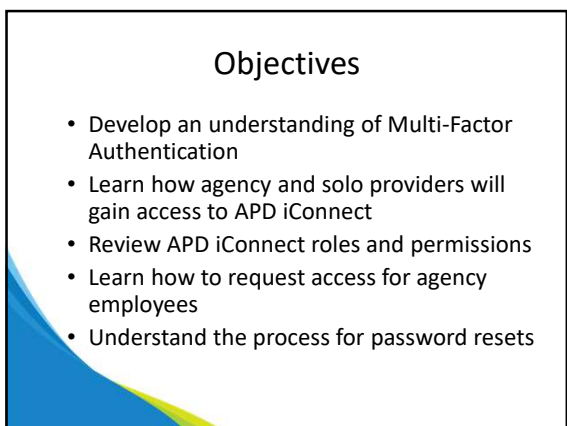
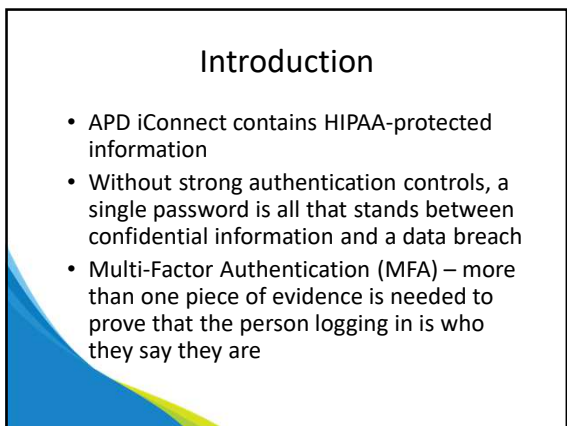


1



2



3

Example

- In a traditional computer system, you only need a username and password to log in.
 - The username is who you *claim* to be
 - The password is evidence your claim is true since ideally *only you* should know your password
- However, a password is only one piece of evidence that you are who you claim to be

4

Example

- With MFA, APD requires 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**
 - Will be your cell phone and/or your landline phone
 - Receive **SMS text message** with 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 smartphone
- Once you provide the second piece of evidence, you will be logged in

5


Agency Owners/Solo Provider Set-Up

- Agency owners and solo providers will be required to provide certain information for identity-proofing
 - First and last name
 - Residential address
 - DOB
 - **Unique** email address
 - Telephone number

6

Agency Owners/Solo Provider Set-Up


- This information will not be shared
- It is used with APD's third-party partner for the sole purpose of identity verification before creating an account with ID Proofing Admin Security (ID PASS)
- An ID PASS account is required for all agency and solo providers



7

Agency Owners/Solo Provider Set-Up


- Each provider will be emailed instructions for how to complete the identity-proofing process
- *NOTE: Agency and solo providers are encouraged to monitor the provider advisories posted on <https://apd.myflorida.com/providers/advisories.htm>*
- Emails for set-up may go to spam or blocked folders



8

Agency Owners/Solo Provider Set-Up


- Look for an email from "APD Online Applications User Account Service"
– no.reply@apdcares.org
- The link in the email **will have an expiration date**
- Follow the instructions in the email to create your APD iConnect account
- If you do not receive an email, call the APD iConnect Support Desk at 1-800-353-5168



9

Configuring MFA Access


- Once completed, agency owners and solo providers will be provided with a username by ID PASS
- Users will be able to choose their own password during the ID PASS registration process



10

Configuring MFA Access

- Access the APD.Direct user management portal at <https://apddirect.my.centify.com>
- Enter the username given by ID PASS and click **“Next”**
- Then, enter the password chosen when setting up the user account on the ID PASS system




11

Configuring MFA Access




The screenshot shows the APD Direct logo on the left and a 'Sign In' form on the right. The form has a 'User Name' label and a text input field containing the placeholder 'firstname.lastname@apd.direct'. A blue 'Next' button is located at the bottom right of the form.



