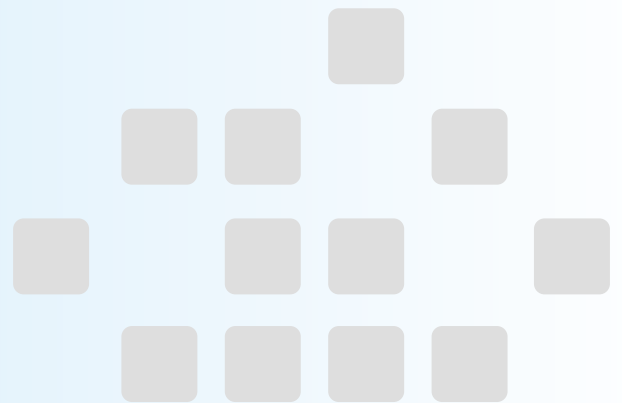


**Best**  
The World's ~~First~~ Free Email Security Service



# SAFENTRIX Outbound Email Security Quick Start Guide

## Contents

|  |    |
|--|----|
| Introduction   | 3  |
| Outbound Email Security - Details                            | 3  |
| Word of Caution  | 4  |
| Outbound SMTP Relay Service for Individual Users             |    |
| Concept  | 5  |
| Installation   | 6  |
| Outbound Email Security for Mail Servers - Helper Web Site   | 11 |
| Outbound SMTP Relay Service for Mail Servers Using SPF       | 11 |
| Outbound SMTP Relay Service for Mail Servers Using SMTP Auth | 14 |

## Introduction

SAFENTRIX is a complete Email Security Solution protecting your Inbound as well as Outbound Emails from Virus/SPAM and other misuse. This document explains the concepts in SAFENTRIX Outbound Email Security and how to activate the same.

This document assumes that you are familiar with Email and DNS systems and protocols. If that is not the case, we would recommend that you refer to SAFENTRIX Outbound Email Security Installation Guide.

## Outbound Email Security - Details

Once you activate SAFENTRIX Outbound Email Security for your domain(s) , your users as well as Email servers can relay outgoing emails through SAFENTRIX Servers. When emails are sent through SAFENTRIX Servers,

1. SAFENTRIX scans the emails for Virus/SPAM. If any is found, the message is bounced back to sender.
2. If no Virus/SPAM is found, the email is delivered to the destination.

SAFENTRIX provides the following three mechanisms for setting up Outbound Email Security.

1. **Outbound SMTP Relay Service for Individual Users:** This allows your users to send Emails through SAFENTRIX Servers using SMTP Auth. Email administrator can choose to use the user's current Email password as SMTP Auth password (or) allow the user to set a new SMTP Auth password and use it to relay through SAFENTRIX Servers.
2. **SPF based Outbound Relay Service for Mail Servers:** This service is meant for Email Servers that have a fixed (aka Static) IP. This is the recommended mechanism for implementing Outbound Email Security for your mail servers. In this mechanism, you have to add SPF records allowing the Email server to send emails for your domain. SAFENTRIX uses this information to relay emails from your servers.
3. **SMTP Auth based Outbound Relay Service for Mail Servers:** This service is meant for Email servers that are on a dynamic IP and support SMTP Auth for sending outgoing emails.

In the following sections, we will present instructions on implementing Email Security using each of the above mechanisms.

## Word of Caution

SAFENTRIX provides Outbound Email Security using SMTP Relay service mechanism. There are no restrictions on the usage either in terms of number of emails that can be sent or in terms of Bandwidth utilization.

However, SAFENTRIX bars sending of Unsolicited Bulk Emails through its Servers. SAFENTRIX has robust mechanisms for identifying SPAM/Virus and Unsolicited Bulk Emails. If you use SAFENTRIX for sending Unsolicited Bulk Emails your domain will be blacklisted and barred from using SAFENTRIX Services in future.

Please find below some of the activities that are not allowed:

1. Sending SPAM emails.
2. Obtaining a mailing list from a third party and sending emails.
3. Sending emails to in-house non-opt in mailing lists.

