Security

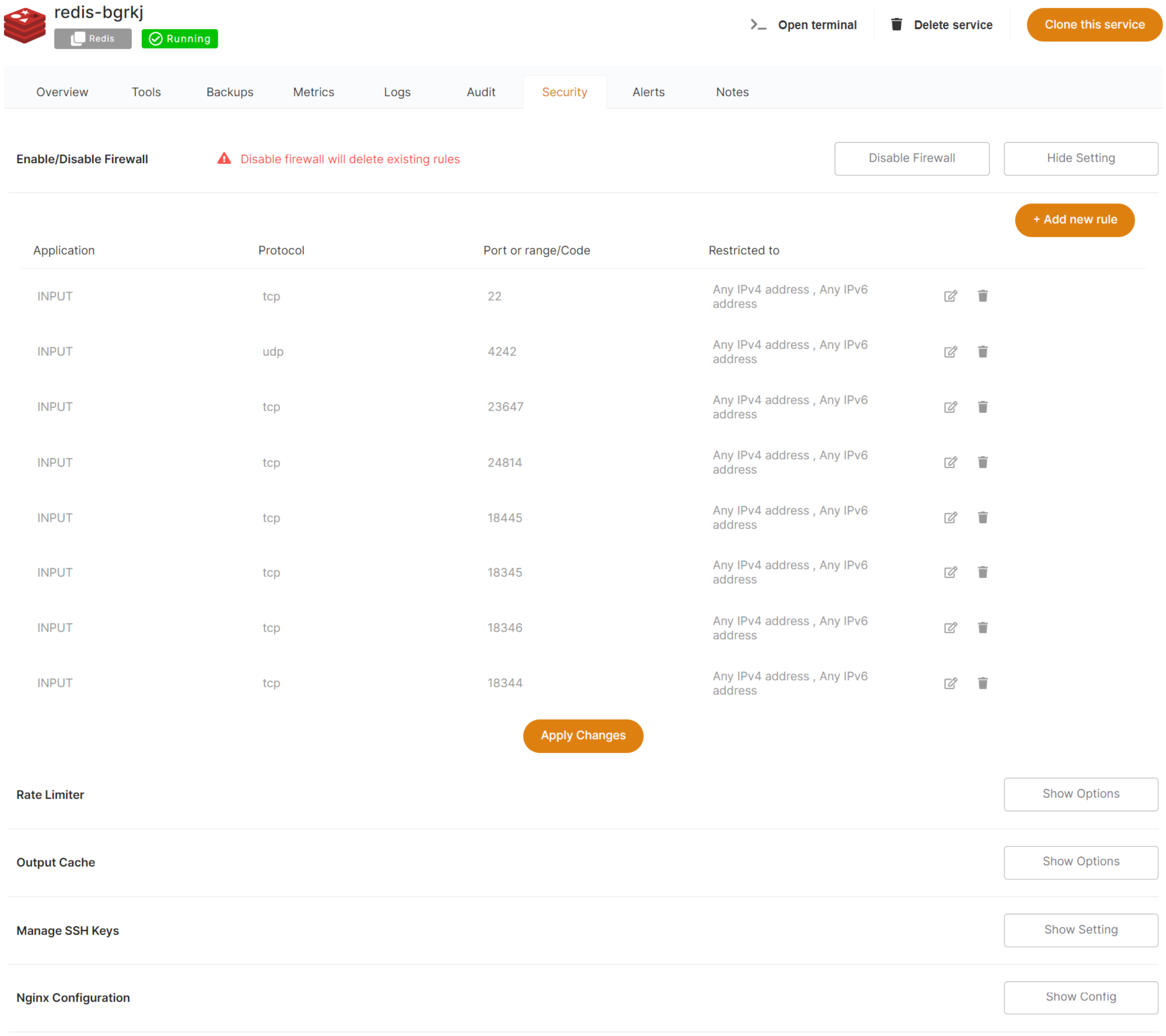
Overview

We automatically setup all services with several layers of security activated by default.

This includes:

- Automated SSL / TLS
- Network Firewall
- IP Rate Limiter
- Output Cache
- Accidental termination protection & Grace period
- Manage SSH Keys

Each of these features are accessible from your Dashboard via the *Security* tab.



Enable/Disable Firewall

⚠ Disable firewall will delete existing rules

Application	Protocol	Port or range/Code	Restricted to
INPUT	tcp	22	Any IPv4 address , Any IPv6 address
INPUT	udp	4242	Any IPv4 address , Any IPv6 address
INPUT	tcp	23647	Any IPv4 address , Any IPv6 address
INPUT	tcp	24814	Any IPv4 address , Any IPv6 address
INPUT	tcp	18445	Any IPv4 address , Any IPv6 address
INPUT	tcp	18345	Any IPv4 address , Any IPv6 address
INPUT	tcp	18346	Any IPv4 address , Any IPv6 address
INPUT	tcp	18344	Any IPv4 address , Any IPv6 address

Rate Limiter

Output Cache

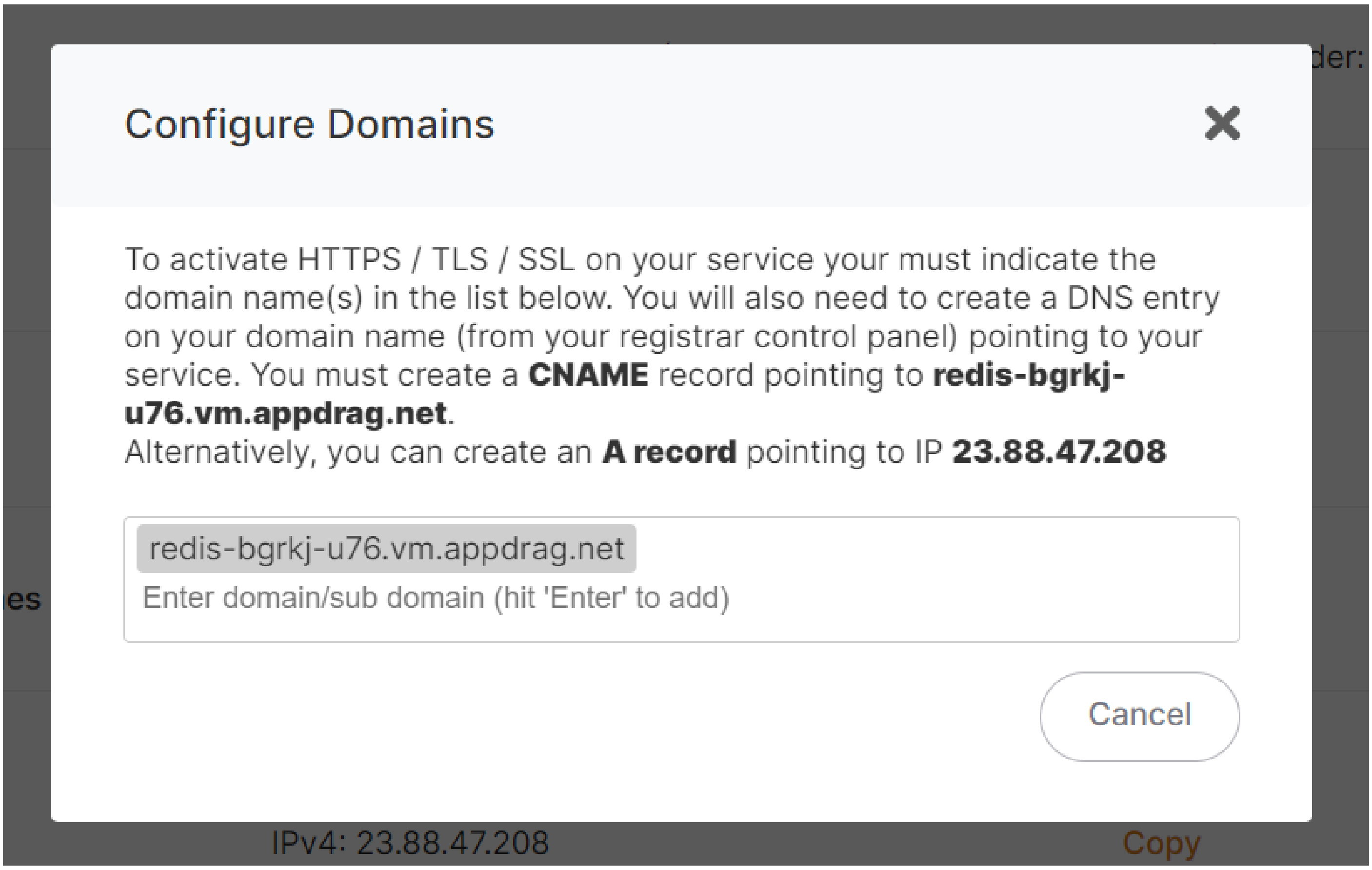
Manage SSH Keys

Nginx Configuration

Custom domain and automated encryption (SSL/TLS)