12


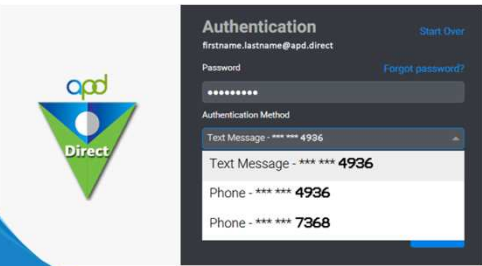
Configuring MFA Access

- After entering the username and password, select your choice for **second authentication factor** and click **“Next”**
- You will receive a separate authentication request according to the option you choose
- *NOTE: You already registered at least one phone number when you completed the ID PASS registration.*



13


Configuring MFA Access



14

Enrolling a Smartphone



- Users can enroll their personal smartphone if they want to use the **Mobile Authenticator App**
- A smartphone can use the Mobile Authenticator App *even when the phone number is not entered* in the user’s personal profile in the ID PASS system
- **Fingerprint or face recognition must be enabled on the smartphone in order to use the Mobile Authenticator App**



15

Enrolling a Smart Phone


- Download and install the Idaptive Mobile Authenticator app
Apple App Store:
<https://apps.apple.com/us/app/idaptive/id499910663>
Google Play Store:
<https://play.google.com/store/apps/details?id=com.centrifymdm.samsung>



16



Enrolling a Smartphone

- After installing the **Idaptive App**, return to the **User Management portal** and click the **“Devices”** tab
- Click the **“Add Devices”** button on the left side of the page



17

Enrolling a Smartphone



18

Enrolling a Smartphone

- Open the **Idaptive App** and touch the **QR code** icon on the bottom left corner of the app screen
- Aim the smartphone's camera at the **QR code** on the User Management portal
- Your smartphone will automatically begin the enrollment process
- Follow the instructions the app provides



19


Enrolling a Smartphone



20

Logging In to APD iConnect


- Always start by accessing the APD.Direct user management portal at <https://apddirect.my.centify.com>
- After entering your username and password, you will be asked to choose a **second authentication factor**



21

Logging in to APD iConnect


- The phone numbers you've registered and whether you've enrolled a device to use the Idaptive App determines which choices you may see



22

Logging in to APD iConnect


- Mobile Authenticator
 - You will receive a login request through the **Idaptive App**
 - Follow the login instructions and touch **"Approve"** on the **Login Request** under the **Notifications** screen



23

Logging in to APD iConnect

- Text Message
 - You will receive an SMS text message containing a **code** and a **link**
 - Either:
 - Enter the **code** on the system's login form OR
 - Simply touch the link to open your smartphone's web browser and approve the **Login Request** from there




24

Logging in to APD iConnect

- Phone
 - You will receive an authentication phone call
 - When prompted, use the phone keypad to enter the PIN you previously set up


WARNING: If you receive an authentication request when you are *not* logging in to an APD system, it may mean 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



25

Logging in to APD iConnect

- Once you have completed MFA, you will be directed to the User Management Portal
- The APD Applications icon will take you to APD iConnect
- The ID PASS icon will allow agency owners to use the ID PASS system to manage employee user accounts



26


Logging in to APD iConnect



27

APD iConnect Roles and Permissions



- Since APD iConnect is a statewide database of consumer and provider information, there are security measures to limit a user's access
- When ID PASS registration is completed, based on a person's job, a role or multiple roles are assigned
- Roles have specific permissions for what that user can see



28

APD iConnect Roles and Permissions


- Providers will have access to a maximum of five roles



29

APD iConnect Roles and Permissions

- Service Provider Role
 - Needed by all agency owners and solo providers
 - Grants access to your agency provider record
 - Should be limited to only you and designated staff (authorized in writing to act on your behalf)



30

APD iConnect Roles and Permissions

- Service Provider Role
 - Gives access to view and can make changes to all portions of your provider record and your claims
 - Can see all authorizations
 - Can see other employee information
 - Can change addresses
 - Can communicate with your provider enrollment specialist/liaison
 - Can see any POR/Corrective Actions
 - Can see Qlarant reviews (in the future)

