



agency for persons with disabilities
State of Florida

Information
Security
Management

ACCESS TO INTERNET-FACING APD SYSTEMS

Getting Started with Multi Factor Authentication

Abstract

Multi Factor Authentication (MFA) prevents breaches by requiring more than just a password to gain access to information systems. This guide instructs the system user on how to set up and use Multi Factor Authentication (MFA) to access APD information systems remotely.

Contents

Introduction.....	2
Multi Factor Authentication (MFA)	2
How does it work?	2
Setting up Access Using MFA	3
Step 1: Log in to the APD.Direct User Management portal.....	3
Step 2: Changing your Phone Call Authentication PIN	4
Step 3: Changing your Authentication Phone Numbers.....	5
Before setting your phone numbers	5
Questions and Answers	5
Step 4: Enrolling a Smart Phone	7
Using Multi Factor Authentication (MFA)	9
Logging in to a System	9
Mobile Authenticator	9
Text Message	9
Phone.....	9
WARNING	9
Resetting Your Password	10
How does it work?.....	10
Accessing APD Applications.....	11
APD.Direct User Management Portal.....	11
APD Applications Portal.....	12
Appendix A: Enabling Finger Print Recognition on your Smart Phone.....	13
On an iPhone®	13
On an Android™ phone	13

Introduction

Access to Internet-facing APD systems (such as iConnect) requires more rigorous authentication than access to a system that is not Internet-facing.

Without strong authentication controls, a single password is all that stands between confidential information and a data breach.

To address this risk, access to Internet-facing APD systems requires Multi Factor Authentication.

Multi Factor Authentication (MFA)

“Multi Factor Authentication” means more than one piece of evidence proves the person logging into a system is indeed the person he/she claims to be.

For example:

In a traditional computer system, a user name and password are all that are required for you to log in. The user name is who you *claim to be*, and the password is evidence your claim is true (since ideally, *only you* should know the password for your user account.) However, a password is only one piece of evidence that you are who you claim to be.

With Multi Factor Authentication (MFA), we require more than one piece of evidence. The first piece of evidence can be your password – it’s ***something you know***. The second piece of evidence will be ***something you have***. This can be many things (a fingerprint or a key, for example) but for remote access, it is common to use your telephone as evidence of ***something you have***.

How does it work?

When you log in to an Internet-facing APD system, you will be prompted for your password (as usual), and you will also be prompted to choose a second method of authentication. Depending on the phones you’ve set up to use with MFA, the choices for your second method of authentication may be:

- Receive an **SMS text message** with a One Time Passcode, (enter this code into the log in form.)
- Receive a **voice phone call**, (enter your PIN on the telephone keypad.)
- Use the **Mobile Authenticator App** on your smart phone. (See [Step 4: Enrolling a Smart Phone](#))

Once you’ve provided the second method of authentication, you will be logged in.

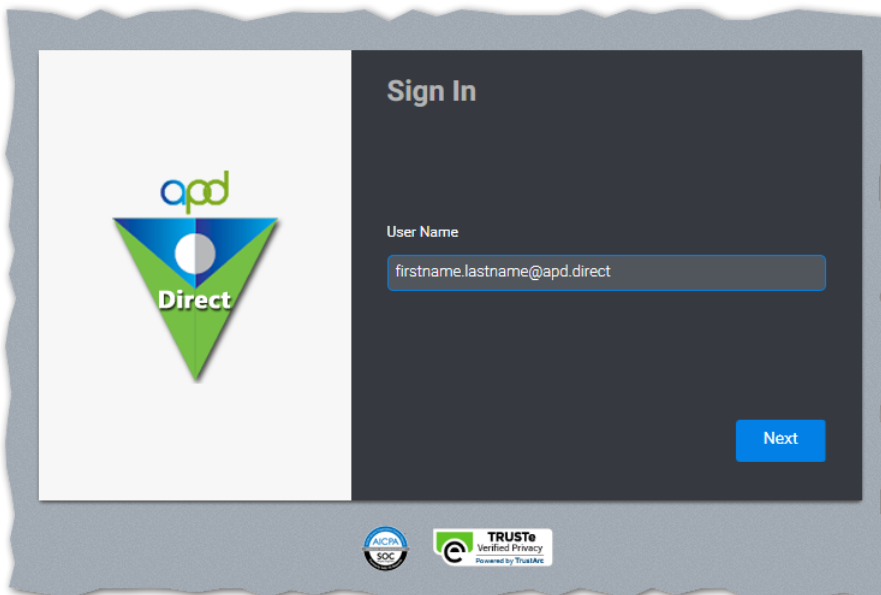
Setting up Access Using MFA


To ensure you have access to Internet-facing APD systems (such as iConnect), please follow the steps below and on the following pages to set up Multi Factor Authentication (MFA) for your user account.

