

Symantec Hosted Mail Security Getting Started Guide

Redirecting Your MX Record

You have successfully activated your domain within the Symantec Hosted Mail Security Console. In order to begin the filtration process, you or your Internet Service Provider (ISP) must redirect this domain's MX Record. As a result, Symantec will be able to receive your email messages, filter them for spam and viruses, and ultimately forward safe and unquarantined messages on to your mail server.

The redirect of your MX Record should look like this (you would specify `<domain>.<xxx>`):

`<domain>.<xxx>.inbound10.symantecmail.com` preference level of 10
`<domain>.<xxx>.inbound10.symantecmail.net` preference level of 10

This process should be completed for each domain that you are converting to the Symantec Hosted Mail Security Console.

If you have never redirected your MX Record and aren't sure whether you have the ability to perform this function, you should contact your ISP or Host as they may control access to your record and may be able to complete this change for you.

Locking SMTP Ports

Before locking down the SMTP port, we recommend that you allow for [at least three days](#) after redirecting your MX records. Thereafter, you must lock down the SMTP port that your email traffic is delivered to. Because spammers can often archive the name of your email server and send messages directly to you (bypassing the advertised path that all email should follow with the MX Record), you should only allow email from Symantec. If you do not lock down the SMTP port, you may still receive viruses and spam sent directly to your email server.

IPs for Symantec Lockdown at the Firewall

To ensure that no mail is presented to your mail server without being processed by Symantec Hosted Mail Security, you will need to restrict all IP access to your mail server with the exception of the following subnet. The preferred setting is to include the Classless Inter-Domain Routing (CIDR) for the entire Class 8 C notation. Alternate settings are also provided below.

Preferred Setting

If your firewall solution accepts Classless Inter-Domain Routing (CIDR) and can support Class 8 C notation please include the following:

| CIDR | Starting IP | Ending IP |
|-----------------|--------------------|------------------|
| 208.65.144.0/21 | 208.65.144.0 | 208.65.151.255 |
| 208.81.64.0/22 | 208.81.64.0 | 208.81.67.255 |

Network Mask:

Network Address 208.65.144.0 / Netmask 255.255.248.0

Network Address 208.81.64.0 / Netmask 255.255.252.0

Alternate Setting (1)

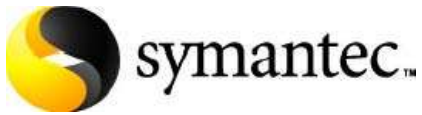
If your firewall solution accepts Classless Inter-Domain Routing (CIDR) and only supports Class 1 C notation, you will need to include the following entries to the entire subnet:

| CIDR | Starting IP | Ending IP |
|-----------------|--------------------|------------------|
| 208.65.144.0/24 | 208.65.144.0 | 208.65.144.255 |
| 208.65.145.0/24 | 208.65.145.0 | 208.65.145.255 |
| 208.65.146.0/24 | 208.65.146.0 | 208.65.146.255 |
| 208.65.147.0/24 | 208.65.147.0 | 208.65.147.255 |
| 208.65.148.0/24 | 208.65.148.0 | 208.65.148.255 |
| 208.65.149.0/24 | 208.65.149.0 | 208.65.149.255 |
| 208.65.150.0/24 | 208.65.150.0 | 208.65.150.255 |
| 208.65.151.0/24 | 208.65.151.0 | 208.65.151.255 |
| 208.81.64.0/24 | 208.81.64.0 | 208.81.64.255 |
| 208.81.65.0/24 | 208.81.65.0 | 208.81.65.255 |
| 208.81.66.0/24 | 208.81.66.0 | 208.81.66.255 |
| 208.81.67.0/24 | 208.81.67.0 | 208.81.67.255 |

Alternate Setting (2)

If your firewall solution does not accept Classless Inter-Domain Routing (CIDR) notation, you will need to include the starting and ending IP address for either the Class 8 C addresses or the Class 1C addresses which are included above.

Any of the above changes can be done by creating a firewall rule, or restricting access at the server level. We highly recommend that you lock down this subnet at your firewall as the priority preference. Please consult with your network administrator before making any changes. For additional information



regarding the restriction of IP addresses please refer to instructions from your firewall setup or from your firewall provider.

IPs to Be Removed

The following subnet(s) have been removed from service. Please remove the following subnet(s) if they are included in your current firewall configuration:

216.183.122.64/26

198.65.127.0/24

Confirming Account Information

Now that your order has been processed, use the Symantec Hosted Mail Security account information you completed in the Service Activation process to log on. To access the Symantec Hosted Mail Security console, please visit:

<https://hostedmailsecurity.symantec.com>

The end user service license agreement is also attached to this message and will be sent via regular mail with your license certificate. This is a legal and enforceable contract between you and Symantec. By using the user name and password provided by Symantec, or by using the Symantec Hosted Mail Security service, you agree to the terms and conditions of this Agreement. If you do not agree to these terms and conditions, then do not use the user name or password and make no use of the service.

