

Multi Factor Authentication (MFA) for NCEdCloud

*Required for users with LEA Administrator and
LEA Data Auditor Roles*

*Version 1.2
Mark Scheible, MCNC
May 2019*

Table of Contents

Introduction	3
Checking for Users with Privileged Roles	4
Configuring Your MFA One-Time Password	4
Before Logging In -> Download One of the Apps	4
Setting up MFA	5
SS#1	5
Enter your 10-digit UID (username) and click “Go”	5
SS#2	6
Next enter your Password and click “Go”	6
Setting Up Your One-Time Password	7
Once OTP is Setup:	8
SS#4	8
Resetting the OTP for Privileged Users	9
Reasons for Resetting the OTP	9
How to Reset the OTP in NCEdCloud	9
Figure SS#5 - Reset OTP	10
SS#5	10
Appendix A - Setting Up MFA with Google Authenticator	11
“Google Authenticator” app:	11
Add a New Service - Click on “+” in Authenticator screen	11
Next: Select “Scan Barcode” at bottom of screen	12
SS#7	12
SS#8	13
SS#9	14
Appendix B - Setting Up MFA with the RapidIdentity App	15
RapidIdentity App	15
Under Personal Account - Select “Scan QR Code”	15
SS#10	15
Camera View to Scan QR Code	16
SS#11	16
Submitting Scanned Information to Rapid Identity App	17

SS#12	17
SS#13	18
SS#14	19
Appendix C - Setting Up MFA with Authy (desktop app)	20
Authy Desktop Authenticator	20
Register the application	20
Once Configured	20
SS#15	20
Enter your Master Password	21
SS#16	21
Click on the “+” to Add your NCEdCloud Account	22
SS#17	22
Enter Code From the NCEdCloud OTP Setup Page	23
SS#18	23
Fill in the Account Name and Select a Generic Color	24
SS#19	24
Click on the NCEdCloud entry to get your 6-digit Code (883 004)	25
SS#20	25
SS#21	25

Introduction

As a part of continuing efforts to enhance the security posture of statewide IT systems, and due to the access **NCEdCloud LEA Administrators** and **LEA Data Auditors** have to student and employee data, Multi-Factor Authentication (MFA) will now be required for users with either of these roles in the NCEdCloud IAM Service. NCDPI will be rolling out MFA for these privileged users statewide on **Thursday, May 9th, 2019**. This is a first step towards expanding similar security measures to educators and administrators with privileged access to staff and student data. MFA will not be required for users with **LEA Help Desk** and **LEA Student Help Desk** roles.

The NCEdCloud implementation of MFA - also known as 2-factor authentication - will take advantage of a “One-Time Password” or OTP. Most likely, many users have already used something similar when accessing personal online accounts that require additional security measures and they receive a 6-digit code on their phone to enter into the application. However, in this case you will be running an application on your mobile device so **there is no requirement to provide your cell number or receive a text message**. (However, if you choose to use the Authy desktop application described below, your cell number is required to register the app.)

For the NCEdCloud implementation we will be using an Authentication application which will provide you with a 6-digit code to enter when you login. Three applications (Google Authenticator, RapidIdentity, and Authy) are approved for NCEdCloud’s OTP generation. (Others may work, but have not been tested.) **Please download/install one of these before logging in, once MFA has been turned on for your LEA or Charter School.**

This document contains instructions on how to configure your One-Time Password (OTP) in the NCEdCloud IAM Service. Additionally, there are instructions for LEA Administrators to RESET the OTP for their privileged users in the event they need to reconfigure their MFA, for instance if you purchase a new phone, accidentally delete your app, etc.

Appendices A, B, and C provide setup instructions and links for the authenticator applications for mobile devices and laptops/desktops. Any of these will work with NCEdCloud, so you only need to pick one.

Checking for Users with Privileged Roles

Now might be a good time to review who in your LEA or Charter School has the **LEA Administrator** and/or **LEA Data Auditor** privileged roles and whether they are still needed. Communication about the MFA rollout to these users will be your responsibility. This document can be sent to all users impacted by this change.

If you are not familiar with how to check who has these privileged roles, the process will require an “advanced search” under your **Profiles** tab in NCEdCloud. The steps are:

1. Click on **Profiles** (side navigation)
2. Click on **Manage LEA Employees**
3. Check the **Advanced Search** box
4. Click on **Define Criteria**
5. In the Criteria window click on **Add Criteria**
6. In the dropdown box select **NCEdCloud Roles**
7. Enter ONE of the roles below in the empty value box
 - a. **LEA Administrator**
 - b. **LEA Data Auditor**
8. Click on **Save** at the bottom of the window
9. Then click on the **Search** button to see your users with that role
10. You can repeat the process by clicking on **Define Criteria** and entering the other role in the value box