Step 1: Log in to the APD.Direct User Management portal

Go to the **APD.Direct** user management portal at the following URL:

<https://apddirect.my.centriify.com>



Enter the **username** you were given by the **ID PASS** system and click **“Next”**, then enter the **password you chose** when you set up your user account on the **ID PASS** system. 

After inputting your **user name** and **password**, select your choice for a **second authentication factor**, and click **“Next”**.



You will receive a separate authentication request according to the option you choose (for example, by SMS text message or voice phone call.)



*(Note: You already registered at least one authentication phone number when you set up your user account on the **ID PASS** system.)*

Step 2: Changing your Phone Call Authentication PIN

If you would like to change your **phone call authentication PIN**, follow these directions:



(Note: You already set your phone PIN when you set up your user account on the ID PASS system.)

Click the **“Account”** tab, and then click the **“Set”** button next to the **“Phone PIN”** heading.

The screenshot shows the 'User Management Portal' interface. At the top, there's a navigation bar with 'Apps', 'Devices', 'Activity', and 'Account' tabs. The 'Account' tab is selected. Below the navigation bar, the user's profile 'Firstname Lastname' is shown. On the left, there's a 'Security' sidebar with 'Passcodes', 'Personal Profile', and 'Organization'. The main content area is 'Security Settings', which includes 'Password' and 'Phone PIN' sections. The 'Phone PIN' section shows it was 'Configured successfully. February 1, 2018' and has an 'Edit' button. Two red callouts with numbers 1 and 2 point to the 'Account' tab and the 'Edit' button respectively.

Enter a **PIN** in the boxes, then click **“Save”** when finished.

The screenshot shows a 'Phone PIN' dialog box. It has a title 'Phone PIN' and a subtitle 'Set a PIN for Phone Call authentication.' Below this, there are two rows of input boxes. The first row is labeled 'New PIN' and has four boxes. The second row is labeled 'Optional (more secure)' and has four boxes. A red callout with number 1 points to the input boxes. A red callout with number 2 points to the 'Save' button. A note box on the right says 'Note: You may enter up to 8 digits'.

Step 3: Changing your Authentication Phone Numbers

If you would like to change your **authentication phone numbers**, follow these directions:



Note: *You already registered at least one authentication phone number when you set up your user account on the ID PASS system.*

Before setting your phone numbers, you'll want to know the following:

- You can enter up to 3 phone numbers:
 - “Office Number”
 - “Mobile Number”
 - “Home Number”
- **Only** the “Mobile number” can receive **SMS text message** One-Time Passcodes.
- **Any** number can go into any field.

For example: You could put your mobile phone in the “Home Number” field – it just wouldn’t be able to receive SMS text message One-Time Passcodes.
- All 3 phone numbers can receive voice phone call authentication.
- At least 2 phone numbers, or 1 smart phone using the Mobile Authenticator App, will be required to receive a password reset. (See [Step 4: Enrolling a Smart Phone](#))

This table shows which numbers can be used for which types of authentication:

	SMS Text Messages	Phone Calls
Office Number	✗	✓
Mobile Number	✓	✓
Home Number	✗	✓


Questions and Answers that will help you decide which phone numbers to use:

My mobile phone doesn’t receive SMS text messages. Will I still be able to use it to authenticate?

- **Yes.** If you have a mobile phone that doesn’t receive SMS text messages, you can still receive a voice phone call for authentication, or if it’s a smart phone, you can use the **Mobile Authenticator App**. The choice is yours.

I don’t want my mobile phone to receive SMS text messages. How do I prevent this?

- **You have 2 choices** if you don’t want your mobile phone to receive SMS text messages for authentication:
 - 1) When a login page asks you which method of authentication you’d like to use, simply select “Phone” or “**Mobile Authenticator**” instead of “Text Message”.

 **(Note:** *Using the “Mobile Authenticator” option requires that you’ve enrolled your phone to use the Mobile Authenticator App – see [Step 4: Enrolling a Smart Phone](#))*
 - 2) You can enter your mobile phone number into one of the other two fields (“Office” or “Home”). This way, your mobile phone won’t receive SMS text messages.

3) Which phone numbers should I use if I want to get my password reset when I forget it?

- Password resets require two factors of authentication. There are 2 options to accomplish this:
 - 1) You need to have **2 phone numbers** registered so you can receive 2 authentication phone calls. *(SMS text messages aren't allowed for password resets.)*
 - 2) On a smart phone, you can use the **Mobile Authenticator App** for one factor of authentication, and an **authentication phone call** to the same smart phone for the second factor.



(Note: Using the "Mobile Authenticator" option requires that you've enrolled your phone to use the Mobile Authenticator App – see [Step 4: Enrolling a Smart Phone](#))

Once you've decided which phone numbers to use, enter them into the User Management portal:

From the "**Account**" tab, click on the "**Personal Profile**" link on the left side of the page, then click the "**Edit**" button and enter your phone numbers. Click "**Save**" when done.

The screenshot shows the 'User Management Portal' interface. At the top, there's a navigation bar with 'Apps', 'Devices', 'Activity', and 'Account' (circled in red). Below this is a header with a user profile icon and 'Firstname Lastname'. On the left, a sidebar lists 'Security', 'Passcodes', 'Personal Profile' (highlighted with a red arrow and a callout box labeled '1'), and 'Organization'. The main content area shows an 'Edit' button (with a callout box labeled '2') and several input fields: 'First Name' (with 'Firstname'), 'Last Name' (with 'Lastname'), 'Display Name' (with 'Firstname Lastname'), 'Email Address' (with 'firstname.lastname@example.com'), 'Office Number' (with '123-456-789'), 'Mobile Number' (with '123-555-1234'), and 'Home Number' (with '123-555-4321'). A callout box labeled '3' points to these three number fields with the text 'Enter your phone numbers'. At the bottom, there are 'Save' and 'Cancel' buttons, with a callout box labeled '4' pointing to the 'Save' button and the text 'Click "Save" to finish'.

Step 4: Enrolling a Smart Phone

You may enroll your personal smart phone if you want to use the **Mobile Authenticator App**.

*(Hint: A smart phone can use the **Mobile Authenticator App** even when it's **phone number** is **not entered** in your **Personal Profile**.)*



You must enable finger print recognition on the smart phone to use the Mobile Authenticator App.

For help enabling finger print recognition, see [Appendix A: Enabling Finger Print Recognition on your Smart Phone](#).

First, download and **install the Mobile Authenticator App** on your smart phone.

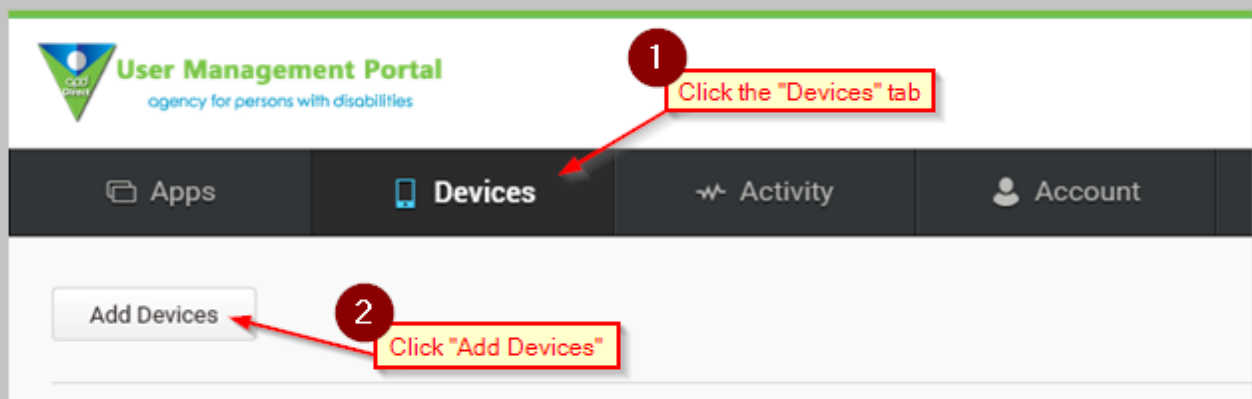
- **Apple App Store®:**
<https://itunes.apple.com/us/app/centrify-mobile-manager/id499910663>
- **Google Play™ store:**
<https://play.google.com/store/apps/details?id=com.centrify.mdm.samsung>



