

MyID Self Service Portal User Guide

For MyID MFA and PSM



Call us on: +44 (0)1455 558 111 (UK & EMEA)
+1 408 706 2866 (US)

Email us: info@intercede.com

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Intercede may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Intercede, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Intercede on the issues discussed as of the date of publication. Because Intercede must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Intercede, and Intercede cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. INTERCEDE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2024 Intercede. All rights reserved.

TABLE OF CONTENTS

Introduction.....	3
Your Welcome.....	3
Your first logon.....	3
Updating your account	4
Changing your phone number.....	4
Resetting your password.....	5
Unlocking your account.....	5
Changing your Grid pattern	6
Setting your Phrase answers	7
Changing your One Time Code Settings	8
Changing your YubiKey OTP Settings	9
Setup your own device	10
MyID Authenticator	10
Adding your device to your account.....	10
YubiKey OTP	15
Adding your device to your account.....	15
Passkey / FIDO Token.....	18
Adding your FIDO / Security Key to your account	18
Adding a Synced Passkey to your account.....	21

Introduction



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.

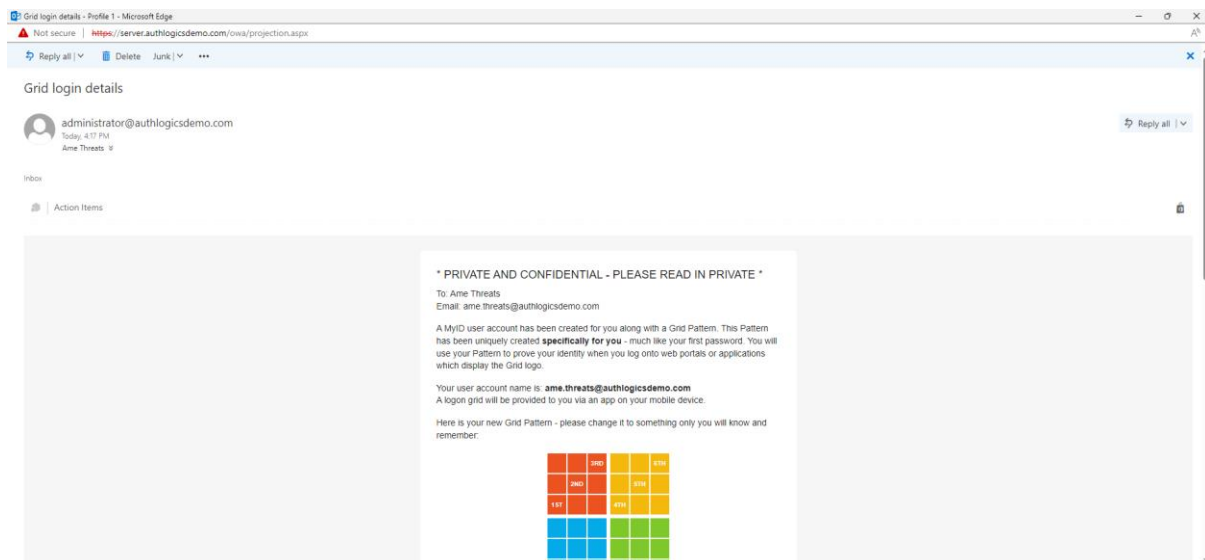
The MyID Self Service Portal is a website which allows the end user to perform simple tasks without having to get help from the IT helpdesk. End users can:

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

Tip: Some of these features may have been disabled by your IT administrator.

Your Welcome

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, please contact your IT team.

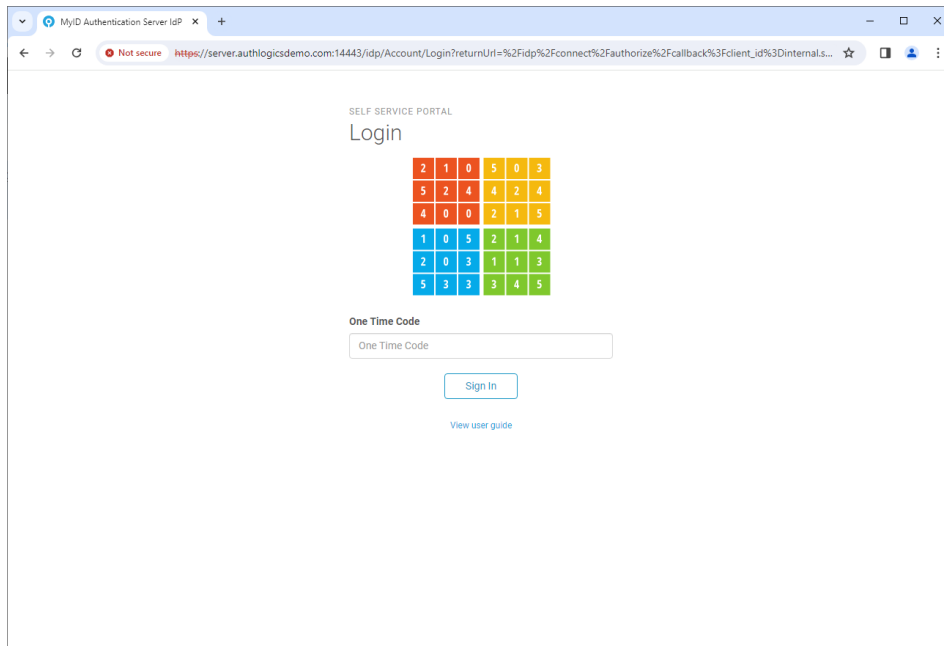


Your first logon

Click the link in your welcome email to access the Self Service Portal.

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

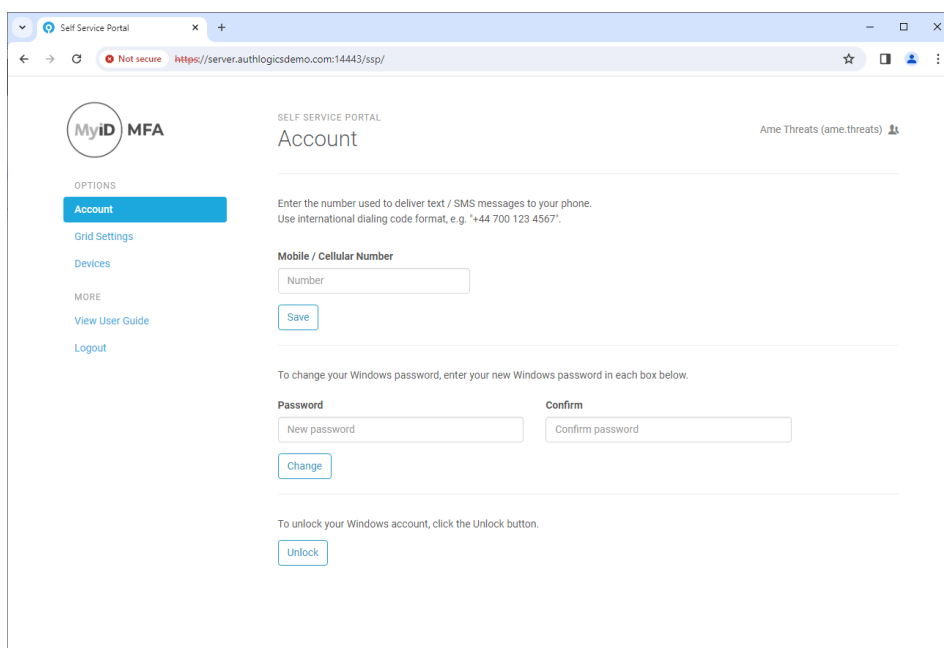
Tip: You can get your login details by using the information in the welcome email.



Updating your account

Changing your phone number

To change your Mobile / Cellular phone number, reset your password or unlock your account, select **Account** from the menu.



To change your phone number, enter your new number and click **Save**, and if successful, the following message will be displayed:

www.intercede.com | info@intercede.com | +44(0)1455 558 111| +1 888 646 6943

Your Mobile / Cellular phone number was updated successfully.

Resetting your password

To reset your network password simply enter your new password in both password boxes.

A popup balloon may appear which help guide you through choosing a new password which meets the 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:

To reset your new Windows password in each box below.

✗ Not previously compromised

Password

Confirm

If you choose a good password:

To reset your new Windows password in each box below.

✓ Not previously compromised

Password

Confirm

Click **Reset** to save the new password, and if successful, the following message will be displayed:

Your Password was updated successfully.

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.

To unlock your Windows account, click the Unlock button.

