

3 - Admin Panel - Manage Users, Domains, Aliases and More

The [Admin Panel](https://admin.emailarray.com/) is located at this link: <https://admin.emailarray.com/>.

This interface will let you manage your domains, users (mailboxes), aliases, lists, branding, and domain-wide preferences.

Some settings overlap with the User-defined settings. In these cases, the User preferences will take over. For example, as an Admin, you can blacklist the domain "abcd.com," but if a user whitelists "joe@abcd.com," the whitelist will take priority.

Check the pages below to find out how to perform everyday administration tasks.

What's my Admin username?

When you signed up for an account, you chose a username (it might be your signup email address) and password for managing your account. This is the Admin Account that you can use to log in to the [Admin Panel](#).

- [Change Admin password](#)
- [Manage Sub-Admins](#)
- [Security](#)
 - [2FA - Two-factor authentication](#)
 - [Restrict Login Access: Admin IP Access Lists](#)

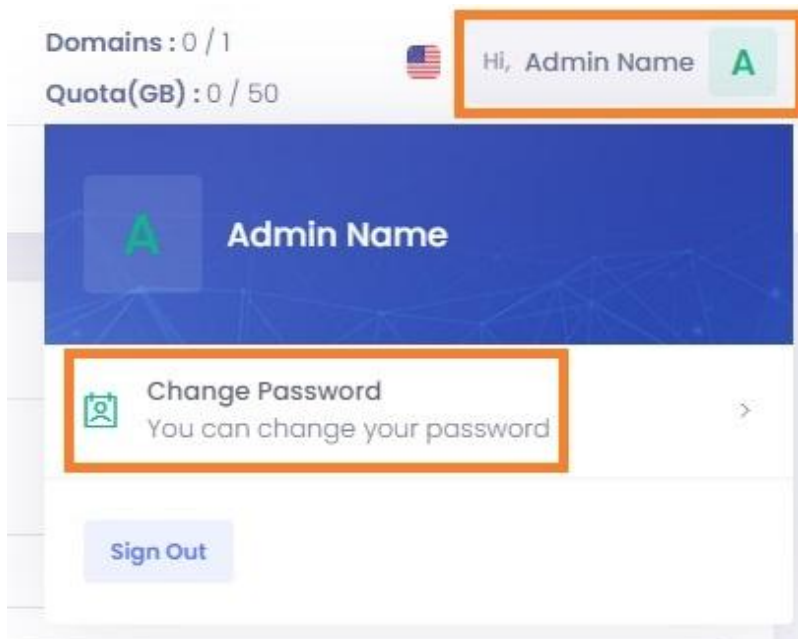
- [Security Incidents](#)
- [User Trusted Login IPs](#)
- [Manage Domains](#)
- [Manage Users](#)
- [Manage Alias Domains](#)
- [Manage Aliases](#)
- [Manage Lists](#)
- [Manage Smart Lists](#)
- [Filtering: Whitelist / Blacklist](#)
 - [Set Domain Spam filter preferences](#)
 - [Manage Whitelists and Blacklists](#)
 - [Whitelist / Blacklist by IP - IP Access List](#)
- [Set Branding](#)
- [Logs](#)
 - [Outgoing logs - Track all Remote Deliveries](#)
 - [Incoming Logs - Track All Incoming Email](#)
 - [Last Logins – Monitor User Login Activity](#)

Change Admin password

Update Admin's password

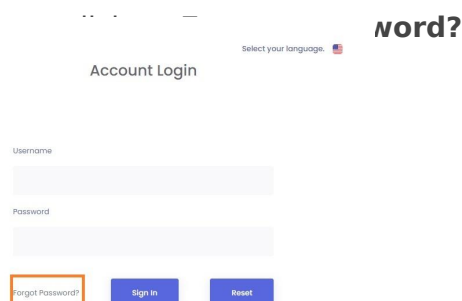
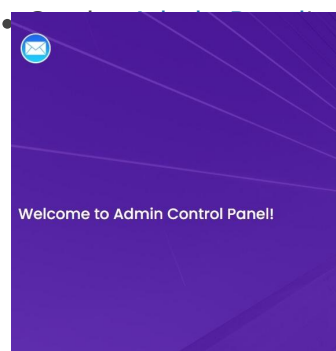
To change your Admin's password:

- Log in to the [Admin Panel](#).
- Click on your name in the top right corner. In that menu, click on **Change Password**.
- Fill in your new password, confirm it and click on **Change**.

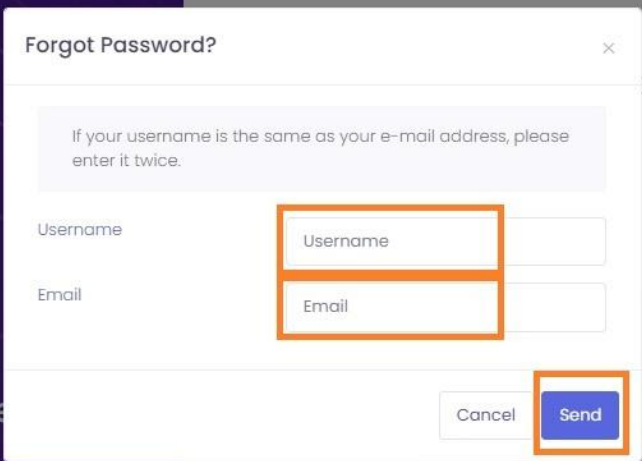


Reset Admin's password

If you don't remember your Admin password, you can request a password reset:

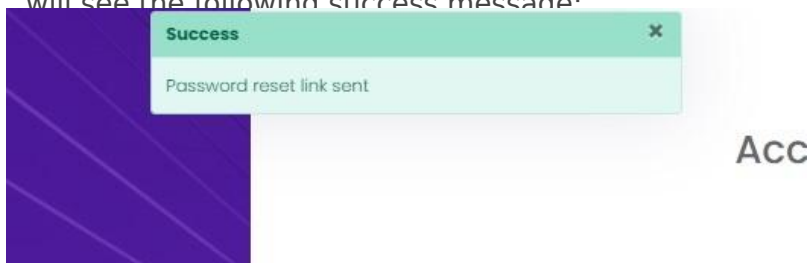


- In the new pop-up window, fill in your **Admin username** and recovery **e-mail address** the same as your e-mail address,

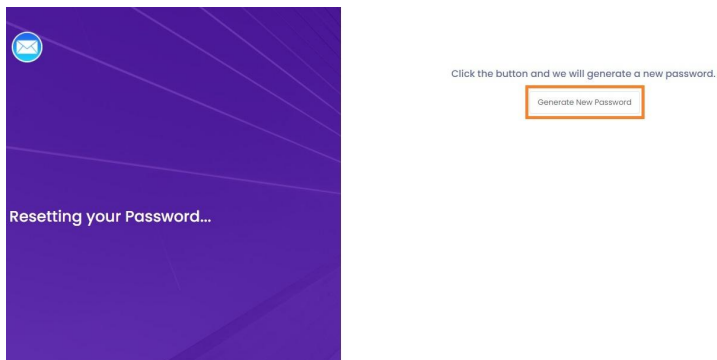


The screenshot shows a 'Forgot Password?' modal window. At the top, it says 'Forgot Password?' with a close button. Below that, a message states: 'If your username is the same as your e-mail address, please enter it twice.' There are two input fields: 'Username' and 'Email'. Both fields are highlighted with orange boxes. At the bottom right of the modal, there are two buttons: 'Cancel' and 'Send'. The 'Send' button is highlighted with an orange box. In the background, parts of the main page are visible, including a 'Forgot Password?' link and a 'Sign In' button.

- Click on **Send**. You will receive an e-mail with a link to reset your password. If your Admin username and recovery e-mail address match what we have on file for your account, you will see the following success message:



- Click on the link you received, and you should see the following page. Click on the



the next page. **Copy the new**

Click the button and we will generate a new password.



[Go to Login Page](#)

- **If you have 2FA (Two Factor Authentication) enabled for your Admin account, you can reset your password, but you still need to use the 2FA code from your 2FA App when logging in.**
- After you log in, please use the **Change Password** feature (see the steps above) to set up a custom password.

If resetting the password fails, check if your Admin account was locked for unpaid invoices. Please check your billing status for any failed invoices or contact support for more information.

Manage Sub-Admins

A Sub-Admin is a special Admin account. You can restrict the permissions on different levels (view, edit, delete permissions, or no access) for different sections of the Admin Panel (Users, Domains, Logs, etc.). Furthermore, you can restrict login access to only specific known IPs.

Some examples for using sub-admins are the following:

- API integration - you shouldn't use your main Admin account to authenticate with the API.
- WHMCS plugin - use a Sub-Admin to authenticate your WHMCS plugin
- dividing the work and responsibilities within a team - each team member can have a Sub-Admin

Best Practices

API Integration

For API authentication, you must use an Admin username and password. This is the setup we recommend:

- secure your main Admin account by activating Two-factor authentication. You can continue to use these credentials for Admin Panel direct login and perform actions via the web interface of the Admin Panel.
- create a Sub-Admin for API access only. You can enable only the permissions you integrate with the API or allow unrestricted access.
- secure your API Sub-Admin by restricting login access to specific IPs - these should be the IPs of your servers that connect through the API.
- optional: create other Sub-Admin for your team members that will use the web interface.

WHMCS Plugin

To connect your WHMCS using our plugin, you must authenticate using an Admin username and password. This is the setup we recommend:

- secure your main Admin account by activating Two-factor authentication. You can continue to use these credentials for Admin Panel direct login and perform actions via the web interface of the Admin Panel.
- create a Sub-Admin for WHMCS access only. You can allow unrestricted permissions.
- secure your WHMCS Sub-Admin by restricting login access to specific IPs - the IP of your WHMCS server.
- optional: create other Sub-Admin for your team members that will use the web interface.

Team members

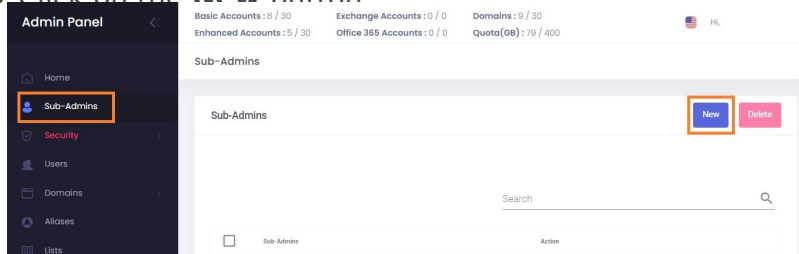
We don't recommend you share the same Admin account with other people, but instead, create a Sub-Admin for each member. This way, you can enable two-factor authentication for each and adequately secure your account.

Furthermore, you can set specific levels of access for each of the Sub-Admin and restrict the responsibilities of each member of your team.

