PROTECTIMUS

Multi-Factor Authentication Provider

Protectimus is a powerful OATH-certified MFA solution designed for strong, flexible, and cost-effective authentication. Our platform supports cloud-based and on-premise deployments, a wide range of OTP authentication methods, and advanced security features like transaction verification.

With Protectimus, you get seamless integration, robust protection, and expert support - everything you need to secure your business against unauthorized access.

oath CERTIFIED

CITRIX Ready

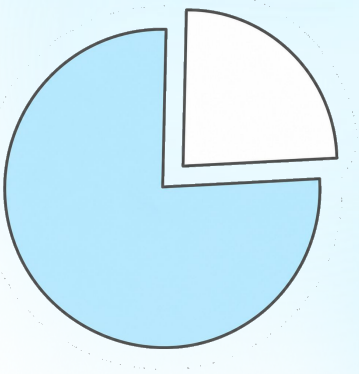
Microsoft Partner

www.protectimus.com
sales@protectimus.com

Shocking Statistics

80%

of all breaches
are caused by
stolen or weak passwords



Almost all

of these breaches
could be prevented with
multi-factor authentication!

- ➔ **80% of breaches** are caused by stolen or weak passwords (Verizon Report).
- ➔ **99.9% of automated attacks** can be blocked with multi-factor authentication (Microsoft).
- ➔ In 2024, over **560 million records** were exposed due to missing or weak authentication. (Snowflake breach)
- ➔ **73% of passwords** are reused across multiple accounts, increasing breach risks (LastPass).
- ➔ **Credential stuffing attacks** have surged **300%** in the USA, targeting accounts without multi-factor authentication (FBI).

With stolen credentials at the heart of most breaches, enabling **multi-factor authentication (MFA)** is one of the most effective ways to block automated attacks, prevent unauthorized access, and significantly reduce security risks.

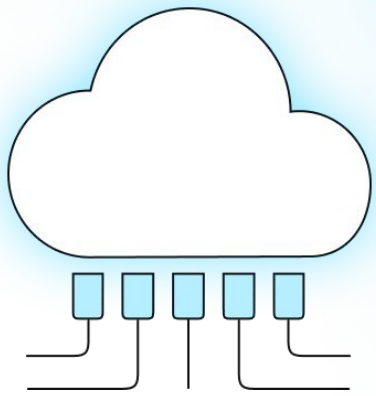
www.protectimus.com
sales@protectimus.com

Cloud MFA Service and On-Premise MFA Platform

Cloud-Based MFA Service

If you need multi-factor authentication quickly and with minimal effort, choose the Cloud MFA Service.

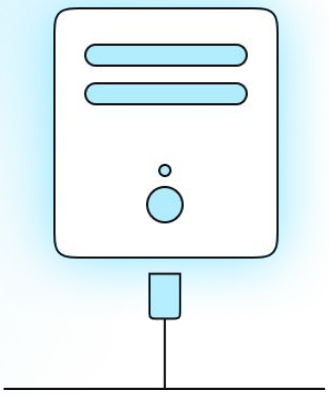
With the Cloud MFA Service, you can quickly implement multi-factor authentication in your project. You pay only for what you actually use and don't need to worry about equipment, administrators, load distribution, or other infrastructure issues — everything is already set up and ready to use. This solution is SaaS-based.



On-Premise MFA Platform

If you want full control over the authentication system, choose the On-Premise MFA Platform.

It is designed for installation in your environment, giving you complete control over your data and processes. The MFA platform's efficiency depends entirely on you and your equipment. You can create the most secure services by blocking external access to the system with an army of firewalls and skilled admins.



PROTECTIMUS

www.protectimus.com
sales@protectimus.com

Easy Integration Into Your Infrastructure

Easily integrate Protectimus into your existing infrastructure with our API, SDKs, and ready-to-use components. Connect seamlessly with Active Directory, ADFS, Windows, RDP, RADIUS, OWA, Roundcube, and more. Our integration options make the process simple, and our support team is always here to help.

Integrations Out-of-the-box
Enhance your security effortlessly with our pre-built integrations. Seamlessly connect with popular platforms like ADFS, OWA, Office 365, Windows & RDP, and RADIUS-supported devices, software, and VPNs such as Cisco AnyConnect and FortiGate VPN, among others.

