# Onboarding Series

## Session IV: Security Profiles & Access Management

June 6, 2024

# Overview

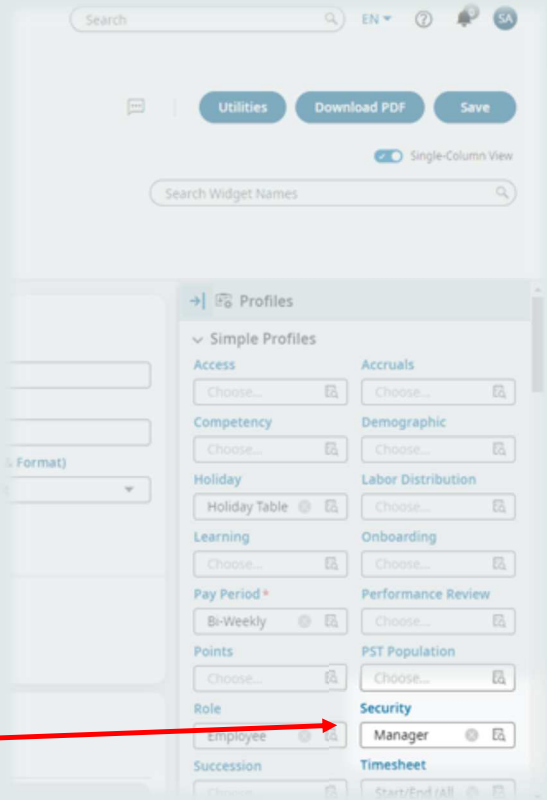
+ Security Profiles and Group Access
+ Manager Group Access vs. listing an employee as a manager
+ Security Profile Overview
+ Authentication policies
+ Troubleshooting Access

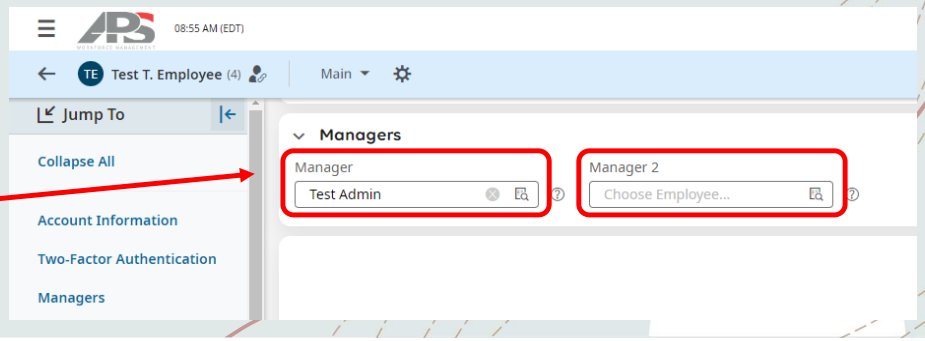
# Terms and Phrases

- **Manager** – refers to when a user is assigned under the managers widget on an employee's profile
- **Manger Group Access** – refers to the specific report page that shows the groups that a user has permissions for
- **Group Access** – general term to refer to who a user can see
- **Security Access** – general term to refer to what a user can see
- **Permissions** – general term for who and what a user can see; their total combined access in the system

# General Information

- When an employee is onboarded, they will always default to having access to their information only.
- Increasing someone's access has two parts: the security profile and the group access. Group access can be given in one of two ways: *manager group access* or *assigning the individual as a manager* over specific employees.
- The security profile is assigned on an employee's profile under the Simple Profiles section > Security.
- Manager Group Access is assigned by APS.
- You can assign someone as a manager over an employee(s) by going to the employee's profile to the Managers widget, then adding the new manager into one of the manager slots.



