PROTECTIMUS

Two-Factor Authentication Provider

Protectimus is a powerful ecosystem for building strong authentication based on the use of one-time passwords (OTP). Protectimus is a combination of comfortable security and an affordable price

The authentication platform is certified by the industry initiative OATH and supports all the standard algorithms for generating one-time passwords. Data signing based on the OCRA algorithm and transaction data verification make funds transfers the most secure and convenient for the user. Customers can use a wide range of software and hardware tokens.

The Protectimus technical support service will provide the necessary assistance during the process of integration and system use.
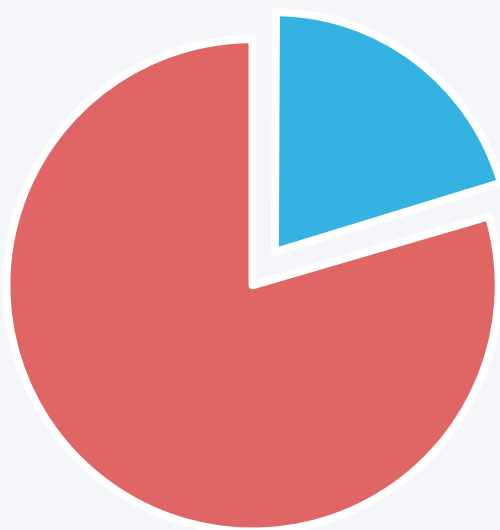
![Protectimus logo]

Shocking Statistics

In 2021 companies lost

$56

billion to cybercriminals.

83% of these

security breaches could be prevented with two-factor authentication!

- Protectimus is ranked among top 500 world cybersecurity vendors and top 10 London cybersecurity companies. Only 11 UK companies were included in Global Cybersecurity 500 and we are proud to be one of them!

- Every day Protectimus protects hundreds of companies from phishing, spear phishing, keyloggers, credential stuffing, brute force attacks, trojans, social engineering, man-in-the-middle (MITM) attacks,

- Protect your users today not to regret tomorrow!

Cloud-Based 2FA Service & On-Premise 2FA Platform

Software as a Service

If you need two-factor authentication quickly and with minimum effort, choose the Cloud 2FA Service.

Using the Cloud Service, you can quickly implement two-factor authentication into your project. You do not need to worry about equipment, administrators, load distribution, and other infrastructure problems. Everything is already functional and ready for use. This solution is SAAS-based.

You pay only for what you actually use. You may suspend the services provided at any time by simply deactivating your service plan.

On-Premise Platform

If you want to have full control over the authentication system, choose the On-Premise 2FA Platform.

It is intended for installation in your environment. Using the platform will require more work on your part, but you will be rewarded with the full control over all your data and processes!

You know that the two-factor authentication platform's efficiency depends only on you and your equipment; you can create the most secure services, blocking access to the system from external sources with an army of firewalls and geeky admins.

Easy Integration Into Your Infrastructure

The Protectimus two-factor authentication solution can be integrated into your infrastructure using an API, SDK, or ready-to-use integration components for Active Directory, Winlogon, RDP, Ubuntu, macOS, RADIUS, OWA, ADFS, Roundcube, etc. Choose the solution that fits your needs or get in touch with our support team if none of the listed solutions works for you. We are always ready to customize our solutions to your requirements.

2FA for Windows & RDP
A ready-made 2FA component for Windows and RDP, it takes a few clicks to protect access to your personal or enterprise Windows accounts

2FA for Linux
Integrate Protectimus cloud service or on-premise platform with Ubuntu via RADIUS to protect your corporate Linux accounts with MFA

2FA for macOS
Protectimus MFA solution can be integrated with macOS via RADIUS to protect the macOS user accounts with two-factor authentication

2FA for RADIUS
Protectimus cloud service and on-premise platform integrate easily with any device or system that supports the RADIUS protocol

oath
initiative for open authentication
CERTIFIED

CITRIX® Ready

2FA for VPN
Connect Protectimus SAAS service or platform with any VPN service including SonicWall, Sophos, Cisco, and Azure VPN via RADIUS

