Administrator's guide

SAAS Service / On-Premise Platform

Ver. 1.0.0 EN
of 13 april 2020

Contents

1. Protectimus Authentication Server Setup

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

- **Service** - a cloud-based (SaaS) solution, which enables you to have an easy start and effective maintaining of authentication infrastructure.
- **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.

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

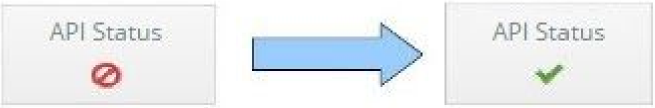
To register in the Service open the registration page https://service.protectimus.com, fill out the registration form and click Register. The confirmation email will be sent to the provided email address. After clicking the link in the email your address will be confirmed and you will be able to use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

2. API Activation

Activate API in the Service

When using the Service, you'll need to activate a payment plan for the API. To do so, navigate to the "Service plans" 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.



API activation and license in the Platform

To get the licence visit licensing page (http://platform_path/licensing), choose the appropriate volume of service and get the licence key. Using this key you will be able to pay the licence or receive the demo licence from Protectimus.

After receiving the licence file download it to the server and put a path to it in the configuration file **protectimus.platform.properties** in **licence.file.path parameter**. Restart your application server to accept the changes.

3. How to Get Started (Basic and Additional Settings)

Basic settings, required for the operation of Protectimus two-factor authentication Service or Platform, include:

1. Adding Resource
2. Adding Users
3. Adding Tokens
4. Assigning Tokens to Users
5. Assigning Tokens with Users to a Resource

Also, some additional features are available. They allow:

- Adding Administrators
- Adding and assigning Geographic and Time Filters
- Setting up Intelligent Identification
- Setting up Notifications about important events
- Changing security settings for your own account in Protectimus Service

PLEASE NOTE!

1. Depending on the chosen model, a user may be authenticated with a static password, a one-time password, or both a static password and a one-time password. For a user or a token to be authenticated, this user or token has to be assigned to the requested resource (if both a user and a token are authenticated on a resource simultaneously, this user has to be assigned to this resource with this token). See the section Assigning Users and Tokens to Resource for more information on possible methods of user authentication.

2. To facilitate the task of the administrator the system offers a user self-service mechanism which allows users to independently perform a number of actions related to issuing and managing their tokens and their own data. See the section User's Self-Service Portal for more information on setting up the User’s Self-Service Portal and it’s features.

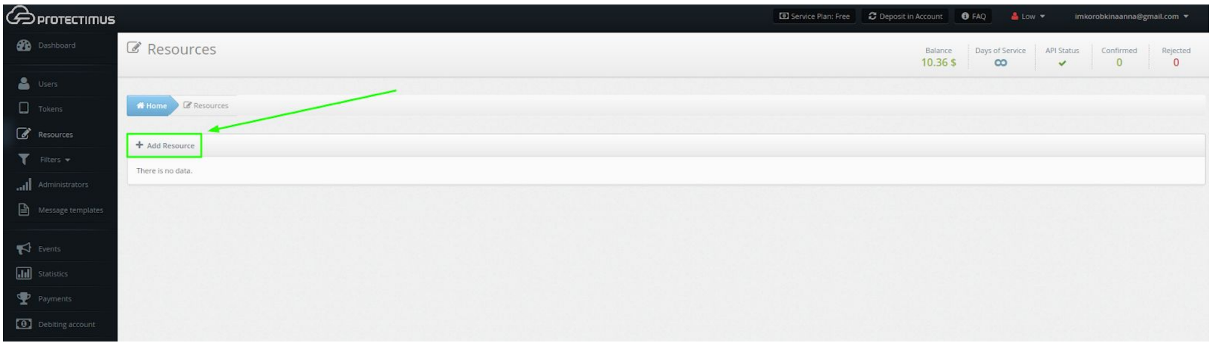
4. Resources

A Resource serves as a means to group Users and provides flexible possibilities for delegating authorities and responsibilities. A Resource may be a web project, a portal, an application, or a department of your employees. The chief system administrator may add other Administrators to the system and assign them to specific Resources. Such regular Administrators may only perform actions within a Resource to which they are assigned, but they may see all Users and all Tokens existing in the system, regardless of whether or not they are assigned to the Resources under this Administrator's management.

The number of Resources (projects) that you may create depends on the Service Plan you select. If you need to create more Resources, please select the desired or required number of Resources by customizing your Service Plan. Only the chief system administrator can change a Service Plan, deposit funds in the account, and view payment statistics.

How to Add a Resource

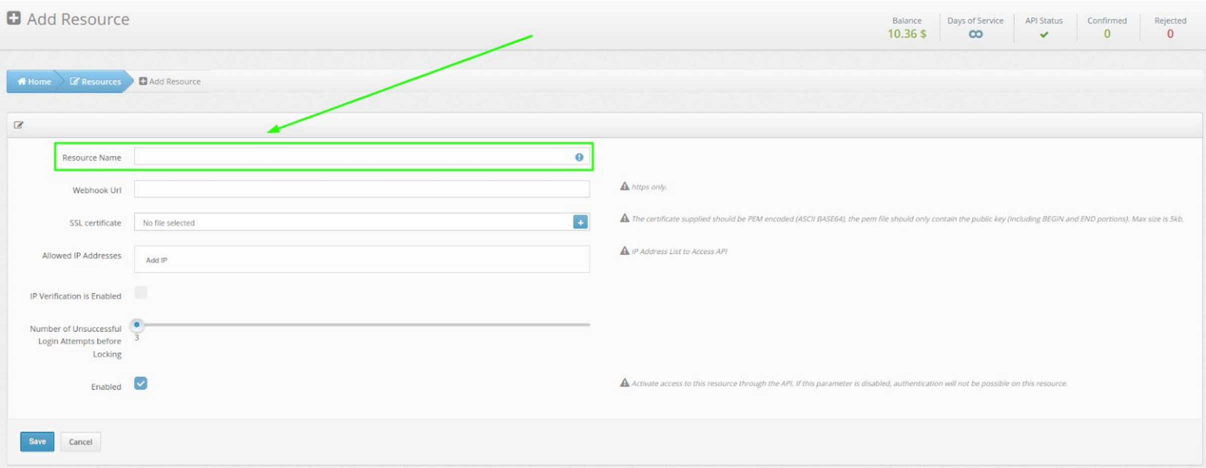
To create a Resource, click the **Resources** button in the menu on the left, and then click the **Add Resource** button in the table header.



Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

There is no data.

This will take you to the Resource adding page, where you'll need to specify just a **Resource Name**, the remaining parameters are optional.



Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Resource Name

Webhook Url — *https only.*

SSL certificate: No file selected — *The certificate supplied should be PEM encoded (ASCII BASE64), the pem file should only contain the public key (including BEGIN and END portions). Max size is 5kb.*

Allowed IP Addresses: Add IP — *IP Address List to Access API*

IP Verification is Enabled ☐

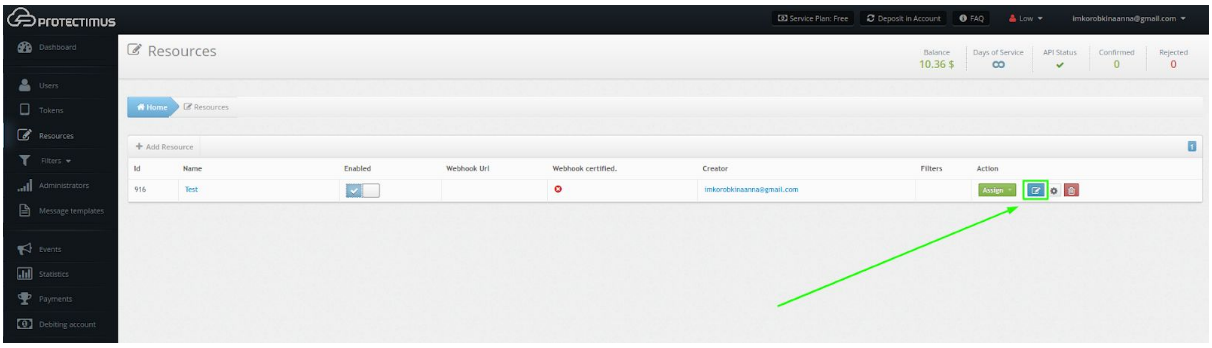
Number of Unsuccessful Login Attempts before Locking: 3

Enabled ☑ — *Activate access to this resource through the API. If this parameter is disabled, authentication will not be possible on this resource.*

- **Webhook URL**. Whenever there is an update for the Resources, we will send a POST request containing a JSON update to the specified webhook URL. In case of an unsuccessful request, we will give up only after a reasonable amount of attempts. Currently, webhook is used to receive the result of INTERACTIVE authentications. INTERACTIVE authentications are supported by Protectimus Bot token.
- **SSL certificate**. The public key certificate certifies the belonging of the public key to the indicated webhook. The certificate supplied should be PEM encoded (ASCII BASE64), The pem file must contain only the public key beginning with "-----BEGIN CERTIFICATE----- " and end with "----- END CERTIFICATE -----"
- **Allowed IP Addresses**. Allows you to restrict access to the system only from trusted IP addresses.
- **IP Verification is Enabled**. Enables the restriction of access to the system only from trusted IP addresses.
- **Number of Unsuccessful Login Attempts before Locking**. The value of this parameter should be specified between 3 and 10. If a User or Token is not authenticated successfully, the number of failed authentication attempts will be increased for this User. When the threshold number of failed attempts for the specified Resource is exceeded, this User will be locked. A User can be unlocked through the web interface or the API (the edit user method). If a User is authenticated successfully, the number of failed authentication attempts will be set at zero, if the threshold number of failed attempts for the specified resource is not exceeded, and if this User has not yet been locked.
- **Enabled.** Allows you to enable or disable the Resource.

How to Edit a Resource

To edit a Resource, click **Resources** in the menu on the left, select the desired Resource and click on the **blue button on the right**. You will be taken to the Resource settings page where you can make changes.



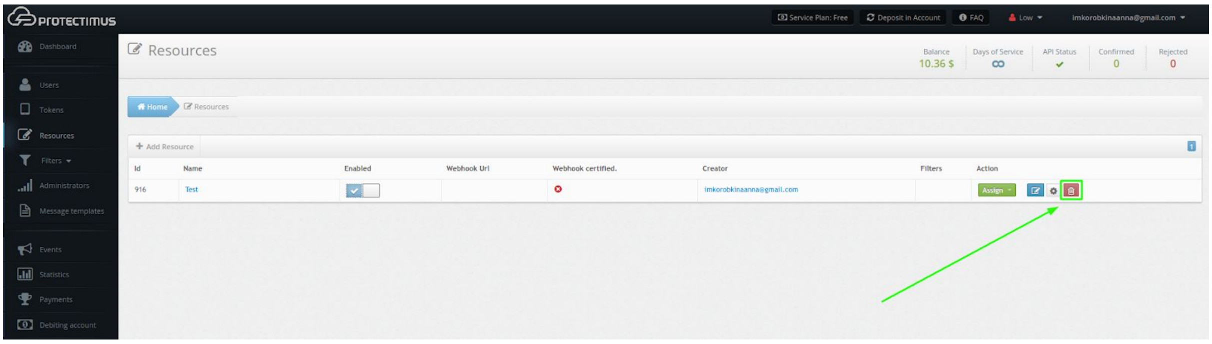
Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Id	Name	Enabled	Webhook Url	Webhook certified.	Creator	Filters	Action
916	Test	✓		⊗	imkorobkinaanna@gmail.com		Assign

How to Delete a Resource

A Resource may be deleted only by the Administrator who created it or by the chief system administrator.

