

## Background

Sun Tsu once wrote that ‘the control of a large force is the same principle as the control of a few men: it is merely a question of dividing up their numbers’.

The Network Box Mail Portal system addresses just that – control itself, and the delegation of that control. While the my.network-box.com web interface permits the administrator to view and control the Mail policies of the organization, at the gateway, Mail Portal allows the administrator to delegate that control to end-users and put them in control of their own email (while still being restricted by overall company policy).

Network Box, as a managed service, has always been primarily managed from the NOC (Network Operation Centre). This provides for centralized configuration, backup, monitoring and maintenance of the Network Box device. However Network Box also permits for delegation of certain management functions (such as anti-spam, quarantine release, content filtering policies, etc) to the local administrator (via a web-based interface called “my.network-box.com”). Network Box Mail Portal contains patent-pending technology, and implements a "virtual per-user administrative interface", extending delegation of manageability and maintenance of the security gateway down to the per-user level. This is an industry first.

The Mail Portal system allows end users in organizations using SMTP email servers to have direct control of their quarantined emails for the first time. This means that in the event that an end user sees an email which has (in their opinion) been incorrectly blocked as spam; they can, with no more effort than ticking a checkbox, and clicking a single button have that email released. Using the same very easy to understand report, they can also tick an additional checkbox, to request that the sender is white listed in the future.

## CONTENT

Background.....	1
Implementation.....	2
Customisation.....	3
Mail Portal Report.....	4
Mail Portal Web Interface.....	6
Clustering.....	7
Conclusion.....	7

NOVEMBER 2007

*No part of this publication including text, examples, or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Network Box Corporation Limited.*

Network Box Corporation Limited,  
 16th Floor, Metro Loft,  
 38 Kwai Hei Street, Kwai Chung,  
 Kowloon, Hong Kong  
 Telephone: +852 2736-2083  
 Fax: +852 2736-2778  
[www.network-box.com](http://www.network-box.com)

## Implementation

Mail Portal delivers this functionality via two systems:

- 1. An email-based report.** This is sent periodically (monthly, weekly, daily, or a custom-reporting period at a minimum hourly), to all users who had mail activity during the reporting period. It reports on traffic for that user through the Network Box, and allows click-to-release quarantine release and request for white listing.
- 2. A Web-based interface.** This is accessible either via the email report, or via username + password, and shows the users email traffic on the box. The user can search for past email, and can release from quarantine and/or whitelist/blacklist (if so authorized).

To avoid the issue of the administrator having to maintain accounts for all his end-users, security is implemented via two mechanisms:

- The links in the email report contain secure encrypted security tokens. Possession of the email (and its tokens) permits the user to access his Mail Portal web interface without requiring a username or password. The secure tokens defend against users accessing each other's Mail Portals (as they are only known by the user holding the report and the Mail Portal system itself). Possession of the email report is sufficient to gain secure access to Mail Portal (without requiring a username or password).
- As an alternative, users can use the SETTINGS tab of Mail Portal to create passwords for themselves. They can then login to Mail Portal directly (without requiring a link from an email report) using their email address and password. An administrative interface is provided (under the my.network-box.com administrative system) to permit administrators to reset/remove passwords for users (or alternatively, the user can just click on a link in a Mail Portal report to gain access to Mail Portal and reset the password for themselves).

Should the administrator need to oversee or assist users with this, he can use the my.network-box.com administrative system to assign/reset Mail Portal users directly. Using secure token-based authentication, user account and password maintenance is in the hands of the users themselves. This reduces administrative overhead, but still permits the administrator to help (using my.network-box.com Mail Portal user administration) the users if necessary.

