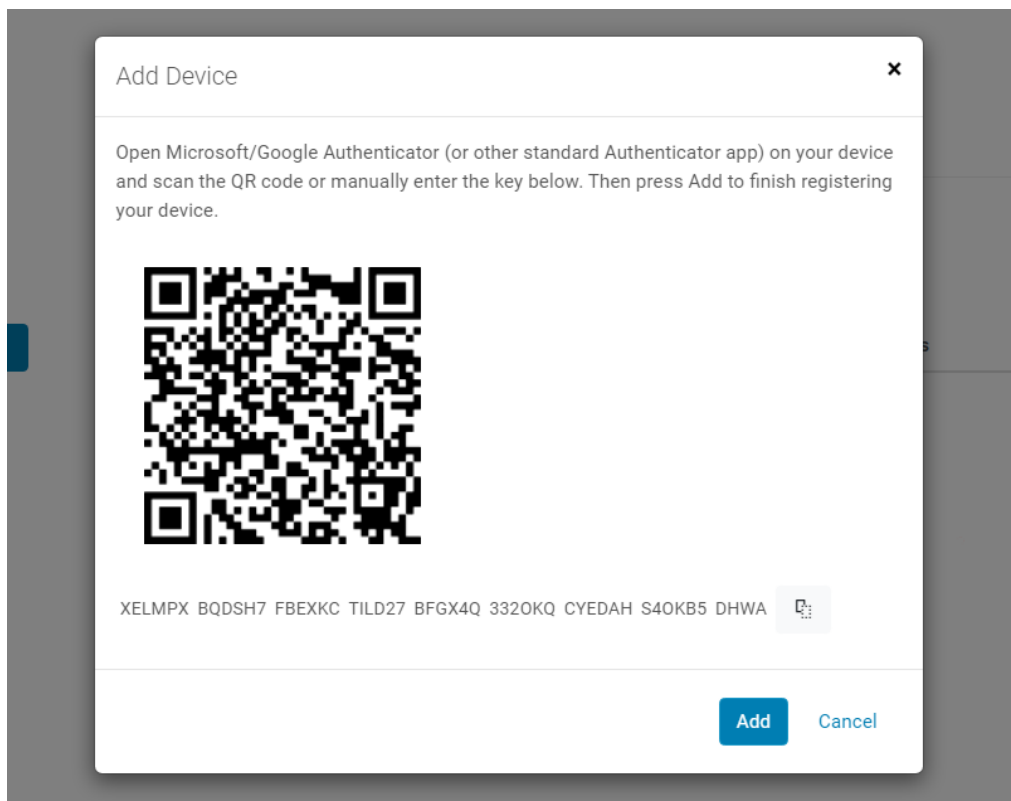


4. From the drop-down list, select **Authenticator App**.

- 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**.

SELF SERVICE PORTAL (ADMINISTRATOR)

MyID

OPTIONS

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

MORE

- View User Guide
- Logout

Devices

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

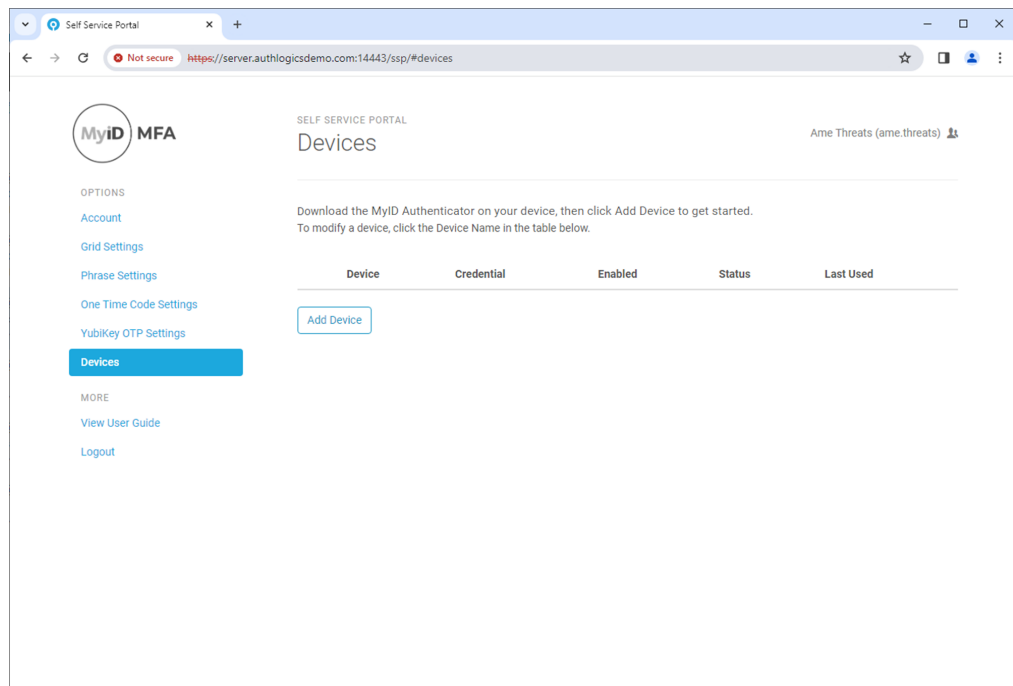
To provision your YubiKey OTP hardware device, insert the YubiKey token into your PC.

5.3.1 Adding your YubiKey device to your account

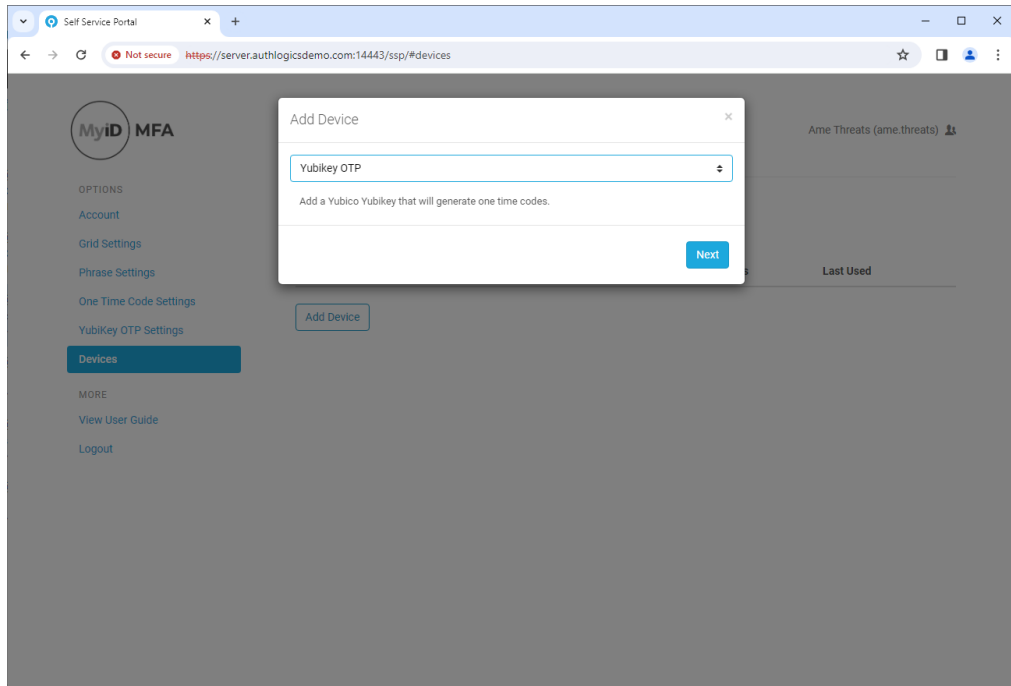
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the **MyID Authentication Server Installation and Configuration Guide**.