Manage Sub-Admins

Add a Sub-Admin

- Go to the [Admin Panel](#).
- Log in using your **main Admin username** and password.
- Click on **Sub-Admins** in the menu.
- Click on the **New** button



- Fill in the details of your new Sub-Admin:
 - Sub-Admin **username**
 - Sub-Admin **password**
 - Sub-Admin **e-mail address** - will be used for password recovery
 - Sub-Admin **full name**
- Select the **permissions** for each section. Each level of permission is numbered; the higher levels include the ones below it (level 2 includes level 1, level 3 includes level 1 and 2, etc.):
 - Account History: see the actions performed by Admin and Sub-Admins on the Home page
 - Users: view/manage/remove/impersonate Users (mailboxes). The highest level is **5 - Impersonate** and allows you to "sign in as" the User into Webmail and User Panel.
 - Domains: view/manage/remove Domains.
 - Aliases: view/manage/remove Aliases.
 - Lists: view/manage/remove distribution Lists.
 - Smart Lists: view/manage/remove Smart Lists.
 - Branding: view/update branding settings for the main Admin account.
 - Filtering: view/modify/remove whitelist and blacklist entries for Spam Filtering.
 - Logs: view Incoming and Outgoing Logs, Last logins.
- Click on the **Add Subadmin** button to save.

Example:

Username	<input type="text" value="Username"/>		company-api	✓
Password	<input type="password" value="Password"/>		luh\$bg/3--	✓
Email Address	<input type="text" value="Email Address"/>		api@company.com	✓
Full Name	<input type="text" value="Full Name"/>		API	✓
Account History	0 - No access	⌵	0 - No access	⌵
Users	0 - No access	⌵	5 - Impersonate	⌵
Domains	0 - No access	⌵	3 - Remove	⌵
Aliases	0 - No access	⌵	3 - Remove	⌵
Lists	0 - No access	⌵	3 - Remove	⌵
Smart Lists	0 - No access	⌵	3 - Remove	⌵
Branding	0 - No access	⌵	0 - No access	⌵
Filtering	0 - No access	⌵	0 - No access	⌵
Logs	0 - No access	⌵	0 - No access	⌵

Remove a Sub-Admin

- Go to the [Admin Panel](#).
- Log in using your **main Admin username** and password.
- Click on **Sub-Admins** in the menu.

Admin Panel

Basic Accounts : 8 / 30 Exchange Accounts : 0 / 0 Domains : 9 / 30
Enhanced Accounts : 5 / 30 Office 365 Accounts : 0 / 0 Quota(GB) : 79 / 400

Sub-Admins

Sub-Admins

Search

Sub-Admins	Action
<input type="checkbox"/> teammember1	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> teammember2	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> company-api	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

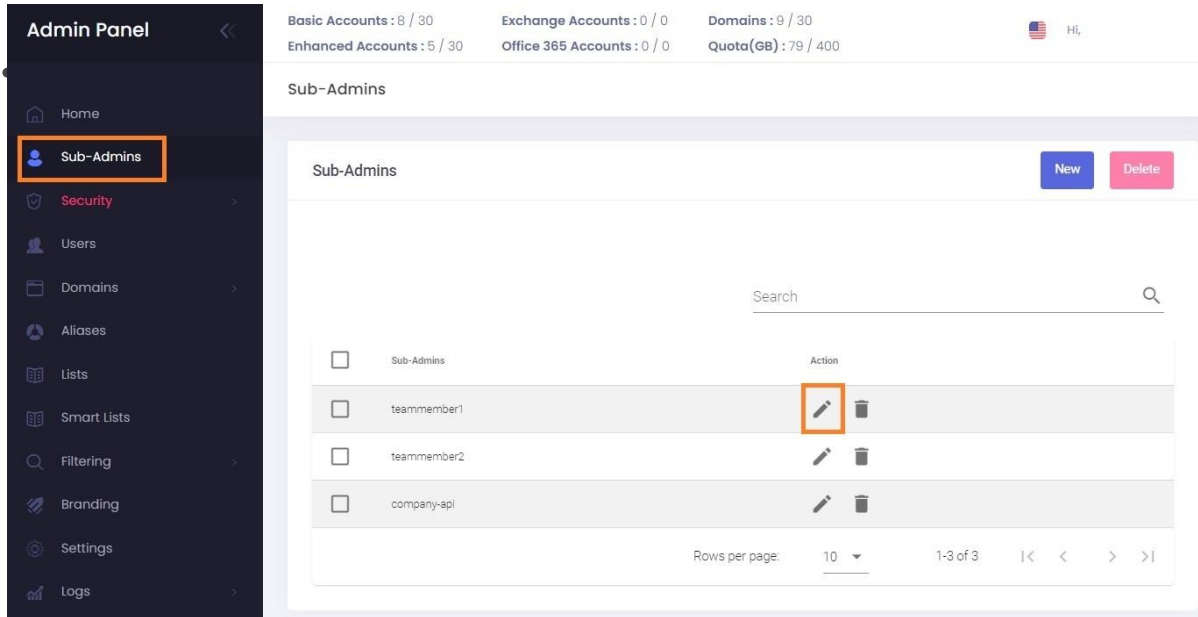
Rows per page: 10 1-3 of 3 |< > |

Update a Sub-Admin

You can update all the details and permissions of a Sub-Admin.

- Go to the [Admin Panel](#).
- Log in using your **main Admin username** and password.

- Click on **Sub-Admins** in the menu.
- Click on the **Edit (pencil)** button next to the Sub-Admin you want to update.
- Update the details. Leave the Password field blank if you want to update permissions but



Update teammember2

Higher level permissions include the ones before them

Username	teammember2
Password	Password
Email Address	
Full Name	teammember2
Account History	0 - No access
Users	5 - Impersonate
Domains	3 - Remove
Aliases	0 - No access
Lists	0 - No access
Smart Lists	0 - No access
Branding	0 - No access
Filtering	0 - No access
Logs	0 - No access

Cancel Update

Restrict Sub-Admin login access

Log in as the Sub-Admin and [follow the instructions for restricting login access](#).

Two-factor authentication for Sub-admins

Log in as the Sub-Admin and [follow the instructions for enabling two-factor authentication](#). Please note you cannot enable two-factor authentication for a Sub-Admin that you use for API or WHMCS authentication - use restricted login access instead.

Security

2FA - Two-factor authentication

Two-factor authentication, or **2FA** as it's commonly abbreviated, adds an extra step to your basic login procedure. Without 2FA, the password is your single factor of authentication: you enter your username and password, then you're done.

With 2FA, you log in to the Admin Panel by entering your username and password and the six-digit code provided by an app installed on your smartphone.

After the latest update of the Admin Panel, you will be prompted to enter the 2FA code in a new pop-up window.

Enable 2FA for the Admin Panel

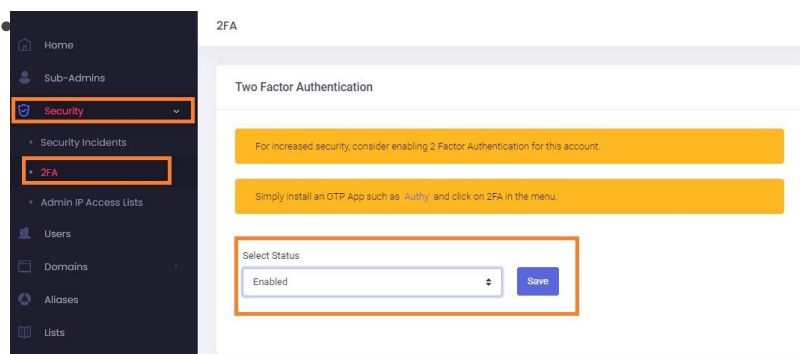
If you're using this Admin account as credentials for the API, the API login will fail after enabling 2FA. To solve this, create a Sub-Admin with special permissions for the API authentication only.

What you need:

- a smartphone with a 2FA App installed (OTP / 2-Step Verification / 2-Factor Authentication), such as [Authy](#) or [Google Authenticator](#).

To enable 2FA for your Admin account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **2FA**



on the **Save** button.

- Recheck the requirements: have a 2FA App installed on your phone.
- When ready, click on the **Next** button.

1. Please make sure you already installed an OTP App, such as [Authy](#).

2. In step 2, you will have to scan the QR Code using the OTP App.

3. When you are ready, hit the 'NEXT' button below.


Enable Two Factor Authentication: Step 2 ×

1. Scan this QR code using your OTP App.

2. Once the account is added, you will be given a 6 digit code.

3. Enter the code in the field below.

4. Hit 'SAVE' button below before your code expires.



Challenge:

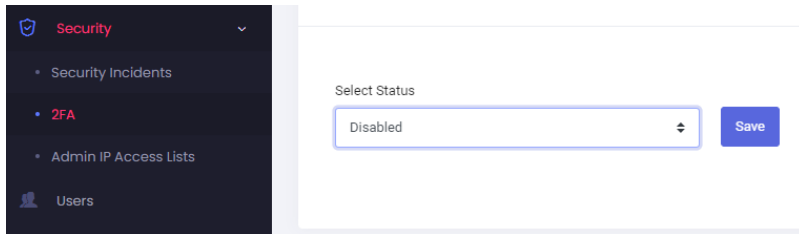
the generated six-digit code in the

es.

Disable 2FA for the Admin Panel

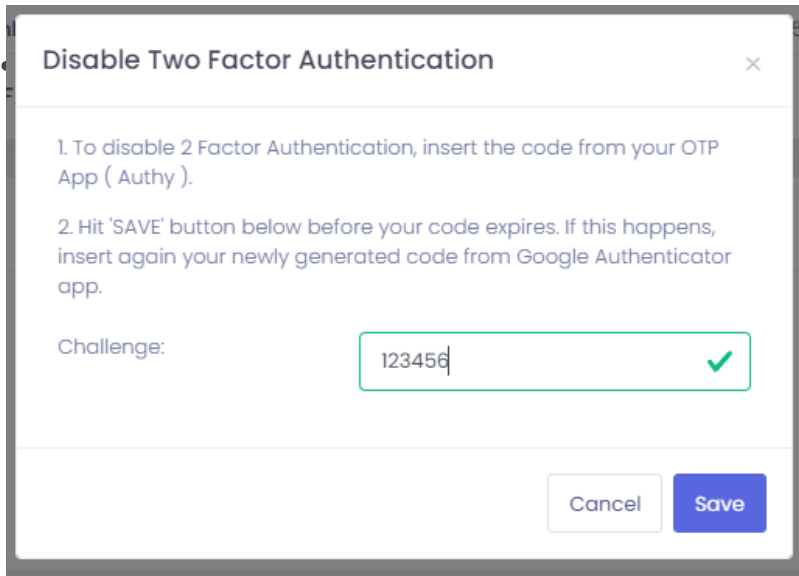
To disable the 2FA for your Admin account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **2FA**
- Update the dropdown **Select Status** to **Disabled**. Click on the **Save** button.