API
Integrate Protectimus MFA with your systems with ease using our user-friendly API. Protectimus RESTful API supports XML and JSON data transmission and comes with auxiliary libraries for Java, Python, and PHP.

SDK
We provide convenient auxiliary libraries for popular programming languages Java, Python, and PHP. These SDKs facilitate a seamless and efficient integration process, allowing you to enhance your security measures effortlessly. Download our SDKs to start integrating Protectimus with ease.

Customisation
You can request branding for tokens, applications, and even the platform, as well as customize our solution to fit your processes and integration needs. If you have specific requests, please let us know - we'll be happy to help.

oath CERTIFIED CITRIX Ready Microsoft Partner

PROTECTIMUS

www.protectimus.com
sales@protectimus.com

Explore Our Pre-built Integrations

MFA for AD, LDAP, Databases
The first MFA software to integrate directly with databases and directories (AD, LDAP, custom databases), turning static passwords into dynamic OTPs

MFA for Windows & RDP
MFA solution for Windows 7 / 8 / 8.1 / 10 / 11 and Windows Server 2012 R2 / 2016 /2019 / 2022. Protects both local accounts and remote desktops (RDP)

MFA for ADFS
The Protectimus MFA solution integrates easily with ADFS 3.0 or 4.0

MFA for OWA & EAC
An installer that helps to set up OWA two-factor authentication (Exchange 2013, 2016, 2019) and Exchange Admin Center (EAC) in just a few minutes

MFA for SSO
Use Protectimus ADFS or Office 365 components to enable single sign-on (SSO) with extra security from time-based one-time passwords

MFA for Roundcube
The Roundcube 2FA plugin lets you easily integrate a professional MFA solution into Roundcube webmail

MFA for RADIUS
Protectimus cloud MFA service and on-premise MFA platform integrate easily with any device or system that supports the RADIUS protocol

MFA for VPN
Connect Protectimus SAAS service or on-premise platform with any VPN service including SonicWall, Sophos, Cisco, and Azure VPN via RADIUS

MFA for macOS
Protectimus integrates with macOS via RADIUS to secure user accounts

MFA for Linux
Integrate Protectimus cloud service or on-premise platform with Ubuntu via RADIUS to protect your corporate Linux accounts with MFA

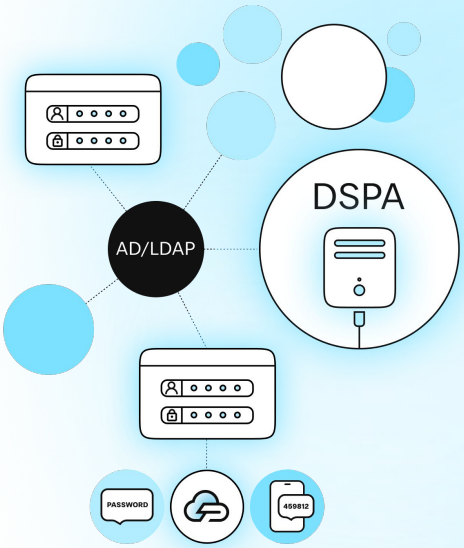
MFA for Citrix
Compatibility with Citrix ADC, Citrix Gateway, Citrix Virtual Apps та Citrix Virtual Desktops has been confirmed during testing by Citrix

API and SDK
We provide flexible RESTful API, detailed documentation, and prepared SDKs for Java, PHP, and Python

oath CERTIFIED CITRIX Ready Microsoft Partner

www.protectimus.com
sales@protectimus.com

Protectimus DSPA
(Dynamic Strong Password Authentication)



Protectimus integrates **directly with Microsoft Active Directory (or any other user directory)** to replace traditional static passwords with secure one-time passwords generated using the TOTP algorithm. These passwords constantly change according to a schedule defined by the administrator, turning standard Active Directory authentication into OTP-based authentication.

The administrator defines the one-time password rotation interval, starting from 30 seconds with configurable step-based increases. Password rotation policies can be configured individually for each user, and administrators can choose which user groups are required to use Protectimus Dynamic Strong Password Authentication (DSPA).