## Customisation

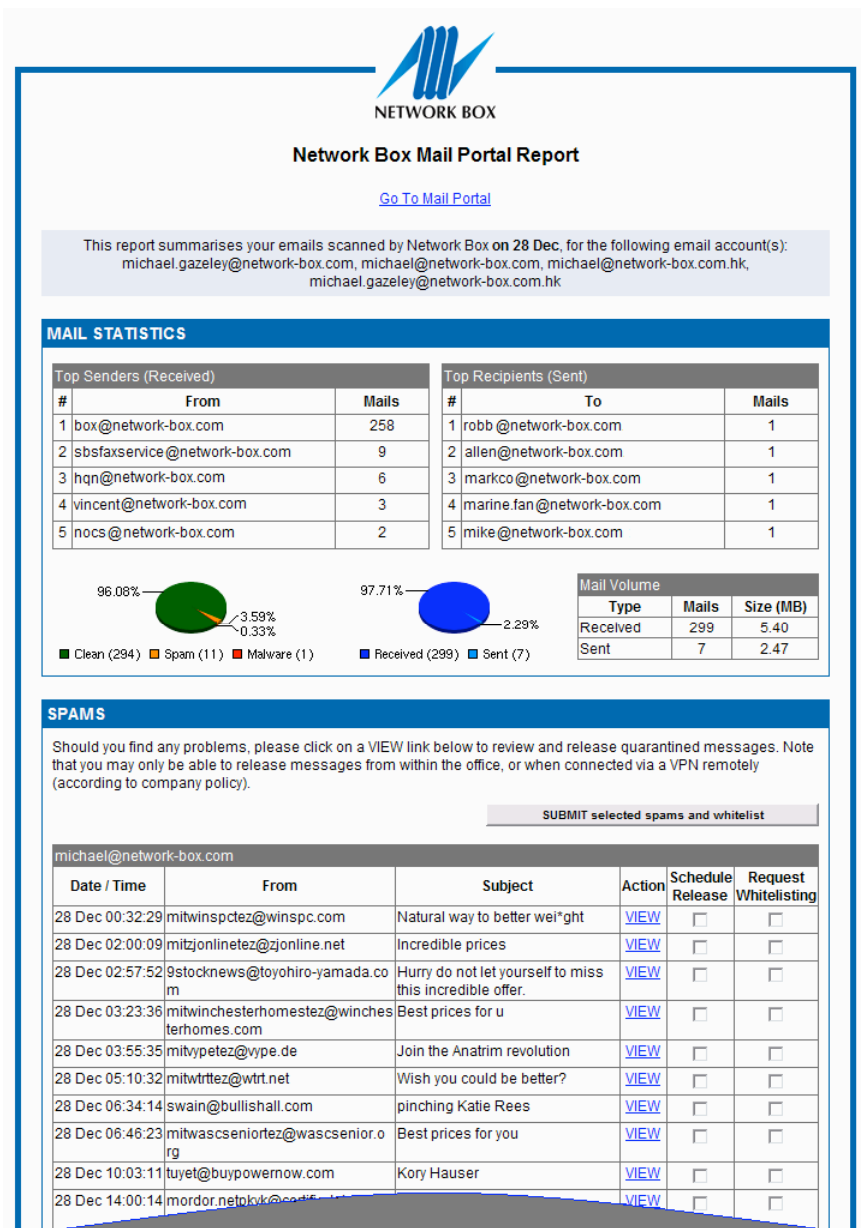
Extensive customization is configurable in the Mail Portal system, including:

1. The presence/removal of different fields (and columns) in the Mail Portal report can be configured. This allows for functionality to be made available to, or removed from, users of the system. Examples of this include permitting/denying users the rights to:
  - For Web Interface:
    - Release spam from quarantine
    - Release malware (non-viral) from quarantine
    - Release malware without protective warning envelope
    - Personally whitelist senders of email
    - Personally blacklist senders of email
    - Utilise AJAX 'Live Watch' technology
  - For Mail Report:
    - Use HTML Forms in the report (as opposed to links)
    - Include mail activity charts in the report
    - Access Full Mail Portal Web Interface (from report)
    - Show date/time email received
    - Show sender
    - Show subject
    - Show threat (for malware)
    - View message in Full Mail Portal Web Interface
    - Quarantine Release
    - Request administrative global whitelisting senders
    - Personally whitelist senders
2. Default language of the report (customizable on a per-user basis).
3. Reporting period (monthly, weekly, daily, or a custom reporting period configurable down to hourly).
4. In the case where a particular user has multiple email addresses, the Mail Portal (email report and web interface) can be configured to group all those email addresses under one account. Grouping can also be configured on a wildcard basis (e.g.: \*@acme.com).

## Mail Portal Reports

The Mail Portal report is usually delivered to end users on a daily basis. However, this report is configurable, and can be delivered monthly, weekly, daily, or customized (down to hourly), to conform to whatever timeframe suits the customer’s organizational requirements.

These reports (an example can be seen below) are delivered via email, to each of the users in the organization who wish to receive them. Individual reports would normally be sent to all users who had email activity (either inbound or outbound) during the reporting period, but it is possible to configure the list of users to receive the report, and for some users to opt out if they do not want these reports.



The purpose of the report is to give the users a concise summary of their overall email usage, and a list of what was blocked by the box (and why). The users can quickly scan the report, and take action (quarantine release, whitelisting, etc) directly from their mail client, as appropriate.

Users can immediately see all of the emails sent to them which were blocked (either as spam or malware), during the reporting period. In the unlikely event that any emails were incorrectly blocked, users can schedule these emails for release from quarantine, and also request that the sender be whitelisted in the future (to avoid that particular sender's emails being incorrectly blocked again by the anti-spam system).

