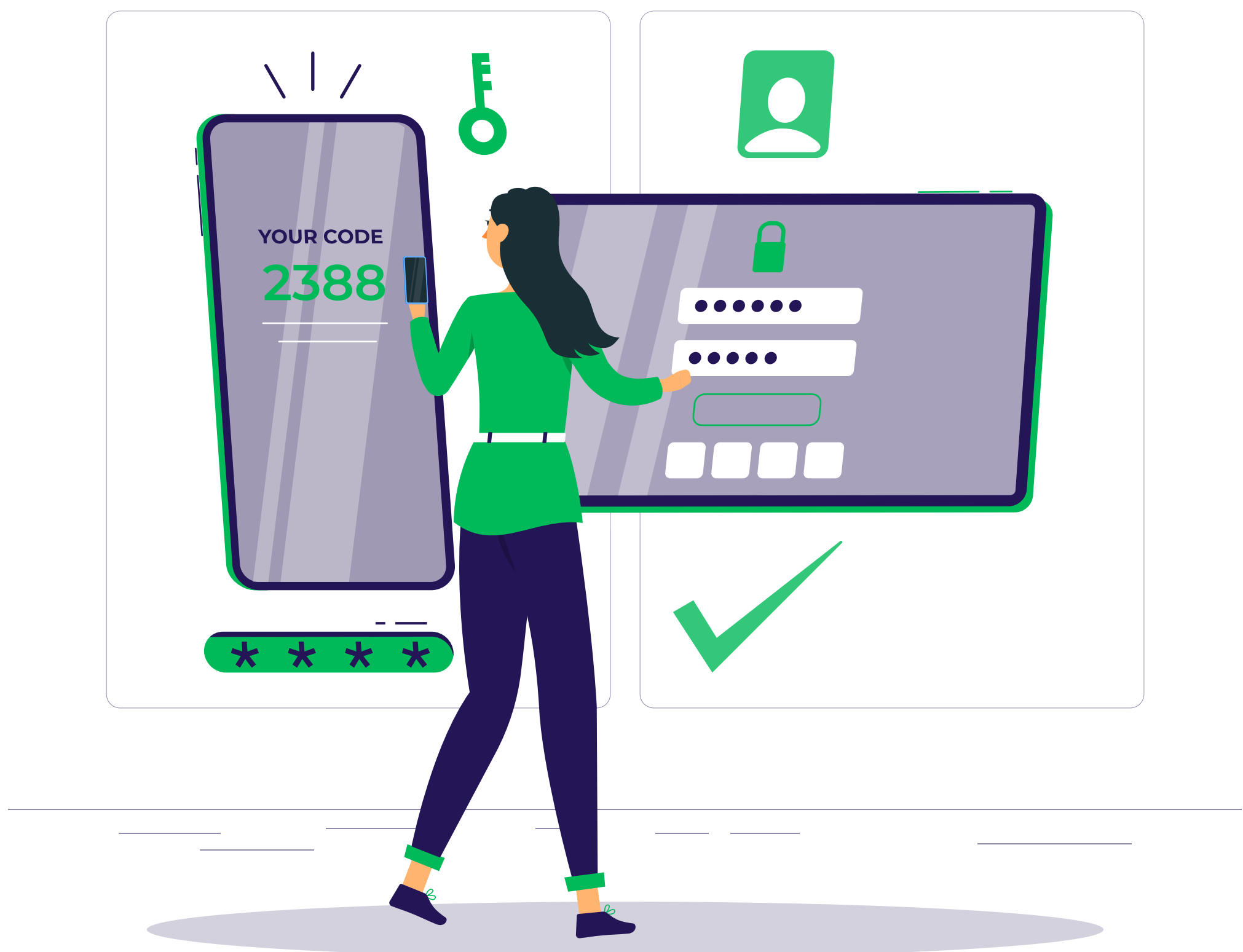


# Delinea's

# AUTHENTICATION

# PROFILES

Flexible MFA. Uncompromising Security. Tailored Authentication. Seamless Security.



For more content like and follow me:



@bertblevins

Delinea uses authentication profiles to provide a structured and flexible way to enforce Multi-Factor Authentication (MFA) policies and enhance security across its platform. Below are the key reasons why Delinea incorporates authentication profiles:

1


Standardized Security Framework

Authentication profiles act as a **centralized framework** for defining and managing authentication requirements. By standardizing these configurations, Delinea ensures consistency in how MFA is applied across different scenarios, reducing the risk of configuration errors.


2

Tailored Security for Different Use Cases


Different situations demand varying levels of security. Authentication profiles allow administrators to customize challenges based on specific needs, such as:



**New Device Logins:**  
Require stricter challenges to prevent unauthorized access.



**Password Resets:**  
Enforce additional verification to protect against phishing or social engineering attacks.



**Step-Up Authentication:**  
Add an extra layer of security when accessing sensitive resources or performing high-risk actions.