> If you have activated the firewall on your service ensure port 80 is open or else certificate creation/renewal will fail

Access the "Manage SSL Domains" option within the "Custom Domain Names" row located in the overview tab of the service dashboard.



Configure Domains

To activate HTTPS / TLS / SSL on your service your must indicate the domain name(s) in the list below. You will also need to create a DNS entry on your domain name (from your registrar control panel) pointing to your service. You must create a **CNAME** record pointing to **redis-bgrkj-u76.vm.appdrag.net**.
Alternatively, you can create an **A record** pointing to IP **23.88.47.208**

redis-bgrkj-u76.vm.appdrag.net

Enter domain/sub domain (hit 'Enter' to add)

IPv4: 23.88.47.208

From there you can manage allowed domains for SSL. If you want to add a new domain, just type it and press enter to add it to the list of authorized domains. You will also need to create a DNS entry to point your domain to the IP address of your service.

You can either create an A record or CNAME record to point to your service. CNAME is preferred as it won't change even if your IP change (eg: this can happen if your clone/migrates your service to another provider.

Once added, you can verify if your DNS entry is propagated with a tool like https://dnschecker.org/

Once propagated SSL should work instantly on your service. The certificate will be automatically generated and renewed.

> For some software you will also have to update an env var to indicate the domain to be used. To do that in the overview screen of your service click on UPDATE CONFIG button > Env tab > there update the domain env var with your own domain

Cloudflare users

If you are using Cloudflare reverse proxy (orange cloud icon) please check detailed instructions about Cloudflare & Elestio here:

https://docs.elest.io/books/security/page/using-cloudflare

Troubleshooting SSL not generated

You can display the nginx log with this command in a terminal:

```
cd /opt/elestio/nginx;
docker-compose logs -f;
```

press ctrl+c to stop displaying the live logs

Reset SSL_DATA folder

In some cases, the **/opt/elestio/nginx/ssl_data** folder can become corrupted, if this happens, connect to a terminal and try this:

```
cd /opt/elestio/nginx/;
docker-compose down;
mv ./ssl_data/ ./ssl_data_old/;
```

```
mkdir ./ssl_data/;
chmod 777 ./ssl_data/;
docker-compose up -d
```

Once executed just open your custom website url again and your certificate should be generated and your site served over SSL/TLS.

Using Cloudflare

Cloudflare DNS:

If you wish to use Cloudflare for DNS ONLY, you can configure it just like any other DNS provider, and simply follow the steps for adding a custom domain as usual.

> WARNING: Your domain DNS entry **must have a GRAY cloud, not an ORANGE (proxied) cloud next to the entry.**

> **Using Cloudflare's proxy for your domain without additional configuration will cause all incoming connections to fail!**

> This is the correct image shown for DNS-only entries.

Cloudflare Proxy

Even though Elest.io automatically provides SSL and has a firewall, there can be advantages to using Cloudflare for Proxying traffic, notably DDoS attacks and automatic filtering of scripted attacks.

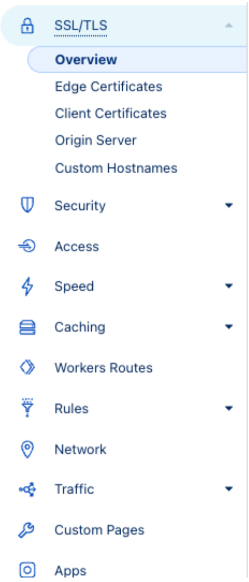
> Note: Cloudflare only proxies traffic on certain ports. If you want to use this hostname for SSH, FTP, or other services whose ports are not listed in the above link, you must configure Cloudflare to provide DNS only or use Cloudflare's Spectrum offer.

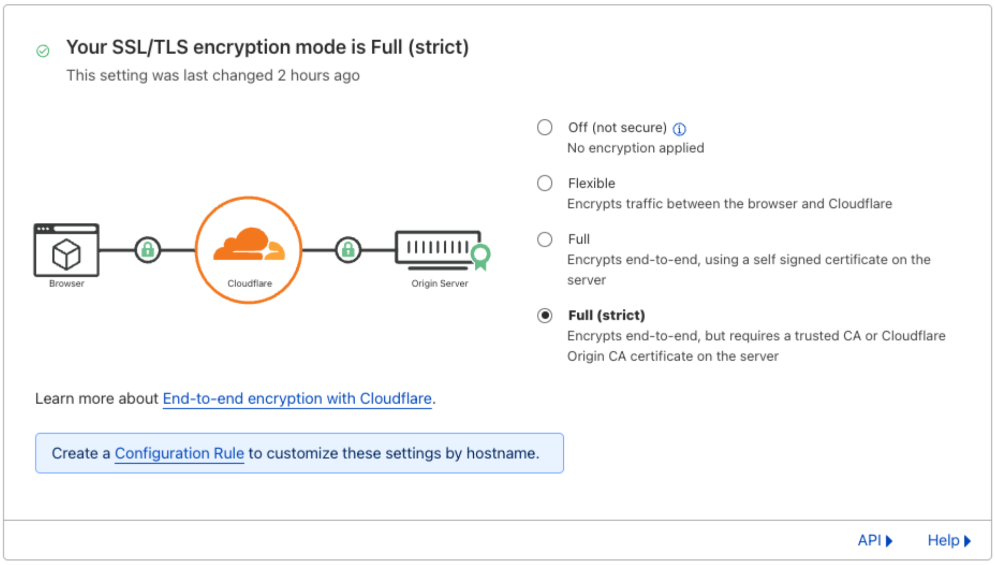
Because Elest.io already creates an SSL certificate for your website trusted by a root CA, the recommended configuration is to set Cloudflare to use Strict SSL verification when connecting to your server.

> Before continuing, ensure you have already configured the domains as per the instructions on the previous page.

Option 1: To set up strict SSL verification for your **whole domain**:

1. Navigate to the `SSL/TLS` section of your domain's dashboard.
2. Select the `"Full (strict)"` option.
3. Your changes will be saved automatically. You're done!