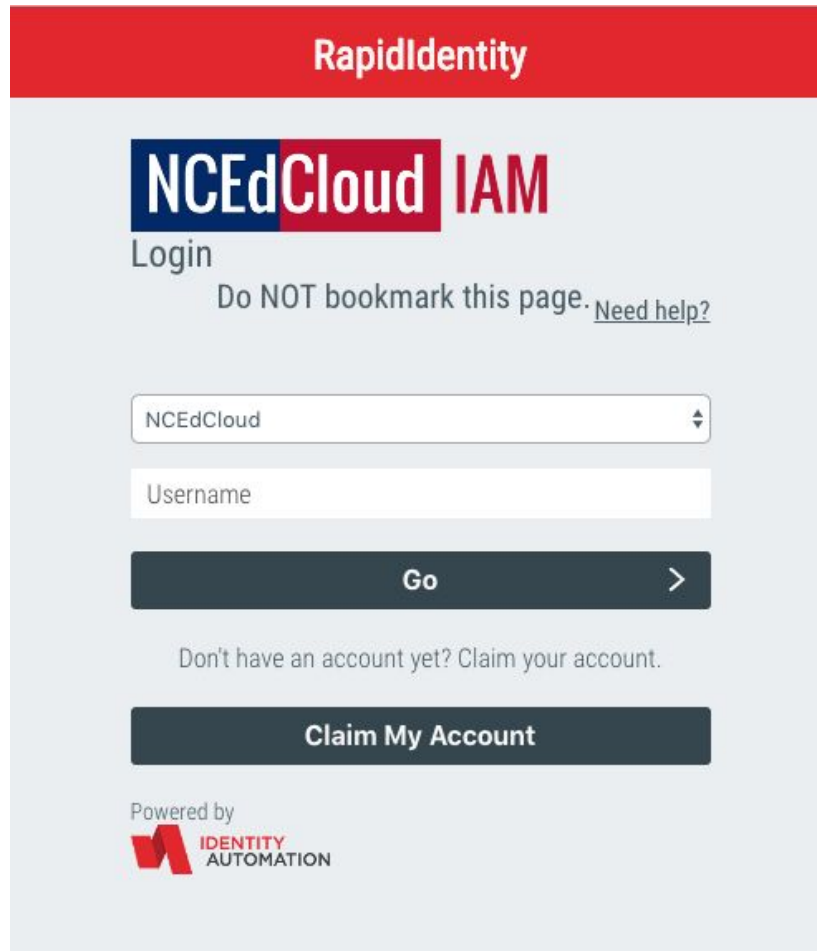
Configuring Your MFA One-Time Password

Before Logging In -> Download One of the Apps

When MFA is activated for your LEA or Charter School (during a pilot or the statewide rollout), you will need to configure the One-Time Password (OTP) functionality the first time you login. **To prepare for MFA being activated, you should download one of the mobile apps for your phone, or download and install Authy (or another desktop authentication application) on your desktop.** Enter any configuration information required by the application prior to logging in to setup your OTP.

Setting up MFA

When you access my.ncedcloud.org after MFA is activated, you will be presented with the Username and Password screens as usual.



RapidIdentity

NCEdCloud IAM

Login

Do NOT bookmark this page. [Need help?](#)

NCEdCloud

Username

Go >

Don't have an account yet? Claim your account.

Claim My Account

Powered by
IDENTITY
AUTOMATION

SS#1

Enter your 10-digit UID (username) and click “Go”

RapidIdentity

NCEdCloud IAM


Login

Do NOT bookmark this page. [Need help?](#)

Go >

Start Over ↺

Powered by

 **IDENTITY**
AUTOMATION

SS#2

Next enter your Password and click “Go”

Setting Up Your One-Time Password



RapidIdentity


NCEdCloud IAM

One-Time Password
Do NOT bookmark this page.

You are required to set up One-Time Password before proceeding.

Scan the barcode below with the RapidIdentity app or another one-time password app.






FPOVFIV6NXN23MUEI2EEPSCPRE4F5F4R


Go >


Start Over ↺

Powered by
 **IDENTITY**
AUTOMATION




SS#3

If you are using a **mobile device app** for password authentication, then you will need to use your app to scan the QR code (barcode) displayed on the OTP setup screen (see the blue arrow on Figure SS#3). 

If you are planning to use a **desktop app like “Authy”**, then you will need to copy the alphanumeric code below the QR code (see the red arrow on the diagram above),  and enter it into your browser application

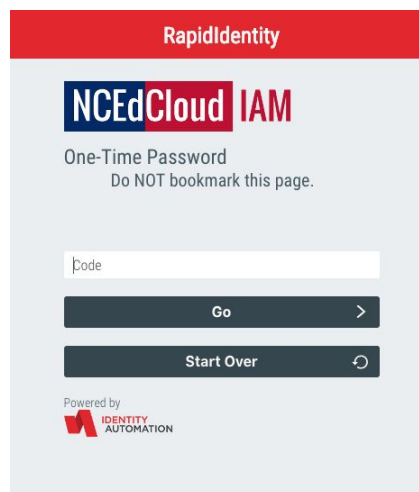
** See the specific Appendix (A,B,C) for application setup instructions for Google Authenticator, RapidIdentity, and Authy.*

After setting up your authentication app (e.g. RapidIdentity, Google Authenticator, or Authy), **enter the 6-digit code** provided by the app in the “Code” window on the One Time Password setup page (SS#3), and click “Go”. 

You will then be taken to the NCEdCloud Applications page as before.

Once OTP is Setup:

Thereafter, every time you logon to NCEdCloud (after entering your Username and Password and clicking on the “Go” button), you will be presented with a 3rd screen to enter your 6-digit code from your authentication application.



SS#4

Resetting the OTP for Privileged Users

Reasons for Resetting the OTP

MFA is required for all users with the LEA Administrator or LEA Data Auditor roles. Once MFA is enabled statewide, these users will be required to set up their One Time Password the next time they login. Once configured, the authenticator applications should not need to be updated, however, there are a few reasons a user might need their OTP reset:

1. If the user accidentally deletes their authentication app
2. If the user gets a new mobile device and the authenticator application needs to be added or reconfigured
3. If the user wants to change to a different authenticator application
4. If the user wants to have BOTH a mobile app and a Desktop app configured at the same time.
 - a. This is possible, but the QR and alternate codes both need to be used/captured at the time the OTP is set up in NCEdCloud
 - b. If the user wants to have Authy configured on their desktop after they've already set up their phone app, they'll need their MFA OTP **Reset** by an LEA Administrator for their LEA / Charter School, then they'll need to scan the QR code on their mobile device and copy the alphanumeric code below it to enter into Authy.

