

Table of Contents – How to Use Portalguard

Overview	2
What’s Covered in this User Guide?	2
Password Basics	2
How do I change my password with Portalguard?	3
I’ve Forgotten My Password. How Do I Recover My Password Instead of Resetting It?.....	4
My Password Has Expired. How Do I Reset My Password?	7
What are Challenge Questions and Why Should I Use Them?	9
How do I reset my Challenge Questions?	10
What are One-Time Passcodes?	11
How Do I Change My Alternate Email Address?	11
How Do I Add or Delete a Mobile Phone?	12
What is the Google Authenticator?	13
How Do I setup the Google Authenticator?.....	14
Printing out OTPs for Future Use	15
I get “Authentication Failed” when I try to login to Portalguard. What can I do?	17
How to Get Additional Help	17
Feedback	17
Document History	17

Portalguard User Guide

Overview

The Portalguard password management system allows you to easily manage your UAFS campus password that you use to log into Windows, Blackboard, email, and other campus systems. Portalguard replaces the home-grown LionsPass password system. It is a commercially supported system that has many more features and much more functionality than LionsPass. Using the Portalguard password management system will make your life better by reducing the time and effort needed to maintain your campus password. Features include:

- Ability to reset your password either before or after it has expired without the aid of Technology Services staff. This allows resetting your password even when there are no Technology Service Desk staff on duty, such as when the campus is closed.
- For fully online distance learners, support for managing your password without ever having to visit the campus.
- Ability for anyone to reset their password from virtually anywhere in the world using their computer, tablet or smartphone.
- Ability to view your current password without having to reset it.
- Automated alert emails when a password has been changed, to help thwart imposters.
- Ability to quickly and easily reset your expired password from any campus PC—no Windows login or password kiosk station required.
- Ability for Technology Service Desk staff to provide password reset assistance without the user having to reveal sensitive information.

What's Covered in this User Guide?

This document shows campus technology users how to take advantage of the most important features that Portalguard offers. Those features include registration, password reset, password recovery, and unlocking accounts. It also discusses good password practices, using one-time passcodes, using the Google Authenticator, and other related information.

Password Basics

In order to ensure that every network user (student or employee) has full access to the technology resources they need while at the same time preventing inappropriate access, the UAFS campus network employs the combination of a user name (also referred to as a user ID or network ID) and a password. Combined they form the security credentials needed to authenticate you to the network. For example, when logging into campus computers or Blackboard, you must enter both a userID and password.

Your security credentials are only as strong as the weakest link, so it's vital to provide as much strength as possible in each link, from the length of the password to how often it must be changed. To help keep your credentials strong and prevent imposters and others from gaining unauthorized access, certain guidelines must be followed. These guidelines include:

- **Never, ever sharing your password with anyone, even UAFS Technology Services staff.** You should never give your password to anyone, ever. You are the only person who should know your password. If you have trouble remembering your password, keep a copy of it in a location that only you have access to. Do not leave your

password anywhere where it will be visible to other people. If you give your password to anyone, you will be held responsible for any damage that they might do with it.

- **Keeping passwords reasonably complex so that they are not easily guessed.** UAFS passwords must be at least 10 characters long. They must contain a mix of upper case, lower case, numbers, and select special characters. Do not use your userID as part of your password.
- **Changing your password frequently.** Arkansas state law requires that UAFS network users change their passwords at least every 90 days.
- **No reusing old passwords.** You must use a new password—one you’ve not used in the past—when changing your password. The new password must differ from the last password by at least 3 characters.

How do I change my password with Portalguard?

Use this method if you need to change your password before it expires.

1. Login into to Portalguard:
<https://portalguard.uafs.edu>



2. Click on the “Change now” link



3. Provide your current password, and click “Continue”



4. Type in your new password, confirm your new password, and click on “Set Password”

Set Password
Please provide your new password, confirm it then click the 'Set Password' button

Username

New Password
 Show password

Confirm New Password

5. You should see “Password Successfully Set”

Set Password

Password Successfully Set

Linked Account Status

System	Username	Success
Active Directory	[REDACTED]	<input checked="" type="checkbox"/>
OpenLDAP	[REDACTED]	<input checked="" type="checkbox"/>

[Click here to continue.](#)

I've Forgotten My Password. How Do I Recover My Password Instead of Resetting It?