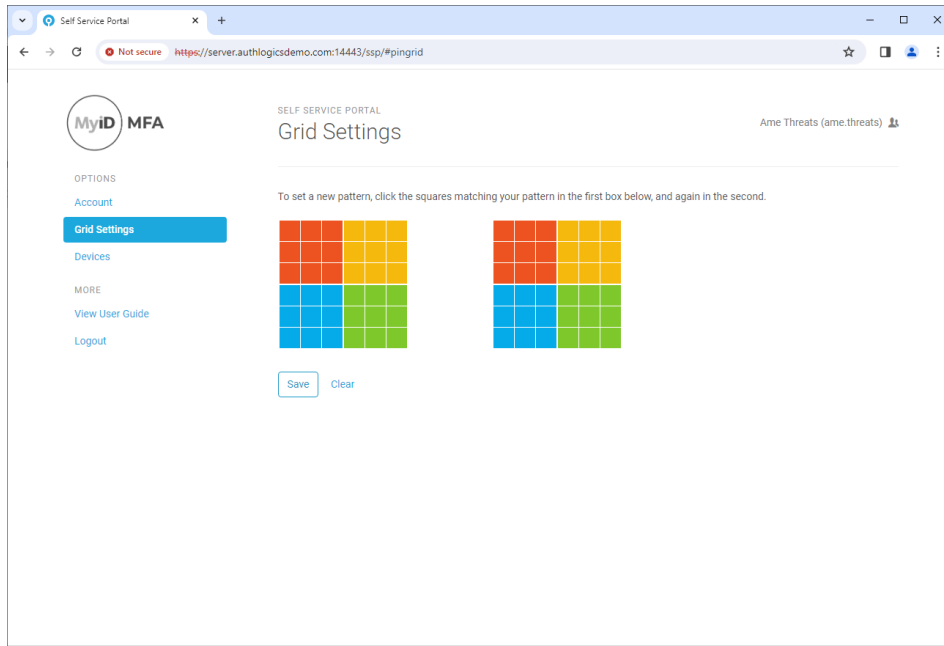
Simply click **Unlock**, and if successful, the following message will be displayed:

Your account was unlocked successfully.

Changing your Grid pattern

To change your Grid pattern, select **Grid Settings** from the menu.

On the first grid, click the squares you will use for your new pattern. Then click the same squares on the second grid to confirm your new pattern.



Click **Save** to apply the changes, and if successful, the following message will be displayed:

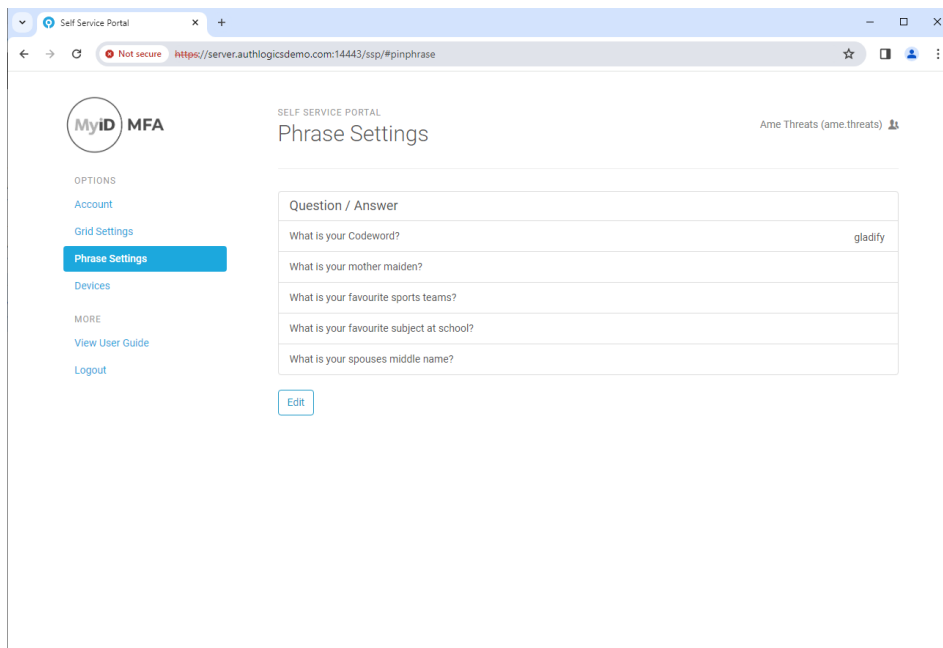
Your Pattern was updated successfully.

Setting your Phrase answers

To answer the Phrase questions provided by your IT team, select **Phrase settings** from the menu.

To add or update your answers, click **Edit**. Highlight the question you wish to answer and type in your answer.

Tip: Spaces are not counted as a letter, so multiple word answers will be treated as a single word.



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 with the "MyID MFA" logo and a list of options: "Account", "Grid Settings", "Phrase Settings" (which is highlighted with a blue bar), "Devices", "MORE", "View User Guide", and "Logout". The main content area has a header "Ame Threats (ame:threats)" and 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 is an "Edit" button.

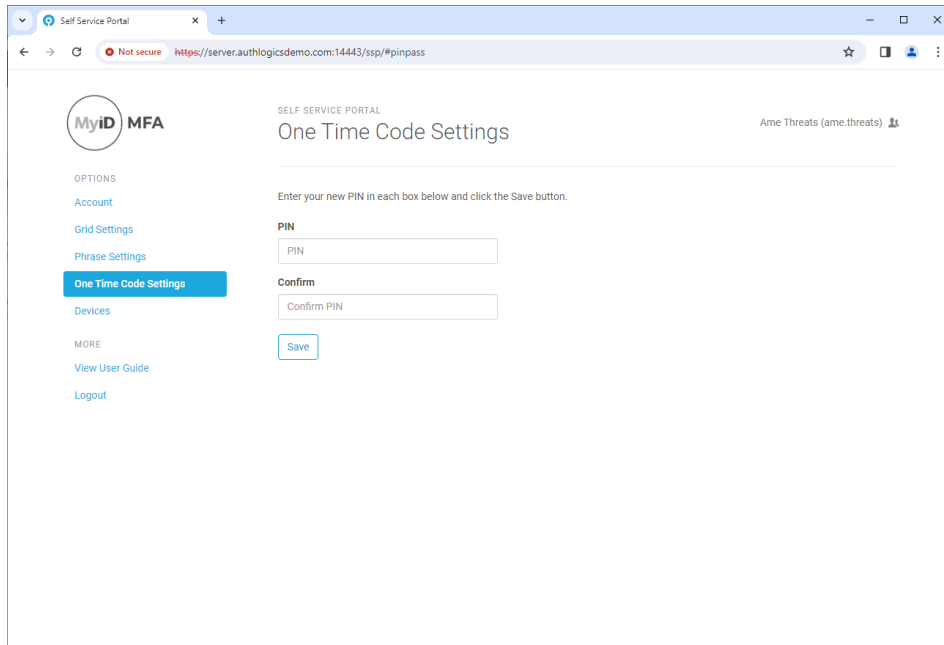
Click **Save** to apply the changes, and if successful, the following message will be displayed:

PINphrase answers have been successfully updated.

Changing your One Time Code Settings

To change your One Time Code PIN, select **One Time Code Settings** from the menu.

Enter your new PIN code in both PIN boxes.



The screenshot shows a web browser window with the address bar displaying "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 the following items: "Account", "Grid Settings", "Phrase Settings", "One Time Code Settings" (highlighted in blue), "Devices", "MORE", "View User Guide", and "Logout". The main content area contains the text "Enter your new PIN in each box below and click the Save button." Below this text are two input fields: "PIN" and "Confirm". The "Confirm" field has a placeholder text "Confirm PIN". A "Save" button is located below the "Confirm" field. In the top right corner, there is a user profile icon and the text "Ame Threats (ame.threats)".

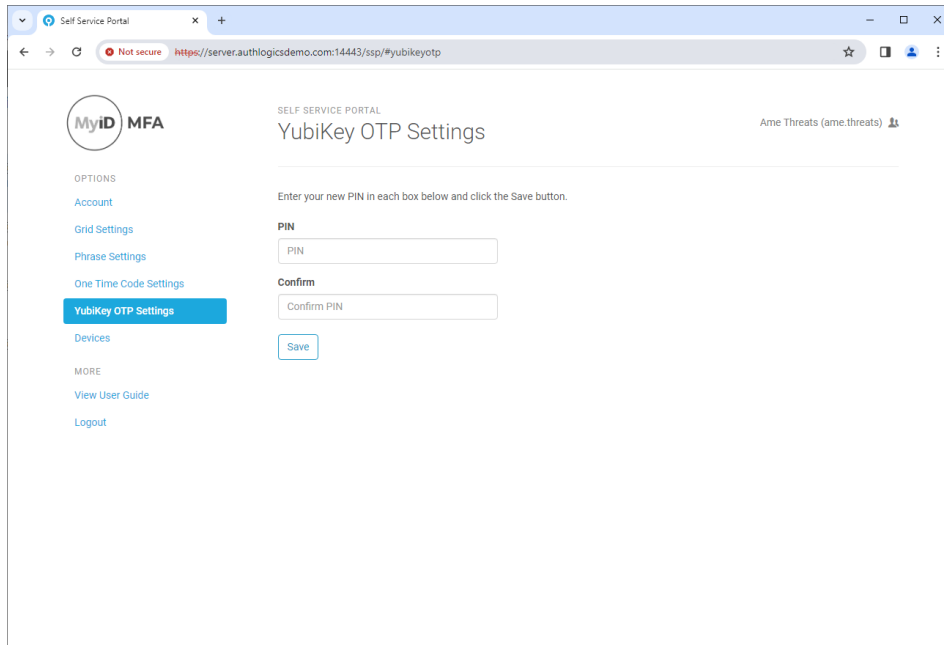
Click **Save** to apply the changes, and if successful, the following message will be displayed:

Your PIN was updated successfully.

