



Spamity™ Monitor Deployment Guide

1.0



Table of Contents

Table of Contents	2
About This Document	3
Intended Audience	4
Document Conventions.....	5
Document Version Number	5
Type Styles.....	5
Use of Square Brackets []	6
Use of Angle Brackets //	6
Related Resources	6
Making Comments on this document	6
Overview	7
Spamity™ Monitor	8
Required Software Components	10
Hardware Requirements.....	10
Implementation Scenarios	13
Installing Spamity Monitor	14
Spamity Monitor	14
Configuring Spamity Monitor	15
Introduction.....	15
Starting and Stopping Procedures	18

Chapter

1

About This Document

Welcome to *Spamity Monitor* Guide. This guide introduces you to Bitspan's *Spamity Monitor* application, which provides real-time inbound spam email identification, as well as optional historical reporting.

In brief, you will find the following information in this guide:

- an overview of the application, including details about its email data collection and optional reporting functionality
- deployment planning checklists for installation and configuration
- database preparation, sizing and scaling guidelines
- general system requirements

This guide is valid only for the 1.0 release(s) of the product.

Note: For versions of this guide created for other releases of this product, please visit the Bitspan Technical Support website, or request the Documentation Library CD, which you can order by e-mail from Bitspan Order Management at orderman@bitspan.com.

This chapter provides an overview of this guide, identifies the primary audience, introduces document conventions, and lists related reference information. It contains these Chapters:

- intended audience
- chapter summaries
- document conventions
- related resources
- making comments on this Document



Bitspan's Spamity Monitor helps you assess the functionality and efficiency of Bitspan's *Spamity* component by providing real-time and historical inbound mail identification capabilities. Alone or in parallel with other mail filtering technologies Bitspan's Spamity Monitor application includes:

- **Spamity™ Agent (BSAS Agent) (Windows Version)**
 - Core spam identification component
- **Spamity Web Reporter API**
 - API for an enterprise-level product that provides powerful report customization, data presentation, and report delivery functions.

Intended Audience

This guide is primarily intended for mail system administrators, system administrators, security administrators and assumes that you have a basic understanding of:

- email messaging concepts, processes, terminology, and applications.
- network design and operation.
- your own network configurations.



Document Conventions

This document uses some stylistic and typographical conventions with which you might want to familiarize yourself.

Document Version Number

A document version number appears at the bottom of the inside front cover of this guide. Version numbers change as new information is added to the guide.

Here is a sample version number:

Spamity_Monitor_01.04.14

You will need this number when you are talking with Bitspan Technical Support about the product.

Type Styles

Italic

In this document italics are used:

- When a term is being defined.

Example

- *A customary and usual practice* is one that is widely accepted and used within a particular industry or profession.
- For emphasis. For example, “Do *not* use this value for this option.”
- For variables, for example, $x + 1 = 7$ where x stands for . . .

Monospace

A monospace font, which is shown in the following examples, is used for:

- All programming identifiers and GUI elements, where applicable. This convention includes the *names* of directories, files, folders, paths, scripts, dialog boxes, options, fields, text and list boxes, all buttons including radio buttons, check boxes, commands, tabs, SMTP events, and error messages; the values of options; logical arguments and command syntax; and code samples.



- For any text the user must manually enter during a configuration or installation procedure:

Example

Enter password at the prompt.

Use of Square Brackets []

In any logical arguments, commands, and programming syntax presented in this document, square brackets are used to indicate that a particular parametric value is optional. That is, the value is not required to resolve a command, argument, or programming syntax. The customer/user decides whether to supply a value and what that value is.

Use of Angle Brackets //

Angle brackets are used to indicate that a value in a logical argument, command, or programming syntax is required, but that the user must supply the data for the value.

Related Resources

Consult these additional resources as necessary:

The Release Notes and Product Advisories for this product, which are available on the Bitspan Technical Support website at <http://bitspan.com/support>.