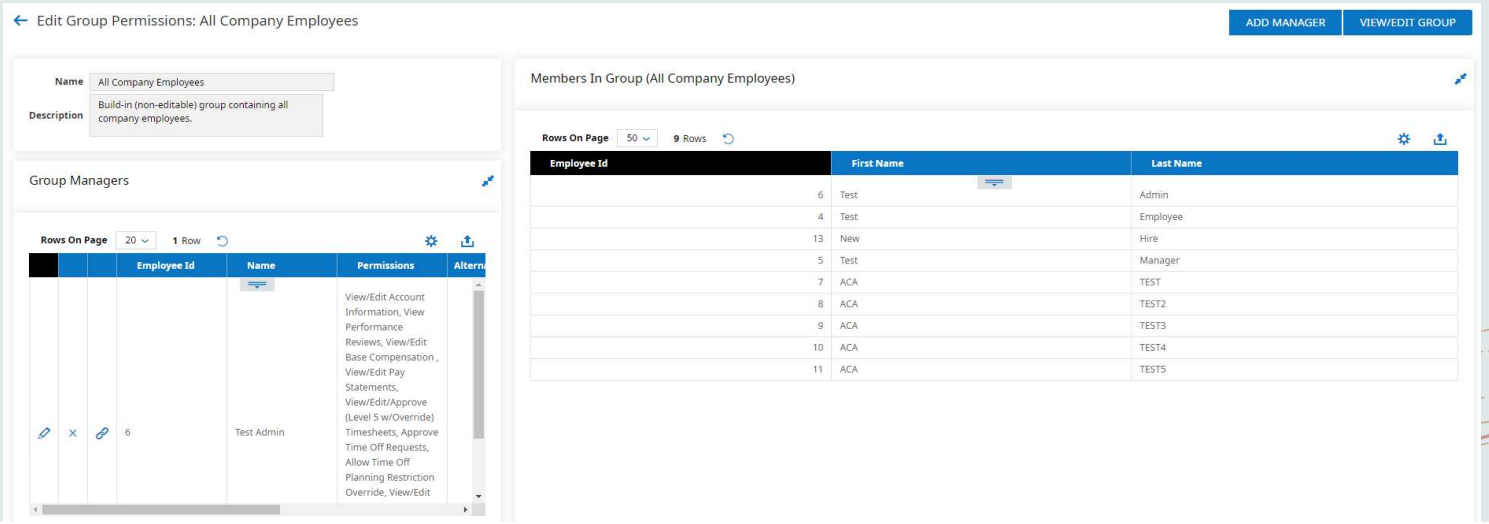



# General Information (continued)

- What is the difference between the security profile, manager group access, and assigning someone as a manager over employees?
  - **Security Profile: (generally) determines WHAT a user has access to**
    - Access is further specified for VIEW, VIEW/EDIT, VIEW/EDIT/ADD, VIEW/EDIT/ADD/DELETE, and/or VIEW/EDIT/APPROVE (for time)
  - **Group Access: (generally) determines WHO a user has access to (both Manager Group Access & assigning a user as a manager over an employee(s))**
    - Manager Group Access is further specified for VIEW, VIEW/EDIT, and/or VIEW/EDIT/APPROVE - this can be different for each person that is setup with access over a specific group.
    - Permissions for each manager slot are configured by APS on the global level for the company; each manager slot has its own permissions. Every user assigned in that slot will have the same permissions. (You cannot give access to person [a] in the Manager 1 slot but give different permissions to person [b] in the same Manager 1 slot. Both persons will have the same permission).
- When an employee is terminated or re-hired, their access remains the same unless changed by the user who is terminating the employee.
  - For example, if you terminate a manager and re-hire them as an employee, they will have the same manager permissions they had prior to leaving.
  - The system will give you a warning message when terminating an account if that person had security and/or group access to other information besides their own, but you must remove group access and change the security profile when terminating if you do not want them to have increased access as a terminated account.