The screenshot shows a 'Security' sidebar on the left with options: Security Incidents, 2FA (highlighted), Admin IP Access Lists, and Users. The main content area has a 'Select Status' dropdown menu with 'Disabled' selected and a 'Save' button.

- Insert the token from your 2FA App (such as Authy or Google Authenticator) in the



The dialog box is titled 'Disable Two Factor Authentication' and contains the following instructions:

1. To disable 2 Factor Authentication, insert the code from your OTP App (Authy).
2. Hit 'SAVE' button below before your code expires. If this happens, insert again your newly generated code from Google Authenticator app.

Below the instructions, there is a 'Challenge:' label and a text input field containing the code '123456'. A green checkmark is visible to the right of the input field. At the bottom right, there are 'Cancel' and 'Save' buttons.

- After you see the confirmation message that the 2FA was disabled, you can delete the entry from your 2FA app.

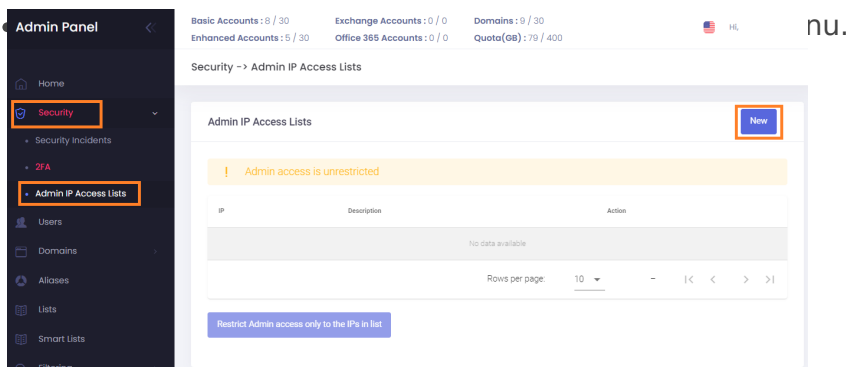
Restrict Login Access: Admin IP Access Lists

You can increase the security of your account by restricting login access for your Admin (or Sub-Admins) account to a list of know IPs, such as your office, your home, and server IPs for API or WHMCS authentication.

This feature works only with static IPs. Make sure your internet provider doesn't use dynamic IP addresses which change over time.

Add a new IP to the Access List

- Go to the [Admin Panel](#).
- Log in using your Admin (or Sub-Admin) username and password.



- Click on the **New** button.
- Fill in the IP and a description.
- Click on the **Add** button to save.

IP

Description

Cancel Add

Restrict Admin Login Access to only the IPs in the Access List

- Go to the [Admin Panel](#).
- Log in using your Admin (or Sub-Admin) username and password.

Security -> Admin IP Access Lists

Admin IP Access Lists

! Admin access is unrestricted

IP	Description	Action
1.1.1.1	Office	
2.2.2.2	Server API	
3.3.3.3	Home Office	

Rows per page: 10 1-3 of 3 |< < > >|

Restrict Admin access only to the IPs in list

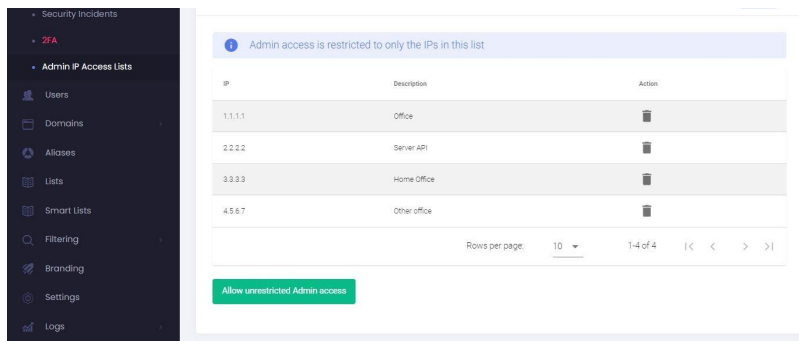
- Click on the **Restrict Admin access only to the IPs in list** button.

Restrict Admin access only to the IPs in list

Warning: make sure your IP is in the Admin IP Access List. Otherwise, you might lock yourself out.

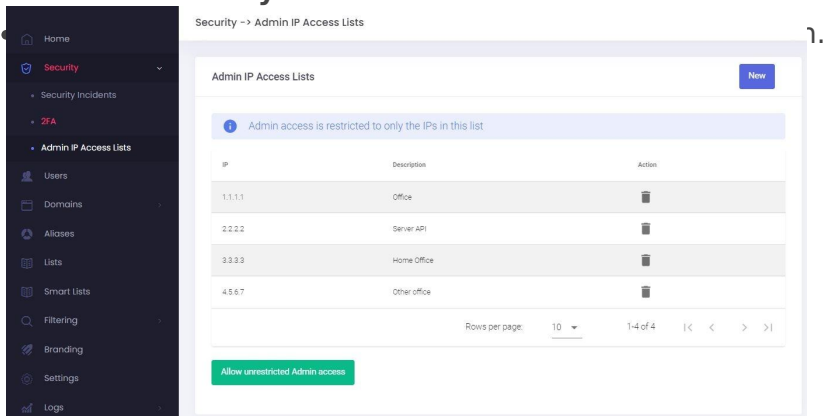
Cancel Restrict

- Access is now restricted to the IPs in your list:



Allow unrestricted access for Admin (or Sub-Admin)

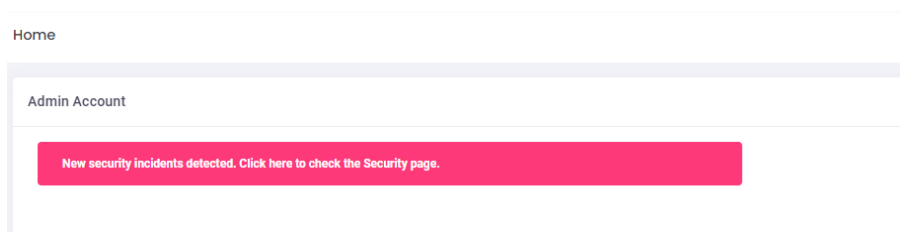
- Go to the [Admin Panel](#).
- Log in using your Admin (or Sub-Admin) username and password.
- Click on **Security** → **Admin IP Access Lists** in the menu.



Security Incidents

When you log in to the Admin Panel, on the Home page, you might see this warning message:

New security incidents detected. Click here to check the Security page.



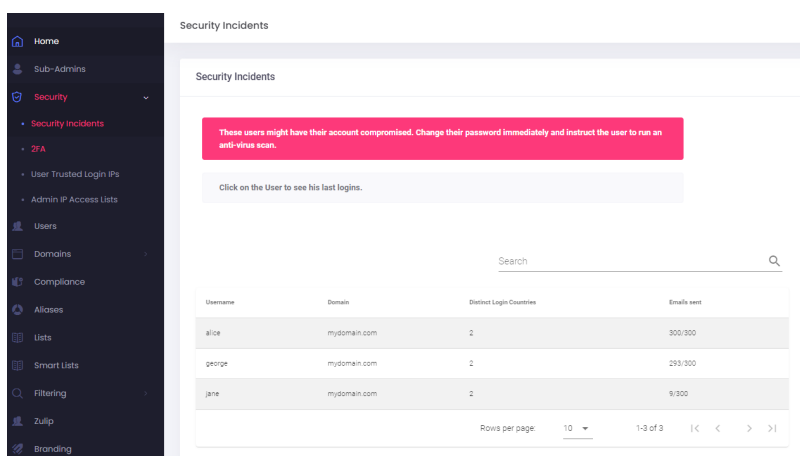
This happens when we detect suspicious logins from more than one location for one of your Users.

Click on the error message to go to the Security Incidents page and review each case.

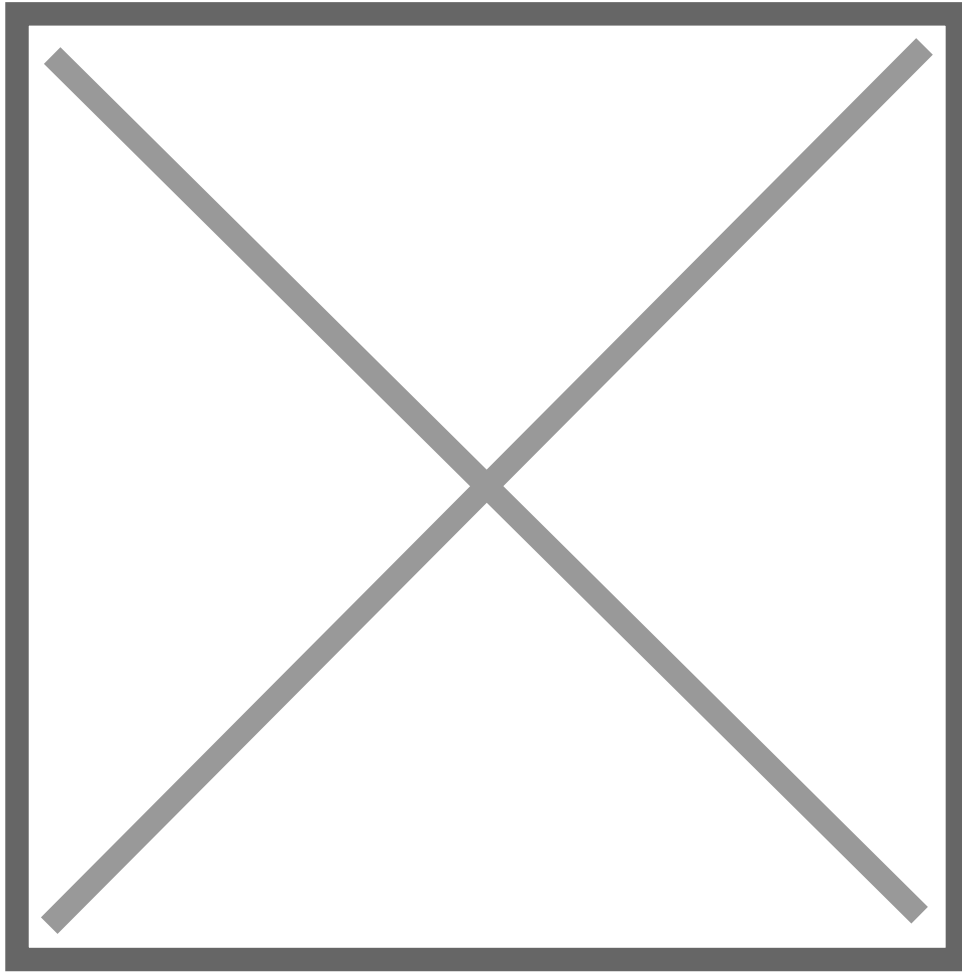
How to review a Security Incident case

To review the security incidents:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **Security Incidents**; or click on the error message from the Home page.
- You will see a list of Users that have triggered the warning.