This flexibility allows organizations to match security measures with the level of risk.

3

Improved User Experience


By defining pass-through durations (time intervals before users are prompted again for MFA), authentication profiles balance security with usability. For example:

01



Regular logins may require a longer pass-through duration (e.g., 12 hours) to reduce interruptions.


02



High-risk actions or sessions (e.g., accessing admin settings) may require a shorter duration or immediate re-authentication.

This approach minimizes friction for users while maintaining robust security.

For more content like and follow me:

@bertblevins

## 4 Compatibility with Identity Policies

Authentication profiles integrate seamlessly with identity policies, enabling organizations to enforce MFA dynamically. Identity policies dictate the conditions under which a specific profile applies, such as user roles, locations, devices, or the sensitivity of the accessed resources. This integration ensures MFA is applied intelligently and contextually.

## 5 Support for a Wide Range of Authentication Mechanisms

By supporting various authentication methods—such as passwords, mobile authenticators, SMS codes, and FIDO2 authenticators—authentication profiles provide flexibility to meet the diverse needs of users and organizations. This ensures compatibility with existing infrastructure while promoting modern, secure authentication practices.

## 6 Enhanced Security Posture

Authentication profiles are a critical component in defending against account compromise, phishing, and other cyberattacks. By enforcing MFA challenges and tailoring them to specific scenarios, Delinea reduces the likelihood of unauthorized access, even if a primary credential (e.g., a password) is compromised.

## 7 Simplified Administration

For IT administrators, authentication profiles make it easier to manage security configurations across the platform. Profiles can be pre-defined or customized, then assigned to users or groups through identity policies. This simplifies deployment and ensures that security policies can adapt to organizational changes.

## Summary

Delinea uses authentication profiles to provide a secure, customizable, and user-friendly way to implement MFA across its platform. By combining structured configurations with flexible options, authentication profiles help organizations strengthen security while maintaining a smooth user experience.

**For more content like and follow me:**



**@bertblevins**

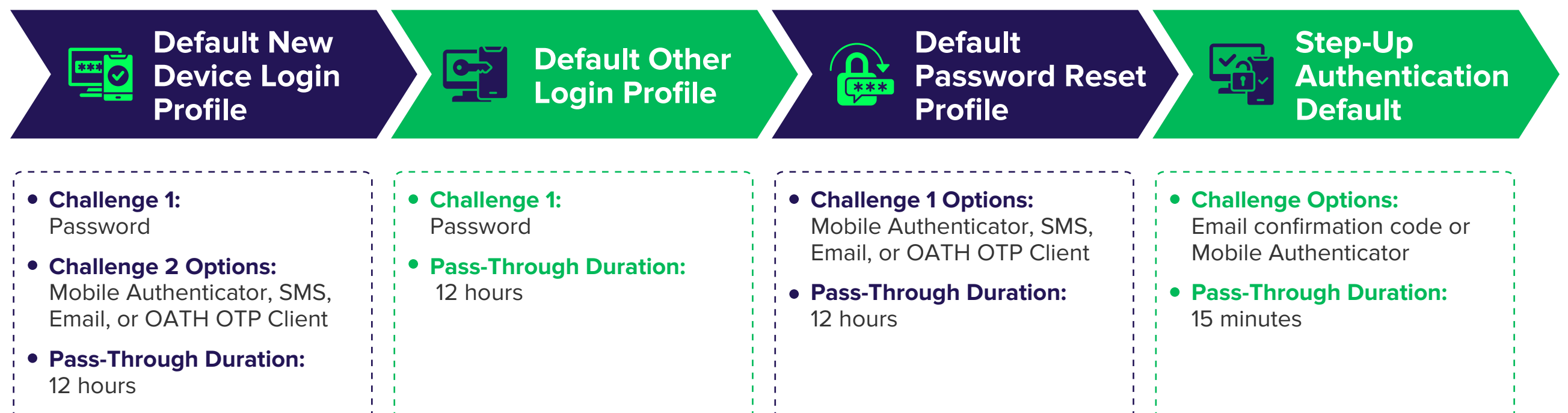
# Authentication Profiles in the Delinea Platform

Authentication profiles are a key component of the Delinea Platform, enabling the implementation of Multi-Factor Authentication (MFA). These profiles define the authentication challenges required for logging into the platform and set the duration before users are prompted to authenticate again. They work hand-in-hand with identity policies, which determine when and under what conditions the authentication challenges specified in the profile are applied.