Your SSL/TLS encryption mode is Full (strict)

This setting was last changed 2 hours ago

○ Off (not secure)
No encryption applied

○ Flexible
Encrypts traffic between the browser and Cloudflare

○ Full
Encrypts end-to-end, using a self signed certificate on the server

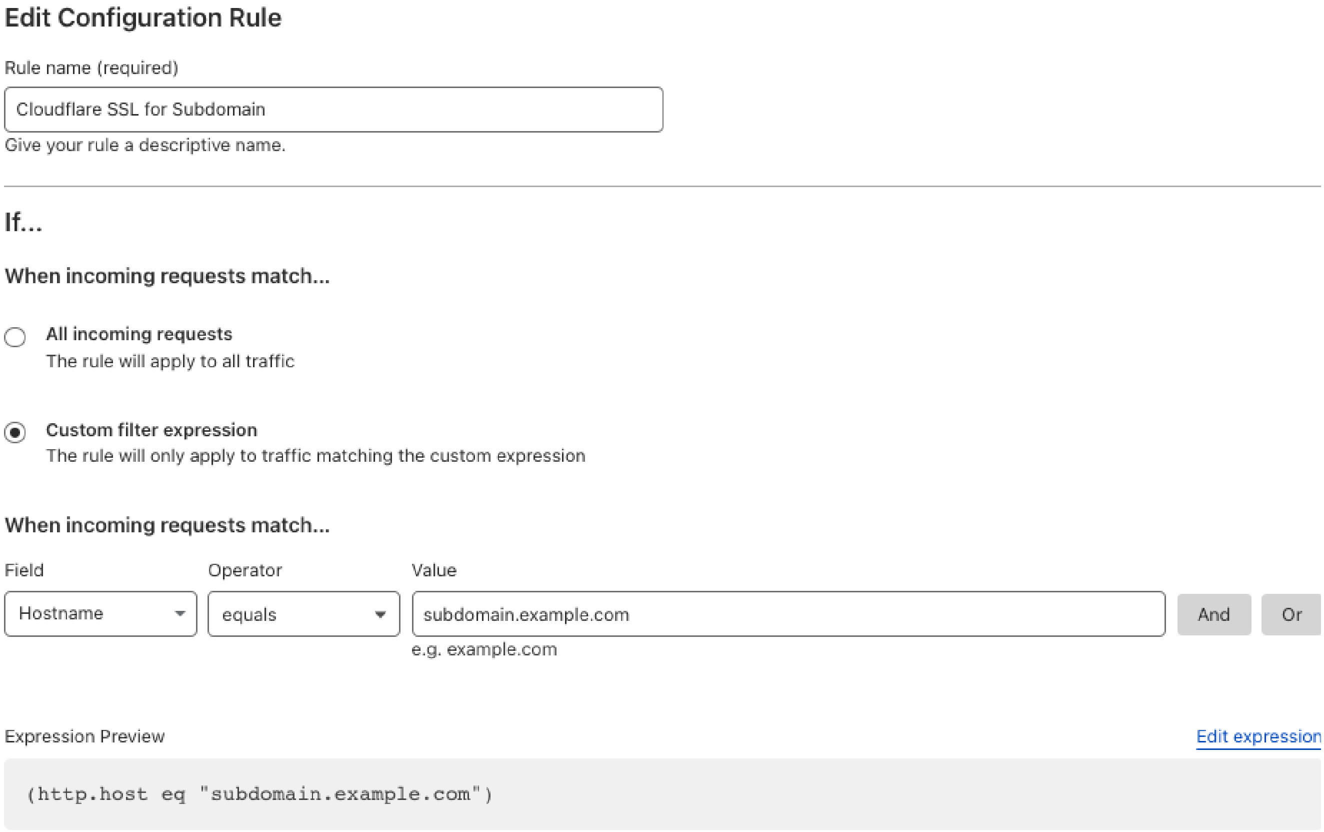
● **Full (strict)**
Encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server

Learn more about End-to-end encryption with Cloudflare.

Create a Configuration Rule to customize these settings by hostname.

Option 2: To set up strict SSL verification for a **specific subdomain:**

1. In your domain's dashboard, navigate to `Rules > Configuration Rules` and click `Create Rule`
2. Name your rule, and configure the incoming request filters.



Edit Configuration Rule

Rule name (required)

Cloudflare SSL for Subdomain

Give your rule a descriptive name.

If...

When incoming requests match...

○ All incoming requests
The rule will apply to all traffic

● Custom filter expression
The rule will only apply to traffic matching the custom expression

When incoming requests match...

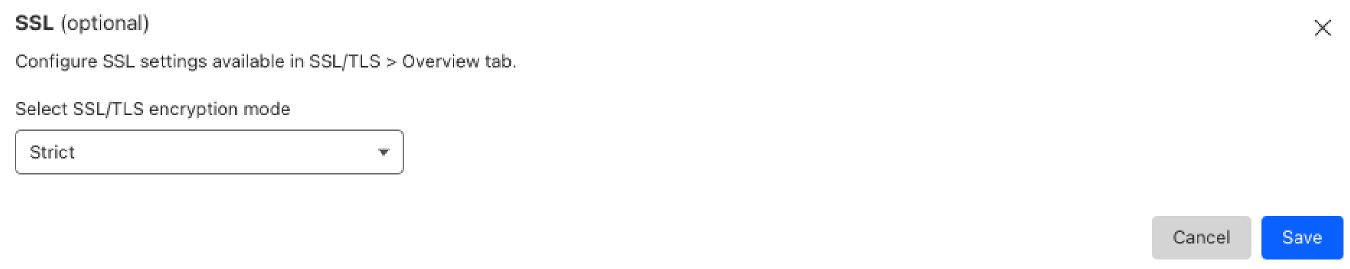
Field	Operator	Value
Hostname	equals	subdomain.example.com

e.g. example.com

Expression Preview

```
(http.host eq "subdomain.example.com")
```

3. Configure the SSL to `Strict`



SSL (optional)

Configure SSL settings available in SSL/TLS > Overview tab.

Select SSL/TLS encryption mode

Strict

4. Click `Save`

Option 3: Manual configuration (Advanced)

If you need a custom implementation, you can disable the creation of an SSL certificate with the following steps.

> Create a CNAME record for your Cloudflare entry and point to the CNAME provided for that service in the Elestio dashboard.

> These changes can be overwritten in the future if you modify the list of domains via the Elest.io dashboard.

1) Connect to the VM with SSH and type this:
nano /opt/elestio/nginx/.env

there remove your domain from the first line and save with CTRL+X

then type this command:
cd /opt/elestio/nginx;
docker-compose down;
docker-compose up -d;

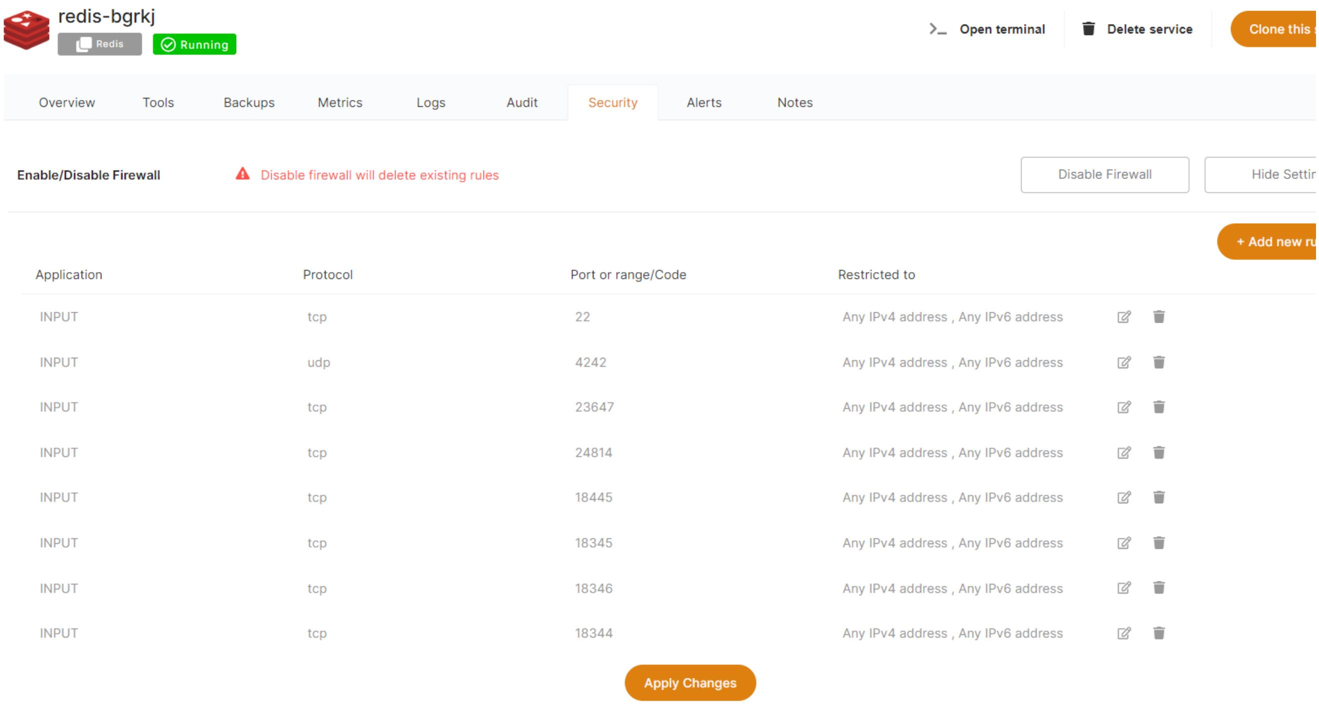
After that, nginx won't try again to obtain an SSL certificate for your domain.

Network Firewall

> By default, we only open the ports necessary for the application you have deployed.

How can I restrict access to my service by IP address?

From the Dashboard, select "***Security***", then "***Show Settings***" on the Firewall row



Enable/Disable Firewall

Disable firewall will delete existing rules

Application	Protocol	Port or range/Code	Restricted to
INPUT	tcp	22	Any IPv4 address , Any IPv6 address
INPUT	udp	4242	Any IPv4 address , Any IPv6 address
INPUT	tcp	23647	Any IPv4 address , Any IPv6 address
INPUT	tcp	24814	Any IPv4 address , Any IPv6 address
INPUT	tcp	18445	Any IPv4 address , Any IPv6 address
INPUT	tcp	18345	Any IPv4 address , Any IPv6 address
INPUT	tcp	18346	Any IPv4 address , Any IPv6 address
INPUT	tcp	18344	Any IPv4 address , Any IPv6 address

From there you can modify, remove, or add new rules to open a port from your service to the internet (or just to a specific target IP).

> All services come preconfigured with firewall rules that match the software you are deploying.

> You have to keep port 80 open to any ipv4/ipv6 or else Letsencrypt won't be able to generate an SSL certificate.

Here is a compilation of the ports necessary for Elestio Automation:

Mandatory	Application	Protocol	Port	Usage
✔	Input	TCP	22	Automation SSH
□	Input	UDP	4242	Nebula/ Global IP
□	Input	TCP	18345	VS Code
□	Input	TCP	18374	Open Terminal
□	Input	TCP	18346	File Explorer
□	Input	TCP	18445	Tail Logs
□	Input	TCP	18344	Terminal

□ => Ports are necessary only if you are utilizing specific tools and activating global private IP functionality.

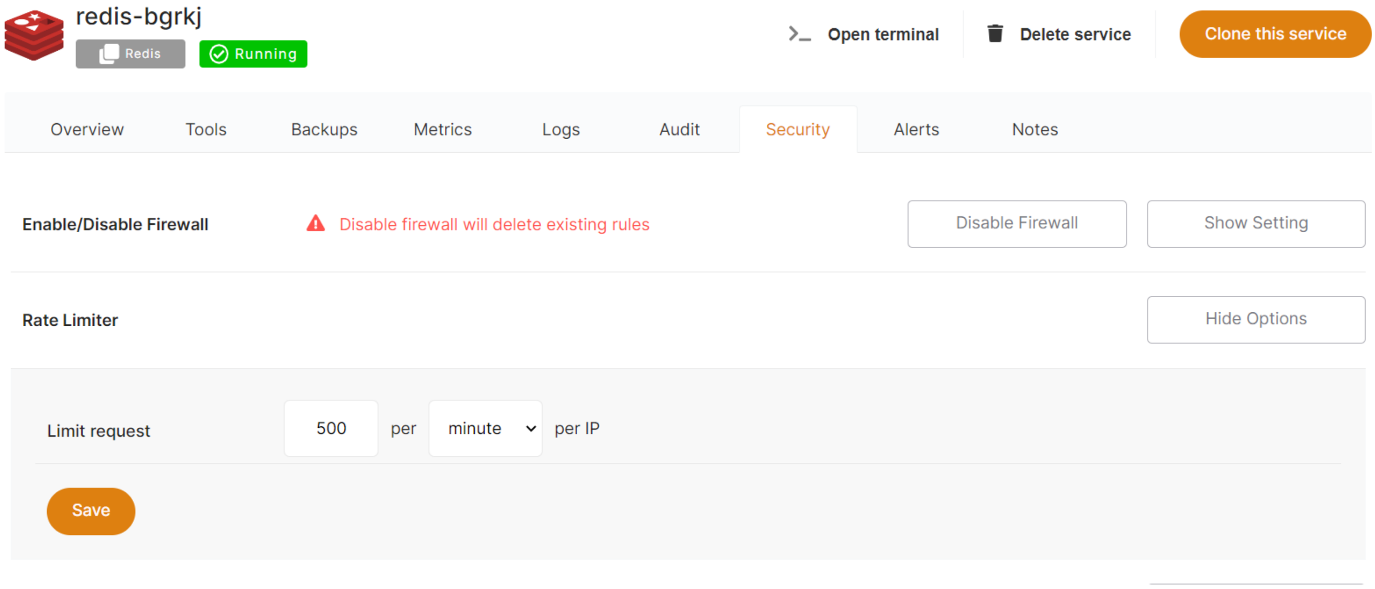
IP rate limiter

From the Dashboard, click on *Security* then Rate Limiter > *Show Options.*

From here, you can easily modify and adjust your service's rate limiter configurations, by amount and per minute or second, per IP address.

> By default, all services are preconfigured with a rate limiter of 150 requests per minute and per IP address.

> Rate limiter is used only for web traffic.



redis-bgrkj

Enable/Disable Firewall

⚠ Disable firewall will delete existing rules

Rate Limiter

Limit request 500 per minute per IP

Output Cache

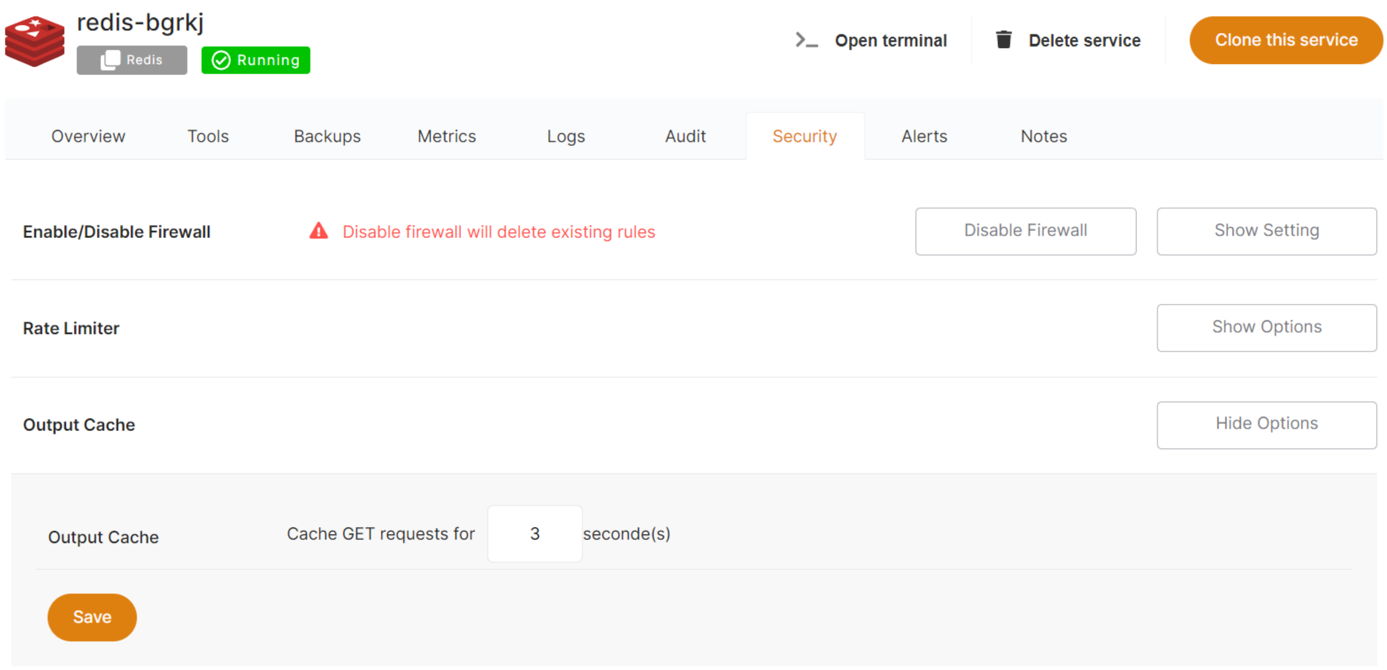
From the Dashboard, navigate to the *Security* tab and select *Show Options* under Output Cache.

