Logs

- Outgoing logs - Track all Remote Deliveries
- Incoming Logs - Track All Incoming Email
- Last Logins – Monitor User Login Activity

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.

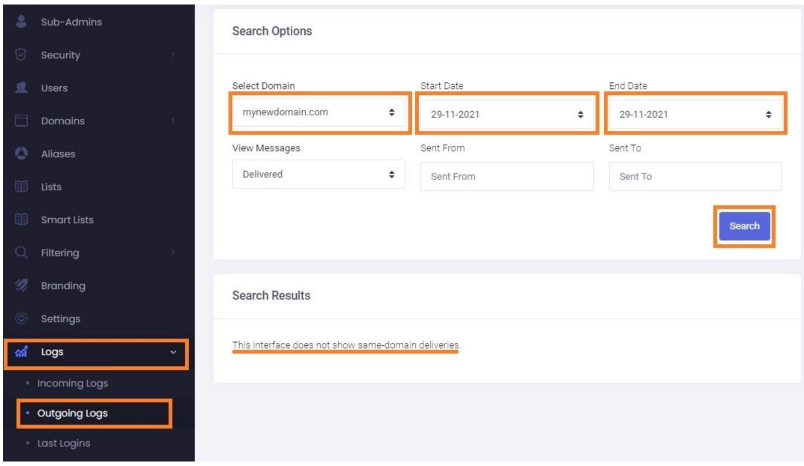
You will see a list of emails sent by all users for the selected domain and time period.

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.



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 Results

This interface does not show same-domain deliveries.

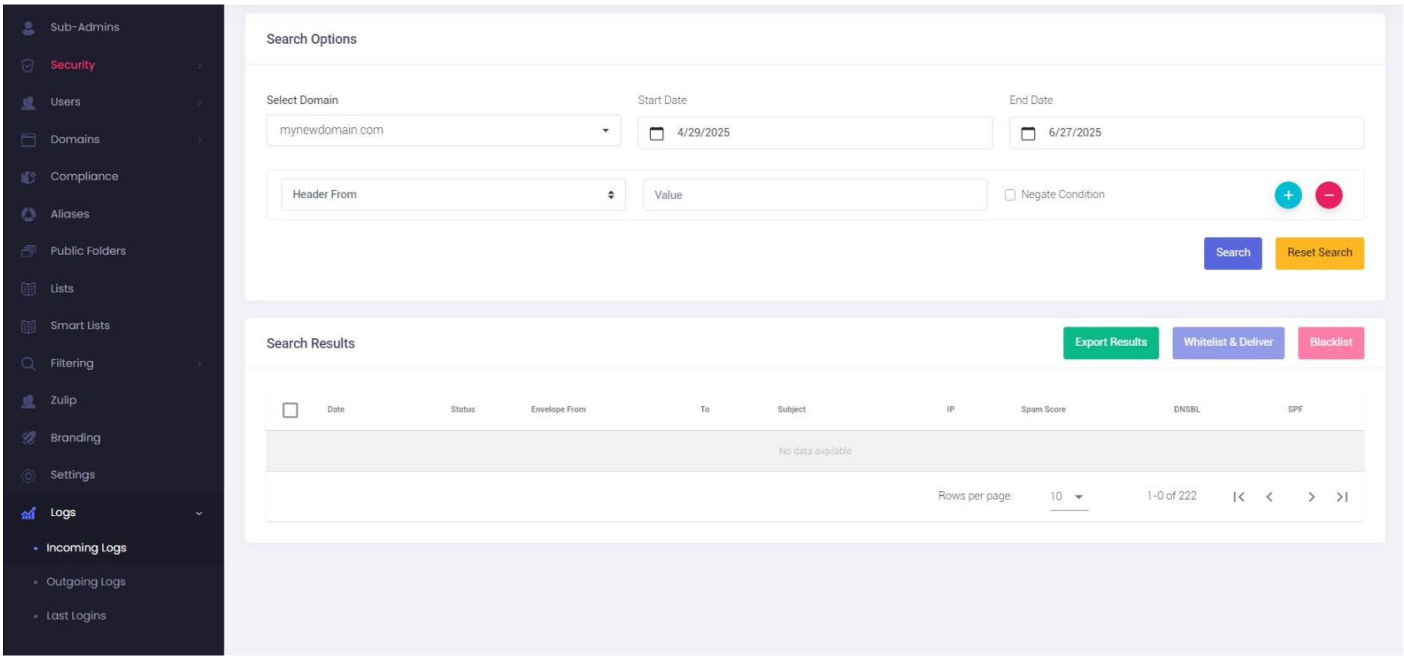
Incoming Logs - Track All Incoming Email

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.



Search Options

Select Domain: mynewdomain.com

Start Date: 4/29/2025

End Date: 6/27/2025

Header From | Value | □ Negate Condition

Search Results

□	Date	Status	Envelope From	To	Subject	IP	Spam Score	DNSBL	SPF
No data available									

Rows per page: 10 1-0 of 222

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

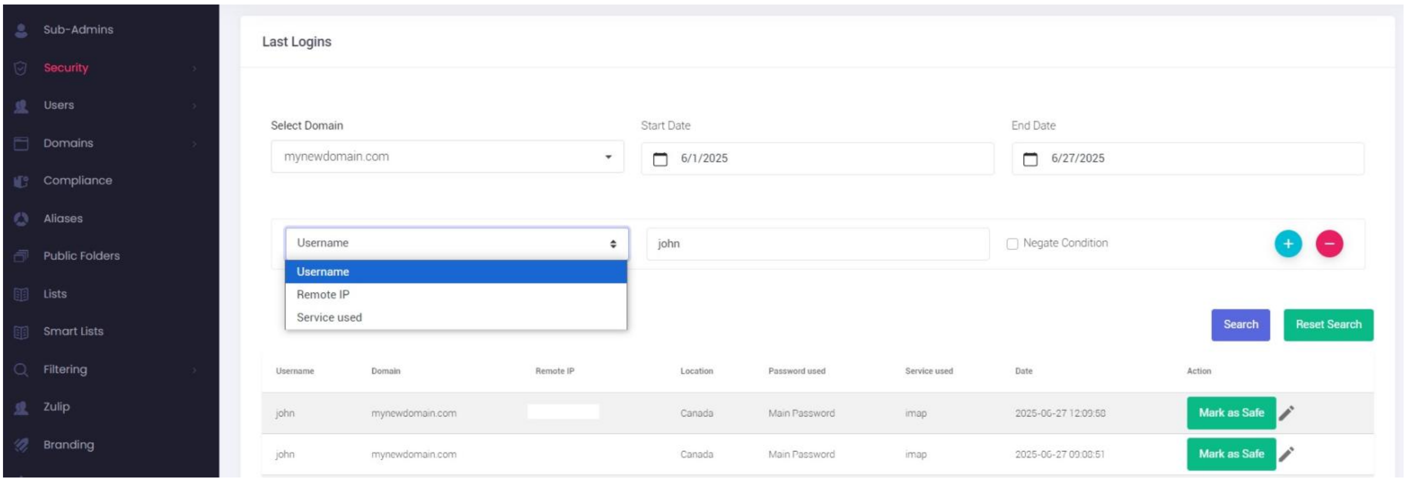
The **Last Logins** section in the Admin Panel allows you to monitor when users last accessed their mailboxes, from which IPs and locations, and what services or credentials were used.

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

□ Negate Condition

Username	Domain	Remote IP	Location	Password used	Service used	Date	Action
john	mynewdomain.com	[redacted]	Canada	Main Password	imap	2025-06-27 12:09:58	Mark as Safe
john	mynewdomain.com		Canada	Main Password	imap	2025-06-27 09:08:51	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.