Alternatively, you can simply search for **Centrify®** in the app repository.

(See the picture above-right for an example of the app icon.)

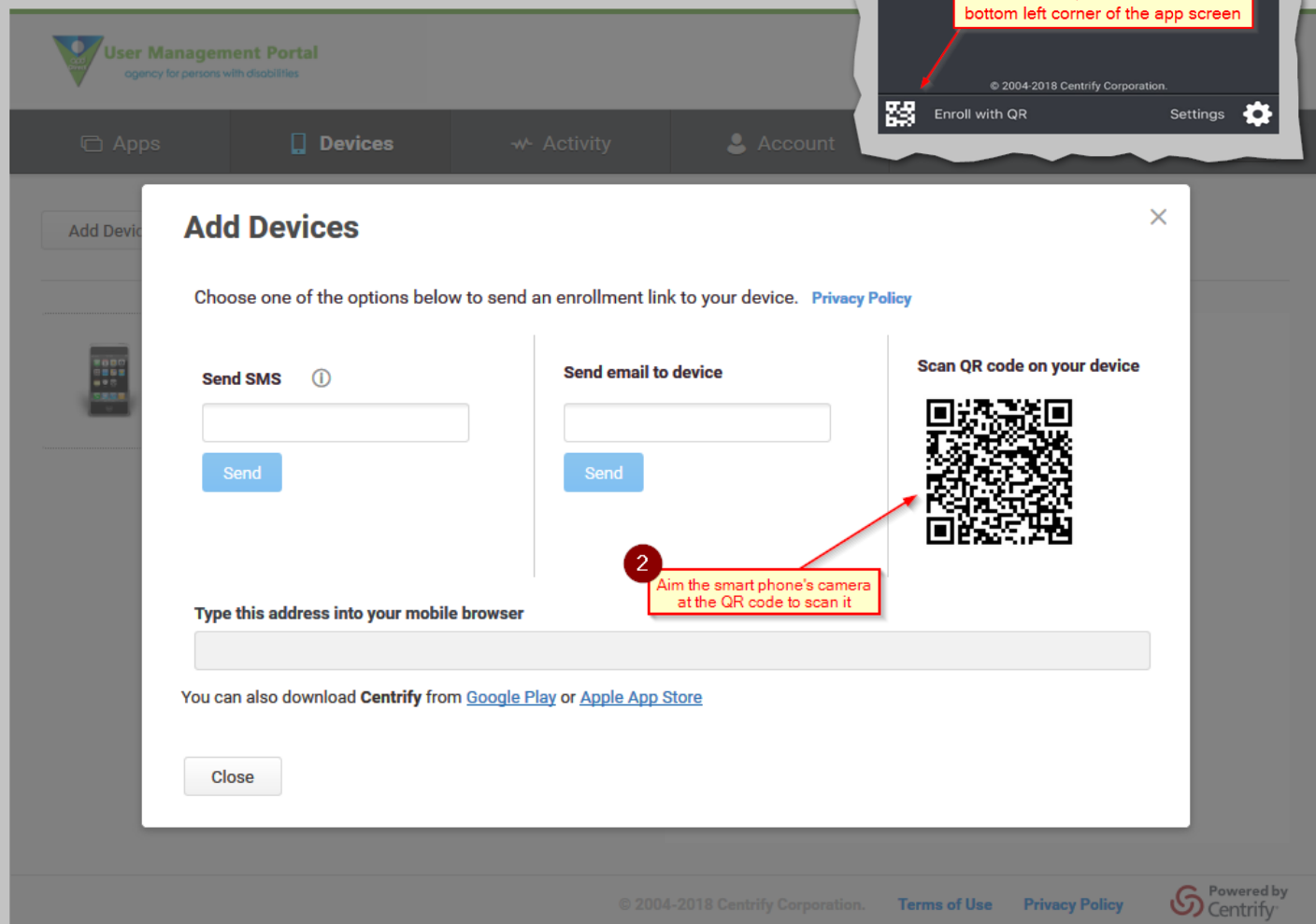
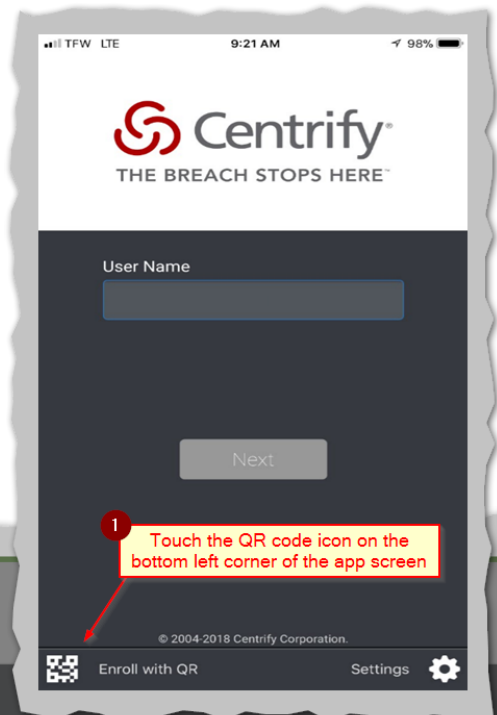
After installing the **Mobile Authenticator App**, return to the **User Management portal**, click the **"Devices"** tab, and then click the **"Add Devices"** button on the left side of the page.