To delete a Resource, click **Resources** in the menu on the left, find the Resource you are going to delete, click on the **red button with the image of the bin** and confirm the action.



Id	Name	Enabled	Webhook Url	Webhook certified.	Creator	Filters	Action
916	Test	✓		☒	imkorobkinaanna@gmail.com		Assign

5. Users

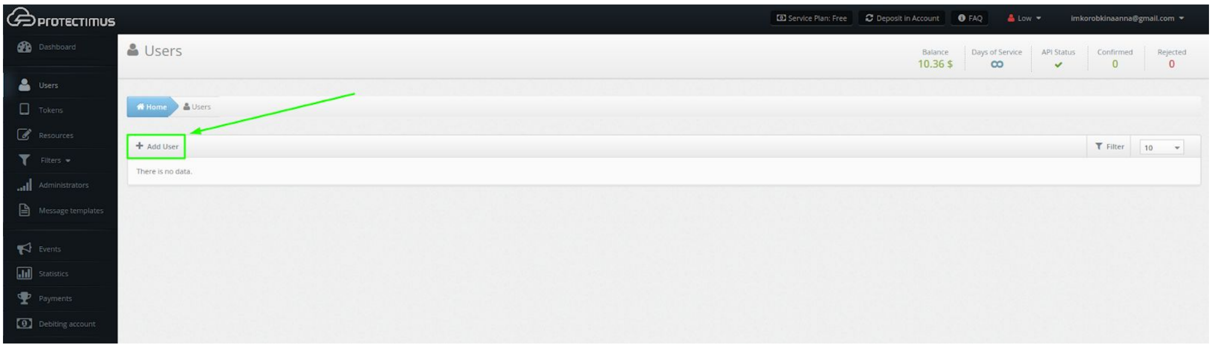
You may store a certain set of data on your Users in Protectimus system (first name, last name, email address, phone number), but the key parameter is a User’s Login (username).

You can add the Users manually, but the system also offers a User’s Self-Service mechanism. It is set up for every Resource separately; it can be done in the Self-Service tab on the page containing a Resource’s detailed information. See the section User's Self-Service Portal for more information on setting up the User’s Self-Service Portal and it’s features.

The number of Users that you may add depends on the Service Plan you select. If you need to add more Users, please select the desired or required number of Users by customizing your Service Plan. Only the chief system administrator can change a Service Plan, deposit funds in the account, and view payment statistics.

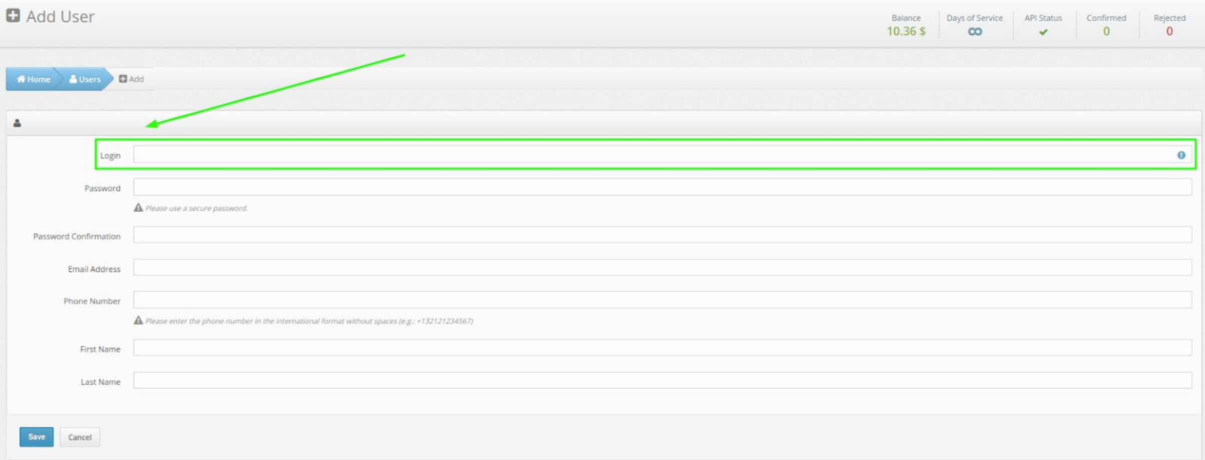
How to Add Users

To add a User, click the **Users** button in the menu on the left, and then click the **Add User** button in the table header.



There is no data.

This will take you to the User adding page, where you'll need to specify **Login** and other parameters if desired. The User Login must contain only **Latin characters, numbers, and the following symbols: _-@∾!#%+.$.** Spaces and any other symbols are not allowed.



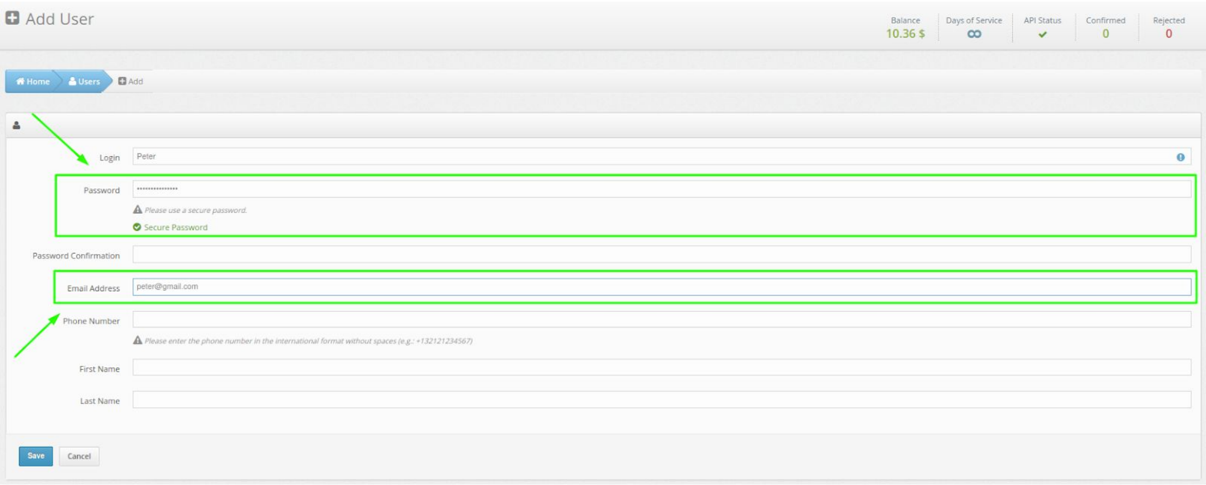
Please use a secure password.

Please enter the phone number in the international format without spaces (e.g.: +132121234567)

PLEASE NOTE!

If you plan to activate the registration of Tokens through the Self-Service Portal, Users must additionally have a **password** in Protectimus system or an **email address** on record. A verification code will be sent to the registered email address to allow Users to log into the portal. If a User has both a password and a registered email address, that User will use the password to log in. After a Token is issued for a User and assigned to a Resource, the User will also be asked to input an OTP password from the Token when logging in.

Some add-on components, such as Protectimus RProxy, can automatically create Users that are preconfigured to use the Self-Service Portal. Detailed instructions for setting up a User's Self-Service Portal with notes for integrations through the RProxy component are available here.



Add User

Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Home > Users > Add

Login	Peter
Password	•••••••••••••••
Password Confirmation	
Email Address	peter@gmail.com
Phone Number	
First Name	
Last Name	

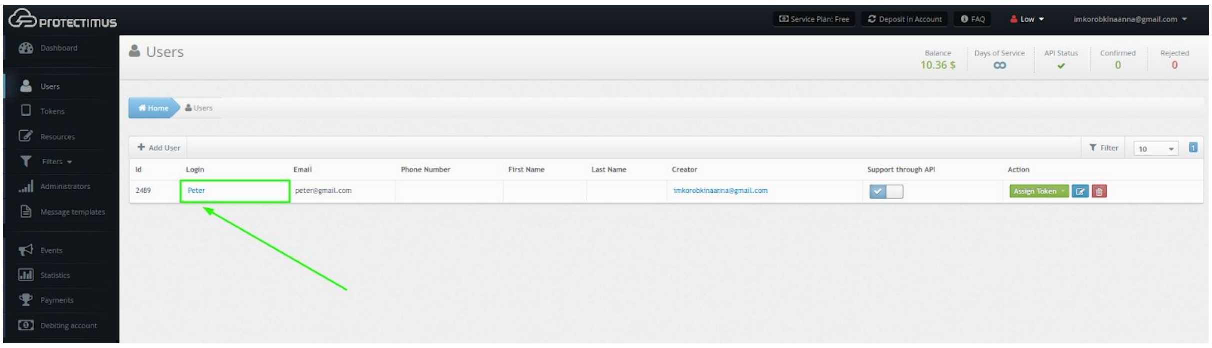
Please use a secure password.

✓ Secure Password

Please enter the phone number in the international format without spaces (e.g.: +132121234567)

How to Edit Users

To edit a User information, click the **Users** button in the menu on the left, find them in the list of Users and click the User's **login**. After doing so, you'll be taken to the page for viewing User’s detailed information.



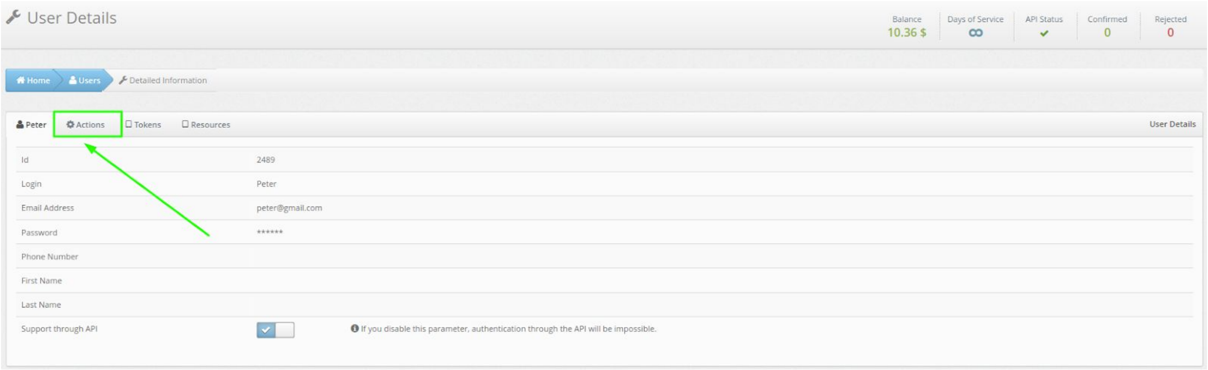
Users

Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Home > Users

Id	Login	Email	Phone Number	First Name	Last Name	Creator	Support through API	Action
2489	Peter	peter@gmail.com				imkorobkinaanna@gmail.com	✓	Assign Token

Next, navigate to the **Actions** tab.