As a result, Active Directory users authenticate using **one-time passwords instead of permanent static credentials**. To generate OTPs, users can use the Protectimus SMART authenticator app or chatbots on Telegram, Viber, or Facebook. Access to the app or messenger can be additionally protected with a PIN code or biometrics, adding an extra layer of security to the authentication process.

www.protectimus.com
sales@protectimus.com

Protectimus MFA for Windows and RDP

The Protectimus Winlogon & RDP solution adds two-factor authentication (2FA) to **Windows 7, 8, 8.1, 10, 11, and Windows Server 2012, 2016, 2019, and 2022**.

It secures access both locally and via Remote Desktop Protocol (RDP).

- ➔ Easy installation - our installer simplifies MFA setup, getting you up and running in minutes.
- ➔ Offline mode with backup codes – users can log in even when offline.
- ➔ Automatic user and token registration.
- ➔ Mass deployment – deploy via MSI and Group Policy (GPO).
- ➔ RDP access control – filter by IP and set custom policies.
- ➔ Separate policies for RDP & local login.
- ➔ Support for various authentication methods: Password, Smartcard, Windows Live ID (WLID), PIN, Windows Hello (Face, Fingerprint).
- ➔ Microsoft account compatibility.

www.protectimus.com
sales@protectimus.com

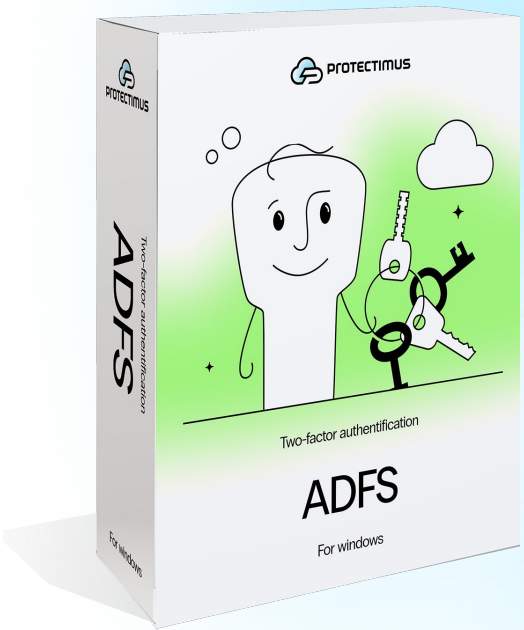
Protectimus MFA for OWA and EAC

Secure **Outlook Web App & Exchange Admin Center (Exchange 2013, 2016, 2019)** with two-factor authentication.

- ➔ Quick & Easy Setup – our installer enables MFA configuration in minutes.
- ➔ Admin Protection – adds 2FA for Exchange Admin Center (EAC) to safeguard admin accounts.
- ➔ Flexible Access Policies – enable MFA for specific Active Directory groups or all users.
- ➔ Custom Authentication Frequency – define how often users must enter OTPs (e.g., every 12 hours).
- ➔ Broad Token Support – supports TOTP and OCRA hardware tokens, the Protectimus Smart OTP app, SMS codes, and OTPs via Telegram, Viber, or Messenger.
- ➔ Self-Service for Users – reduce admin workload by allowing users to manage their own 2FA tokens.
- ➔ Advanced Security Controls – implement geographic and time-based login restrictions (e.g., access only during business hours).

www.protectimus.com
sales@protectimus.com

Protectimus MFA for ADFS



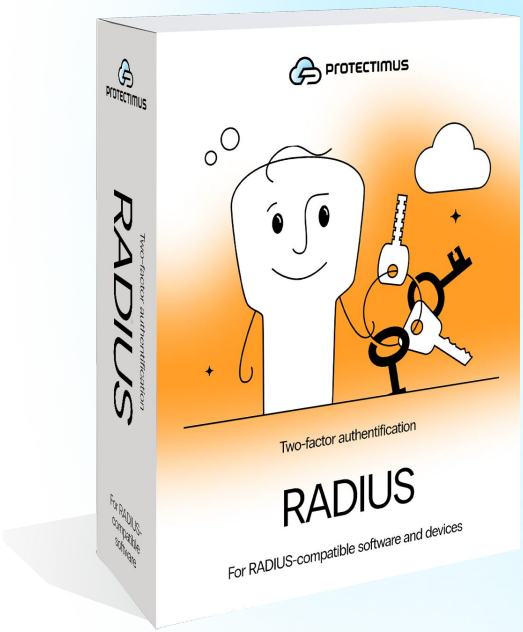
The Protectimus MFA solution seamlessly integrates with **Active Directory Federation Services (ADFS 3.0 & 4.0),** enhancing security with minimal effort.

