Welcome to Protectimus

Developer's Introductory Guide for 2FA Implementation

Ver. 1.0.0 EN
05 Dec 2024

Contents

Welcome to 2FA Integration with Protectimus

We are happy to welcome the specialists tasked with the implementation of two-factor authentication with the purpose of ensuring secure protection of a resource or a project from unauthorized access. Here you can find all the basic information on the process and available variants for the integration with Protectimus. Using the relevant links, you will access documents that contain detailed information on all aspects of the integration process. First of all, let us review the key terms:

- **Authentication** is a process of verifying a user's identity, i.e. verifying whether or not a user is the person that this user claims to be.
- **One-Time Password (OTP)** is a password that is valid for only one authentication session.
- **Token** is a device or software for generating one-time passwords.
- **Resource** is a project or a system that needs to be protected with two-factor authentication. It serves the purpose of grouping of users and tokens, and defining the general rules for obtaining access to the system. For example, you have two websites: an online store and your company's website. You need to create two resources that will represent these two websites to divide their users and specify access rules.

Understanding the principles of our system's operation will make the integration process faster. Let us review the main principles.

General Rules

- A user may have many tokens assigned to it, but a token may only be assigned to one user.
- If a token is deactivated, it will not be involved in the authentication process. Consequently, if your user loses a token, and you need to provide access to this user, you simply need to deactivate the lost token, and this user will be able to login with its password. It is important not to confuse this with locking, which will not allow a user to be authenticated with this token.
- For you to be able to authenticate users through the API, your account must have an activated service plan.
- The user that registered in the system first and invited all other administrators is the chief system administrator (or the superuser).

Administration

- A system may be managed by several administrators; The chief system administrator (or the superuser) can perform all actions in the system, except for editing and deleting tokens that are used by other administrators to access the system.
- All other administrators have access to the system within the resources to which they are assigned and to which they are allowed access. Besides, administrators can see the current balance but have no access to the financial module; they cannot change a service plan, but they can see the history of funds credited and debited to an account.
- All administrators have access to users, tokens, and filters, but they can only be deleted by the chief system administrator (or the superuser) or the administrator that created them.

User Authentication on Your Resource

User authentication is always performed for a specific resource; therefore, a user must be assigned to the resource to which this user should have access. If a user is not assigned to a resource, this user will have no access to this resource. The method of assigning a user to a resource depends on the authentication method chosen by you. Protectimus supports several user authentication methods:

1. **User authentication with a static password.** This method requires that a user should have a password, and that this user should be assigned to the resource for which authentication is performed.

   Note: *In essence, this method is one-factor authentication.*

   Note: *Protectimus will ensure secure storage of your users' passwords and will not use them for any purpose other than their intended purpose. You can find detailed information about this on the PRIVACY POLICY page.*

2. **User authentication with a one-time password.** This method requires that a user should have a token, and that this user should be assigned to a resource WITH this token. This method will not work if a user and a token are assigned to a resource separately from each other.

3. **User authentication with a static password and a one-time password.** It is a combination of the two methods described above. A user must be assigned to a resource WITH a token. This user must have a password. If a user's token is deactivated, OTP authentication will not be performed, in which case only this user's static password and this user's compliance with the filters' requirements, if any, will be authenticated.

4. **Token authentication on a resource.** This method allows you not to assign a token to any specific user, but simply to verify the validity of a one-time password generated. This method requires that a token should be assigned to a resource.

   Note: *During authentication, it is verified, among other things, whether or not a request meets the requirements of the filters on this resource.*

   Note: *If a user's authentication is not successful because this user enters an incorrect OTP, the value of the counter of failed authentication attempts for this token will be increased. When the threshold of failed authentication attempts for the specified resource is exceeded, a token will be locked. A token can be unlocked either through the web interface or through the API (the Editing Token method). If a user's authentication is successful, the counter of failed authentication attempts is reset to zero if it has not exceeded the allowable limit for this resource, and if this user has not yet been blocked.*

Integration

To integrate Protectimus into your project, you can use these two methods:

1. **Integration using pre-built integration components.** Easily integrate with popular systems like Active Directory, ADFS, OWA, Office 365, Windows & RDP, RADIUS-supported devices, software, and VPNs such as Cisco AnyConnect and FortiGate. Detailed integration guides are available on our website.
2. **Integration using the API.** For integration through the API, we provide a set of auxiliary libraries for the following programming languages: Java, Python, and PHP. If there is no client for your programming language, you can use detailed descriptions of all the API methods using this link.
3. **Integration using the IFrame Widget.** You can find the IFrame Widget Setup Instructions using this link.

Note: *For your convenience, on the service's home page you can find a list of actions to be performed for the integration with our service. Use this list for reference to make sure that you did not forget to perform any action.*

Contacts

Technical questions, software distribution and any help:

support@protectimus.com

Partnership, sales, business opportunities:

sales@protectimus.com

Call us:

Ireland: +353 19 014 565

USA: +1 786 796 66 64

Corporate Information

Protectimus Limited

Carrick House

49 Fitzwilliam Square

Dublin 02, N578

Ireland