User Details

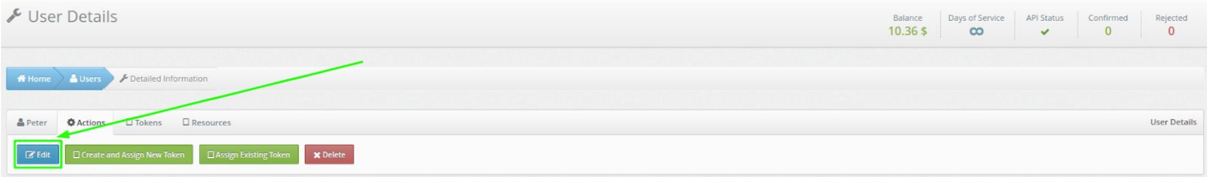
Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Home › Users › Detailed Information

Id	2489
Login	Peter
Email Address	peter@gmail.com
Password	******
Phone Number	
First Name	
Last Name	
Support through API	☑

If you disable this parameter, authentication through the API will be impossible.

Click the **Edit** button, make any necessary changes and save them. On this tab, you can also create and assign new or existing Token to the User or delete the User.



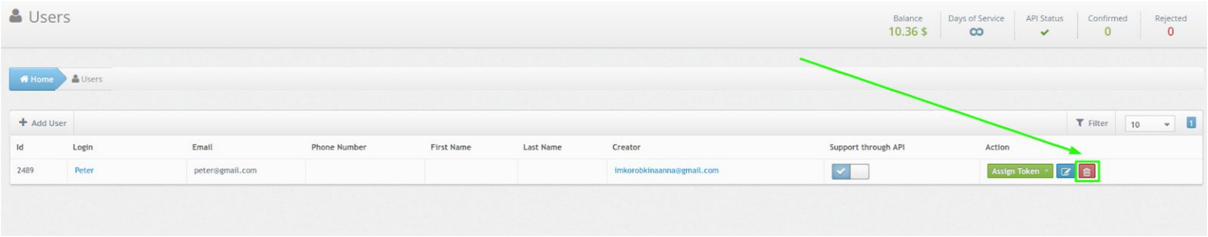
User Details

Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Home › Users › Detailed Information

How to Delete Users

To delete a User, click the **Users** button in the menu on the left, find the User you are going to delete, click on the **red button with the image of the bin** (first button on the right) and confirm the action.



Users

Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Home › Users

Id	Login	Email	Phone Number	First Name	Last Name	Creator	Support through API	Action
2489	Peter	peter@gmail.com				imkorobkinaanna@gmail.com	☑	Assign Token

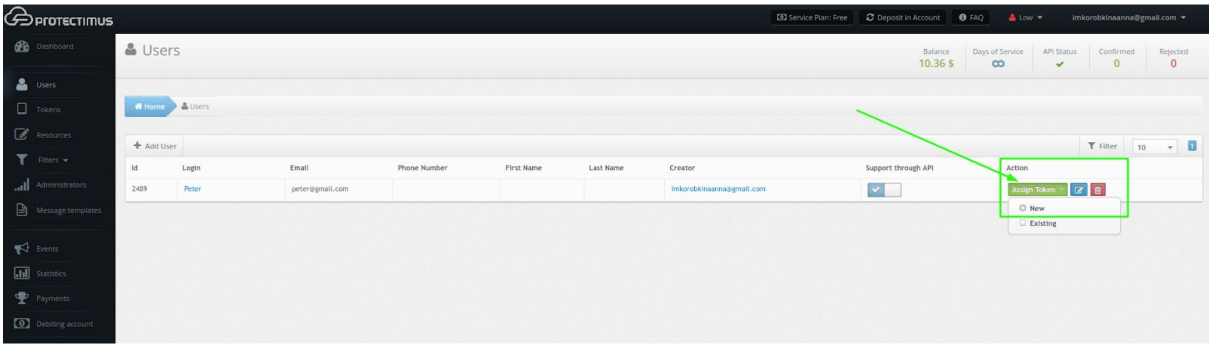
How to Assign a Token to a User

It’s necessary to specify what Token a User owns. There are three ways to do this:

- To assign an already existing Token to a User;
- To add a new Token, if this has not been done before, and assign it to a User;
- To activate the Self-Service Portal, through which users can add software tokens and activate hardware tokens themselves.

How to Assign a New Token to a User

Go to the **Users** tab (click the **Users** button in the menu on the left), find the desired User in the list of Users and click **Assign Token - New.**



Id	Login	Email	Phone Number	First Name	Last Name	Creator	Support through API	Action
2489	Peter	peter@gmail.com				imkorobkinaanna@gmail.com	✓	Assign Token

Select the Token that you want to add. It can be:

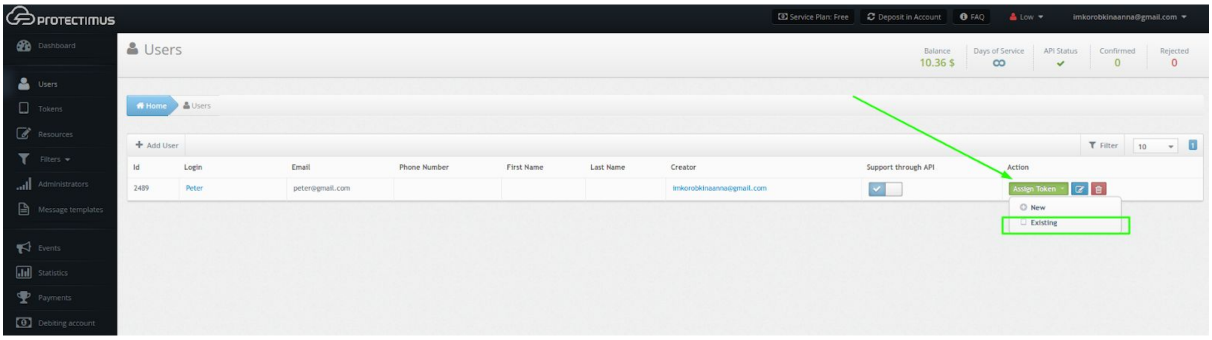
1. **Hardware Token** (Protectimus One, Two, Slim, Ultra, Crystal or tokens from other manufacturers).
2. **Software Token** (the 2FA application Protectimus Smart, delivery of OTP password via email, SMS or via chatbots in Facebook Messenger, Telegram, Viber).
3. **Universal Token** (this mechanism allows adding any hardware tokens from other vendors).

After selecting the desired type of OTP Token, you will need to fill in all necessary fields, enter a one-time password from the token and click the **Save** button.

For more information about creating Tokens, see the Tokens section.

How to Assign an Existing Token to a User

If you have already created a Token (for more information about creating Tokens, see the Tokens section), click the **Users** button in the menu on the left, find the desired User in the list of Users and click **Assign Token - Existing**, select the required Token and click **Assign.**

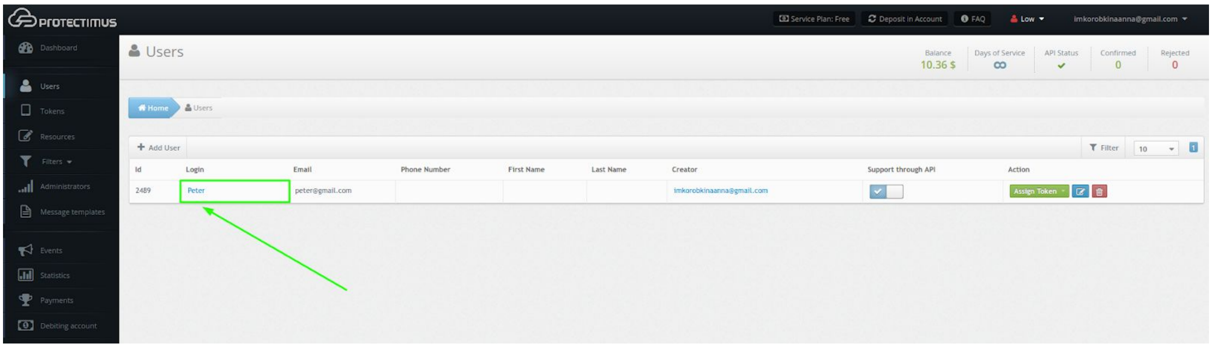


Id	Login	Email	Phone Number	First Name	Last Name	Creator	Support through API	Action
2489	Peter	peter@gmail.com				imkorobkinaanna@gmail.com	✓	Assign Token

How to Deactivate a User's Token

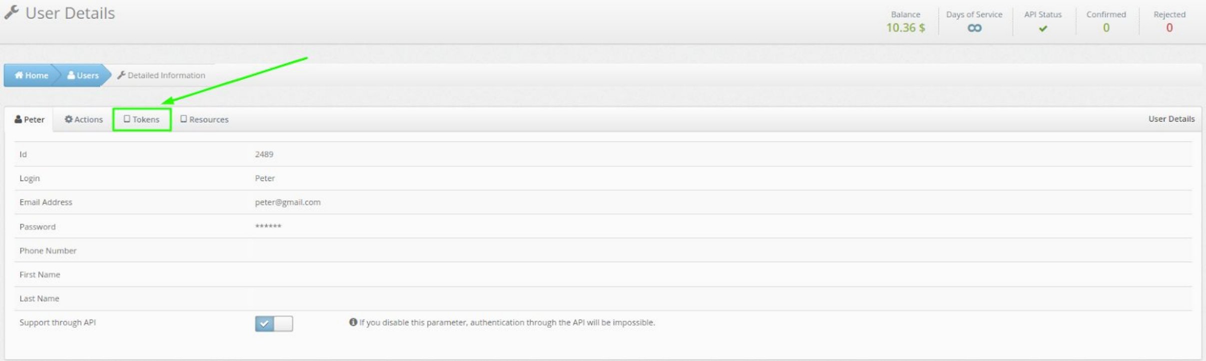
If a user loses their token, but you want to provide urgent access to this user, you will only need to deactivate this token, in which case this token will not be involved in the user authentication process.

To disable the Token, go to the Users section (click on the **Users** button in the menu on the left), find the desired User in the list and click on their **Login**.