Open the **Mobile Authenticator App** and touch the **QR code** icon on the bottom left corner of the app screen.

Aim the smart phone's camera at the **QR code** on the **User Management portal**.

Your smart phone will automatically begin the enrollment process. Simply follow the instructions the app provides.



Using Multi Factor Authentication (MFA)

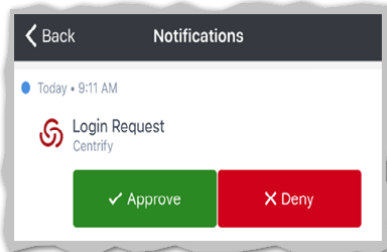
Logging in to a System

After inputting your **user name** and **password** as you normally do, you will be asked to select your choice for a **second authentication factor**.

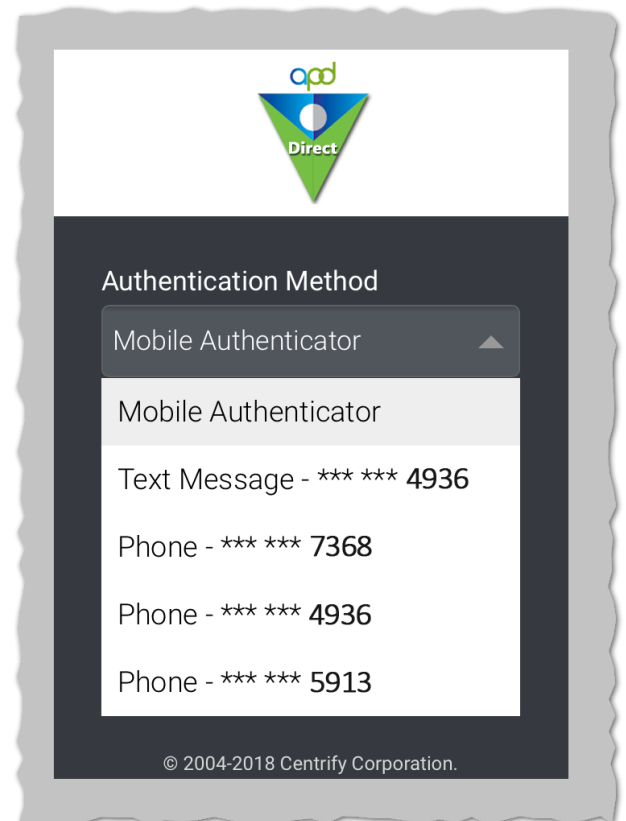
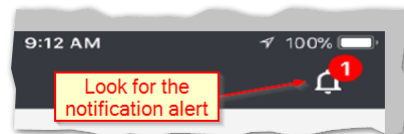
Depending on which phone numbers you've registered and whether you've enrolled a device to use the **Mobile Authenticator App**, the choices may be any of the following:

Mobile Authenticator

- You will receive a **Login Request** through the **Mobile Authenticator App** (on the device you've enrolled). Simply follow the instructions and touch "**Approve**" on the **Login Request** under the **Notifications** screen to complete your login.

