VIPRE Email Security

Server Edition

User Guide

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

Document Version: VESS-UG-10.3.1

Last updated: Friday, September 3, 2021

Contents

1 Introduction 6

1.1 What is VIPRE Email Security 6

Components 6

1.2 About VIPRE Email Security - Server Edition 8

1.3 About this Guide 8

1.4 Terms and conventions 8

1.5 Technical Support 9

1.6 System Requirements 9

1.7 Features 10

2 Installing VIPRE Email Security 12

2.1 Before you Install VIPRE 13

2.2 Installing VIPRE Email Security 13

2.3 The Welcome Wizard 14

3 Managing System Settings 23

3.1 Working with Domains 24

Active Directory 24

Domains 24

VIPRE and Active Directory Domains 24

Antispoofing 24

3.2 Replicating Server Configuration Changes 29

3.3 Configuring Databases 30

3.4 Working with Agent Registration and Unprocessed Email Settings 31

Access 31

Unprocessed Folder Notifications 31

Unprocessed Email Settings 32

3.5 Setting System Notifications and Logging Parameters 33

System Logging 33

3.6 Managing Licensing and Updates 34

NTLM Authentication 34

3.7 Managing Quarantine and Reporting Security 36

3.8 Managing Archives Settings 40

4 Working with Policies and Recipients 41

4.1 Policies and Recipients 42

4.2 Working with Recipients 42

4.3 Managing Global Antispam Activity 43

Antispam Engine settings 44

X-Headers 45

Regular Expressions 46

Ordinary Characters 46

Hex Characters 46

Tabs 46

Page Breaks 46

Line Breaks 46

Special Characters 46
Wildcard Character 46
Repetition Operators 46
Interval Operator 47
Alternation Operator 47
Class Expressions 47
Simple Characters 47
Negated Class Expressions 47
Range Expressions 47
Character Class Operators 47
Expression Anchoring 47
Tagged Expressions 48
Connection Filtering 50
How Connection Filtering helps You 51
Allowed IPs 51
4.4 Managing Antispam Policies 57
4.5 Managing Global Antivirus Activity 65
The Antivirus Plug-in 65
4.6 Managing Global Attachment Filtering 69
The Attachment Filter Plug-in 69
Global Attachment Filter Settings and Rules 70
Policy Settings and Rules 70
S.M.A.R.T. Detection 70
Imbedded Email Attachments 70
Notifications 70
X-Headers 71
4.7 Managing Attachment Filtering Policies 74
4.8 Managing Global Disclaimer Settings 78
Tokens 79
4.9 Managing Disclaimer Policies 82
4.10 Managing the Quarantine Store 83
5 Managing Reports 86
5.1 About Reporting 86
5.2 About Message Tracking 88
Search Query 88
Results 88
Expanding Results 89
Filtering Results 89
6 Appendix 1 - Message Tracking details 92
Glossary 103
Contacting VIPRE Support or Sales 111

1 Introduction

VIPRE is a policy-based messaging security application. As a System Administrator, you can use VIPRE to enforce email security policies that protect your network against spam, phishing, viruses and other messaging security threats.

This chapter covers the following topics:

1.1 What is VIPRE Email Security 6

1.2 About VIPRE Email Security - Server Edition 8

1.3 About this Guide 8

1.4 Terms and conventions 8

1.5 Technical Support 9

1.6 System Requirements 9

1.7 Features 10

1.1 What is VIPRE Email Security

VIPRE is a policy-based messaging security framework solution for your corporate email security management.

Components

VIPRE includes nine components that you install on your network:

Component	File	Description
Plug-in Manager Service	NinjaPimSvc.exe	Service that is responsible for invoking the VIPRE Plug-ins for filtering at the SMTP Level.
Updates Service	NinjaUpdSvc.exe	Controls updates from VIPRE to your company server
Monitoring Service	NinjaWatchSvc.exe	Service that monitors the health of the VIPRE system.
Remoting Service	NinjaRemSvc.exe	Service that enables remote connection and configuration of settings
Quarantine Viewer	Ninja.Tools.QuarantineViewer.exe	Application that enables local and remote users access to the Quarantine Repository.

Report Viewer	Ninja.Tools.ReportViewer.exe	Application that enables local and remote users access to the reports generated by VIPRE
Welcome Wizard	Ninja.WelcomeWizard.exe	Wizard that setups all settings prior to first use.

1.2 About VIPRE Email Security - Server Edition

VIPRE Email Security - Server Edition uses layered approach to inspect messages, clean your network, and manage your email security. It uses multiple scanning engines to detect spam and viruses, while integrating other messaging security rules. VIPRE secures all messages at the server not at the end-user’s computer.

VIPRE contains three main sections:

- **System Settings** - Use the system Settings to manage and configure the Active Directory domains and Antispoofing used in VIPRE, replicate configuration changes to other servers, configure reporting and storage databases, register Transport agents, manage unprocessed email settings, set email and messenger alerts, configure logging parameters, and manage licensing and updates.
- **Policies, Antivirus, and Quarantines** - Use the Policies, Antivirus, and Quarantine section to customize actions for recipients, configure global antispam, antivirus, and attachment filter activity, manage antispam and attachment filter policies, and manage quarantined viruses and attachments intended for recipients.
- **Reports** - Use the reports section to customize, preview, and print reports. The Message Tracking feature help clarify why VIPRE has allowed or blocked each message. Admins can easily review how and why messages were handled, in a single location within the application.

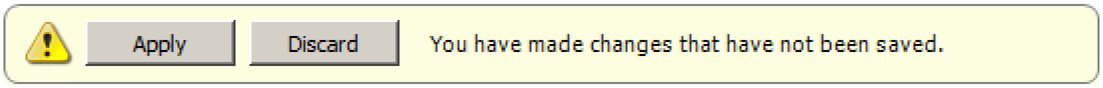
Also, take a look in the glossary for more information about concepts and terms used in this guide and in VIPRE.

1.3 About this Guide

This guide shows you how to install, set up, and use VIPRE so you can effectively protect your network. It assumes that you have detailed knowledge of the Windows operating systems used in your company.

1.4 Terms and conventions

VIPRE uses most standard windows toolbar, menu, and list expansion conventions. However, after making modifications in any area, a confirmation prompt appears at the top of the open tab.



You have made changes that have not been saved.

Screenshot 1: Confirm Change Dialog Box

The following table contains a description of formatting conventions used in this manual:

Table 1: Terms and conventions used in this manual

Term	Description
ℹ	Additional information and references essential for the operation of VIPRE.

Term	Description
❗	Important notifications and cautions regarding potential issues.
>	Step by step navigational instructions to access a specific function.
Bold text	Selectable items such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and file names.

1.5 Technical Support

If the information in this guide does not resolve a situation or answer a question you might have, or if you have a question about updating your version of VIPRE, please contact VIPRE Technical Support using the information below:

Telephone (USA) – 877-757-4094

Web support form – https://www.vipre.com/contact/

Website URL – https://www.vipre.com/products/business-protection/email/

1.6 System Requirements

Use the following system requirements to run VIPRE effectively:

Microsoft Exchange:

- Exchange 2016
- Exchange 2013
- Exchange 2010
- Exchange 2007

Other requirements:

- **CPU**: 2GHz or higher with multiple cores
- **RAM**: At least 1GB more than what is allocated for running Exchange
- .NET Framework 3.5
- **Browser**: Internet Explorer 6.0 or higher (for disclaimer editing)
- **Additional Space**: 400MB for installation (Quarantine store requires more space)
- **File format**: Disk partitions must be formatted for the NTFS file system. This requirement applies to:
  - System partition
  - Partition storing messaging suite binaries
  - Partitions containing quarantine store files
  - Partitions containing database files

ℹ VIPRE supports any operating system that the above versions of Exchange will install on.

ℹ The Exchange Server is not required if you are installing only the report and quarantine viewers.

1.7 Features

VIPRE includes the following features:

Policy-based plug-in management

Create customizable policies using VIPRE's integrated plug-in management. VIPRE supports plug-ins for antispam, antivirus, and attachment filtering.

You can also create custom policies for groups of users or a single user by pulling the information from Active Directory. Set the parameters based on user and/or organizational requirements. Simply associate all users with VIPRE's default plug-in polices or create separate policy templates for different groups or individuals.

Easily deploy in Exchange environments

Install, configure, and manage all of your messaging security from a centralized location. VIPRE also integrates with Microsoft Exchange to provide antispam, antivirus, and file attachment protection.

Server-based enterprise antispam filtering

VIPRE uses multiple detection capabilities including RBL technology and the Antispam Engine. VIPRE can be configured to delete, quarantine, add Subject line identification, or send to a custom folder in the end user's Exchange mailbox. Custom rules capabilities provide the ability to control spam and any other type of email. You can supplement the spam detection engine with a variety of rules created on a number of email message properties (such as body, sender IP, header, or subject).