From here, you can modify your output cache configurations.

All GET requests are cached for 3 seconds, which is useful in preventing Denial of Service (DOS) attacks.

> All services come preconfigured with Output cache by default.

> Output cache is used for web traffic only.



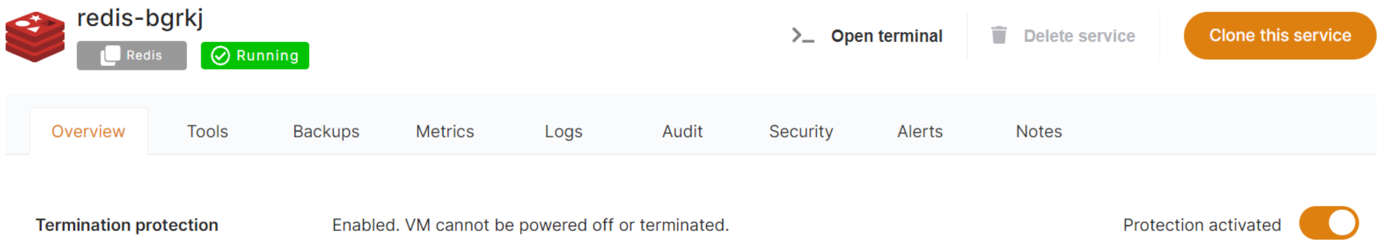
redis-bgrkj

Disable firewall will delete existing rules

Output Cache — Cache GET requests for 3 seconde(s)

Termination protection & grace period

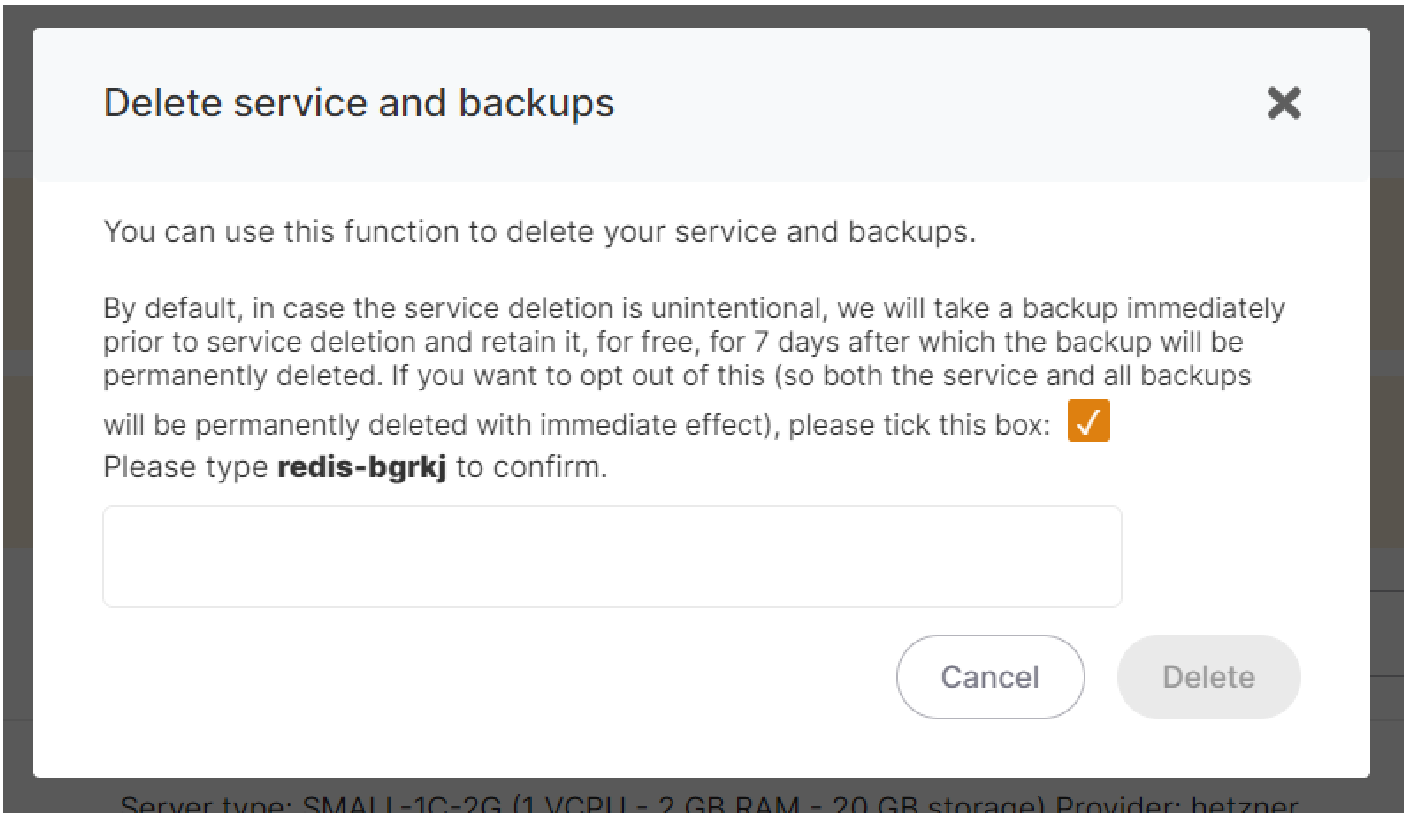
You can enable or disable the **Termination protection** option from your Dashboard *Overview*, using the toggle on the right-hand side. This setting is disabled by default.



Termination protection — Enabled. VM cannot be powered off or terminated. — Protection activated

> It's not possible to change software versions, delete, shut down, power off, reset or reboot your service when Termination protection is enabled. To make these changes, you must first disable Termination protection.

> Our grace period for storing backups after the deletion of service is 7 days, making it easier for you to restore your service in this window of time for any reason.



You can use this function to delete your service and backups.

By default, in case the service deletion is unintentional, we will take a backup immediately prior to service deletion and retain it, for free, for 7 days after which the backup will be permanently deleted. If you want to opt out of this (so both the service and all backups will be permanently deleted with immediate effect), please tick this box: ☑

Please type **redis-bgrkj** to confirm.