2FA for Citrix
Compatibility with Citrix NetScaler and XenApp has been confirmed during testing by Citrix, as proven by the Citrix Ready badge

2FA for OWA
Set up OWA two factor authentication with a ready to use Outlook Web App 2FA plugin compatible with Exchange 2013, 2016, 2019

2FA for SSO
Set up single sign-on (SSO) additionally protected with two-factor authentication using the Protectimus SSO component

2FA for AD, LDAP, Databases
Protectimus DSPA (Dynamic Strong Password Authentication) component adds 2-factor authentication directly in AD, LDAP, databases

2FA for ADFS
Protectimus offers a ready-to-use component for strengthening authorization and authentication mechanisms in ADFS

2FA for Roundcube
Roundcube 2FA plugin enables you to easily integrate a professional MFA solution into the Roundcube webmail client

API and SDK
We provide flexible RESTful API, detailed documentation, and prepared software development kits for Java, PHP, and Python

Protectimus Winlogon & RDP

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

It protects access to the Windows computers both locally and via RDP (Remote Desktop Protocol).

- Easy to install.
- Works in offline mode. Backup code feature, which allows users to log into their local Windows accounts when their computers are offline.
- Automatic registration of users and tokens.
- Mass installation on several computers, it's possible to create and deploy an MSI through GPO (Group Policy Object).
- RDP access filtering with IP and IP access control.
- Different access policies for RDP and Winlogon.
- PIN support in Windows 10.
- Microsoft account support.
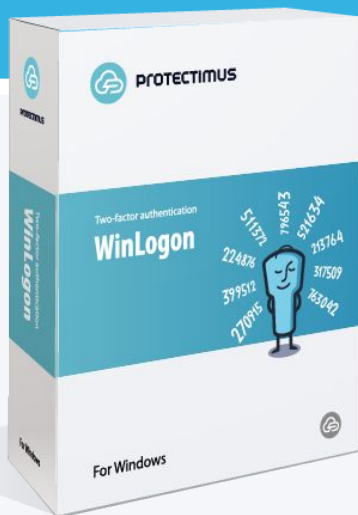
Protectimus ADFS

The Protectimus 2FA solution for Active Directory Federation Services (ADFS) is easy to integrate into your infrastructure if you use **ADFS 3.0** or **ADFS 4.0**.

For that purpose, we developed the Protectimus ADFS module with an easy-to-use installer and detailed setup instructions.

Active Directory Federation Services allows you to configure access using Single Sign-On (SSO) technology for all key web applications and cloud services used on your corporate network.

This way, through ADFS 3.0 and 4.0, you can configure Protectimus two-factor authentication for a wide variety of services, including AWS, Asana, Desk, Dropbox, Evernote, Expensify, Freshdesk, GitHub, GoToMeeting, Jira SSO, Namely, Microsoft Office 365, OpenDNS, Salesforce, Citrix ShareFile, Slack, Splunk, SugarCRM, Sumo Logic, Cisco Webex, Workday, Workplace, Zendesk, Zoom, etc.

Integrating ADFS with Protectimus will take no more than 15 minutes.

Protectimus Outlook Web App (OWA)

The Protectimus Outlook Web App (OWA) two-factor authentication solution adds 2FA to enterprise email servers running **Microsoft Exchange 2013, 2016, and 2019**.

We've created an installer that helps to set up OWA two-factor authentication in just a few minutes.

- Easy to install.
- Supports the Protectimus Users' Self-Service feature, administrators don't need to waste time assigning and issuing tokens to each OWA email user individually, they can activate the self-service feature, giving their users the ability to create and manage tokens for Outlook 2FA themselves.
- Supports all kinds of Protectimus OTP tokens.
- Supports geographic filters and time-based filters that allow you to configure OWA multi-factor authentication so that users can log into their accounts only from chosen countries at certain times of a day, for example, only during business hours.

Protectimus DSPA
(Dynamic Strong Password Authentication)

Protectimus integrates **directly with Microsoft Active Directory (or any other user directory)** to add a six-digit password onto users' static passwords. The six digits are a one-time password generated using the TOTP algorithm, so they constantly change. Active Directory users' and computers' passwords now look like this: P@ssw0rd!459812, where P@ssw0rd! is the fixed part, and 459812 is a one-time password.