- Check how many messages were sent in the last 24 hours and the number of distinct login countries. A higher number might suggest a compromised account.
- Click on each user to see a list of their Last Logins. Contact the customer if you suspect the account was compromised.



Possible reasons why the User is on the Security Incidents list

Compromised account

The User's account was compromised and an attacker is sending emails on his behalf or accessing the contents of his emails. This might happen if the User doesn't use a strong password, has malware installed or accessed his account from an insecure location / device and threat actor intercepted their password.

Third-party applications

Some applications that the User has setup will access the contents of his emails from different servers which will trigger the suspicious login warning. **You should inform the customer that the application has full access to their mailbox and make sure to read their Terms & Conditions about data processing.**

If the User is comfortable with the app having access to their data, you can follow the steps to **Mark IP as Safe.**

Some examples of such applications include:

- CRM applications (such as [Hubspot](#), [Salesforce](#), etc.)
- Sales automation applications
- Email clients (such as [Outlook](#), [MyMail](#), etc.) that read and process all the User's data through their servers. This includes your password in the clear(!) and all e-mail content

User is traveling

A legitimate case is when the User is traveling and is logging in from new locations.

Mobile connection

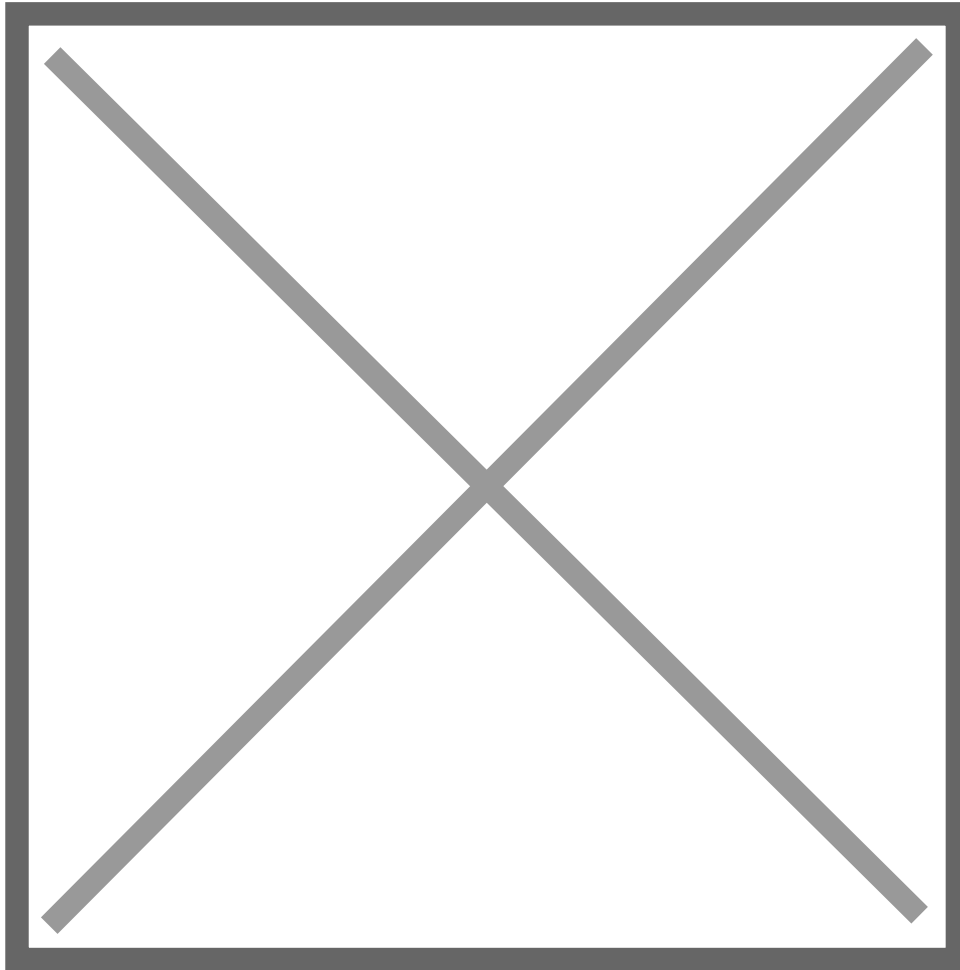
The User is accessing the service using a mobile connection that keeps renewing the IP.

Mark IPs as safe

In case of legitimate use, the IPs can be marked as safe and will not trigger the Security Incident warning anymore.

To mark an IP as safe:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **Security Incidents**; or click on the error message from the Home page.
- Click on the User for which you want to mark an IP as safe. This will take you to his **Last Logins** logs.



- In the Last Logins logs, you can click on the **Mark as Safe** button next to the IP you want to whitelist.
- In the new pop-up, give a description to the IP (mandatory) and choose whether you want to mark as safe only the IP or the entire network (with options from /31 to /22)
- If you wish to whitelist all of Google's IPs, please set the Range to /17
- If you wish to whitelist all of myMail's IPs, please set the Range to /22



- Click on the **Mark as Safe** button to save the changes.
- You can remove an entry anytime.

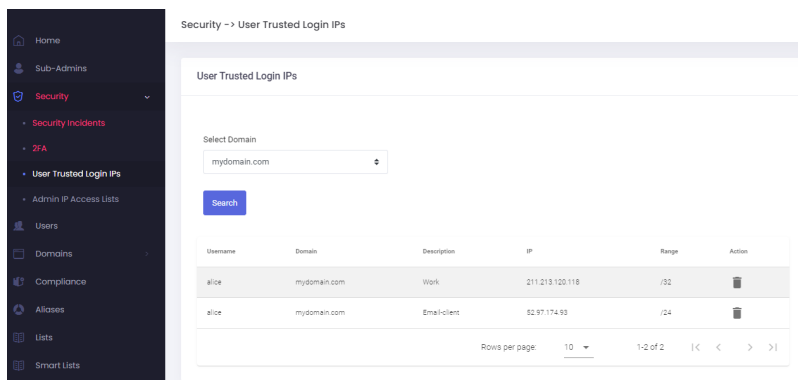
User Trusted Login IPs

You can mark as safe the IPs that your Users log in from. Use the Mark as Safe feature whenever a Security Incident is considered as safe - logins from the safe IP will not trigger Security Incident warning anymore.

Manage User Trusted Login IPs

To manage the User trusted login IPs for an account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **User Trusted Login IPs**
- Select the domain from the dropdown and click on the **Search** button.
- A list of all trusted IPs that were previously Marked as Safe will show.



- You can delete an entry at anytime
- To add a new trusted IP, [follow these steps](#).

Manage Domains

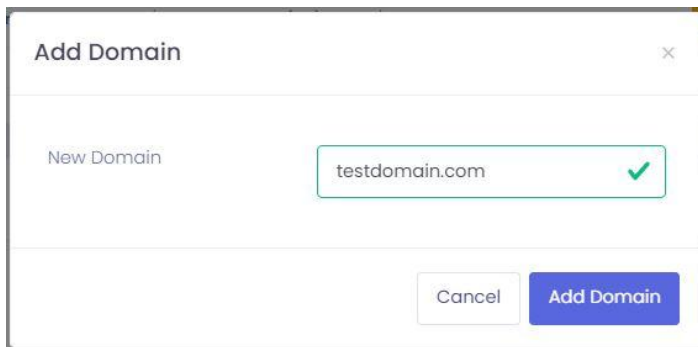
Domains are managed from the [Admin Panel](#). Here you can add or remove domains, set up a catchall, or define a domain-level time zone or footer.

Adding a New Domain

This guide will walk you through the process of adding a new domain to your account via the **Admin Panel**.

Steps to Add a Domain

- Navigate to the [Admin Panel](#).
- Log in using your **Admin username** and **password**.
- Verify that you have a sufficient domain quota available. This information is visible in the top menu bar of the Admin Panel.
- In the side menu, click on **Domains**.
- Click on the **New** button, located in the upper right corner of the Domains section.



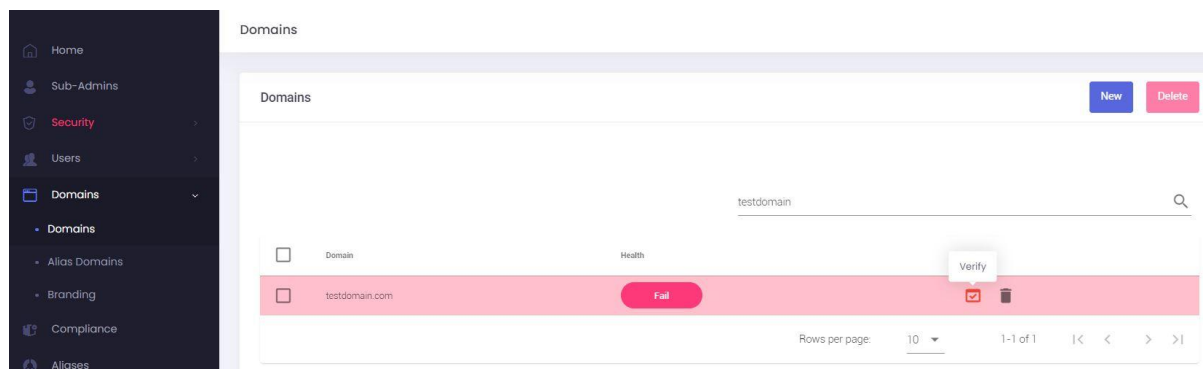
- In the **New Domain** field, enter the full domain you wish to add (e.g., `testdomain.com`).
- Click on **Add domain** to create the domain.

You won't be able to add any mailboxes (Users) until you verify the domain ownership.

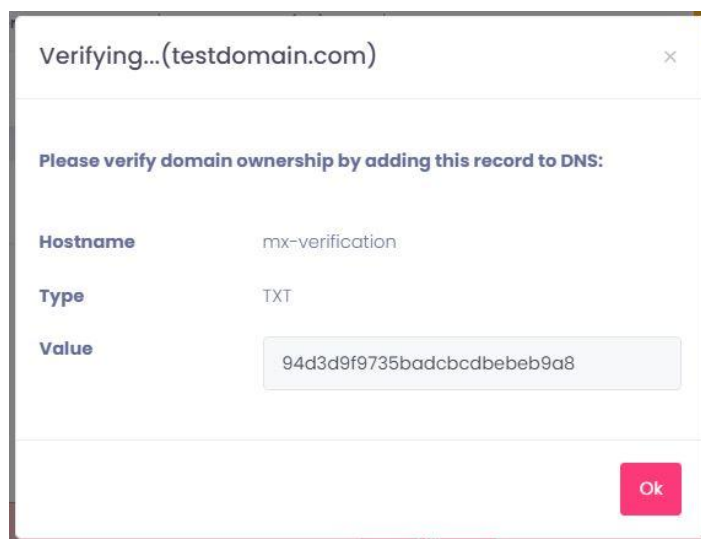
Verify Domain Ownership

After adding your domain, you must verify your ownership. This is done by adding a specific TXT record to your domain's DNS settings at your domain registrar or DNS provider.