Greylisting

Greylisting is a feature that will help verify that a sending mail server is a real mail server instead of a spammer. When an email is received from a domain that has not recently sent an email to your domain, the Greylisting module will request a resend from the sending mail server.

SMTP rules dictate that all mail servers are required to resend the message (the default for Microsoft Exchange is 5 minutes). Spammers do not use mail servers, and will not resend the message. Legitimate mail servers will resend the message.

Greylisting will prevent many spam emails from being downloaded by the server, reducing the amount of emails that need to be processed by VIPRE.

Support for Sender Policy Framework (SPF)

Use the SPF to test whether a specific email originated from its claimed domain. VIPRE allows users to participate in SPF, helping reduce the risk of phishing and fraudulent email.

Aggressive virus detection and elimination

VIPRE uses its premium antivirus engine to scan inbound and outbound email. You can set scanning parameters to quarantine pieces of an email, essentially breaking apart the email message and only quarantining infected attachments instead of stripping all attachments.

Email content inspection and attachment filtering

Use VIPRE to configure inspection and filtering on a per-policy basis. VIPRE's Suspicious Mail Attachment Removal Technology (S.M.A.R.T) filter scans the header of a file to verify that an attachment is what it says it is and has not just been renamed. You can also set rules based on users and file types that enable you to quarantine potentially harmful content or attachments by files extension including .doc, .exe, .dll, .pdf, visual basic scripts, and more.

Configurable reporting options for all plug-ins

VIPRE delivers system reporting for all plug-ins with a set of pre-defined reports with the ability to generate custom reports based on individual needs. The database-driven reporting engine can generate reports with information at the system, group, and/or user level. You can choose reporting options to show the number of inbound mail messages scanned, number of spam deleted or marked, number of viruses intercepted, number of filters triggered, percentage of viruses by name, and more.

2 Installing VIPRE Email Security

Now that you have been introduced to VIPRE, you are ready to install it and start protecting your email. You should have already downloaded a purchased or evaluation version of VIPRE.

This chapter covers the following topics:

2.1 Before you Install VIPRE 13

2.2 Installing VIPRE Email Security 13

2.3 The Welcome Wizard 14

2.1 Before you Install VIPRE

Make sure your network meets the proper requirements before starting the installation and setup:

- Gather necessary information for the server installation
- Install VIPRE
- Check for latest news and updates and set initial parameters.

2.2 Installing VIPRE Email Security

The installation process installs all of the components needed to run the application. You must be logged in with Administrative rights to install VIPRE.

To install VIPRE:

1. Close all other Windows programs that you have open on your computer.
   a. Open **Windows Explorer**; then, navigate to the location where you saved the *setup.exe* file on your computer;
   b. Double-click *setup.exe* to open the InstallShield Wizard.
2. Click **Next**. The **Installation Requirements** window opens.
3. If your system meets the requirements listed in the window, select the **Yes, my system meets the Installation Requirements** check box. If your system does not meet the requirements, cancel the installation and upgrade your system to meet the required parameters.
4. Click **Next**. The License Agreement window opens.
5. Make a selection:

   To accept the license agreement:

   a. Select **I accept the terms in the license agreement**
   b. Click **Next**. The **Customer Setup** window opens. Go to step 6.

   To decline the license agreement:

   a. Select **I do not accept the terms in the license agreement**
   b. Click **Cancel**. The wizard closes.
6. Make a selection:

   To accept the default setup (recommended):

   - Click **Next**. The Destination Folders window opens.

   To disable or change the setup of the VIPRE, Report Viewer, or Quarantine Viewer:

   a. Click the arrow next to the item
   b. Select the features to be installed or disabled
   c. Click **Next**. The Destination Folders window opens.
7. Make a selection:

To use the current destination folders:

- Click **Next**. A **disclaimer** dialog box opens. Proceed to Step 8.

To change the destination folder for the application and/or temporary files:

a. Click **Change**

b. Select a new folder from the explorer window

c. Click **OK**. You return to the Destination Folders window.

d. Click **Next**. A disclaimer dialog box opens.

8. This dialog box informs you that while VIPRE scans messages, it will copy them to the temporary directory specified in the box below the warning text. However, if an Antivirus product scans this directory, it could prevent VIPRE from working properly.

> ❗ You must prevent antivirus products from scanning the temporary directory specified in this disclaimer. Refer to your antivirus software documentation for further instruction.

9. Select the **I have read this warning regarding file system AV scanning** check box, and then click **OK**. You are returned to the Destination Folders window.
10. Click **Next** on the Destination Folders window. The **Ready to Install the Program** window opens.
11. Click **Install**. VIPRE installs on your computer. After the installation is complete, the **InstallShield Wizard Completed** window opens.
12. Make a selection:

To automatically launch the Welcome Wizard after you click Finish:

- Select the **Launch the Welcome Wizard** check box.

To automatically launch the readme file after you click Finish:

- Select the **Show the readme file** check box.

13. Click **Finish**. The installation is completed and launches the **Welcome Wizard** or the **readme** file, if you selected them to be displayed.

2.3 The Welcome Wizard

The Welcome Wizard helps you set up a few basic parameters before you start using VIPRE. Using the Welcome Wizard is optional, since you can make these same settings from the VIPRE Console.

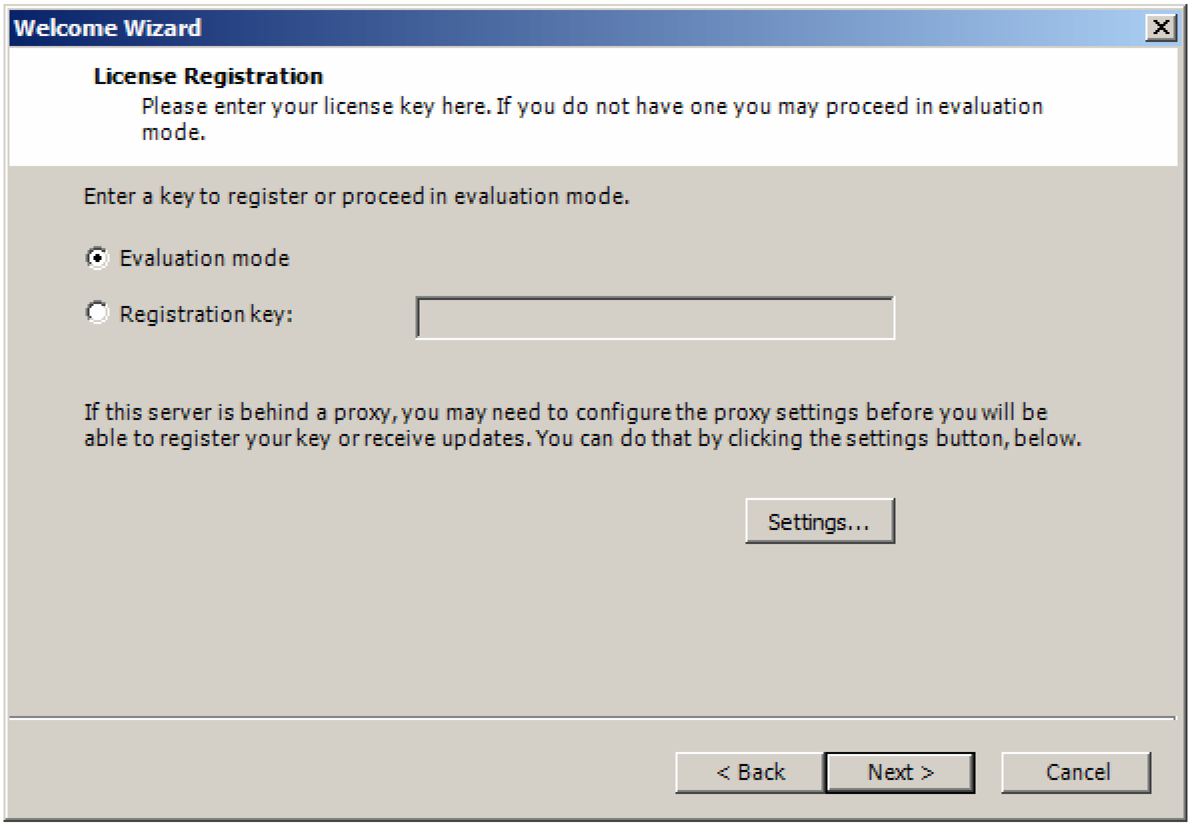
To setup basic parameters in VIPRE using the Welcome Wizard:

1. If you selected to launch the Welcome Wizard after installation, the **Welcome Wizard** window opens automatically.

- Click **Next**. The **License Registration** window opens.