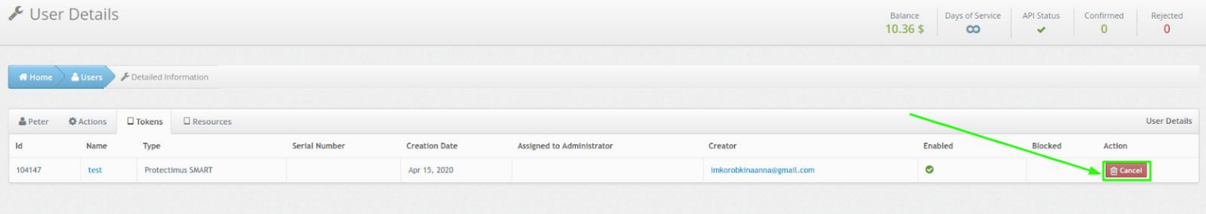
Id	Login	Email	Phone Number	First Name	Last Name	Creator	Support through API	Action
2489	Peter	peter@gmail.com				imkorobkinaanna@gmail.com	✓	Assign Token

Go to the **Tokens** tab.



Id	2489
Login	Peter
Email Address	peter@gmail.com
Password	******
Phone Number	
First Name	
Last Name	
Support through API	✓ If you disable this parameter, authentication through the API will be impossible.

Click the **Cancel** button.



Id	Name	Type	Serial Number	Creation Date	Assigned to Administrator	Creator	Enabled	Blocked	Action
104147	test	Protectimus SMART		Apr 15, 2020		imkorobkinaanna@gmail.com	✓		Cancel

For the information about deleting and reissuing Tokens, see the Tokens section.

6. Tokens

We divide all Tokens into hardware (physical) tokens and software (virtual) tokens. This classification is based on the peculiarities of entering and using the secret key for a specific type of tokens. Software tokens include the following: Protectimus SMART, Google Authenticator, Protectimus SMS, Protectimus BOT, and Protectimus MAIL tokens; hardware tokens include: Protectimus One, Protectimus Two, Protectimus Slim, Protectimus Ultra, and any hardware tokens from other vendors.

Any tokens that work based on the standard OATH algorithms may be used in our system. It may be done by adding a Universal Token. Of course, in this case, you will need to have sufficient knowledge about your token. We support several types of popular tokens from other manufacturers, which significantly simplifies your task.

The number of Tokens that you may add depends on the Service Plan you select. If you need to add more Tokens, please select the desired or required number of Tokens by customizing your Service Plan. Only the chief system administrator can change a Service Plan, deposit funds in the account, and view payment statistics.

The administrator can add Tokens and assign them to Users manually or activate the Self-Service Portal that allows Users to independently perform a number of actions related to issuing and managing their Tokens and their own data. The system Administrator determines which actions are available to Users. The Self-Service Portal must be enabled and configured separately for each resource.

The Tokens provided in our system may be used not only by your users, but also by you or your Administrators for protecting access to Protectimus. Therefore, a Token assigned to an Administrator may only be managed by the Administrator to whom it is assigned. For other Tokens, the same approach applies as for all other objects in the system: any Administrator can edit them, but only the creator or the chief system administrator can delete them.

If a User loses their Token, but you want to provide urgent access to this User, you will only need to deactivate this Token, in which case this Token will not be involved in the User authentication process.

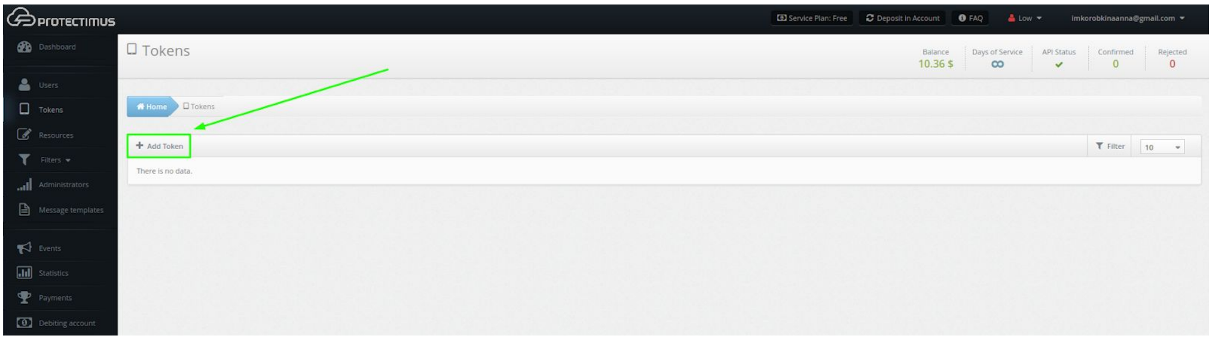
If an Administrator loses a Token, this Administrator will need to use the backup access mechanism to verify this Administrator’s other authenticators. After that, a request for deactivating a Token will be created. Only the chief system administrator or the technical support service will be able to satisfy this request.

PLEASE NOTE!

One User can use only one Token for authentication on one Resource.

How to Add Tokens Manually

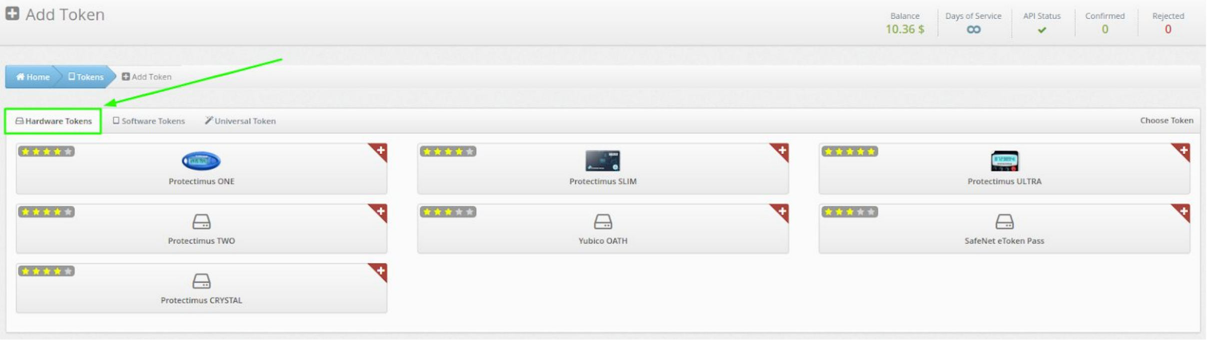
To create a Token, click the **Tokens** button in the menu on the left, and then click the **Add Token** button in the table header.



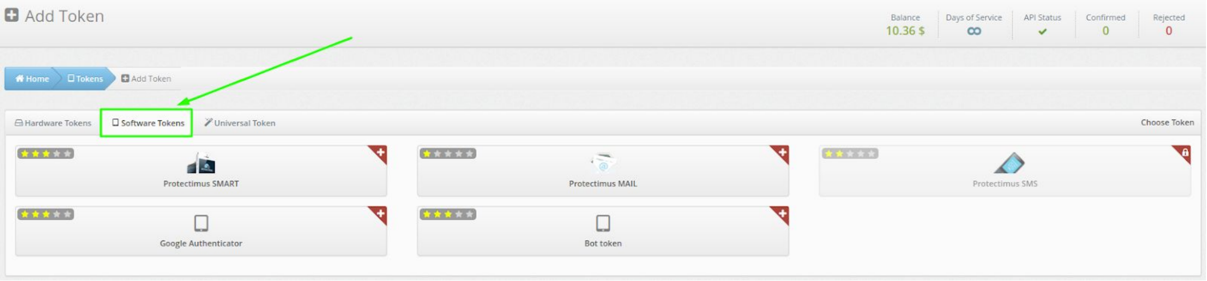
There is no data.

After that, select the Token that you want to add. It can be:

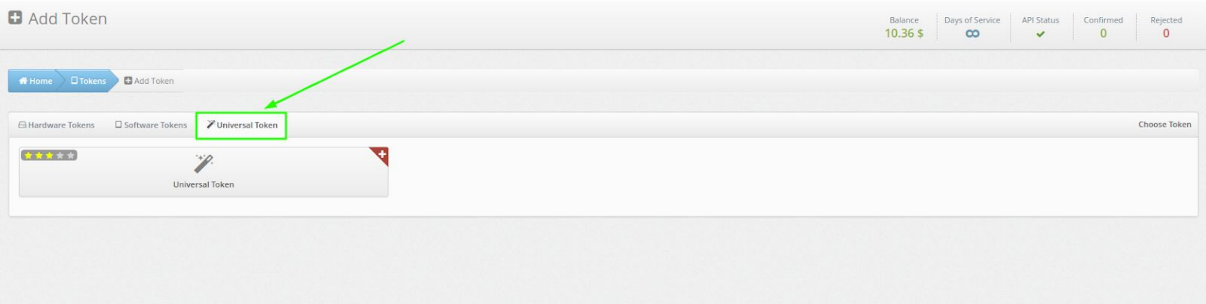
1. **Hardware tokens.** Protectimus One, Protectimus Two, Protectimus Slim, Protectimus Ultra, Protectimus Crystal, Yubiko OATH, SafeNet eToken Pass.



2. **Software tokens.** 2FA application Protectimus Smart available on iOS and Android, any other in-app authenticator, delivery of OTP password via email, SMS or via chatbots in Facebook Messenger, Telegram, Viber).



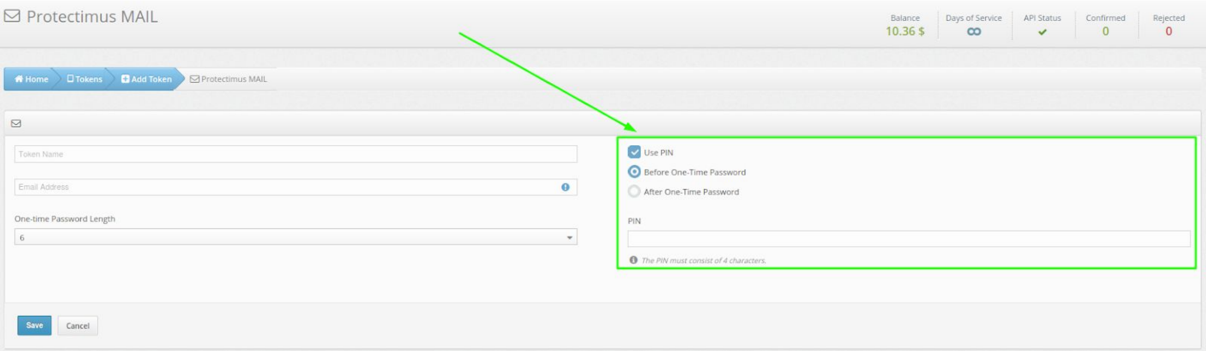
3. **Universal token.** This mechanism allows adding any hardware tokens from other vendors.



After selecting the desired type of OTP token, you will need to fill in all necessary fields, enter a one-time password from the token and click the **Save** button.

PLEASE NOTE!

You can also use the PIN code with any type of tokens you choose. If you activate the PIN code function, the user will have to enter the PIN code in the input field together with a one-time password (before or after a one-time password, depending on the choice of administrator). The one-time password and the PIN should be entered as one string without spaces or any other characters between them. This is an additional level of protection for the user account. Even if an attacker brute forces the static password and takes possession of the user's token, it’s impossible to compromise an account without a PIN code.