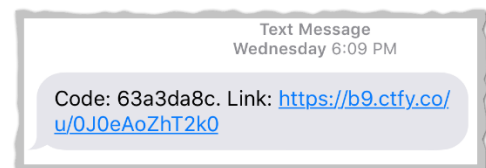


(Note: If you do not see the Login Request, check the upper right corner of the app for an alert.)



Text Message

- You will receive an SMS text message containing a **Code** and a **Link**. You can either enter the **Code** on the system's login form, or you can simply touch the **Link** to open your smart phone's web browser and approve the **Login Request** from there.



Phone

- You will receive an authentication **Phone Call**. When the voice prompts you, simply use the phone key pad to enter the PIN you previously set in the **Access Control portal**, and then press the **#** key. (See [Step 2: Set your Phone PIN](#) under the [Setting up Remote Access Using MFA](#) section.)

WARNING: If you receive an **authentication request** when you are **not logging in** to an APD system, it means someone has your password and is attempting to log in as you. **DENY** the request and **report this** to **APD Information Security** immediately at: security@apdcares.org



Resetting Your Password

Password resets are a big deal. The person who receives the password reset takes control of the user access account – *whether that person is the legitimate owner of the user account or not.*

The following rules prevent unauthorized takeover of a user access account through a password reset:

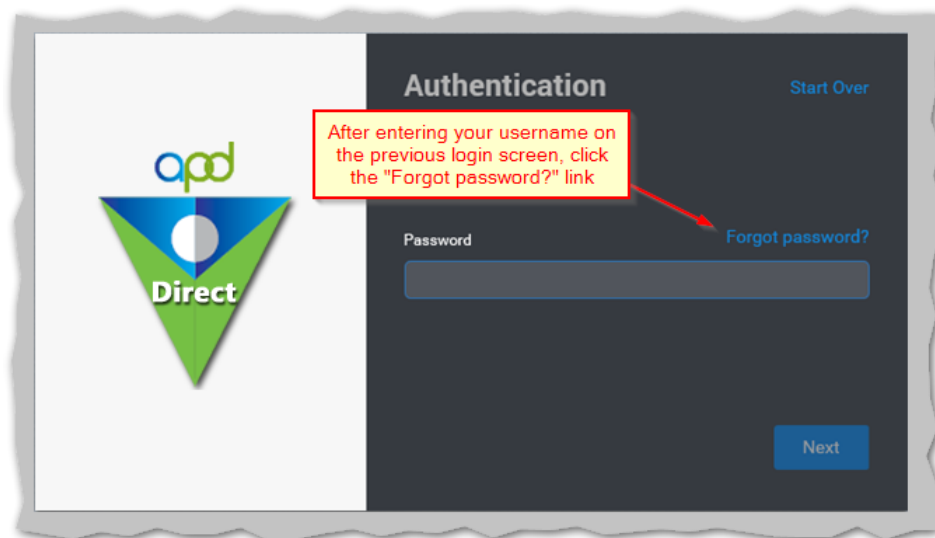
- 2 authentication factors are required
- SMS text messages are not allowed

This means you have **2** choices for password reset authentication:

- Enter your **PIN** in **2** separate voice authentication **Phone Calls**
- Use the **Mobile Authenticator App** (*using your fingerprint*) for one authentication factor, and enter your **PIN** in a voice authentication **Phone Call** for the second factor

How does it work?

On the **APD Access Control portal** login screen, first **enter you user name**, and then you will see a **"Forgot password?"** link. Click this link to begin the process.



