Managing TRITON AP-EMAIL in the cloud

Topic 45000/ Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions

The following troubleshooting and management articles are available for TRITON AP-EMAIL with Email Cloud Module:

Changing managed service

Topic 45002 / Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions

Overview

This article describes how to switch to TRITON AP-EMAIL with Email Cloud Module from another managed service, without losing or delaying any of your organization's email.

Switching to TRITON AP-EMAIL

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 Cloud TRITON Manager and configuring the domains and routes.
3. Our staff carry 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 TRITON AP-EMAIL in the cloud

Topic 45003 / Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions

Websense 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 the 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 against both viruses that bypass the service and also new viruses, caught by Websense's ThreatSeeker technology, for which an antivirus pattern update has yet to be created.

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servers within the corporate network as well; this ensures that viruses cannot pass between insecure, unprotected, or out-of-date PCs within your corporate network.

Branding your outbound email

Topic 45004 / Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions

Outbound annotations can be used as a branding tool. In fact, any email sent by your company could 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, the design is very 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 the Cloud TRITON Manager Help.

End-user message report is no longer received

Topic 45005 / Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions

Overview

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

Report subscription

The EUMR is a facility that gives end users visibility of emails processed by the cloud service.

The EUMR displays a list of clean and suspicious messages. The end user can click on the message subject and see the message in a secure area, and optionally request the delivery of spam-blocked emails. The administrator can allow the user 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 an EUMR, the user fills in the simple Web form at: http://www.websense.com/content/messagereport.aspx.

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

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

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

- Accessing their last EUMR 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?

Topic 45006 / Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions

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

Topic 45007 / Updated: 21-Jan-2015

Applies To:	Websense Cloud Email Protection Solutions Websense Cloud Web Protection Solutions

Overview

This article describes what to do if you lose access to the Company Master User cloud portal 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 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 knows who is supposed to have a portal logon, or is responsible for the portal account.

In order to create a new account or reset the password on an existing account, you need to supply Websense with written instructions nominating a person as the cloud 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 Websense by post or by fax.

These steps are necessary because Websense 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.