To add a device to your account:

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

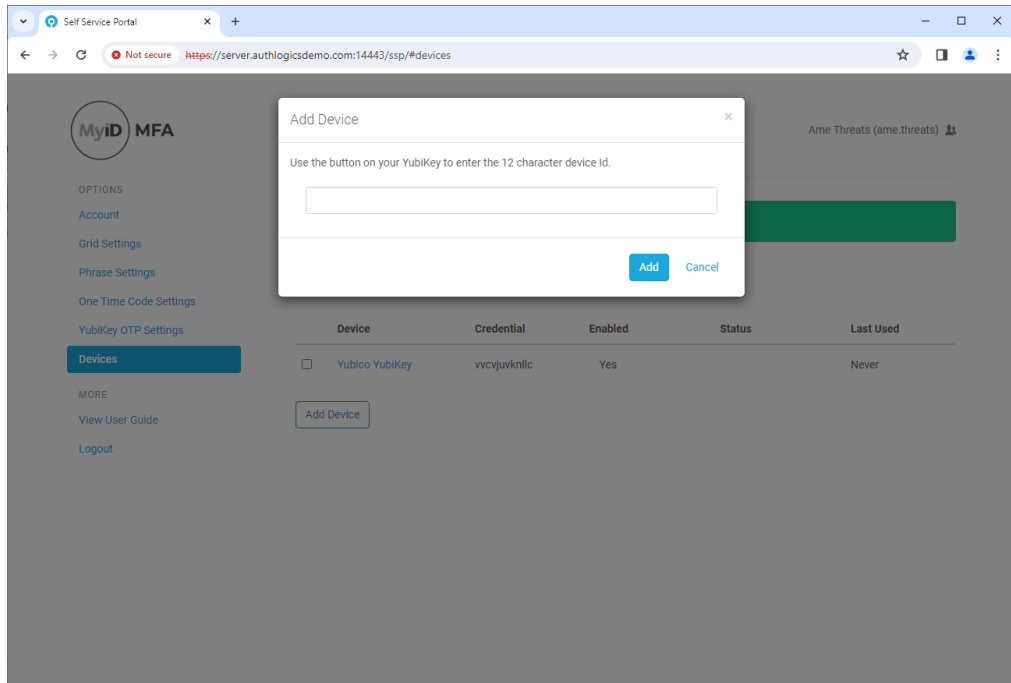


2. Click **Add Device**.

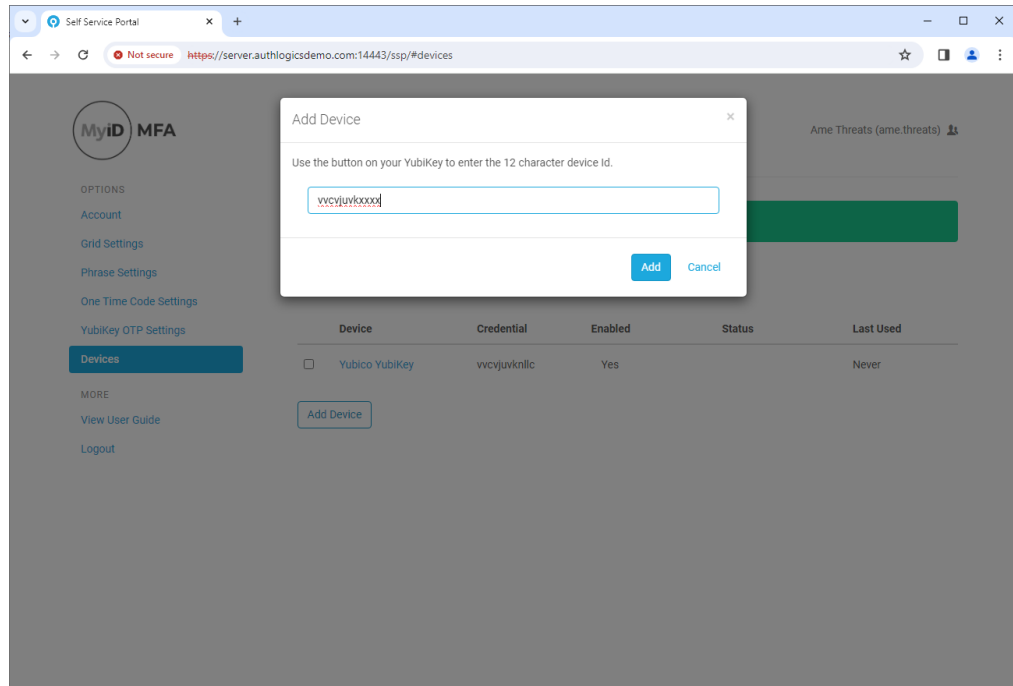


Note: If this option is not available, your user account has not been set up to use YubiKey tokens. Contact your administrator for assistance.