Some bulk email activities that are allowed:

1. Sending transactional emails to your clients/prospects.
2. Sending a Newsletter to your opt-in clients/prospects

*Please also note that as per policy, you can only send emails through SAFENTRIX using valid "From:" email addresses. If you send out emails using invalid/non-existent "From:" email addresses, you will not be able to use SAFENTRIX for Outbound Email Security.*

## Outbound SMTP Relay Service for Individual Users

### Concept

Select group of (or all) users from your domain can be given Outbound SMTP Relay service privilege. Once this is done, users who have Outbound SMTP Relay privilege can use the following details to send out emails:

| Description                                      | Value  |
|--|--|
| Outgoing SMTP Server Address                     | smtp.safentrix.com   |
| Outgoing SMTP Server port                        | 2525 (Alternately 25, 587 can be used)   |
| Outgoing SMTP Server requires Authentication     | Yes  |
| Outgoing SMTP Server Authentication Account name | Email address of user  |
| Outgoing SMTP Server Authentication Password     | Administrator can decide either:<br>Can be same as Login password of user (or) User can set a password for SMTP Relay at <a href="http://www.safentrix.com/setsmtppassword">http://www.safentrix.com/setsmtppassword</a> . |
| SSL/TLS  | Available but Optional. If SSL is chosen, user should choose Outgoing SMTP Server port as 465  |

For compliance purposes, SAFENTRIX has an Archival mode for Individual users. If this mode is chosen, a Bcc (Blind Carbon Copy) of every email sent out by the user through SAFENTRIX is sent to an "Archive Email ID".

This option can be set on a per-user basis.

## Installation

Outbound SMTP Relay Service for individual users can be enabled by following these instructions. The instructions are given in form of a check list. We recommend that you tick off each step as you complete them. This way you can be sure that no steps are missed.

| Step No.  | Description   | Done |
|-----------|---|------|
| <b>1.</b> | <b>ACTIVATE THE DOMAIN IN SAFENTRIX</b>   |      |
|           | Activate the domain of user Email address in SAFENTRIX. If not done, please refer to SAFENTRIX Quick Start Guide in SAFENTRIX Support page  |      |
|           | Point Domain's MX record to 'a.as.safentrix.com' and 'b.as.safentrix.com'   |      |
|           | Goto <a href="http://www.safentrix.com/drsafentrix">http://www.safentrix.com/drsafentrix</a> , enter your SAFENTRIX account name and Domain name. If the page says "Everything in your setup is fine", proceed to the next step. Otherwise, follow the instructions given in that page and try this step again.   |      |
| <b>2.</b> | <b>ACTIVATE OUTBOUND EMAIL SECURITY AND INDIVIDUAL USER RELAY PRIVILEGES</b>  |      |
|           | Login to SAFENTRIX Control panel  |      |
|           | Click on User's domain  |      |
|           | Click on "Outbound Email Security" Link   |      |
|           | Click on "Enable" link next to "Outbound Mail Filtering status" field.  |      |
|           | Check the "Allow individual users to relay messages through SAFENTRIX Servers using SMTP Auth" check box.   |      |
| <b>3.</b> | <b>(OPTIONAL) SPECIFY MOBILE NUMBER FOR SMS NOTIFICATIONS</b>   |      |
|           | <p>In case SAFENTRIX notices SPAM/Virus/Unsolicited Bulk Emails from any user, it will disable the Outbound relay privilege for that user temporarily and send an Email alert informing the same.</p> <p>Optionally SAFENTRIX can also send a SMS alert to your Mobile number. Sending alerts by SMS is a chargeable service and is only done if there is sufficient balance in your SAFENTRIX Account. Every SMS alert is charged at the rate of INR 10/USD 0.25</p> <p>You can enable SMS alerts by following the instructions below.</p> |      |

