

Government Self-Service enhanced security

Frequently Asked Questions (FAQ)

What is an enhanced security login experience?

Enhanced security is the first layer of protection to your [government self-service account](#), and you will soon notice an extra step to verify your identity, in addition to your password.

Why is this important?

The extra step, also known as two-factor authentication, significantly enhances security.

What are the benefits?

- **Increased security:** Adds an extra layer of protection, making it much harder for attackers to gain access to accounts.
- **Reduced risk:** Helps mitigate the risk of unauthorized access and data breaches.
- **Compliance:** Helps organizations meet compliance requirements in various industries.

How do providers enroll?

- To register to use [self-service](#) for the first time, users will be prompted to add an email address to receive their initial security code.
- Existing users will be prompted to choose a method to receive the security code when they log in.

What communication methods are available to receive their security code after their first log in?

- **Authenticator Apps:** Apps like Microsoft Authenticator generate unique codes for verification.
- **SMS/text messages:** A code is sent to a registered mobile phone number.
- **Voice Calls:** An automated call prompts the user to enter a code or press a button.
- **Email:** A code is sent to a registered email address.

Will users be required to use a mobile phone?

While mobile phones are a common method for receiving security codes, other options like email and authenticator apps are available.

What other changes should they expect to see?

We have removed the security questions as they are no longer needed.