- Once the domain is added, it will appear in the domain list with a **Fail** health status indicating it needs verification, with a checkmark option to **Verify**



- To retrieve the necessary TXT record for verification, locate the newly added domain in the list. Click on the **Verify** button (represented by a red checkmark icon).
- A pop-up window will appear, displaying the **Hostname**, **Type**, and the unique **Value** required for the DNS record.
 - Hostname: `mx-verification`
 - Type: `TXT`
 - Value: copy the unique string from your pop-up window



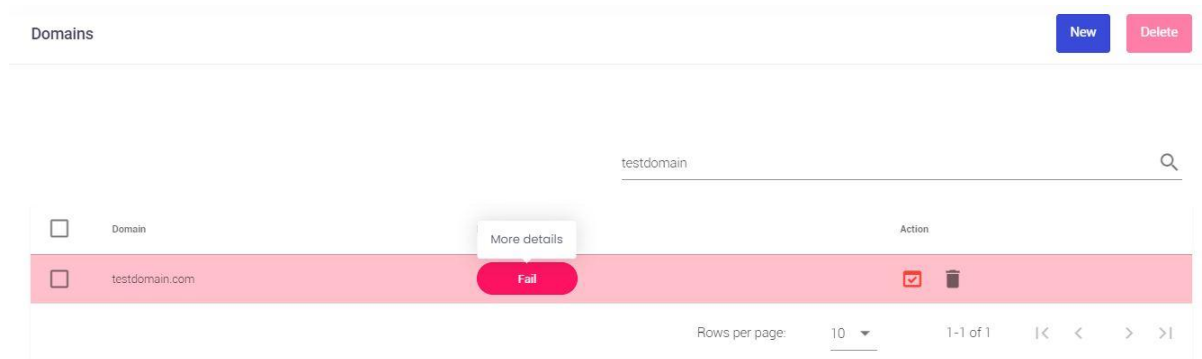
- Go to your domain registrar's or DNS provider's control panel and add a new TXT record with the provided Hostname and Value.

Improve Domain Health

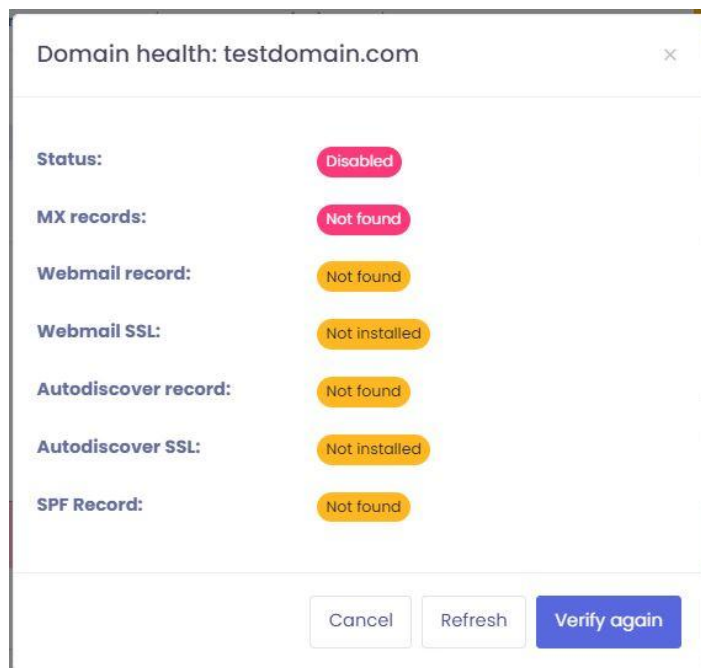
Once domain ownership is verified, you should configure additional DNS records to ensure proper email functionality and improve your domain's overall health.

If you are planning an email migration to this new domain, you may choose to postpone making changes to critical records like MX records until the migration process is complete to avoid any disruption to your current email flow.

- In the Domains list, you can click on the **Health status** (e.g., "Fail" as shown in the example) option to see the **Domain health** status.



- The **Domain health** pop-up will show the status of various essential records. (See image below, which displays statuses for MX records, Webmail record, Webmail SSL, Autodiscover record, Autodiscover SSL, and SPF Record).
- Status is **Disabled** if the domain ownership was not verified / **Enabled** if the domain was verified.



- When you are ready, follow your service's specific [DNS Configuration guide](#) to set up the following records correctly::
 - **MX records** - These direct incoming emails for your domain to the correct mail servers. They are crucial for receiving emails.
 - **SPF record** - This is a TXT record that lists authorized mail servers permitted to send emails on behalf of your domain, helping to prevent email spoofing and

improve deliverability.

- **Webmail record** (optional) - This is typically a CNAME record that allows you to access your webmail interface via a custom URL (e.g., `webmail.yourdomain.com`).
- **Autodiscover record** (optional) - This record simplifies the process of configuring email clients (like Outlook or mobile email apps) by allowing them to automatically discover server settings.
- **Webmail SSL and Autodiscover SSL:** These will typically generate automatically once the corresponding Webmail and Autodiscover DNS records are correctly set up and have propagated. Please allow up to **30 minutes** (or sometimes longer, depending on DNS propagation) for their status to update in the Domain Health pop-up.
- After configuring these records, you can use the **Refresh** or **Verify again** button in the "Domain health" section to update the status.

Remove a Domain

- Navigate to the [Admin Panel](#).
- Log in using your **Admin username and password**.
- Click on **Domains** in the menu.
- Click on the delete icon next to the domain you wish to remove
- An alert pop up will appear, showing the domain that will be deleted. Click on **Delete** to confirm.

Removing a domain will PERMANENTLY erase all domain data from our servers, including all the users' messages, the aliases, lists, and all preferences.

Edit a Domain

- Go to the [Admin Panel](#).
- Log in using your **Admin username and password**.
- Click on **Domains** in the menu.
- Click on the **edit icon** next to the domain you wish to edit
- You can edit the following information:
 - Domain-level **Timezone** and **Home Country**
 - **Catchall**
 - Enable / disable **Local Delivery**

- Enable / disable **Audit** domain

You cannot change the name of a domain. The only way to accomplish this is to create the domain with the new name (correct a misspelling, add a hyphen, etc.) and then request a migration from the old domain to the new one by opening a support ticket.

Set a Catchall

A **Catchall** address allows you to capture messages destined for non-existing mailboxes. It can help you salvage important messages that were sent to mistyped addresses. Still, on the other hand, it will surely cause you to receive many Spam emails sent via a dictionary attack, where the sender puts commonly used aliases.

To enable a **Catchall**:

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Domains** in the menu.
- Click on the **edit icon** next to the domain you wish to edit
- In the **Domain Catchall** field, you can choose from the following:
 - **No catchall**: this disables the catchall feature
 - **Accept & Delete**: the catchall will automatically delete all the messages received
 - **Username**: the catchall will forward all received messages to the selected Username (mailbox)

Set a Footer

A **domain-level Footer** will show up in all the emails that all the users of the domain send.

To add a domain **Footer**:

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Domains** in the menu.
- Click on the **footer icon** next to the domain you wish to update
- Fill in the Footer message using the available HTML editor.
- Click on **Update** to finish.

Manage Users

Each mailbox is defined as a User in the Admin Panel. Here you can manage all of your Users: add new ones, remove or edit any user's settings, as well as login into the User's Control Panel to manage their preferences.

Before adding a new user please make sure you have a sufficient User quota (available mailboxes and quota), which can be checked in the top menu bar of your Admin Panel.

Adding a User

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Users** in the menu bar.
- Click on the **New** button.
- Choose the **Account Type** from the dropdown list.
- Choose the **Domain** where you want to add an account from the drop-down list.
- Enter the **Username** to add (only the part before the @ sign).
- Enter the **Password**. Note: Passwords must contain at least 8 characters, including upper/lowercase, numbers, and a symbol.
- Enter the **Name** of the user to add, for your control (user's full name, with spaces).
- Enter the **Quota** for the user, in Gigabytes (GB). In order to assign 5GB, simply type 5. To specify 500 MB (Half of a gigabyte), specify 0.5.
- Optional: you can click on **More Options** to define the User's **Language**, **Timezone** or **Localization** and **Date format**.
- Click on the button **Add User** to finish.

If you receive the error that the User already exists, check if you already have an Alias or a Distribution List with the same name. The username must be unique on a domain level, which means you cannot have a mailbox and an Alias with the same name.

Removing a User

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Users** in the menu bar.
- Select your domain from the **Select Domain** drop-down box.
- Click on the delete icon (trash icon) next to the account you wish to remove.
- An alert pop-up will appear, showing the User that will be deleted. Click on **Delete** to confirm.

Deleting an account deletes all its e-mails and data. Be careful!

Editing a User

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Users** in the menu bar.
- Select your domain from the **Select Domain** drop-down box.
- Click on the **pencil icon** (edit) next to the User you wish to edit
- You can update the:
 - Name
 - Password
 - Account type (change from Basic to Enhanced and vice versa)
 - Quota (increase or decrease)
- Click on **More Options** to update the:
 - Language
 - Timezone
 - Date format.
- **Disabled** - set to Yes if you want to temporarily deactivate the mailbox, without deleting the emails.
- **Only local SMTP** - enable this if you want to restrict the User to only send local emails (only to the same domain).
- Click on **Update User** to save your changes.

Logging in as a user

Admins are able to log in as the User, making it possible to [manage several aspects](#), such as autoresponder, forwarders, rules, black & whitelist on user level, track e-mails sent by account (in Track deliveries) and so on, which are only available on the user level. End users can login with their respective e-mail addresses [directly to the User Panel](#).

- Go to the [Admin Panel](#)
- Log in using your Admin username and password.
- Click on **Users** in the menu bar.
- Click on the **arrow icon** next to the account you wish to login as in the User Panel.
- Click on the **mailbox icon** next to the account you wish to login as in the Webmail.
- Click on the **key icon** next to the account you wish to generate One Time Password (OTPassword). This password is valid for 5 minutes and you can use it to troubleshoot the User's issue.

Manage Alias Domains

An Alias Domain is an exact copy of a real domain. It is useful when you have multiple domains that should all share the same characteristics.