-or-

1. If you are opening the Welcome Wizard at a later time:
    a. Click **Start** > **VIPRE** > **Welcome Wizard**
    b. Click **Next**. The **License Registration** window opens.



Welcome Wizard

License Registration

Please enter your license key here. If you do not have one you may proceed in evaluation mode.

Enter a key to register or proceed in evaluation mode.

● Evaluation mode

○ Registration key:

If this server is behind a proxy, you may need to configure the proxy settings before you will be able to register your key or receive updates. You can do that by clicking the settings button, below.

Screenshot 2: License Registration

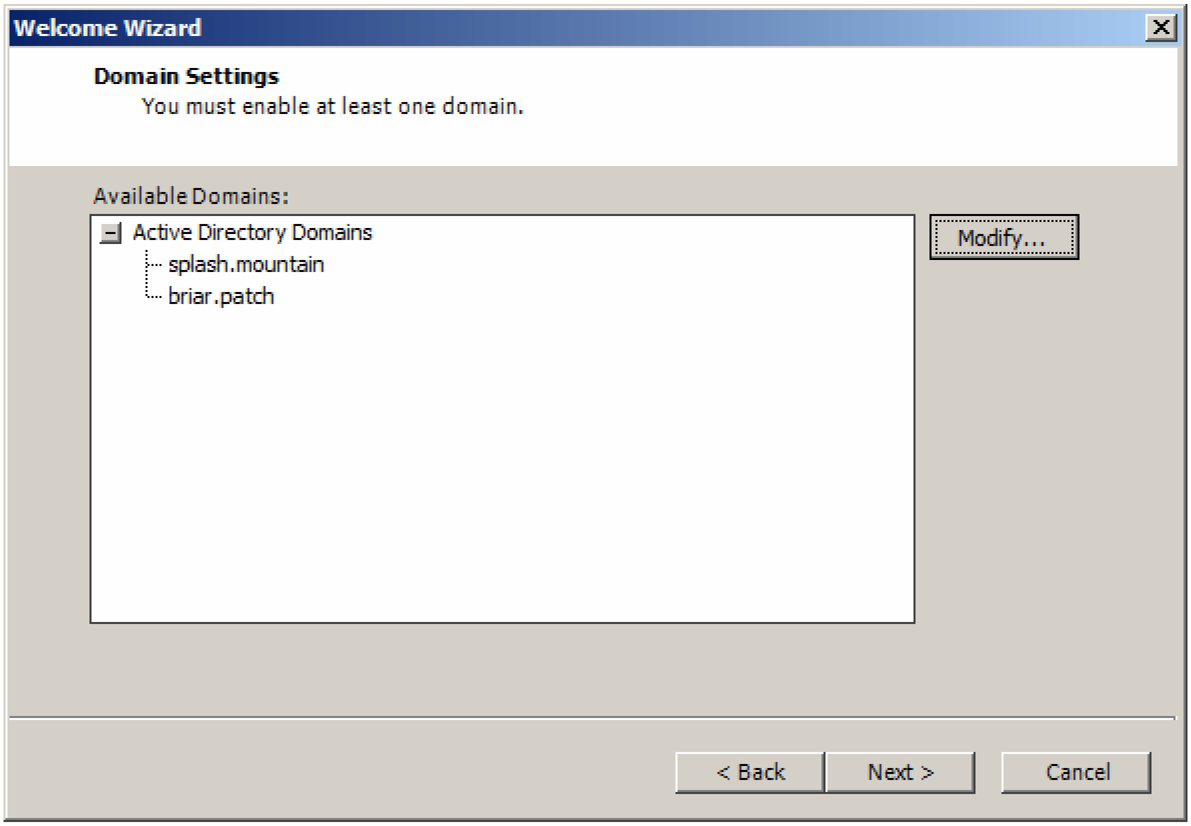
2. Make a selection:

If you are using VIPRE in evaluation mode:

a. Select **Evaluation Mode**
b. Click **Next**. The **Domain Settings** window opens.

If you have a registration key for VIPRE:

a. Select **Registration Key**
b. Type the key in the field below
c. Click **Next**. The **Domain Settings** window opens.



Domain Settings

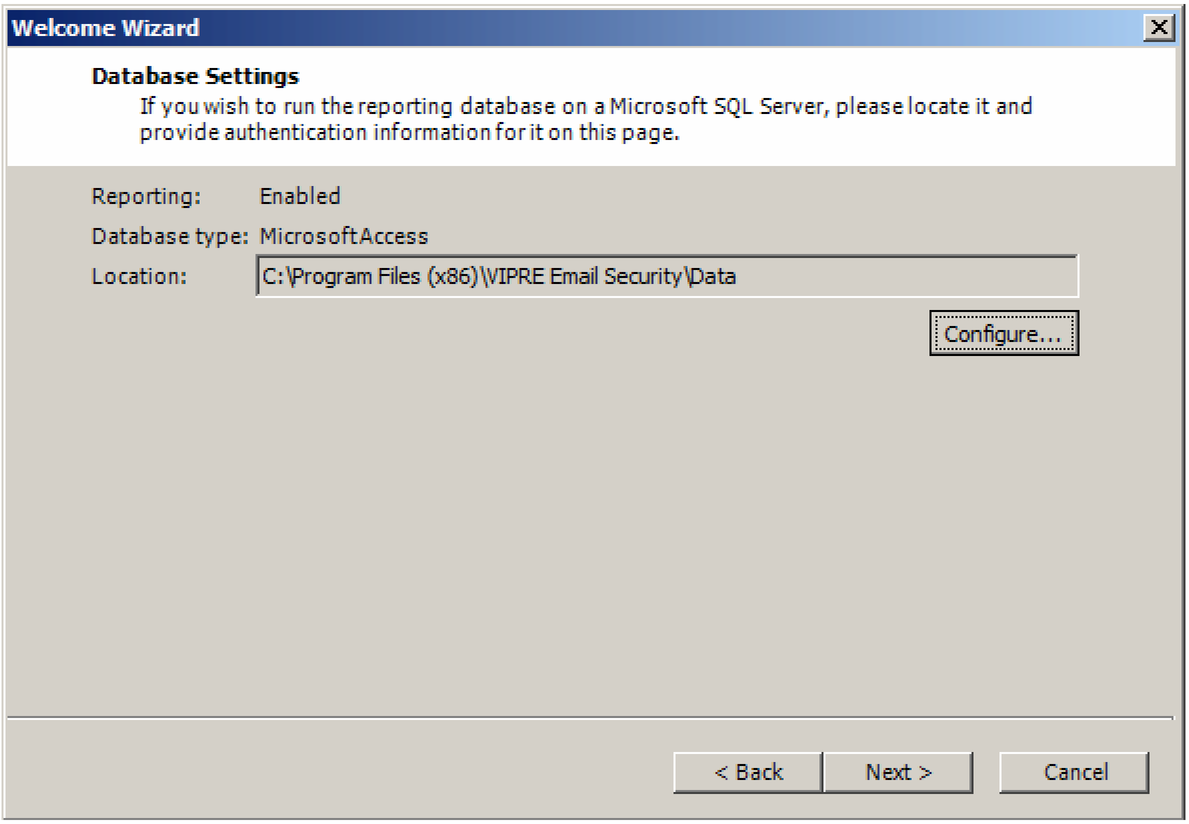
You must enable at least one domain.

Available Domains:

- Active Directory Domains
  - splash.mountain
  - briar.patch

Screenshot 3: Domain Settings

3. To modify the settings for the listed domains, click **Modify**; then, add or remove domains on the Active Directory Domains window. We recommend that you use the default domain.
4. Click **Next**. The **Database Settings** window opens.