If you ever have the experience of changing your password and then forgetting what you changed it to, the Recover Password feature of Portalguard makes it easy to see what your current password is rather than having to change it again. Please note that this process will display your password on the screen in plain text, so be sure no one else is able to view your screen during this process.

1. Go to the Portalguard page at <https://portalguard.uafs.edu>
2. Type in your username and click on the “Self Service” button.

UAFS UNIVERSITY OF ARKANSAS FORT SMITH **PortalGuard**

Username

Password Show password

3. Click the "Recover/See Current Password" radio button and click "Continue"

End-User Self Service
Please choose an action and click the button below to continue.

Username
[Masked Input]

Recovery Actions Available

- Unlock Account
- Reset Forgotten Password
- Recover/See Current Password

Continue **Cancel**

4. Type in answers to at least 3 of your challenge questions, and click the "Continue" button

Requested Action: Recover/See Current Password

1) What is your Mother's maiden name?
[Masked Input]

2) What is your Father's middle name?
[Masked Input]

3) What is your Mother's middle name?
[Masked Input]

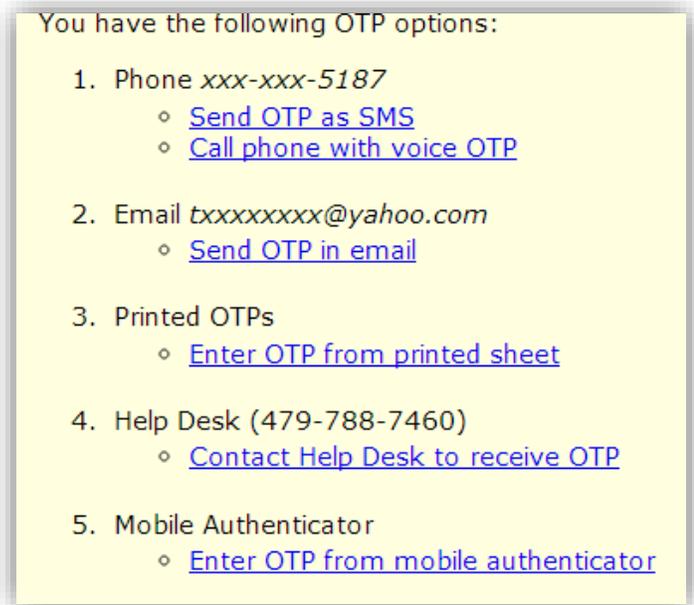
4) Which foreign country would you like to visit?
[Text Input]

6) What was the model of your first car?
[Text Input]

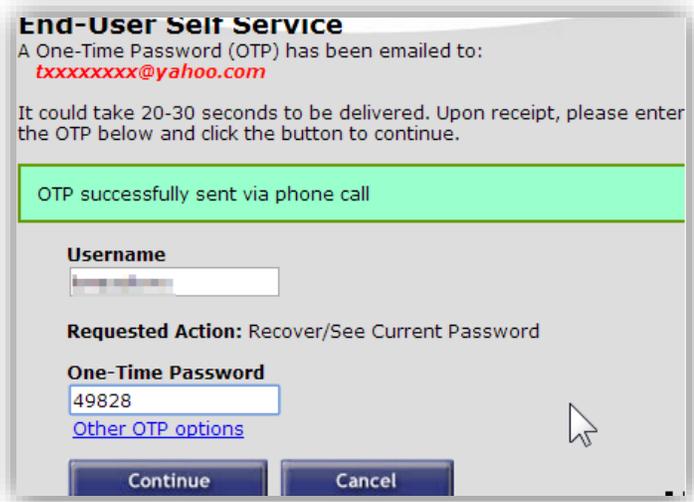
<< **>>** **Continue** **Cancel**

- 5. An OTP will be sent to your alternate email account.

