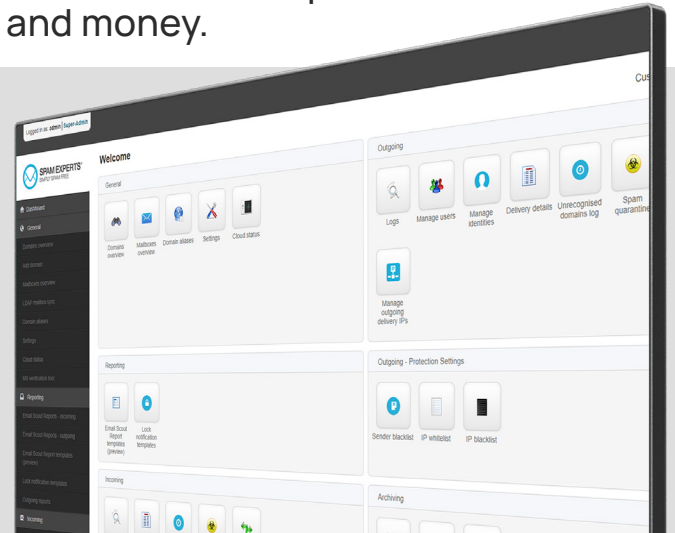


# SpamExperts Outgoing Email Filter

A powerful solution to safeguard networks from outbound spam and malware, helping web hosts save time and money.

A compromised account or script can lead to unknowingly sending out malware from your network. N-able™ Spam Experts helps web hosts and ISPs/telcos strengthen email protection. The outgoing filter helps prevent outbound spam and IP blocking while increasing email delivery and continuity. The solution can be deployed in a redundant cloud environment or on-premises.

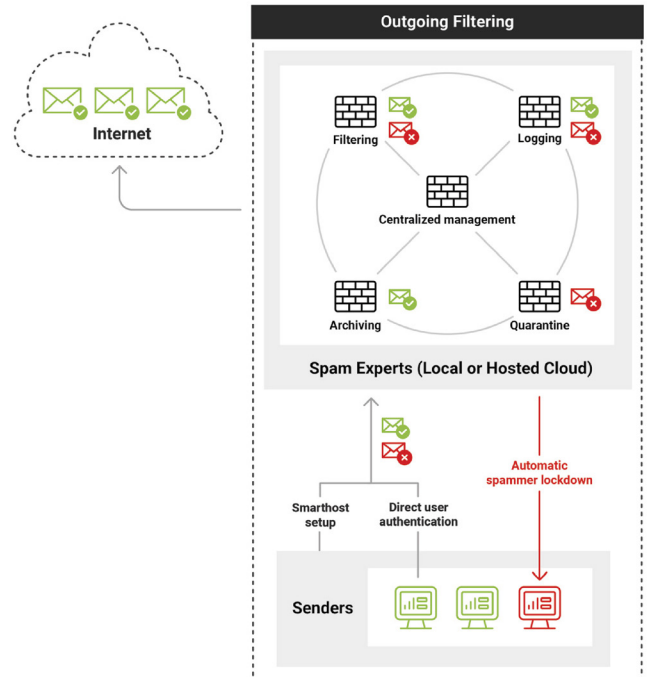


## How it works:

N-able® SpamExperts outbound spam and virus filter is an email gateway solution. Activation is done via the web interface or by using the API directly. Implementation can be done through a smart host setup, where all outbound emails are rerouted through the filtering system before going out to the internet.

Alternatively, the outgoing filter can authenticate on a per-user basis, where the filtering systems are directly used as outgoing SMTP servers.

By including N-able SpamExperts in your email delivery process, you add an extra layer of redundancy and protection to your infrastructure. Outbound messages are first delivered to our server, where we filter them to make sure only legitimate emails leave your network. Spam email is then stored in quarantine for your review and control.



## Helps save resources and protect business and sender reputation

- Protects networks against outbound, email-based threats.
- Provides control over potentially malicious activity within the customer's network, through proactive email monitoring and filter reports.
- Offers the ability to automatically or manually lock down potentially compromised accounts to prevent spreading viruses and safeguard a company's reputation.

## Gives customers and users visibility and control over their email flows

- Offers real-time visibility into threats.
- Helps secure outbound email continuity and delivery via timely lockdown of compromised accounts.
- Helps improve manageability of potentially malicious activity.

## Offers dual deployment options and integrates with a broad range of tools

- Cloud or on-premises deployment.
- Free plug-ins to integrate with the most popular control panels and other email collaboration tools.
- Multiple branding options available.

**SPAM EXPERTS**  
SIMPLY SPAM FREE

**Log Search**

All connections that are handled by the filter (other than when the filter is disabled, and those handled by denial of service protection) result in a log entry that records meta-data about the message, its classification, and what happened to it. This information is kept for a period of time controllable at the domain level, and is then purged. There is a short delay, typically well under 10 minutes, before log entries are available here.

For now, the deprecated quarantine page may still be used.

[Export entries as CSV](#)

[Email this search](#)

**Query Rules** Match  All  Any

Domain equals Type to view suggestions

Status is one of Quarantined

Quick select:  Accepted  Not accepted

Log search

# Features at a glance

## Outbound filtering setup

- Outgoing delivery IP management, including reputation checks for local cloud users.
- Detection of end users based on user-defined rules and automatic locking of end user accounts when suspicious activity is detected, including customizable admin notification.
- Automatic handling of received ARF reports.
- IP / sender / recipient allow list / blocked list.

## Filtering technologies

- Filtering at SMTP and data level, SL/TLS traffic encryption.
- Custom rules: simple matches or regular expressions on message content or metadata, custom rate limiting, and attachment restrictions.
- Protection against brute force authentication attempts, including auditing.
- Support for BATV (PRVS), DKIM signing.

## Web interface/control panel

- Multilingual, brandable interface with multilevel access (super admin, admin, reseller, domain, and email-address level).
- Authentication against remote LDAP server (email user level).
- OAuth 2 / OpenID® Connect authentication (admin level) and optional two-factor authentication.
- HTTPS, including forcing, free certificate generation and management.

**Try it free**

30 days, full version

© 2021 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein.