

Multi-Factor Authentication (MFA) in the NCEdCloud IAM Service

(MFA Rollout for Privileged NCEdCloud Accounts)

- Mark Scheible, MCNC

Introduction to MFA for NCEdCloud Privileged Users

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.

The following slides will introduce you to the One-Time Password (OTP) setup screen, the “Reset OTP” button for LEA Administrators, and provide links to the apps used to obtain the 6-digit code needed when you login to the NCEdCloud.

Links to MFA Apps (Mobile Devices or Desktop)

“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>

“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>

“Authy Desktop” authenticator:

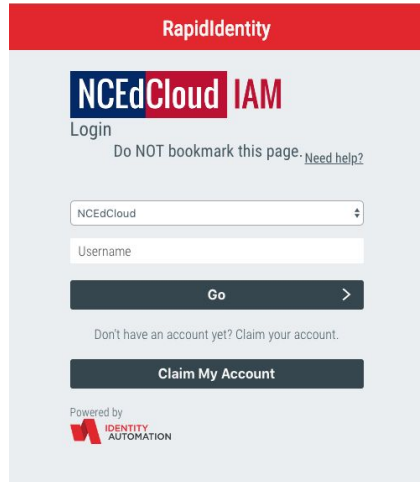
(Home page) <https://authy.com/>

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

Setting Up MFA One-Time Password

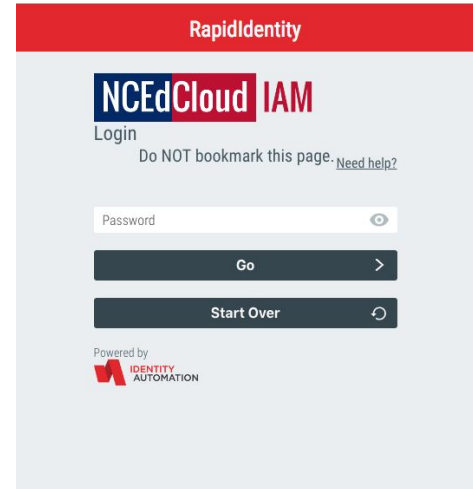
When MFA is activated for your LEA or Charter School on May 9th, you will need to set up a **One-Time Password (OTP)** the first time you login.

Access **my.ncedcloud.org**
and enter **Username**



The screenshot shows the login page for NCEdCloud IAM. At the top, there is a red header with the text "RapidIdentity". Below the header, the "NCEdCloud IAM" logo is displayed. Underneath the logo, the word "Login" is shown, followed by the instruction "Do NOT bookmark this page. [Need help?](#)". There are two input fields: the first is labeled "NCEdCloud" and contains a dropdown arrow; the second is labeled "Username". Below these fields is a dark grey button with the text "Go" and a right-pointing arrow. At the bottom of the form area, there is a link that says "Don't have an account yet? Claim your account." and a dark grey button with the text "Claim My Account". At the very bottom, it says "Powered by" followed by the "IDENTITY AUTOMATION" logo.

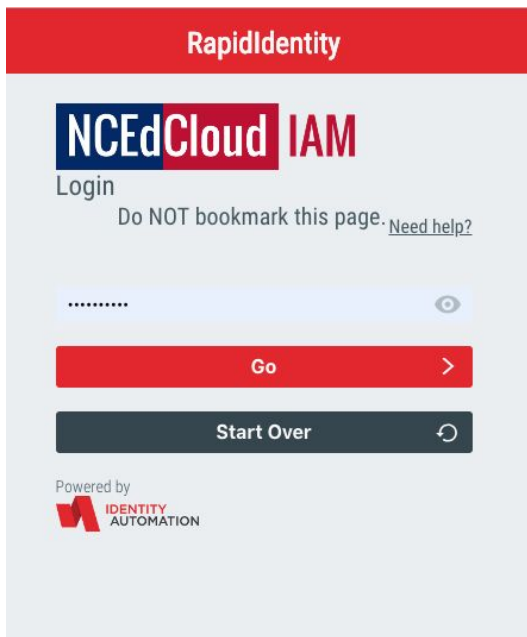
Enter **Password**



The screenshot shows the login page for NCEdCloud IAM, similar to the previous one but with the "Password" field filled in. The "Go" button is now disabled. Below the "Go" button is another dark grey button with the text "Start Over" and a circular refresh icon. At the bottom, it says "Powered by" followed by the "IDENTITY AUTOMATION" logo.

Setting Up a One-Time Password

Login (click “Go”)



RapidIdentity

NCEdCloud IAM

Login

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

.....

Go >

Start Over ↻

Powered by
IDENTITY
AUTOMATION

OTP Setup Screen

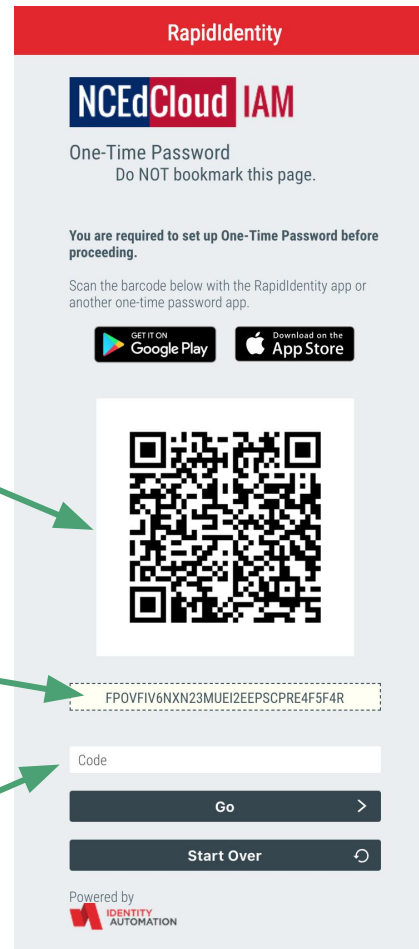
Scan **QR Code** using
Smartphone App

OR

Enter this **code** into
Authy

THEN

***Enter 6-digit Code**
Provided by app here



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.