Making Comments on this document

If you like or dislike anything about this document, please feel free to email your comments to techpubs@bitspan.com.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the information in this document only and to the way in which the information is presented. Speak to Bitspan technical support if you have suggestions about the product itself. When you send us comments, you grant Bitspan a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.



Chapter

2

Overview

To provide visibility into its message identification capabilities, including accuracy and scalability, Bitspan has created several tools to monitor and report on its message identification facility. These include the applications, *Spamity Monitor* and *Spamity Web Reporter*.

Spamity Monitor runs on a Windows platform and analyzes inbound email packets received on the SMTP port, which can be local or remote, for presence of spam by creating a fingerprint and doing a cross match against its spam fingerprint definition library.

Additionally, if enabled, *Spamity Monitor* can report its findings to a centralized ODBC database where the data can be visualized using readymade canned reports - using Bitspan's *Spamity Web Reporter* web-based application. Together, *Spamity Monitor* and *Spamity Web Reporter* allow for fast assessment of Bitspan's email identification technologies with minimal impact (if any) to existing email delivery environments.

All the identification processes take place within your network.

IMPORTANT NOTE

Neither the Spamity Monitor nor the BS-Reporter components send any of your email, in whole or in part, outside your own network.

In addition, the results are *NOT* shared with any server outside your network. This ensures testing without compromising network security.

