

IBM Express Managed Security Services for Email Security

Anti-Virus Administrator's Guide

Version 5.31

Table of Contents

1. Service overview	3
1.1 Welcome	3
1.2 Anti-Virus (AV) features.....	3
1.3 How does AV work?.....	3
2. AV notification messages.....	4
2.1 Overview	4
2.2 Notification message types.....	4
2.3 Controlling administrator and user receipt of virus notifications	4
2.4 Setting originator email address for virus notifications.....	5
3. Virus quarantine holding pen	6
3.1 Overview	6
3.2 Releasing an email from quarantine.....	7
4. AV statistics	8
4.1 Overview	8
4.2 Viewing virus statistics.....	8
5. AV reports.....	10
5.1 Overview	10
5.2 Configuring AV reports	11
5.2 Configuring AV reports	11

1. Service overview

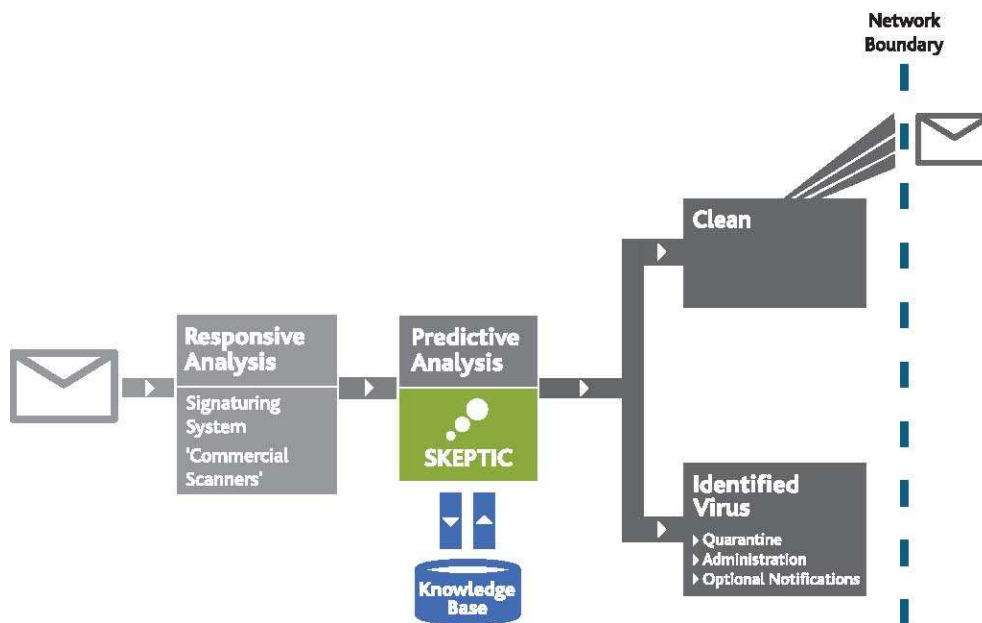
1.1 Welcome

Welcome to the Administrator's Guide for the E-mail Security Anti-Virus Service. The following information provides a walk-through of how to set-up the Anti-Virus Service.

1.2 Anti-Virus (AV) features

- Incorporates multiple commercial scanners to intercept known viruses
- Leverages Skeptic predictive technology to identify and stop unknown or dynamic threats
- Extremely effective at protecting clients during 'zero-hour' virus outbreaks when Anti-Virus signatures are not available
- Virus infected email quarantined for 30 days, retrievable by administrator
- Notifications can be auto-generated to sender, intended recipient and administrator.

1.3 How does AV work?



1.3 Anti-Virus service overview

AV re-routes all your inbound and outbound email through the Control Towers where it is scanned by three industry-leading scanners before being passed on to its final destination.

Polling for signature updates is automatically performed every ten minutes. 'Instant updates' are carried out in the event of a new outbreak.

The Skeptic scanner sits at the core of the AV service. It uses predictive technology to identify and

stop new virus and malware outbreaks as they occur.

If an email is virus free, it is delivered to the intended recipient. If a virus is detected the email is quarantined. The service has no discernible impact on email delivery times making it transparent to the recipient.

The InSight Service management tool is used to request AV reports and view virus statistics.

2. AV notification messages

2.1 Overview

Notification messages are emailed to the email sender and/or intended recipient when a virus has been sent to or from a client domain.

Default AV notification settings can be applied to all of a client's domains or custom settings can be applied to individual domains.

2.2 Notification message types

There are 3 types of notification message:

1. **Administrator Notification** – sent to the AV administrator when a user has sent or has been sent a potential virus
2. **Sender Notification** – sent to the sender of a potential virus
3. **Recipient Notification** – sent to the intended recipient of a potential virus (if this email address is inside the client's network).