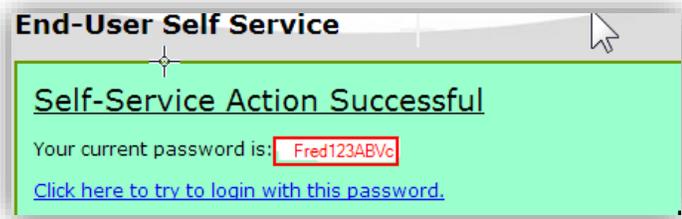
If you do not have access to your alternate email, you can click on the "Other OTP options" link, and choose another OTP option. This example shows 5 different options to choose from. You may have less options, depending on what you have personally setup in Portalguard.



- 6. Once the OTP number is received, enter it in the corresponding OTP field, then click the "Continue" button.



7. Your password will now be revealed on the screen.



My Password Has Expired. How Do I Reset My Password?

If your password expires and you wish to reset to a new password, follow this method.

1. Go to the Portalguard page at <https://portalguard.uafs.edu>
2. Type in your username and click on the "Self Service" button.



3. Click on the "Reset Forgotten Password" radio button and click "Continue".



4. Type in answers to at least 3 of your Challenge Questions, and click the "Continue" button.

Requested Action: Recover/See Current Password

1) *What is your Mother's maiden name?*
.....

2) *What is your Father's middle name?*
....

3) *What is your Mother's middle name?*
....

4) *Which foreign country would you like to visit?*

5) *What was the model of your first car?*

<< >> Continue Cancel

5. An OTP will be sent to your alternate email account.

If you do not have access to your alternate email, you can click on the "Other OTP options" link, and can choose your alternate OTP options. This example shows 5 options to choose from. You may have fewer options, depending on what you have personally setup in Portalguard.

End-User Self Service

A One-Time Password (OTP) has been emailed to:
txxxxxxxx@yahoo.com

It could take 20-30 seconds to be delivered. Upon receipt, please enter the OTP below and click the button to continue.

Username

Requested Action: Recover/See Current Password

One-Time Password

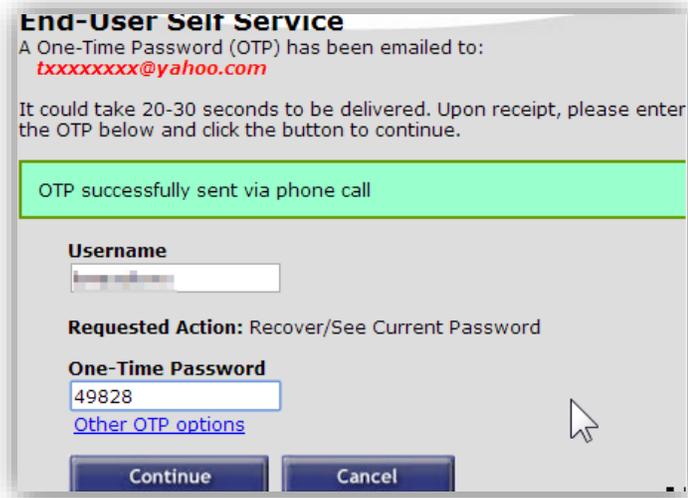
[Other OTP options](#)

Continue Cancel

You have the following OTP options:

- Phone xxx-xxx-5187
 - [Send OTP as SMS](#)
 - [Call phone with voice OTP](#)
- Email txxxxxxx@yahoo.com
 - [Send OTP in email](#)
- Printed OTPs
 - [Enter OTP from printed sheet](#)
- Help Desk (479-788-7460)
 - [Contact Help Desk to receive OTP](#)
- Mobile Authenticator
 - [Enter OTP from mobile authenticator](#)

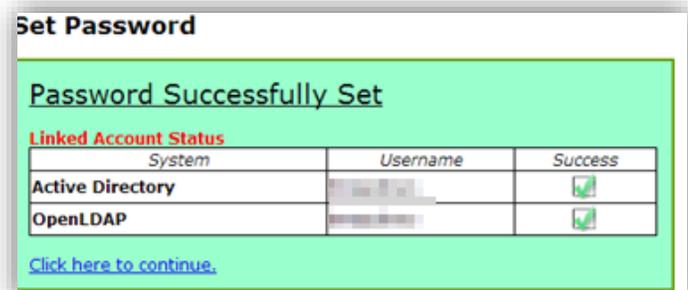
- This user chose the option to “Call phone with voice OTP”. Once the OTP number is entered, click the “Continue” button.