Server type: SMALL-1C-2G (1 VCPU - 2 GB RAM - 20 GB storage) Provider: hetzner

Manage SSH Keys

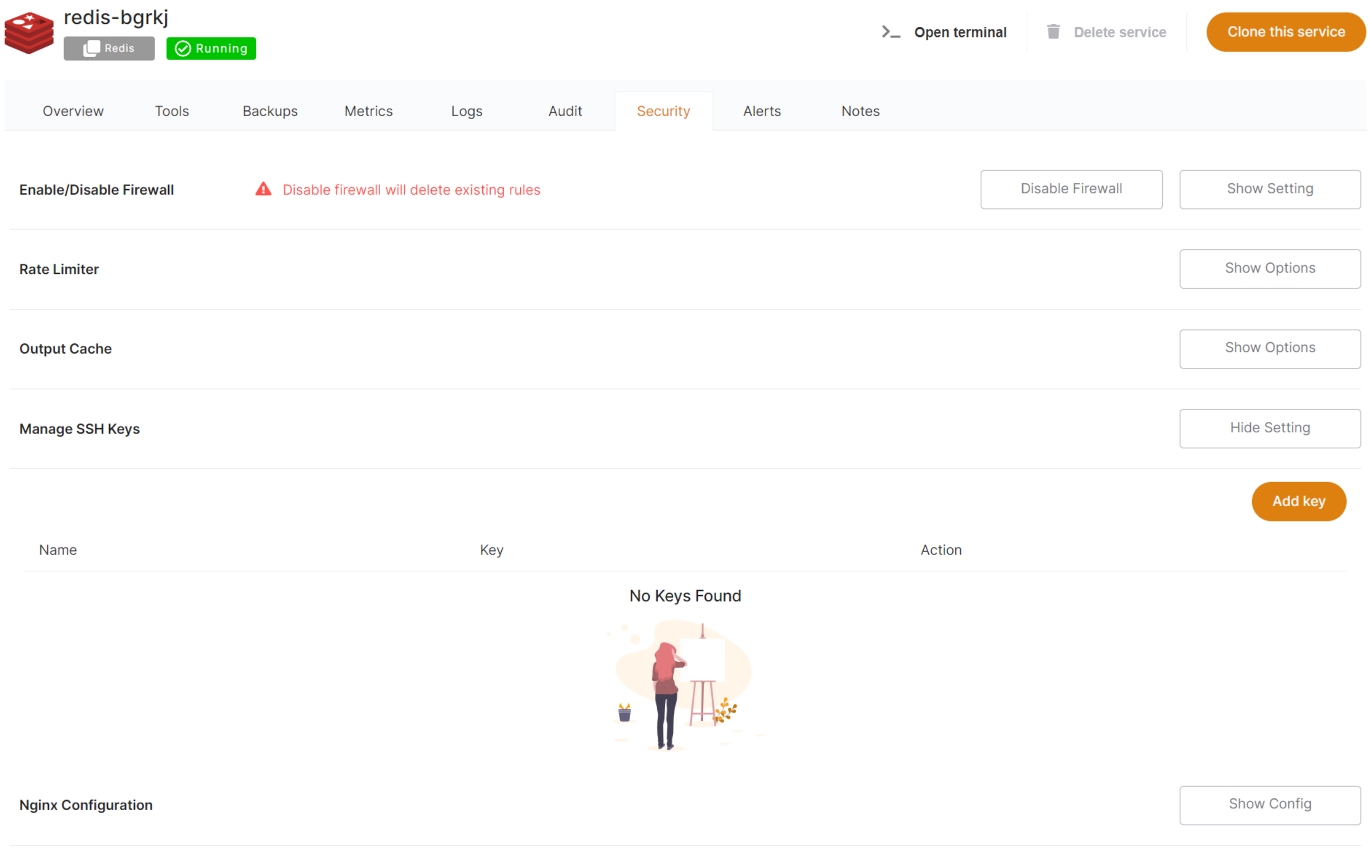
From the Dashboard, navigate to the *Security* tab and select the *Show Options* button to Manage SSH Keys.
From here, you can add or remove SSH keys allowed on the server.

Add an SSH key

Click on the *Add key*. Simply give your key a title and save!

Deleting an SSH key

Select the 'trash' icon to the right of the key you wish to delete. We'll always double-check with you before making a deletion, just to be sure!



Disable firewall will delete existing rules

Name	Key	Action

No Keys Found

How to connect to an Elestio service with SSH keys

Connecting to an Elestio service Using Existing SSH Keys from a Mac/Linux Machine

Step 1: Check for Existing SSH Key Pair

First, verify if you have an existing SSH key pair by checking the `.ssh` directory. Open a terminal and execute the following command:

```
ls ~/.ssh
```

The file with the `.pub` extension is your public key.

If you don't have an existing SSH key pair, you can generate a new one using the following command:

```
ssh-keygen -b 4096 -t rsa
```

Step 2: Copy your SSH Public Key to your Elestio service

1. Copy the Public Key to Clipboard:
   Navigate to the `.ssh` directory by typing

```
cd .ssh
```

Display the contents of your public key using `cat`. For example, if your public key is `id_ed255518.pub`, you can view it with:

```
cat ~/.ssh/id_ed255518.pub
```

Copy the displayed public key and add it to your Elestio service.

2. Add the Public Key to Elestio:
    - Open your Elestio service and navigate to the 'Security' tab.
    - Go to **'*Manage SSH Keys*'** and click on the 'Add key' button.
    - Paste your public key into the provided field.

Step 3: Confirm and Test Connection

To test the SSH connection to your VM, use the following command from your local machine:

```
ssh root@IPV4_TARGET_VM
```

Replace "IPV4_TARGET_VM" with the actual IPv4 address of your target VM, which you can find in the 'Overview' tab of your service.

For example:

```
ssh root@128.144.84.22
```

If the connection is successful, you'll be logged into your VM □□

Connecting to an Elestio service Using Existing SSH Keys from a Windows Machine with WSL (Windows Subsystem for Linux)

Step 1: Set up WSL (Windows Subsystem for Linux)

Before proceeding, you need to ensure that WSL is installed and configured on your Windows machine. Here's how you can set up WSL:

1. Enable WSL: Open PowerShell as Administrator and run the following command:

   ```
   wsl --install
   ```

   This command will automatically enable the necessary features and install the latest version of WSL on your system.
2. Install a Linux Distribution: After WSL is installed, visit the Microsoft Store and search for your preferred Linux distribution (e.g., Ubuntu). Click "Install" to download and install it.
3. Initialize WSL: Once the distribution is installed, launch it from the Start menu. This will initialize the distribution and prompt you to create a user account and set up a password.
4. Update and Upgrade: After the setup is complete, it's a good idea to update and upgrade the packages within your Linux distribution to ensure you have the latest versions. You can do this by running the following commands:

   ```
   sudo apt update sudo apt upgrade
   ```

   Follow the same tutorial to connect to an Elestio service using existing SSH keys from a Mac/Linux machine.

SMTP service

All deployed services include a basic preconfigured SMTP service, useful for sending alerts and notifications from your service.

This is free, but comes with a few limitations:

- You can only send transactional emails. Marketing emails are not permitted.

  > *Any violation of this will lead to a suspension or termination of your service.*

- You can send up to 300 transactional emails per hour. That's up to 7200 emails per day!
- All emails must be sent from **[domain]@vm.elestio.app** where **[domain]** is the URL of your service.

  > *Attempts at sending from any other email address will be rejected.*

- The SMTP service is only available from the global private network IP of your VM.

Of course in several cases you will want to change the smtp configuration in the web UI of your software to use another smtp service. It's useful if you want to be able to configure another sender address or to overcome any limitations stated above.

