APPTIX
Connecting Your Business. Anywhere.

# Email Anti-Virus

## Admin Guide

Document Revision Date: May 7, 2013

# Contents

# About Anti-Virus

Anti-Virus re-routes your inbound email and outbound email through the infrastructure. Multiple scanners, including the Skeptic™ scanner, scan the emails before they pass on to the final destination. Skeptic uses predictive technology to identify and stop new virus and malware outbreaks as they occur and before Anti-Virus signatures are available. (A virus signature is a unique string of bits that defines a specific computer virus. The signature is then used to detect instances of the virus.) Polling for signature updates is performed automatically every 10 minutes. Instant updates are carried out in the event of a new outbreak.

If an email is virus-free, it is delivered to the intended recipient. If a virus is detected, the email is quarantined. Any email that is found to be infected with a virus is quarantined for 30 days. Notifications can be generated automatically to the intended recipient, and Administrator. The service has no discernible effect on email delivery times.

Use the portal to configure Anti-Virus to your requirements.

## Viral URL links

Anti-Virus offers protection against positively-identified viral URL links within emails. Such links differ from email virus threats; the user performs a direct action to follow the link to an infected Web site.

To counter such threats, Anti-Virus actively follows the suspicious link in an email and checks the web site for viruses or other types of potentially harmful content or payload. If or when a suspicious link is confirmed as viral, a signature is created. Further emails that contain that link are treated as being infected with the virus and are quarantined.

To keep latency to a minimum, it is important to note that scanning for viral URL links does not happen in real time. Emails containing unknown URLs are delivered as normal, and the links are normally analyzed within a few minutes following the delivery. If a URL is found to be malicious, a signature is created and all future email with that link is quarantined.

This procedure means that on rare occasions you may receive an email that contains a potentially harmful link (before the link is confirmed as viral). When the URL is confirmed as viral, we email you a 'missed' report. The report informs you that you received an email containing a viral link before it was found to be malicious.

**NOTE:** To benefit from a real-time solution to protect your organization from web-based threats and viruses, inquire about Web Security.

## Defining Administrator Alerts

An administrator alert is an email that is sent to the Anti-Virus Administrator when a user has sent or has been sent a potential virus.

Alerts to Administrators contain the Pen number for the quarantined email. The Pen number is a unique reference number that is used to locate and release the email from within the portal. Currently, the content of virus alerts is not configurable.

**To specify an address for administrator alerts to be sent to**

1. Select **Services** > **Email Services** > **Anti-Virus**.
2. In the **Virus Settings** page **Administrator Alerts** section, enter the Anti-Virus Administrator's email address.
3. Click **Save and Exit**.

## Defining Global or Domain Settings

You can configure the Anti-Virus settings globally for all domains, or you can configure custom settings for an individual domain. Typically, you configure the Anti-Virus service using your global settings and making fewer changes for individual domains.

If you make changes to the settings for an individual domain, you cannot then change it back to using global settings.

**To apply settings for a specific domain:**

1. Select **Services** > **Email Services** > **Anti-Virus**.
2. In the **Virus Settings** page, do one of the following:
   - To specify global settings, select **Global Settings** from the drop-down list.
     The settings in the page are editable. The changes you make are applied only to all of your domains.
   - To specify custom settings for a domain, select the domain from the **Global Settings** drop-down list.
     When you select a specific domain to work with, the name of the domain displays as a heading.
     The fields in the page are editable and inherit the global settings, until you make a change. The changes you make are applied only to the selected domain.

## Defining User Alerts

A user alert is an email that is sent to the intended recipient of a potential virus, if the recipient's email address is inside the client's network.

Alerts to users contain the Pen number for the quarantined email. The Pen number is a unique reference number that is used to locate and release the email from within the portal. Currently, the content of virus alerts is not configurable.

**To specify whether the recipients of an infected email receive alerts:**

1. Select **Services** > **Email Services** > **Anti-Virus**.
2. In the **Virus Settings** tab, **User Alerts** section, select **Yes** or **No** as appropriate.
3. Click **Save and Exit**.

## Releasing a Quarantined Email

When Anti-Virus intercepts a virus in an email, it places the infected email into a holding pen. The infected email is stored for up to 30 days before it is deleted. This quarantine period ensures that the virus is isolated and cannot infect the intended recipient's computer.

Each quarantined email has a unique identifier, which is known as a Pen number. This number is stated in the administrator alerts and user alerts that are issued when an email containing a suspect virus is received.

An administrator can allow a virus-infected email to be released from the quarantine pen and delivered to the intended recipient.

**To release an email from quarantine:**

1. Select **Services** > **Email Services** > **Anti-Virus**.
2. In the **Virus Settings** tab, select **Virus Release**.
3. Enter the **Pen number** of the virus.
   The **Pen number** is found in the administrator alert.
4. Click **Go**.
   Details of the quarantined email display in a pop-up window.
5. Locate the required entry and click the **Release** option in the right-hand column.
   A disclaimer displays.
6. To release the quarantined email, click **Confirm**.
   A confirmation message displays.
   The email containing the virus is released to the intended recipient.

## Limiting the Size of Emails Received into the Organization

You can set a maximum size above which inbound emails are not received. You cannot specify the maximum size to be more than 1,000,000 KB.

**To set an email size limit:**

1. Select **Services** > **Email Services** > **Anti-Virus**.
2. In the **Virus Settings** tab, in the **Set maximum email size to** box, enter the maximum size for emails (in KB).
3. Click **Save and Exit**.