Chapter 3 Spamity™ Monitor

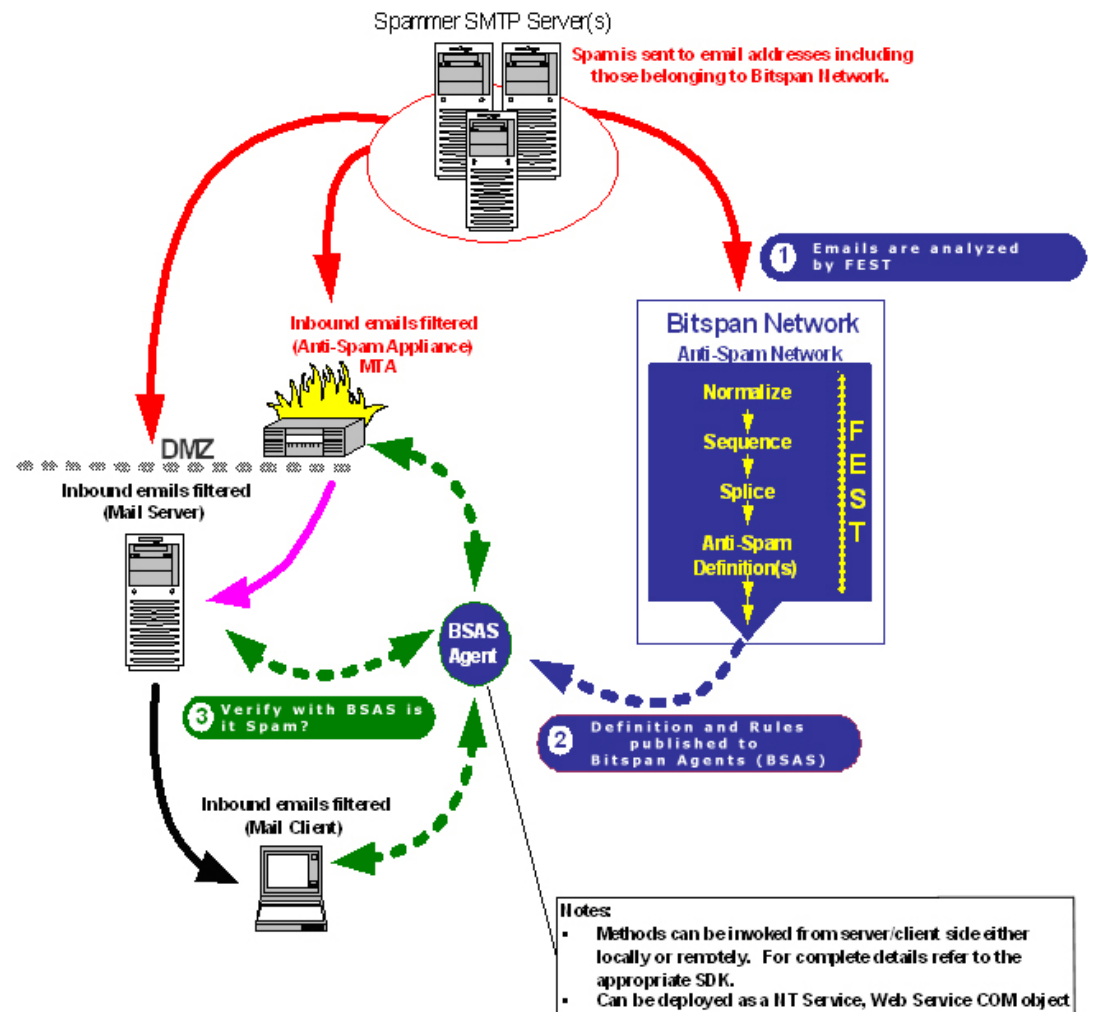
3

Bitspan’s *Spamity™ Monitor* is a Windows-based application that utilizes Bitspan’s unique email identification component to assess Spamity™ of inbound emails and thus identify spam email from a pool of heterogeneous emails (spam and non-spam). Spamity™ is the degree of spam-ness, or likelihood that an email is in fact spam.

How it works?

When the application is started, an instance of Spamity Agent (BSAS Agent) is started. Diagram 1 depicts how Spamity Agent (BSAS Agent) receives spam definitions from the Bitspan centralized server.

Diagram 1: Spamity Component (BSAS Agent)



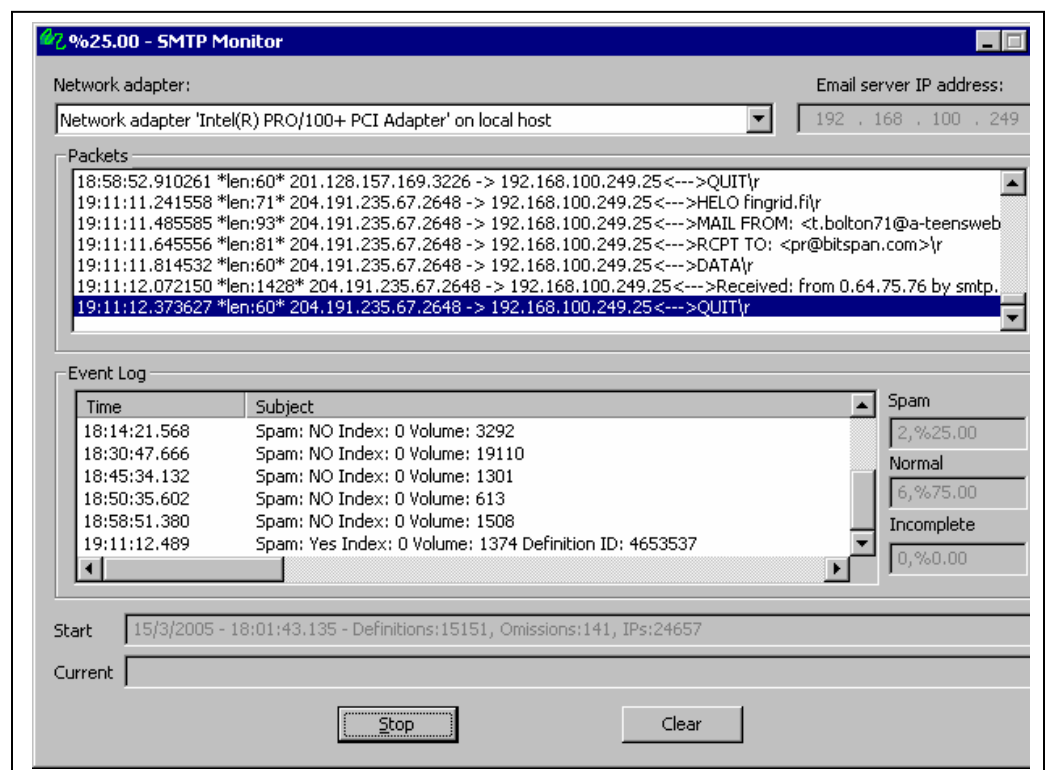


Once the Spamity Agent component (BSAS Agent) is started, the Spamity Monitor application can listen-in (eavesdrop) on a local or remote port running any one of the following services:

- Mail Services (SMTP)
- MTA (Message Transfer Agent)
- SMTP-Relay
- Firewall Services
- Third Party Email application

When it receives an inbound email, it calls a function available on the Spamity Agent component (BSAS Agent) and passes the email information to the Spamity Agent component. The Spamity Agent **LOCALLY** assesses the spamity by looking through its indexed spam fingerprint library and then reports the result back to the Spamity Monitor application. The match **MUST** be 100%. Otherwise it will not be considered a spam. The Spamity Agent component (BSAS Agent) runs independently from the Spamity application, as it constantly receives spam updates from the Bitspan server.

Email packets arriving at the designated port are assessed for Spamity. The running results are shown on the application's graphical user interface (GUI) – see below:





By itself, Spamity Monitor reports the count and percentage of emails it has processed and identified as spam, since start up. This amount of detail may be good enough for some implementations. However, to get the best type of reporting, Bitspan recommends you implement *Spamity Web Reporter*. Spamity Monitor can be configured to log its findings to a centralized ODBC-compliant database for creation of more complex reports using the Spamity Web Reporter application component. For more information, please refer to Bitspan's Spamity™ Web Reporter 1.0 Guide.

Required Software Components

The Spamity™ Monitor can run on Windows 2000 or Windows XP.

- Windows 2000 or XP with latest service packs and updates

Optional Software Components

By itself Spamity Monitor's graphical user interface (GUI) reports the count and percentage of email it has processed and identified as spam since start up. Optionally, Spamity Monitor can be configured to log its findings to a centralized ODBC-compliant database for creation of more complex reports using the Spamity Web Reporter component.

Spamity Monitor can log its findings in any ODBC-compliant database. These include:

ODBC compliant database:

- Microsoft SQL Server 2000 or MSDE
- Microsoft Access 2000
- Oracle 9.xi
- MySQL

Hardware Requirements

Hardware architecture will naturally vary depending on your needs. If ODBC logging is enabled, then enough space must be allocated on the server where the Spamity Monitor database is maintained. This database will store captured email as well as additional Spamity Monitor related data.



Option 1: No ODBC Logging:

- Minimum Hardware Requirement

Peak Email Count/hour	CPU/Memory Requirement
< 999	Pentium III with 512 MB RAM
>1000-9999	Pentium IV with 1.0 GB RAM

- Network connectivity
 - a. Internet Access. The Spamity Monitor component uses definitions from the central definition provider. To function, it must be able to download these definitions. To do so, it **must have access to port 80 of Bitspan's definition server at <http://spamity.bitspan.net>**
 - b. Ability capture TCP packets on the port (local or remote), which receives inbound email. To assure this, please choose the option that is best:
 - i. No network configuration change is required, if:
 1. Spamity Monitor application is running on the **SAME** host, where email messages are being received (i.e. Mail Server, MTA, etc.) without any modification of the MIME header.
 2. *or*, Spamity Monitor application is running on a **DIFFFERENT** host, but this host and the host where email messages arrive (SMTP Server, MTA, etc.), are connected directly using a common *hub* (**not switch**).
 - ii. If the host system where the Bitspan Spamity Monitor application is running and the server where email messages arrive (SMTP Server, etc.)
 1. reside on different network segments, or
 2. separated by routers, or
 3. connect to a switch

then you *must* configure the switch and/or the network device to send a copy of the incoming email packets to a specific port on the host running the Spamity Monitor application. In such instances, you must configure the Spamity Monitor application to listen to a local port, where the packets are being received.



