



## Administrator's guide

Protectimus 2FA Platform Integration  
using RADIUS protocol

Ver. 1.0.4 EN  
12 May 2021

# Contents

Integration process / deployment of software solution	3
Protectimus authentication server	4
Getting started with Protectimus SAAS Service	4
Getting started with Protectimus On-Premise Platform	4
Working with the Protectimus system	5
Resources	5
API key	6
API activation	6
Protectimus RProxy configuration	7
How to install system updates	10
Contacts	11
Corporate Information	11

## Integration process / deployment of software solution

One of the possible ways to interact with Protectimus is by means of the RADIUS protocol.

Solution integration consists of setting up and configuring Protectimus RProxy, as well as configuring any other devices or applications which support RADIUS protocol.

Configuring authentication policies allows the transmission of an authentication request over the RADIUS protocol, which is then received and processed by the Protectimus RProxy component. Having received the request, the RProxy component, in turn, contacts the Protectimus authentication server to verify the one-time password supplied by the user.

There are several methods of delivery of the Protectimus authentication server. To expedite the process of establishing reliable authentication, provide free trials, and just to put the figurative burden on "other people's shoulders," we've designed a service using the SaaS model.

Installation of the Protectimus platform on your own hardware is a second option. This option allows you to implement authentication in an isolated environment.

If necessary, Protectimus specialists can also prepare an individualized cluster in the cloud, according to the client's needs.

The functionality of the system is preserved, regardless of which server placement option you choose. To switch from one option to another, all that's needed is to change a few settings, connecting to the API at its new address.

Next, a more detailed overview of the integration process.

## Protectimus authentication server

There are two options in the distribution of Protectimus Authentication Server:

- **Service** - a cloud-based (SaaS) solution, which enables you to have an easy start and to maintain the authentication infrastructure effectively.
- **Platform** - on-premises solution for installation in the customer's environment to handle all the processes. The authentication platform and instructions on its installation are available upon request from Protectimus support, at the following email address: [support@protectimus.com](mailto:support@protectimus.com).

**Note!** We suggest starting testing with cloud service to speed up integration processes. Switching between cloud and on-premise servers is as simple as changing a few strings in the configuration file.

### Getting started with Protectimus SAAS Service

To register in the Service open the registration page <https://service.protectimus.com>, fill out the registration form and click "Register". The confirmation email will be sent to the provided email address. After clicking the link in the email your address will be confirmed and you will be able to use Protectimus cloud-based authentication Service.

### Getting started with Protectimus On-Premise Platform

If you need to have all the components of a two-factor authentication system in your infrastructure, our solution is also available as an On-Premise platform that is installed on the client's premises or in a client's private cloud.

You can download the Protectimus On-Premise Platform and instructions for installing it on Windows here: <https://www.protectimus.com/platform/>

Instructions for deploying the Protectimus two-factor authentication platform on other operating systems are available upon request to Protectimus support at [support@protectimus.com](mailto:support@protectimus.com).

## Working with the Protectimus system

### Resources

Resources are used to logically group users and tokens, and to easily manage them. To create a resource, click the "Resources" button in the menu on the left, and then click the "Add resource" button in the table header. This will take you to the resource adding page, where you'll need to specify just a name for the resource and other parameters, if desired.

**PROTECTIMUS** Service Plan: Custom Deposit in Account FAQ

Dashboard Users Tokens Resources Filters Administrators Message templates Statistics Payments Debiting account Events

**+ Add Resource** Balance 1390.36 \$ Days of Service 79

Home Resources Add Resource

Resource Name: MyResource

Allowed IP Addresses: Add IP ⚠ IP Address List to Access API

IP Verification is Enabled: ☐

Number of Unsuccessful Login Attempts before Locking: 3

Enabled: ☒ ⚠ Activate access to this resource through the API; if this parameter is disabled, authentication will not be possible on this res

Save Cancel

After creating the resource, you'll be taken to a page with a list of available resources, where you can see the resource you've just created. In addition, the ID of the resource will be displayed in the table; you'll use it in Protectimus's connection settings.