For example, your company might own several domains: longcompanyname.com, shortcompanyname.com, and oldcompanyname.com, but you don't want to create separate users for each domain. You can set up longcompanyname.com as the **primary domain** and the other two as **Alias Domains**. Every user, alias, or list you set up on the primary domain will be available on the Alias Domains. Remote senders can use any domain name to reach your users, and the message will be delivered only once, into a single mailbox. It's a great way to consolidate your domains.

Add an Alias Domain

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Domains** in the menu and choose **Alias Domains**.
- Select the primary domain from the drop-down list
- Click on the **New** button.
- Enter the name of the **Alias Domain**
- Click on the **Add** button.
- Make sure to modify your DNS settings and add the MX records for the alias domain. They should be:
 - Primary with a preference of 5: mx.emailarray.com
 - Secondary with a preference of 10: mx2.emailarray.com

Remove an Alias Domain

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Domains** in the menu and choose **Alias Domains**.
- Select the primary domain from the drop-down list
- Click on the delete icon next to the domain alias you wish to remove
- An alert pop up will appear, showing the alias domain that will be deleted. Click on **Delete** to confirm.

Manage Aliases

An Alias allows you to create an e-mail address that forwards to a real e-mail account. For example, you can create several aliases such as first.name@domain.com and webadmin@domain.com that point to john@domain.com. john@domain.com would be the only mailbox created.

Adding an Alias

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Aliases** in the menu bar.
- Click on the **New Alias** button.
- In the **Alias** field, type the alias (just the part before the at sign)
- In the **Domain field**, select the domain in which you will create an Alias.
- In the **Forward Destination**, choose **Internal** if you want to forward to an email address of the same domain or **External** to forward to any domain. **External** aliases are limited to 4 per account. After this limit, they count as regular mailboxes.
- In the **Forwards to** field, specify the e-mail account where emails will be sent to, for this alias.
- Click on the button **Add Alias**.

An Alias is a unique e-mail address that has to be unique across your entire domain. No other e-mail account or distribution list may have the same name as the Alias.

If you receive the error "**Alias already in use**," it means you already have an existing Alias, User, or Distribution List with the same name.

Removing an Alias

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Aliases** in the menu bar.
- Select the domain which has the alias you want to remove in the drop-down list
- Click on the delete icon next to the alias you wish to remove
- An alert pop up will appear, showing the alias that will be deleted. Click on **Delete** to confirm.

Manage Lists

Distribution Lists let you reach multiple e-mail addresses at once. For example, you could create a **sales** address for your sales team (sales@mydomain.com), a **support** address for your technical support team (support@mydomain.com), and so on.

Distribution Lists can be managed from the Admin Panel:

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.

Adding a List

- Click on **Lists** in the left menu bar.
- Click on the button **New List**.
- In **List Name**, type in the name of your list (only the word before the '@' sign)
- In the **Domain field**, choose the domain in which the list will be created.
- In **List Type**, choose Distribution List.
- Click on the **Add List** button.

Managing List Members

Adding new members

- Click on **Lists** in the menu bar.
- Click on the **pencil icon** next to the list you wish to edit
- You can add **internal members** (hosted by us, unlimited) or **external members** (hosted by another provider, maximum 4 per list).
- To add an **internal member**, select the email address from the list and click on **Add Member** button.
- To add an **external member**, type in the input field the email address and click on **Add Member** button.

Deleting members

- Click on **Lists** in the menu bar.
- Click on the **pencil icon** next to the list you wish to edit

- Remove members by clicking on the **delete icon** next to the member which you want to delete.
- A confirmation pop-up will appear, showing the member that will be deleted. Click on **Delete** to confirm.

Removing a Distribution List

- Click on **Lists** in the menu bar.
- Click on the **delete icon** next to the list which you want to delete.
- An alert pop up will appear, showing the list that will be deleted. Click on **Delete** to confirm.

Manage Smart Lists

A **Smart List** is a type of **distribution list** with more options to make it easier to specify members and who is allowed to send emails to that list.

Just as a distribution list, a Smart List lets you reach multiple email addresses at once. For example, you could create a **team** address for your whole office team (team@mydomain.com), a **billing** address for your accounting team (billing@mydomain.com), and so on.

Smart Lists can be managed from the Admin Panel:

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.

Adding a Smart List

- Click on **Smart Lists** in the left menu bar.
- Choose a **Domain** from the list.
- Click on the button **New List**.
- In **List Name**, type in the name of your list (only the part before the '@' sign).
- In **List type**, you have two options:
 - **Specify Members** (add each member one by one, by email address), or
 - **All domain users** (automatically include all valid emails of the chosen domain).
- In **List security**, you can choose who can send emails to this smart list:
 - **Only members can post**: all or only some emails from the same domain can post,
 - **Password protected**: only senders that include the password at the beginning of the subject line can send (email subject example, with a custom password between square brackets: [mypass]My Subject),
 - **No protection**: anyone can send emails to this list.
- If you choose **Password protected**, type in the chosen **password** in the input field. You can share this password with accepted senders and instruct them to include it in the email subject (for example: [customPassword]My Subject - the password will be removed before recipients receive the email).
- You can choose to **Send a copy of the message to the sender**.
- Click on the **Add Smart List** button to finish the setup.

Managing Smart List Members

Adding new members to a Smart List where List Type is **Specify Members**:

- Click on **Smart Lists** in the menu bar.

- Choose a **Domain** from the list to show the available Smart Lists.
- Click on the **member icon** next to the list you wish to edit
- You can add **internal members** (hosted by us, unlimited) or **external members** (hosted by another provider, maximum 4 per list).
- You can choose if they can post to this smart list by setting **Can post** to **Yes** for each member you add.
- To add an **internal member**, select the email address from the dropdown, and click on **Add Member** button.
- To add an **external member**, type in the input field the email address and click on **Add Member** button.

Deleting members

- Click on **Smart Lists** in the menu bar.
- Choose a **Domain** from the list to show the available Smart Lists.
- Click on the **member icon** next to the list you wish to edit.
- Remove members by clicking on the **delete icon** next to the member which you want to delete.
- A confirmation pop-up will appear, showing the member that will be deleted. Click on **Delete** to confirm.
- If the Smart List type is **All domain users**, you can only remove the member's permission to post to that list.

Removing a Distribution List

- Click on **Smart Lists** in the menu bar.
- Choose a **Domain** from the list to show the Smart Lists.
- Click on the **delete icon** next to the smart list which you want to delete.
- An alert pop up will appear, showing the list that will be deleted. Click on **Delete** to confirm.

Filtering: Whitelist / Blacklist

Set Domain Spam filter preferences

An administrator can set domain-wide Spam filter preferences through the Admin Control Panel.

The setting would apply to all users that don't have a [personal preference set](#). A user's preference always overrides a domain-wide preference.

The domain-wide Spam filter preferences can be found at this location:

- Go to <https://cp.emailarray.com/admin>
- Log in using admin username and password.
- Click on **Filtering** in the top menu bar
- Select the **Domain** for which you wish to modify the settings in the drop-down list

The options are:

Accept e-mails from:

- **Everyone:** This is the default option and lets all messages reach the Inbox (the default)
- **Whitelist & Address book only:** This option only allows messages present in the Whitelist & Address book to reach the Inbox, the rest will be sent to your spam folder.

System default is to accept emails from everyone, moving detected spam to each user's spam folder. To disable spam folder for a user, you need to access the Filtering option in the user control panel, as noted in [this FAQ](#) and set to send Spam to inbox, which is basically the same as if you had disabled antispam for that user.

The option to accept only from white-listed senders and contacts in your address book is a nice alternate way of receiving practically no spams in your inbox, at the cost of having to check your spam folder or spam reports, from time to time.

Enable autowhitelist: All e-mails sent by e-mail accounts of your domain automatically add the recipient's address to the domain's auto-whitelist. An interesting option, but possibly dangerous if a user account is compromised, sends spams and automatically all recipients of such spams are added to the domain level auto-whitelist (accessible in Filtering > Auto-Whitelist), which would require cleaning up the auto-whitelist.

Filter sensitivity: The filtering system can be adjusted on a scale from 1 to 10, with 10 being the most restrictive while 1 is the most permissive. We find that the default setting of Normal Sensitivity is just right for most users.

Keep Spam for: How many days to keep the Spam messages in the Spam folder. Default is 7 days.

Send Spam Report: This defines how often the users will receive in their Inbox the summary of Spam messages trapped over the past few hours. Default is every 12 hours.

Spam E-mail Report Format: Lets you choose the format of the Spam Report message. Default is HTML and TEXT.

After making any changes, click on the **Update Settings** button.

Manage Whitelists and Blacklists

Notice that the best way to add whitelist records is using the Spam Monitor reports, as it automatically delivers the email and adds the sender to your whitelist. Our system uses the Sender instead of the From in the email header for blacklist and whitelist, which is automatically done if you authorize emails through spam reports.

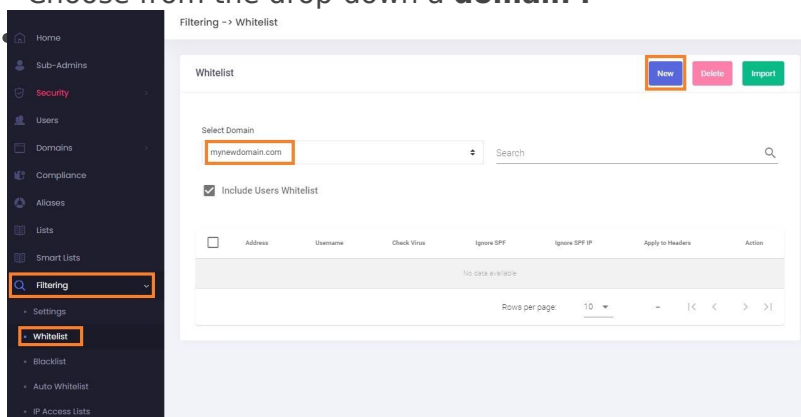
If you enter an email address manually to your black or whitelist and notice it doesn't work, check the email header and look for the **X-Barracuda-Envelope-From:** field, which should be used. Yet another possibility is that the sender might change every time you receive a certain email. In this case, you can use [Rules](#) to delete undesired messages based on the part of the From header address or subject.

Besides being able to whitelist or blacklist an address for the entire domain manually, Administrators can also manage the automatic whitelist. The automatic whitelist is a domain-wide whitelist built from the email-sending patterns of all your users. It ensures that communication with trusted recipients always goes through without being filtered.

Add a sender to the whitelist.

This will treat the sender as safe and deliver all incoming emails to the Inbox folder (or another folder if you have set up delivery rules)

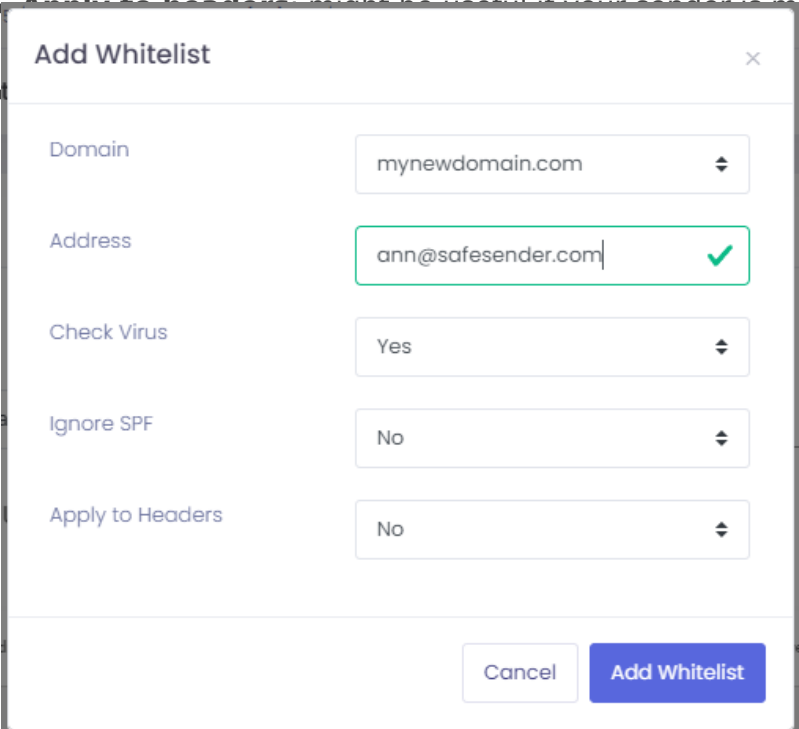
- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Filtering** → **Whitelist** in the menu.
- Choose from the drop-down a **domain** .



- In the **Address** field, type the email address (or just the domain) you want to whitelist.

- **Check virus:** select whether you still wish to check for viruses (Recommended: Yes).
- **Ignore SPF:** select whether you want to ignore SPF (Recommended: No, because it exposes you to forged emails). If the sender is marked as Spam because of the failed SPF, please use the **Whitelist** option from the **Spam Monitor** emails or [whitelist from the Webmail](#). This will ensure you have the correct IP address needed to ignore SPF.

Apply to Headers might be useful if your sender is misconfigured (Recommended: No,



Add Whitelist

Domain: mynewdomain.com

Address: ann@safesender.com ✓

Check Virus: Yes

Ignore SPF: No

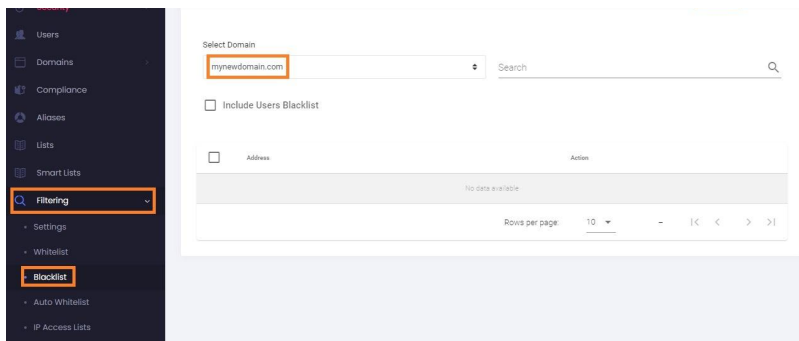
Apply to Headers: No

Cancel Add Whitelist

Add a sender to the blacklist

This will treat the sender as high-risk, and all incoming emails from this sender will be rejected (no copy of the email will be saved).

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Filtering** → **Blacklist** in the menu.
- Choose from the drop-down a **domain** .
- Click on the **New** button.



- In the **Address** field, type the email address (or domain) that you want to blacklist.

 The image shows a modal dialog box titled 'Add Blacklist' with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first is labeled 'Domain' and contains the text 'mynewdomain.com'. The second is labeled 'Address' and contains the text 'soamsender.com', which is highlighted with a green border and a green checkmark icon to its right. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Add Blacklist'.

Remove a sender from the whitelist or blacklist

Sometimes, users accidentally whitelist or blacklist a sender, and you might wish to remove those entries.

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Filtering** → **Blacklist** (or **Filtering** → **Whitelist**) in the menu.
- Select the **domain** which has the entry you want to remove from the drop-down list.
- Click on the **Include Users Blacklist** (or **Include Users Whitelist**) option to include user-generated entries.
- Optional: search for the desired sender email or domain.

Select Domain: mynewdomain.com Search

☒ Include Users Blacklist

<input type="checkbox"/>	Address	Username	Action
<input type="checkbox"/>	info@safesender.com	john	
<input type="checkbox"/>	info@spamsender.com	john	
<input type="checkbox"/>	no-reply@spamsender.com	john	
<input type="checkbox"/>	spamsender.com		

Rows per page: 10 1-4 of 4 |< < > >|

- Click on the **delete** icon (garbage sign) next to the entry you wish to remove.
- An alert pop-up will appear, showing the entry that will be deleted. Click on the **Delete** button to confirm.

View the automatic whitelist and/or remove items from it

The automatic whitelist is a domain-wide whitelist built from the email-sending patterns of all your users. It ensures that communication with trusted recipients always goes through without being filtered.

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Filtering** → **Auto Whitelist** in the menu.
- Choose from the drop-down a **domain** .
- **Pick a date:** choose a specific day or **All days** to show all entries.
- **Address like:** optional; specify a search term.

Filtering -> Auto Whitelist

Auto Whitelist

Select Domain: mynewdomain.com Pick a Date: All days

Address Like:

<input type="checkbox"/>	Username	Address	Check Spam	Check Virus	Action
No data available					

Rows per page: 5 1-0 of 1 |< < > >|

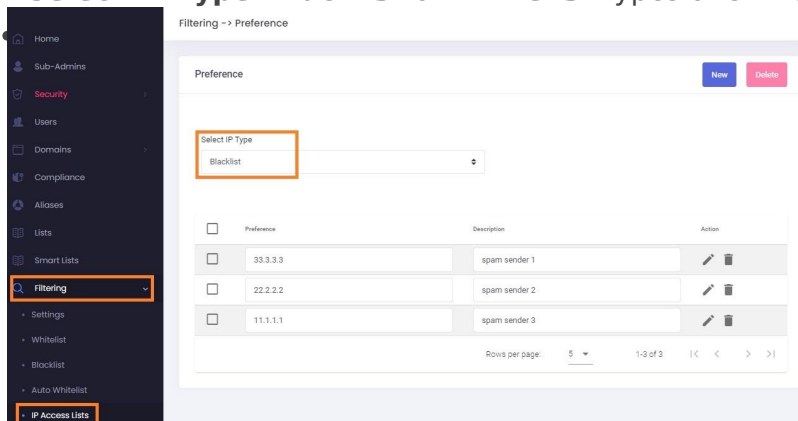
- Click on the **delete** icon (garbage sign) next to the entry you wish to remove.

- An alert pop-up will appear, showing the entry that will be deleted. Click on the **Delete** button to confirm.

Limiting by IP: add the sender's IP to whitelist or blacklist

Sometimes, you need to blacklist or whitelist an entire IP.

- Go to the [Admin Panel](#).
- Log in using your Admin username and password.
- Click on **Filtering** → **IP Access List** in the menu.
- **Select IP Type: Blacklist** or **Whitelist** types of entries.



- Click on the **delete** icon (garbage sign) next to the entry you wish to remove.
- An alert pop-up will appear, showing the entry that will be deleted. Click on the **Delete** button to confirm.
- To add a new entry, click on the **New** button.
- **Preference:** select where you wish to add the entry for, blacklist or whitelist.
- **Value:** a valid IP.
- **Description:** add some details so you can remember this entry.
- Click on the **Add** button.

Preference

Blacklist



Value

44.4.4.4



Description

spam sender 4

Cancel

Add

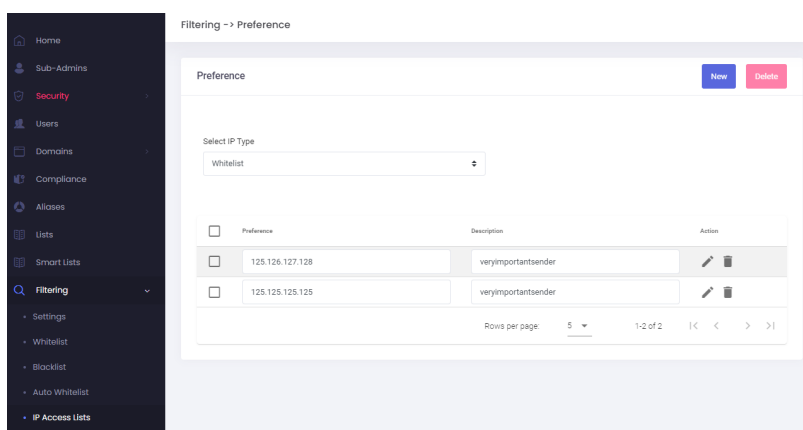
Whitelist / Blacklist by IP - IP Access List

Whitelist Incoming Email by IP

In some limited cases, a legitimate sender has been compromised and all of his incoming emails are marked as Spam. Until the legitimate sender will fix their reputation, you can whitelist their incoming emails. This is a type of whitelist based on IPs. If you specify an IP or IP range as whitelist, e-mails sent from such locations will never be marked as spam, for all your domain's e-mail accounts.

To whitelist a sender's incoming email by IP:

- Log in to the [Admin Panel](#)
- From the menu, go to **Filtering → IP Access List**
- Select the IP Type from the dropdown: **whitelist**.
- A list of existing IPs that were marked as trusted will appear
- You can edit each entry or delete it.



- To add a new entry, click on the **New** button.
- In the new pop-up:
 - **Preference:** choose **Whitelist**
 - **Value:** the **IP of the sender** - get their IP from the Incoming Logs. You may specify a single IP or an IP range using CIDR notation, for example: 192.168.0.0/24
 - **Description:** such as sender's domain or company name - so you can easily remember it later
- Click on the **Add** button to whitelist the incoming email from this IP.

New ×

Preference

Whitelist

Value

1.2.3.4 ✓

Description

sender.com

Cancel

Add

Blacklist Incoming Email by IP

Some spammers will change the email address or domain regularly which makes it harder to blacklist by e-mail / domain only. For this cases, you can blacklist a sender by IP. If you specify an IP or IP range as blacklist, e-mails sent from such locations will be marked as blacklisted and deleted by default, for all your domain's e-mail accounts (this rule can be changed on User level, from the *User Panel* → *Delivery Rules* → *BlacklistDelete* or from the *User Panel* → *Filtering* → *Blacklisted messages* option).