One-time Password Length: 6

☑ Use PIN

● Before One-Time Password

○ After One-Time Password

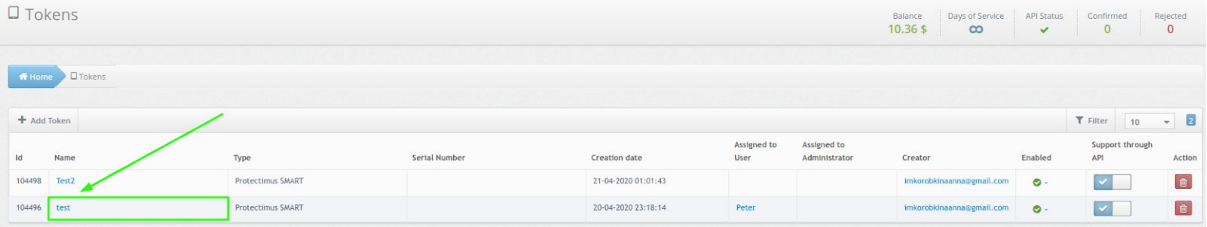
PIN

The PIN must consist of 4 characters.

After adding the token, you need to assign the token to a specific user (assign a token to the user) and connect the user and token with the resource (assign the token with the user to the resource).

How to Edit Tokens

Go to the **Tokens** tab (click the **Tokens** button in the menu on the left), find the desired Token in the list of all Tokens, and click on its **name**.



□ Tokens

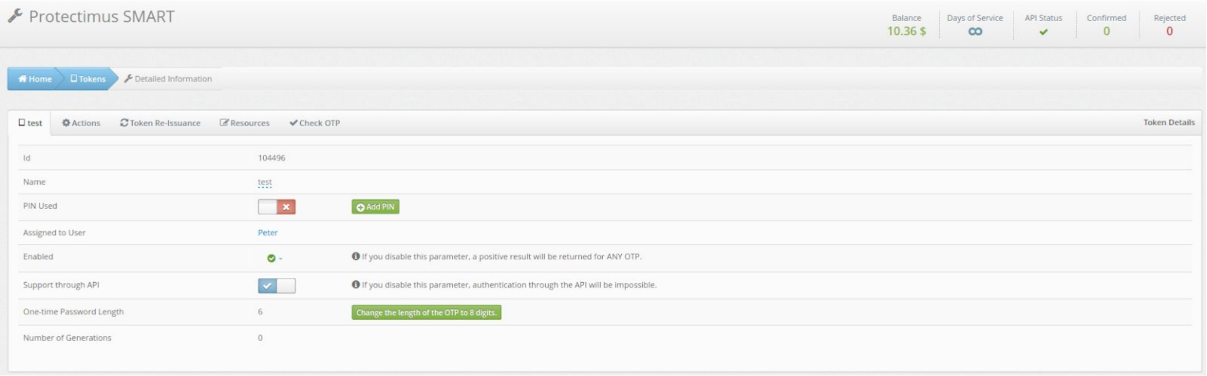
Balance 10.36 $ | Days of Service ∞ | API Status ✓ | Confirmed 0 | Rejected 0

Home › □ Tokens

Id	Name	Type	Serial Number	Creation date	Assigned to User	Assigned to Administrator	Creator	Enabled	Support through API	Action
104498	Test2	Protectimus SMART		21-04-2020 01:01:43			imkorobkinaanna@gmail.com	✓ -	✓	🗑
104496	test	Protectimus SMART		20-04-2020 23:18:14	Peter		imkorobkinaanna@gmail.com	✓ -	✓	🗑

You will see the page with detailed information about the Token where you can:

- change the name of the Token,
- add / change / delete PIN code,
- change the length of the one-time password.



Protectimus SMART

Balance 10.36 $ | Days of Service ∞ | API Status ✓ | Confirmed 0 | Rejected 0

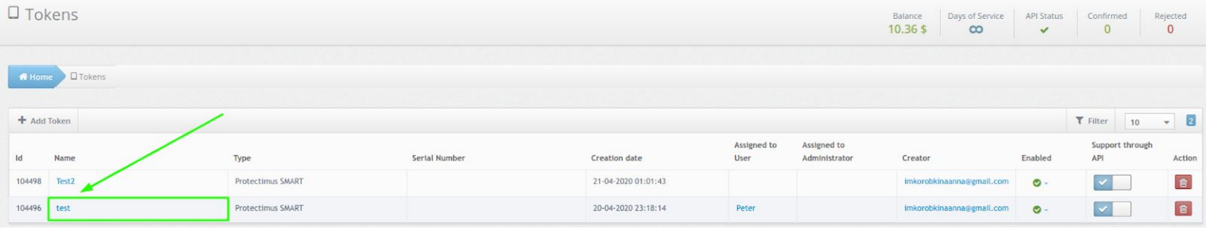
Home › □ Tokens › Detailed Information

Id	104496	
Name	test	
PIN Used	✗	Add PIN
Assigned to User	Peter	
Enabled	✓ -	If you disable this parameter, a positive result will be returned for ANY OTP.
Support through API	✓	If you disable this parameter, authentication through the API will be impossible.
One-time Password Length	6	Change the length of the OTP to 8 digits.
Number of Generations	0	

Token Re-Issuance

If a User loses their Token, but you want to provide urgent access to this User, you will only need to deactivate this Token, in which case this Token will not be involved in the User authentication process.

To re-issue the Token, go to the **Tokens** section (click the **Tokens** button in the menu on the left), find the desired Token in the list of all Tokens, and click on its **name.**



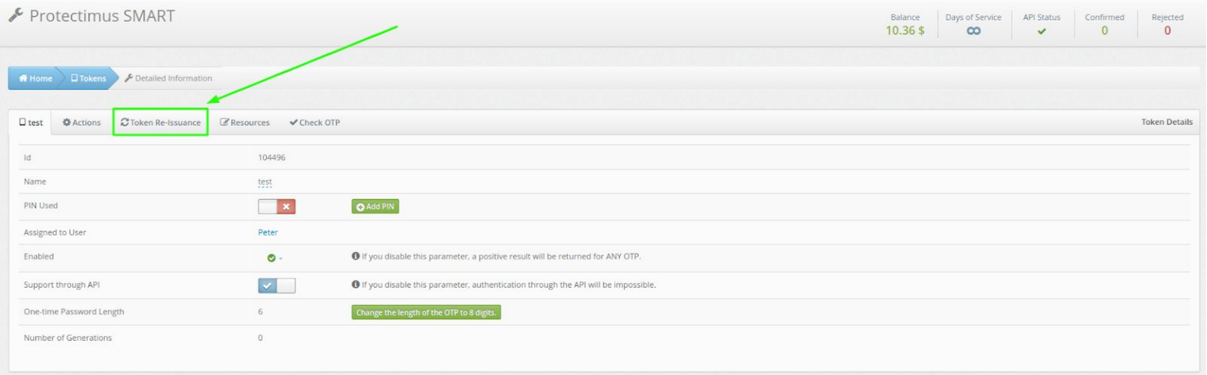
□ Tokens

Balance 10.36 $ | Days of Service ∞ | API Status ✓ | Confirmed 0 | Rejected 0

Home › □ Tokens

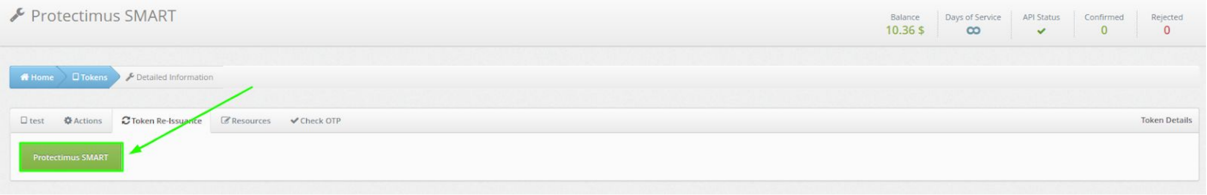
Id	Name	Type	Serial Number	Creation date	Assigned to User	Assigned to Administrator	Creator	Enabled	Support through API	Action
104498	Test2	Protectimus SMART		21-04-2020 01:01:43			imkorobkinaanna@gmail.com	✓ -	✓	🗑
104496	test	Protectimus SMART		20-04-2020 23:18:14	Peter		imkorobkinaanna@gmail.com	✓ -	✓	🗑

Go to the **Token Re-Issuance** tab.



Id	104496	
Name	test	
PIN Used	☒	
Assigned to User	Peter	
Enabled	✓ -	If you disable this parameter, a positive result will be returned for ANY OTP.
Support through API	☑	If you disable this parameter, authentication through the API will be impossible.
One-time Password Length	6	
Number of Generations	0	

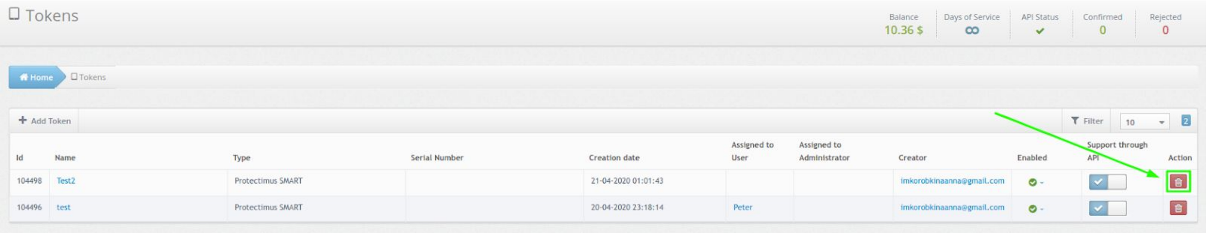
Click on the name of the Token, fill in all the required fields and click on the **Re-Issue** button.



How to Delete Tokens

Only the creator or the chief administrator can delete the Token.

To delete the Token, go to the **Tokens** section (click the **Tokens** button in the menu on the left), find the desired Token in the list of all Tokens, and click on the **red button with the image of the bin** (the first button on the right).



Id	Name	Type	Serial Number	Creation date	Assigned to User	Assigned to Administrator	Creator	Enabled	Support through API	Action
104498	Test2	Protectimus SMART		21-04-2020 01:01:43			imkorobkinaanna@gmail.com	✓ -	☑	🗑
104496	test	Protectimus SMART		20-04-2020 23:18:14	Peter		imkorobkinaanna@gmail.com	✓ -	☑	🗑

User's Self-Service Portal

The User’s Self-Service mechanism allows users to independently perform a number of actions related to issuing and managing their tokens and their own data. The system administrator determines which actions are available to users.

The list of possible actions includes:

- Register New Token
- Existing Token Registration
- Re-Assign Token
- Unassign Token
- Token Synchronization
- PIN Setup
- Remove PIN
- Create Password
- Change Password
- Change Email Address
- Change Contact Phone Number
- Change Login
- Change First Name and Last Name
- Manage user environment

PLEASE NOTE!

The Protectimus RProxy component can automatically create Users that are preconfigured to use the Self-Service Portal.