GET IT ON Google Play

Download on the App Store



FPOVFIV6NKN23MUEI2EEPSCPRE4F5F4R

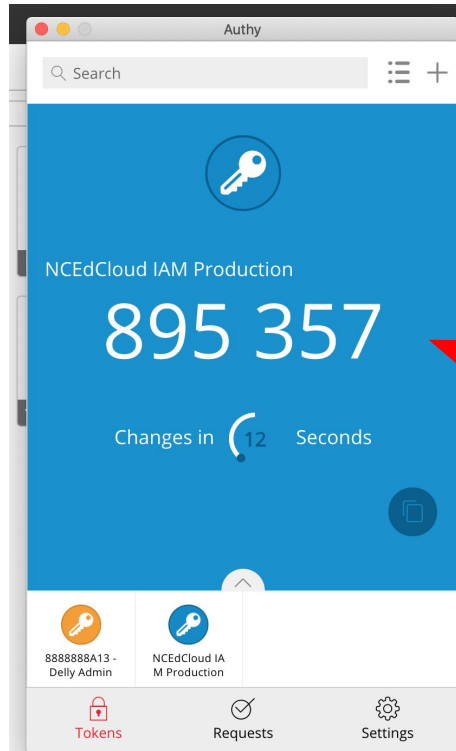
Code

Go >

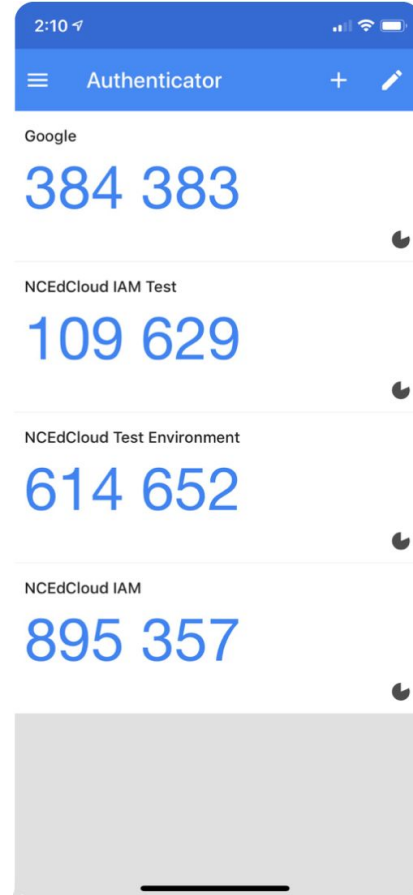
Start Over ↻

Powered by
IDENTITY
AUTOMATION

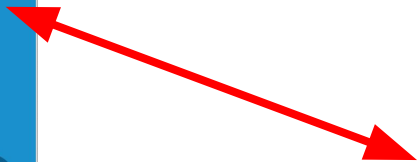
Authentication App View



Authy Desktop



Google Authenticator



Ongoing MFA Login

After your **One-Time Password** is set up for your account, you will be presented with a 3rd screen after you click “Go” on the password screen, every time you login to NCEdCloud:

Enter your 6-digit code
from your authentication
app

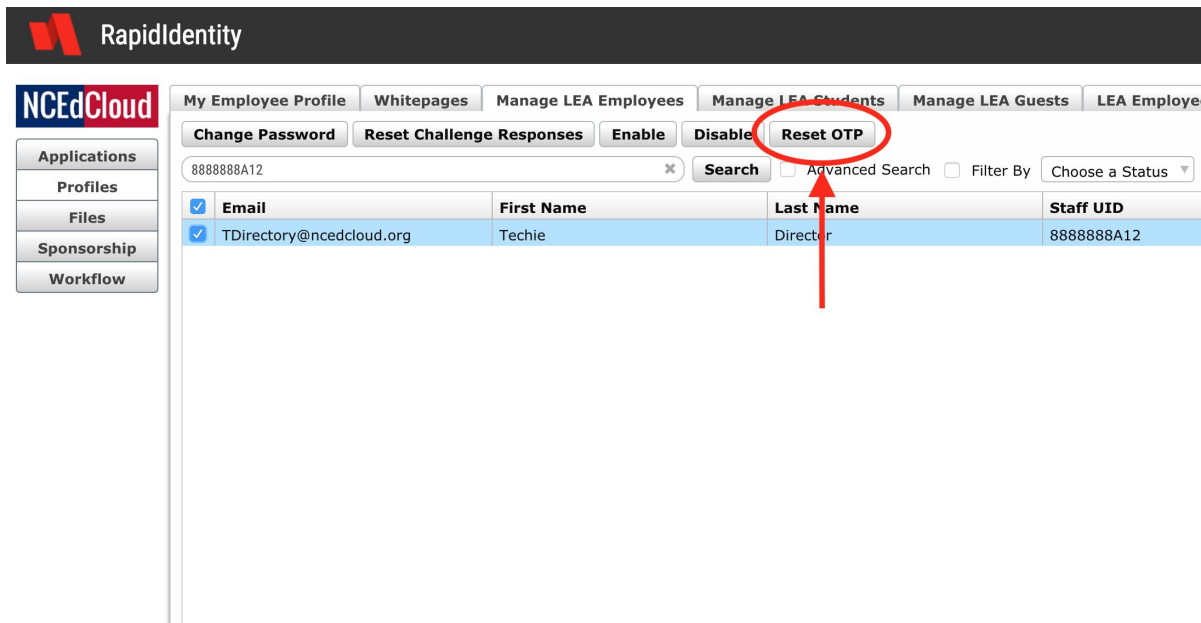
A screenshot of the NCEdCloud IAM One-Time Password login screen. The screen has a red header with 'RapidIdentity' in white. Below the header is the 'NCEdCloud IAM' logo, with 'NCEdCloud' in blue and 'IAM' in red. Underneath the logo, it says 'One-Time Password' and 'Do NOT bookmark this page.' There is a text input field labeled 'Code'. Below the input field are two buttons: 'Go' with a right arrow and 'Start Over' with a refresh icon. At the bottom, it says 'Powered by' followed by the 'IDENTITY AUTOMATION' logo.