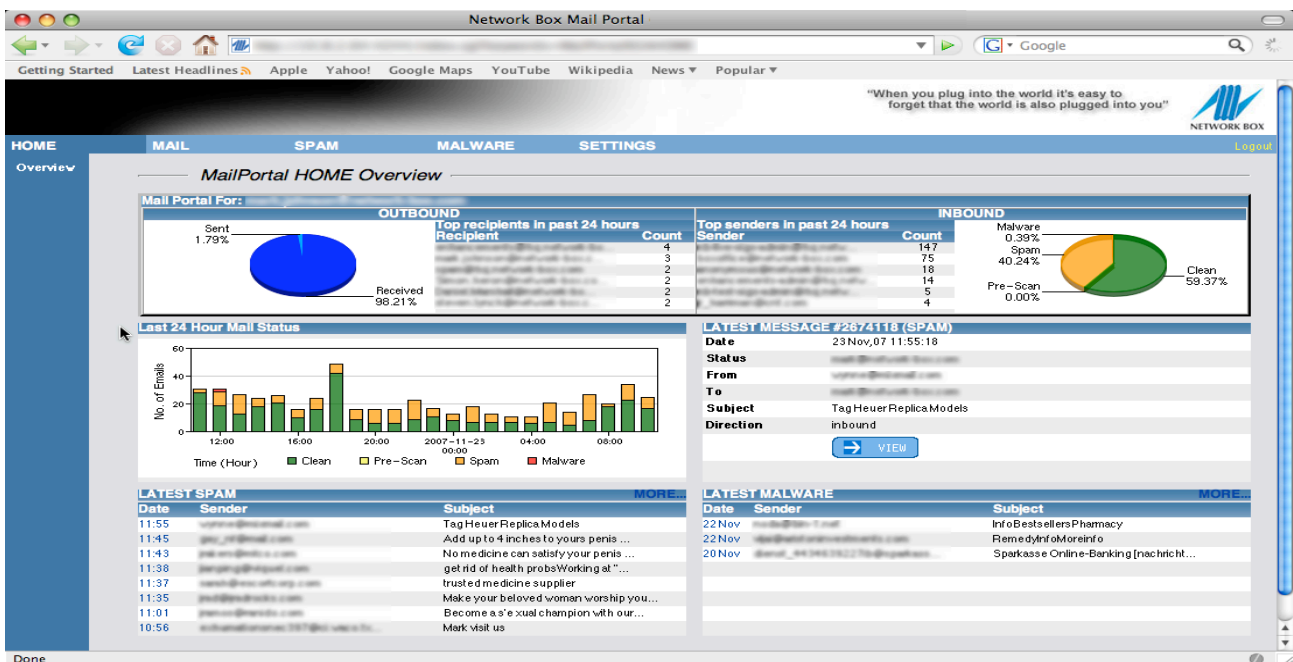
Even if a sender is white listed however; it is worth noting that in the event any future email from that sender contains company policy violations, or a computer virus, or a computer worm; it will still be quarantined as malware by the Network Box. Anti-Spam whitelisting is not dangerous as such - just because a sender is whitelisted in the Network Box anti-spam system, they will not automatically be white listed by the anti-virus, anti-spyware or organizational policy systems.

## Mail Portal Web Interface

Mail Portal provides two alternate / complementary web interfaces:

1. The **“Release” web interface** provides a single screen used to provide confirmation of whitelist and quarantine release requests from the Mail Portal Report. When the user clicks on a link, or clicks SUBMIT, on the Mail Portal Report, a HTTP/HTTPS request is sent to the Release web interface to perform the action. This service is very light weight and provides scalability to thousands of users.
2. The **“Full” web interface** provides a comprehensive web-based user portal. It is accessed either via direct login to Mail Portal or via clicking the VIEW or “Go To Mail Portal” links on the Mail Portal Report. It provides the following sections:
  - o HOME: An overview report on mail activity (updated in real-time using AJAX technology).
  - o MAIL: Reporting and searching on all mail activity.
  - o SPAM: Reporting and searching on spam quarantine. Includes functions to maintain personal whitelist and blacklists, as well as spam quarantine release.
  - o MALWARE: Reporting and searching on malware quarantine. Includes malware quarantine release.
  - o SETTINGS: Personal configuration settings and preferences.

The Mail Portal web interfaces are accessible over either HTTP or HTTPS connections. If using HTTPS, up to 256bit AES encryption may be specified. Access to the system can be configured in the firewall to control external (Internet) access; either direct or over VPN, to allow “road-warriors” and home users to access the portal and release email while “on the road,” or from home.



## Clustering

Mail Portal (and quarantine release) supports clustering of Network Boxes over a wide or local area network.

Network Boxes can be configured to report mail activity back to a single centralized log server, even though they locally quarantine spam and malware. In such a configuration, Mail Portal (reporting and web interface) runs on that centralized log server, and the users get one report and one web interface showing them the status of email their emails.

Distributed quarantine release is supported, so that if the users request a quarantine release, the cluster handles the queuing of the release request to the remote Network Box and error notification. The cluster can be geographically distributed using VPN technology available for Network Box.

## Conclusion

When the Network Box NOC manages the box, they get a view of the entire box and all it does. When the administrators manage the box, using [my.network-box.com](http://my.network-box.com), they get a view of the box and all it does. When the users manage the box, using Mail Portal, they get a view of just their portion of the box. Administrators see all the email going through the box, users see only their email. Thus users get a "virtual view" of just their subset of the security gateway.

Mail Portal provides an industry-first, patent-pending, per-user virtual administrative interface for email. Reducing administrative overhead, while still maintaining an overview, this system puts control back in the hands of the users.