- ➔ Quick & Easy Setup – deploy in minutes with an intuitive installer and detailed setup guide.
- ➔ Secure SSO Access – with ADFS Single Sign-On (SSO) and Protectimus, you can secure access to all key web applications and cloud services across your corporate network, including AWS, Asana, Dropbox, Evernote, GitHub, Jira SSO, Office 365, Salesforce, Slack, Zoom, and many more
- ➔ Broad Token Support – supports TOTP hardware tokens, the Protectimus Smart OTP app, SMS codes, and OTPs via Telegram, Viber, or Messenger.
- ➔ Self-Service for Users – reduce admin workload by allowing users to manage their own 2FA tokens.
- ➔ Advanced Security Controls – implement geographic and time-based login restrictions, such as access only during business hours.

oath CERTIFIED · CITRIX Ready · Microsoft Partner

www.protectimus.com
sales@protectimus.com

Protectimus MFA for RADIUS



Secure your **VPN, Wi-Fi, firewalls, and any RADIUS-based system** with two-factor authentication. The Protectimus RADIUS solution integrates seamlessly with Cisco AnyConnect, Citrix Gateway, VMware Horizon, FortiGate, SonicWALL, OpenVPN, and more.

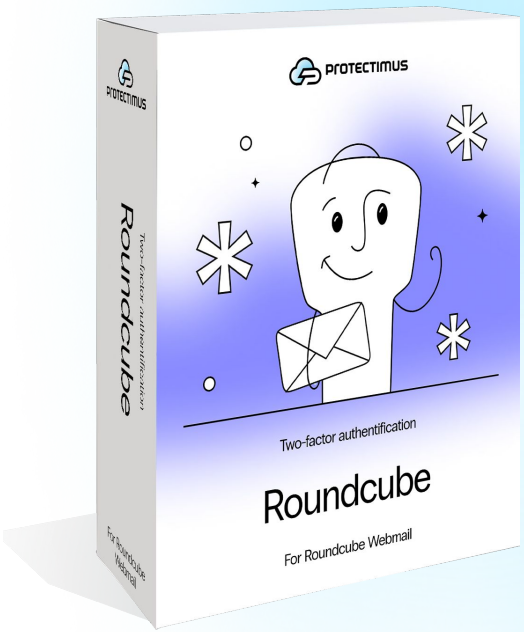
The Protectimus MFA connector works as a RADIUS server. It accepts incoming RADIUS authentication requests from the RADIUS device and contacts the Protectimus MFA server for two-factor authentication (2FA).

- ➔ Seamless Integration – works with any RADIUS-compatible software or hardware.
- ➔ User Self-Service – reduces admin workload by allowing users to manage their own OTP tokens.
- ➔ Flexible Authentication – supports all Protectimus OTP tokens, including hardware, mobile apps, SMS, and chatbots.
- ➔ Advanced Security – enforce IP filtering, geographic restrictions, and time-based access rules (e.g., business hours only).
- ➔ Trusted & Reliable – Citrix Ready Partner certification ensures compatibility.

oath CERTIFIED CITRIX Ready Microsoft Partner

www.protectimus.com
sales@protectimus.com

Protectimus MFA for Roundcube



Enhance email security with OATH-certified two-factor authentication (2FA) for **Roundcube Webmail**.

The Protectimus Roundcube plugin ensures maximum protection against unauthorized access as well as easy integration and professional support.

