Managing Forcepoint Email Security Cloud

Managing Forcepoint Email Security Cloud | Document last updated: June, 2022

This guide includes the following troubleshooting and management articles for Forcepoint Email Security Cloud:

- *Switching email service provider*
- *Using antivirus software with the Forcepoint Email Security Cloud service*
- *Branding your outbound email*
- *Personal email report is no longer received*
- *What is the Postmaster address used for?*
- *Resetting the Company Master User portal account*

Switching email service provider

Overview

This article describes how to switch to Forcepoint Email Security Cloud from another email service, without losing or delaying any of your organization's email.

Switching your email service

1. Ensure your email server and firewall can accept messages from our service in addition to your current managed service.
2. Complete the enrollment to our service, logging on to the Forcepoint Cloud Security Gateway Portal and configuring domains and routes.
3. Forcepoint carries out our usual security checks on the domains and routes you specified.
4. When the checks are complete, because the service now knows the routing to your systems, it will begin to route email from existing customers of our service directly to your system, rather than via the service which is being replaced.
5. You can (at a time of your choosing) change the DNS MX records and your outbound mail server routing to point to our service instead of the service being replaced. This ensures that all other email is now routed via our service.
6. You must then continue to allow your email server and firewall to accept emails from the service being replaced for a period to ensure that all email has been delivered from it. This period of time is determined by the time required for the service being replaced to return any failed email delivery notifications for emails held in retry schedules, and your requirement to release emails held in quarantine areas.
7. You can then lock down your firewall and mail server to only accept emails from our service.

Using antivirus software with the Forcepoint Email Security Cloud service

Using antivirus software with the cloud email service | Forcepoint Email Security Cloud

Forcepoint recommends a multi-tiered antivirus strategy.

Apart from email, viruses can arrive on a corporate network by a variety of routes such as Web browsers, FTP, instant messaging, and file sharing tools.

The cloud service does not scan email within a corporate network: its role is to ensure that viruses cannot pass between the Internet and your corporate network. In addition, we cannot scan encrypted messages or file attachments. We therefore suggest running desktop-level antivirus solutions alongside the service. This ensures you are protected both against known and new viruses caught by Forcepoint ThreatSeeker technology, and against viruses that bypass the service or arrive in your network by other means.

Best practice is to run antivirus products on your email servers within the corporate network as well; this ensures that viruses cannot pass between unsecure, unprotected, or out-of-date machines within your corporate network.

Branding your outbound email

Branding your outbound email | Forcepoint Email Security Cloud

Outbound annotations can be used as a branding tool. In fact, any email sent by your company can contain corporate identifying marks that brand or market the corporate image. This branding can appear at the top, bottom or side of an email.

Your marketing team is completely free to decide how outgoing emails should be branded: using HTML and the _MESSAGE_ substitution tag, designing your brand message is easy. The example below shows how to create an annotation that gives each outgoing HTML email a column on the right of the message body showing the company logo and brand message:

```
<TABLE>
<TR>
<TD>
_MESSAGE_
<TD>
<IMG SRC="http://mycompany.com/mycompany_logo.gif"><BR>
My company address<BR>
My company disclaimer
</TABLE>
```

If you require any further help with the setup of annotations, refer to Forcepoint Cloud Security Gateway Portal Help.

Personal email report is no longer received

Overview

If you have noticed that you are no longer receiving a personal email report (formerly the end-user message report) by email, this article explains why.

Report subscription

The Personal Email Subscription is a facility that gives end users visibility of email messages processed by the cloud service.

The personal email report displays a list of clean and suspicious messages. End users can click the message subject and see the message in a secure area, and optionally request the delivery of spam-blocked emails. The administrator can allow users to have their own black/white lists, and it is also possible to configure whether the user is able to release a copy of a spam message.

To receive a personal email report, the user fills in the simple Web form at: https://www.mailcontrol.com/utility/message_report.mhtml.

In the personal email report there is a link to define the subscription details so that the report can be received on a regular basis. The user can select how often they want to receive the report.

Once users have confidence in the spam detection ability of the service, they often choose to receive the report less frequently or not at all. For this reason, the personal email subscription automatically expires after 3 months. The user will see re-subscribe warnings on their reports as the subscription expiry date nears.

If one of your users reports that they are no longer receiving their personal email report, they can re-subscribe by either:

- Accessing their last report and clicking on the re-subscribe link
- Filling in the simple Web form at: http://www.websense.com/content/messagereport.aspx

What is the Postmaster address used for?

What is the Postmaster address used for? | Forcepoint Email Security Cloud

When you create a new policy within your account, you are required to enter a postmaster email address. This address is used as the sender address when notifications are issued under that policy. Other than that, it is not used. If possible, you should use an address that can be replied to, so that if an end user replies to a notification, the message is delivered.

Note that RFC 2821, which defines SMTP, requires a postmaster address to be maintained for each domain receiving email. This does not have to be the address you provide in the portal.

Resetting the Company Master User portal account

Resetting the company master user portal account | Forcepoint Email Security Cloud

Overview

Each Forcepoint cloud portal account has a super administrator user, known as the company master user. This user is the initial contact for your account and has the highest rights and privileges. This article describes what to do if you lose access to the company master user account, and cannot use the automated password recovery procedure.

Resetting the password or creating a new logon account

You might find that you need Support assistance with a password reset or a completely new logon account in the following situations:

- The only IT administrator has left the company.
- The only IT administrator has forgotten the account password and cannot reset it.
- Nobody at your organization knows who is responsible for the service, or who has a portal account.

In order to create a new account or reset the password on an existing account, you must supply Forcepoint with written instructions nominating a person as the portal administrator. The written instructions should come from an authorized person (for example, the company IT manager or the nominee's direct manager), and adhere to the following rules:

- The letter must be written on paper with the company letterhead.
- The authorizer's name and job title must be included, and clearly legible.
- The authorizer and the nominee for portal administrator must be two different people.
- The letter must specify the name and contact details of the nominee.

The written authorization can be sent to Forcepoint by post or by fax.

These steps are necessary because Forcepoint takes your account security very seriously. We then take steps to verify your details before resetting the password or creating a new logon account. This can take 2 business days, assuming the supplied written authorization is acceptable.