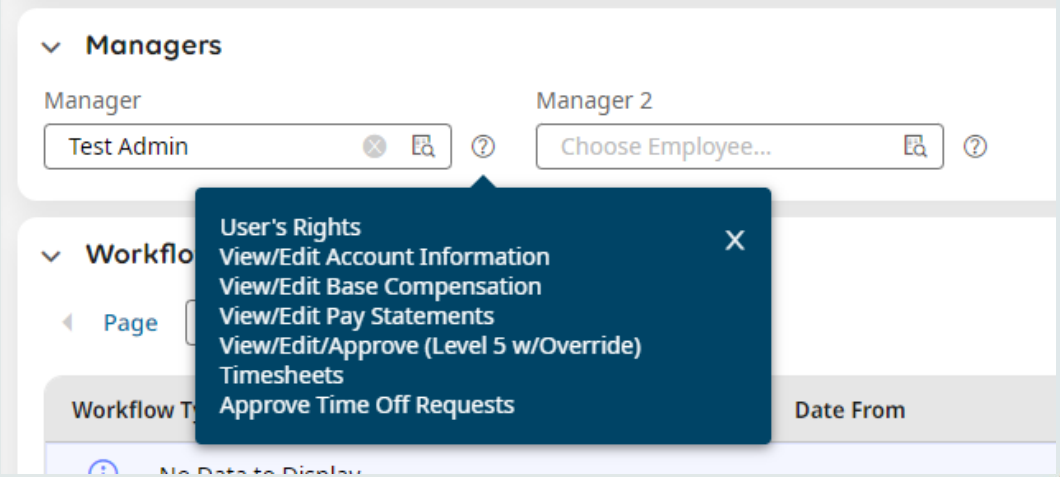
# How to tell what someone has access to

- In a Group: Menu > Settings > Global Setup > Groups > Manager Group Access
  - Use the filters to search for the user that you want to see the permissions for
  - Click the people icon to see the permissions for that specific group
  - The left will show you the managers in the group and what they are allowed to see
  - The right will show you the employees assigned to the group that the managers can see
- Each user can have different permissions for the groups they have been given access to
  - Groups can be used so that a user can have access to view/edit permissions for one set of employees while having separate access for another



# How to tell what someone has access to (continued)

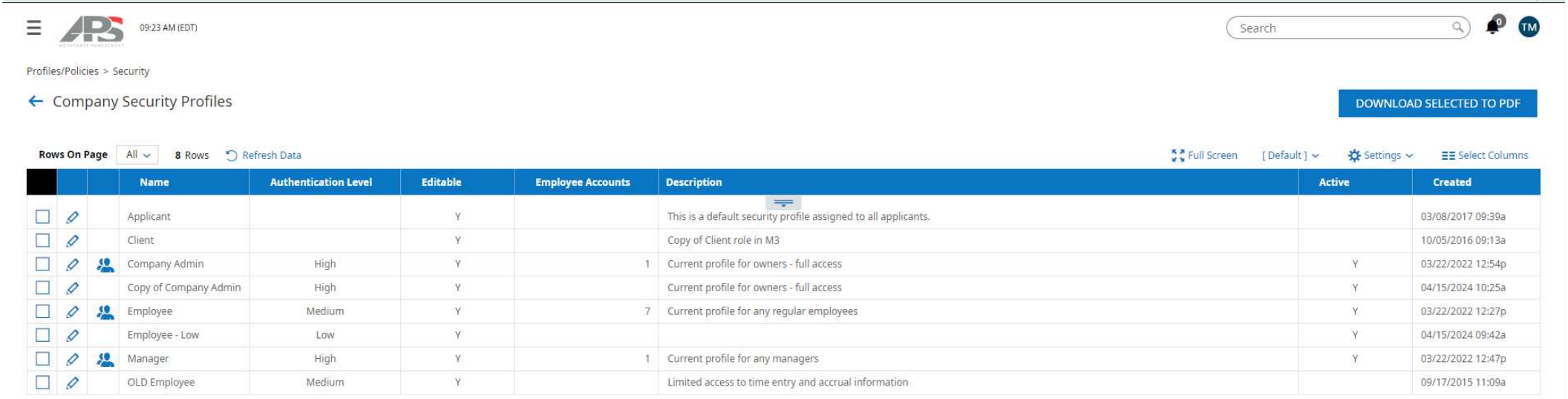
- Go to the manager widget on an employee's profile and hover over the question mark to the right of the manager field to
- This field will have the same permissions regardless of who is assigned to this field
  - Permissions for this field are set up in the Company Setup



For the most part, security profiles are what a user can see, and groups are who a user can see.