Changing your YubiKey OTP Settings

To change your YubiKey OTP PIN, select **YubiKey OTP Settings** from the menu.

Enter your new PIN code in both PIN boxes.



The screenshot shows a web browser window with the address bar displaying "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 with the following items: "MyID MFA", "Account", "Grid Settings", "Phrase Settings", "One Time Code Settings", "YubiKey OTP Settings" (highlighted in blue), "Devices", "MORE", "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". The "Confirm" field has a label "Confirm PIN" above it. A "Save" button is located below the "Confirm" field. In the top right corner, there is a user profile icon and the text "Ame Threats (ame.threats)".

Click **Save** to apply the changes, and if successful, the following message will be displayed:

Your PIN was updated successfully.

Setup your own device

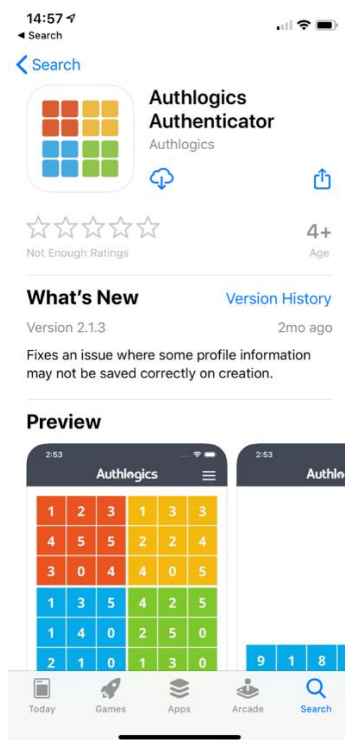
MyID supports authentication technologies. These technologies include MyID MFA technologies PUSH, One Time Code and Grid authentication, YubiKey OTPs and Fido tokens, passkeys and standard OATH authenticators like Google and Microsoft Authenticator. The following section details how to enable the various technologies supported within MyID MFA.

MyID Authenticator

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



Tip: When installing the Authlogics Authenticator app please ensure that the device's clock and time zone are correct otherwise you may not be able to logon with the app.

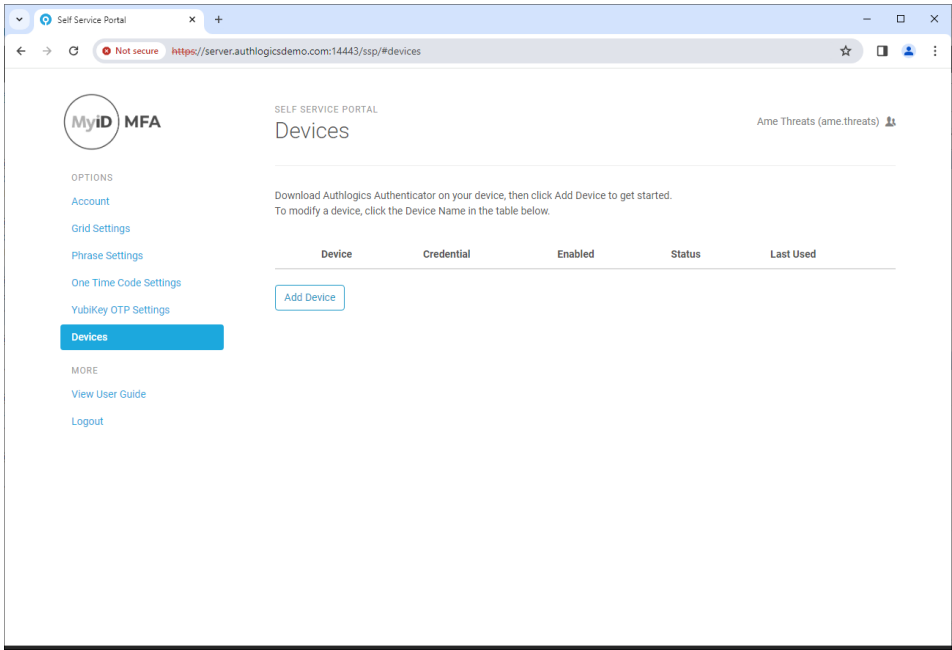


Alternatively, download the 3rd-party OATH app from the relevant vendor. For example, Microsoft or Google Authenticator

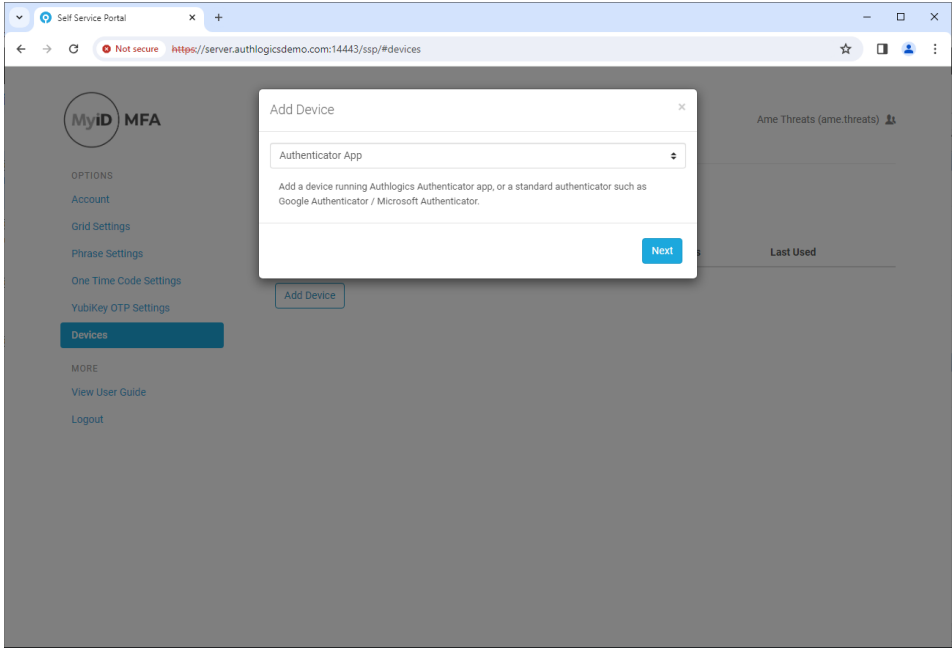
Adding your device to your account

To add a device to your account logon to the Self Service Portal and select **Devices** from the menu.

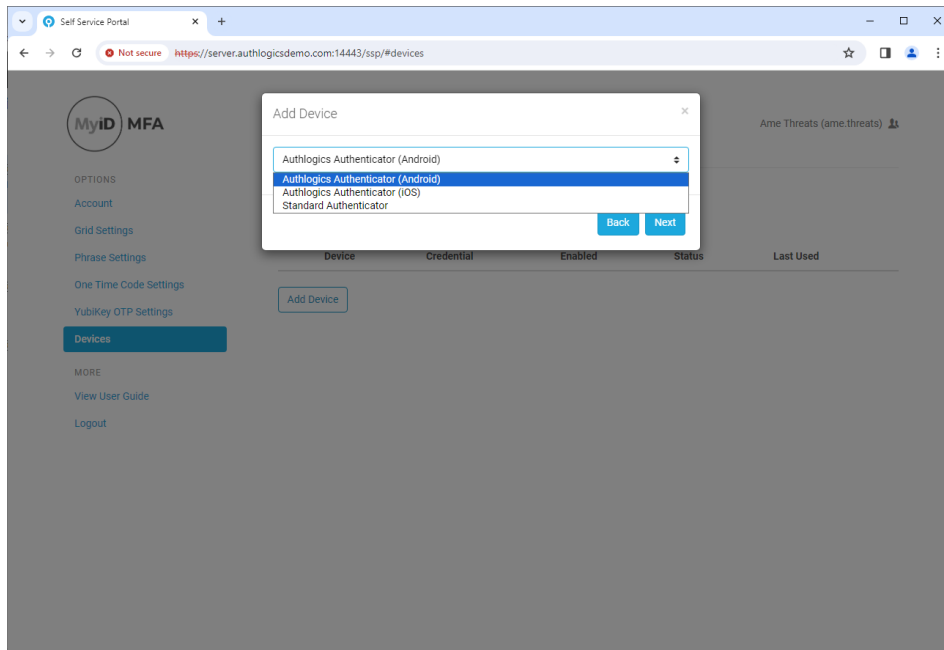
Install the Authlogics Authenticator App from the relevant App Store using the buttons on your device.