**PROTECTIMUS** Service Plan: Custom Deposit in Account



Dashboard Users Tokens Resources Filters Administrators Message templates

**Resources** Balance 1390.36 \$

Home Resources

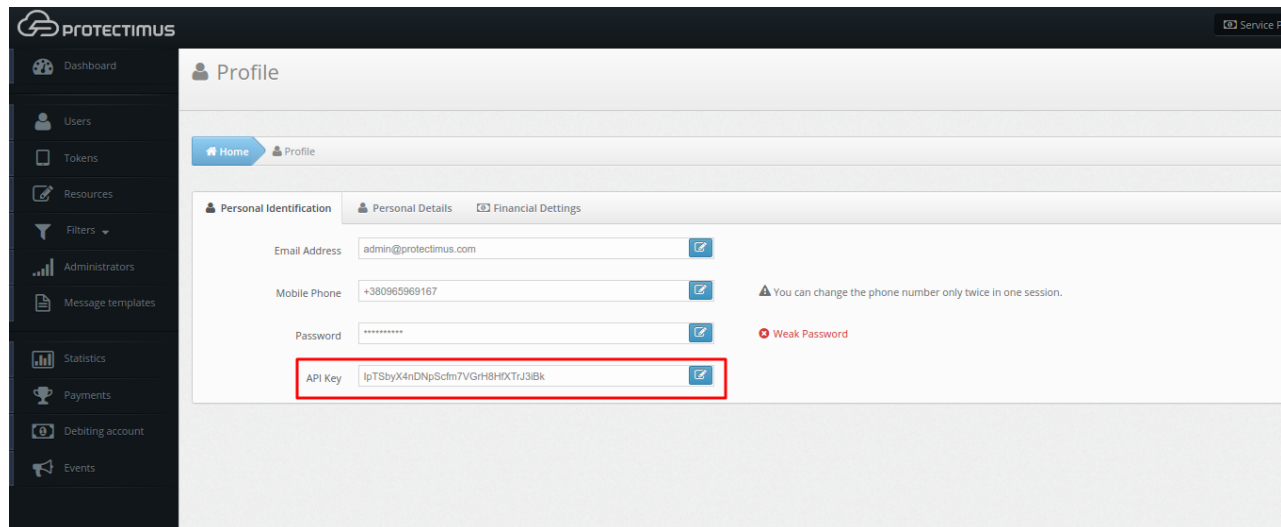
The resource has been successfully created.

+ Add Resource

Id	Name	Enabled	Creator	Filters	Action
268	MyResource	<input checked="" type="checkbox"/>	brezanov@gmail.com		Assign  

## API key

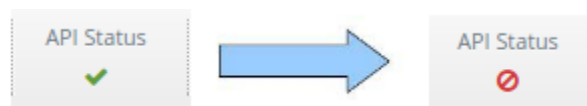
To connect to Protectimus, you'll also need an API key, which is located in the user profile. In order to access a user profile, click the user's login in the top right corner of the interface, and choose the "Profile" entry from the drop-down list.



## API activation

When using the SaaS solution, you'll need to activate a payment plan for the API. To do so, navigate to the "Payment plants" page at <http://service.protectimus.com/pricing> and activate the plan you'd like to use. Your account won't be charged until you activate a plan, but you won't be able to use the API until you do so. You can also deactivate a payment plan at any moment, if for some reason you won't need to use the service for more than one day. When you deactivate a plan, a one-time fee is charged to your account for that day, according to the rates in the active plan. When a plan is active, you'll be charged once per day automatically.

After activating a payment plan, the API status icon will change to the "enabled" state, indicating that the service is ready for operation through the API.



The Protectimus system is ready for use. SMS and email user authentication tokens will automatically be created when a user logs in for the first time. Other kinds of tokens can also be used after creating them on the Protectimus server. To receive additional information about the use of other kinds of tokens, contact Protectimus customer service.

## Protectimus RProxy configuration

To receive the latest version of Protectimus RProxy, contact Protectimus customer [service at support@protectimus.com](mailto:support@protectimus.com).

For RProxy to function, Java 8 must be installed. RProxy can be started using the following command:

```
java -jar RProxy.jar
```

RProxy settings can be configured by specifying them in the **rproxy.properties** file, which must be located in the same directory as the executable.