Detailed instructions for setting up a User's Self-Service Portal with notes for integrations through the RProxy component are available here.

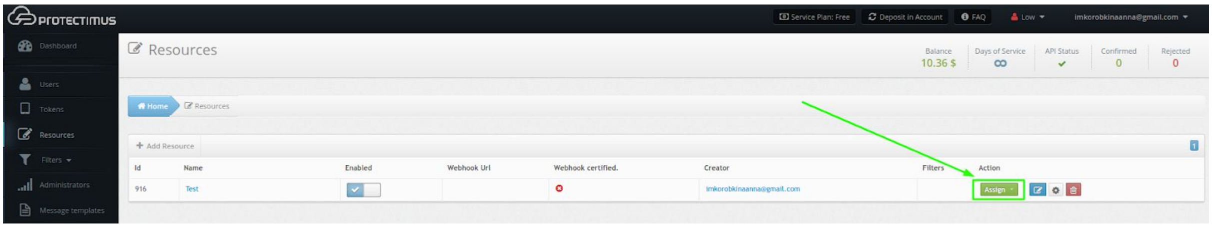
7. Assigning Users and Tokens to Resource

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 selected. 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.
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 by the Token. This method requires that a Token should be assigned to a Resource.

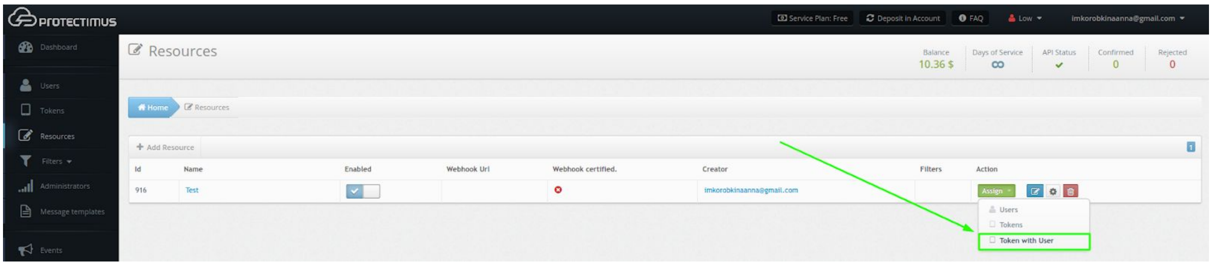
How to Assign Tokens With Users to a Resource

Go to the **Resources** section (click the **Resources** button in the menu on the left) and click the **Assign** button.



Id	Name	Enabled	Webhook Url	Webhook certified.	Creator	Filters	Action
916	Test	✓		✗	imkorobkinaanna@gmail.com		Assign

Choose **Token with User**, select the Tokens that should be assigned to the Resource and click **Assign**.



Id	Name	Enabled	Webhook Url	Webhook certified.	Creator	Filters	Action
916	Test	✓		✗	imkorobkinaanna@gmail.com		Assign

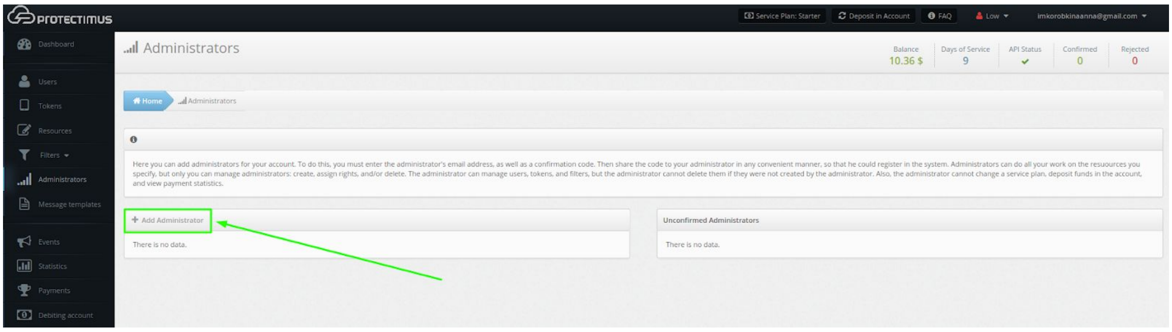
8. Administrators

You may need help in effectively managing a large number of Users and Resources. Create an Administrator, which will allow you to delegate the required scope of work. An Administrator has access only to the Resources that they have your permission to manage; thus, they will be responsible only for the specific tasks assigned.

Administrators can do all your work on the Resources you specify, but only the chief system administrator can manage Administrators: create, assign rights, and/or delete them. The Administrator can manage Users, Tokens, and Filters, but the Administrator cannot delete them if they were not created by the Administrator. Also, the Administrator cannot change a Service Plan, deposit funds in the account, and view payment statistics.

The number of Administrators that you may add depends on the Service Plan you select. If you need to add more Administrators,customize your Service Plan.

To add an Administrator, click the **Administrators** button in the menu on the left, and then click the **Add Administrator** button.



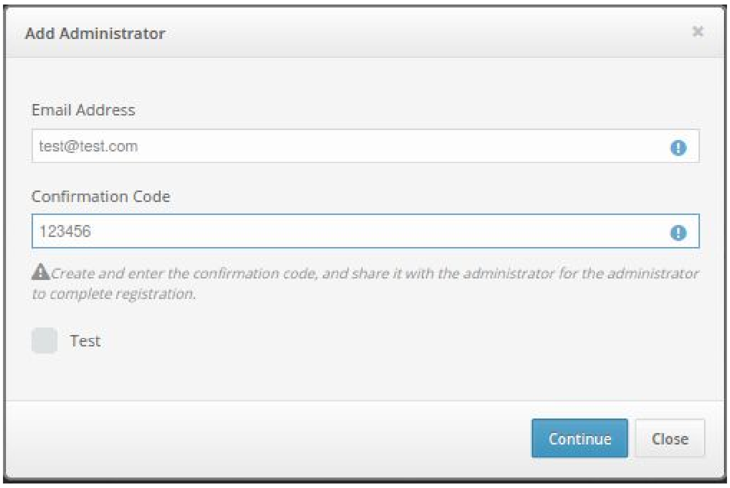
Balance 10.36 $ | Days of Service 9 | API Status ✓ | Confirmed 0 | Rejected 0

Here you can add administrators for your account. To do this, you must enter the administrator's email address, as well as a confirmation code. Then share the code to your administrator in any convenient manner, so that he could register in the system. Administrators can do all your work on the resuources you specify, but only you can manage administrators: create, assign rights, and/or delete. The administrator can manage users, tokens, and filters, but the administrator cannot delete them if they were not created by the administrator. Also, the administrator cannot change a service plan, deposit funds in the account, and view payment statistics.

There is no data.

There is no data.

Enter the **Administrator's email**, **confirmation code**, select the Resources that the Administrator will have access to, and click **Continue**.



Email Address: test@test.com

Confirmation Code: 123456

Create and enter the confirmation code, and share it with the administrator for the administrator to complete registration.

□ Test

Then share the confirmation code to your Administrator in any convenient manner, so that he could register in the system.

9. Filters

If you wish to limit access to your Resource depending on a User's country, you can create a Geographic Filter. When you need to limit User access to your Resource depending on the login time, you can create a Time Filter.

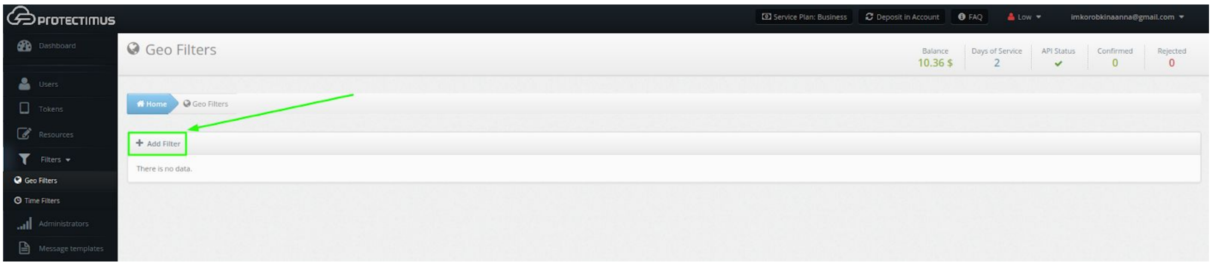
Do not forget to assign the created Filter to the Resource that you wish to apply it to.

The number of Filters that you may add depends on the Service Plan you select. If you need to add more Filters, please select the desired or required number of Filters by customizing your Service Plan. Only the chief system administrator can change a Service Plan, deposit funds in the account, and view payment statistics.

How to Add a Geographic Filter

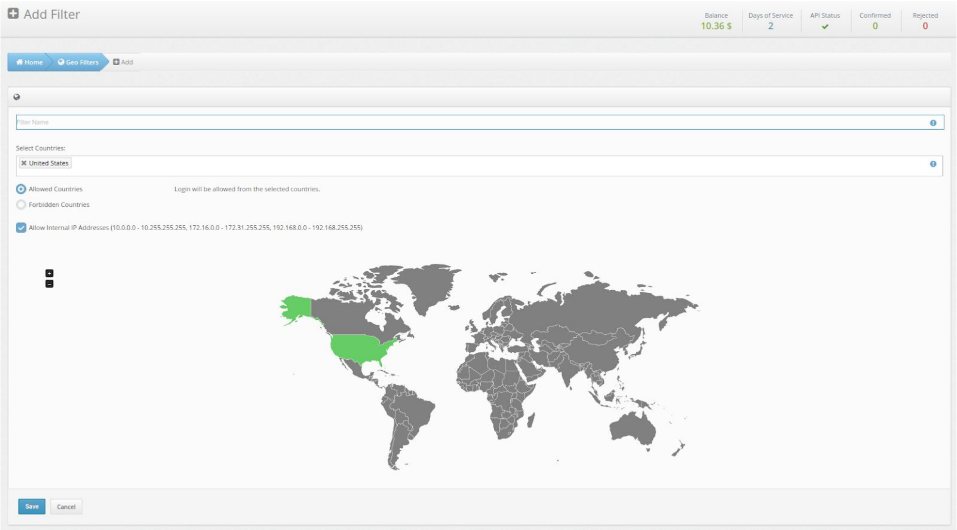
This feature allows you to open access to the Resource only from certain countries. If someone tries to login from a forbidden country, then they will not have access to the account, if from allowed, then the system will ask for a one-time password. You can also deny access only from selected countries.

Go to the **Geo Filters** section (click the buttons **Filters - Geo Filters** in the menu on the left), and then click the **Add Filter** button.



There is no data.

Enter the Filter Name and select the countries in which access to your Resource will be allowed or denied. After that click **Save**.



