PROTECTIMUS

DSPA for LDAP/AD

Dynamic Strong Password Authentication

DSPA component allows you to apply the strong authentication principles to a standard one-factor infrastructure based on static passwords. It protects accounts right in the user directory (AD/LDAP, DBMS).

The Protectimus DSPA component installed on the client's premises changes users' passwords on a schedule. Passwords are composed of two parts: a static part, specified by the user, and a dynamic part, a one-time password generated using the TOTP algorithm.

Protectimus Solutions LLP
HQ: 8-12 New Bridge Street,
London, England, UK
R&D office: 23 Sumska Street,
Kharkiv, 61057, Ukraine

Protectimus USA LLC
18431 NE 28th Ave,
Aventura, Fl 33160, USA

www.protectimus.com
sales@protectimus.com

What problems does Protectimus DSPA solve?

1. Existing multi-factor authentication solutions protect only part of the Infrastructure

All standard MFA solutions add two-factor authentication only to endpoints. This leaves hackers a chance to attack your infrastructure bypassing two-factor authentication and calling your user directory straightforward.

For example, it's possible to call Active Directory via the Windows command line, and it's enough to know user login and password to perform an action on their behalf.

Using Protectimus DSPA to enable system protection, you can be certain that nobody will have access to AD, LDAP or user accounts in your database without a dynamic password, no matter where the request comes from or is directed.

2. Administrators need to install and support 2FA plugins on multiple platforms

Now, to configure two-factor authentication for all employees and all the services that the company uses, the administrator must implement several 2FA plugins for different platforms and install additional software on each client machine. Moreover, all this software needs to be constantly updated.

After integrating the Protectimus DSPA component with Active Directory, 2-factor authentication dynamic passwords will be required on all services connected to AD (Winlogon, RDP, ADFS, OWA, etc.)

www.protectimus.com
sales@protectimus.com

How does it work?

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; a chatbot on Telegram, Viber, or Facebook; or special hardware tokens for Protectimus DSPA.

PROTECTIMUS

www.protectimus.com
sales@protectimus.com

What is Protectimus DSPA?

Scheduled password changes

The Protectimus DSPA component for Active Directory two-factor authentication regularly changes users' passwords in AD. The administrator specifies the password change interval. In this system, passwords are composed of two parts: a static part (specified by the user) and a dynamic part (a one-time password generated using the TOTP algorithm). The resulting passwords look like this: P@ssw0rd!459812.

On-premise platform

The Protectimus DSPA component for Active Directory security and Protectimus two-factor authentication platform are installed on the client's premises. You can manage all the data and processes yourself to ensure the maximum level of infrastructure security. The Protectimus on-premise platform is designed for multidomain environments. It also offers cluster, replication, and backup features.

Hassle-free administration

Unlike traditional MFA solutions, Protectimus DSPA frees administrators from the need to install additional software on client machines and update it periodically. After integrating the Protectimus DSPA component with Active Directory, multi-factor authentication passwords will automatically be required to log into all systems connected to Active Directory MFA (Winlogon, RDP, OWA, etc.)

Protectimus DSPA (Dynamic Strong Password Authentication) is the first database security solution that provides two-factor authentication for account protection directly in Active Directory and other user directories (LDAP, databases).

PROTECTIMUS

oath initiative for open authentication CERTIFIED

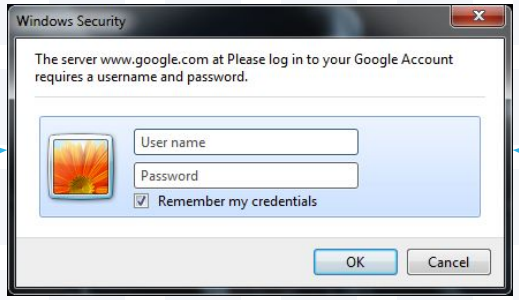
CITRIX Ready

PROTECTIMUS

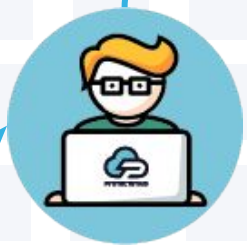
DSPA for LDAP/AD

Dynamic Strong Password Authentication

The password looks like:
P@ssw0rd!459812



Standard WinLogon window



Users get access by entering their password and a one-time code from the Protectimus Smart OTP app on their smartphone

Active Directory

Any user directory, for example, LDAP or database

Scheduled password change (5 min)

Protectimus Smart mobile app

Protectimus on-premise platform with DSPA component

PROTECTIMUS

oath initiative for open authentication CERTIFIED

CITRIX Ready

www.protectimus.com
sales@protectimus.com

OTP tokens to choose from

Protectimus Smart OTP app

The free Protectimus Smart OTP app for two-factor authentication is available for iOS and Android. When creating a new TOTP token, users can set their desired time interval in multiples of 30 seconds. This makes it possible to use the Protectimus Smart software token for two-factor authentication in Active Directory with Protectimus DSPA.