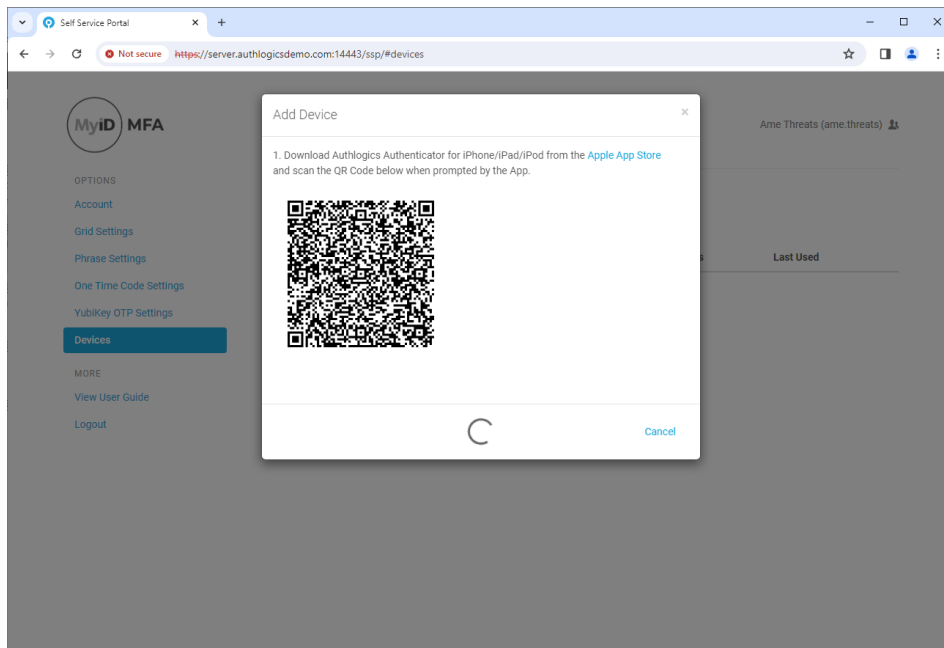
Click *Add Device*



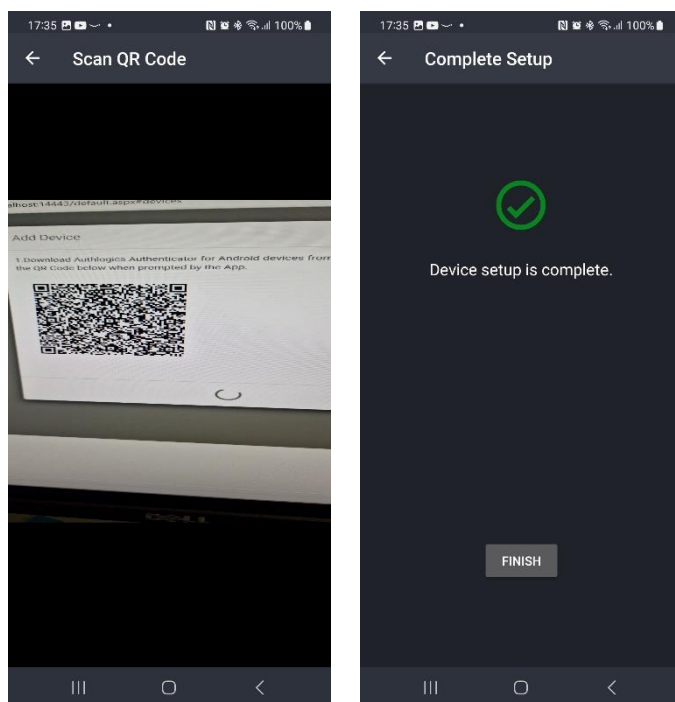
Select *Authenticator App*



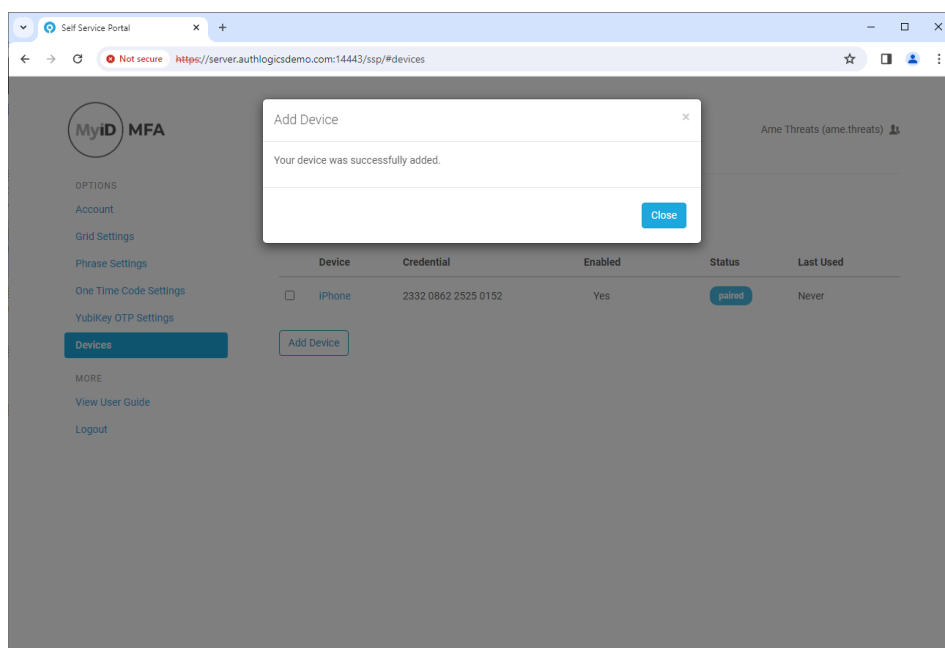
Authlogics Authenticator Android and iOS relate to the Authlogics MFA app; Standard Authenticator refers to 3rd-party OATH tokens. Choose the type of device you have and click **Next**.



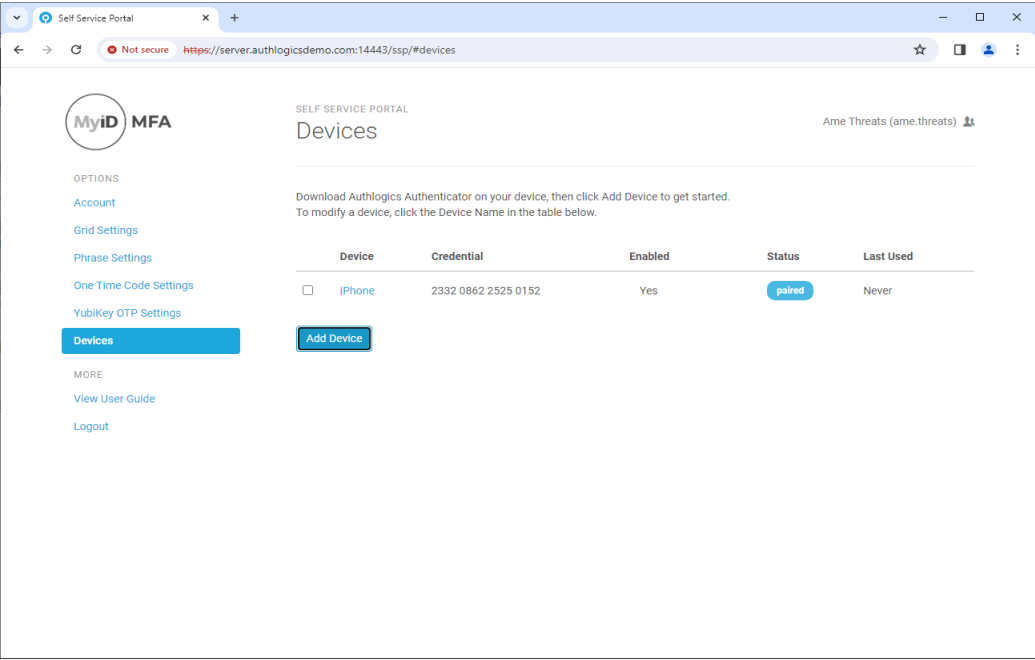
Scan the QR code with the Authlogics Authenticator App.



Tap Finish.



Click Close.



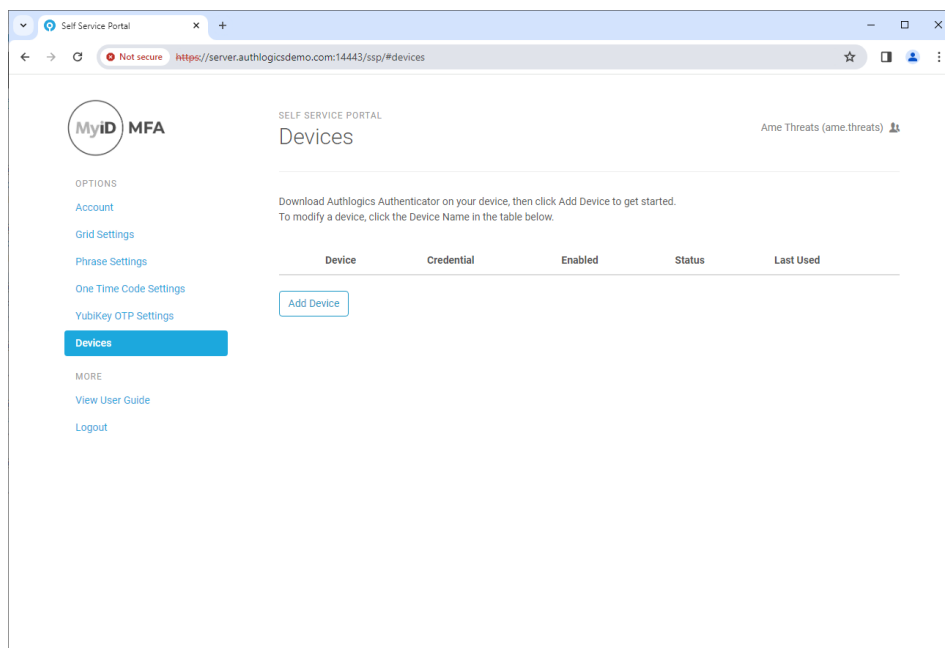
The new device will be visible under devices. Your device is now ready for use a multi-factor authentication token for your MyID account.