Select Countries:
✖ United States

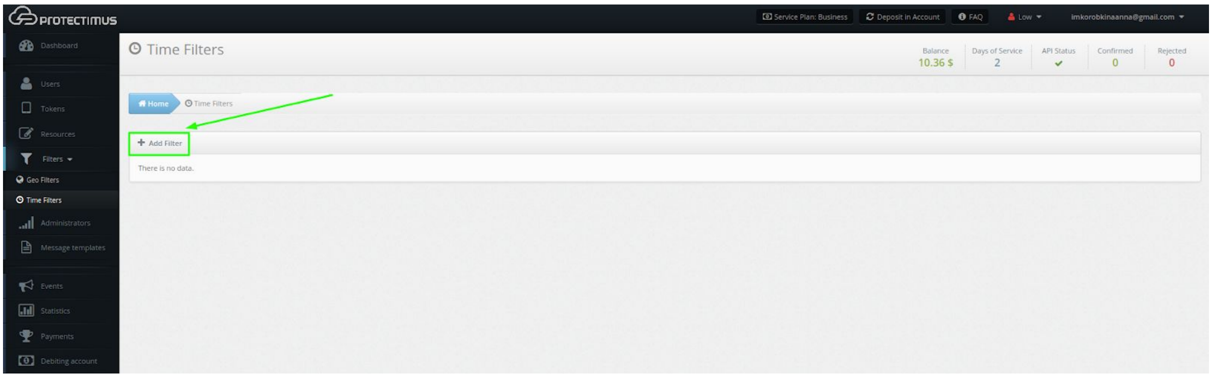
● Allowed Countries — Login will be allowed from the selected countries.
○ Forbidden Countries

☑ Allow Internal IP Addresses (10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255)

How to Add a Time Filter

This feature allows granting access to a Resource only at certain time; for example, only during business hours. This approach significantly increases the level of protection against unauthorized account access. It's perfect for corporate environments: even if a User leaves their Token at work, nobody can access the User's account outside of working hours.

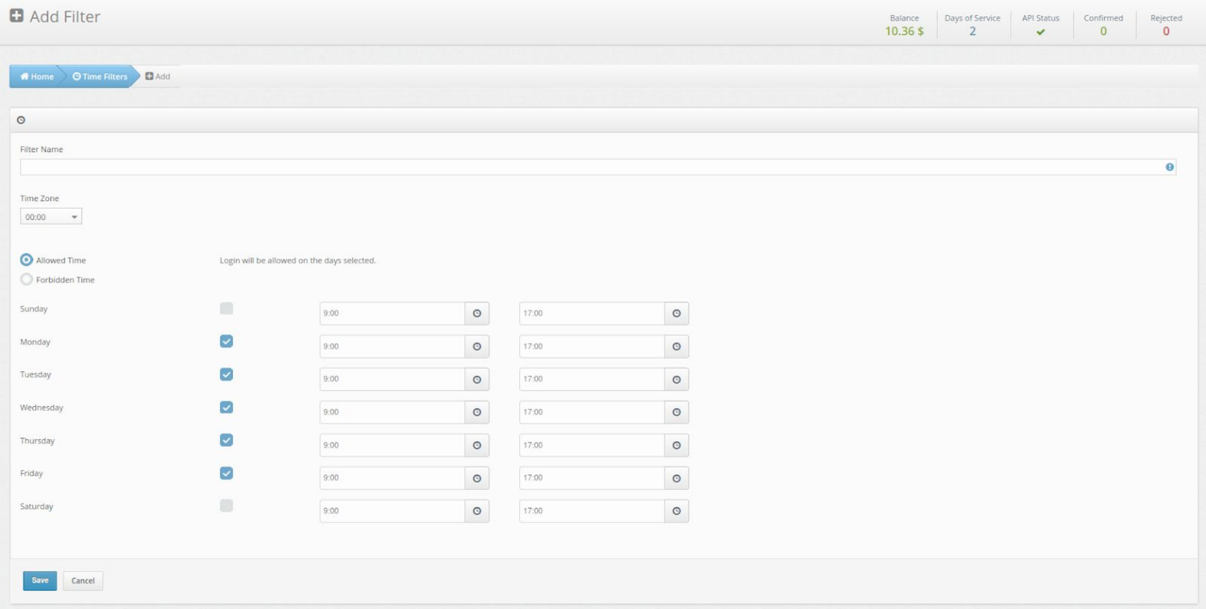
Go to the **Time Filters** section (click the buttons **Filters - Time Filters** in the menu on the left), and then click the **Add Filter** button.



Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	2	✓	0	0

There is no data.

Enter the Filter Name, specify the time zone, mark the days of the week and specify the time at which access to your Resource will be allowed or denied. After that click **Save**.



Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	2	✓	0	0

Filter Name

Time Zone: 00:00

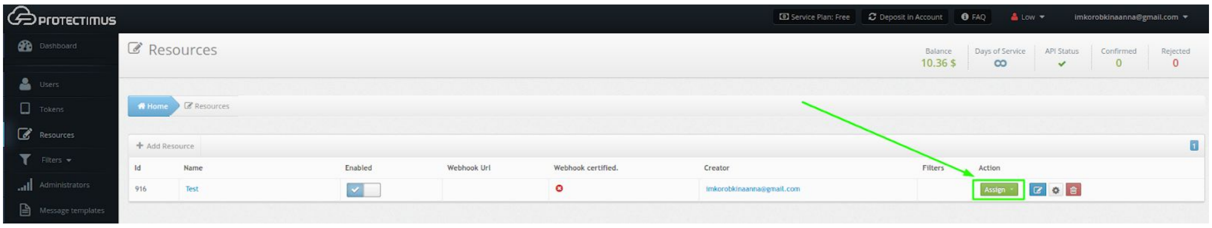
● Allowed Time
○ Forbidden Time

Login will be allowed on the days selected.

Sunday	□	9:00	17:00
Monday	☑	9:00	17:00
Tuesday	☑	9:00	17:00
Wednesday	☑	9:00	17:00
Thursday	☑	9:00	17:00
Friday	☑	9:00	17:00
Saturday	□	9:00	17:00

How to Assign Filters to a Resource

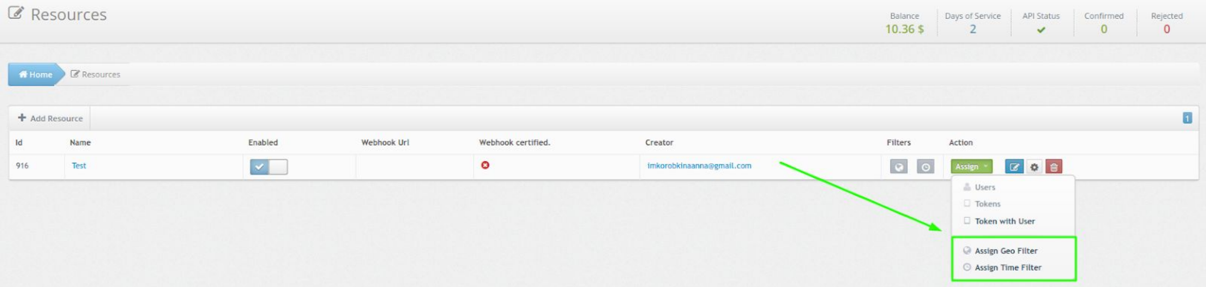
Go to the **Resources** tab (click the **Resources** button in the menu on the left) and click the **Assign** button.



Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	∞	✓	0	0

Id	Name	Enabled	Webhook Url	Webhook certified.	Creator	Filters	Action
916	Test	✓		☒	imkorobkinaanna@gmail.com		Assign

Select a **Geo Filter** or a **Time Filter**, depending on which filter you want to assign. After that, select the desired filter from the list that appears, and click **Assign**.



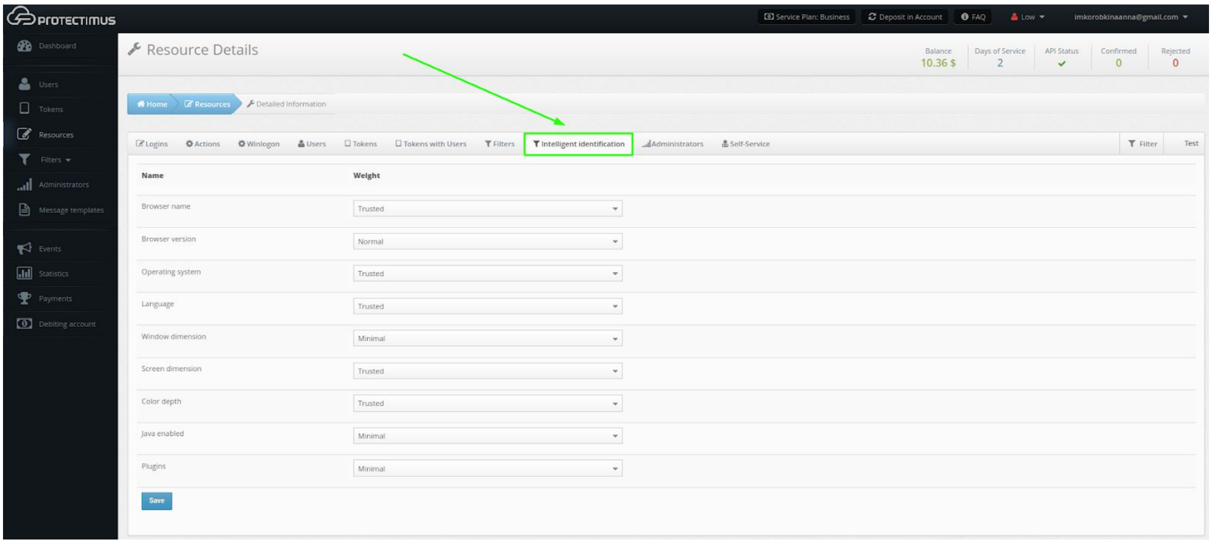
Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	2	✓	0	0

Id	Name	Enabled	Webhook Url	Webhook certified.	Creator	Filters	Action
916	Test	✓		☒	imkorobkinaanna@gmail.com		Assign

10. Intelligent Identification

This feature may also be called smart identification or user environment analysis. We created it to make things more convenient for users in systems where a certain amount of trust is permissible. Nobody loves typing in one-time passwords, so we devised a way of analyzing the user’s environment (browser name and version, operating system and language, window size and screen resolution, color depth, presence or absence of Java, plugins, etc.); a one-time password is required only once an established mismatch threshold has been exceeded.

To activate the Intelligent Identification function, go to the **Resources** section (click on the **Resources** button in the menu on the left), select the desired Resource from the list, click on its **name** and go to the **Intelligent Identification** tab.