- ➔ Fast & Easy Setup – deploy MFA in ~15 minutes with the Protectimus 2FA plugin.
- ➔ User Self-Service – eliminates admin workload as users create and manage their own OTP tokens.
- ➔ Flexible Authentication – supports TOTP hardware tokens, the Protectimus Smart OTP app, SMS codes, and OTPs via Telegram, Viber, or Messenger.
- ➔ Advanced Security Controls – enforce IP filtering, geographic restrictions, and time-based access rules (e.g., business hours only).

www.protectimus.com
sales@protectimus.com

Wi-Fi SMS Authentication for Ubiquiti UniFi

Secure your guest Wi-Fi network with Protectimus SMS authentication for Ubiquiti UniFi Controller. Our solution is fully compatible with Ubiquiti UniFi Controller and supports integration with any SMS provider via SMPP. Customization for other Wi-Fi controllers is also available.

How It Works

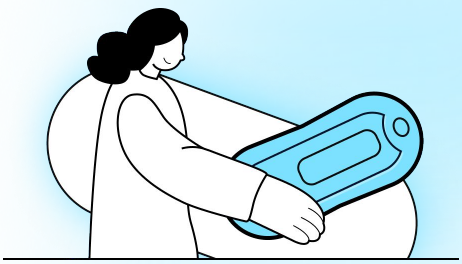
- ➔ Users enter their phone number when connecting to Wi-Fi.
- ➔ They receive a unique one-time password via SMS.
- ➔ They enter the OTP in the login field.
- ➔ Protectimus verifies the code and grants or denies access.

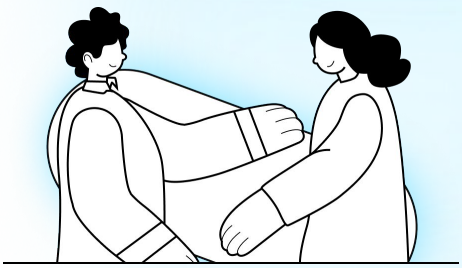
Logging & Compliance

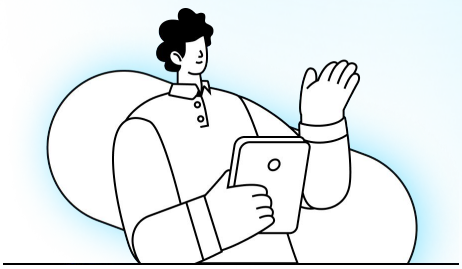
Protectimus logs user access data in CSV format, including MAC addresses, assigned IPs, and phone numbers. Data retention can be customized to meet local regulations, typically requiring storage for at least 6 months.

www.protectimus.com
sales@protectimus.com

Electronic Visit Verification (EVV)







Ensure accurate and privacy-friendly visit tracking with the Protectimus EVV solution, built on Time-Based One-Time Passwords (TOTP).

How It Works

- ➔ The patient receives a TOTP hardware token, which can be placed anywhere in their home.
- ➔ The caregiver records a one-time password (OTP) from the token at the start and end of the visit.
- ➔ These OTPs are entered into the Protectimus EVV system.
- ➔ The system calculates the exact visit times based on the OTP timestamps.

Why Choose Protectimus EVV?

- ➔ Privacy-Friendly – no GPS tracking or video monitoring.
- ➔ Accurate Time Verification – OTPs provide precise timestamps.
- ➔ Easy & Cost-Effective – no internet, apps, or additional infrastructure needed.

www.protectimus.com
sales@protectimus.com

Advanced Authentication Methods

Protectimus provides secure and flexible authentication methods, including hardware OTP tokens (classic & programmable), mobile apps, SMS, push notifications, email authentication, and chatbots (Telegram, Viber, Messenger). Choose the best option for your security needs with a seamless user experience.

HARDWARE TOTP TOKENS

Protectimus Slim NFC

A programmable TOTP token compatible with any OATH-based MFA system.

Protectimus Two

A classic hardware TOTP token with pre-installed secret keys and SHA-1 support.

Protectimus Flex

Programmable hardware TOTP token in a key fob format that fits any authentication system.

