

MyID MFA and PSM Version 5.2

Self Service Portal User Guide

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



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 password	9
3.3 Unlocking your account	10
4 Changing your multi-factor authentication settings	11
4.1 Changing your Grid pattern	12
4.2 Settings your Phrase answers	14
4.3 Changing your One Time Code settings	15
4.4 Changing your YubiKey OTP settings	16
5 Setting up your own device	17
5.1 MyID Authenticator app	18
5.1.1 Legacy Authlogics Authenticator app	18
5.1.2 Alternative Authenticator apps	18
5.1.3 Adding your MyID Authenticator device to your account	19
5.2 Other authenticator apps	23
5.2.1 Adding your standard authenticator device to your account	23
5.3 YubiKey OTP	26
5.3.1 Adding your YubiKey device to your account	26
5.4 Passkey / FIDO Token	29
5.4.1 Adding your FIDO / Security Key device to your account	29
5.4.2 Adding a Synched Passkey to your account	34
5.5 Editing devices	38
5.6 Removing devices	40



1 Introduction

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

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

You can:

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

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

1.1 Language requirements

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

- English
- German

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

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

Product support and documentation are available only in English.



2 Accessing the Self Service Portal

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



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



2.1 Your first logon

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

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

	J	О м	lyID Au) Authentication Server IdP × +	-	-		×
÷	-	\rightarrow	G	Not secure https://server.authlogicsdemo.com:14443/idp/Account/Login?returnUrl=%2Fidp%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3Dinternal.s	\$		4	:
				SELF SERVICE PORTAL				
				Login				
				2 1 0 5 0 3				
				5 2 4 4 2 4				
				4 0 0 2 1 5				
				1 0 5 2 1 4				
				2 0 3 1 1 3				
				5 3 3 4 5				
				One Time Code				
				One Time Code				
				Sign In				
				View user guide				

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.

Self Service Portal X +		- 🗆 ×
← → C ONot secure https://server.authlo	gicsdemo.com:14443/ssp/	☆ 🛛 😩 :
(MyiD) MFA	self service portal Account	Ame Threats (ame threats) 🤱
OPTIONS Account Grid Settings Devices	Enter the number used to deliver text / SMS messages to your phone. Use international dialing code format, e.g. "+44 700 123 4567". Mobile / Cellular Number	
MORE View User Guide	Number	
Logout	To change your Windows password, enter your new Windows password in each box be	low.
	Password Confirm	
	New password Confirm password	
	Change	
	To unlock your Windows account, click the 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.

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

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



3.2 Resetting your password

To reset your network password:

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

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

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

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

X Not previously compromised	our new Windows password in each box below.
Ρά	Confirm
•••••	•••••
Reset	

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

T ✓ Not previously compromised	our new Windows password in each box below.
Ρε	Confirm
•••••	••••••
Reset	

3. Click Reset to save the new password.

If successful, the following message appears:

Your Password was updated successfull

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.



3.3 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:

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.

Self Service Portal	x +	-	×
← → C 😋 primary.a	uthlogicsdemo.com:14443/ssp/#pingrid	☆	÷
MyiD	self service portal (administrator) &		
OPTIONS Account	To set a new pattern, click the squares matching your pattern in the first box below, and again in the second.		
Grid Settings Phrase Settings			
One Time Code Settings			
YubiKey OTP Settings Devices			
MORE			
View User Guide Logout	Save Show/Hide Pattern Clear		

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.

Self Service Portal X +		- 🗆 X
← → C ONot secure https://server.authlog	gicsdemo.com:14443/ssp/#pinphrase	☆ 🛛 😩 :
MyiD MFA	self service portal Phrase Settings	Ame Threats (ame.threats) 🄱
OPTIONS Account	Question / Answer	
Grid Settings	What is your Codeword?	gladify
Phrase Settings	What is your mother maiden?	
Devices	What is your favourite sports teams?	
MORE	What is your favourite subject at school?	
View User Guide	What is your spouses middle name?	
Logox	Edit	

- 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.

Self Service Portal X +		- 🗆 X
← → C ONot secure https://serv	er.authlogicsdemo.com:14443/ssp/#pinpass	☆ 🔲 😩 🗄
MyiD MFA	SELF SERVICE PORTAL One Time Code Settings	Ame Threats (ame.threats) 北
OPTIONS Account	Enter your new PIN in each box below and click the Save button.	
Grid Settings	PIN	
Phrase Settings	PIN	
One Time Code Settings	Confirm	
Devices	Confirm PIN	
MORE	Save	
View User Guide		
Logout		

- 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.