31

APD iConnect Roles and Permissions

Basic Information	
Provider Name	Example Provider
Residential Monitor	
OSA (if applicable) Facility Name	Licensing Specialist
Licensed Name Licensed for capacity	Area Behavior Analyst
Active	Yes
External	Yes
Exclude from Selection	No
QA Workstream Worker	Medical Provider ID 12345678
	Provider EIN 98-123456789

32


APD iConnect Roles and Permissions

- Service Provider Admin – QA Role
 - Gives access to some portions of your provider record
 - Designed for the admin support person who may assist with agency management
 - Some access is view-only
 - Some access is add/edit access
 - Can edit your provider demographic information
 - Can complete forms
 - Can add notes
 - Can assign supervisors for employees
 - Can submit and view claims

33

APD iConnect Roles and Permissions


- **Service Provider Worker Role**
 - Cannot see your agency record at all
 - Has access to consumer records for whom you have an authorization
 - Access is limited to information needed to deliver authorized services and add documentation
 - Can add notes for the WSC to see
 - Cannot access agency authorizations or claims
 - Is needed for all EVV Workers



34

APD iConnect Roles and Permissions


- **Provider EVV Manager Role**
 - Limited access to your agency
 - Can see authorizations
 - Has access to EVV scheduling
 - Can review EVV activities and submit EVV claims
 - Has access to consumer records for whom you have an authorization
 - Can see and submit claims



35

APD iConnect Roles and Permissions

- **Billing Agent**
 - Designed for those who's sole purpose is to submit claims on your behalf
 - Can be a 3rd party or an employee
 - Very limited access to your agency
 - Can see provider demographics
 - Has access Notes to communicate with you
 - Has no access to consumer records
 - Can see and submit claims



36

Managing Agency Provider Employees

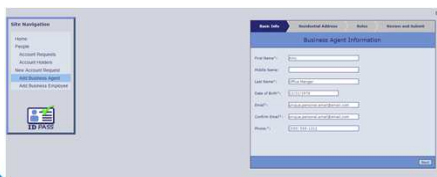
- With ID PASS, agency owners are able to request access for their employees
- The access request will also include defining what roles they will need
- The access request also includes specifying whether the person will need access to the APD iConnect application, the EVV mobile site, or both