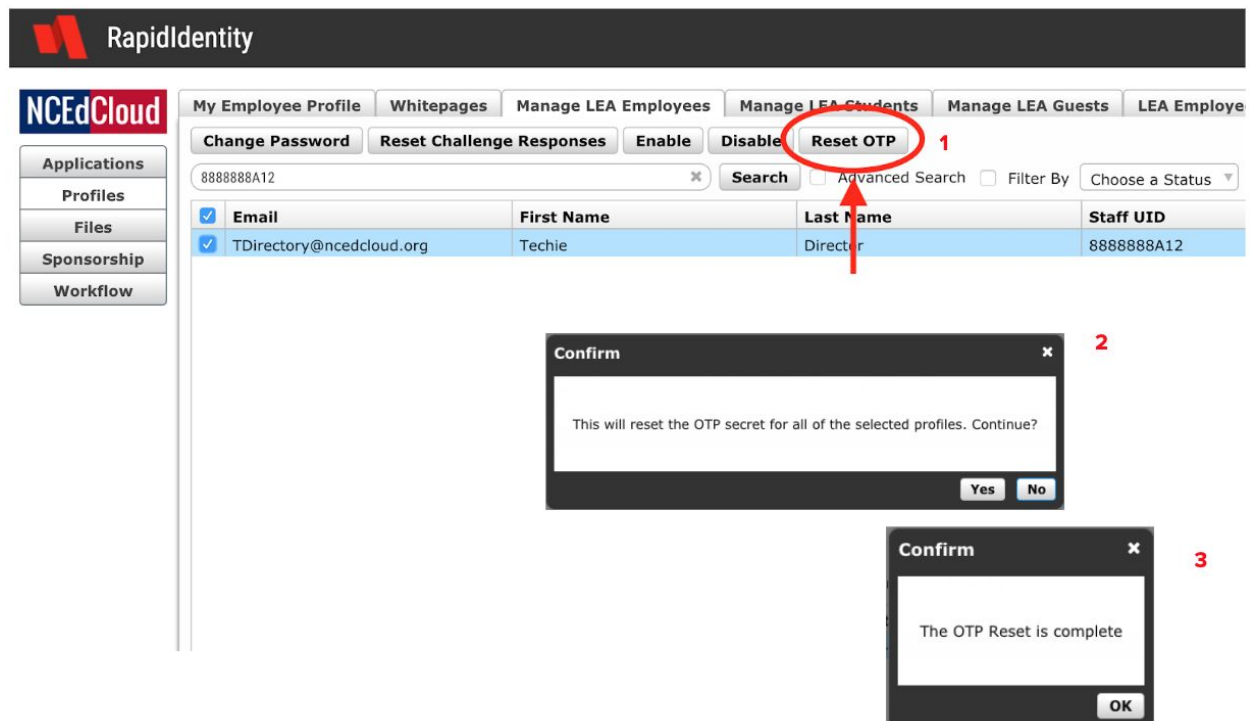
How to Reset the OTP in NCEdCloud

LEA Administrators can reset another privileged user's OTP in the Profiles section of the NCEdCloud IAM Service. Simply enter the user's UID (username) in the search field, select the user's entry (checkbox) and the "Reset OTP" button "lights up". Once this button is clicked (and confirmed), the user will no longer have a valid MFA configured in NCEdCloud and will be presented with the One-Time Password setup page the next time they login.

When the user logs in following the "reset", they should have their new device ready with whichever authenticator app they wish to use to scan the QR code (SS#3 - Blue Arrow), and/or their Authy app should be open and ready to add the code they are given from NCEdCloud (SS#3 - Red Arrow).

Figure SS#5 - Reset OTP

The location of the Reset OTP button is circled in red in Figure SS#5 below.



SS#5

Appendix A - Setting Up MFA with Google Authenticator

“Google Authenticator” app:

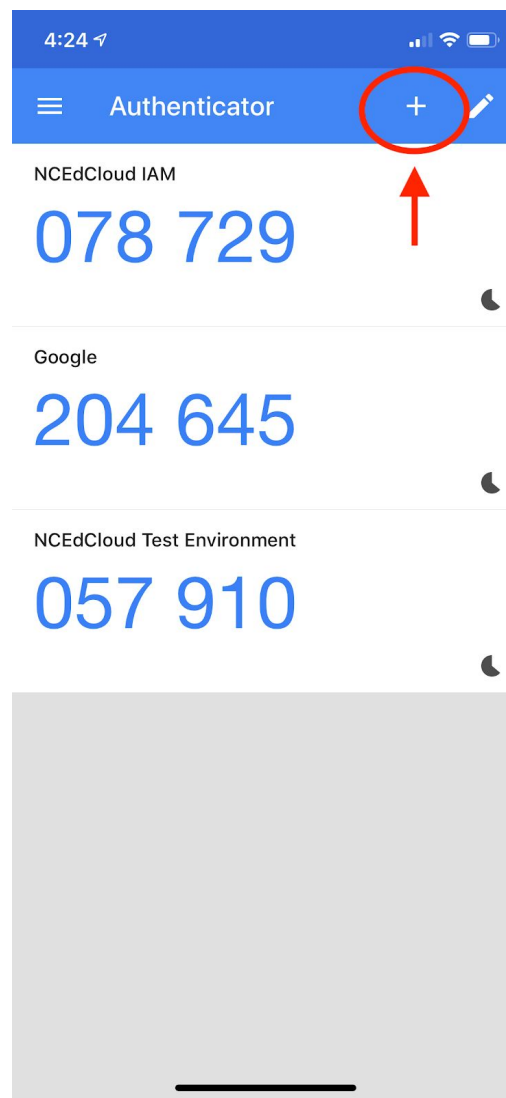
(Android)

<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>

(iPhone)

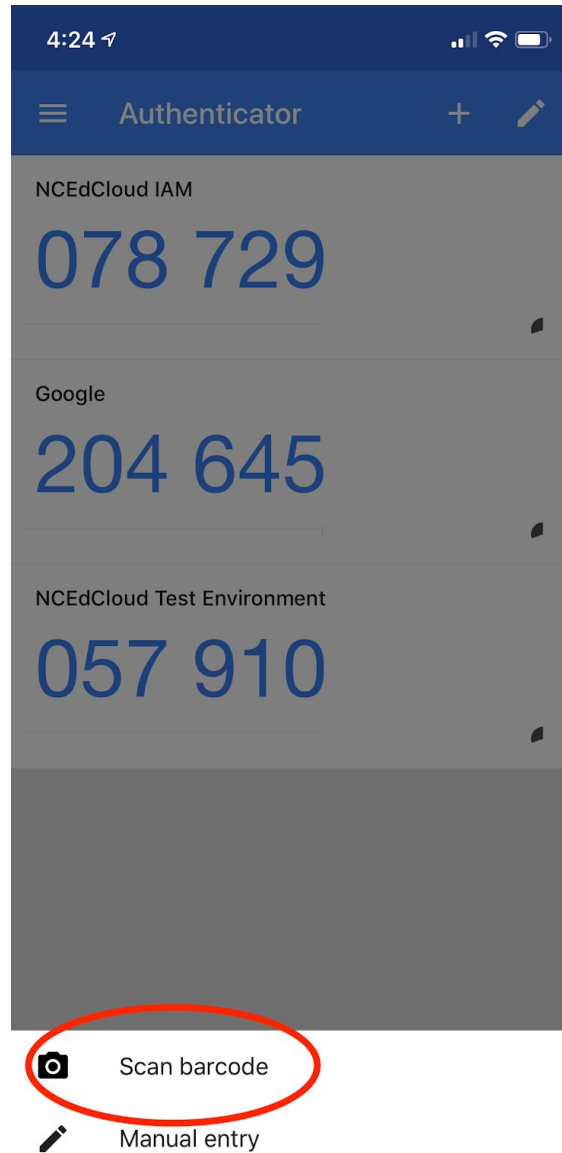
<https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8>