Database Settings

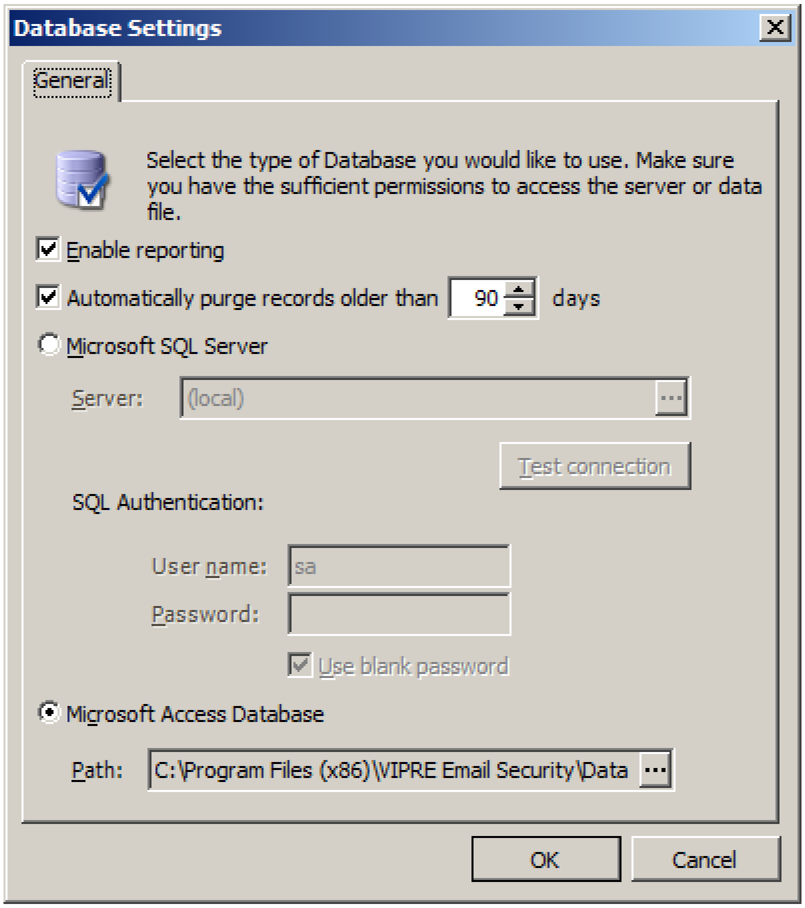
If you wish to run the reporting database on a Microsoft SQL Server, please locate it and provide authentication information for it on this page.

Reporting: Enabled

Database type: MicrosoftAccess

Location: C:\Program Files (x86)\VIPRE Email Security\Data

5. Click **Configure** to configure the database settings. The **Database Settings** dialog box opens.



Database Settings

General

Select the type of Database you would like to use. Make sure you have the sufficient permissions to access the server or data file.

☑ Enable reporting

☑ Automatically purge records older than 90 days

○ Microsoft SQL Server

Server: (local)

Test connection

SQL Authentication:

User name: sa

Password:

☑ Use blank password

● Microsoft Access Database

Path: C:\Program Files (x86)\VIPRE Email Security\Data

OK Cancel

Screenshot 4: Database Settings dialog box

6. Make a selection:

To enable reporting on an SQL server:

a. Select the **Enable reporting** check box
b. Select the **Microsoft SQL Server** or **Microsoft Access database** in which to store the Reporting database

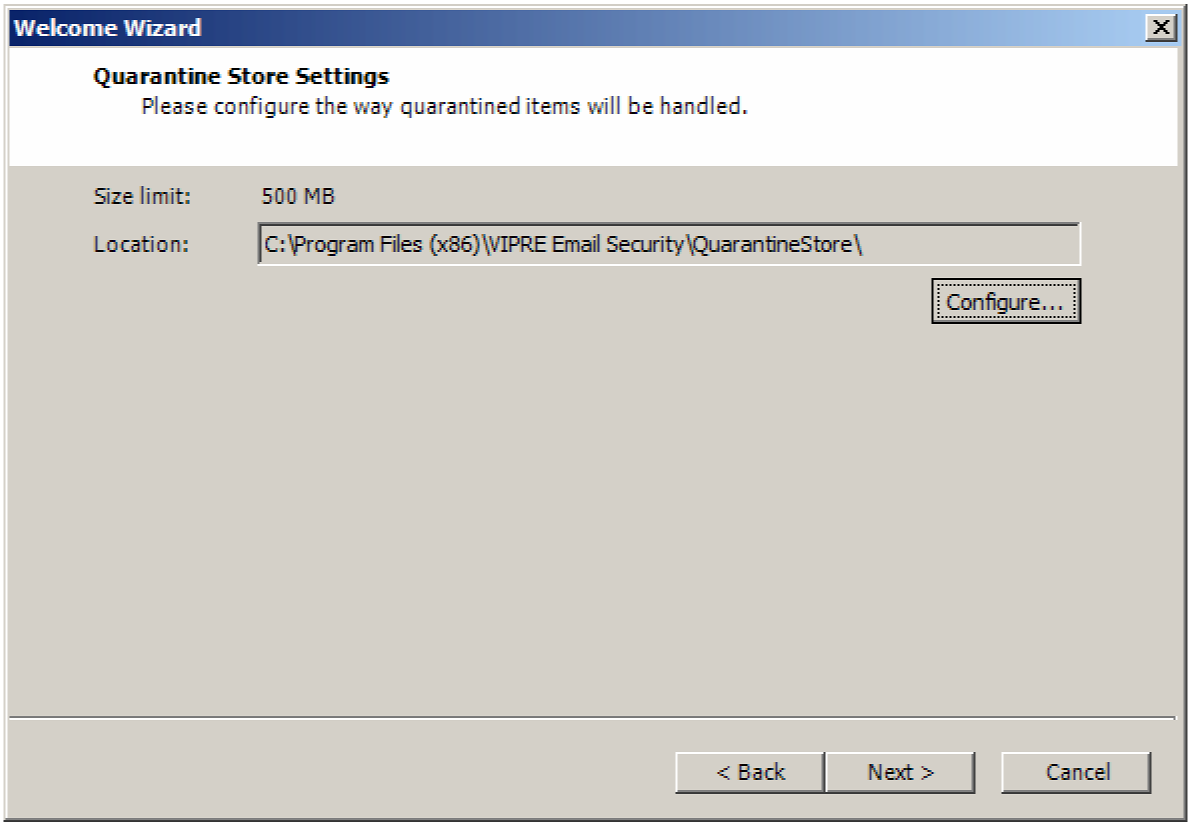
To run the Reporting Database on a Microsoft SQL Server:

a. Select **Microsoft SQL Server**
b. Add the Server info
c. Enter your SQL user name and password.

To run the Reporting Database on a Microsoft Access Database:

a. Select **Microsoft Access Database**
b. Type or select the path of the database

7. Click **OK**; then click **Next**. The **Quarantine Store Settings** window opens.

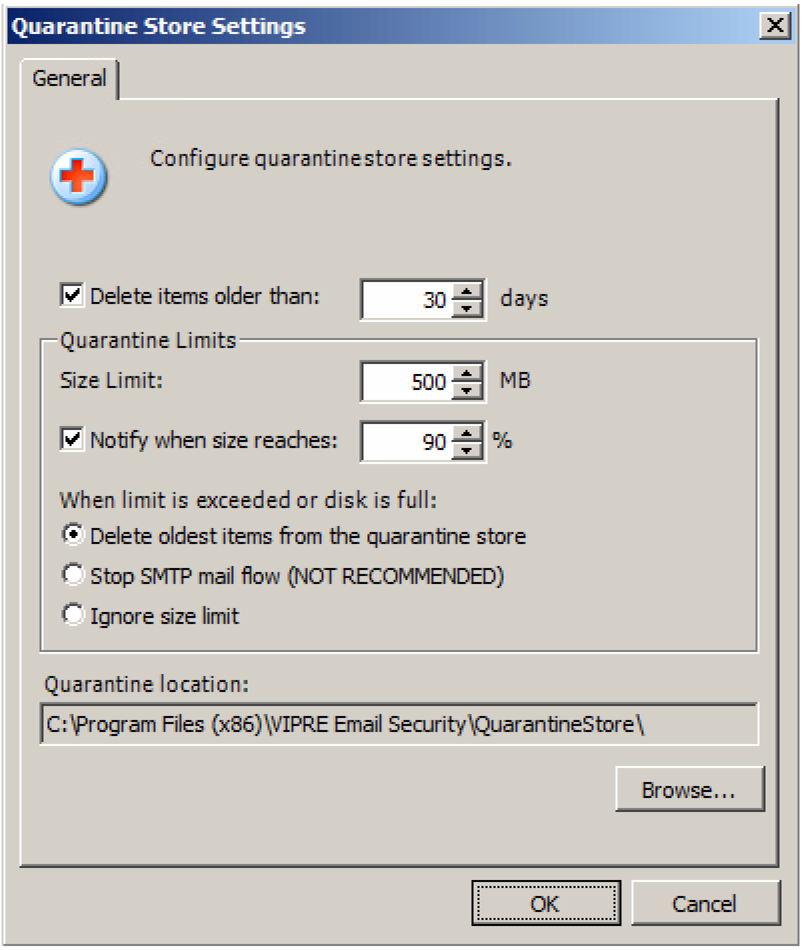

Welcome Wizard
Quarantine Store Settings
Please configure the way quarantined items will be handled.
Configure...
< Back
Next >
Cancel

Size limit: 500 MB

Location: C:\Program Files (x86)\VIPRE Email Security\QuarantineStore\

Screenshot 5: Quarantine Store Settings

8. Click **Configure** to configure the Quarantine Store settings. The **Quarantine Store Settings** dialog box opens.



Quarantine Store Settings

General

Configure quarantine store settings.