You will be asked **two times** to choose an authentication method (**Phone** or **Mobile Authenticator**). Simply choose how you want to authenticate, and then follow the instructions. You will do this **twice**, and then you will be presented a form to choose a new password.

Accessing APD Applications

APD.Direct User Management Portal

Log in to the **APD.Direct** user management portal at the following URL:

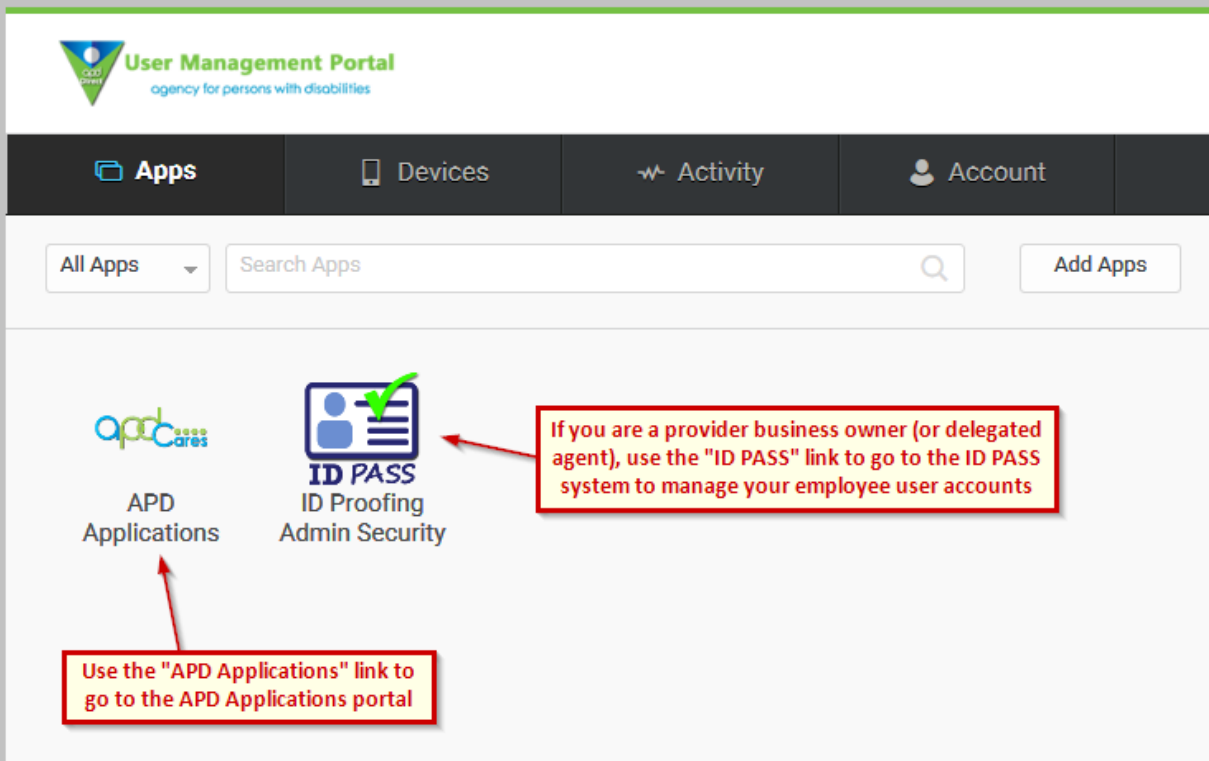
<https://apddirect.my.centrify.com>

You will land on the default “**Apps**” page.

Clicking on the “**APD Applications**” icon will open the **APD Applications Portal** in a new window. You **will not have to log in** a second time.