Self Service Portal X +		- 🗆 X
← → C ONot secure https://server.authl	ogicsdemo.com:14443/ssp/#yubikeyotp	☆ 🛛 😩 :
MyiD MFA	self service portal YubiKey OTP Settings	Ame Threats (ame.threats) 🤱
OPTIONS Account	Enter your new PIN in each box below and click the Save but	on.
Grid Settings	PIN	
Phrase Settings	PIN	
One Time Code Settings	Confirm	
YubiKey OTP Settings	Confirm PIN	
Devices	Save	
MORE		
View User Guide		
Logout		

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

If successful, the following message appears:

Your PIN was updated successfully.



5 Setting up your own device

MyID MFA supports several authentication technologies. These technologies include:

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

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

- Information on obtaining and using the MyID Authenticator app. See section *5.1*, *MyID Authenticator app*.
- Information on using alternative authenticator apps. See section *5.2*, *Other authenticator apps*.
- Information on using YubiKey devices.
 See section 5.3, YubiKey OTP.
- Information on using Passkey / FIDO tokens.
 See section 5.4, Passkey / FIDO Token.
- Instructions for editing devices. See section 5.5, *Editing devices*.
- Instructions for removing devices.
 See section 5.6, Removing devices.



5.1 MyID Authenticator app

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



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

5.1.1 Legacy Authlogics Authenticator app

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



5.1.2 Alternative Authenticator apps

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



5.1.3 Adding your MyID Authenticator device to your account

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

To add a device to your account:

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

MyiD	self service portal Devices				Dacie Guerard (dacie.guerard) 🤱	L
OPTIONS						
Account	Download the MyID Auth To modify a device, click	enticator on your device, the	en click Add Device to get s e below	tarted.		
Devices						
MORE	Device	Credential	Enabled	Status	Last Used	
View User Guide						
Logout	Add Device					

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

Authenticator App		\$
Add a device running the My Authenticator / Microsoft Au	vID Authenticator app, or a stand uthenticator.	dard authenticator such as Google
		_

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





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

MyID Authenticator (Android)	\$
MyID Authenticator (Android)	
MyID Authenticator (iOS)	
Standard Authenticator	

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.

Add Device	×	
1. Download the MyID Authenticator for Android Devices from Google Play and scan the QR Code below when prompted by the App.		
Cance	l	





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



Device setup is complete.



9.



8. Click **Finish**.

Add D	evice			×		Ame Threats (ame.threats) 💄
Your de	vice was success	fully added.				
				Close		
	Device	Credential	Enabled		Status	Last Used
	iPhone	2332 0862 2525 0152	Yes		paired	Never
Add	Device					
Click Cl	ose.					
MyiD		self service portal Devices				Dacie Guerard (dacie.guerard) 🏦
OPTIONS Account Devices		Download the MyID Auther To modify a device, click th	nticator on your device, then click he Device Name in the table belov	Add Device to get sta 	irted.	
MORE		Device	Credential	Enabled	Status	Last Used
View User (Guide	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.

MyiD	self service portal Devices	Dacie Guerard (dacie.guerard) 🄱			
OPTIONS Account	Download the MyID Autho	enticator on your device, the the Device Name in the tabl	n click Add Device to get s e below.	tarted.	
Devices	,,				
MORE	Device	Credential	Enabled	Status	Last Used
View User Guide	Add Device				
Logout	Add Device				

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

Add Device	×
Authenticator App	\$
Add a device running the MyID Authenticator app, or a standard authenticator so Authenticator / Microsoft Authenticator.	uch as Google
	Next

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





5. From the list, choose Standard Authenticator.



6. Click Next.

Open Microsoft/G and scan the QR o your device.	Google Authenticator (or oth code or manually enter the P	ier standard Authenticator key below. Then press Add	app) on your device to finish registering
	89		
			HWA C:

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	SELF SERVICE PORTAL				(Administrator) 🛓		
OPTIONS							
Account	Your device has been added succ						
Grid Settings							
Phrase Settings	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.						
One Time Code Settings							
YubiKey OTP Settings	Device	Credential	Enabled	Status	Last Used		
Devices	Standard Authenticator	1531 6525 5196 1349	Yes		Never		
MORE							
View User Guide	Add Device						
Logout							

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.

✓ O Self Service Portal × + - □ ×							
← → C ② Not secure https://serve	er.authlogicsdemo.com:14443/ssp/#o	devices			☆ 🛛 😩 :		
MyiD MFA	self service portal Devices				Ame Threats (ame.threats) 🤱		
OPTIONS Account Grid Settings	OPTIONS Account 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. Grid Settings						
Phrase Settings	Device	Credential	Enabled	Status	Last Used		
One Time Code Settings YubiKey OTP Settings	Add Device						
Devices							
MORE							
View User Guide							
Logout							





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.