Add a New Service - Click on “+” in Authenticator screen



SS#6

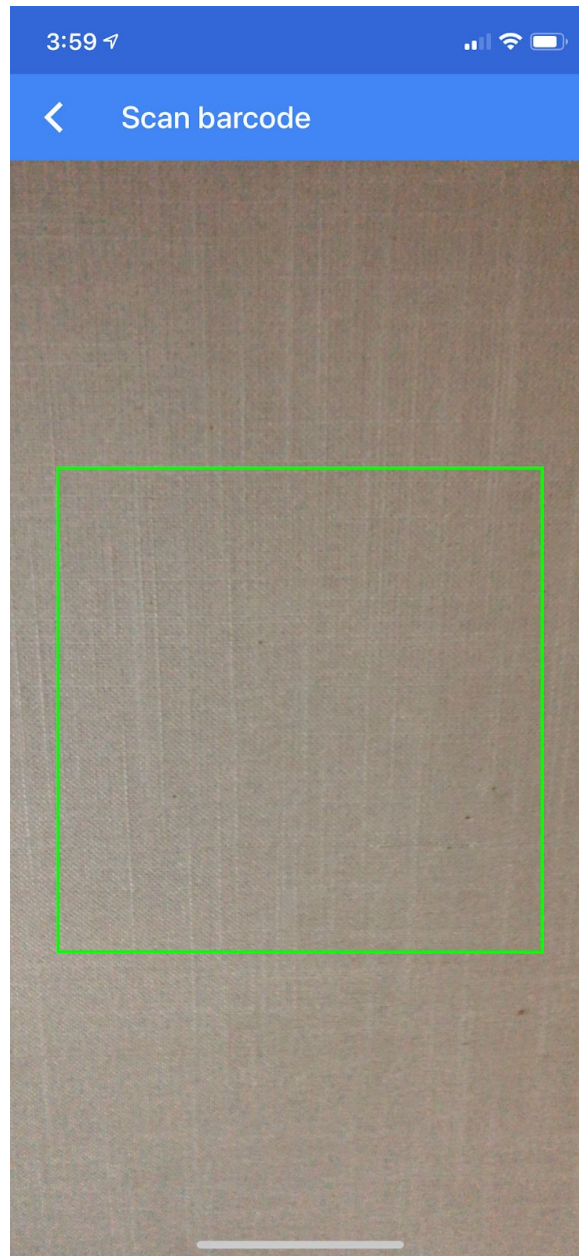
Next: Select “Scan Barcode” at bottom of screen



SS#7

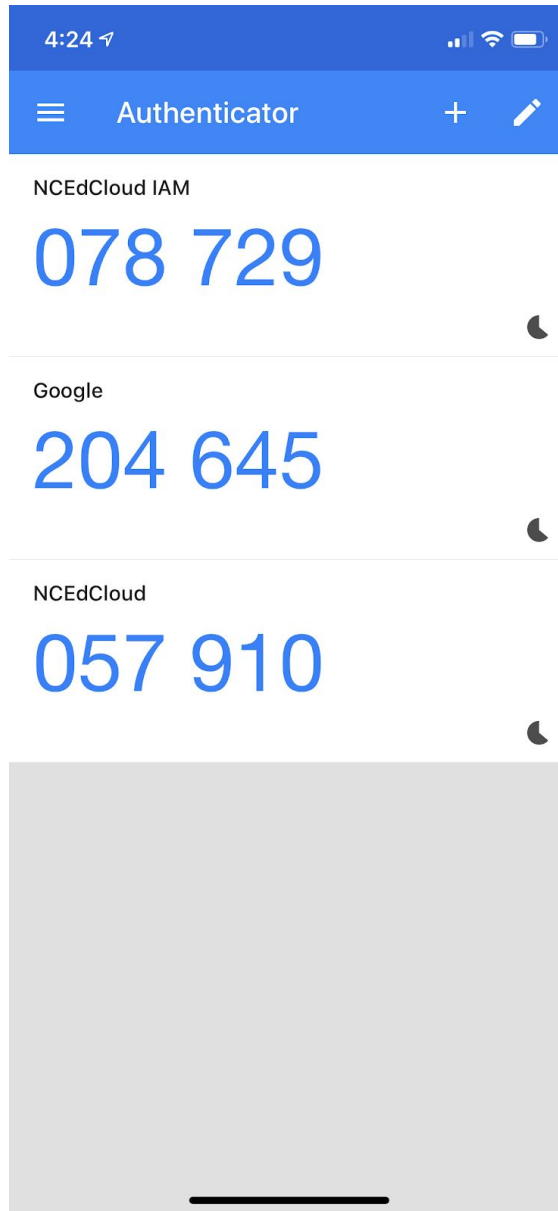
After selecting “Scan Barcode” your camera will show a box on the screen (see below).

Center the camera “box” over the QR barcode and Google Authenticator will automatically create a new item in your list of systems with the name “NCEdCloud IAM” (See SS#9)



SS#8

Note the top entry in SS#9 (NCedCloud IAM), which provides you with a 6-digit code to enter in the NCedCloud One-Time Password Setup screen shown in SS#3 at the Green arrow (**only enter the 6 digits, NOT the Space**).