37

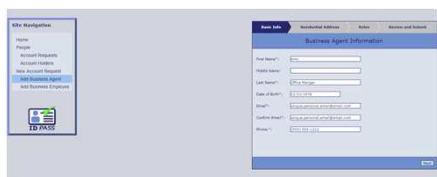
Managing Agency Provider Employees

- Once logged into ID PASS, use the menu to request new accounts



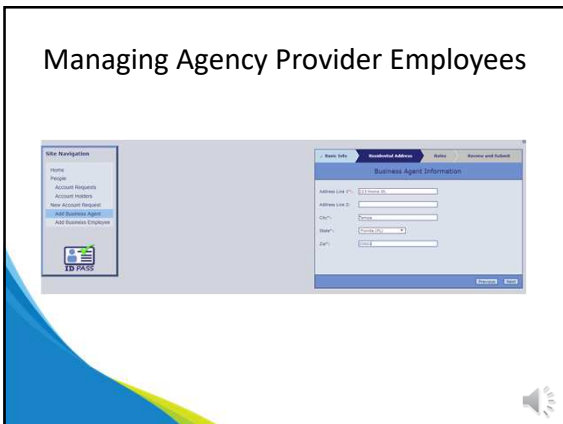
38

Managing Agency Provider Employees



39

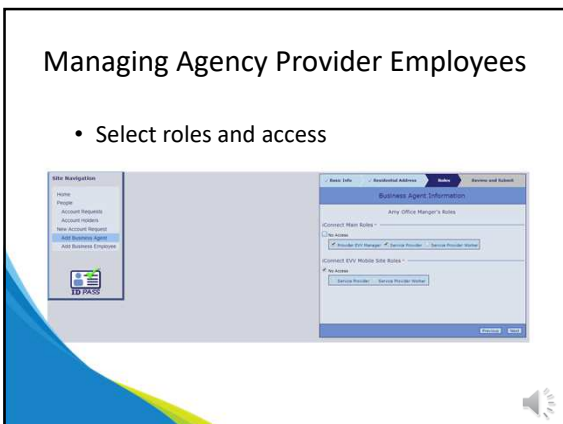
Managing Agency Provider Employees



40

Managing Agency Provider Employees

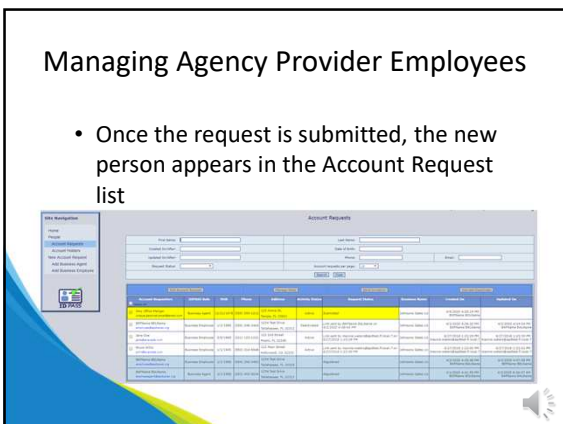
- Select roles and access



41

Managing Agency Provider Employees

- Once the request is submitted, the new person appears in the Account Request list



42

Password Resets


- Password resets are a serious matter, since the person who receives the password reset takes control of the user account access
 - *Whether the person is the legitimate owner of the user account or not*



43

Password Resets


- Rules are in place to prevent unauthorized takeover of user access account
 - Two authentication factors are required
 - SMS text messages are **not allowed**



44

Password Resets


- Two choices for password reset authentication
 - Enter your PIN in two separate voice authentication phone calls
 - Two separate phone numbers
 - Combination of mobile authenticator app and phone call
 1. Adaptive authenticator app (using fingerprint or face recognition)
 2. Enter your PIN in a voice authentication phone call



45


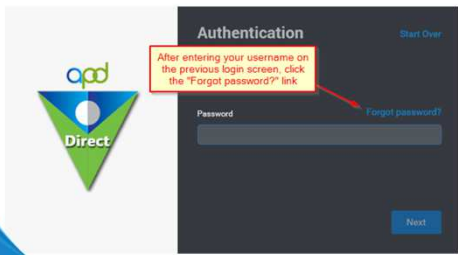
Password Resets

- On the APD Access Control portal login screen, enter your username and click next.
- You will see the “Forgot password?” link
- Click to begin the process



46


Password Resets



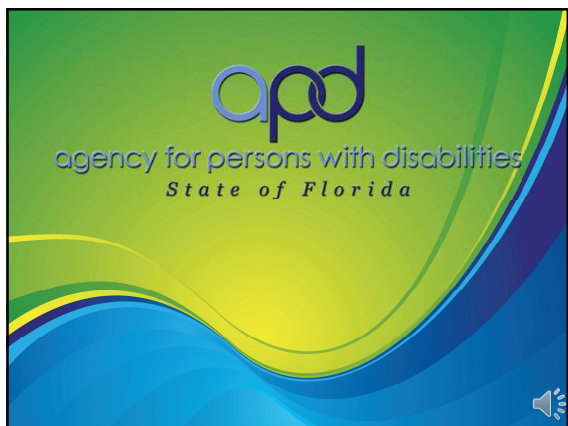
47

Password Resets

- You will be asked two times to choose an authentication method
 - Phone OR Mobile Authenticator
- Choose your authentication method and then follow the instructions
- **You will do this twice before you are prompted to choose a new password**



48



49