Both administrator and recipient notification emails contain the Pen Number for the quarantined email. This unique reference number can be used to locate and release the email from within InSight (see [section 3.2](#)).

Note: the content of virus notification messages is currently not customer configurable.

2.3 Controlling administrator and user receipt of virus notifications

You can control whether or not a user receives a notification if they have sent, or are sent, a virus.

1. Select **ADMIN** from the top-left menu bar
2. Select **Domains** from the top-right menu bar

3. Select **Edit Default Banners & Email Settings**
4. Select **Misc.**

Default Banners & Email Settings

Banners **Misc**

Email Virus Alerts to: virus@mydomain.com

Alert my users if they send a virus: Yes No

Alert my users if they were sent a virus: Yes No

Maximum Email Size (in kB): 20000 Leave blank for unlimited

SMS Alerts to:

Must be prefixed by country code (e.g. 44 7717 123456 for UK, 1 501 123 456 for US)

Click this button to update these settings: **Update**

Click this button to exit without changes: **Cancel**

2.3 Controlling administrator and user receipt of virus notifications

5. Set **Email Virus Alerts** to the administrator email address. If the administrator does not require email virus alerts then leave this field blank
6. Set **Alert my** users if they send a virus and **Alert my users if they were sent a virus** options accordingly.

Note: these settings can be made either as domain defaults or for individual domains. If domain defaults have not been set, each domain will default to **'Yes'** for both options.

2.4 Setting originator email address for virus notifications

You can define the email address from which virus alerts appear to be sent from. For example, you may wish email alerts sent to internal and external users to be sent from an internal administrator email account. This means that alert recipients can respond to an email account within the client's organization.

Note: this can be done only on an individual domain basis i.e. the email address specified must be in the same domain the alerts apply to.

1. Select **ADMIN** from the top-left menu bar
2. Select **Domains** from the top-right menu bar
3. Select **Edit Banners & Email Settings** for the required domain
4. Select the **Misc.** tab

Banners & Email Settings for Domainb.com

Banners **Misc**

Email Virus Alerts from:	<input checked="" type="radio"/> alert@domainb.com <input type="radio"/> []@domainb.com
Domain Settings:	<input type="radio"/> Use Domain Defaults: <input checked="" type="radio"/> Use Custom Settings
Email Virus Alerts to:	[]
Alert my users if they send a virus:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Alert my users if they were sent a virus:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Maximum Email Size (in kB):	[] Leave blank for unlimited
SMS Alerts to:	<input type="radio"/> No Alerts <input checked="" type="radio"/> Default Alert Numbers <input type="radio"/> Custom Alert Numbers
domainb.com	<input type="text"/> <small>Must be prefixed by country code (e.g. 44 7717 123456 for UK, 1 501 123 456 for US)</small>
Click this button to update these settings: <input type="button" value="Update"/> Click this button to exit without changes: <input type="button" value="Cancel"/>	

2.4 Setting originator email address for virus notifications

5. Set **Email Virus Alerts from** option accordingly.

Note: the email address will also be used for sending Image Control alerts if this service is enabled.

3. Virus quarantine holding pen

3.1 Overview

When AV intercepts a virus in an email, it places the infected email into a holding pen where it is stored for up to 30 days before being 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 known as a Pen Number. This number can be found either in administrator and recipient virus notification messages, or by browsing through the InSight Anti-Virus statistics.

An administrator can allow the virus infected email to be released and delivered to the original recipient or to a specified email account.

3.2 Releasing an email from quarantine

1. Select **STATISTICS** tab from the top-left menu
2. Select **Virus** from the top-right menu
3. Enter the Pen Number in the **Pen Number** field and select **Search**

The screenshot shows a web browser window titled "Insight Account Management - Microsoft Internet Explorer". The interface has a dark blue header with navigation links: [STATUS](#), [STATISTICS](#), [ADMIN](#), and [LOG OFF](#). Below the header is a sub-menu with tabs: [Email](#), [Virus](#) (selected), [Spam](#), [Image](#), and [Content](#).

Under the "Virus" tab, there are filters for [Day](#), [Week](#), [Month](#), and [Year](#). A message states: "Viewing virus statistics for the last 7 days." To the right, there is a search box with the text: "If you know the Pen Number for an infected email less than 30 days old that you'd like to release, type it here:" and a "Search" button.