☑ Delete items older than: 30 days

Quarantine Limits

Size Limit: 500 MB

☑ Notify when size reaches: 90 %

When limit is exceeded or disk is full:

● Delete oldest items from the quarantine store

○ Stop SMTP mail flow (NOT RECOMMENDED)

○ Ignore size limit

Quarantine location:

C:\Program Files (x86)\VIPRE Email Security\QuarantineStore\

Screenshot 6: Quarantine Store Settings Dialog Box

9. Make a selection:

To delete items older than a certain amount of days:

a. Select the **Delete items older than** check box

b. Enter or select the number of days in the days selection box

To update the quarantine limit information:

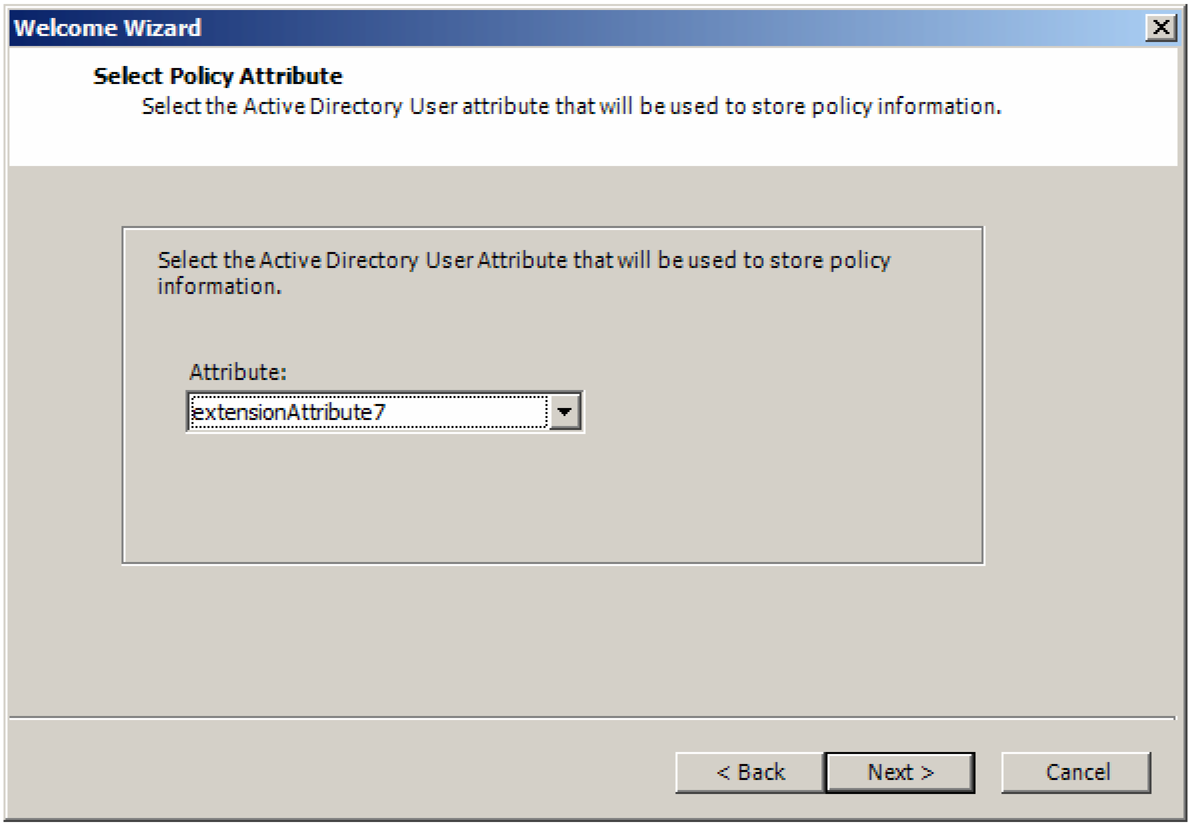
a. Select or type the limits in the fields under the **Quarantine Limits** heading

b. Click **Next**. The Select Policy Attribute window opens.

To change the location of the Quarantine Store:

a. Select **Browse**, select the new location

b. Click **Next**. The **Select Policy Attribute** window opens.



Select Policy Attribute

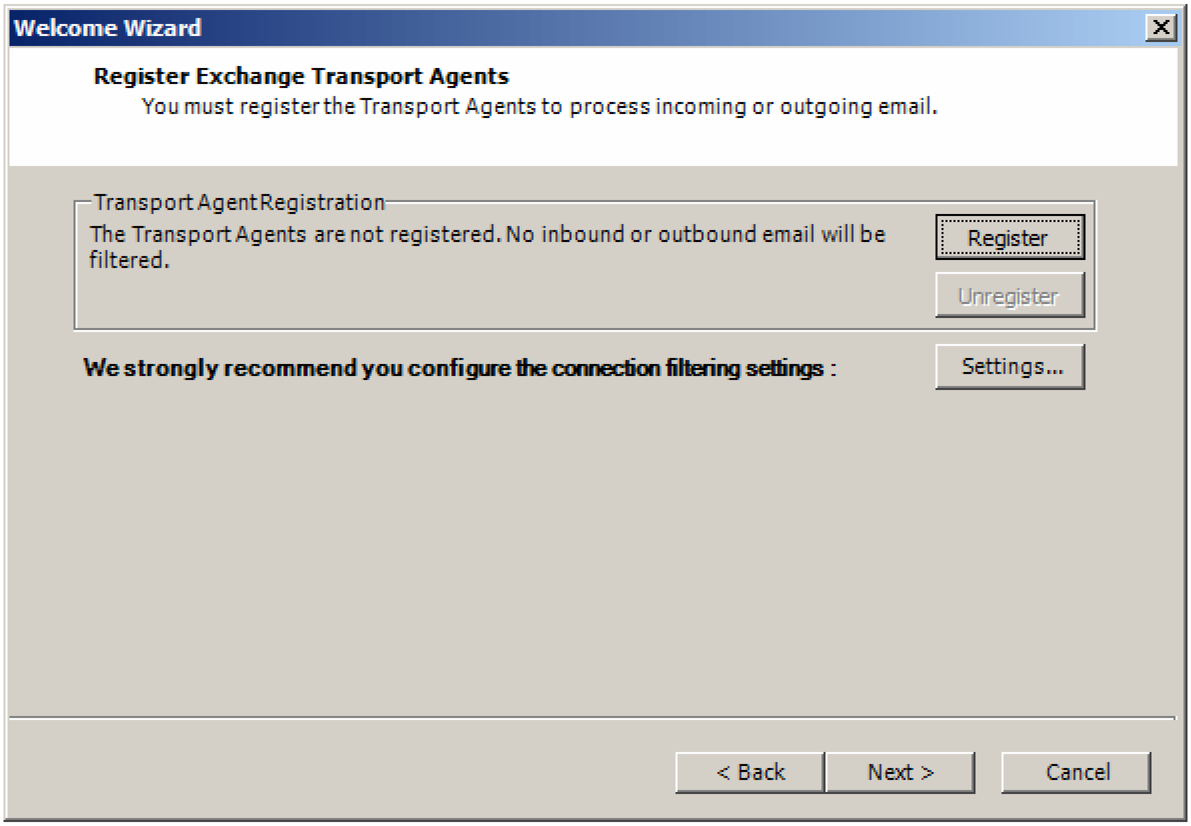
Select the Active Directory User attribute that will be used to store policy information.

Select the Active Directory User Attribute that will be used to store policy information.

Attribute: extensionAttribute7

Screenshot 7: Select Policy Attribute

10. Select an Active Directory attribute that VIPRE will use to store policy information from the **Attribute** drop-list
11. Click **Next**. The **Register Exchange Transport Agents** window opens.



Welcome Wizard

Register Exchange Transport Agents

You must register the Transport Agents to process incoming or outgoing email.

Transport Agent Registration

The Transport Agents are not registered. No inbound or outbound email will be filtered.

We strongly recommend you configure the connection filtering settings :

Screenshot 8: Register Exchange Transport Agents window

12. To register your agents, click **Register**.

-or-

To unregister your agents, click **Unregister**.

13. To configure the connection filtering settings, click **Settings**. The **Connection Filtering Settings** dialog box opens.
14. Make your desired settings for the connection filtering, and click **OK**. Your settings are applied and you are returned to the **Register Exchange Transport Agents** window.
15. Click **Next**. The **Initial Setup Completed** window opens.
16. Click **Finish**. The wizard exits and applies your initial configuration settings.

Now that the wizard is completed, you can start using the VIPRE Console.

3 Managing System Settings

Use this chapter to configure the system parameters necessary to run VIPRE properly.