New “Reset OTP” Button for LEA Administrators

Only LEA Administrators will have this functionality (e.g. user gets a new phone, deletes their app, etc.)

To reset a user’s OTP, enter their UID in the search field, click Search, and check the user checkbox. Then click on “**Reset OTP**”.

The user will then be presented with the One-Time Password setup screen at their next login.



The screenshot displays the RapidIdentity user management interface. At the top, the 'RapidIdentity' logo is visible. Below it, a navigation bar contains several tabs: 'My Employee Profile', 'Whitepages', 'Manage LEA Employees', 'Manage LEA Students', 'Manage LEA Guests', and 'LEA Employee'. The 'Manage LEA Employees' tab is active. On the left side, there is a sidebar menu with options: 'Applications', 'Profiles', 'Files', 'Sponsorship', and 'Workflow'. The main content area shows a search field with the UID '888888A12' and a 'Search' button. Below the search field, there are several action buttons: 'Change Password', 'Reset Challenge Responses', 'Enable', 'Disable', and 'Reset OTP'. The 'Reset OTP' button is circled in red, and a red arrow points to it from below. A table below the buttons lists user information:

	Email	First Name	Last Name	Staff UID
<input checked="" type="checkbox"/>	TDirectory@ncedcloud.org	Techie	Director	888888A12

MFA Resources on the NCEdCloud Website

NCEdCloud MFA Webpage:

Information, documents, links, etc. on the NCEdCloud MFA rollout webpage: <https://ncedcloud.mcnc.org/mfa>

How to Identify Users with Privileged Roles:

[Finding Users with Privileged Roles in NCEdCloud](#)

Instruction Guides for setting up Authentication Applications

[Setting up your OTP with Google Authenticator](#)

[Setting up your OTP with RapidIdentity](#)

[Setting up your OTP with Authy Desktop](#)

FAQs

Why is MFA being required for NCEdCloud?

MFA is being added as additional security to protect employee and student data files. Employees with LEA Administrator and LEA Data Auditor roles have access to these files.

Who will be required to use Multi-Factor Authentication (MFA) in NCEdCloud?

At this time, only employees with **LEA Administrator** or **LEA Data Auditor** privileged roles will be required to use MFA and enter a One-Time Password (OTP) with each login to NCEdCloud.

Will I be required to use my personal phone to obtain the 6-digit code to enter?

It depends. You have two options to obtain the 6-digit code required at login - an app that runs on a mobile device (phone or tablet), or a desktop version (Authy) that runs on your laptop.

FAQs (page 2)

Do I need to provide my mobile phone number to set up MFA?

It depends on the app. Both the Google Authenticator and RapidIdentity app that run on your mobile device use a time-based one-time password (TOTP) algorithm to provide a valid 6-digit code (it is not texted to your phone). However, Authy requires that you enter your cell number when installing and registering the app.

Will other roles be required to use MFA in the NCEdCloud in the future?

Yes. Eventually MFA will be implemented for all privileged roles in the NCEdCloud IAM Service, including LEA Help Desk and LEA Student Help Desk.

What devices is the Authy Desktop authenticator compatible with?

The Authy Desktop Authenticator is available for both Windows and macOS and there is a Chrome extension available to install it on Chromebooks. There is also a mobile app version available (like Google Authenticator and RapidIdentity), that runs on Android and iOS.

FAQs (page 3)

How often will I need to enter my OTP?

The short answer is once per day. You are required to enter your OTP (6-digit code) the first time you open a session (login) to the NCEdCloud IAM Service. If you completely shut down your browser during the day, or change devices, you will need to re-enter your OTP.

How long do I have to enter the 6-digit code from my app into the OTP screen?

Each 6-digit code generated by any of the authentication applications is good for 30 seconds from the time it is first displayed. Most apps have a timer that shows you how long you have until the code “expires”. If you only have a few seconds left, it is best to wait for a new code to be generated so you have time to enter it into the NCEdCloud OTP login screen.

Questions?

MFA Website: ncedcloud.mcnc.org/mfa

Email questions to: mscheible@mcnc.org