



Spamity™ Web Reporter

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™ Reporter	8
Required Software Components	8
Hardware Requirements	8
Installing Spamity™ Web Reporter	9
Configuring Spamity™ Web Reporter	10
Introduction	10
Testing Spamity™ Web Reporter	12

Chapter

1

About This Document

Welcome to the *Spamity Web Reporter* Guide. This guide introduces you to Bitspan's *Spamity Web Reporter* application, which provides historical inbound email reporting in conjunction with Bitspan's *Spamity Monitor* application.

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

- an overview of the application
- deployment planning checklists for installation and configuration
- database preparations and sizing and scaling guidelines
- general system requirements

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

Note: For releases 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 Web Reporter helps you assess the functionality and efficiency of Bitspan's *Spamity Monitor* by providing detailed historical reports on its inbound mail identification assessments.

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 this guide.

Here is a sample version number:

Spamity_Web_Reporter_01.04.14

You will need this number when you are talking with Bitspan Technical Support about this 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 applications, *Spamity Monitor* (for more information, please refer to *Spamity Monitor Guide*) and *Spamity Web Reporter*.

Spamity Web Reporter uses a centralized ODBC database, where the data from the *Spamity Monitor* is recorded. Using this database and a series of canned reports – the *Spamity Web Reporter* allows for the generation of quick reports on the state and efficacy of Bitspan’s email identification technologies.

IMPORTANT NOTE

The *Spamity Web Reporter* component does NOT sent any of your emails, in whole nor in part, to a host outside your network.

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



Chapter 3 Spamity™ Reporter

3

Bitspan's *Spamity™ Web Reporter* is a web-based application that utilizes the Spamity database to create a range of reports. For details about the reports, please refer to the "*Spamity Web Reporter – User's Guide*".

How it works?

The Spamity Monitor writes the results of its analysis into a centralized database. The statistics reflect emails received from any one of the following services:

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

Spamity Reporter reads the data from the database and creates custom reports using its predefined report templates.

Required Software Components

The Spamity™ Web Reporter can run on Windows 2000 or Windows XP.

- Windows 2000 or Windows XP with latest service packs and updates
- Web server (Microsoft Internet Information Server (IIS)) with latest services packs and updates.
- access to Spamity™ Web Reporter database server and database instance

Hardware Requirements

- 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 access to Spamity Web Reporter database



Chapter

4

Installing Spamity™ Web Reporter

Instructions for installing on Windows 2000 or later

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

[installation media drive:]\Spamity\Reporter

2. Locate and double-click on “setup.exe”.

Follow the wizard instructions to complete the installation.

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

3. Proceed to Chapter 5. Configuring Spamity Web Reporter

Chapter

5

Configuring Spamity™ Web Reporter

Introduction

Spamity Reporter is configured using the “reporter.cfg” file located on the installation path.

A typical reporter.cfg file looks like the following:

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

In order for the Spamity Web Reporter to work correctly, the configuration file must be available and it must contain valid information.



Each of the configuration entries is briefly discussed here:

Section

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)
<i>db_server</i>	No*	Database server name
<i>db_catalog</i>	No*	Database name (default: Bitspan) - <i>Not required for Oracle.</i>
<i>db_username</i>	No*	Username for accessing the DB
<i>db_password</i>	No*	Password for accessing the DB

* = *required only when db_connect = true*



Chapter

6

Testing Spamity™ Web Reporter

To verify that the Spamity Web Reporter is properly configured go to:

“[http://\[hostname\]/Bitspan/WebReporter/Test.asp](http://[hostname]/Bitspan/WebReporter/Test.asp)”