

ANNOUNCEMENT: SPAM SOAP TO RELEASE SERVICE ADVANCEMENTS OVER DECEMBER 15-16.

As part of our commitment to provide you with the most effective and easy-to-use managed security services in the industry, in mid-December, Spam Soap will deploy the following service advancements:

Increased Spam Soap Console Availability

What's Changing? – Spam Soap will enable greater access to the Spam Soap Console during planned or emergency maintenance, ensuring that the administrative console will be available for configuration and support of Spam Soap services during maintenance windows. Two significant areas on the Spam Soap Console - Quarantine and Reports - will remain accessible during scheduled or emergency maintenance unless they are directly being serviced.

Why? – Efficiency. Customers are no longer restricted from accessing the entire Spam Soap Console during planned or emergency outages, but rather, only the areas undergoing maintenance.

Impact – Maintenance on the Quarantine database will prevent access to end user or administrative spam quarantines, but will not affect access to Reports. Conversely, maintenance on the log database will affect access to reports on the Overview and Reports pages, but will not affect access to spam quarantines. A 'Page Unavailable' message will be displayed whenever a particular area is inaccessible due to maintenance. Additionally, you may subscribe to our Service Alerts [RSS feed](#) for the most up to date Service Alerts.

Expanded Protection from Notorious Spammers

What's changing? – The Spam Soap Threat Management team continually monitors the performance of the third-party Real-time Blackhole Lists (RBLs) and its own proprietary global deny lists, to ensure customers are receiving the broadest and most current protection. This continuous monitoring process has resulted in the identification of additional known spammers not currently on the existing RBL; these are being added to Spam Soap's roster of third-party RBLs. As a result of these additional RBLs Spam Soap offers a more comprehensive filtering system, which also includes domain-level allow and deny lists, user-level allow and deny lists, and recipient deny lists will be in place for all Spam Soap Email Defense Service packages.

Why? – Better spam protection: expanding the number of third-party RBLs decreases the likelihood that messages originating from suspect addresses will reach Spam Soap customer inboxes.

Impact – The expansion of third-party RBLs will have the following effects on Core Filtering functionality:

- The expanded list of RBLs will be enabled by default for all new policy sets to ensure the highest level of spam identification, which automatically blocks messages from suspect IP addresses prior to filtering by the entire Spam Soap Stacked Classification Framework®.
- NEW: customer-level and user-level allow lists will supersede the Spam Soap RBLs on a per address basis, giving customers even greater control over how their incoming email is handled. Spam Soap will compare a sending address against the customer-level and user-level allow list prior to RBL filtering, and will deliver the message if the address appears on an allow list, while still blocking other un-defined email addresses from offending sending IPs.
- With the expanded RBL protection, customers will see a decrease in overall messages filtered and quarantined by Spam Soap, as messages found to originate from highly suspect IP addresses will be blocked in the RCPT TO phase of the SMTP conversation.
- Messages blocked due to inclusion of the sending IP address on a third-party RBL will be listed on the Spam Detection Summary report within the Email Defense Service tab on the Spam Soap Console.
- Spam Soap customers can control their filtering selections for RBLs. If by chance a customer would like to opt out of utilizing the RBL protection, they may choose to do so. However, for security purposes, it is not recommended.
- Customers that currently opt in for protection via one of the Mail Abuse Prevention System lists, will be automatically included in the new RBL protection.

(continued on back)

Improved Outbound Email Authentication and Security

What's Changing? – Spam Soap is adding an additional layer of authentication for all outbound email in order to ensure that mail is sent from only registered domains (e.g. customer.com) or sub-domains (e.g. marketing.customer.com), combined with IP addresses that are authorized for outbound traffic within the Spam Soap system.

Why? – Protecting Customer's Mail: by validating all outbound mail sent from registered domains, sub-domains, and IP addresses, Spam Soap is helping to curb outbound abuse by blocking phishing attacks, and spam sent through botnet accounts and open relays.

Impact – Spam Soap will compare the sending IP and "MAIL FROM" addresses of each outbound message with those entered into the Spam Soap Console for each customer, and will block all outbound traffic being sent from non-authorized domains and sub-domains. To ensure you are not sending messages via an open relay, please see your Spam Soap Setup Instructions for details on checking your email environment for open relay(s).

Maintenance Timeframe

Spam Soap will deploy these service advancements over the weekend of December 15th. Customers will see the changes in effect on Monday, December 17th. For details about the maintenance window, please visit <http://www.spamsoap.com/support>. If you have questions about this service update, contact Spam Soap Customer Support Services at 866.772.6688 or via <http://www.spamsoap.com/support>.