Check out our list of recommended SMTP providers:

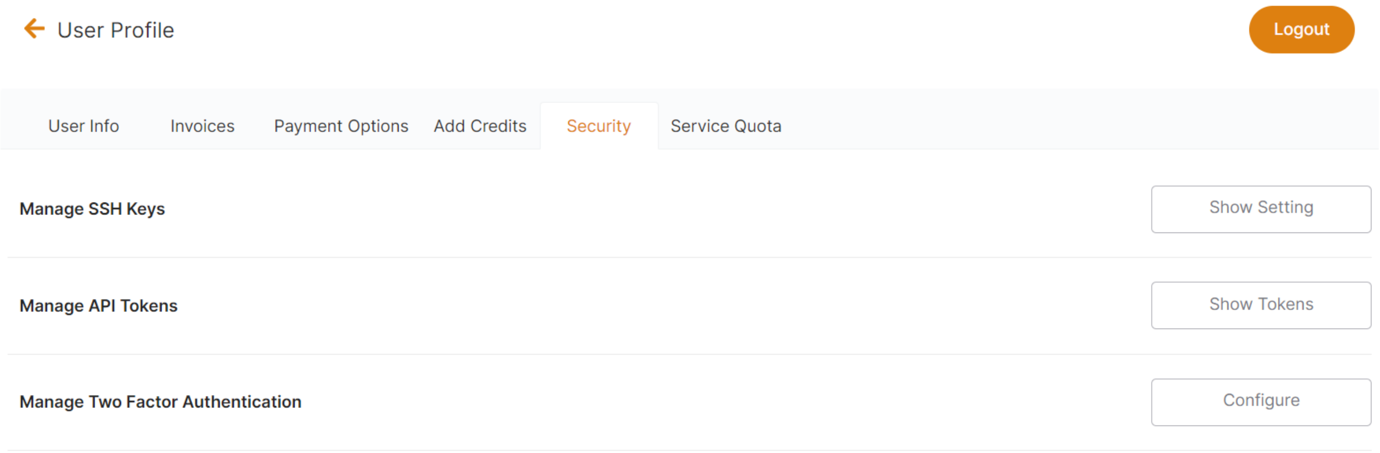
- AWS SES
- SendInBlue
- Mailgun
- Sendgrid

Multi-factor authentication

By default, Elestio uses Email-based MFA, each time you log in to Elestio we will send you an email with a one-time code to enter into our UI to be able to connect. This protection is in place to enforce security and avoid account hacking.

We also have TOTP-based MFA, this is more secure because it's based on an app installed on your phone to generate TOTP codes instead of us sending them by email. So even if your mailbox is compromised your Elestio account will still be safe.

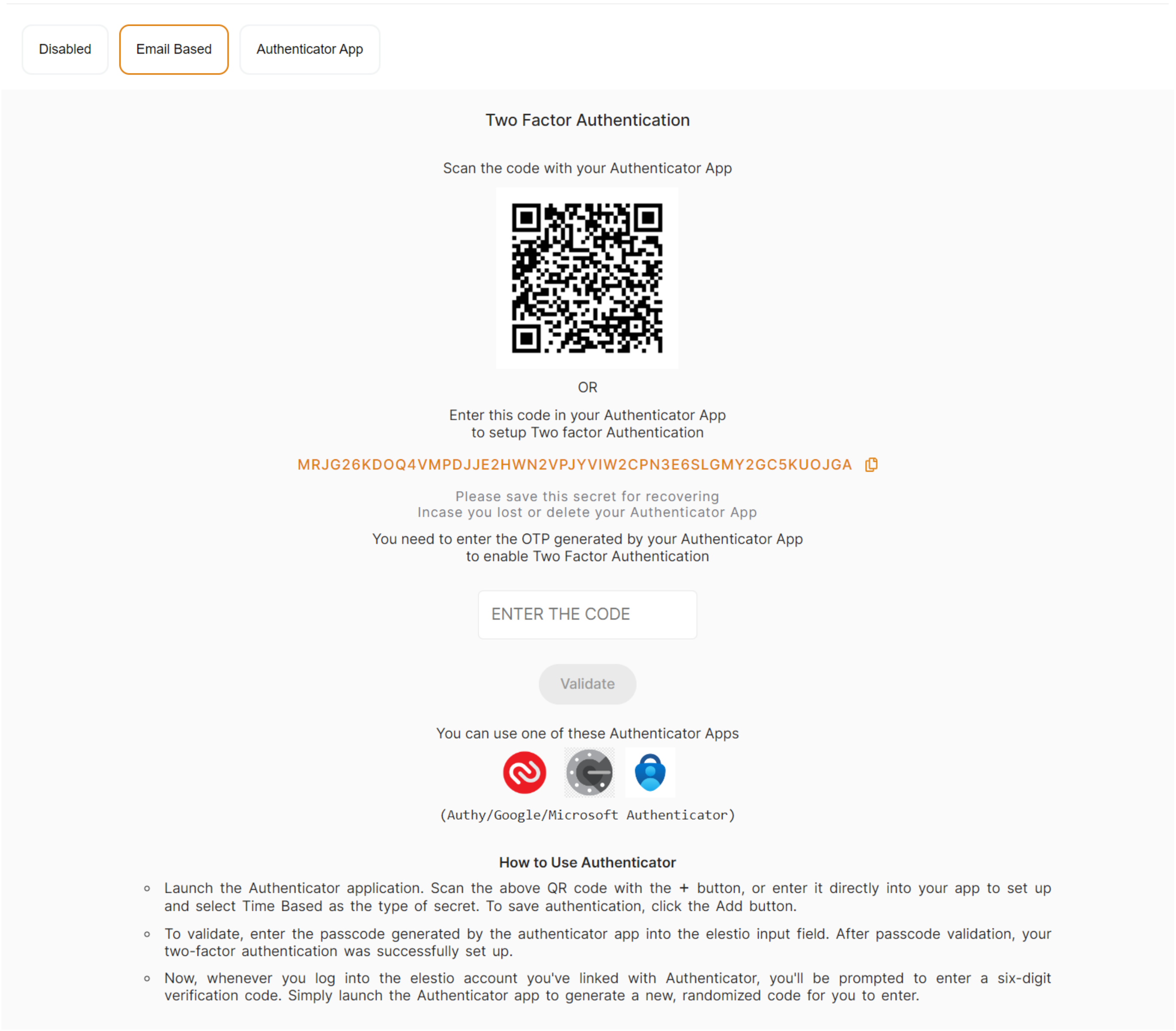
We recommend all users use TOTP Generator, you can activate it in a few clicks from our dashboard > user profile > Security tab.



Manage SSH Keys

Manage API Tokens

Manage Two Factor Authentication



Two Factor Authentication

Scan the code with your Authenticator App

OR

Enter this code in your Authenticator App
to setup Two factor Authentication

MRJG26KDOQ4VMPDJJE2HWN2VPJYVIW2CPN3E6SLGMY2GC5KUOJGA

Please save this secret for recovering
Incase you lost or delete your Authenticator App

You need to enter the OTP generated by your Authenticator App
to enable Two Factor Authentication

You can use one of these Authenticator Apps

(Authy/Google/Microsoft Authenticator)

How to Use Authenticator

- Launch the Authenticator application. Scan the above QR code with the + button, or enter it directly into your app to set up and select Time Based as the type of secret. To save authentication, click the Add button.
- To validate, enter the passcode generated by the authenticator app into the elestio input field. After passcode validation, your two-factor authentication was successfully set up.
- Now, whenever you log into the elestio account you've linked with Authenticator, you'll be prompted to enter a six-digit verification code. Simply launch the Authenticator app to generate a new, randomized code for you to enter.