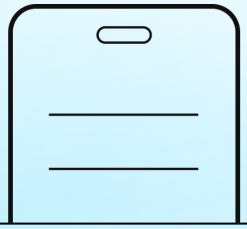
Protectimus Shark

A classic hardware TOTP token with pre-installed secret keys and SHA-256 support.

oath CERTIFIED · CITRIX Ready · Microsoft Partner

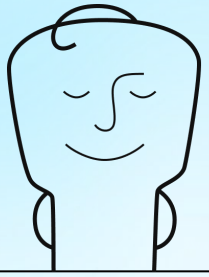
www.protectimus.com
sales@protectimus.com

SOFTWARE OTP GENERATION AND DELIVERY METHODS



Protectimus Smart OTP

A free 2FA app with cloud backup, easy migration, and biometric/PIN protection.

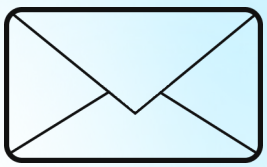


Protectimus Bot

Free OTP delivery via chatbots on Facebook Messenger, Telegram, and Viber.

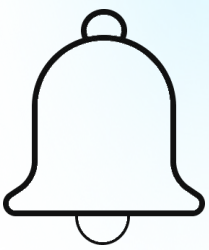
Protectimus SMS

OTP delivery via SMS with the option to add your own provider via SMPP.



Protectimus Mail

Free one-time passwords delivery via email - very easy to set up and use.

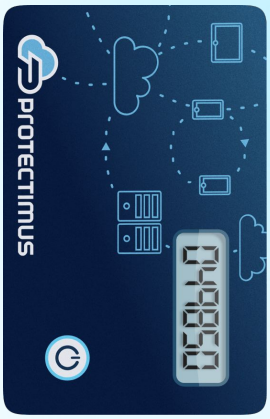


Protectimus Push

OTP delivery via push notifications in the Protectimus Smart 2FA app.

www.protectimus.com
sales@protectimus.com

Programmable TOTP Tokens
Protectimus Slim and Protectimus Flex



Reprogrammable & Versatile

Protectimus Slim NFC and Protectimus Flex TOTP tokens come with pre-installed secret keys but can be reprogrammed using an NFC-enabled Android phone. This makes them compatible with nearly any OATH-based 2FA system, including Google 2FA, Office 365, Azure MFA, Okta, Duo, and more.

Convenient & Secure

These tokens offer a cost-effective solution for businesses — reassign them instead of replacing them. NFC-based setup ensures only you know your secret key. Unlike software-based options, they don't connect to the internet or GSM networks, eliminating the risk of OTP interception via SMS or malware.

Two Form Factors

- ➔ Protectimus Slim – Card-sized, perfect for wallets or ID badges.
- ➔ Protectimus Flex – Key-fob design for easy everyday use.

oath CERTIFIED · CITRIX Ready · Microsoft Partner

www.protectimus.com
sales@protectimus.com

Classic TOTP Tokens
Protectimus Two and Protectimus Shark

Protectimus Two and Protectimus Shark are high-strength, water-resistant hardware TOTP tokens with pre-installed secret keys that cannot be reprogrammed by the end user.

To use these tokens, you must have access to the MFA server to add their secret keys to the authentication system.

Best Use Cases:

- Corporate environments using the Protectimus multi-factor authentication platform.
- Any system where secret keys can be manually added.

Key Differences:

Both tokens offer durability and protection from water and dust, but they differ in supported hashing algorithms:

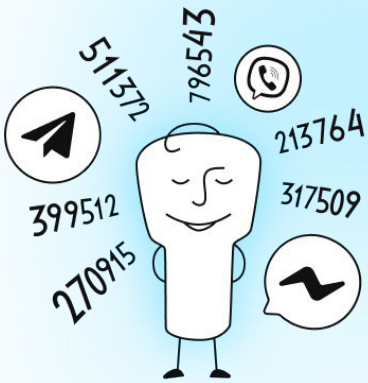
➔ **Protectimus Two** supports **SHA-1.**

➔ **Protectimus Shark** supports **SHA-256**, providing stronger security against brute-force attacks.

PROTECTIMUS

www.protectimus.com
sales@protectimus.com

Easy & Cost-Effective OTP Delivery via Chatbots in Messaging Apps



Convenient
No need to pay for SMS, buy hardware tokens, or ask users to install extra apps. Users simply add the ProtectimusBot chatbot to their favorite messaging app — Telegram, Facebook Messenger, or Viber. Setup takes just 15 seconds, and they're ready to receive OTPs and important messages.