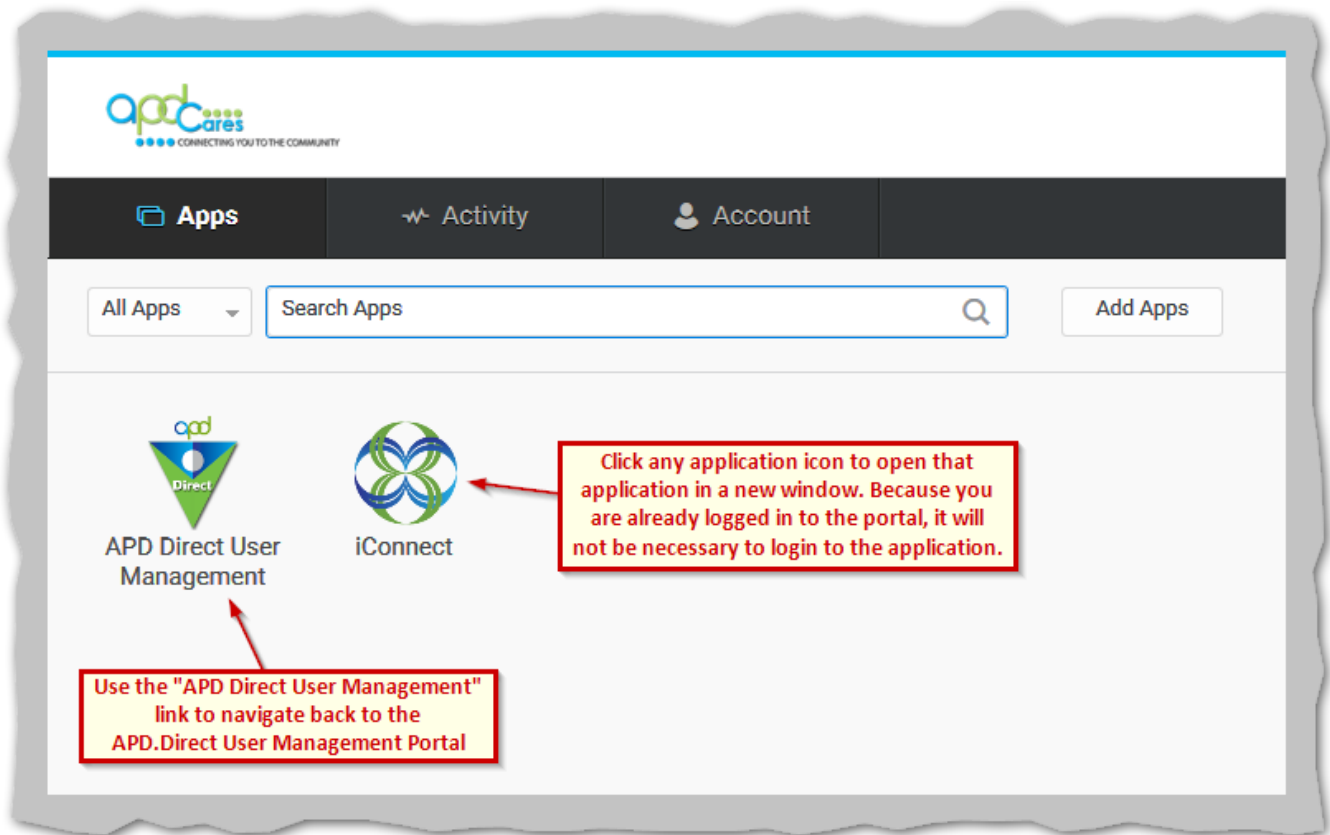


*(Note: If you are a provider business owner (or a delegated agent), you will also see an **ID PASS** icon. Clicking on this icon will open the **ID PASS** system in a new window, where you can manage your employee user accounts. You **will not have to log in** a second time.)*



APD Applications Portal

Inside the **APD Applications Portal**, you will see icons for any applications you are authorized to access. Clicking any of these icons will open the application in a new window. Because **you are already logged in** to the portal, you will **not have to log in** again.



Appendix A: Enabling Finger Print Recognition on your Smart Phone

On an iPhone®

Go to **Settings** > **Touch ID & Passcode**

- Turn on the **iPhone® unlock** switch under the **USE TOUCH ID FOR** heading.
- If you don't have any fingerprints enrolled on your device, touch "**Add a Fingerprint...**" under the **FINGERPRINTS** heading, and then follow the instructions to set at least one fingerprint on your device.
- More information can be found here:

<https://support.apple.com/en-us/HT201371>

On an Android™ phone

Android™ devices vary by manufacturer and model. Because of this, there is no single set of instructions that applies to a particular device.

Generally, you will look in **Settings** > **Security**, or some other similar place, and find the **Fingerprints** setting. For your specific device, you should be able to find instructions through an Internet search.