Messaging chatbots

One-time password delivery is available through the Protectimus Bot chatbots on Telegram, Viber, and Facebook Messenger. This type of software token is also available at no cost. It allows administrators to configure TOTP-based one-time password generation with any time interval. That makes these chatbots an excellent means of authentication for Protectimus DSPA.

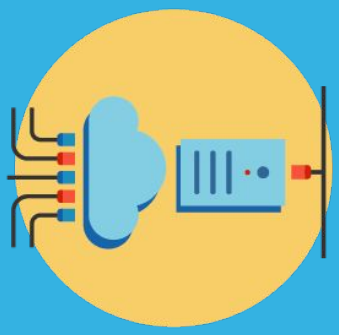
Hardware tokens

Currently, hardware TOTP tokens with 30- and 60-second one-time password generation intervals are available to Protectimus customers. Classic TOTP tokens with extended time intervals (600 seconds), as well as programmable TOTP tokens with support for adding your own secret key and time interval (over 60 seconds), are also in development

PROTECTIMUS

www.protectimus.com
sales@protectimus.com

Protectimus is a powerful ecosystem for building strong authentication



On-premise platform

The Protectimus on-premise platform supports multidomain environments. Clustering, replication, and backup features are also available. Using the on-premise platform gives you total control over the data, processes, and fault tolerance of the system, as well as the server's level of protection against attacks. You can build a security system around your authentication server to your own specifications. You can use any firewall, close off the server completely to outside access, and use any other security measures you desire.

Before installing the Protectimus auth platform on your server, Java (JDK version 8) must be installed, as well as the PostgreSQL DBMS, version 10 or later.

Private cloud

Protectimus two-factor authentication server can be also deployed in the client's private cloud. no matter where the platform is installed, either in your environment or in the private cloud, it supports multidomain environments, clustering, replication, and backup features, as well as it gives the client total control over sensitive data and processes.

Before installing the Protectimus authentication platform on the private cloud, make sure the cloud infrastructure you set up fulfills the following technical specifications: Instance type: 2 Core (CPU), 8 GB (MEM); OS for all Instances: Linux; Cloud Disk: 100GB/per month for each Instance; Network Traffic: 1000GB/per month; Load Balancer.

oath initiative for open authentication CERTIFIED

CITRIX Ready

PROTECTIMUS

How to set up?

Install the platform and the DSPA component

The Protectimus authentication platform and DSPA component are available upon request, please contact support@protectimus.com.

Create a user

In the Users tab, choose Add User. Choose LDAP User as the user type. The user's login must match the user's CN in the directory service.

Create a resource

In the Resources tab, choose Add Resource. Choose LDAP Resource as the resource type.

Assign a user to a resource

In the Resources tab, click Assign, then User. Only LDAP users can be assigned to an LDAP resource.

Activate self-service

Click on the Resource name, navigate to the Self-Service tab. Enable self-service and specify its address. Your users will need to authenticate on self-service with their login (CN) and OTP (sent by email) to issue the tokens and create the passwords, identical to their passwords in AD.

www.protectimus.com
sales@protectimus.com

Key Features

Secure

- The system is based on the principles of strong authentication.
- The DSPA component protects accounts directly in the user directory (AD, LDAP, databases)
- The authentication server and DSPA component are located in the company environment.
- Time-based One-time Password Algorithm (RFC 6238) is used to generate the dynamic part of the passwords.
- Domain Controller Level Authentication.

Easy to use

- There is no need to install additional software on end-user machines.
- One-time passwords are generated with the help of a free application Protectimus Smart OTP.

Protectimus Solutions LLP
HQ: 8-12 New Bridge Street,
London, England, UK
R&D office: 23 Sumska Street,
Kharkiv, 61057, Ukraine

Protectimus USA LLC
18431 NE 28th Ave,
Aventura, Fl 33160, USA

PROTECTIMUS