This chapter covers the following topics:

3.1 Working with Domains 24

3.2 Replicating Server Configuration Changes 29

3.3 Configuring Databases 30

3.4 Working with Agent Registration and Unprocessed Email Settings 31

3.5 Setting System Notifications and Logging Parameters 33

3.6 Managing Licensing and Updates 34

3.7 Managing Quarantine and Reporting Security 36

3.8 Managing Archives Settings 40

3.1 Working with Domains

The Domains feature allows you to manage and configure the Active Directory domains and trusted IPs used in VIPRE.

Active Directory

Active Directory is a directory service used to store information about the network resources across a domain. It allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization. It also stores information and settings relating to an organization in a central, organized, accessible database.

Domains

A Domain is a logical group of computers running versions of the Microsoft Windows operating system that share a central directory database. This central database (known as the Active Directory starting with Windows 2000) contains the user accounts and security information for the resources in that domain. Each person who uses computers within a domain receives his or her own unique account, or user name. This account can then be assigned access to resources within the domain.

VIPRE and Active Directory Domains

The VIPRE management console can query the active directory to retrieve a list of recipients. You can increase the performance of the management console by configuring specific Active Directory Domains to query. This is especially effective if you have remote domains. You can also use the domains settings to configure trusted IPs in your network.

Antispoofing

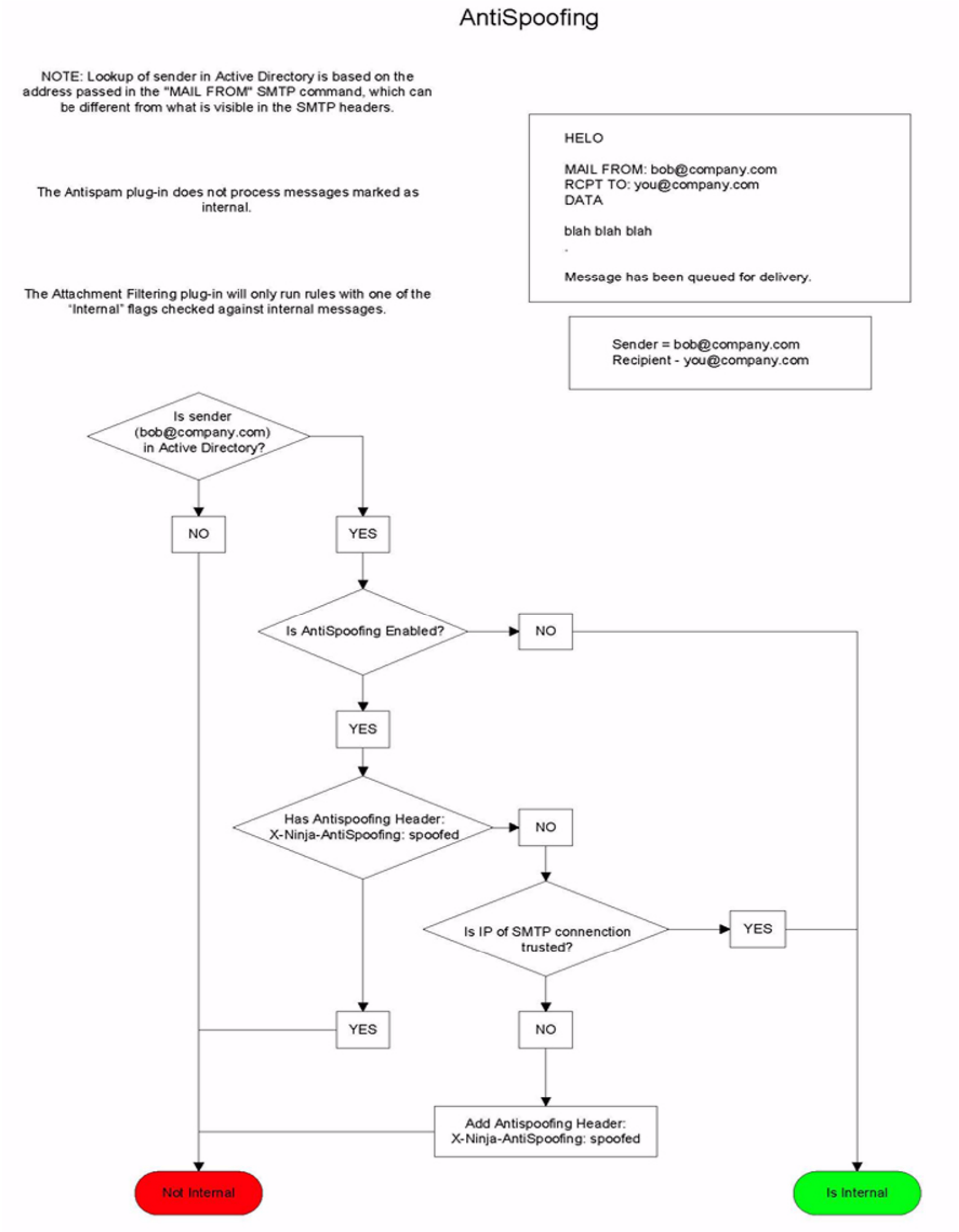
Antispoofing is built into VIPRE as a way of detecting spammers who "spoof" the senders email address to look like address from your domain. When Antispoofing is disabled, VIPRE looks at the address passed to the "MAIL FROM:" command during the SMTP transaction. If this address matches an address in Active Directory, then the message is marked as internal. Internal messages are not scanned by the Antispam plug-in.

When Antispoofing is enabled, there is a series of events that occur. If the address sent in the "MAIL FROM:" command matches an address in Active Directory, VIPRE checks to see if our Antispoofing header has been added. If the header is not present, then the IP address of the SMTP connection is compared against the list of trusted IP's. The message is considered internal only if the IP of the connection matches one in the list. If the IP is not in the list, the Antispoofing header is added and the message is not considered internal. If the header was already present the message it is also not considered internal. The exact syntax of this header is:

X-Ninja-AntiSpoofing: spoofed

For a front-end/back-end server environment, Antispoofing would need to be enabled on the front end servers as well as the back-end. This is because when inbound external messages are passed to the back-end server by the front-end server, that back-end server is going to see the front-end server's IP address on the SMTP connection and will check that if IP is trusted if the front end server didn't already add the Antispoofing header.

Below is a diagram explaining Antispoofing.



NOTE: Lookup of sender in Active Directory is based on the address passed in the "MAIL FROM" SMTP command, which can be different from what is visible in the SMTP headers.

The Antispam plug-in does not process messages marked as internal.

The Attachment Filtering plug-in will only run rules with one of the "Internal" flags checked against internal messages.

```
HELO

MAIL FROM: bob@company.com
RCPT TO: you@company.com
DATA

blah blah blah
.

Message has been queued for delivery.
```

```
Sender = bob@company.com
Recipient - you@company.com
```

Is sender (bob@company.com) in Active Directory?
NO
YES
Is AntiSpoofing Enabled?
NO
YES
Has Antispoofing Header: X-Ninja-AntiSpoofing: spoofed
NO
Is IP of SMTP connenction trusted?
YES
YES
NO
Add Antispoofing Header: X-Ninja-AntiSpoofing: spoofed
Not Internal
Is Internal

Screenshot 9: Antispoofing diagram

To manage Active Directory domains

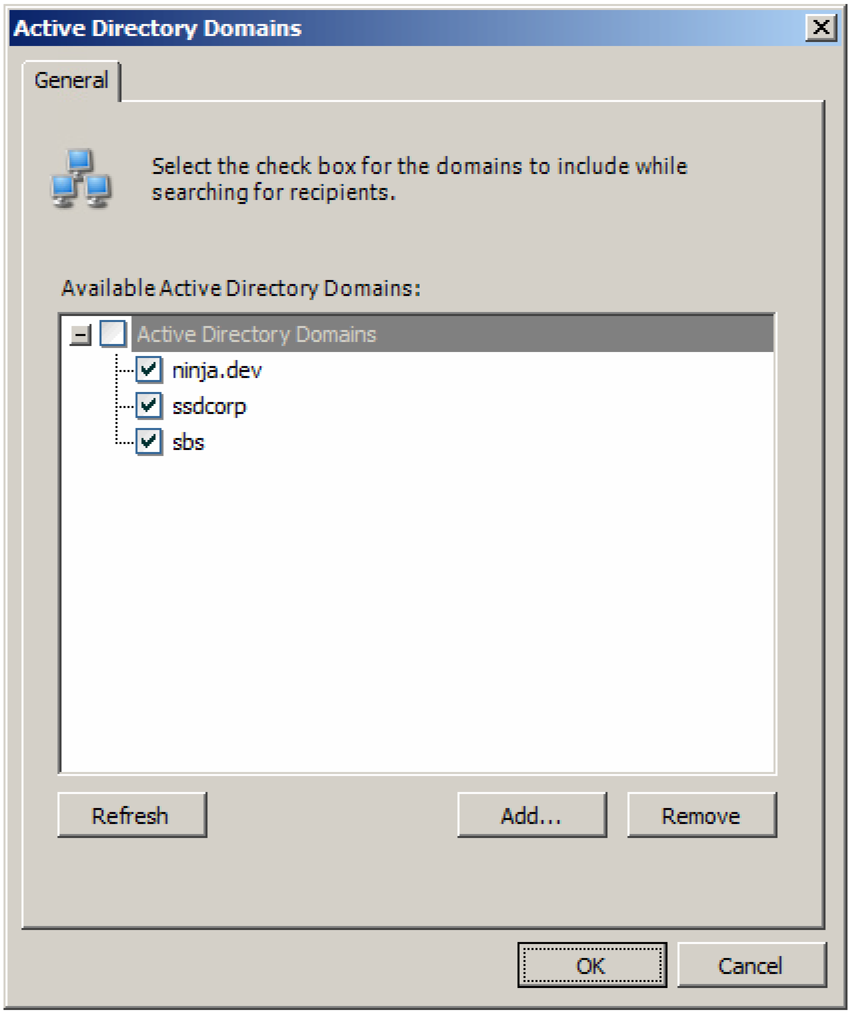
1. Click **Settings**; then, **Domains** in the left pane. The **Domains** tab opens in the right pane.