Option 2: with ODBC Logging Enabled

- Same as Option 1, *plus*:
- Database storage space
Approximately 1 MB for each 1000 Emails/Day



Chapter

4

Implementation Scenarios

Scenario 1:

ABC Company is running Microsoft Exchange 2000 mail server and would like to assess the effectiveness of Bitspan's spam email identification technology.

Option 1: Spamity Monitor running on Mail Server host

1. Install the Spamity Monitor application on the machine running Exchange 2000 Server services.
2. Configure Spamity Monitor application to listen for email on port 25 (SMTP port) – See configuration file for details.
3. Start Spamity Monitor application

Option 2: Mail Server and Spamity Monitor on same HUB

1. Install Spamity Monitor on a separate system (Spamity Monitor Host - SM)
2. Connect the Exchange Server host and SM host to the same hub.
3. Configure Spamity Monitor application to listen on port 25 (SMTP port) of the Exchange Server's IP address -- Refer to *Chapter 6* for details.
4. Start Spamity Monitor Application.

Option 3: Switch between Mail Server and Spamity Monitor Application

1. Install Spamity Monitor on a separate system (*Spamity Monitor Host - SM*)
2. Connect the Exchange Server host and SM host to the same switch.
3. Configure switch to send a copy of packets destined to Exchange Server port 25 to SM host port 25. Spamity Monitor application will "listen" on port 25 of the SM's IP address -- Refer to *Chapter 6* for details.
4. Start Spamity Monitor Application.



Chapter

5

Installing Spamity Monitor

The installation package, whether on CD or from the FTP site, contains a setup file for Spamity Monitor. The file is located in the folder:

D:\Spamity\Monitor

Spamity Monitor

Installing Spamity Monitor on Windows 2000 or later

1. locate and double-click on “setup.exe”
2. follow instructions to complete the installation

As soon as the installation process is finished, a message appears announcing that the installation was successful. The process creates a directory containing the Spamity Monitor application with the name you specify for the Spamity Web Reporter folder during the installation.

Chapter

6

Configuring Spamity Monitor

Introduction

The Spamity Monitor is configured using the `monitor.cfg` file located on the installation path.

A typical `monitor.cfg` file looks like the following:

```
[general]
server_ip = 192.168.100.123

[database]
db_connect = true
db_server = DBServer
db_catalog = Bitspan
db_username = sa
db_password = password

[logging]
log_level = 0
log_file = log.txt
```

In order for the Spamity Monitor application to perform correctly, the configuration file must be available and it must contain valid information.



Each of the configuration entries is briefly discussed here:

Section

General

Option	Required	Valid Values
server_ip	yes	IP address of the server to be monitored
server_port	yes	Valid port number on server_ip

Database

Option	Required	Valid Values
db_connect	No	True, False. if you would like the application to report to database, otherwise it must be false. Please note that the values are case sensitive (e.g. 'true' is a valid value, where 'TRUE' is not)
db_server	No*	Database server name
db_catalog	No*	Database name (default: Bitspan) - <i>Not required for Oracle.</i>
db_username	No*	Username for accessing the DB
db_password	No*	Password for accessing the DB

* = *required only when db_connect = true*



Logging

Option	Required	Valid Values
<i>log_level</i>	yes	0 = log nothing, 1= information & warning and errors, 2= warnings and errors, 3= errors only
<i>log_file</i>	yes	Log file name



Chapter

7

Starting and Stopping Procedures

This chapter provides instructions for starting and stopping reporting components.

Pre-start Information

Before starting the application, it must be installed and properly configured.

Starting Spam Monitor

To start Spamily Monitor:

Select *Start > Programs > Bitspan > Spamily Monitor*

Note:

This is the default location. If you installed the software at a different location, navigate to the appropriate location to start Spamily Monitor.

Stopping Spam Monitor

To stop Spamily Monitor:

Just close the Spam Monitor application from the application GUI.