Provisioning Outbound Message Filtering

Please note that the following steps will be required during the service configuration process to provision Outbound Message Filtering as part of your service package:

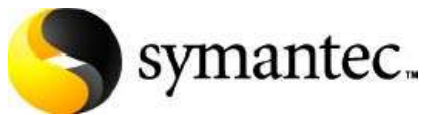
1. Enter the IP address(es) associated with the outbound service on your mail server on the Hosted Mail Security Console Setup tab, Outbound configuration.

2. Establish a relay or Smarthost sending outbound traffic to:

<domain>.<xxx>.outbound10.symantecmail.com

<domain>.<xxx>.outbound10.symantecmail.net

You **MUST** specify a domain and not an IP in your relay or Smarthost and **MUST** use the domains listed above. You supply the <domain>.<xxx>.



After these tasks have been completed, Symantec can accept your outbound email for filtering of virus, worms, and other unwanted content and attachments.

Once you redirect your MX record, Symantec will become your first line of defense against email threats coming from all inbound email directed at the domain(s) Symantec is filtering on your behalf. Symantec Hosted Mail Security will begin to identify and automatically integrate the email boxes on your domain(s). DNS propagation [may take up to 72 hours](#), including any processing time on the part of the host or ISP that is redirecting the MX records. Once we begin to receive your email flow, we will immediately begin real-time filtration and message delivery.

Configuring Fail Safe Notifications

Fail Safe is a feature of the Symantec Hosted Mail Security Console which will store messages for you in the event that your email server cannot accept email, either due to an outage or during planned maintenance periods.

Fail Safe is set to alert up to four (4) contacts of your choice by email should the Console begin to store messages due to a server outage. To establish this process, enter the email addresses of the contacts into the Console. You may access this area of the Console by clicking **Setup** tab > **Fail Safe** tab.

To ensure that the email alerts to your designated contacts are not impacted by the outage of your email server, the Symantec Hosted Mail Security Console will not allow you to enter the email address of a domain that has been provisioned in the system – email addresses that are used for Fail Safe notification should route to cell phones, pagers, or other off-network monitored devices.

Reference Materials

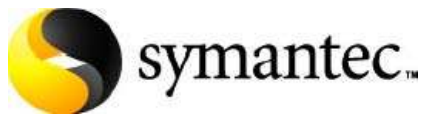
Symantec provides reference materials to assist with the administration and use of Symantec Hosted Mail Security. For quick access to important reference material, please visit http://www.symantec.com/enterprise/products/otherresources.jsp?pcid=2242&pvid=863_1 where you will find downloadable PDF copies:

- Symantec Hosted Mail Security Console Administration Guide
- Symantec Hosted Mail Security Console & Spam Quarantine User Guide

Symantec Hosted Mail Security Frequently Asked Questions

Q: How do I configure the Mail Transfer Agent (MTA)?

A: The service is currently configured to deliver your inbound SMTP traffic to the MTA(s) on your premises configured during the Symantec service setup and activation process. You can change the address where you want your incoming email traffic delivered by using the Symantec Hosted



Mail Security console. Please use caution when making changes to the SMTP hosts configured within the console, as modifications will be enabled instantly and will impact email traffic flow.

Q: What is the Symantec Hosted Mail Security console and how do I log on to it?

A: The Symantec Hosted Mail Security console is a Web-based administration and reporting tool that enables administrators to customize service configuration, policy setting, and reporting. To learn more about administration and use of your service through the console, review the administrator and end-user guides. The *Symantec Hosted Mail Security Console Administration Guide* will help you to navigate the service and to benefit more from the service through suitable policy and reporting configuration.

To log on to the Hosted Mail Security console, type <https://hostedmailsecurity.symantec.com> in your browser (preferably Internet Explorer 6.x) and then enter your email address and the temporary password supplied to you during the provisioning process.

Q: What are the default spam filtering policy settings?

A: Symantec spam filtering detects the likelihood that an email is spam by processing the message through hundreds of rules and tests to ultimately arrive at an overall spam score of medium or high. Through the Symantec Hosted Mail Security console, you can establish policies to tag, quarantine, or deny emails based on corresponding sensitivity levels.

“Spam Reporting” allows end users to receive periodic summaries of their quarantined spam messages. By utilizing this feature, administrators are relieved of the burden of managing the entire spam quarantine at the domain level, by pushing the responsibility to end users who can view and clean their own personal spam quarantine.