SS#9

Appendix B - Setting Up MFA with the RapidIdentity App

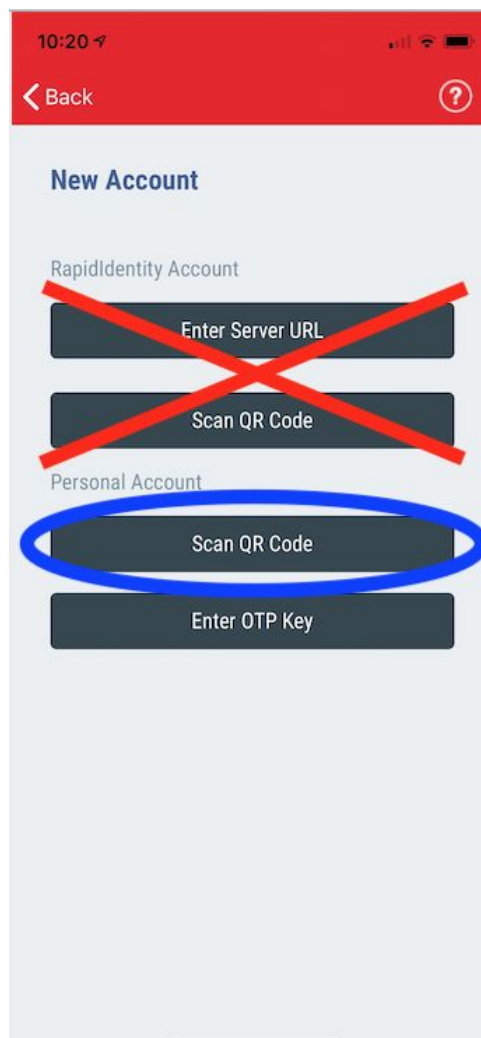
RapidIdentity App

(Android)

https://play.google.com/store/apps/details?id=com.idauto.rim.xamarin.android&hl=en_US

(iPhone) <https://itunes.apple.com/us/app/rapididentity/id1230131130?mt=8>

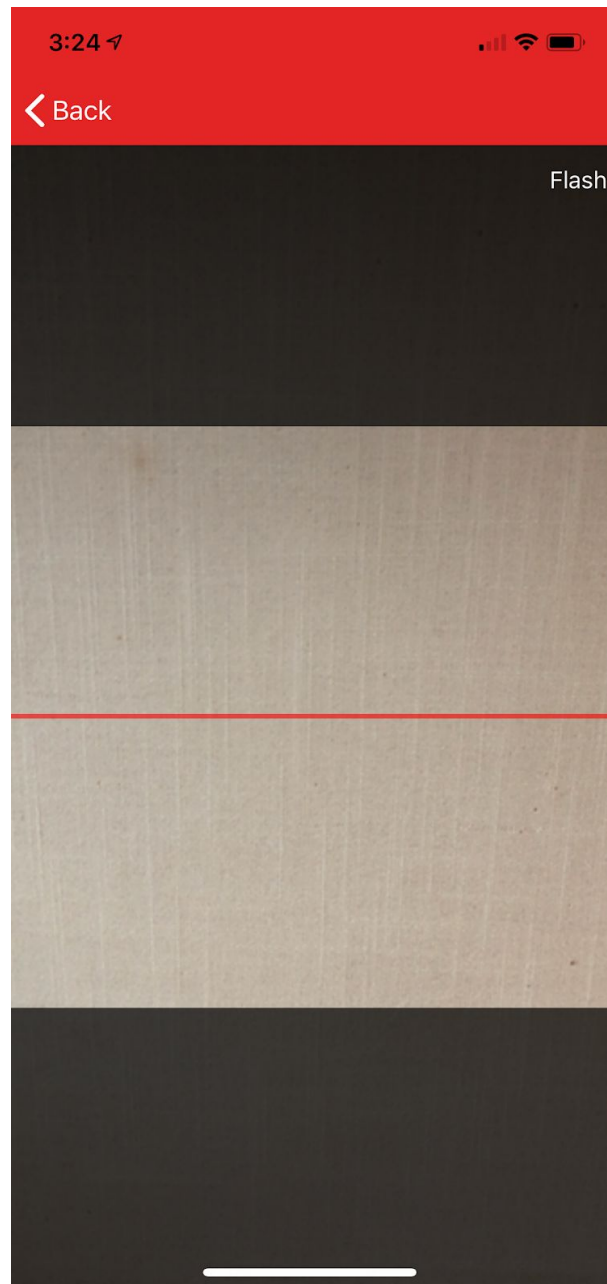
Under Personal Account - Select “Scan QR Code”



SS#10

After selecting “Scan QR Code” your camera will show a box on the screen (see below). Center the red line in the “box” over the QR barcode and the Rapid Identity app will automatically create a new item in your list of systems with the name “NCEdCloud IAM”

Camera View to Scan QR Code

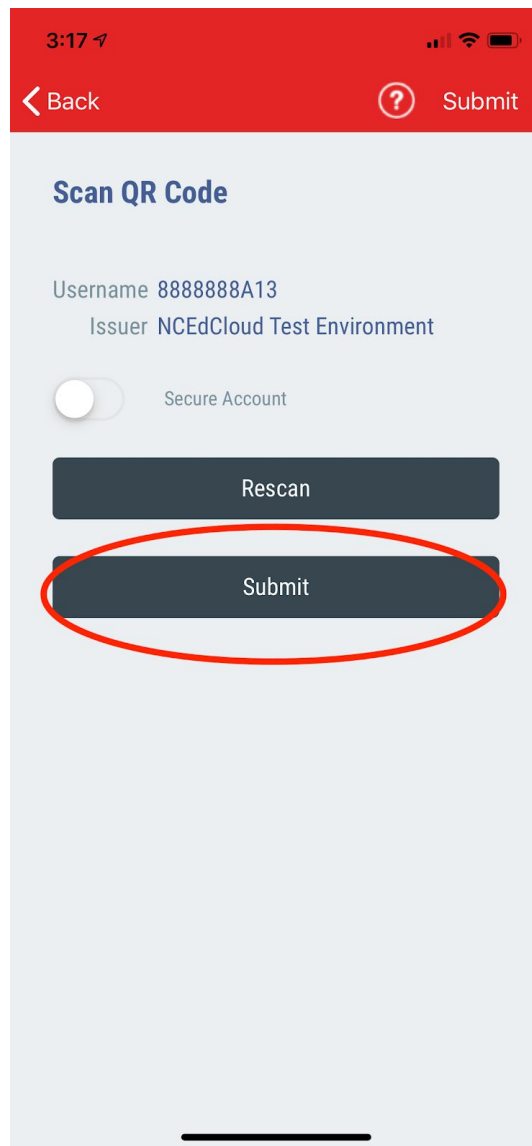


SS#11

Once you've scanned the QR Code, the Rapid Identity App will display the Service "NCEdCloud IAM" (Test in the screen capture below), along with your Username (UID) and ask whether you wish to Submit the scan or Scan Again. Select the "Submit" button to finish your OTP setup on the app.