The administrator sets the one-time password change interval, which can be 30 seconds or longer. The interval must be a multiple of 30 seconds. The Active Directory change password frequency can be set individually for each user. It is also possible to choose which groups of users are required to use Protectimus Dynamic Strong Password Authentication (DSPA) and which are not. The Protectimus DSPA component regularly changes users' passwords on the schedule set by the administrator. In this process, only the six final digits are changed.

Thus, Active Directory user authentication looks like this: users can gain access to their accounts by entering their fixed passwords and the one-time code all in one go. To generate OTPs, users can use the in-app one-time password generator Protectimus SMART or special hardware tokens for Protectimus DSPA.

Protectimus RADIUS 2FA

Protect your VPN, Wi-Fi, firewall, and any RADIUS supporting software with two-factor authentication.

The Protectimus RADIUS 2FA solution can be used with **any software or equipment that supports RADIUS authentication protocol** including Cisco AnyConnect, Citrix Gateway, VMware Horizon, FortiGate, SonicWALL, OpenVPN, and other similar products.

The Protectimus RProxy 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.

The Protectimus RADIUS 2FA software is easy to set up. But if you have any questions, our team is always ready to help you with deploying RADIUS two-factor authentication even in the most complex infrastructure.

- Supports the Protectimus Users' Self-Service feature.
- Supports all kinds of Protectimus OTP tokens.
- Supports geographic filters and time-based filters.
- Citrix Ready Partner.
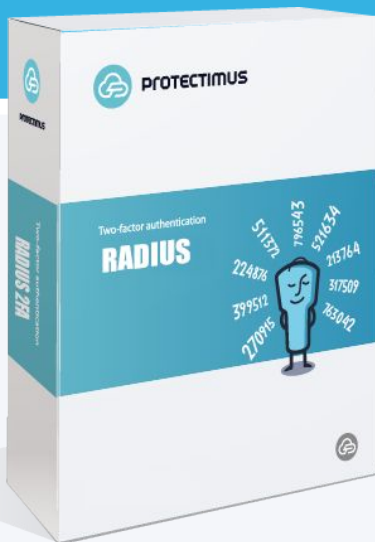
Protectimus Roundcube

Two-factor authentication is essential when protecting access to email clients.

The **Roundcube** 2-factor authentication plugin from Protectimus will help you to easily integrate a professional, OATH-certified MFA solution into the Roundcube webmail client, giving you the maximum protection against unauthorized account access.

- It takes around 15 minutes to configure two-factor authentication in Roundcube with the Protectimus 2FA plugin.
- With the Protectimus Users' Self-Service feature administrators don't need to waste time assigning and issuing tokens to each Roundcube user individually, users will create and manage their OTP tokens themselves.
- Supports all kinds of Protectimus OTP tokens: hardware TOTP tokens, the Protectimus Smart OTP app, SMS authentication, or chatbots in Telegram, Viber, and Messenger.
- Supports IP filtering.
- Supports geographic filters and time-based filters, users can log into their Roundcube accounts only from chosen countries and only during business hours.

PROTECTIMUS

OTP Tokens for Every Need and Taste

PROTECTIMUS TWO

The Protectimus TWO hardware OTP tokens are made in the form of key fobs. They are high-strength, water-resistant

PROTECTIMUS SMART

Using this token, you eliminate the necessity to physically pass the token, transport, create and assign the token

+ Support of Data Signing

PROTECTIMUS FLEX

A programmable hardware TOTP token in a key fob format. You can add a new secret key to the Protectimus Flex OTP token over NFC

PROTECTIMUS SMS

Protectimus SMS allows converting any mobile phone into an authentication device. Using this token, you save time and effort

+ Support of Data Signing

PROTECTIMUS BOT

Free OTP delivery with chatbots in messaging apps - reliable and cost-effective alternative to SMS authentication

+ Support of Data Signing

PROTECTIMUS MAIL

This token allows receiving one-time passwords at the specified email address. It is very easy to create and utilize

+ Support of Data Signing

PROTECTIMUS

oath
initiative for open authentication
CERTIFIED

CITRIX Ready

The Protectimus Slim token is easy to configure, convenient, and reliable

Secure

The programmable token Protectimus Slim mini doesn't connect to the internet or to a GSM network, eliminating the possibility of a one-time password being intercepted when delivered in an SMS, or being read by malware on a smartphone. With this OTP token, unlike standard hardware tokens, only you will know your secret key, thanks to the setup over NFC.

