

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.

The screenshot shows the 'Incoming Logs' interface. On the left is a dark sidebar menu with options: Sub-Admins, Security, Users, Domains, Compliance, Aliases, Public Folders, Lists, Smart Lists, Filtering, Zulp, Branding, Settings, and Logs. The 'Logs' option is expanded, showing 'Incoming Logs', 'Outgoing Logs', and 'Last Logins'. The main content area is titled 'Search Options' and contains a 'Select Domain' dropdown (set to 'mynewdomain.com'), 'Start Date' (4/29/2025), and 'End Date' (6/27/2025) fields. Below these is a filter section with 'Header From' and 'Value' inputs, a 'Negate Condition' checkbox, and '+'/'-' buttons. 'Search' and 'Reset Search' buttons are at the bottom right. The 'Search Results' section shows a table with columns: Date, Status, Envelope From, To, Subject, IP, Spam Score, DNSBL, and SPF. The table is currently empty with a 'No data available' message. At the bottom right of the table area, it says 'Rows per page: 10' and '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.

Revision #1

Created 27 June 2025 15:59:57 by Admin

Updated 27 June 2025 16:11:48 by Admin