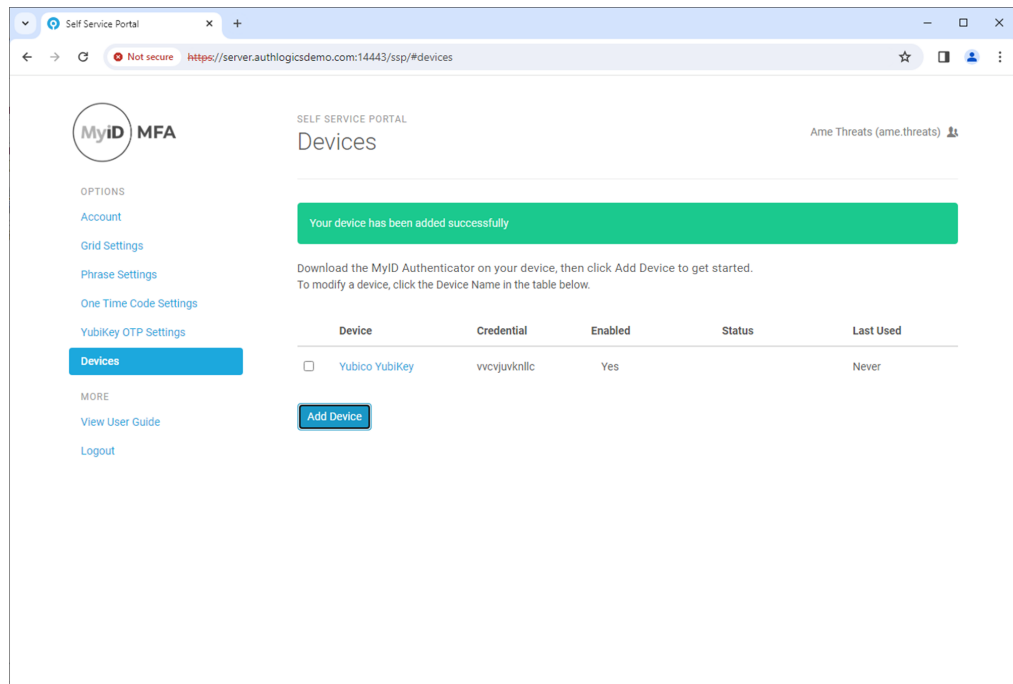
3. Select **YubiKey OTP** and click **Next**.



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

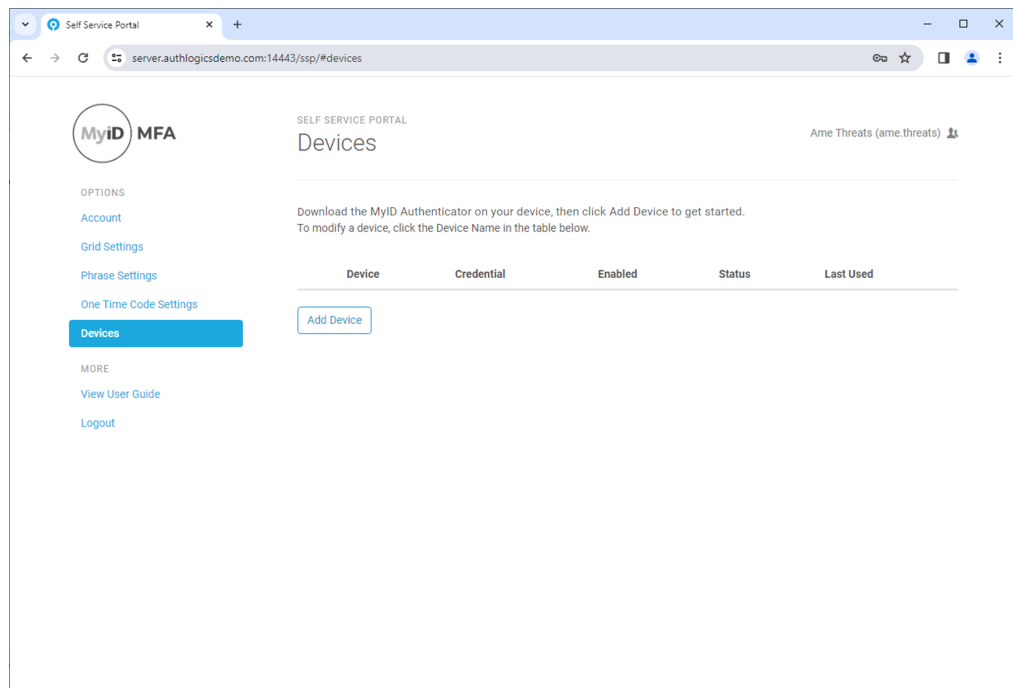
Before adding your FIDO Security Key or a Passkey to your account, ensure that no other MFA devices are attached to the workstation and that you have disconnected all Passkey / FIDO tokens from your PC.

5.4.1 Adding your FIDO / Security Key device to your account

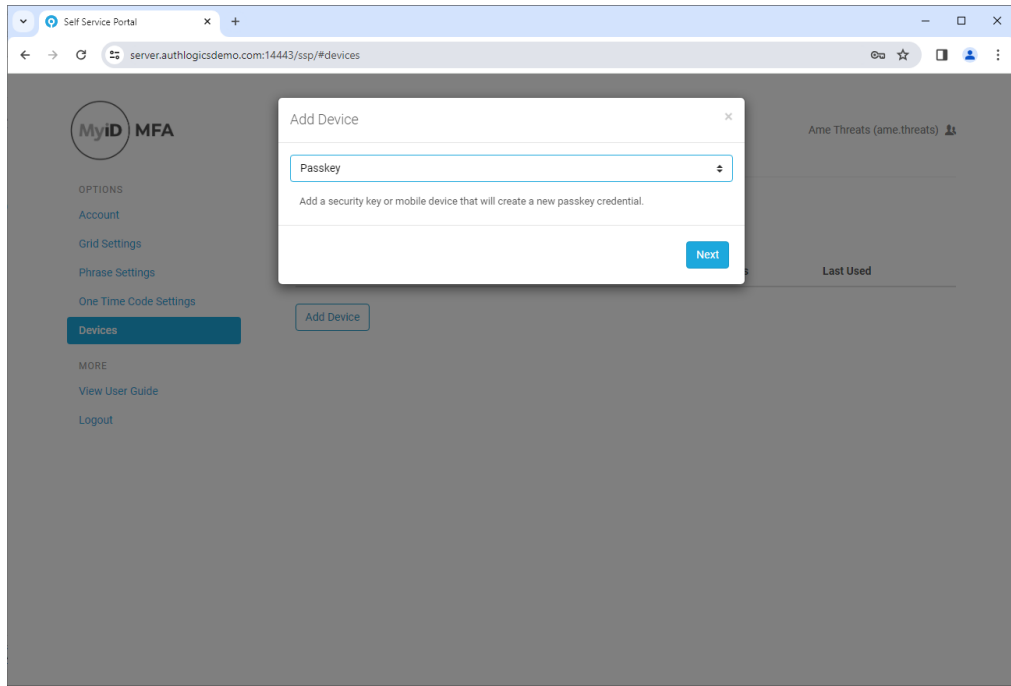
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the **MyID Authentication Server Installation and Configuration Guide**.