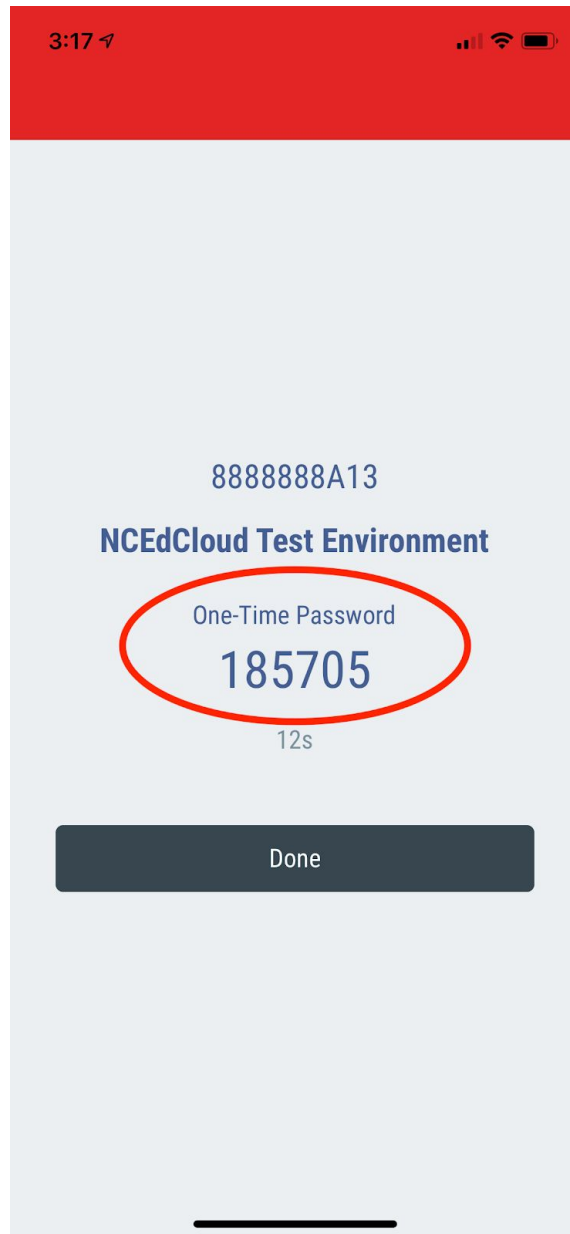
Submitting Scanned Information to Rapid Identity App

Clicking Submit on this screen will show you your 6-digit One-Time Password.



SS#12

Once you receive this screen, you can enter your 6-digit One-Time Password (185705 below) into the NCEdCloud OTP Setup Screen in the box provided (Green arrow in SS#3 above) and click on GO. You have a total of 30 seconds until the password is invalid and you receive a NEW password. You're all done at this point.



SS#13

Once you've entered your 6-digit number to complete the OTP Setup, you can select "Done". You'll see the screen below, which will show up in the future whenever you open the Rapid Identity app to obtain your OTP.



SS#14

Appendix C - Setting Up MFA with Authy (desktop app)

Authy Desktop Authenticator

(Home page) <https://authy.com/>

(Download page) <https://authy.com/download/>

After obtaining Authy from the [www.authy.com](https://authy.com/) website (click on “DOWNLOAD” in the top right corner of their home page) and installing it on your device, you will need to set it up to provide a OTP for logging in to the NCEdCloud IAM Service.

Register the application

Enter your:

- cell number
- email address and a
- Master Password

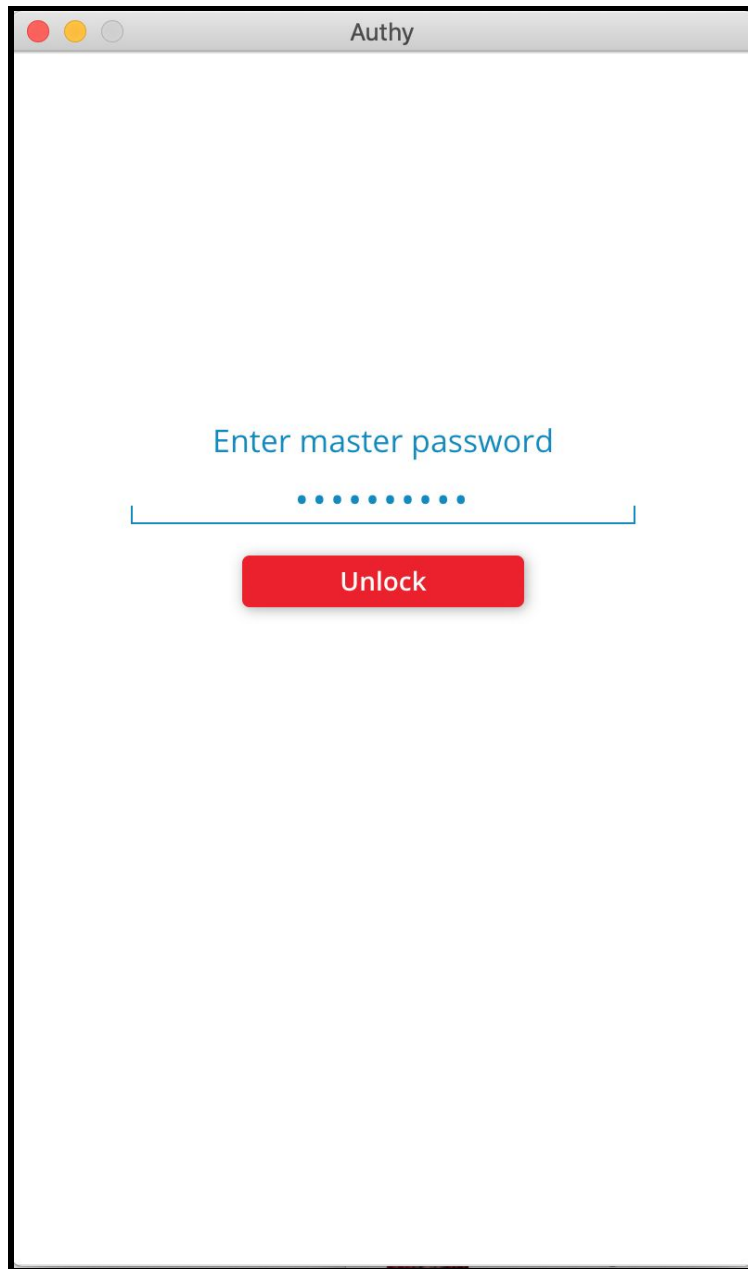
Once Configured

Click on the Authy icon to start the App



SS#15

Enter your Master Password

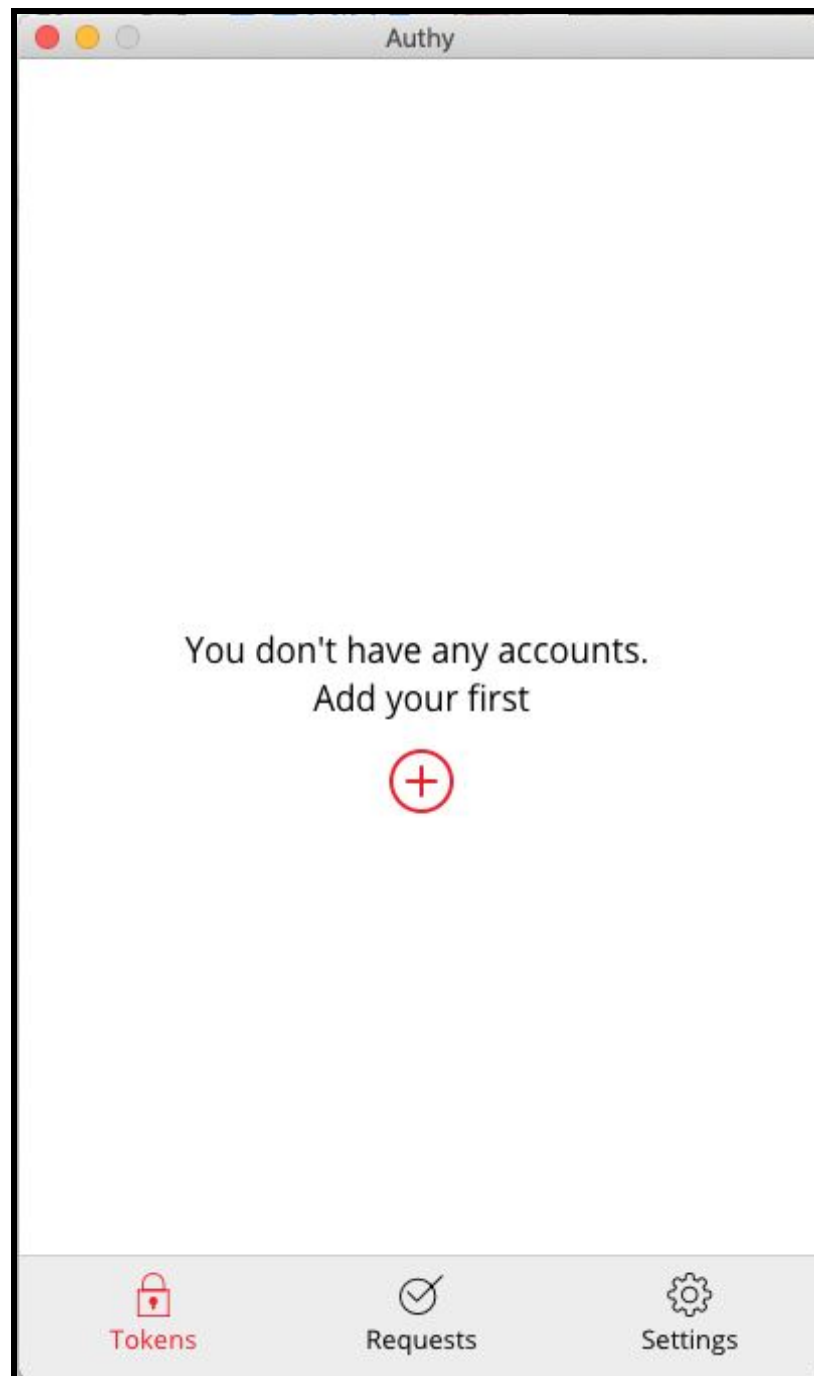


The image shows a screenshot of the Authy application window. The window has a title bar with the text "Authy" and three standard macOS window control buttons (red, yellow, and grey). The main content area of the window is white and contains the following elements:

- The text "Enter master password" in a blue, sans-serif font, centered horizontally.
- A password input field below the text, consisting of a horizontal line with ten blue dots in the center, indicating masked characters.
- A red rectangular button with the word "Unlock" in white text, centered below the input field.

SS#16

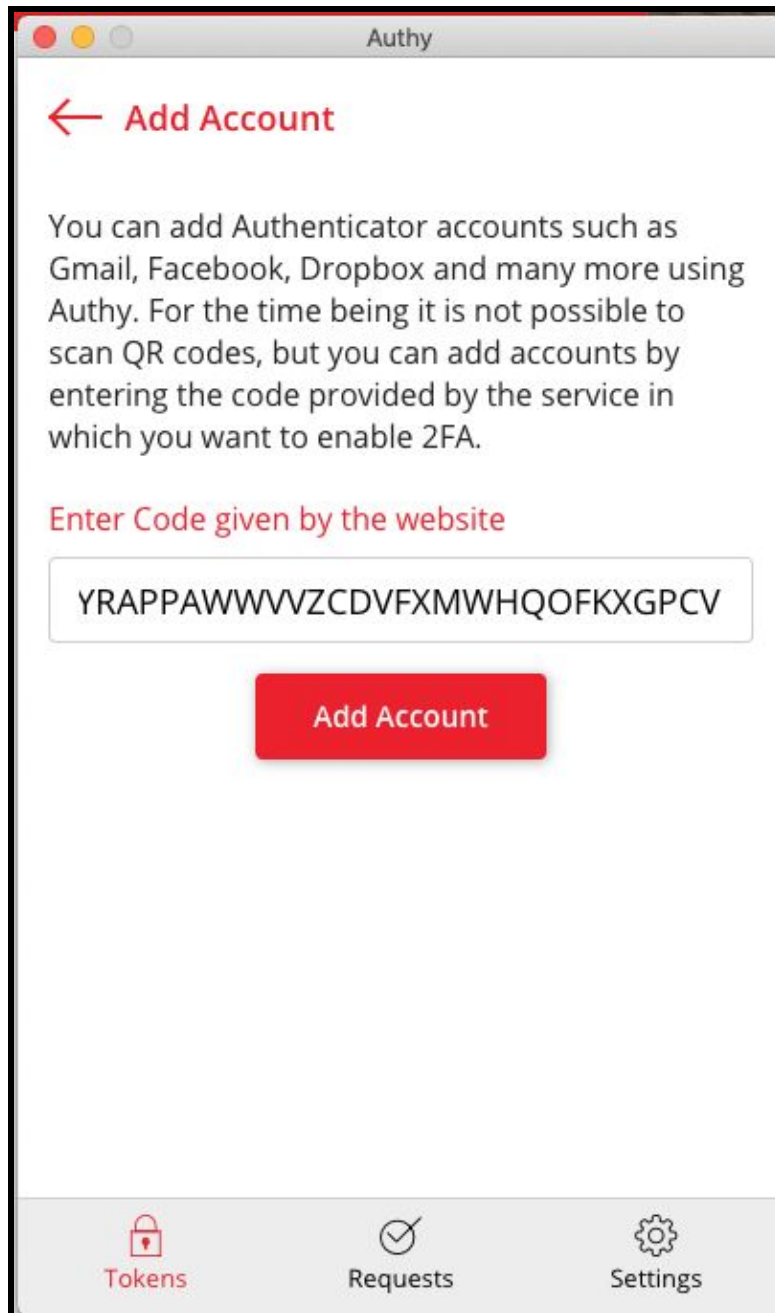
Click on the “+” to Add your NCEdCloud Account