Below the search area, there are links for [By Virus](#) and [By User](#). A table displays virus statistics:

Virus Name	Number Sent	Number Received
	0	12
EICAR	0	5
Email-Worm.Win32.Dumaru.a	0	4
Email-Worm.Win32.Mydoom.am	0	5
Email-Worm.Win32.Netsky.q	0	67
Email-Worm.Win32.Swen	0	2
Email-Worm.Win32.Tanatos.b	0	1
EMLWorm.EM.dam	0	1
EMLWorm.MS.dam	0	1
EMLWorm.SM.dam	0	1
EMLWorm.VW.dam	0	1
EMLWorm.XX.dam	0	4
Exploit/HackedPacker-tElock-v0.71.dam	0	1
Exploit/HackedPacker-UPX.dam	0	4

The browser status bar at the bottom shows "Done" and "Internet".

3.2.1 Entering a Pen Number to release a virus

4. A pop up window will appear displaying the quarantined e-mail's details (see screenshot 3.2.2). To progress select **Release**
5. A further pop up window will appear. To release the quarantined email to a specified email address, enter the email address into **the Infected Email To** field and select **Release**. Alternatively to release the email to the original recipient, leave the **Infected Email to** field blank and select **Release**.

It is also possible to release a virus from within the statistics screen by clicking on a specific **Virus Name** in the 'By Virus' view or **Email Address** in the 'By User' view. When the virus name or email address is selected the following screen will appear:

Virus Statistics

[Day](#) | [Week](#) | [Month](#)

Weekly details for W32/NetSky.V@mm virus

Email Address	Description	Date	Pen	Mail Server	Release
anemail@eg.com	Received from domainX.com	05 July 2004 22:45 GMT	3335811_1089067475	3517	Release...
anemail@eg.com	Received from domainX.com	04 July 2004 21:54 GMT	440643_1088978017	2219	Release...
anemail@eg.com	Received from domainX.com	03 July 2004 02:54 GMT	3352171_1088823267	7707	Release...
anemail@eg.com	Received from domainX.com	07 July 2004 00:41 GMT	473407_1089160850	2202	Release...
Totals:	4 incidents	30 June 2004 to 07 July 2004			

3.2.2 Releasing an email from quarantine

Then simply follow the instructions for releasing the email from quarantine using steps 4-5 above.

4. AV statistics

4.1 Overview

AV provides statistics for viruses detected within inbound and outbound email. Statistics can be viewed by virus or by email user.

4.2 Viewing virus statistics

1. Log in to **InSight**
2. Select **STATISTICS** from the top-left menu
3. Select **Virus** from the top-right menu
4. Statistics can be viewed either **By Virus** (default) or **By User**
5. Select the period for which you want statistics, i.e. Day, Week, Month or Year.

Insight Account Management - Microsoft Internet Explorer

File Edit View Favorites Tools Help

[STATUS](#) [STATISTICS](#) [ADMIN](#) [LOG OFF](#)

[Email](#) **[Virus](#)** [Spam](#) [Image](#) [Content](#)

[Day](#) | [Week](#) | [Month](#) | [Year](#)

Viewing virus statistics for the last 4 weeks.

If you know the **Pen Number** for an infected email less than 30 days old that you'd like to release, type it here:

[By Virus](#) | [By User](#)

Virus Name	Number Sent	Number Received
	0	38
CID-Exploit.dam	0	1
EICAR	1	5
Email-Worm.Win32.Bagle.af	0	4
Email-Worm.Win32.Bagle.ah	0	1
Email-Worm.Win32.Bagle.ai	0	6
Email-Worm.Win32.Bagle.bo	0	3
Email-Worm.Win32.Bagle.g	0	7
Email-Worm.Win32.Bagle.gen	0	3
Email-Worm.Win32.Bagle.n	0	4
Email-Worm.Win32.Dumarua	0	13
Email-Worm.Win32.LovGate.ad	0	187
Email-Worm.Win32.LovGate.ag	0	6
Email-Worm.Win32.Mydoom.am	0	11

Done Internet

4.2.1 AV 'By Virus' Statistics

Insight Account Management - Microsoft Internet Explorer

File Edit View Favorites Tools Help

STATUS **STATISTICS** ADMIN LOG OFF

Email **Virus** Spam Image Content

Day | Week | Month | Year

Viewing virus statistics for the last 4 weeks.

If you know the Pen Number for an infected email less than 30 days old that you'd like to release, type it here:

Search

By Virus | By User

Email Address	Number Sent	Number Received
.00386833@radio0.messagegabels.com	0	4
.com@radio0.messagegabels.com	0	73
.ispmail.ntl.com@radio0.messagegabels.com	0	2
.ntl.com@radio0.messagegabels.com	0	122
.ntlworld.com@radio0.messagegabels.com	0	73
0.qmail@radio0.messagegabels.com	0	1
0003939cb5d8@radio0.messagegabels.com	0	2
00276@radio0.messagegabels.com	0	12
00290@radio0.messagegabels.com	0	12
00427@radio0.messagegabels.com	0	12
01048@radio0.messagegabels.com	0	12
1@radio0.messagegabels.com	0	15
11075200535118249479@radio0.messagegabels.com	0	2
115@radio0.messagegabels.com	0	1

Done Internet

4.2.2 AV 'By User' Statistics

5. AV reports

5.1 Overview

AV reports are scheduled service reports sent via email. They provide an overview of service performance and can be used to monitor service performance and carry out detailed trend analysis.