| Step No.  | Description  | Done |
|-----------|--|------|
|           | <p>SMS Notification is a chargeable service. When you activate this service, SAFENTRIX verifies the Mobile number by sending a confirmation code by SMS. The verification SMS is charged INR 10/USD 0.25.</p> <p>To start the SMS Alert activation process, recharge your account balance by at least INR 50/USD 1.</p>  |      |
|           | <p>Click on the “Change” Link next to “Contact number for notification messages” field.</p> <p>A dialog appears with the text “Please enter the mobile number for notification”. Enter your complete Mobile number (including country code) in the space provided.</p> <p>Please be sure to include the Country code in the start. You can look up your country code in <a href="http://en.wikipedia.org/wiki/List_of_country_calling_codes#Complete_Listing">http://en.wikipedia.org/wiki/List_of_country_calling_codes#Complete_Listing</a>.</p> |      |
|           | Click on “OK”. SAFENTRIX Sends a confirmation code to your Mobile number.  |      |
|           | Click on “Enter Confirmation Code to change” Link  |      |
|           | Enter the Confirmation code sent to you by SMS and click on “OK”   |      |
|           | Now your SMS Notification service is activated and you will receive an SMS if SPAM/Virus/Bulk Email messages originate from an Email address in your account.  |      |
| <b>4.</b> | <b>(OPTIONAL) ENABLE ARCHIVAL MODE</b>   |      |
|           | In “Archival” mode, a copy (Bcc) of all emails sent out by administrator specified users will be sent to a particular “Archive” email address. To enable this mode follow the next two steps.  |      |
|           | Check the box next to “Allow archiving for” field.   |      |
|           | Enter the email address where a copy of emails should be sent in the Edit box next to “Archive Email address for Outbound Emails” field. For security reasons, SAFENTRIX requires that the “Archive” email address be in the same domain as user email address.  |      |

| Step No. | Description   | Done |
|----------|---|------|
| 5.       | <p><b>(OPTIONAL) GET PASSWORD FOR USER FROM EXISTING EMAIL SERVER</b></p> <p>SAFENTRIX allows users to use their existing mail server password for SMTP Auth purpose. However, following conditions need to be satisfied for this mechanism to work:</p>  |      |
|          | <ol style="list-style-type: none"> <li>1. Email server of the user must support either plain POP3 or POP3 over SSL.</li> <li>2. Email server of user must be accessible anywhere from the Internet.</li> </ol> <p>If the above conditions are satisfied, administrators can follow the next steps to complete this operation.</p>   |      |
|          | Check the “Get initial passwords using POP3” Check box  |      |
|          | Give the IP address/Host name of User email server in the Edit box next to “Get Password from mail server address” field.   |      |
|          | <p>When trying to authenticate from the given mail server, SAFENTRIX sends the full Email address as account name. While this will be fine with majority of the Email servers, there are some Email servers that expect the account name in specific format. If yours is one such Email server, you will need to specify the Account name format.</p> <p>Account name format is specified as a string. The string can contain the special sub-string '%u' and '%d'. Wherever '%u' appears, it is replaced by the local part of the email address. Wherever '%d' appears, it is replaced by the Domain part of email address.</p> <p>Specify the format in the Edit box next to “With user name sent in the format” field if your Email server requires sending user name in the non-default format.</p> |      |
|          | If your Email server supports POP3 over SSL and you want SAFENTRIX servers to contact your Email server over SSL, click on the “SSL” radio button next to “Connect to POP Server using” field.  |      |



| Step No. | Description   | Done |
|----------|---|------|
| 6.       | <b>SAVE PREFERENCES</b><br><br>Click on “Submit” to save the above preferences. Outbound Email Security is now active for the domain. Please note that we still have to enable the Outbound Relay privilege for individual users before they can start sending out emails using SAFENTRIX Servers.  |      |
| 7.       | <b>SPECIFY USERS WHO ARE ALLOWED TO RELAY USING SAFENTRIX SERVERS</b><br><br>Create a text file with the names of users whom you want to allow relaying using SAFENTRIX Servers. The text file should contain only the user name (not the full email addresses) with one user per line. For example, if we want to allow Outbound relay privileges for 'info@safentrix.com' and 'sales@safentrix.com', the text file would contain<br><br>info<br><br>sales |      |
|          | Login to SAFENTRIX Control panel  |      |
|          | Click on the Domain name  |      |
|          | Click on “Show Users” link  |      |
|          | Click on “Bulk Operations”  |      |
|          | Click on “Browse” button and select the file with list of user names.   |      |
|          | Click on “Grant Outbound SMTP Permission to Users”.   |      |
|          | As this is a batch mode operation, SAFENTRIX will add this operation to the queue and when the operation is completed, notify you by Email.<br><br>Once the notification comes in, users can start Relaying emails through SAFENTRIX using the Outgoing SMTP details specified before.  |      |