YubiKey OTP

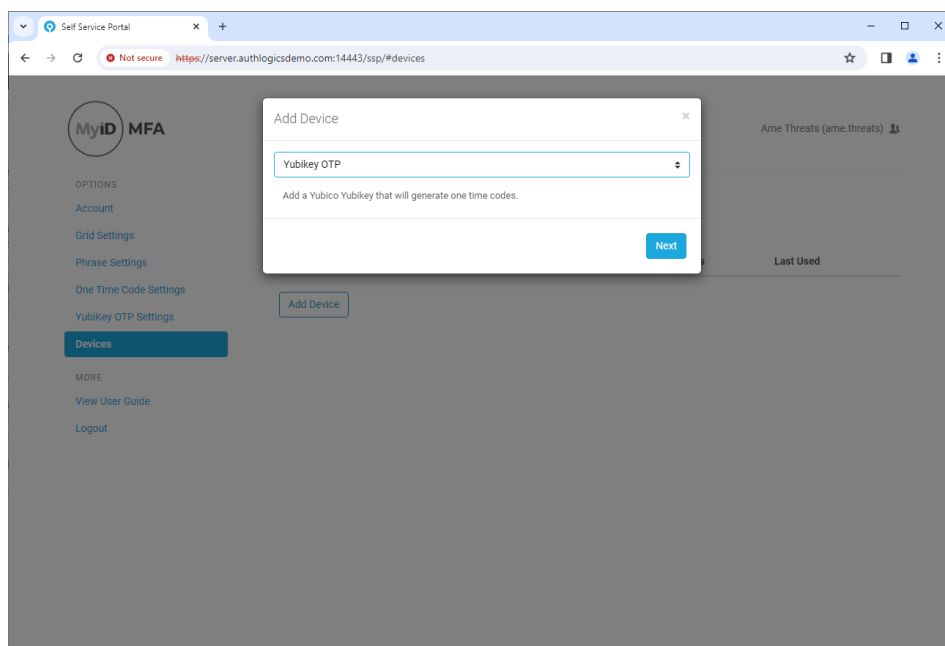
To provision your YubiKey OTP hardware device, insert the YubiKey token into your system.

Adding your device to your account

To add a device to your account logon to the Self Service Portal and select **Devices** from the menu.



Click **Add Device**

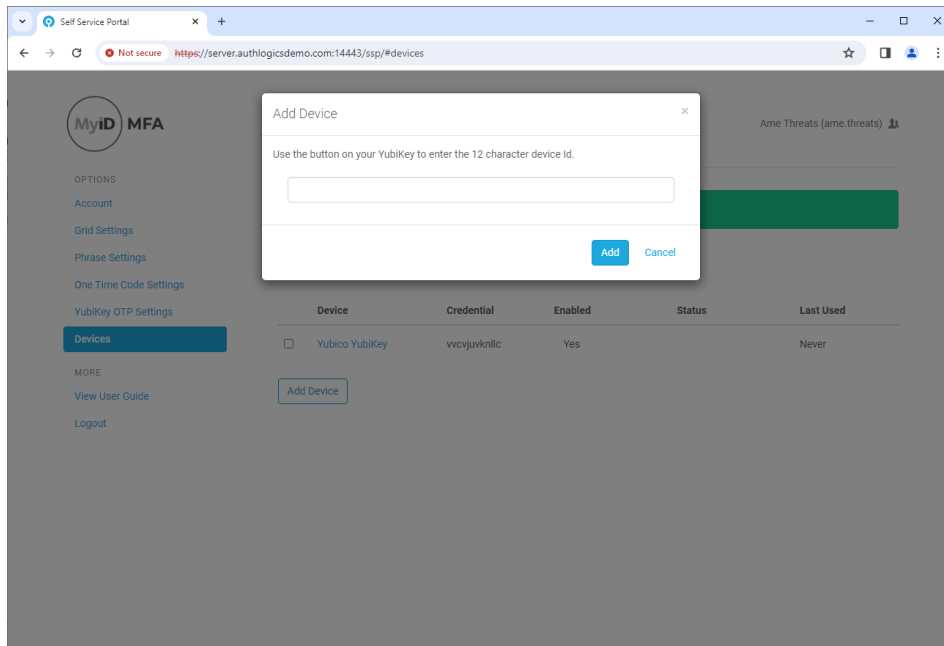


Note

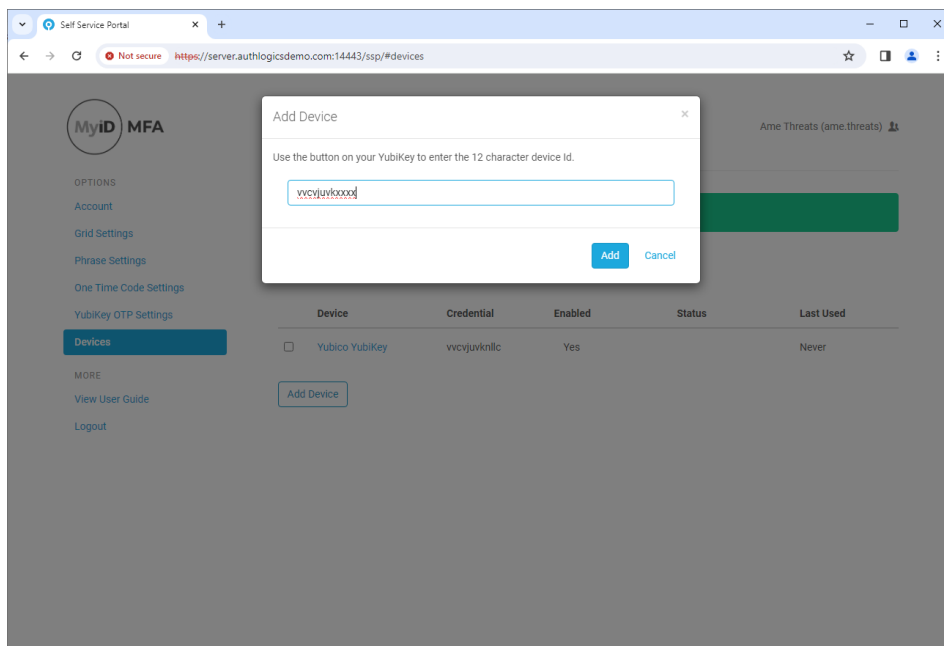
If this option is not available, then your user account has not been set up to use YubiKey tokens. Please contact your administrator for assistance.

www.intercede.com | info@intercede.com | +44(0)1455 558 111 | +1 888 646 6943

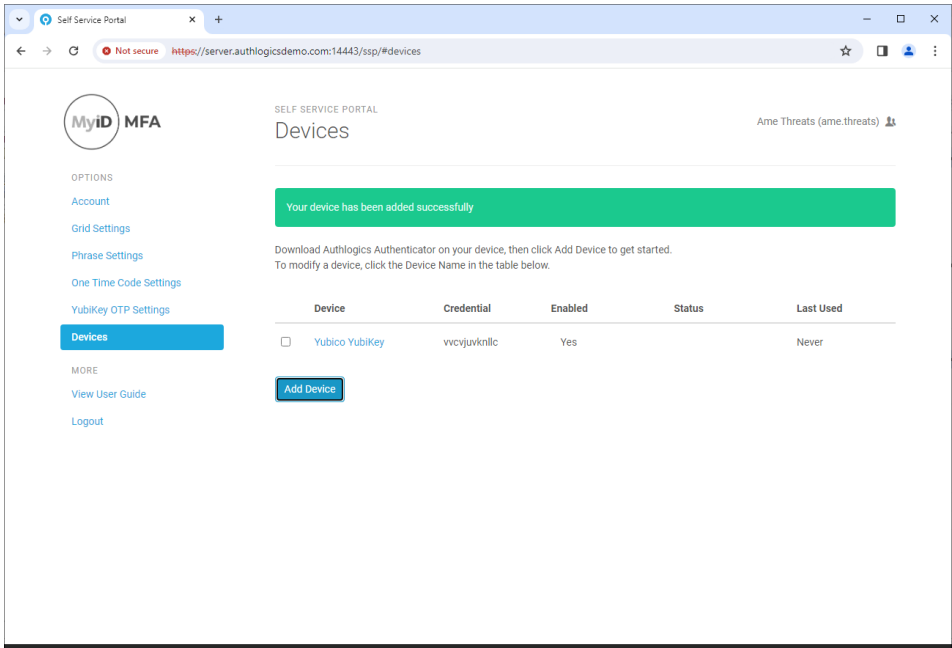
Select **YubiKey OTP**. Click **Next**



Insert your YubiKey OTP and press the YubiKey button.