Universal

The Protectimus Slim mini was developed as a hardware alternative for the Google Authenticator and other OATH-compliant software tokens. It's suitable for authentication systems that support TOTP tokens: Google, Facebook, VKontakte, Dropbox, GitHub, Kickstarter, KeePass, Microsoft, TeamViewer, etc. If you're not sure whether a token is right for you, just ask us!

Reprogrammable

The Protectimus Slim mini TOTP token can be programmed over NFC an unlimited number of times. This is convenient for businesses, as it allows the same token to be re-assigned multiple times for use with different services, unlike non-programmable OTP tokens. It's convenient for clients, too, since the secret key can be changed if necessary.

Free OTP delivery with chatbots in messaging apps: a modern approach to 2FA

Easy

It's the most convenient method for receiving one-time passwords. There's no more need to pay SMS providers, buy hardware OTP tokens, or ask your users to install extra OTP generator apps. Users need only add the ProtectimusBot chatbot to their usual messaging app. And after a quick, 15-second setup process, they will receive one-time passwords and other important messages.

Saving costs

Authentication through chatbots on Telegram, Facebook Messenger, Viber and other messaging apps is completely free. It's just as easy as SMS, but it lets you avoid unnecessary costs. What's more, it's possible to combine one-time password delivery with delivery of important messages, such as information about deposits and withdrawals, allowing you to completely put an end to your SMS expenses.

Secure

Using messaging apps to deliver one-time passwords is secure. Messaging apps use reliable message encryption algorithms, and access to these apps is additionally protected by a password. On top of that, this OTP delivery method allows the use of HOTP and TOTP password generation algorithms, and supports CWYS (Confirm What You see) data-signing function, which protects data even in the event that a OTP password is intercepted by a hacker.

oath
initiative for open authentication
CERTIFIED

CITRIX Ready

Protectimus SMART

Maximum Comfort

Our wide range of tokens allows customers to choose exactly what they need and want.

No need for Internet and GSM

The process of authentication and transaction data signing is performed autonomously, without the use of the Internet and GSM, and one-time passwords are delivered without delays or any technical problems. Your customers will gladly welcome the improved authentication process.

Advantages of the Protectimus SMART Software Token:

- Available for all the main Android and iPhone platforms

Russian, English
- Ability to create several tokens on one device
- Transaction data signing without additional hassle
- Password generation algorithms: by number, by time, server response (OCRA)
- Adjustable password length: 6 or 8 characters
- Use of a check symbol to prevent errors when entering the key manually
- PIN code protection of the application
- Support of Android Smart Watch

White-Labeling Options

Two-Factor Authentication Platform

We are ready to customize all our software and OTP tokens based on a customer's brand.

A white-labeled MFA Platform will be installed in your environment. Hardware and software OTP tokens will be made in your corporate colors displaying your logo.

And even more! If you need any specific functions for the authentication system, our team can do it for you.

Protectimus SMART Application

Want application for one-time passwords generation with custom branding? We can make it for you! On your request, the 2FA application Protectimus SMART can be white-labeled and designed in your corporate style with your company logo and name.

Hardware Tokens

When ordering 1000 pieces or more, **any** Protectimus hardware tokens can be produced in your corporate style.

Use-proven solution

Citrix Ready Partner

Compatibility of Protectimus solution with Citrix products has been officially verified by experts at Citrix. On the results of the audit, Protectimus has been deemed Citrix Ready Partner. Our software is officially recommended for integration with Citrix Gateway, ADC, Virtual Desktops, and Virtual Apps.

Integration of Protectimus solution with Citrix Gateway, ADC, Virtual Desktops, and Virtual Apps is provided through the RADIUS protocol. To get a free consultation or documentation with more detailed instructions on the integration, please contact support.