To add a FIDO Passkey Security Key to your account:

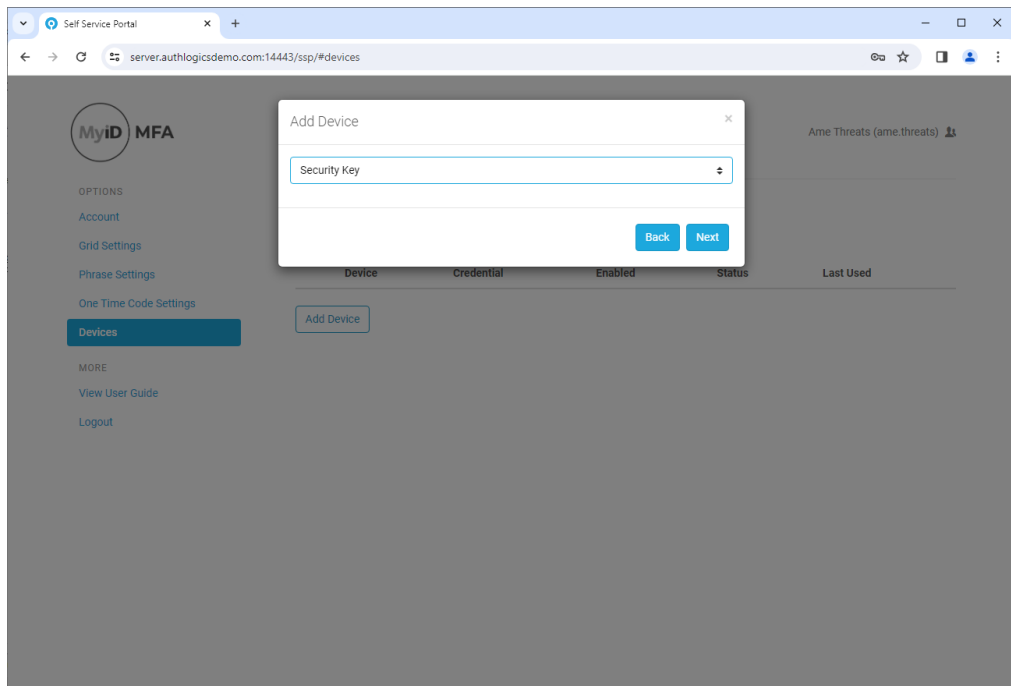
1. Log on to the Self Service Portal, and select **Devices** from the menu.



2. Click **Add Device**.



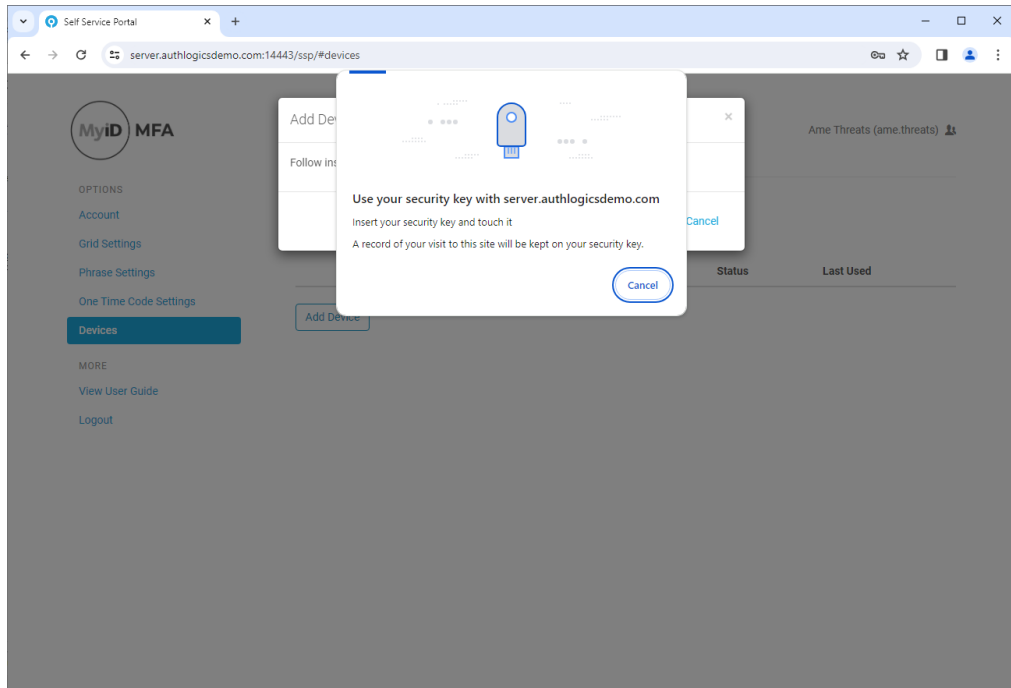
3. Select **Passkey** and click **Next**.



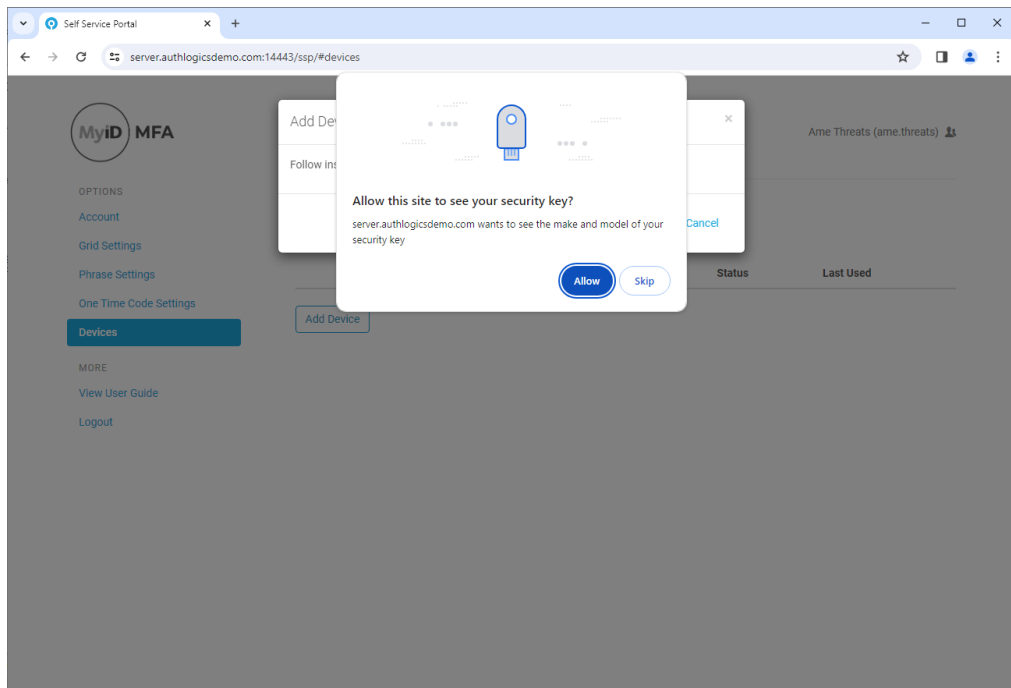
Note: If this option is not available, your user account has not been set up to use Passkeys. Contact your administrator for assistance.