Once the unique YubiKey ID is displayed in the edit box. Click **Add**

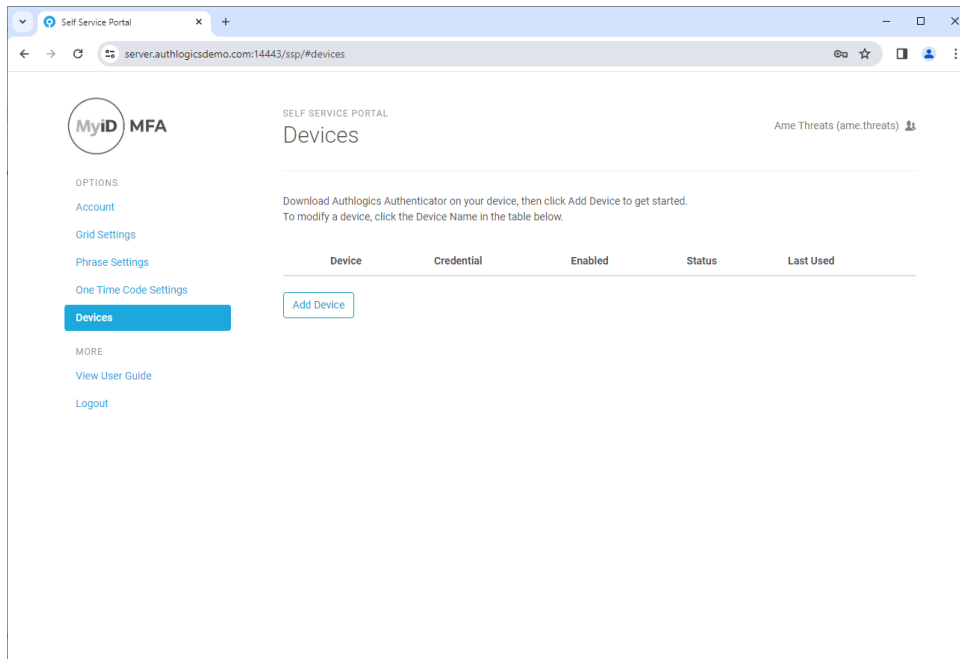


Passkey / FIDO Token

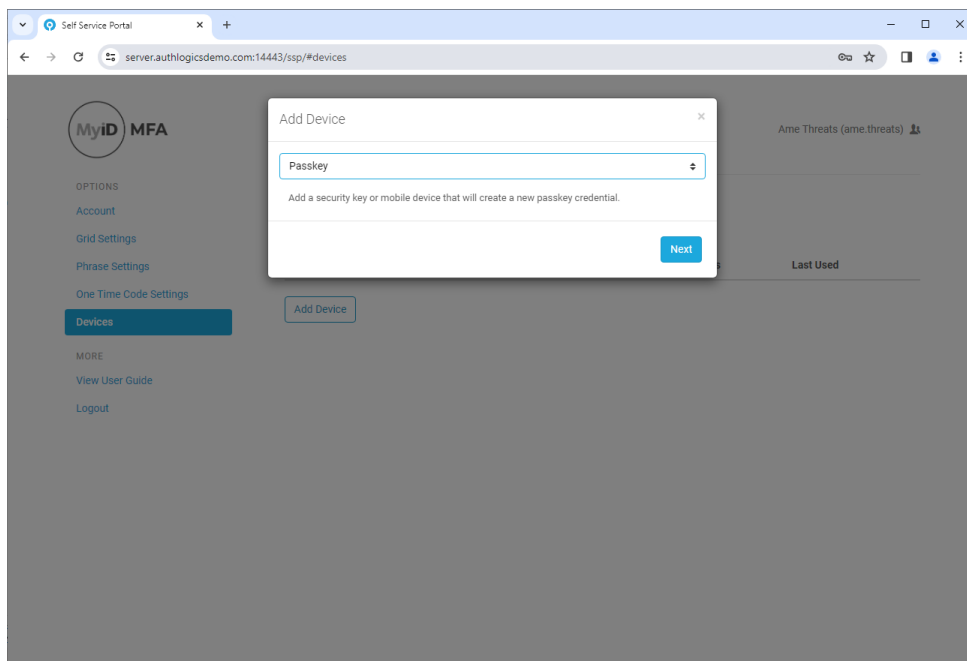
Before adding your FIDO Security Key or a Passkey to your account, ensure that no other MFA devices are attached to the workstation and that all Passkey / FIDO tokens have been removed from the system.

Adding your FIDO / Security Key to your account

To add a FIDO Passkey Security Key to your account, logon to the Self Service Portal and select **Devices** from the menu.



Click **Add Device**



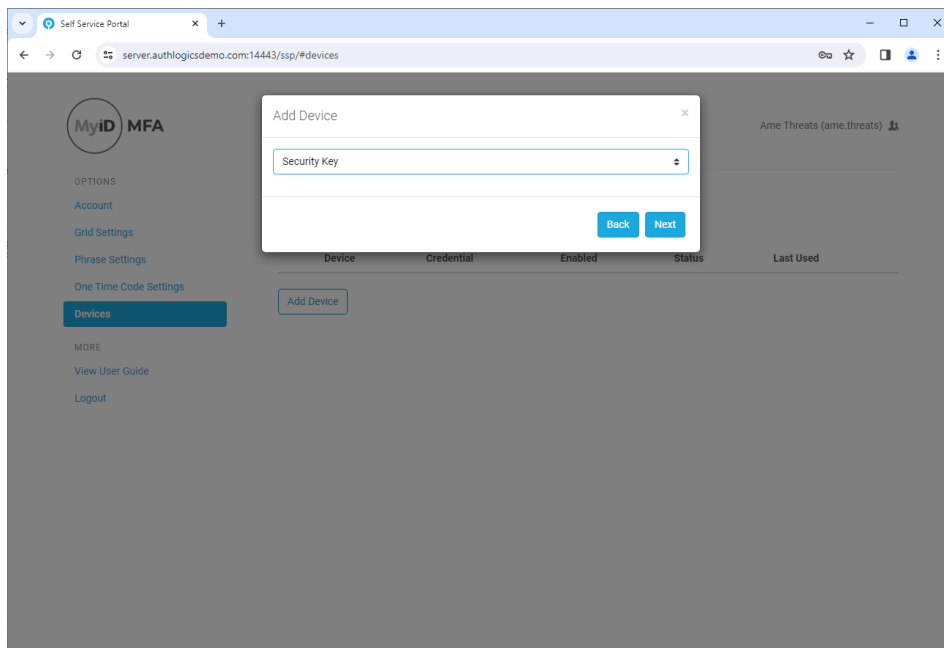


Note

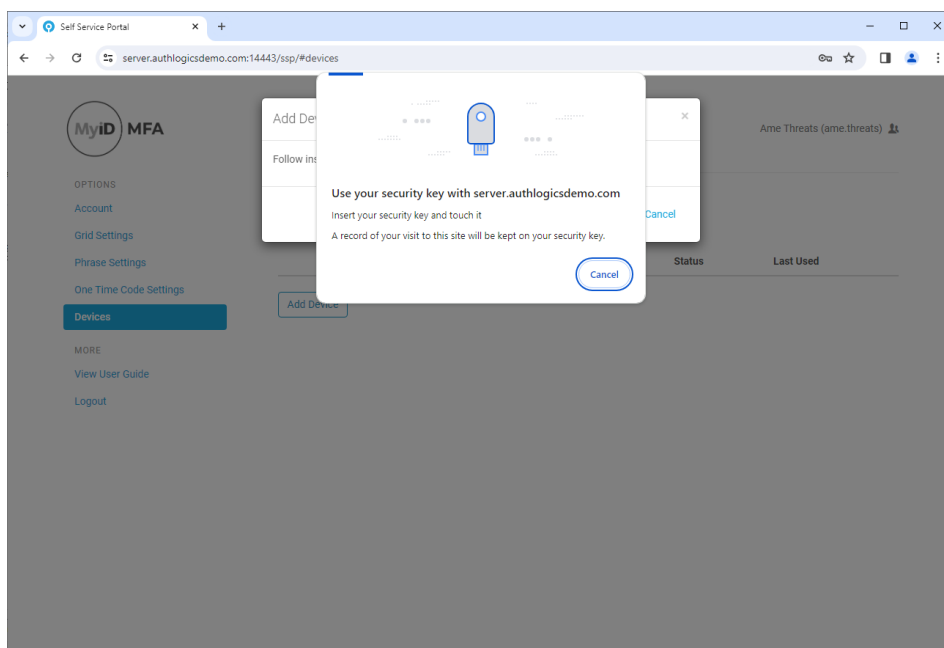
If this option is not available, then your user account has not been set up to use Passkeys. Please contact your administrator for assistance.

A maximum of 2 device-bound passkeys can be provisioned to one account. If you have more than 2 device-bound passkeys already enabled, the option to add more will not be available.