- You should see a message saying “Identity Verified”. Type in your new password and confirm it.



- You should see “Password Successfully Set”



What are Challenge Questions and Why Should I Use Them?

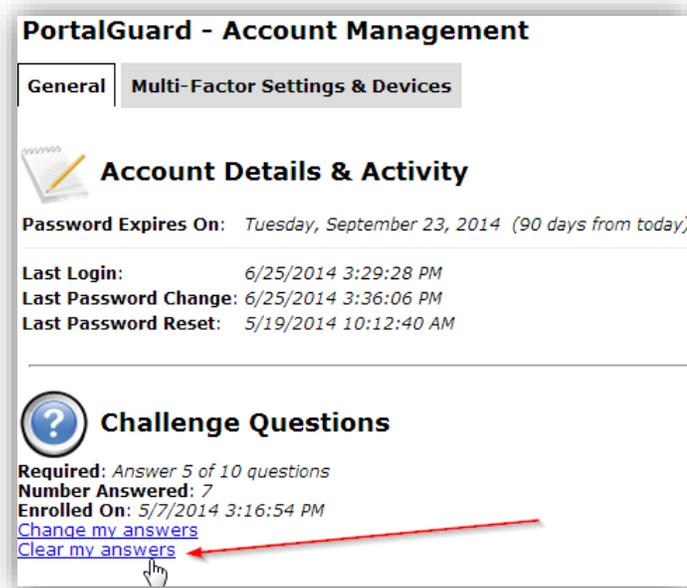
Challenge questions are a way of verifying your identity to the Portalgard system. When your password expires or your account becomes locked, you can use challenge questions combined with one-time passcodes (OTPs) to allow you to reset your password via the Portalgard system without the assistance of UAFS Technology Service Desk staff.

In order to make use of challenge questions in the future, you need to take time in the present to prepare them for use in the future. If you don't set them up before they're actually needed, you won't be able to reset your password without the assistance of the Technology Service Desk staff. Most likely, you will be required to actually visit the Technology Service Desk office with a photo ID to verify your identity, so it's wise to set them up ahead of time.

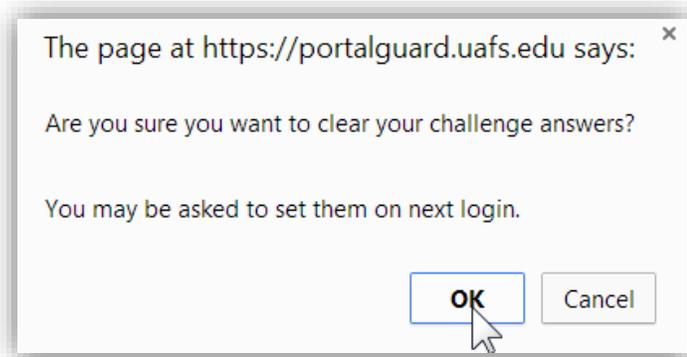
Responses to challenge questions are normally provided as part of the initial registration process. However, you may reset and reenter your challenge question responses at any time.

How do I reset my Challenge Questions?

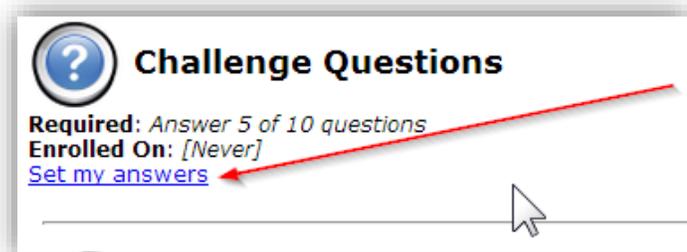
1. Login to Portalguard at <https://portalguard.uafs.edu>, and click on "Clear my answers"



1. Portalguard will ask you "Are you are sure you want to clear your challenge answers? Click "OK"



1. Click on "Set my answers" to start over



What are One-Time Passcodes?

