comsignTRUST

Comsign Authenticator

One-Time Password

www.comsigntrust.co.il

Why use a one-time password (OTP)

Prevents attackers from being able to access your accounts using stolen passwords, since the one-time passwords are only valid for the first sign-in.

Eliminates the need to remember multiple passwords, since users only need to remember one password and their device will generate the unique code each time they log in.

OTPs do not require additional software or hardware components. Therefore, the cost of these components is eliminated.

Data security is critical for you and your organization

Banking | Finance | Electronic trade
Insurance | Governance | Transportation
Health | Schools | Energy | Vehicles
High-tech | Media | Real Estate | Security
Higher education | Pharmaceuticals

One-time password (OTP)

Double protection for double security

The Comsign Authenticator generates a one-time OTP password valid for a single access attempt, effectively preventing identity theft. This solution is meticulously designed to meet the global need for enhanced network security and protection of sensitive information and data.

It implements a robust verification mechanism supporting Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA). By generating one-time passwords, it ensures secure access to applications and prevents unauthorized system entry. Authentication using two or three distinct methods offers a stronger alternative to traditional password mechanisms, ensuring a more secure and reliable user verification process:

1 **SOMETHING YOU HAVE**
The physical OTP component (app or token)

2 **SOMETHING YOU KNOW**
A permanent personal identification number (PIN)

3 **SOMETHING YOU ARE**
Finger print, facial recognition

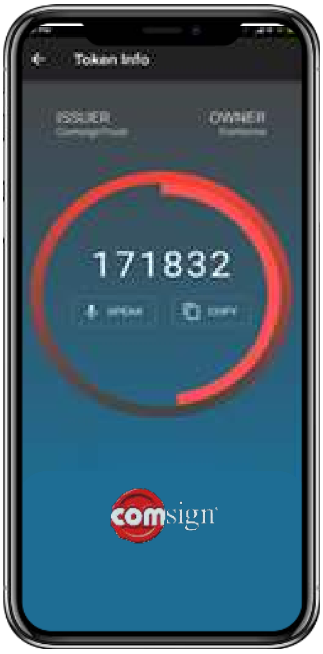
OTP components

Hard token (Hard Token) - a small device that looks like a key ring decoration or a small calculator with LCD screen. Generates the OTP and presents it on the screen of the token.

Soft token (Soft Token) - a mobile app which generates the OTP code Download on the APP Store and Google PLAY.

IVR (voice message) - After logging in, you'll receive an OTP by phone call. Enter the code provided to gain access.

SMS - After entering the system you'll receive your OTP through an SMS Enter the code into the OTP field in the system you are attempting to access and you will be granted access.



How OTP works?

Accessing the OTP Interface:

1 Enter a unique code to access the OTP interface.

2 Receive a one-time password via app, OTP token, or SMS, valid for 30-60 seconds.

3 Enter the OTP into the app, VPN, website, or secure database.

4 The Comsign server will validate the OTP. Access is granted if the OTP is correct; otherwise, access is denied.

Main features

- **Works Anywhere:** No internet connection required
- **OTP Read-Out:** Option to have the OTP code read aloud
- **User-Friendly Interface:** Convenient and easy to use
- **Customizations:** Client-specific adjustments available
- **Simple Migration:** Easy transition from existing OTP systems
- **Push Notifications:** Allows identification without a password
- **Integration:** Easy integration with apps, VPNs, and databases
- **User Management:** Add or remove users effortlessly
- **Reporting:** Export reports on active users, canceled users, tokens in use, authentication attempts, and more

Prevent unauthorized access to your system or network with Comsign OTP.
This simple and secure two-factor authentication solution allows protection against advanced cyber attacks.

comsignTRUST

CONTACT US

@ www.comsigntrust.com

☎ *8770

✉ info@comsigntrust.com

in Comsigntrust