| Step No. | Description   | Done |
|----------|---|------|
| 8.       | <p><b>(OPTIONAL) SPECIFY USER FOR WHOM ARCHIVAL MODE IS TO BE ENABLED</b></p> <p>If you want to enable Archival mode for select users, create a text file containing those user names, one per line. Suppose we want to specify Archival mode for 'info@safentrix.com' and 'sales@safentrix.com', the text file would contain</p> <pre>info sales</pre>   |      |
|          | Login to SAFENTRIX Control panel  |      |
|          | Click on the Domain name  |      |
|          | Click on “Show Users” link  |      |
|          | Click on “Bulk Operations”  |      |
|          | Click on “Browse” button and select the file with list of user names.   |      |
|          | Click on “Enable Archiving of Outbound emails for Users”.   |      |
|          | As this is a batch mode operation, SAFENTRIX will add this operation to the queue and when the operation is completed, notify you by Email.   |      |
|          | Whenever this set of users send out emails through SAFENTRIX, a Bcc of the email will be sent to the Archive email address.   |      |
| 9.       | <p><b>USER LEVEL OPERATION</b></p> <p>The above completes all the work to be done by you. If you have configured Outbound SMTP Relay Service to use the existing passwords (from POP Servers), users can start using SAFENTRIX Outbound Relay service right away.</p> <p>However, if you have chosen the default password mechanism, Each user has to do the following once, before they can start relaying email through SAFENTRIX Servers:</p> <ol style="list-style-type: none"> <li>1. Goto <a href="http://www.safentrix.com/setsmtppassword">http://www.safentrix.com/setsmtppassword</a>.</li> <li>2. Enter their Email address.</li> <li>3. An email confirmation link will be sent to the user.</li> <li>4. User has to click on the link and Enter a password.</li> <li>5. This will be user's Outgoing Email Relay password.</li> </ol> <p>User can start relaying emails using the above password and the “Outgoing Email Server” details mentioned before.</p> |      |

## Outbound Email Security for Mail Servers - Helper Web Site

Configuring SAFENTRIX Outbound Security Service requires you to know certain details about your Email Server. For example, some sections below require you to know the following:

1. HELO greeting of your Email Server.
2. Configure SPF records/Check whether SPF records are configured properly for your Email Server.

If you are not sure about these details or want to double check the details, you may do the following:

1. Send an email from your Email server to [test@allaboutspam.com](mailto:test@allaboutspam.com)
2. You will receive a bounce message with a Web link.
3. Click on the Web link and you will find all details about your Email Server.

## Outbound SMTP Relay Service for Mail Servers Using SPF

SAFENTRIX provides Outbound Email Security for Email servers. If your email server is on a Static IP, it can be configured to send all Outbound emails to 'smtp.safentrix.com' using SPF mechanism. SAFENTRIX servers will scan the outgoing emails for Virus/SPAM/Unsolicited Bulk Emails and if none is found, will deliver to the recipient.

SAFENTRIX will also send email/SMS alerts if any misuse of your Email server is found.

SAFENTRIX can be configured to relay outbound emails from your Email server by following these instructions:

If you have multiple Outgoing Email Servers, you have to repeat the following steps for each one of them.

| Step No. | Description  | Done |
|----------|--|------|
| <b>1</b> | <b>PRE REQUISITES</b>  |      |
|          | Make a list of all the domains your Email Server is sending outgoing Emails for.   |      |
|          | Add and activate the above list of domains in SAFENTRIX. For example, if your email server is sending out emails for domains 'safentrix.in' and 'safentrix.com', both domains must be present in SAFENTRIX and must be active.   |      |
|          | Make sure that all the above domains are present in a single SAFENTRIX account.  |      |
|          | Using <a href="http://www.safentrix.com/drsafentrix">http://www.safentrix.com/drsafentrix</a> , confirm that each of the above domains has been added to SAFENTRIX and activated.  |      |
|          | <p>Confirm that the 'HELO' greeting sent by your Email server is</p> <ol style="list-style-type: none"> <li>1. Same as your primary domain name (or)</li> <li>2. Sub domain of your primary domain name.</li> </ol> <p>By default, most of the Email server have this right, and no change will be required. However, if your Email server is configured to send a different 'HELO' greeting, you may want to change it to conform to the above condition.</p> |      |
| <b>2</b> | <b>INSTALLATION</b>  |      |
|          | Configure a SPF record in your DNS Server such that SPF check returns a 'pass' for the primary domain (which is in 'HELO' greeting) when relayed from your Email server IP.  |      |
|          | For more help on configuring SPF records, please visit <a href="http://old.openspf.org/wizard.html">http://old.openspf.org/wizard.html</a> .   |      |
|          | Login to SAFENTRIX Control panel   |      |
|          | <p>For each of your domains which the Email server relays email for (as in the above list), do the following:</p> <ol style="list-style-type: none"> <li>1. Click on domain name.</li> <li>2. Click on "Outbound Email Security"</li> <li>3. Click on "Enable" link next to "Outbound Mail Filtering Status" field.</li> </ol>   |      |