One-time passcodes (also called one-time passwords) are a temporary numeric code used, in combination with your challenge question responses, to validate your identity to the Portalguard system. Portalguard provides numerous methods of delivering OTPs including using an alternate email account, sending a text message to your mobile phone, letting you hear them via a voice recording, or using the Google Authenticator application. These methods are collectively referred to as Multi-factor Settings and Devices in the Portalguard system.

Your alternate email account is normally setup during the initial Portguard registration process. However, you may change the email address used for your alternate account at any time. The use of a mobile phone as a way to get an OTP is optional but recommended.

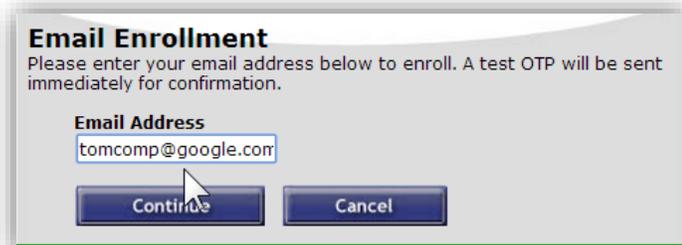
How Do I Change My Alternate Email Address?

To add or change an alternate email address, you **must have access** to your alternate email account at the time of registration. This can be through a web browser, a smartphone, a tablet, etc. Be sure you can access your alternate email account before proceeding.

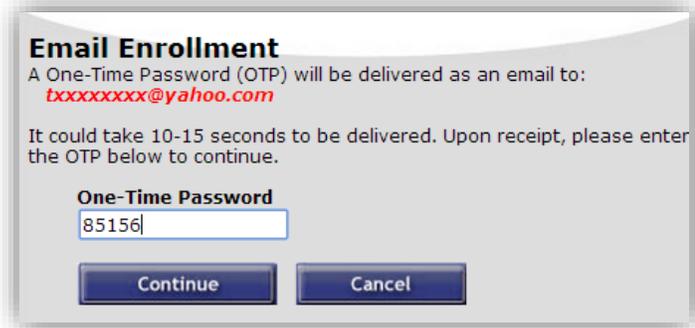
1. Login to Portalguard at <https://portalguard.uafs.edu>
2. On the General tab, find and click on the "Add my email". If you already have an email address set, click on "Change my email"



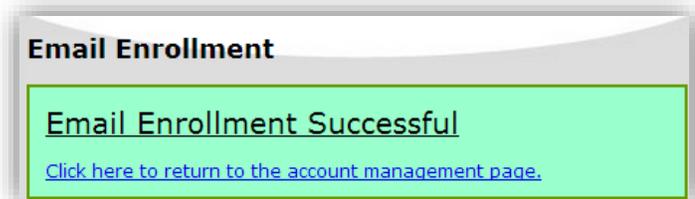
3. Enter your alternate email address and click on "Continue"



4. Access your alternate email and type in the OTP that you received in the email. Click "Continue"



5. You should see a "Successful" enrollment



How Do I Add or Delete a Mobile Phone?

To add or change an mobile phone entry, you **must have access** to the mobile phone at the time of registration. Be sure your phone is turned on and connected to the service provider before proceeding.

1. Login to Portalguard at <https://portalguard.uafs.edu>
2. Click on "Multi-Factor Settings & Devices", then click on "Remove" or click on "Add new phone"



Phone	Enrolled	
(479) [redacted] [US] (mobile)	6/20/2014 10:48:35 AM	Remove

3. Add in your phone number with area code then select whether or not to receive text message OTPs on your phone. Then click the "Continue" button.

Enrollment - Mobile Phone
Please enter your current password and your phone number to enroll. You may also be prompted to select a mobile phone carrier from a drop-down list. A test message will be sent immediately for confirmation. You can skip this enrollment but you will be asked to enroll again during your next login.

To permanently suppress reminders for this authentication type, check the box below before skipping. You can always enroll from the Self Service button on the main login form.

