Security FAQs

General Information

The security settings are tied to Authentication Level Policies assigned to users based on their security and group permissions. Below is a matrix of the standard configuration.

CATEGORY	AUTHENTICATION LEVEL POLICIES		
	LOW	MEDIUM	HIGH
Security Profile	Employee	Manager	Administrator
Max Password Age	180 Days	180 Days	180 Days
Length	15-64	15-64	15-64
MFA Options	N/A	Email, Text, Voice, or Authentication App	Email, Text, Voice, or Authentication App
MFA Recertification Frequency	N/A	7 Days	7 Days

* Your company may differ depending on the products and permissions you have given to your team. Refer to the "Security/Authentication Levels by Employee" report in your My Saved Reports to view authentication levels currently assigned to employees. Employees and managers with access to other employee information will be assigned a medium authentication level at a minimum.

Frequently Asked Questions

1. **What is Multi-Factor Authentication (MFA), Virtual Code Authentication (VCA) and 2 Factor Authentication (2FA)?**
    a. MFA, VCA and 2FA are used interchangeably. These authentication methods require the user to provide two or more verification factors to gain access to an application.
2. **What are authentication policies?**
    a. There are three authentication policies (Low, Medium, and High). The policies contain configuration settings for passwords and two-factor authentication. These policies are assigned to employees based on the security permissions they have and if they are a manager of an account group. The application will automatically assign the authentication policy levels to the employee. You cannot individually assign authentication policies to users.
3. **When I hire a new employee, how do they login?**
    a. If you hire the employee with an email, they will automatically get the "Account Created" email which will list their username and give them a link to the Website to

login. From there, they will click "Forgot your Password?" to register their account and create their unique password.

4. **How will these security changes affect my employees logging in?**
   - **a.** The new security updates will not require that an employee login using the MFA settings if their authentication level in their security profile is classified as "low". If they are classified as "Medium" or "High" they will be prompted to set their authentication preferences when they login.
   - **b.** If the employee hasn't changed their password in more than 180 days, then the system will prompt them to change their password the next time they login, and concurrently every 180 days.
5. **Does this impact my employees clocking in & out on a physical time clock, a tablet in kiosk mode, or .clock desktop method?**
   - **a.** No. These settings will only apply to users trying to login to the system. If they are simply punching in and out without logging in, it will not require MFA (no matter the authentication level).
6. **How will I get my VCA code?**
   - a. Depending on your Authentication Level, if MFA is required (Medium and High) you can choose between the Virtual Code or Authentication App methods. The Virtual Code methods will allow Email, Text, and Phone options if you are a "Medium" or "High" authentication. The Google or Microsoft Authentication App is an alternative method that is a free downloaded app on your mobile device that produces a randomly generated code every 30 seconds. These are two examples of free authentication apps that will work in the application for verification purposes. Other authentication apps may also work but will require testing to confirm.
7. **I didn't originally setup a voice option for MFA… how do I set that up?**
   - **a.** After the new security rules have been enabled, the system will allow you to login with the previously established MFA settings, but will prompt you to configure new destinations based on the security settings associated with your authentication level.
8. **How do I reclassify someone as "low"?**
   - a. You would have to take away some of their permissions that are placing them in a higher authentication level by changing their security profile assigned to that employee and reviewing group authorities. You can review the *Security/Authentication Level by Employee* Report

9. **The security profile for Employee has been assigned a "Medium" authentication level. How do I get that security profile default authentication level to register as a "low" authentication?**
    a. If security profile permissions and defaults need to change, you would need to contact Innovative at IBSsupport@ibspayroll.com
10. **Where can I find the Authentication Levels tied to Security profiles/employees?**
    a. If you go to your My Saved Reports and search for "*Security/Authentication Level by Employee*" you will find a report that will show you each person, their security profile and authentication level.
11. **Is MFA required for external applicants?**
    a. No, external applicants using the .careers page will not be required to MFA. They will be required to adhere to the password policy requirements.

Helpful New Features

Reports

- Security/Authentication Level By Employee
- Two-Factor Request Log

Columns

- Inactive Days Until Locked (Employee Information)'
- Authentication Level (Employee Information)
- Security Profile: Authentication Level (Employee Information)
- Authentication Type (Global Access Report)
- Authentication Level (Global Access Report)

Notifications

- Account Created (New Hires)
- Password Changed
- Password Expiring
- Password Reset
- VCA Settings Changed