Self Service Portal X +					- 0
← → C ONot secure https://server.a	uthlogicsdemo.com:14443/ssp/#device	es			🖈 🔲 😩
(MyiD) MFA	Add Device			×	Ame Threats (ame.threats) 🛓
OPTIONS	Use the button on your YubiKey	to enter the 12 characte	r device Id.		_
Grid Settings Phrase Settings			Add	Cancel	
	Device	Credential	Enabled	Status	Last Used
Devices	Yubico YubiKey	vycyjuvknilc	Yes		Never
MDRE View User Gulde Logout	Add Device				





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

Self Service Portal X +					- 🗆 X
← → C ONot secure https://server	authlogicsdemo.com:14443/ssp/#device	25			☆ 🛛 😩 :
MyiD MFA	Add Device Use the button on your YubiKey	to enter the 12 character	device Id.	×	Ame Threats (ame.threats) 🤱
Account Grid Settings Phrase Settings One Time Code Settings	vezyluvkoood	_	Add	Cancel	
YubiKey OTP Settings	Device	Credential	Enabled	Status	Last Used
Devices MORE View User Guide Logout	Yubico Yubikey Add Device	vvcvjuvknilc	Yes		Never

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

Self Service Portal X +					- 0
← → C O Not secure https://serve	r.authlogicsdemo.com:14443/ssp/#devic	ces			* 🛯 🔺
(MyID) MFA	SELF SERVICE PORTAL				Ame Threats (ame.threats) 🤱
OPTIONS Account Your device has been added successfully Grid Settings Phrase Settings 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.					
One Time Code Settings	Device	Credential	Enabled	Statue	Last llead
Devices	Yubico YubiKey	vycyjuyknilc	Yes		Never
MORE View User Guide Logout	Add Device				

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.

 ✓ O Self Service Portal × + 					- 🗆 X
← → C 😨 server.authlogicsdemo.com:	14443/ssp/#devices				∞ ☆ 🛛 😩 i
(MyiD) MFA	self service portal				Ame Threats (ame.threats) 🎎
OPTIONS Account Grid Settings	then click Add Device to below.) get started.			
Phrase Settings	Device	Credential	Enabled	Status	Last Used
One Time Code Settings	Add Device				
Devices	Add berice				
MORE					
View User Guide					
Logout					





2. Click Add Device.

O Self Service Portal X +	- 🗆 X
← → C ts serverauthlogicsdemo.com:14443/ssp/#devices	∞ ☆ 🛛 💄 :
Add Device × Passkey	Ame Threats (ame.threats) 🛓
Account Crid Settings Phrase Settings One Time Code Settings Add Device Add Device	s Last Used
MORE View User Guide Logout	

3. Select Passkey and click Next.

Self Service Portal X +		- 🗆 X
← → C 🖙 server.authlogicsdemo.com	n:14443/ssp/#devices	∞ ☆ 🛯 💄 i
MyiD MFA	Add Device × Security Key	Ame Threats (ame.threats) 🛓
Account Grid Settings Phrase Settings	Back Next Device Credential Enabled Status	Last Used
One Time Code Settings Devices	Add Device	
View User Guide		

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.

	Add Device	_	_	×	Ame Threats (ame threats)
	Your device was successfully add	ed.			
Account				Close	
Grid Settings					
Phrase Settings	Download Authlogics Authentica To modify a device, click the Devi	tor on your device, then ce Name in the table be	click Add Device to get low.	started.	
One Time Code Settings					
Devices	Device	Credential	Enabled	Status	Last Used
MORE	YubiKey Bio Series	passkey	Yes	device bound	Never
View User Guide					
Logout	Add Device				

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.

Self Service Portal X +					- 🗆 ×
← → C 25 server.authlogicsdemo.com:144	143/ssp/#devices				∞ ☆ 🛛 💄 i
(MyiD) MFA	self service portal Devices				Ame Threats (ame.threats) 🤱
OPTIONS Account Grid Settings	Download the MyID Aut To modify a device, click	henticator on your device, the Device Name in the table	then click Add Device to below.	get started.	
Phrase Settings	Device	Credential	Enabled	Status	Last Used
One Time Code Settings	Add Davies				
Devices	Add Device				
MORE					
View User Guide					
Logout					





2. Click Add Device.

Self Service Portal X +		- 🗆 X
← → C 🖙 server.authlogicsdemo.com:1	4443/ssp/#devices	ca 🖈 🔲 😩 🗄
MyiD MFA	Add Device ×	Ame Threats (ame threats) 🤽
OPTIONS Account Grid Settings	Add a security key or mobile device that will create a new passkey credential.	
Phrase Settings	Next	Last Used
One Time Code Settings Devices	Add Device	
MORE		
View User Guide Logout		

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.