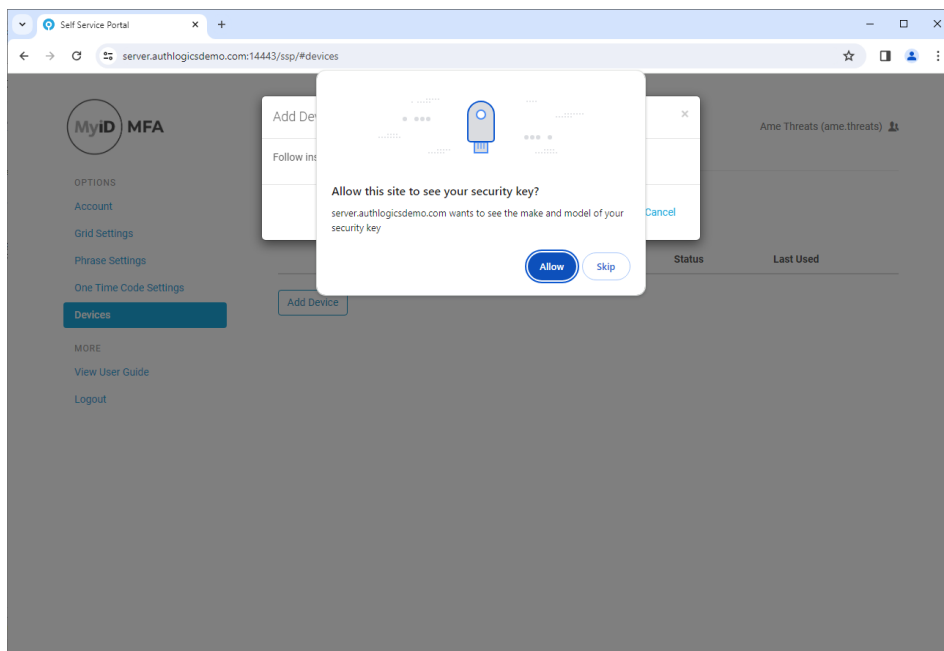
Select **Passkey** Click **Next**



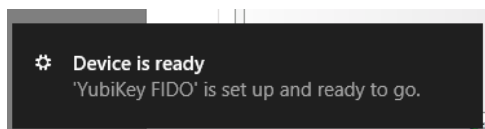
Select **Security Key**. Click **Next**.



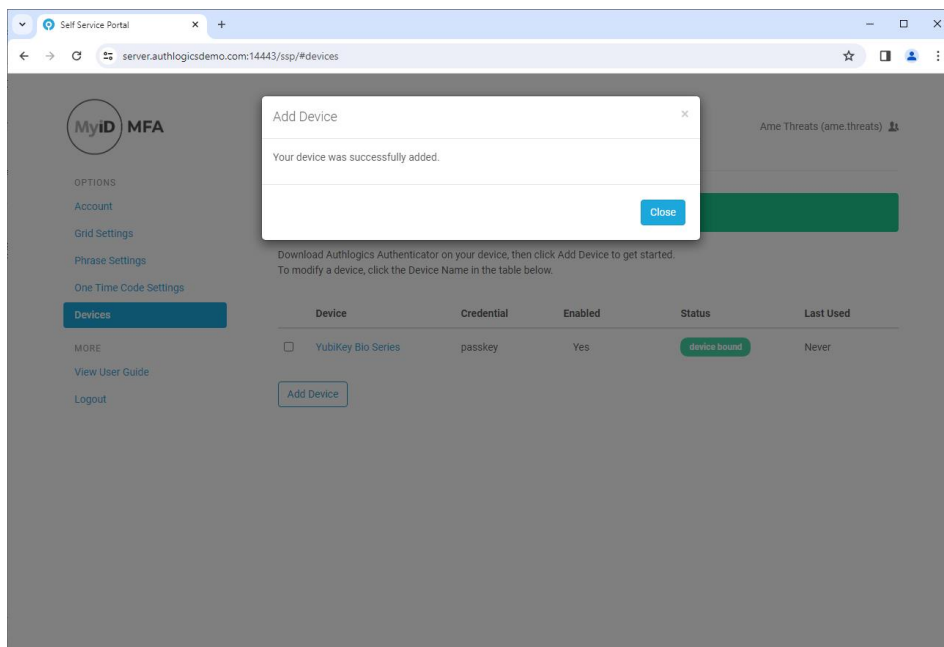
Insert your Security key and press the FIDO token's button.



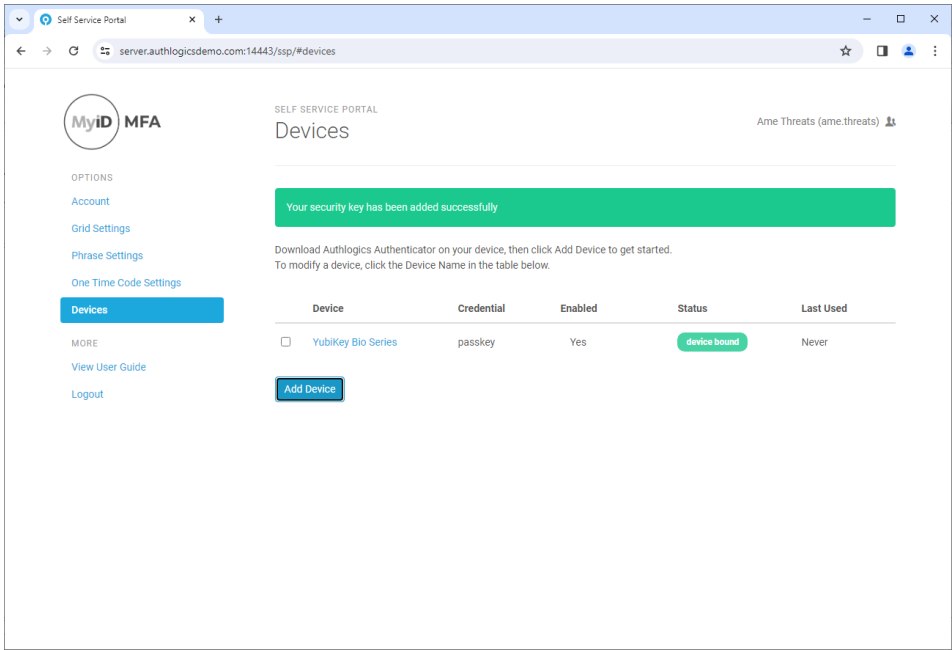
When prompted, Click **Allow**.



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

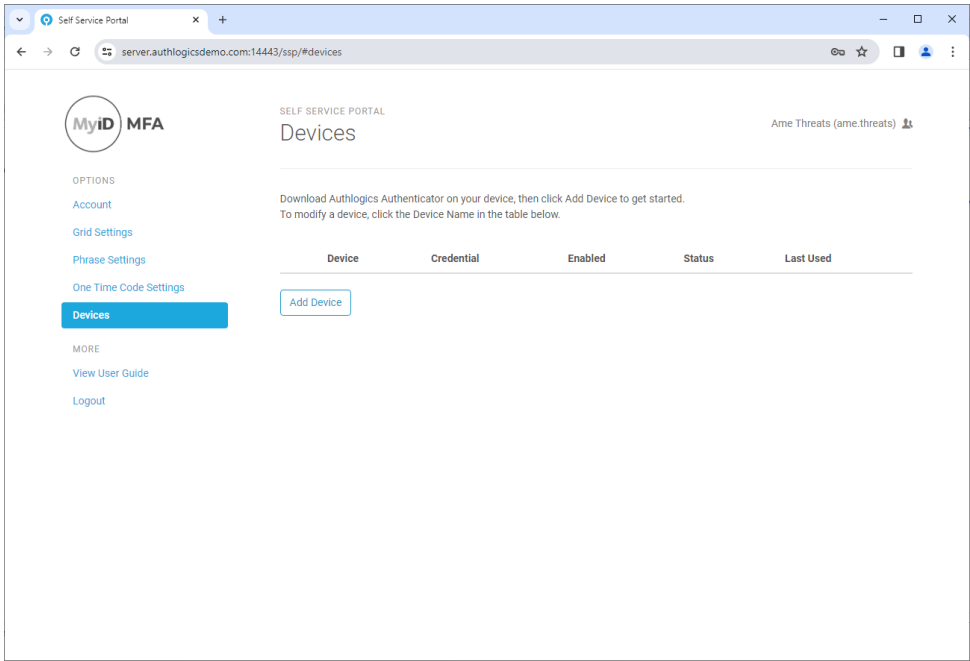


The device has been successfully added. Click **Close**.