# Security Profiles

- The security profile determines what a user can do within the system
- Menu > Settings Tab > Profiles/Policies > Security
  - Can also navigate by clicking the blue "Security" hyperlink on the profiles section on an employee's profile




| Name | Authentication Level | Editable | Employee Accounts | Description | Active | Created |
|---|---|---|---|---|---|---|
| Applicant | | Y | | This is a default security profile assigned to all applicants. | | 03/08/2017 09:39a |
| Client | | Y | | Copy of Client role in M3 | | 10/05/2016 09:13a |
| Company Admin | High | Y | 1 | Current profile for owners - full access | Y | 03/22/2022 12:54p |
| Copy of Company Admin | High | Y | | Current profile for owners - full access | Y | 04/15/2024 10:25a |
| Employee | Medium | Y | 7 | Current profile for any regular employees | Y | 03/22/2022 12:27p |
| Employee - Low | Low | Y | | | Y | 04/15/2024 09:42a |
| Manager | High | Y | 1 | Current profile for any managers | Y | 03/22/2022 12:47p |
| OLD Employee | Medium | Y | | Limited access to time entry and accrual information | | 09/17/2015 11:09a |

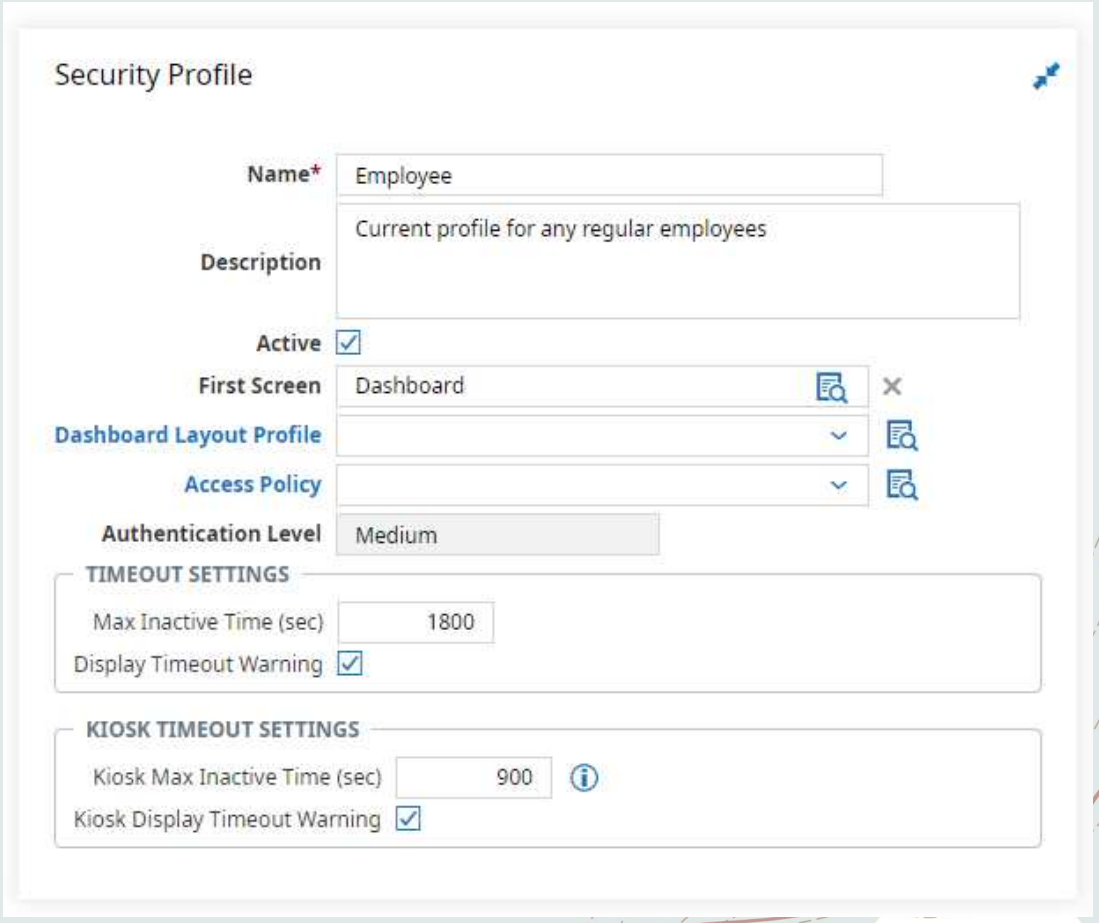
# Security Profiles (continued)