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.

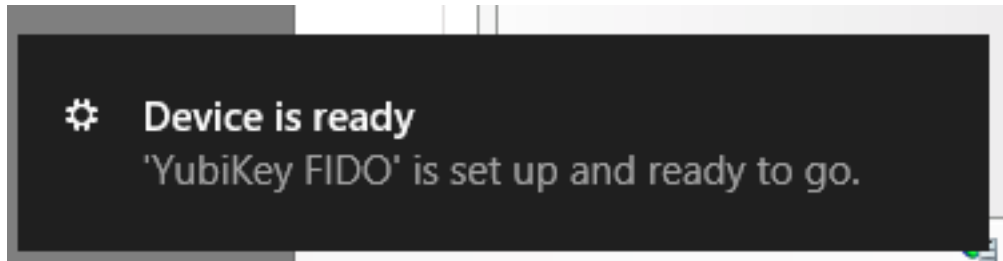
4. Select **Security Key** and click **Next**.



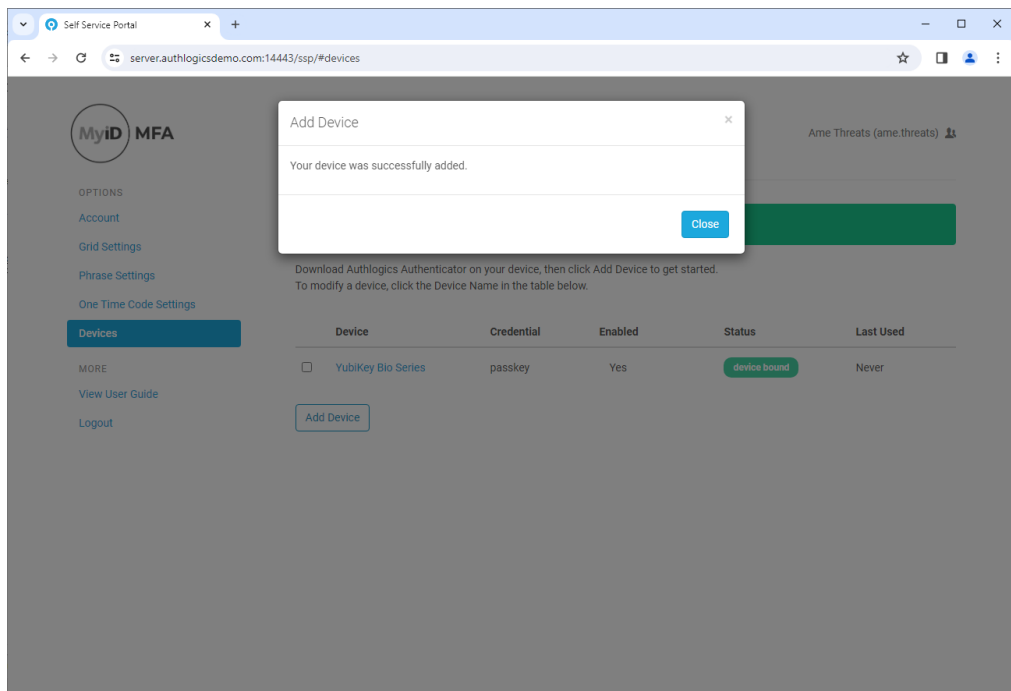
5. Insert your security key and press the FIDO token's button.



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

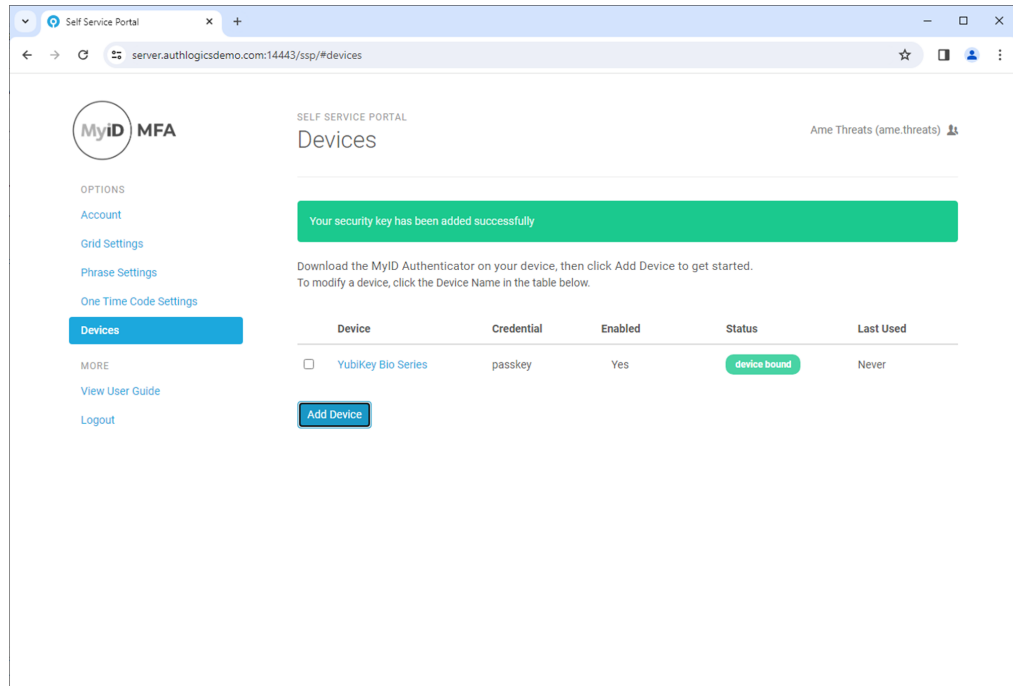


The underlying system notifies you that the FIDO token is set up and ready for use.