SS#17

Enter Code From the NCedCloud OTP Setup Page

Authy cannot use QR codes (as of this writing), so you will need to **enter the code** provided by the NCedCloud One-Time Password screen (see SS#3 - Red Arrow). **Then click the “Add Account” button.**



SS#18

Fill in the Account Name and Select a Generic Color

Enter NCEdCloud in the Account Name box (you can also add your UID or name if you would like).

Select one of the Generic colors for screen highlights when your 6-digit Code is displayed. (Note that the Token Length above the Save button is set to 6-digit.) Then complete your entry by clicking on the Save button.

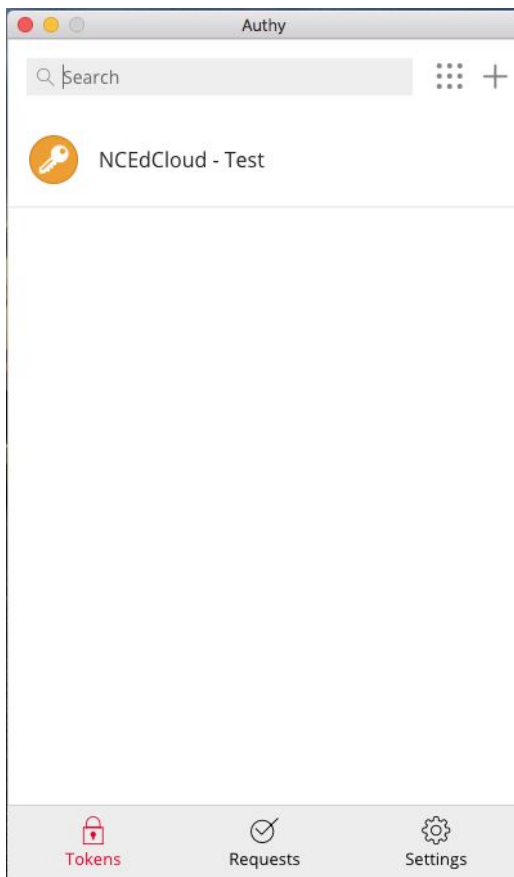
The screenshot shows the 'Authy' app interface. At the top, there's a title bar with the word 'Authy'. Below it, a red arrow points left to the text 'Account Name and Logo'. A text input field contains '8888888A13 - Delly Admin'. Below this is a list of generic colors: 'Generic Orange' (selected with a green checkmark), 'Generic Purple', and 'Generic Red'. Below these are logos for 'Amazon Web Services' and 'Amazon.com'. At the bottom, there's a 'Token length' section with three radio buttons: '6-digit' (selected), '7-digit', and '8-digit'. Below this are two buttons: a red 'Save' button and a red 'Delete' button. At the very bottom, there's a navigation bar with three icons: 'Tokens' (a padlock), 'Requests' (a checkmark), and 'Settings' (a gear).

SS#19

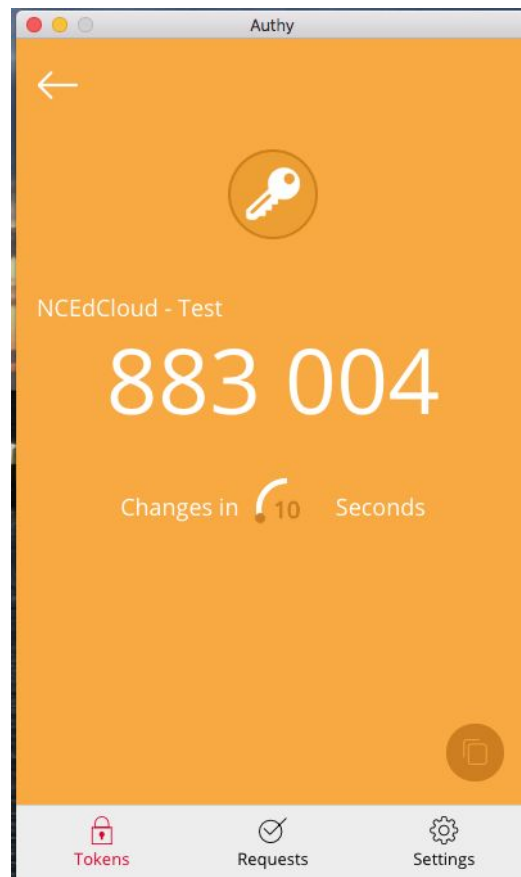
Click on the NCEdCloud entry to get your 6-digit Code (883 004)

Authy can display your account in different “views” by clicking on the square of dots to the right of the Search box. The full screen view also displays your 6-digit code and the time remaining until it changes (30 seconds per code).

If you click on the compact view (below), it will display a full box with the 6-digit code and the remaining time.



SS#20



SS#21

Once you have your 6-digit code, enter it in the One-Time Password setup screen (if it's the first time you're logging in with MFA enabled), or in the One-Time Password login screen shown in screen shot #4 (SS#4).

January 2019 - MAS