## Key Features of Authentication Profiles

### 1 Built-in Profiles

The Delinea Platform includes several default authentication profiles designed for common use cases:



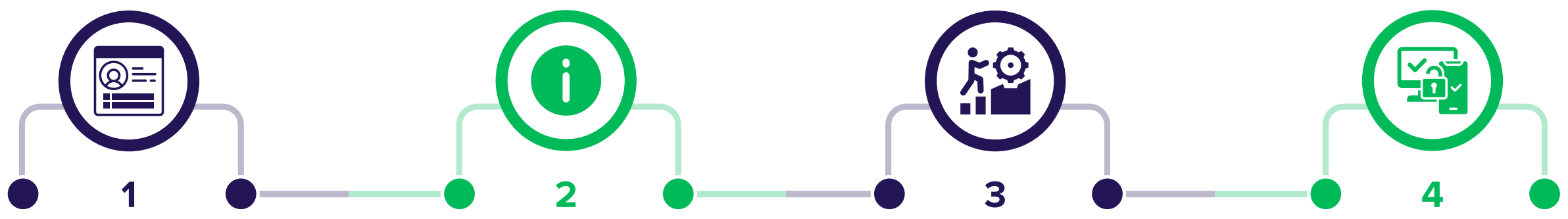
### 2 Creating Custom Profiles

Administrators can design custom authentication profiles tailored to their organization's needs by defining the following:

For more content like and follow me:



@bertblevins



**Profile Name:**

A unique identifier for the profile.

**Description:**

A brief explanation of the profile's purpose.

**Challenge Pass-Through Duration:**

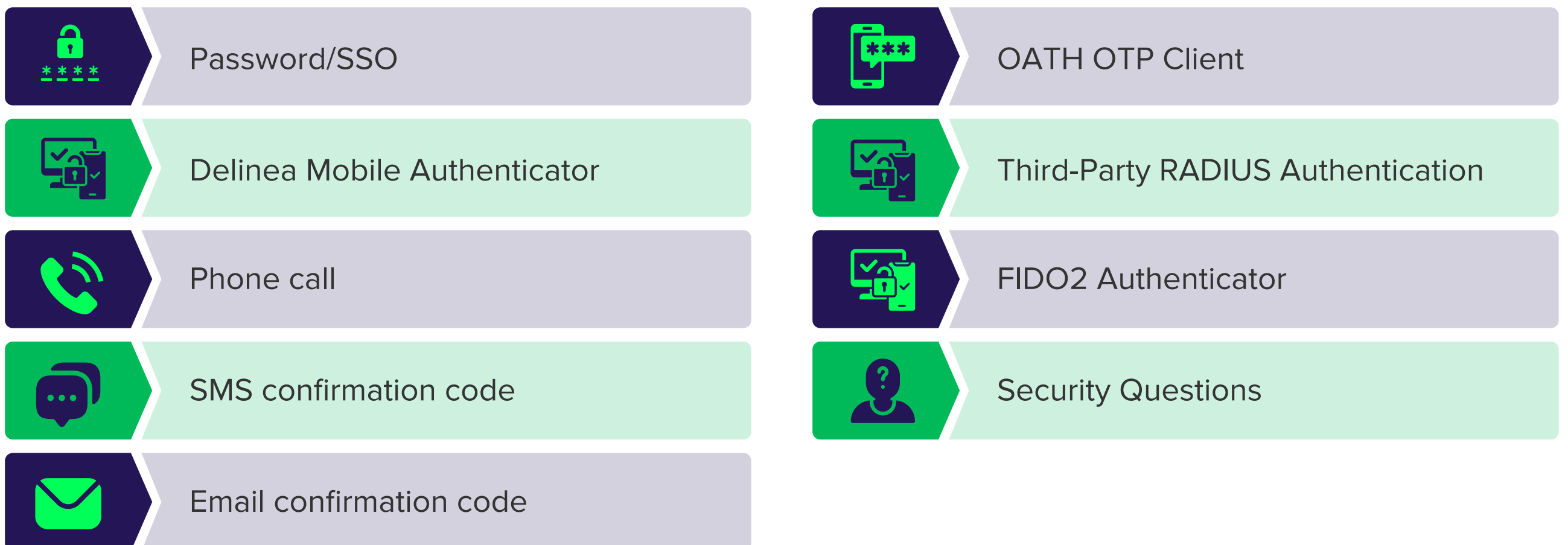
The time interval before users are re-prompted for MFA, applicable specifically to step-up authentication requests.

**Authentication Challenges:**

The choice of one or more mechanisms for Challenge 1 and Challenge 2.

### 3 Supported Authentication Mechanisms

The Delinea Platform supports a variety of authentication methods, offering flexibility in securing user access:



### 4 Assigning Profiles to Identity Policies

After creating an authentication profile, it can be linked to an identity policy. These policies define the specific scenarios under which the authentication profile's challenges are enforced, ensuring a seamless and secure user experience.

Authentication profiles in the Delinea Platform provide administrators with robust tools to customize and enforce MFA, balancing security requirements with user convenience.

For more content like and follow me:



@bertblevins



**Share your  
thoughts in  
comments  
below**

**For more content like and follow me:**



**@bertblevins**