| Step No. | Description  | Done |
|----------|--|------|
| <b>3</b> | <b>CONFIGURE YOUR EMAIL SERVER</b>   |      |
|          | Please note that SPF records are DNS based and it might take some time (typically 4-6 hours) for the SPF record to be active.  |      |
|          | To be on the safe side, wait for about 8 hours after the above changes are completed.  |      |
|          | Reconfigure your Email server to send out all emails using 'smtp.safentrix.com'  |      |
|          | Monitor your Email server queue to see if emails are getting delivered successfully.   |      |
|          | If there are any problems with the setup, SAFENTRIX will reject the outgoing emails with a temporary (4xx) error code. This ensures that your emails do not bounce even if the Installation was not done properly. |      |
|          | If the above happens, see the Error message given by SAFENTRIX and take appropriate action to fix the problem.   |      |

Even though SPF mechanism is time consuming and requires technical expertise to setup, we recommend this mechanism for all email servers with a Static IP.. That is because the SPF mechanism used by SAFENTRIX for relaying emails has the maximum security.

## Outbound SMTP Relay Service for Mail Servers Using SMTP Auth

If your Email server is on a dynamic IP, SPF records cannot be configured. Therefore, SAFENTRIX allows you to implement Outbound Email Security for your email server using SMTP Auth (aka SMTP Authentication). SAFENTRIX Servers support PLAIN and LOGIN mechanisms for SMTP Authentication.

In this setup, you obtain an account name and password from SAFENTRIX for outgoing emails. Then the same is set in your Email server and the relay server is specified as 'smtp.safentrix.com'.

Detailed instructions are given below:

| Step No. | Description   | Done |
|----------|---|------|
| <b>1</b> | <b>PRE REQUISITES</b>   |      |
|          | Make a list of all the domains your Email Server is sending outgoing Emails for. Add and activate the above list of domains in SAFENTRIX. For example, if your email server is sending out emails for domains 'safentrix.in' and 'safentrix.com', both domains must be present in SAFENTRIX and must be active. |      |
|          | Make sure that all the above domains are present in a single SAFENTRIX account.   |      |
|          | Using <a href="http://www.safentrix.com/drsafentrix">http://www.safentrix.com/drsafentrix</a> , confirm that each of the above domains has been added to SAFENTRIX and activated.   |      |
| <b>2</b> | <b>INSTALLATION</b>   |      |
|          | Login to SAFENTRIX Control panel  |      |
|          | For each of your domains which the Email server relays email for (as in the above list), do the following:  |      |
|          | 1. Click on domain name.  |      |
|          | 2. Click on "Outbound Email Security"   |      |
|          | 3. Click on "Enable" link next to "Outbound Mail Filtering Status" field.   |      |
|          | Goto SAFENTRIX Control panel Login Home page  |      |
|          | Click on the Primary domain name of your Email server   |      |
|          | Click on "Outbound Email Security"  |      |

| Step No. | Description  | Done |
|----------|--|------|
|          | Generate a secure password (with alphanumeric as well as random characters). This will be your Domain SMTP Auth password.  |      |
|          | Specify the password in the edit box next to "SMTP Auth password" and in the edit box next to "SMTP Auth confirm password".  |      |
|          | Click on "Submit". 3 CONFIGURE YOUR EMAIL SERVER   |      |
|          | Reconfigure your Email server to send all outgoing emails using 'smtp.safentrix.com'. While sending out emails, configure your Email server to use "SMTP Auth" using PLAIN (or) LOGIN mechanisms.                  |      |
|          | The account name for "SMTP Auth" should be the primary domain name of your email server.   |      |
|          | Password for "SMTP Auth" should be the password generated in the steps above.  |      |
|          | Monitor your Email server queue to see if emails are getting delivered successfully.   |      |
|          | If there are any problems with the setup, SAFENTRIX will reject the outgoing emails with a temporary (4xx) error code. This ensures that your emails do not bounce even if the Installation was not done properly. |      |
|          | If the above happens, see the Error message given by SAFENTRIX and take appropriate action to fix the problem.   |      |