To blacklist a sender's incoming email by IP:

- Log in to the [Admin Panel](#)
- From the menu, go to **Filtering** → **IP Access List**
- Select the IP Type from the dropdown: **blacklist**.
- A list of existing IPs that were marked as untrusted will appear
- You can edit each entry or delete it.

Home

Sub-Admins

Security

Users

Domains

Compliance

Aliases

Lists

Smart Lists

Filtering

Settings

Whitelist

Blacklist

Auto Whitelist

IP Access Lists

Filtering → Preference

Preference

Now Delete

Select IP Type

Blacklist

<input type="checkbox"/>	Preference	Description	Action
<input type="checkbox"/>	44.4.4.4	spam sender 4	✎ 🗑
<input type="checkbox"/>	125.126.127.128	blacklisted.com	✎ 🗑
<input type="checkbox"/>	222.222.222.223	spamdmain.com	✎ 🗑
<input type="checkbox"/>	111.111.111.112	spamdmain.online	✎ 🗑

Rows per page: 5 1-4 of 4 < >

- To add a new entry, click on the **New** button.
- In the new pop-up:

- **Preference:** choose **Blacklist**
- **Value:** the **IP of the sender** - get their IP from the Incoming Logs. You may specify a single IP or an IP range using CIDR notation, for example: 192.168.0.0/24.
Warning: blacklisting an IP range may cause legitimate emails to not be delivered.
- **Description:** such as sender's domain - so you can easily remember it later
- Click on the **Add** button to blacklist the incoming email from this IP. All incoming email from this IP will be marked as blacklisted and deleted by default.

New

×

Preference

Blacklist

⬆

Value

1.2.3.4

✓

Description

spam.com

✎

Cancel

Add

Set Branding

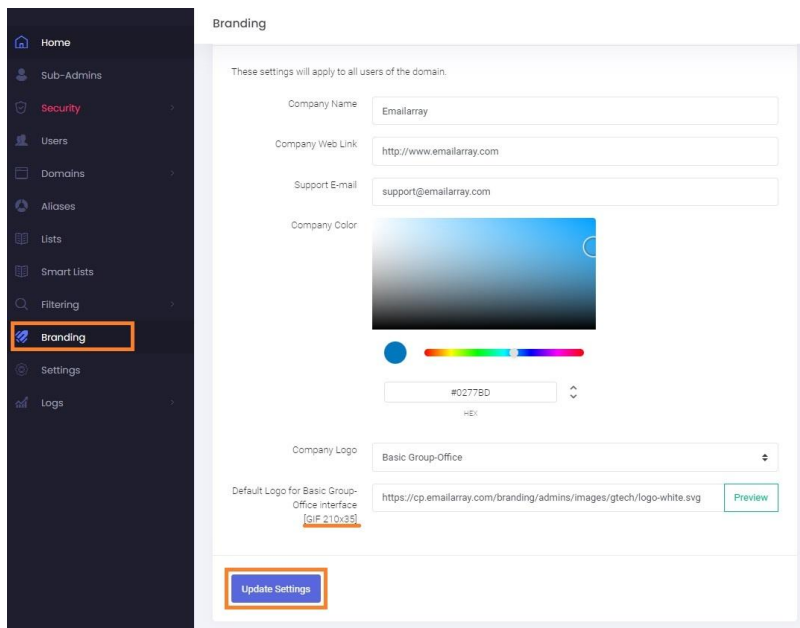
The Admin Panel allows you to personalize the name and logo being displayed in the Webmail. Regular mail services (IMAP, SMTP, POP) are offered through the anonymous domain **emailarray.com**.

The branding applies to the Webmail interface.

It is also possible to set a different sender for Spam reports sent by the system.

To update the branding for your account:

- Go to the [Admin Panel](#)
- Log in using your Admin username and password.
- Click on **Branding** in the menu bar
- Update the fields
- Click on the **Update Settings** button to save the changes.



The screenshot shows the 'Branding' settings page in the Admin Panel. The left sidebar contains a menu with 'Branding' highlighted. The main content area is titled 'Branding' and includes a note: 'These settings will apply to all users of the domain.' The settings are as follows:

- Company Name:** Emailarray
- Company Web Link:** http://www.emailarray.com
- Support E-mail:** support@emailarray.com
- Company Color:** A color picker showing a blue gradient, with a hex code input field set to #0277BD.
- Company Logo:** Basic Group-Office
- Default Logo for Basic Group-Office interface:** https://cp.emailarray.com/branding/admins/images/gtech/logo-white.svg (with a 'Preview' button)

At the bottom, there is a blue 'Update Settings' button.

Company Name: Enter your company name - it will be displayed as the Webmail page title in the browser

Company Web Link: Enter the link to your website

Support e-mail: Enter the e-mail address used as the sender for **Spam Reports**

Company Color: Change the primary color for the Webmail to customize the look and match your own branding guidelines

Default Logo: Notice the required file extension is *.GIF, and the size of the logo must be 210px x 35px. You have to publish your image to a web server via FTP (you can upload it on your website, too) and make sure the image is publicly accessible. For a quick check, you should be able to see the logo when pasting the URL in a new incognito window in your browser.

Logs

Outgoing logs - Track all Remote Deliveries

From the Admin Panel, you can track all the messages sent by your users through our outbound servers.

How to Access Outgoing Logs:

1. Log in to the [Admin Panel](#) using your Admin username and password.
2. From the menu, go to **Logs** → **Outgoing Logs**.
3. Select a **Domain**, **Start Date**, and **End Date**.
 - You can review Remote Delivery data **for up to 30 days** in the past.
4. Click the **Search** button.

You will see a list of emails sent by all users for the selected domain and time period.

Filtering Options:

Use the filter s to refine your search:

- **View Messages** dropdown - choose one of the following:
 - **Delivered** messages
 - **Temporarily Rejected** messages (e.g., user is over quota)
 - **Permanently Rejected** messages (e.g., invalid mailbox, blacklisted)
 - **All Messages**
- **Sent To** - (Optional) Enter the recipient's email address or part of it.
- **Sent From** - (Optional) Enter the sender's specific email address.

The Outgoing Logs do not display emails sent between addresses on the same domain, as those are delivered locally and bypass external logging.

Sub-Admins

Security

Users

Domains

Aliases

Lists

Smart Lists

Filtering

Branding

Settings

Logs

Incoming Logs

Outgoing Logs

Last Logins

Search Options

Select Domain

mynewdomain.com

Start Date

29-11-2021

End Date

29-11-2021

View Messages

Delivered

Sent From

Sent From

Sent To

Sent To

Search

Search Results

This interface does not show same-domain deliveries

Incoming Logs - Track All Incoming Email

Use the **Incoming Logs** section in the Admin Panel to track all emails received by your domain. This tool helps you analyze delivery status, sender information, and potential issues with incoming mail.

Tip: Use filters to quickly identify spam, delivery issues, or suspicious activity. You can apply multiple filters to narrow down results efficiently.

How to Access Incoming Logs:

1. Log in to the [Admin Panel](#) using your Admin username and password.
2. From the menu, go to **Logs → Incoming Logs**.
3. Select a **Domain**, **Start Date**, and **End Date**.
 - You can review incoming email data **for up to 60 days** in the past.
4. Click the **Search** button to view the results.

Filtering Options:

You can customize your search by adding one or more filters. Click the **+** button to add more filters to the search. All filters are optional.

Available filter fields include:

- **Header From** – The address in the email’s “From” header.
- **Envelope From** – The actual sending address used in the SMTP transaction.
- **Remote IP** – The IP address the message was sent from.
- **To** – The recipient’s address.
- **Subject** – Keywords from the email subject line.
- **Delivered** – Search for messages that were successfully delivered.
- **Delivered To** – The final delivery address (helpful for aliases or forwarding).
- **Undelivered** – Find messages that failed to be delivered.
- **Rejected** – Messages rejected due to policy or security settings.

You can also check the **Negate Condition** box next to any filter to exclude results matching that condition.

Understanding Search Results:

The search results table includes:

- **Date** – When the message was received.
- **Status** – Delivery status (delivered, undelivered, rejected, spam).
- **Envelope From** – The actual SMTP sender address.
Hover to see the "Header From" address as shown in the email client.
- **To** – Recipient address.
- **Subject** – Message subject.
- **IP** – Sending server’s IP address.
- **Spam Score** – Spam rating assigned to the message.
- **DNSBL** – Indicates if the IP was listed in a DNS blacklist.
- **SPF** – Shows whether the SPF check passed.

You can also:

- **Export Results** to a CSV file.
- **Whitelist & Deliver** selected messages.
- **Blacklist** unwanted senders or IPs.

Last Logins – Monitor User Login Activity

The **Last Logins** section in the Admin Panel allows you to monitor when users last accessed their mailboxes, from which IPs and locations, and what services or credentials were used.

This feature is useful for detecting unusual login patterns, troubleshooting access issues, or verifying account activity.

Tip: Use this log to spot suspicious login attempts, such as logins from unexpected countries or unknown IP addresses.

How to Access the Last Logins Section:

1. Log in to the [Admin Panel](#) using your Admin username and password.
2. From the menu, go to **Logs** → **Last Logins**.
3. Select the **Domain**, and set the **Start Date** and **End Date** to define the period you want to analyze.
4. Optionally, use filters to narrow down the search (see below).
5. Click **Search** to view the login activity.

Last Logins

Select Domain: mynewdomain.com Start Date: 6/1/2025 End Date: 6/27/2025

Username: john Remote IP: Negate Condition: ☐

Search **Reset Search**

Username	Domain	Remote IP	Location	Password used	Service used	Date	Action
john	mynewdomain.com		Canada	Main Password	imap	2025-06-27 12:09:50	Mark as Safe
john	mynewdomain.com		Canada	Main Password	imap	2025-06-27 09:00:51	Mark as Safe

Filtering Options:

To refine your search, you can add one or more filters by clicking the **+** button. You can also exclude specific values by checking the **Negate Condition** box.

Available filters include:

- **Username** – Search for logins by a specific user.
- **Remote IP** – Filter by the IP address from which the login originated.
- **Service used** – Filter by the protocol used (e.g., IMAP, SMTP, POP3).

Filters can be combined for more precise results.

Understanding the Results:

Each login entry includes the following information:

- **Username** – The mailbox username that logged in.
- **Domain** – The associated domain of the mailbox.
- **Remote IP** – The IP address from which the login occurred.
- **Location** – Estimated location based on IP.
- **Password used** – Indicates whether the main mailbox password or an app-specific password was used.
- **Service used** – The service used for the login (e.g., IMAP, SMTP, POP3).
- **Date** – The exact timestamp of the login.
- **Action** – You can **Mark as Safe** to acknowledge a known login.