This tab lists the domains available on the network and signifies which domains are currently enabled for processing. VIPRE queries these domains for user information pertaining to individuals who send and receive email.

2. Click **Modify**. The **Active Directory Domains** dialog box opens. See Step 3.

This dialog box lists the same domains as seen on the Domains tab, except that the check boxes associated with each domain can be selected or cleared.

3. To delete a domain, select the domain; then click **Remove**. The domain is removed from the **Active Directory** list.



Active Directory Domains

Select the check box for the domains to include while searching for recipients.

Available Active Directory Domains:

□ Active Directory Domains
- ☑ ninja.dev
- ☑ ssdcorp
- ☑ sbs

Screenshot 10: Active Directory Domains Dialog Box

4. Make a selection:

To add a new domain:

- Click **Add**. See To add a domain to the Active Directory Domains list.

To include or remove a domain in a search for recipients:

- Select or clear the check box next to the domain.

To refresh the Active Directory list:

- Click **Refresh**.

To accept the updates to the Active Directory Domain list:

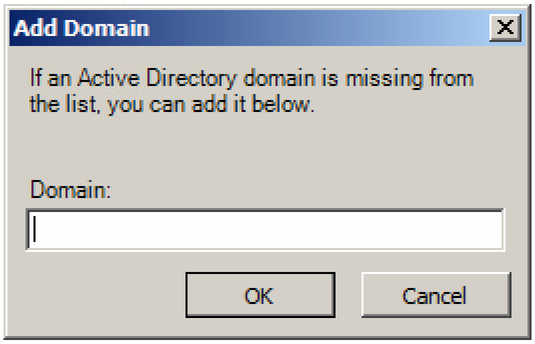
- Click **OK**.

To cancel the updates without saving the information:

- Click **Cancel**.

To add a domain to the Active Directory Domains list

1. Click **Settings**; then, **Domains** in the left pane. The Domains tab opens in the right pane.
2. Click **Modify**. The Active Directory Domains dialog box opens.
3. Click **Add**. The Add Domain dialog box opens.



Add Domain

If an Active Directory domain is missing from the list, you can add it below.

Domain:

Screenshot 11: Active Directory Domains Dialog Box - Add a Domain

4. Type the domain in the **Domain** field.
5. Click **OK**.

To configure Antispoofing

1. Click **Settings**; then, **Domains** in the left pane. The **Domains** tab opens in the right pane.
2. Click the **Antispoofing** tab.
3. Select the **Enable Antispoofing** check box.
4. Make a selection:

To add an address to the list of trusted IPs:

- Click **Add**. The **IP Address** dialog box opens. Go to To add an IP address to the allowed IP list.

To import an address list:

- Click **Import**. Go to To import an IP address list.

To export the address list:

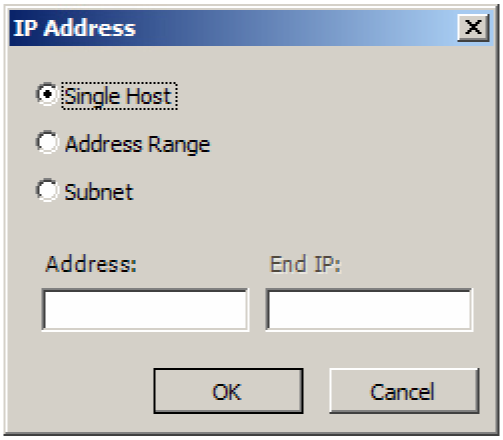
- Click **Export**. Go to To export an IP address list.

5. To edit an address in the list, select the address from the list; then click **Edit**. The **IP Address** dialog box opens. Go to To edit an IP address on the allowed IP list.

6. To delete an address from the list, the address from the list; then click **Remove**. The IP address, address range, or subnet address is removed.

To add an IP address to the allowed IP list

1. Select **Settings**; then, **Domains**. The **Domains** tab opens in the right pane.
2. Click the **Antispoofing** tab.
3. Under Allowed IPs, select the **Enable Antispoofing check box**.
4. Click **Add**. The **IP Address** dialog box opens.



Screenshot 12: IP Address

5. Make a selection:

To add the address for a single host:

- Select **Single Host**; then, type the address in the **Address** field.

To add the host addresses in a specific range:

- Select **Address Range**; then, the address and range in the **Address** and **Range** fields.

To add the address for a subnet:

a. Select **Subnet**
b. Type the address of the subnet and the subnet mask in the **Address** and **Mask** fields.

6. Click **OK**. You return to the **Antispoofing** tab.

To edit an IP address on the allowed IP list

1. Select **Settings**; then, **Domains**. The **Domains** tab opens in the right pane.
2. Click the **Antispoofing** tab.
3. Under **Allowed IPs**, select the **Antispoofing** check box.
4. Select an IP address from the list; then, click **Edit**. The **IP Address** dialog box opens.
5. Update the relevant information.
6. Click **OK**.

To import an IP address list

1. Select **Settings**; then, **Domains**. The **Domains** tab opens in the right pane.
2. Click the **Antispoofing** tab.
3. Under **Allowed IPs**, select the **Antispoofing** check box.
4. Click **Import**. The explorer window opens.
5. Select an XML file to import; then, click **Open**. The IP address list is imported.

To export an IP address list

1. Select **Settings**; then, **Domains**. The **Domains** tab opens in the right pane.
2. Click the **Antispoofing** tab.
3. Under **Allowed IPs**, select the **Antispoofing** check box.
4. Click **Export**. The explorer window opens.
5. Select a location to save the exported XML file; then, click **Save**. The XML file is exported to the folder.

3.2 Replicating Server Configuration Changes

VIPRE can operate in multiple server environments. If you have more than one exchange server, including clustered environments, you can configure VIPRE to replicate any configuration changes from one server to the other servers.

To manage the servers available for replication

1. Click **Settings**; then, **Replication** in the left pane. The **Replication Tab** opens in the right pane.
2. To enable server settings replication, select the **Enable Settings Replication** check box.
3. Make a selection:

To replicate server settings:

- Click **Replicate Now**.

To add a server to the list of servers than can be replicated:

- Click **Add**. Go to To add a server to the Replication Servers list.