The process to activate TOTP MFA on your account

1. Open the account security tab here: **https://dash.elest.io/account/security**
2. Click on Configure button in Manage Two-Factor Authentication.
3. Select the **Authenticator App** tab.
4. Download an authenticator app: **Authy** (recommended) or **Google Authenticator** or **Microsoft Authenticator**
5. Open your authenticator app then scan the QR code on the screen
6. Generate a code with your app and enter it on the Elestio screen
7. Click on Validate

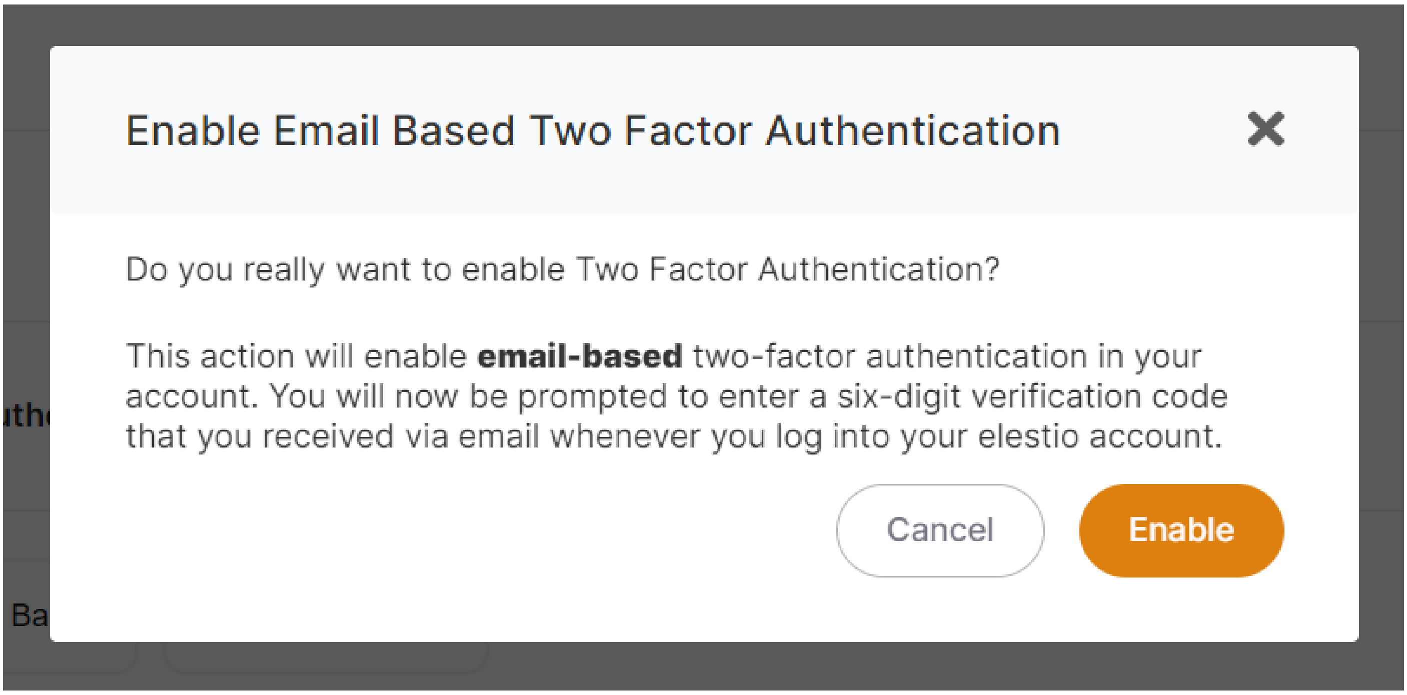
Done, Strong MFA is now enabled on your account, and will be required to login into your Elestio account

> You should keep the text version somewhere safe (in orange in the screenshot), this will allow you to recover in case you lose your phone or authenticator app.

> If you have lost both your authenticator app and text secret, you can contact our support team via ***email*** with proof of identity to get MFA removed from your account.

The process to Activate Email Based MFA on your account

1. Open the account security tab here: **https://dash.elest.io/account/security**
2. Click on Configure button in Manage Two-Factor Authentication.
3. Select the **Email Based** tab.
4. Click on Enable button to activate it.



Enable Email Based Two Factor Authentication

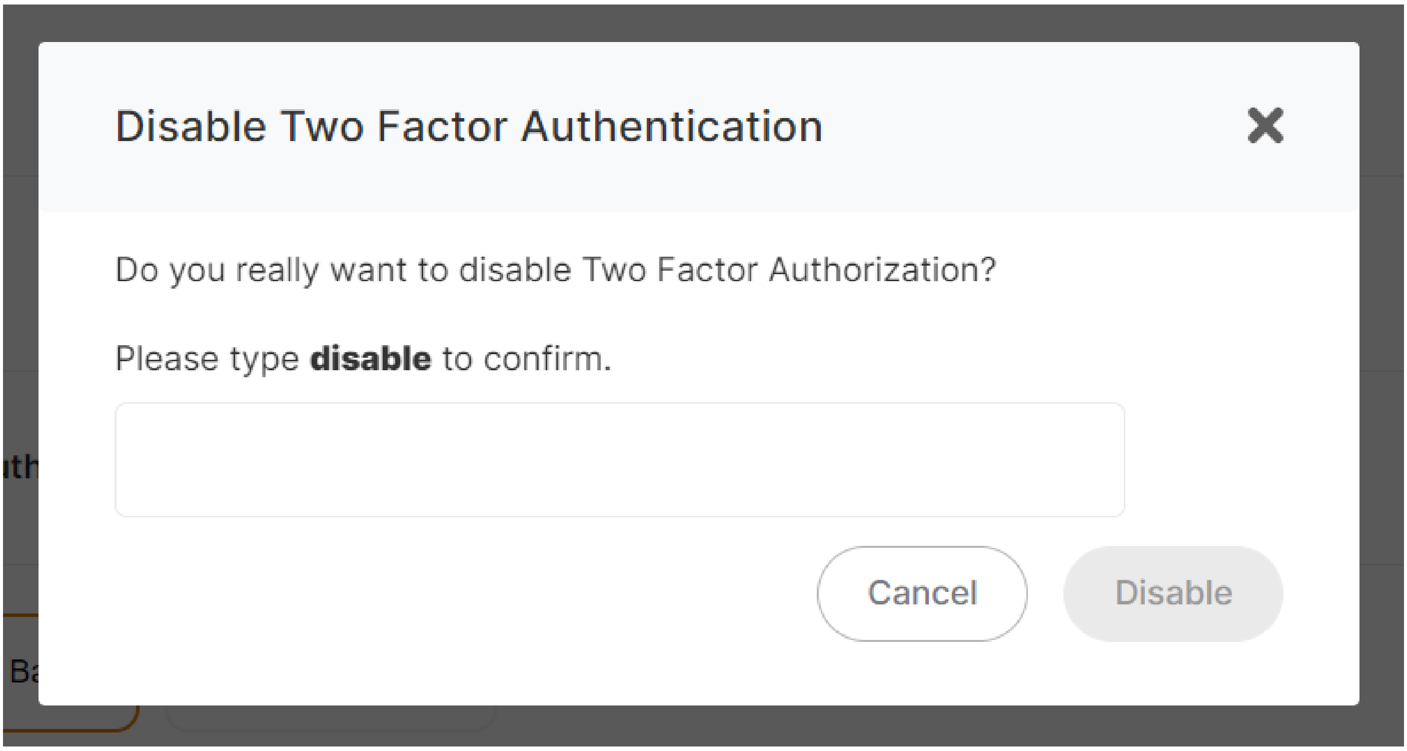
Do you really want to enable Two Factor Authentication?

This action will enable **email-based** two-factor authentication in your account. You will now be prompted to enter a six-digit verification code that you received via email whenever you log into your elestio account.

The process to Deactivate MFA on your account

1. Open the account security tab here: **https://dash.elest.io/account/security**
2. Click on Configure button in Manage Two-Factor Authentication.
3. Select the **Disabled** tab.
4. To confirm the action, type disable in the confirmation input field on the confirmation modal.

5. Click on Disable button to disable it.



Disable Two Factor Authentication

Do you really want to disable Two Factor Authorization?

Please type **disable** to confirm.