Name and Description: Allows you to provide more information on the access the employee will have with this profile.

Active: If you have a security profile that is no longer in use, it can be marked as inactive. This will keep it in the system but remove it from the list of options when selecting a profile for an employee.

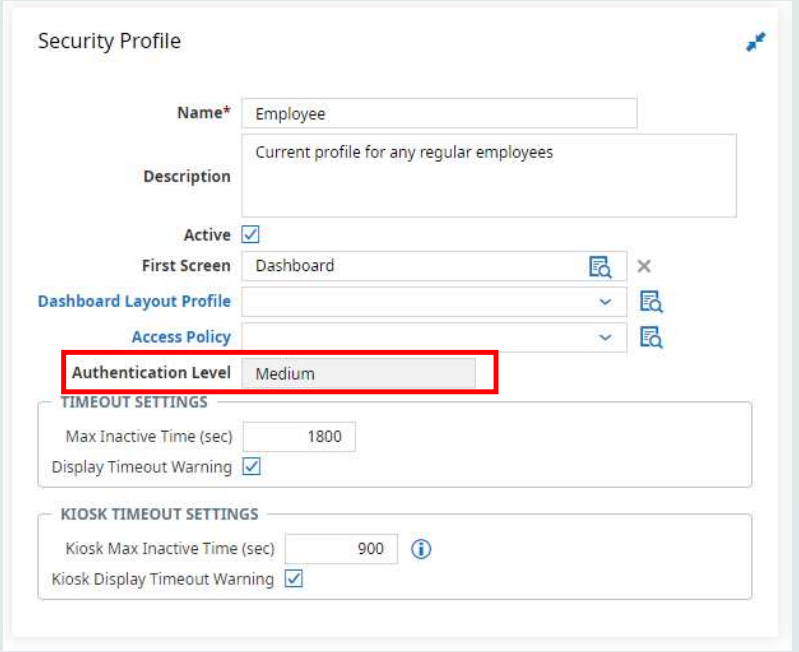
First Screen: First Screen is always set to the dashboard. This is where the system takes the employee by default when they sign in.