Cost-Saving
Chatbot-based authentication is completely free — just as simple as SMS, but without the costs. You can also combine OTP delivery with important notifications, like deposit and withdrawal alerts, eliminating SMS expenses entirely.

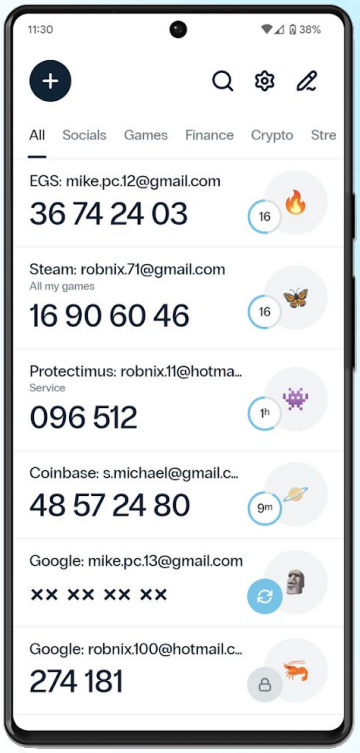
Secure
Messaging apps use strong encryption, and access to them is protected by passwords. This method also supports HOTP and TOTP algorithms, as well as the CWYS (Confirm What You See) data-signing function, ensuring OTPs remain secure even if intercepted.

PROTECTIMUS

www.protectimus.com
sales@protectimus.com

Protectimus Smart OTP

2FA App with Secure Cloud Backup



Download on the App Store

GET IT ON Google Play

Key Features:

- ➔ Encrypted cloud backup – keep your tokens safe, even if you lose your phone.
- ➔ Seamless token transfer – easily move tokens to a new device.
- ➔ Google Authenticator import – migrate your existing tokens effortlessly.
- ➔ PIN & biometric protection – secure access with Touch ID or Face ID.
- ➔ Supports HOTP, TOTP, and OCRA – works with all OATH-compliant systems.
- ➔ Push notifications for 2FA – quick and hassle-free authentication.
- ➔ Confirm What You See (CWYS) – extra security for financial transactions.
- ➔ Custom OTP length – choose between 6 or 8 digits.
- ➔ Multi-language support – English, French, German, Spanish, Italian, Russian, Ukrainian.
- ➔ Organized & customizable – sort tokens into folders, add emojis & descriptions.
- ➔ Error prevention – check symbol feature to avoid typos when entering keys.

oath CERTIFIED

CITRIX Ready

Microsoft Partner

www.protectimus.com
sales@protectimus.com

White-Labeling and Customization Options

We offer branding for tokens, apps, and the platform, plus customization to fit your processes and integration needs. At Protectimus, we prioritize your requirements and are happy to help with any specific requests.

1. Two-Factor Authentication Platform

We offer full customization for our software and OTP tokens to match your brand.

- ➔ **White-Labeled MFA Platform:** we'll deploy a fully branded MFA platform within your environment, with hardware and software OTP tokens featuring your company's colors and logo.
- ➔ **Custom Features:** if you need specific functionalities, our team is ready to tailor the solution to your exact requirements.

2. Protectimus SMART OTP App

Looking for a customized application to generate one-time passwords? We can rebrand the Protectimus SMART OTP app with your company's name, logo, and design style to match your corporate identity.

3. Hardware Tokens

For orders of 1,000 or more, we can produce hardware tokens in your corporate style, ensuring consistency across all your authentication tools.

www.protectimus.com
sales@protectimus.com

Proven Multi-Factor-Authentication Solution

OATH Certified Product

Protectimus is certified by the OATH (Open Authentication) initiative. It supports all major OATH algorithms for OTP generation — HOTP (RFC 4226), TOTP (RFC 6238), and OCRA (RFC 6287). These tested and reliable algorithms are the standard in two-factor authentication. Our Data Signing feature is based on the OCRA algorithm.