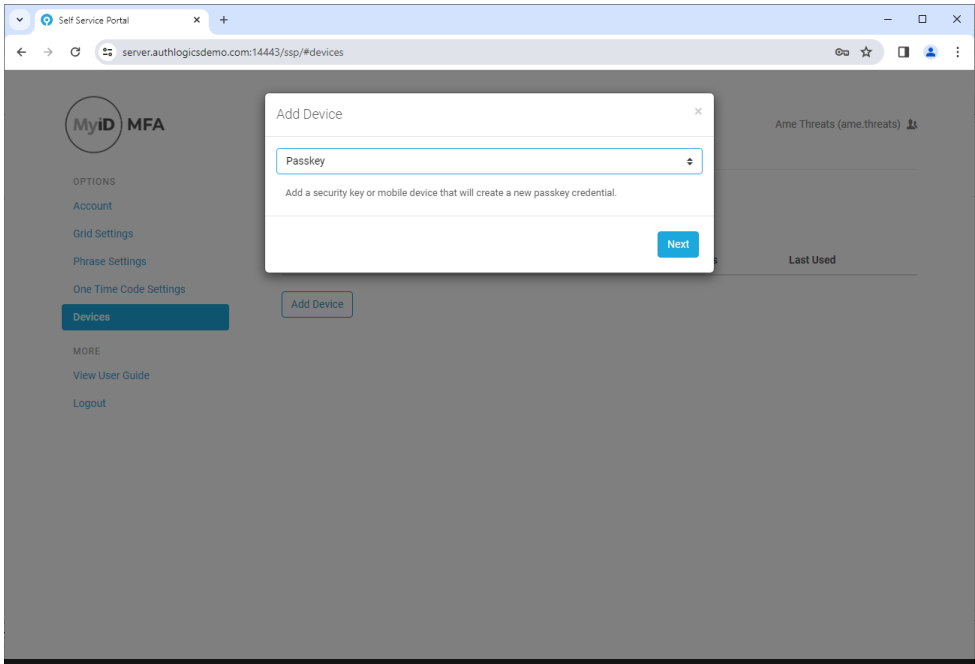


Adding a Synced Passkey to your account

To add a FIDO Passkey Security Key to your account, logon to the Self Service Portal and select *Devices* from the menu.



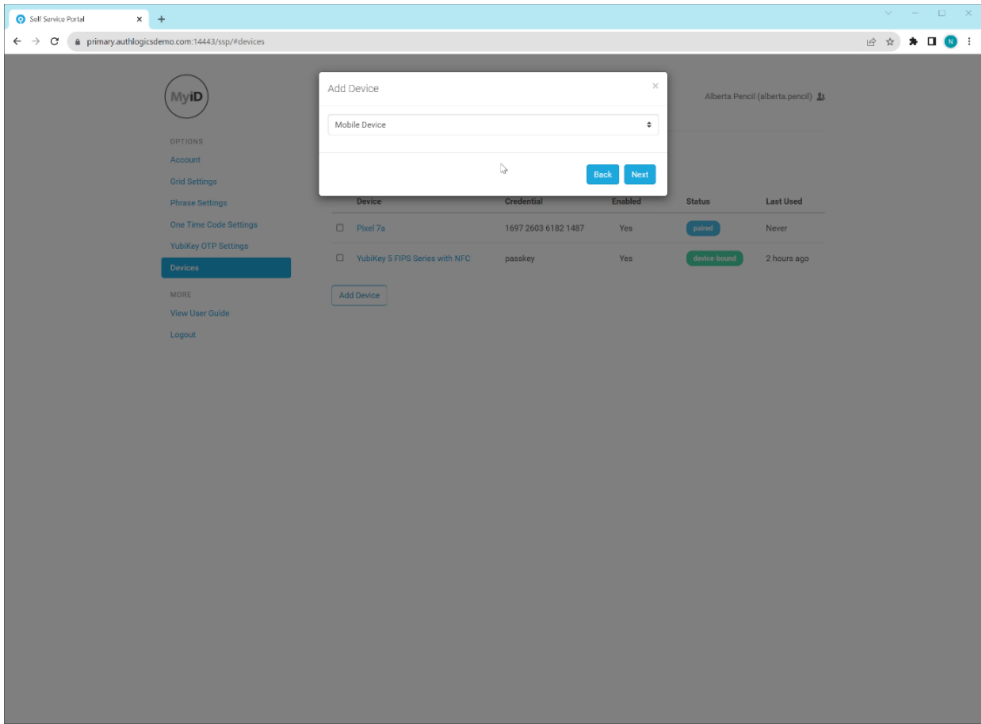
Click *Add Device*



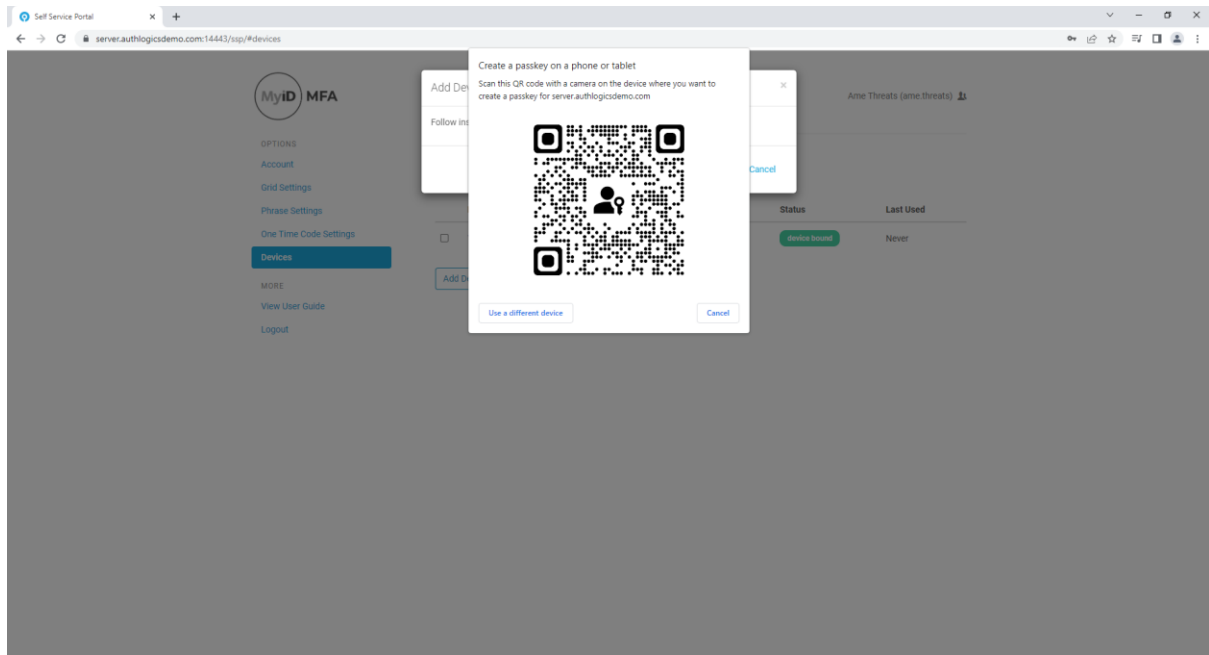
Note

If this option is not available, then your user account has not been set up to use Passkeys. Please contact your administrator for assistance.

Select *Passkey* Click *Next*

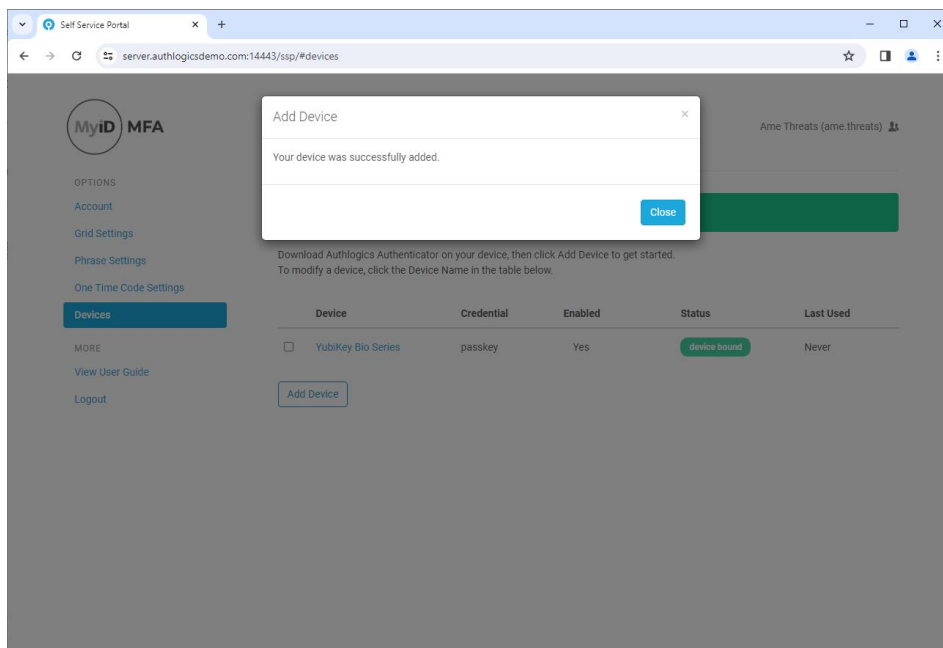


Select *Mobile Device*. Click *Next*.



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 will not be displayed. Open you Mobile phone's camera and scan the QR Code. Once you have scanned the QR Code, follow the instructions on your mobile phone.

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



The device has been successfully added. Click **Close**.