Set the following values in the **rproxy.properties** file:

RADIUS settings	
<code>rproxy.radius.secret</code>	The secret to be used by your authentication proxy server and your RADIUS server.
<code>rproxy.radius.port</code>	The port where the RADIUS server will run.
<code>rproxy.re-enter-otp</code>	When this property is enabled ( <code>rproxy.re-enter-otp = true</code> ), password is not requested after an unsuccessful OTP check.

Configuring the First Authentication Factor Check (Static Password)			
<code>primary-authenticator</code>	<p>This property specifies where exactly the user's static password will be checked.</p> <p>Possible options:</p> <ol style="list-style-type: none"><li>1. PROTECTIMUS - the static password verification will be carried out by the PROTECTIMUS system.  <code>primary-authenticator = PROTECTIMUS</code></li><li>2. LDAP - the static password verification will be carried out on the LDAP (AD) side. To do this, you need to use the appropriate properties:</li></ol> <table><tr><td><code>ldap.url</code></td><td>The hostname or IP address of your domain controller.</td></tr></table>	<code>ldap.url</code>	The hostname or IP address of your domain controller.
<code>ldap.url</code>	The hostname or IP address of your domain controller.		

	<code>ldap.search-base</code>	The LDAP DN of Group or organizational unit containing all of the users you wish to permit to log in.
	<code>ldap.account-name</code>	The username of a domain account that has permission to bind to your directory and perform searches.
	<code>ldap.account-password</code>	The password corresponding to domain account
	<code>ldap.query-attribute</code> <code>ldap.principal-attribute</code>	If you want to authenticate user with "sAMAccountName" instead of "userPrincipalName", specify the attributes "query-attribute" and "principal-attribute" accordingly
<p>3. If static password verification is not required (for example, the service supports the N factor), leave the property empty. In this case, only the OTP password will be checked.</p>		

Setting up connection to the PROTECTIMUS service	
<code>protectimus.login</code>	You login in the PROTECTIMUS system.
<code>protectimus.api-key</code>	You API key in the PROTECTIMUS system.
<code>protectimus.resource-id</code>	ID of the resource that you created in the PROTECTIMUS system.
<code>protectimus.api-url</code>	<p>If you are using the PROTECTIMUS cloud service, specify the following API URL: <code>https://api.protectimus.com/</code></p> <p>If you are using the Protectimus on-premise platform, the API URL will be something like: <code>protectimus.api.url=http://127.0.0.1:8080/</code></p>



protectimus.username. normalization	When normalization is enabled any domain information is stripped from the username, so "username", "DOMAIN\username", and "username@domain.com" would all resolve to a single "username"
----------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### An example configuration file:

```
#-----RADIUS Server-----
rproxy.radius.port = 1812
rproxy.radius.secret = secret
rproxy.re-enter-otp = true
primary-authenticator = LDAP

#-----Protectimus API-----
protectimus.login = test@protectmus.com
protectimus.api-key = apikey
protectimus.resource-id = 1
protectimus.api-url = https://api.protectimus.com/
protectimus.username.normalization = true

#-----LDAP-----
ldap.account-name = cn=user,dc=example,dc=com
ldap.account-password = password
ldap.url = ldap://localhost:389
ldap.search-base = dc=example,dc=com
ldap.query-attribute = sAMAccountName
ldap.principal-attribute = userPrincipalName
```

Now you need to configure your device or application to communicate with RProxy service over RADIUS protocol.

Use `rproxy.radius.port` and `rproxy.radius.secret` for configuration.

## How to install system updates

To update the system, request a new version of the software. Afterwards, to update the platform, replace the WAR archive in the TOMCAT\_HOME/webapps folder with the one you received, if working with a servlet container; or the one in PLATFORM\_DIR if working with Jetty. After replacing the WAR archive, restart the application server.

To update RProxy, simply request a new version, as before. Replace the existing JAR archive with the new one you receive. Restart.

## Contacts

Technical questions, software distribution and any help:

[support@protectimus.com](mailto:support@protectimus.com)

Partnership, sales, business opportunities:

[sales@protectimus.com](mailto:sales@protectimus.com)

Call us:

Ireland +3 537 688 899 22

United Kingdom: +44 20 3808 7124

USA: +1 786 796 66 64

Ukraine: +38 057 706 21 24

Russia: +7 499 677 16 34

## Corporate Information

Protectimus Limited

Carrick House

49 Fitzwilliam Square

Dublin 02, N578

Ireland