Sell Service Portal	× +						
← → C 🖬 primary.aut	hlogicsdemo.com:14443/ssp/#devices						🖻 🖈 🖬 📵
	MyiD	Add Device Mobile Device		×	Alberta Pen	sil (alberta.pencil) 🏦	
	Account Grid Settings			Back Next			
	Phrase Settings One Time Code Settings	Device	1697 2603 6182 1487	Ves	Status	Never	
	YubiKey OTP Settings		passkey	Yes	device-bound	2 hours and	
	Devices						
	MORE View User Guide	Add Device					
	Logout						





4. Select Mobile Device and click Next.

Self Service Portal x +		v - 0 X
← → C a server.authlogicsdemo.com:14443/ssp/#devices		• 순 ☆ 팩 🖬 😩 :
 Canada Manda Xana Anala An	All oral Case a paskay on a phone or table All oral The the chast what scares on the denice submatching Toru Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table Image: Case a phone or table	 ✓ - Ø X ♥ Ø X № I ▲ I

- 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.

Self Service Portal X +					- 🗆 X
← → C 😄 server.authlogicsdemo.com:	14443/ssp/#devices				☆ 🛛 😩 :
\frown	Add Device			×	
MyiD MFA	Your device was successfully adde	d.		Ar	ne Threats (ame.threats) 🤱
OPTIONS Account				Close	
Grid Settings	Download Authlogics Authenticat	or on your device, then (click Add Device to get	started.	
One Time Code Settings	To modify a device, click the Devic	ce Name in the table be	low.		
Devices	Device	Credential	Enabled	Status	Last Used
MORE	YubiKey Bio Series	passkey	Yes	device bound	Never
View User Guide Logout	Add Device				

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		
	Z Fold4	1031 1117 5242 0923	No	Paired	2 days ago		
	Yubico YubiKey	cccccbhlrtbg	Yes		3 seconds ago		
	YubiKey Bio Series	passkey	No	device-bound	Never		
Edi	Edit Device Remove Debug						

3. Click Edit Device.

Edit Device		×
Device Name		
YubiKey Bio Series		
The Device Name can have a maximum length of 50 characters.		
Enabled		
No		Ƴ atus
		Paired
	Cancel	ave
YubiKey Bio Series passkey	No	device-bound
Edit Device Remove Debug		



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	De	self service portal Devices					
OPTIONS Account	Dow To n	nload the MyID Authenticator on y nodify a device, click the Device N	your device, then click Add Devic ame in the table below.	e to get started.			
Grid Settings Phrase Settings		Device	Credential	Enabled	Status	Last Used	
One Time Code Settings		Yubico YubiKey	cccbccuejlck	Yes		Never	
YubiKey OTP Settings Devices		Standard Authenticator	1542 4267 3515 9154	Yes		Never	
MORE		Standard Authenticator	2478 3158 1531 0322	Yes		Never	
View User Guide		Security Key	passkey	Yes	device-bound	Never	
Logout	Ec	lit Device Remove					

3. Click Remove.

MyiD	Remove Device		×] ,	Kayla Bue (kayla.bue) 💄
\bigcirc	Are you sure you want to remove the	device "Standard Authenticator"	?		
OPTIONS Account			Yes No		
Grid Settings					
Phrase Settings	Device	Credential	Enabled	Status	Last Used
One Time Code Settings	Yubico YubiKey	cccbccuejlck	Yes		Never
YubiKey OTP Settings Devices	Standard Authenticator	1542 4267 3515 9154	Yes		Never
MORE	Standard Authenticator	2478 3158 1531 0322	Yes		Never
View User Guide	Security Key	passkey	Yes	device-bound	Never
Logout	Edit Device Remove				



4. Click Yes.

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

MyiD	self service f	self service portal Devices						
OPTIONS								
Account	The token de							
Grid Settings								
Phrase Settings	Download the M To modify a dev	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.						
One Time Code Settings								
YubiKey OTP Settings	Device		Credential	Enabled	Status	Last Used		
Devices	Yubico Y	'ubiKey	cccbccuejlck	Yes		Never		
MORE	Standar	d Authenticator	2478 3158 1531 0322	Yes		Never		
View User Guide		W.						
Logout	Security	Key	passkey	Yes	device-bound	Never		
	Add Device							