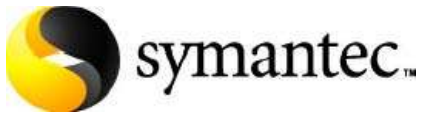
This feature is disabled by default; however, we recommend enabling of the feature for the first several weeks.

Symantec Hosted Mail Security supports an white and black lists through “allow” and “deny” policies that override spam sensitivity levels. Personal allow/deny lists may also be managed at the individual recipient level. However, corporate-based allow/deny lists supersede those of individual end users.

After about four weeks, your allow/deny lists should be sufficiently fine-tuned at both the corporate and end-user levels to set your policy configuration to “deny” for high likelihood spam messages.

For more information on configuring spam policies and associated actions, please refer to the *Symantec Hosted Mail Security Console Administrator User Guide, v3.2* (Administrator guide).

Note: Some messages may be marked as spam when in fact they are legitimate emails. While we believe that these “false positives” will be infrequent, it may happen occasionally, especially to mailing lists and opt-in newsletter traffic. You can quickly alleviate the occurrence of these false



positive filtering results by selecting “allow” for those messages, which will “white list” (i.e. always allow) that message type in the future.

Q: What are the default allow/deny policy settings?

A: While it is easy to construct enterprise level allow/deny lists that override spam sensitivity levels; there are no predefined allow/deny lists. Please note that turning on MAPSSM features will override your allow lists, when an address on this list is also on the MAPS list of probable spammers.

For information on configuring allow/deny list policies and associated actions, please refer to the *Symantec Hosted Mail Security Console Administration Guide*.

Q: What are the default virus and worm scanning policy settings?

A: Symantec Hosted Mail Security is configured with default policies that should provide adequate initial protection against virus threats, until you are more familiar with the service and can customize options to meet the unique needs of your organization.

Currently, your virus protection policy is configured to clean messages that contain viruses or infected attachments. If an infected message cannot be cleaned, the offending attachment(s) will be stripped from the email before delivery occurs. The recipient will be notified in either case with the results of the cleaning attempt.

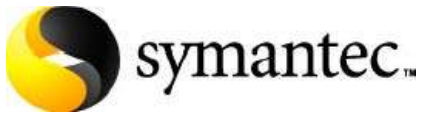
If you prefer, you may establish policies on how infected email should be handled (i.e. denied, cleaned, stripped, or quarantined). To learn more about configuring your virus policies, please refer to the *Symantec Hosted Mail Security Console Administration Guide*.

Q: What are the default attachment filtering policy settings?

A: The default policy settings for attachments allow any and all attachment types and sizes. For information on configuring attachment policies and associated actions, please refer to the *Symantec Hosted Mail Security Console Administration Guide*.

Q: What are the default content filtering policy settings?

A: Symantec uses a “bucket” configuration to organize keywords. These buckets (or content groups) contain related keywords which, when detected, trigger an alert that the message contains unwanted content. Each bucket can be turned on and off, depending on the policies set



for your organization. Additionally, you are able to customize keyword buckets to meet the unique needs of your organization.

Symantec has pre-defined the following three content groups whose content keywords are continuously monitored and updated:

- Profanity
- Sexual Overtones
- Racially Insensitive

The default policy for each group is “inactive.” For information on configuring content filtering policies and associated actions, please refer to the *Symantec Hosted Mail Security Console Administration Guide*.

Sample End-User Email Notice

Symantec has provided the following email sample for your convenience. If desired, send it to your organization’s end users in order to announce the use of the Hosted Mail Security service.

To: [Corporate Email User]

Subject: New Email Security Service

To better protect [Name of Your Organization] and its employees from the harmful effects of unwanted email, we have implemented an email protection and security service that filters all inbound email for spam, viruses, inappropriate content and unauthorized attachments.

You should begin seeing the benefits of this service immediately, as you notice considerably less offensive and distracting email being delivered to your inbox.

You will also start receiving regular Spam Quarantine Reports in your email inbox. Initially, these reports will be emailed to you once a day. They will contain those inbound email messages directed to your email inbox that are suspected of being spam. Spam Quarantine Reports will enable you to more easily and conveniently manage spam by safely viewing the messages that have been quarantined and by providing options for how you would like the messages handled in the future. This process, called “Conditioning the Quarantine,” will ensure that you continue receiving certain messages, which the email filters identify as spam. These include newsletters, association bulletins, and other subscriptions. Once you begin receiving Spam Quarantine Reports, you will have the option to change the frequency of report delivery.

Any email with questionable content or unauthorized attachments will be held (quarantined) by our email administrator until it is determined whether the email should be released to the email user’s Spam Summary Report or deleted from the quarantine. Please review the company email policy to determine why email might be quarantined.



We encourage you to contact [Email Administrator Name] if you believe an email has been misidentified as spam and quarantined. We will be happy to release the email if appropriate.

Sincerely,

[Network Administrator]