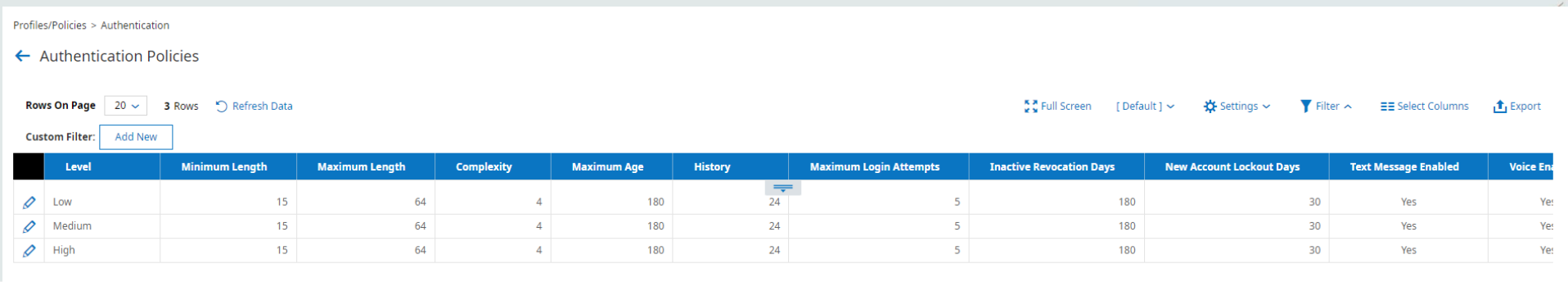
Authentication Level: This determines the password and MFA requirements when an employee logs in. It's determined based on what permissions have been given within the profile. To change the authentication level, access must be added/removed from the profile.



# Authentication Policies

- The Authentication Level within a security profile is determined based on what level of access the profile has.
- The Authentication Policy determines the Two-Factor Authentication and Password requirements for the employee(s).
  - Users with a High level will have to recertify (get a two-factor code) their MFA more often than those with a Low level because of the types of information they have access to.
- To learn more about authentication policies, check out our first session of the onboarding series from 4/18/2024. It is available on our Train to Thrive web page at the link in the chat.




| Level | Minimum Length | Maximum Length | Complexity | Maximum Age | History | Maximum Login Attempts | Inactive Revocation Days | New Account Lockout Days | Text Message Enabled | Voice En |
|---|---|---|---|---|---|---|---|---|---|---|
| Low | 15 | 64 | 4 | 180 | 24 | 5 | 180 | 30 | Yes | Yes |
| Medium | 15 | 64 | 4 | 180 | 24 | 5 | 180 | 30 | Yes | Yes |
| High | 15 | 64 | 4 | 180 | 24 | 5 | 180 | 30 | Yes | Yes |

# Troubleshooting

1) *A user does not have access to some or all of the information that they need access to.*
   - Are they assigned to the right security profile? (*if the security profile is not assigned correctly, they will likely be missing access to both the features and users that they need)*
   - Are they assigned as a manager over the correct employees? / Do they have group access, and if so, is it correct? *(Incorrect group access will result in a lack of employees on reports in the system. If the security profile is assigned correctly but someone cannot see the people that they need to see, this is likely a group issue)*
2) *I've setup a user as a new manager/admin, but their dashboard does not look correct. What's missing?*
   - At this time, a user's dashboard/start widget must be updated by APS once you increase their access. You can simply call or email us and ask us to reset the dashboard/start widget for the user.
3) *I've setup a user as a new manager/admin, but they cannot see some of my saved report views. What's missing?*
   - If the employee cannot view the same reports as you, have you shared the reports with them?
     - This is done individually by report. On the report, select the actions button (three dots) > Save View. On the pop-up, you will need to check the box for "Share", then ensure it is shared with others. You may select the users you'd like to share the report with, or you can leave the filter as "all employees" and only those with the security and group access to view that report will be able to access it.
     - Once you've shared the report, the users you've shared it with can find it in their My Saved Reports when "Others' Settings" is toggled on.
4) Shadow Session – if the shadow session feature is enabled on your security profile, you can shadow a user to see what they have access to. Doing this will allow you to determine whether they are missing access to certain items (likely a security profile issue) or whether they are missing access to certain employees (likely a group access issue).
5) As always, feel free to call or email APS and we can assist you in troubleshooting, too.

# Login As Employee/Shadow Session Feature

- Select the "Login As Employee" button from the Employee Information Page OR Employee Quick Links & Actions > Login As Employee
- This is useful to see who and what the employee can see or edit.
- *If you'd like this feature enabled, please contact APS and ask us to enable the shadow session feature. Please provide all users that you want to have access to this feature.*
- *Check out our second session of the onboarding series and fast forward to 21:17 in the recording to learn more about the shadow session feature.*