Username
cspears

Password
..... Show password

Country
United States

Phone Number (###-###-####)
[]

This phone can receive SMS/text messages
 This phone **cannot** receive SMS/text messages

Permanently Suppress Reminders

Continue Skip

4. You will receive the OTP on your phone. When you do, enter it into the enrollment screen and click "Continue".

Enrollment
A One-Time Password (OTP) will be delivered as a text/SMS to:
xxx-xxx-5187

It could take 10-15 seconds to be delivered. Upon receipt, please enter the OTP below to continue.

One-Time Password
[]

Continue Cancel

What is the Google Authenticator?

The Google Authenticator is a mobile device applications created by Google that can generate OTPs. These OTPs are compatible with the Portalgard system and can be used to validate your identity.

How Do I setup the Google Authenticator?

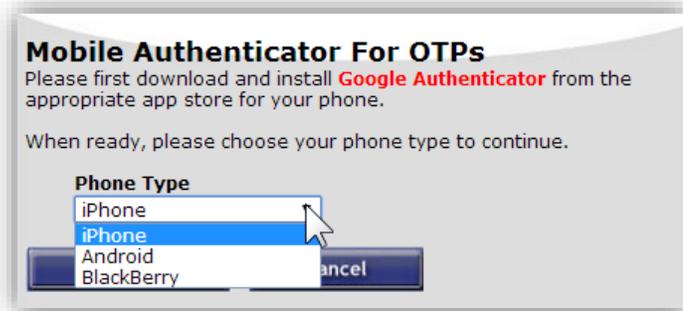
1. Download and install the “Google Authenticator” app on your smartphone or tablet.
2. Login to Portalguard at <https://portalguard.uafs.edu>
3. Click on “Multi-Factor Settings & Devices”, then click on “Enable mobile authenticator”



The screenshot shows the 'PortalGuard - Account Management' interface. The 'Multi-Factor Settings & Devices' tab is selected, indicated by a red arrow. Below the tab, there are three sections: 'Registered Phones' with a table of enrolled devices, 'Printed One-Time Passcodes' with a printer icon and links for clearing or printing OTPs, and 'Mobile Authenticator' with a link to 'enable mobile authenticator' and a red arrow pointing to it.

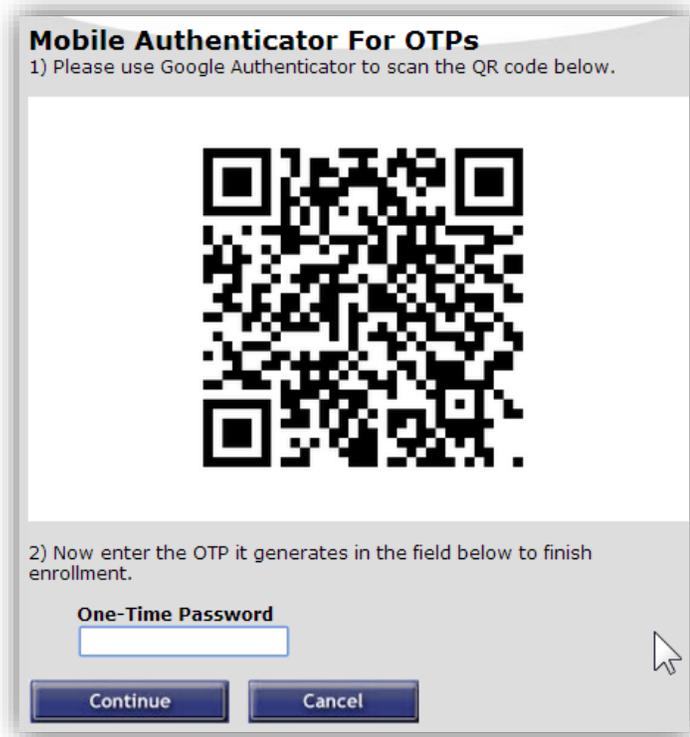
Phone	Enrolled	
(479) 4- [REDACTED] 7 [US] (mobile)	6/25/2014 4:01:12 PM	Remove