Citrix Ready Partner

Protectimus is officially certified as a Citrix Ready Partner, confirming its compatibility with Citrix products. Our solution is recommended for integration with Citrix Gateway, ADC, Virtual Desktops, and Virtual Apps. Integration is seamless through the RADIUS protocol.

Microsoft Partner

Protectimus is also a Microsoft Partner, ensuring seamless integration with Microsoft solutions, including Windows, RDP, ADFS, OWA, AD, Azure and Office 365, for a robust and reliable authentication experience.

www.protectimus.com
sales@protectimus.com

Why Choose Protectimus?

Tailored MFA Solutions

Every customer is unique. We provide personalized service and dedicated support.

Seamless Integration

Our support and development teams offers full assistance to ensure a smooth and hassle-free setup.

Unmatched Security

Protectimus supports event-based (HOTP), time-based (TOTP), and challenge-response (OCRA) OTP generation algorithms, plus transaction data signing for maximum protection.

Cost Savings

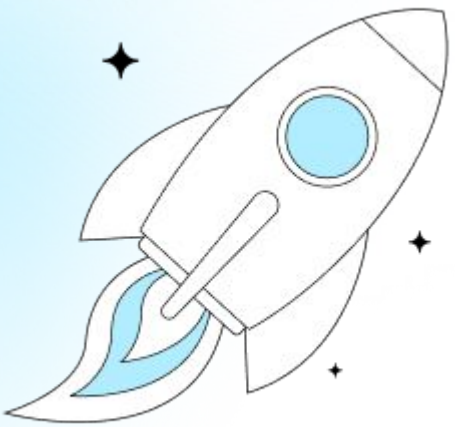
Cut authentication expenses while improving efficiency. Our multi-factor authentication system has helped businesses double the effectiveness of their security budgets.

Custom Features on Demand

Need specific functionality? We adapt our solution to meet your exact requirements.

White-Labeling and Customization

Customize platform, software and hardware tokens with your company's logo and design.



Trusted by Businesses Worldwide

Many companies trust Protectimus MFA solutions to secure corporate data and user accounts. Explore our customer stories to see how we've helped them overcome 2FA challenges and protect critical access points.

volet. sicim FRESENIUS KABI DXC TECHNOLOGY aruba.it

volet.

Over the past years, we've had only positive cases of working together. Protectimus helped us at every stage, from integration to adding additional features that solved our specific tasks. Using Protectimus, we are confident that Volet infrastructure and users are well protected. Protectimus gives us what money can't buy – not a sense of security, but REAL security. I highly recommend it for implementation.

Artem Sh.,
Information Security Director at Volet

sicim

At the moment, my assessment of the company's work is 10 out of 10. An important factor in choosing this two-factor authentication provider was the possibility of customizing the 2FA system for our project. After we got in touch with the Protectimus team and explained the task, they implemented the necessary functionality for us free of charge. There were no problems. Everything works well.

Cristian G,
System Administrator at SICIM

See What Other Clients Are Saying

SpokeChoice paysafecard MoneySolver IPAK YO'LI BANKI IDEMIA

DXC TECHNOLOGY

Protectimus was chosen because of their unique Dynamic Strong Password Authentication (DSPA) technology. Using this product, we added 2FA to all the systems we needed to protect in one fell swoop, as it allowed us to integrate two-factor authentication services straight with Active Directory. We have been using the Protectimus two-factor authentication platform for a year and are satisfied with this product.

Mauro S.,
Xchanging Italy a DXC Technology

IPAK YO'LI BANKI

We opted for Protectimus for several key reasons. First, it allows us to host the MFA server on our premises. Secondly, it provides comprehensive MFA coverage for all entry points to our corporate banking infrastructure, all from a single provider. Thirdly, the option to purchase a lifetime license for Protectimus MFA software has allowed us to secure access to our employees' accounts for the long term.

Information Security Director
at Ipak Yo'li Bank

Get in Touch

Protectimus Ltd
Carrick house, 49
Fitzwilliam Square,
Dublin D02 N578,
Ireland

Telephone Line
Ireland: +353 19 014 565
USA: +1 786 796 66 64

Product issues, questions, or feedback
support@protectimus.com

Potential partnership discussion, sales
sales@protectimus.com