The device has been successfully added.

7. Click **Close**.

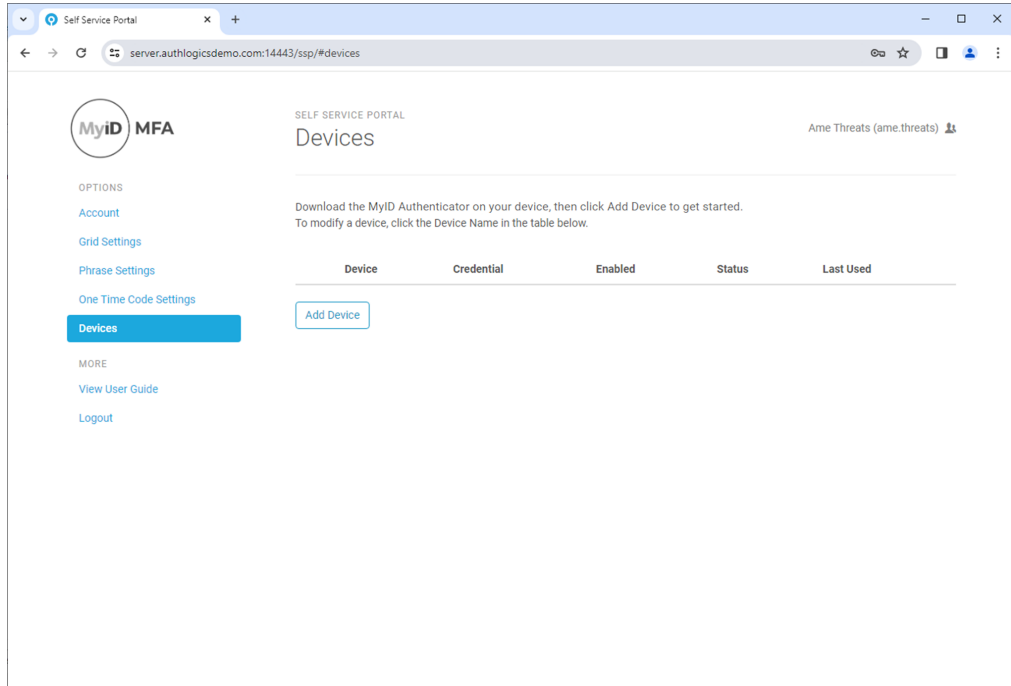


5.4.2 Adding a Synched Passkey to your account

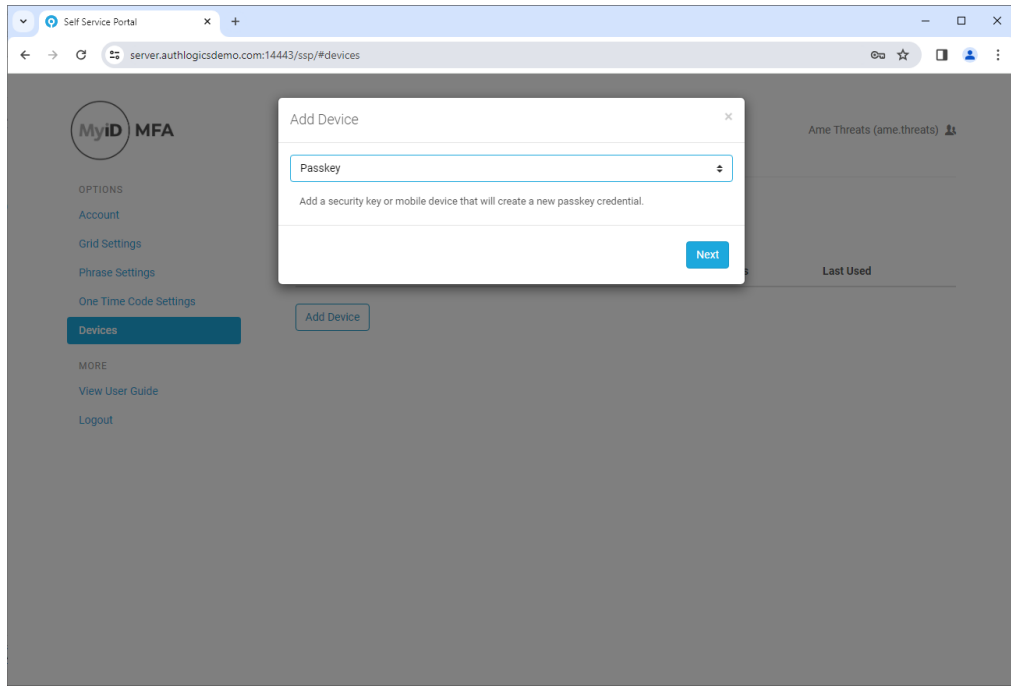
Note: You must have the **Add Token devices** option enabled to be able to add a new device. For more information, see the *Settings tab* subsection of the *Self Service Portal applications properties* section of the *MyID Authentication Server Installation and Configuration Guide*.

To add a FIDO Passkey Security Key to your account:

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

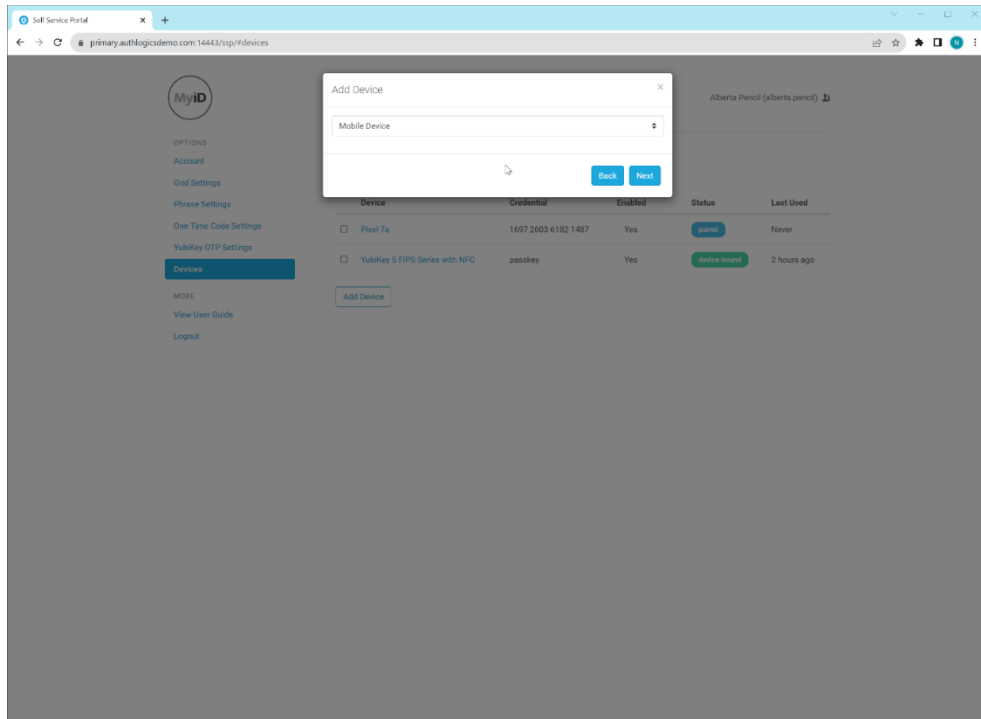


2. Click **Add Device**.

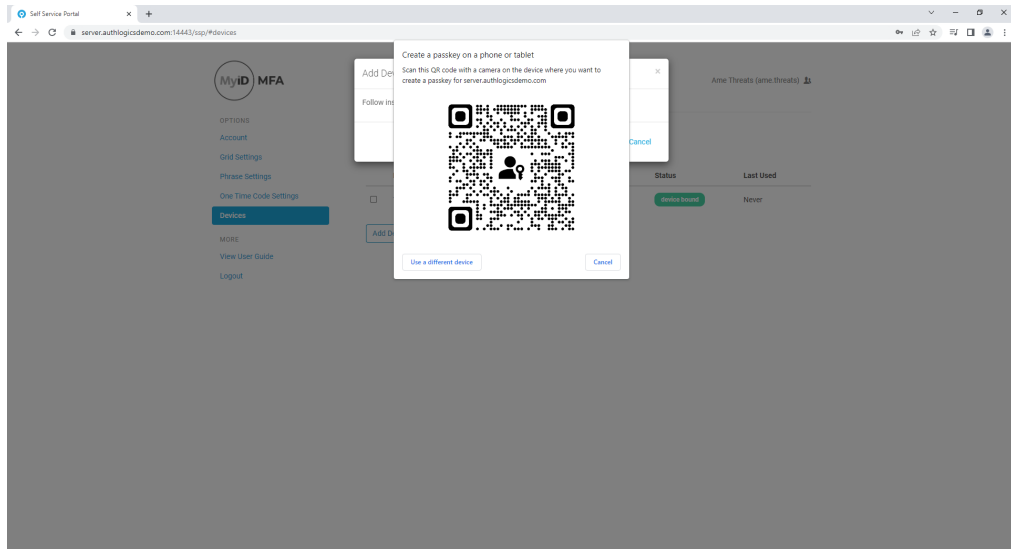


Note: If this option is not available, your user account has not been set up to use Passkeys. Contact your administrator for assistance.

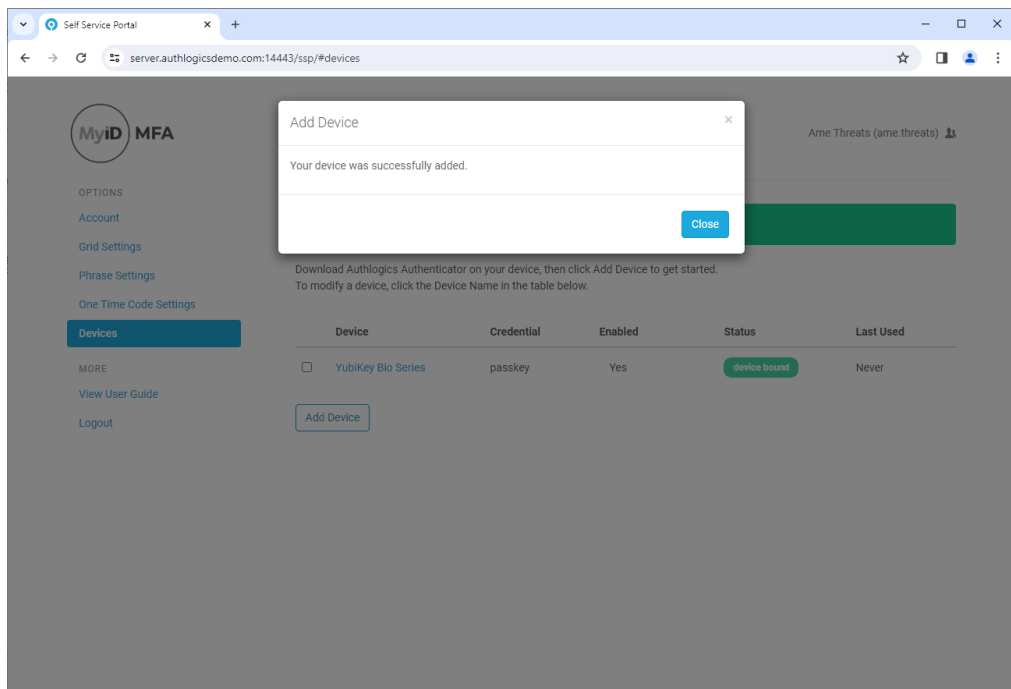
3. Select **Passkey** and click **Next**.