Report content, frequency and recipient email addresses can be configured within InSight.

Reports can be delivered in either Text or CSV (comma separated values) format. Text format is easier to read, while CSV format can be imported into spreadsheet or database applications and is therefore ideal for more detailed analysis or bespoke graph and statistics generation.

5.2 AV report Content

1. **Weekly and Monthly summary** report - a set of tables that provide an overview of key statistics for the AV service for the specified period across all client domains.

- **Service summary for all domains** (mail volume, virus volume sent, virus volume received, total virus volume, virus volume as a percentage of mail).
- **Service summary by domain** (mail volume, virus volume sent, virus volume received, total virus volume, virus volume as a percentage of mail).
- **Virus type for all domains** (virus name, volume sent, volume received, total volume). Note: this is an optional report table.
- **Virus type by domain** (virus name, volume sent, volume received, total volume). Note: this is an optional report table.

2. **Weekly detail report** – provides a detailed log for all client domains listing all virus activity.

- The table within this report lists: date & time email scanned, virus name, virus sent or received, client domain, recipient email address and sender email address.

5.3 Configuring AV reports

1. Select **ADMIN** from the top-left menu bar
2. Select Reports from the top-right menu

View reporting options by clicking on a service below.

Service	Reports	Recipients
Anti-Virus	Weekly Summary Report (Text) Weekly Detail Report (Text)	av-reports@messagelabs.com cwyss@ggs.ch colman@colman.com colman1@colman.com cocolman@colman.com colman2@colman.com
Anti-Spam	Weekly Summary Report (Text) Monthly Summary Report (Text)	admin@messagelabs.com testagain@update.com
Spam Quarantine	Weekly Summary Report (HTML)	test@messagelabs.be test@messagelabs.com
Image Control	Monthly Summary Report (Text)	admin1@messagelabs.com
Content Control	Monthly Summary Report (Text)	test2@messagelabs.com

Powered by MessageLabs

5.3.1 Reports Overview

3. You can now see an overview of the current Reporting settings. The **Reports** column lists currently subscribed to reports and the **Recipients** column the email addresses that will receive those reports.
4. Select **Anti-Virus** from the **Service** column
5. A pop-up window will appear containing the report settings for the AV service.

Anti-Virus Report Settings for Client

Recipients:	admin@eg.com monitor@eg.com	Edit Edit	Delete Delete
Click this button to add a new email address: <input type="button" value="Add"/>			
Reports:	Format	Elements	
Weekly Summary	<input type="text" value="Text"/>	<input type="button" value="Expand >>"/>	
Weekly Detail	<input type="text" value="CSV"/>	<input type="button" value="Expand >>"/>	
Monthly Summary	<input type="text" value="Text"/>	<input type="button" value="Expand >>"/>	
Click this button to update these settings:			<input type="button" value="Update"/>
Click this button to exit without changes:			<input type="button" value="Cancel"/>

5.3.2 AV Reports configuration

- Report recipients can be added, edited or removed within the **Recipients** row.
- The **Reports** row enables you to specify which reports to receive and also the format each report is delivered in. By default the **Format** drop down is set to **None** for each report type. Selecting either **Text** or **CSV** from the drop down list activates the report.
- Content of reports can be defined by clicking on the **Expand>>** text under the **Elements** column.

Anti-Virus Report Settings for Client

Recipients:	admin@eg.com monitor@eg.com	Edit Edit	Delete Delete
Click this button to add a new email address: <input type="button" value="Add"/>			
Reports:	Format	Elements	
Weekly Summary	<input type="text" value="Text"/>	<input type="button" value=" << Collapse"/>	
	Total for all domains	<input checked="" type="checkbox"/>	
	Total by domain	<input checked="" type="checkbox"/>	
	Virus type for all domains	<input checked="" type="checkbox"/>	
	Virus type by domain	<input type="checkbox"/>	
Weekly Detail	<input type="text" value="CSV"/>	<input type="button" value="Expand >>"/>	
Monthly Summary	<input type="text" value="Text"/>	<input type="button" value="Expand >>"/>	
Click this button to update these settings:			<input type="button" value="Update"/>
Click this button to exit without changes:			<input type="button" value="Cancel"/>

5.3.3 An expanded report element

- Certain report elements are mandatory (grayed out ticks) but others can be selected by ticking the relevant element box.

10. To update your report settings click on the **Update** button.