OATH Certified Product

Protectimus multi-factor authentication solution is certified by the worldwide initiative for open authentication OATH.

It supports all standard OATH algorithms of one-time passwords generation - HOTP (RFC 4226), TOTP (RFC 6238), and OCRA (RFC 6287).

These algorithms were thoroughly tested and proven reliable; they have become the standard in the field of two-factor authentication.

The Data Singing feature is developed on the basis of OCRA algorithm.

And the most important: our solution is built on the principles and with the use of enterprise level components. This provides reliability and opens the possibility of flexible configuration and construction of the necessary architecture of any scale.

The advantages of Protectimus are not a marketing ploy – they are real

Individual Approach
For us, each corporate customer is unique and deserves undivided attention. Our team will take great care of you and give you the feeling of being our only customer.

Integration Assistance
To ensure an easy and simple start, Protectimus provides comprehensive support and consultations during the integration process.

Branding
To corporate customers, Protectimus can offer a comprehensive white-label solution. Our products including software and hardware tokens can be manufactured in the signature style of your company.

Customization on Request
If a customer has specific requirements and preferences in terms of the system's functionality, the Protectimus team is willing and ready to meet and implement them.

Unprecedented Security!
Support of all the standard algorithms: by event, by time and by server response, as well as transaction data signing, allow successfully overcoming even the most serious challenges.

And – the most important thing!
We offer you a possibility to begin saving now by decreasing the budget allocated for authentication and distribution of information to users. From experience, we know that using the Protectimus system allows companies to more than double the funds use efficiency.

These companies are already using Protectimus

PANVISION
Workflow management and content management system

arcus global
Building innovative cloud based products for public sector

nexa TECHNOLOGIES
Reliable solutions and services for homeland security

paysafecard
Online payments without bank account or credit card info

iPHH
Data center services and IP Connections

TARIFHAUS
Recommendations for tariffs for mobile phone, Internet, TV, etc.

GROUPE L'OCCITANE
World famous manufacturer of cosmetics and fragrance

Miami-Dade State Attorney main office

DATACENTER
Web hosting, outsourcing, and co-location services

IMsupporting
Live Chat & Support Solutions
Solution for real-time chat and online customers support

accesso
IT solutions to the leisure entertainment and cultural markets

COLLEGE of CENTRAL FLORIDA
College of Central Florida

iC.co.uk internetcentral
Internet connectivity to local, national & global businesses

EmbarkIT
Provider of IT products & services to the public sector

dbConn
Business intelligence and database solutions development

MOGO
Financial technologies: personal loans, mortgage, credit cards

gamesys
Online games development and operating

HORTONWORKS
Data management platform, Big Data analysis

Credit, check discounting, factoring, and credit card reconciliation services

The Exeter
Health care insurance and income protection

SCIENCE MUSEUM
London Science Museum

Whistle
GPS location and activity tracking for dogs and cats

GUDEN
INDUSTRIAL HARDWARE MADE EASY
Provider of industrial hardware, cabinet and door hardware

intertops
Online casino, sports bets, and multiplayer poker

TREMANI
Internet applications and information systems development

New Development Bank
Banking services, loans, mortgages, leasing

REPLIOR
Co-location, backup, complete IT operation, and document storage services

Remitly
Online money transfer services, easy transfers over seas

PEER CODE
Software engineering, web design, user experience design

think S3
Cloud solutions and services for backup, disaster recovery, and data storage

aruba.it
Design and networks installation, information security, support and IT outsourcing

VoiPlatinum
Voice over IP services specializing in Africa, Middle East & Asia Countries

Bottomline Technologies
Domestic and international business payments, efficient cash management, fraud detection

Thailand Bitcoin Exchange

SummitHEALTHCARE
Healthcare systems integration and automation

TAURUS BITCOIN EXCHANGE
Canadian Bitcoin Exchange

advcash
Universal payment system: bank

interkassa
payment acceptance system
Payment acceptance system:

STRATA PT
Business Strategies For Healthy Outcomes
Physical therapy billing and

sicim
The leading network of