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

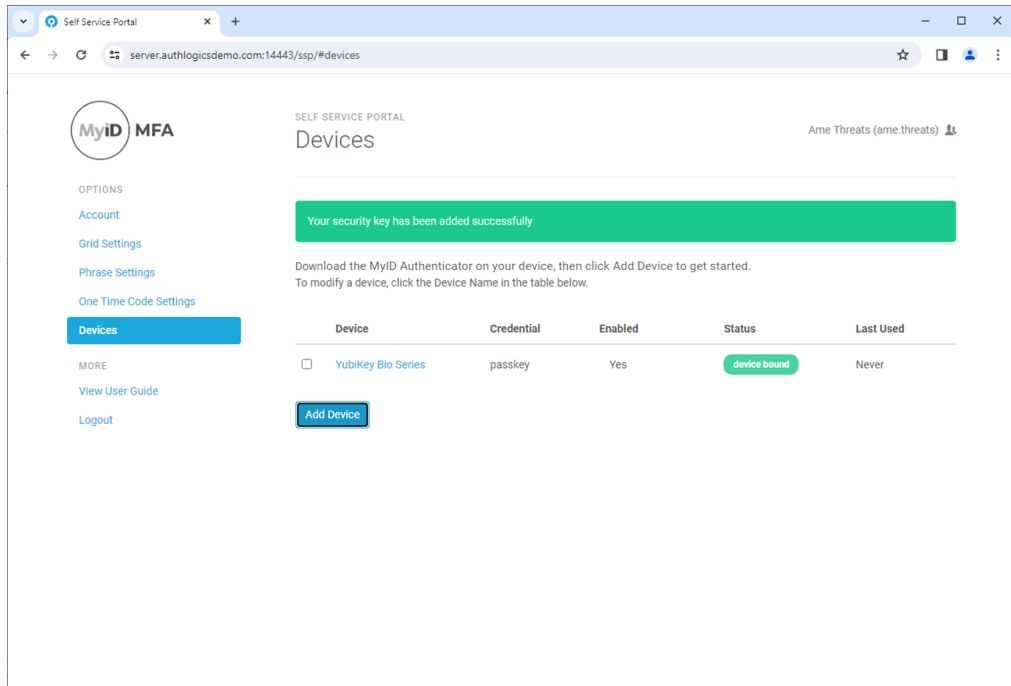


5. Ensure that Bluetooth is enabled on both the mobile device and your workstation. If Bluetooth is *not* enabled on your workstation, the above QR Code is not displayed.
6. Open your mobile phone’s camera and scan the QR Code.
7. Once you have scanned the QR Code, follow the instructions on your mobile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

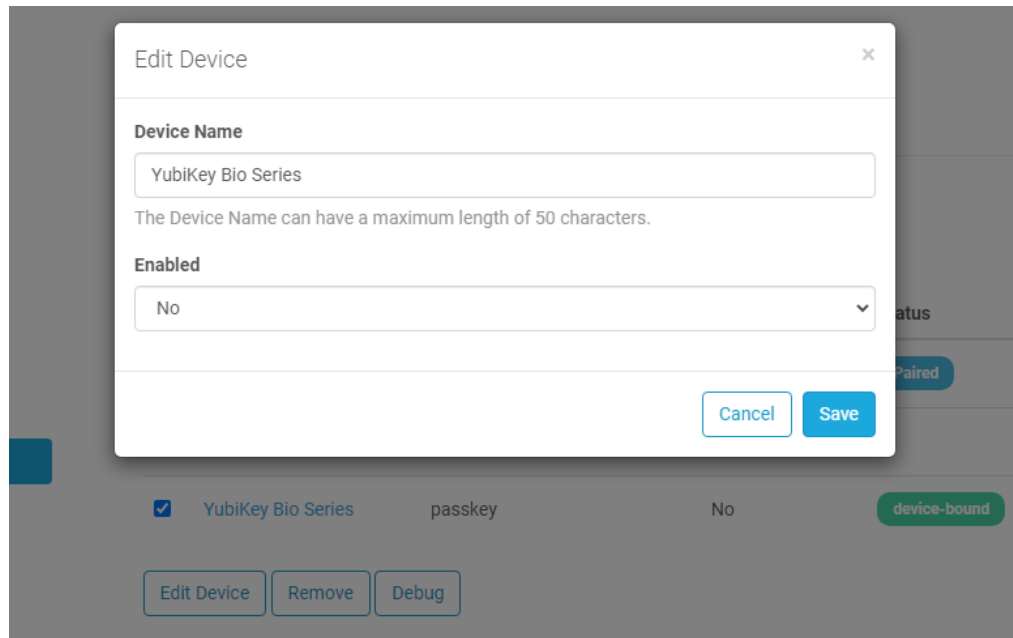
To edit a device:

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

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*.

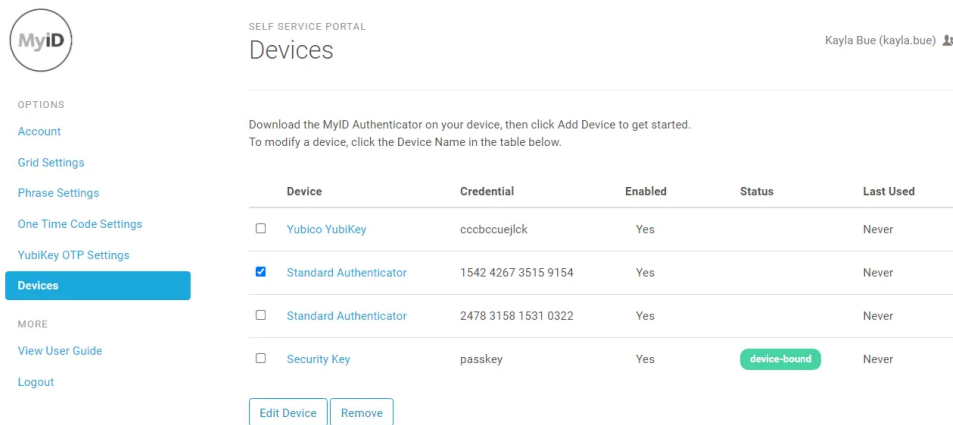
You can remove a device through the SSP.

To remove a device:

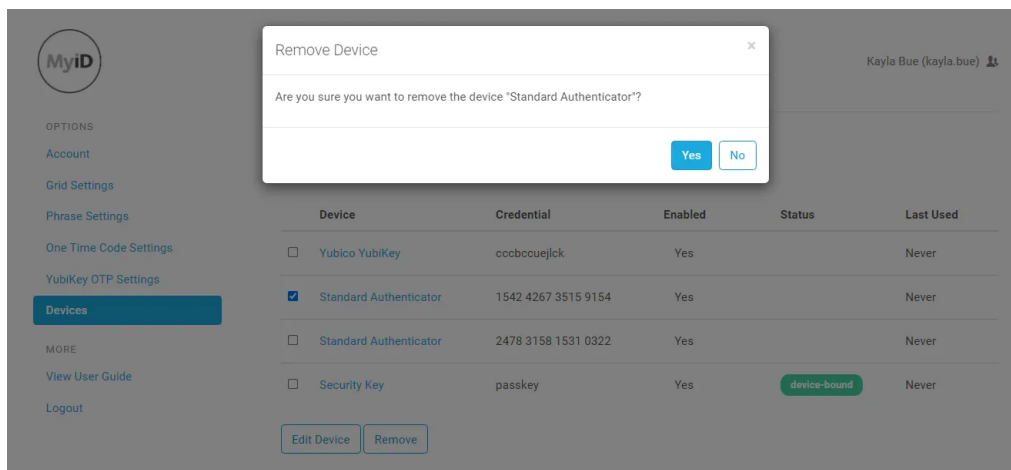
1. Log on to the Self Service Portal, and select **Devices** from the menu.

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.

SELF SERVICE PORTAL

MyiD

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	ccc6ccuejck	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