4. Pick out your type of phone from the drop down box.

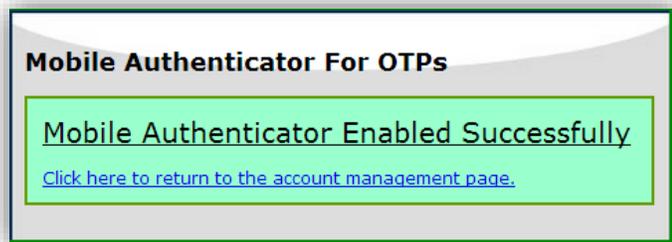


The screenshot shows a dialog box titled 'Mobile Authenticator For OTPs'. It contains instructions to download and install the Google Authenticator app. Below the instructions, there is a 'Phone Type' dropdown menu with a mouse cursor pointing to it. The dropdown menu is open, showing options for 'iPhone', 'Android', and 'BlackBerry'. An 'Cancel' button is visible at the bottom right of the dialog box.

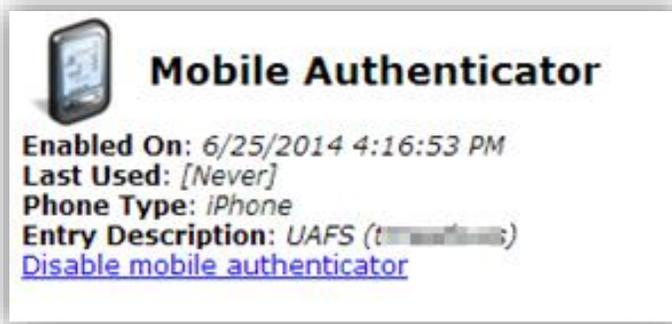
5. Scan the code with the Google Authenticator phone app that you downloaded to your smartphone and enter the "OTP".
6. Enter the OTP that was generated into the field provided.



7. You should see the following screen to show you succeeded



8. Portalguard will now show a link to "Disable mobile authenticator" if you ever want to deactivate it.



Printing out OTPs for Future Use

If you desire, you may print a list of OTPs to carry with you in the event you need to reset your password and you don't have access to the other OTP delivery systems. Printing OTPs is strictly optional.

1. Login to Portalguard at <https://portalguard.uafs.edu>
2. Click on "Multi-Factor Settings & Devices" tab at the top
3. Click on "Print new OTP's"

PortalGuard - Account Management

General **Multi-Factor Settings & Devices**

Registered Phones

Phone	Enrolled	
(479) 4 [US] (mobile)	6/20/2014 10:48:35 AM	Remove

[Add new phone](#)

Printed One-Time Passcodes

Last Printed On: [Never]

[Print new OTPs](#)

4. Codes can be printed out by clicking on the "Print OTP's" button at the bottom. Each code can only be used once, so be sure to scratch a code off after using it.

Backup One-Time Passcodes

1. 009 805
2. 416 002
3. 487 215
4. 971 007
5. 372 563
6. 857 539
7. 013 732
8. 989 462
9. 285 557
10. 667 415

Keep these codes some place safe like your wallet.
Be sure to enter all 6 characters WITHOUT SPACES and draw a line through

These passcodes can be erased or new ones can be generated at:
<https://portalguard.uafs.edu/default.aspx>

OTPs generated on: 6/25/2014 3:49:39 PM

[Print OTPs](#)

5. Once you have printed codes, the "Clear printed OTP's" will show up on the screen if you ever want to clear them and start over.

Printed One-Time Passcodes

Last Printed On: 6/25/2014 3:49:39 PM [Clear printed OTPs](#)

[Print new OTPs](#)

I get “Authentication Failed” when I try to login to Portalguard. What can I do?

1. Click the “Show password” and make sure that you are typing your password in correctly. If this doesn’t work, then you may need to reset your password



2. Click the “Show password” and make sure that you are typing your password in correctly. If this doesn’t work, then you may need to reset your password



How to Get Additional Help

If you still have questions about using Portalguard, please contact the Technology Service Desk by sending an email to uafs@service-now.com or calling (479) 788-7460.

Feedback

We welcome your feedback about this change. Please send your feedback to TSFeedback@uafs.edu

Document History

Version	Date	Revision history or Review (Author)
1.0	July 21, 2014	Initial publication (Terry M & Curtis S)