Balance	Days of Service	API Status	Confirmed	Rejected
10.36 $	2	✓	0	0

Name	Weight
Browser name	Trusted
Browser version	Normal
Operating system	Trusted
Language	Trusted
Window dimension	Minimal
Screen dimension	Trusted
Color depth	Trusted
Java enabled	Minimal
Plugins	Minimal

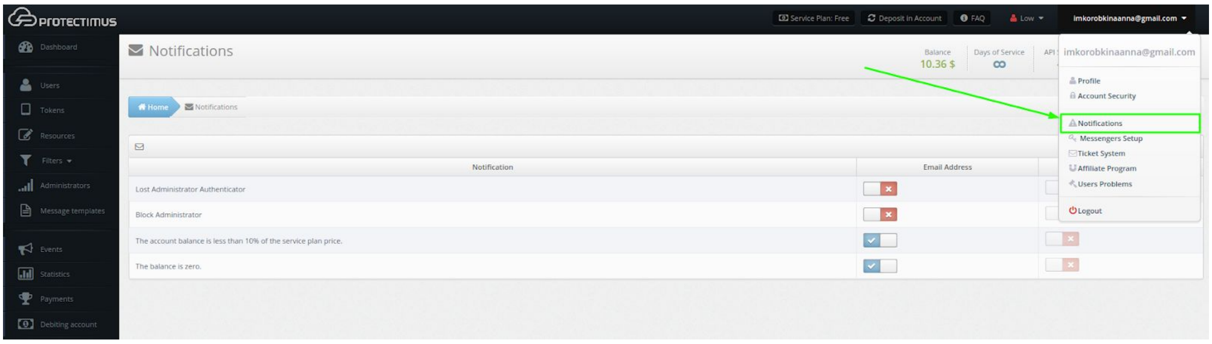
Set the desired “weight” of each parameter (minimal, normal or trusted) and save the settings.

11. Event Notifications

It is important to always have up-to-date information. Protectimus will send you notifications of events that you chose on the notification settings page. You can choose to receive notifications via email or SMS-messages. Stay up to date on the events in the Protectimus authentication system. The list of available types of notifications includes the following:

- The Administrator’s authenticator is lost.
- The Administrator is blocked.
- The account balance is less than 10% of the service plan price.
- The balance is zero.

To go to the Notification settings page, click on your **email in the upper right corner** and select **Notifications.**



Notification	Email Address	
Lost Administrator Authenticator	☒	
Block Administrator	☒	
The account balance is less than 10% of the service plan price.	☑	☒
The balance is zero.	☑	☒

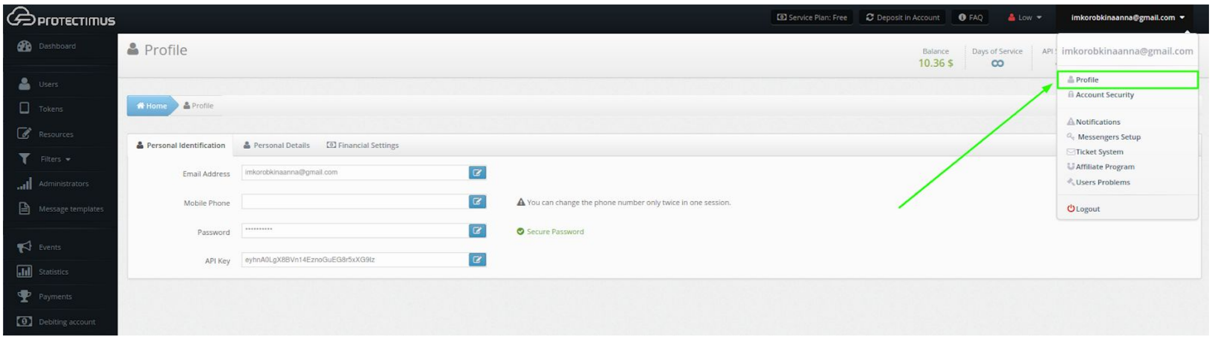
To receive notifications via SMS, [provide your phone number in the profile settings](#).

12. Protectimus Account Security Settings

The entire system is as secure as its weakest link. We put you under no obligation, but we do warn you and recommend that you should utilize all the capabilities offered by Protectimus to ensure maximum protection of all Administrators' accounts. Complete all the steps included here, and you can be certain that you are securely protected.

Use Strong Password

Go to **Profile Settings** to change the password to a stronger one. Click on your **email in the upper right corner** and select **Profile.**



Email Address: imkorobkinaanna@gmail.com

Mobile Phone:

You can change the phone number only twice in one session.

Password: **********

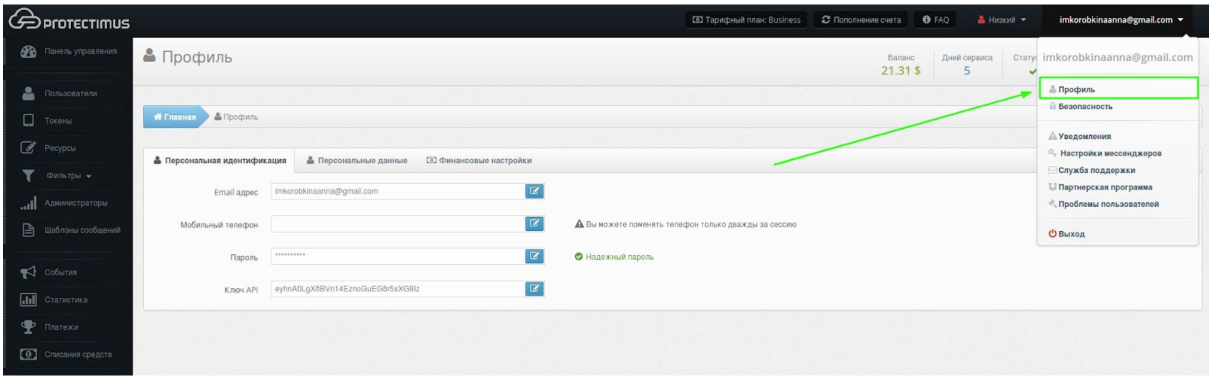
Secure Password

API Key: eyhnA0LgX8BVn14EznoGuEG8r5xXG9lz

A secure password must contain at least 10 characters and include upper- and lower-case letters, numbers and special symbols. A good password should not contain any open access information, for example, your login or phone number; also, you should check to see if your password is on the most frequently used password lists. If it is, such a password will be easy to hack.

Provide Your Phone Number

Go to **Profile Settings** to add your phone number. Click on your **email in the upper right corner** and select **Profile.**



Email адрес: imkorobkinaanna@gmail.com

Мобильный телефон:

Вы можете поменять телефон только дважды за сессию

Пароль: **********

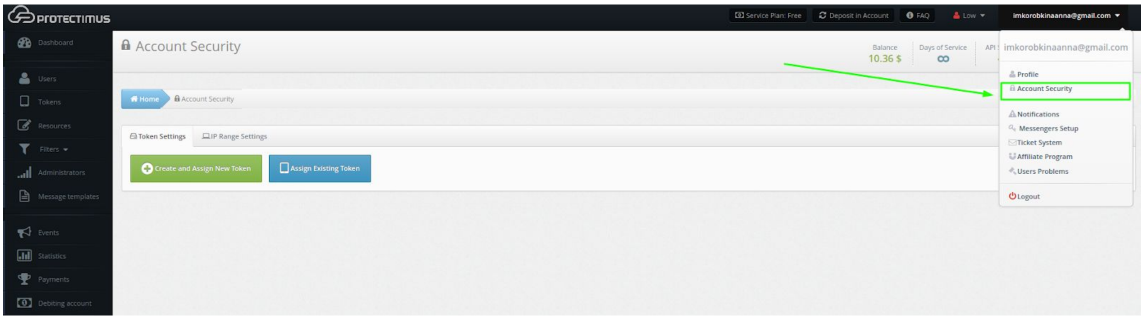
Надежный пароль

Ключ API: eyhnA0LgX8BVn14EznoGuEG8r5xXG9lz

Your phone number will not be used for authentication, but when you change some important parameters, Protectimus may request phone owner verification by sending a verification code to the phone number provided by you. This complicates the work of the attacker and gives you a signal that someone has gained access to your account and is trying to make important changes in it. Also, if you provide your phone number and choose the option of receiving notification via SMS-messages, you will be notified of all the important events in the system. Your number will not be transferred to a third party and will not be used for purposes other than ensuring your safety and awareness.

Create and Assign a Token to Protect Your Account

To set up two-factor authentication for your Protectimus account, go to **Security Settings**. Click on your **email in the upper right corner** and select **Account Security**.

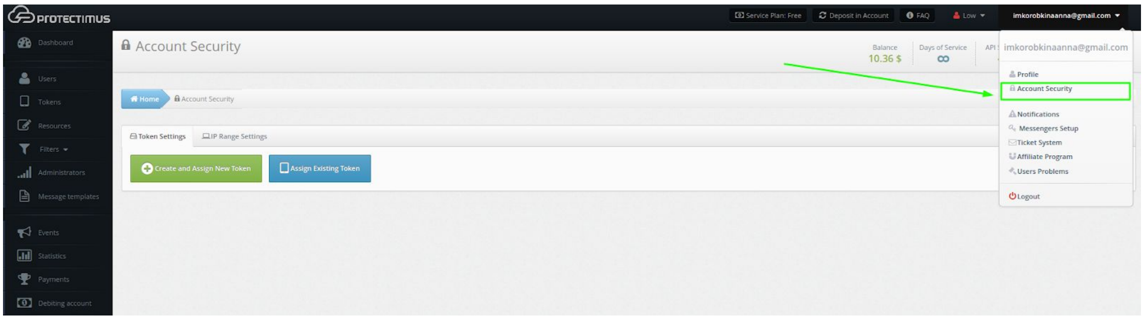


You may create and assign a new Token or assign the existing Token. For more information about creating tokens, see the Tokens section.

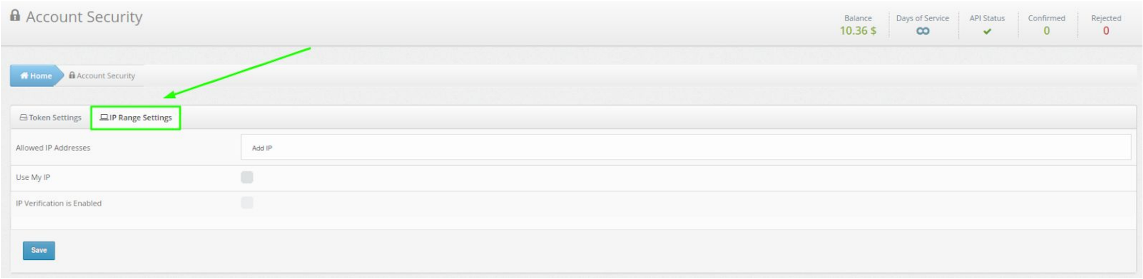
Limit IP Addresses Approved for Access

If you log into the system only from several permanent locations, you may want to limit access to the system from only several approved IP addresses. You can set the allowed addresses on the **Account Security** page on the **IP Range Settings** tab.

Click on your **email in the upper right corner** and select **Account Security**.



Select the **IP Range Settings** tab, add the necessary IP addresses, enable IP verification and click **Save**.



Contacts

Technical questions, software distribution, and any help:

support@protectimus.com

Partnership, sales, business opportunities:

sales@protectimus.com

Call Us:

Ireland +3 537 688 899 22

USA: +1 786 796 66 64

United Kingdom: +44 20 3808 7124

Ukraine: +38 057 706 21 24

Russia: +7 499 677 16 34

Corporate Information

Protectimus Ltd

Carrick house,

49 Fitzwilliam Square,

Dublin D02 N578,

Ireland