To change information for an server on the replication list:

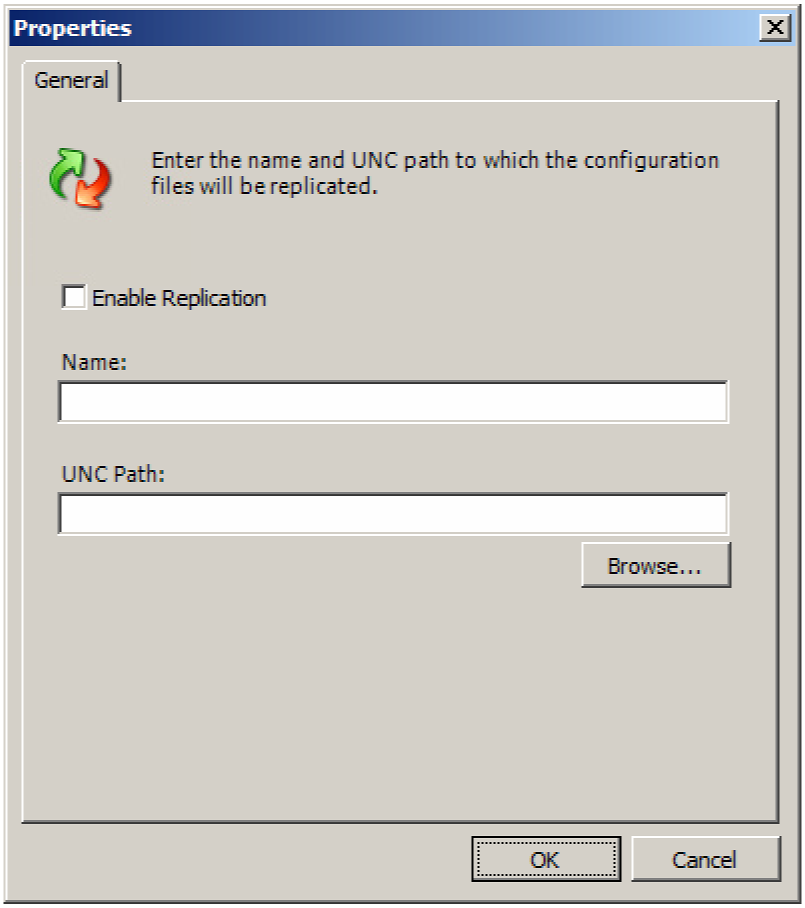
- Click **Edit**. The Properties dialog box opens. Update the information.

To delete an existing server on the replication list:

- Click **Remove**.

To add a server to the Replication Servers list

a. Click **Settings**; then, **Replication** in the left pane. The **Replication Tab** opens in the right pane.
b. Select the **Enable Settings Replication** check box; then click **Add**. The **Properties** dialog box opens.



Enter the name and UNC path to which the configuration files will be replicated.

□ Enable Replication

Screenshot 13: Replication Tab - Properties Dialog Box

4. To enable the server to be replicated, select the **Enable Replication** check box.
5. Type the name of the server in the **Name** field.
6. In the UNC Path field, enter the path to the Settings directory. Click **Browse** if you need to select another location. In a network, the Universal Naming Convention (UNC) is a way to identify a shared file in a computer without having to specify the device on which it is storage device.
7. Click **OK**. You return to the **Replication** tab.

To edit a server on the Replication Servers list

1. Click **Settings**; then, **Replication** in the left pane. The **Replication** tab opens in the right pane.
2. Select the **Enable Settings Replication** check box.
3. Click **Edit**. The **Properties** dialog box opens.
4. Edit the necessary information.
5. Click **OK**. You return to the **Replication** tab.

3.3 Configuring Databases

VIPRE stores its activity records in databases. Access is the default storage database. However, if you are in an environment with heavy mail traffic, it is recommended that you change the reporting database to Microsoft SQL Server.

To configure the reporting database

1. Click **Settings**; then, **Databases** in the left pane. The **Databases** Tab opens in the right pane.
2. Click **Configure**. The **Database Settings** dialog box opens.
3. Make sure the **Enable Reporting** check box is selected.
4. Make a selection:

To enable reporting on an MS SQL Server:

a. Select **MS SQL Server**, add the Server/IP info
b. Select **SQL Authentication**

> A username and password are required for SQL Authentication. Windows authentication for MS SQL Server is not supported at this time.

To enable reporting in MS Access:

a. Select **MS Access**
b. Type or select the path of the Access database.

5. Click **OK**. You return to the **Databases** tab.

3.4 Working with Agent Registration and Unprocessed Email Settings

After a message arrives at an Exchange server via SMTP, that message is handled by a number of Agents. Agents are pieces of code that are associated with certain events and are executed when those events occur. There are two varieties of Agents: Transport Agents and Routing Agents. For more information on Exchange Agents, please go to microsoft.com.

VIPRE registers Agents in order to access specific information and to manipulate the messages during various stages of processing.

Access

The Agents section is accessed through the Agent Registration tab under the Settings heading of the Management Console. When the Agent Registration section loads, Exchange Transport is queried to find out if the agents are registered. This can take several seconds.

Unprocessed Folder Notifications

In the rare case where VIPRE cannot process an email, it sends the email to the unprocessed email folder. After a message is saved to the unprocessed folder, a notification is sent to the list of recipients specified in the Notifications & Logging section of the Management Console, like any other system notification. The following message is sent for unprocessed email:

"The VIPRE application has saved a message in the Unprocessed Folder. Please check logs for details."

> ❗ The Notification Interval is 60 seconds. It determines the interval between notifications. Another notification is only sent if the Unprocessed Folder does not receive any items during the interval period.

To register Transport Agents

1. Click **Settings**; then, **Agents**. The **Agent Registration** tab opens in the right pane.
2. Click **Register**. The **Transport Agents** have been registered.

To unregister Transport Agents

> ℹ For normal operation, transport agents should be kept registered. Typically you should only unregister them when directed by Support as a troubleshooting step.

1. Click **Settings**; then, **Agents**. The **Agent Registration** tab opens in the right pane.
2. Click **Unregister**.

Unprocessed Email Settings

If VIPRE cannot process an email and has no exception handling in place, it sends the email to the Unprocessed Email folder, where you can configure the settings for unprocessed emails.

To configure unprocessed email settings

1. Click **Settings**; **Agents**; then, click the **Unprocessed Email Settings** tab.
2. Make a selection:

   To delete files older than a specific number of days:

   a. Select the **Delete items older than** check box
   b. Type or select the number of days in the **days** box

   To delete files larger than a specific size:

   a. Select the **Delete items older than** check box
   b. Type or select the file size limit in the **MB** box

   To make sure that you are notified when the contents of the Unprocessed Email folder reaches a certain size:

   a. Select the **Notify when size reaches** check box
   b. Type or select the file size in percentage at which you will be notified from the % box.
3. To set the location for the Unprocessed Email folder, click **Browse**, select the location from the explorer window; then, click **OK**.

3.5 Setting System Notifications and Logging Parameters

VIPRE can use email and/or messenger to alert specified personnel in the event of a critical error. For example, if an item went into the unprocessed mail folder, a notification would be sent to the specified recipients.

Managing Email Notifications

1. Click **Settings**; then, **Notifications & Logging**. The **Monitoring and Notifications** tab opens in the right pane.
2. To enable email notifications, select the **Enable email notifications** check box.
3. Make a selection:

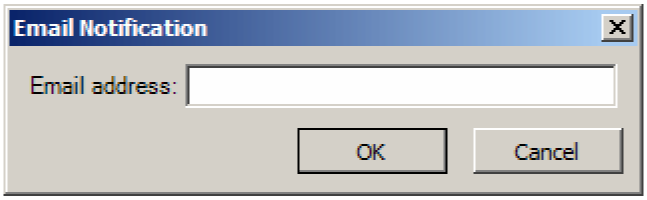
To add a email address that will receive the notification:

a. Click **Add**. The **Email Notification** dialog box opens
b. Type the target email address in the **Email address** field
c. Click **OK**

To remove a target email address:

- Click **Remove**.

4. To edit a target email address, select the email address; then, click **Edit**.



Screenshot 14: Monitoring and Notifications Tab - Email Notifications Dialog Box

System Logging

VIPRE uses logging to record system events. The default level is set to 'High'. We recommend that you change the level only at the request of the support technician.

To manage system logging settings

1. Click **Settings**; then, **Notifications & Logging**. The **Monitoring and Notifications** tab opens in the right pane.
2. Click the **Logging** tab.
3. To set the level at which system events are logged, choose the appropriate level from the **Level** drop-list.
4. Make a selection:

To change the maximum size a log file can reach before a new log file is created,

- Type the number of megabytes in the **Create new log file when size reached:** box.

To change the maximum amount of log files VIPRE will save:

- Type the number in the **Number of log files to keep:** box.

5. To change the directory on which VIPRE stores the log files, type the directory path in the **Directory** field, or click **Browse**; then, search for the folder in which to store the logs.

3.6 Managing Licensing and Updates

You need a registration key to use VIPRE to its full potential. The key is used to check with VIPRE for updates to the available plug-ins. The key is validated on VIPRE's servers to identify the number of users licensed to each plug-in. You can also configure a proxy server as an intermediary between your enterprise workstation and VIPRE to ensure security and administrative control.

NTLM Authentication

VIPRE uses the NTLM authentication protocol. NTLM stands for Windows NT LAN Manager. It is the authentication protocol used on networks that include systems running the Windows NT operating system and on stand-alone systems.

NTLM authentication is based on the data obtained when a user logs on. It consists of a domain name, a user name, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials.

To register your copy of VIPRE

1. Click **Settings**; then, **Updates & Licensing** in the left pane. The **Licensing** tab opens.
2. Type the registration key in the **Registration key** field.
3. Click **Register**. The key is sent to VIPRE for immediate validation. A green check appears above the **Registration key** field if the key is valid. The license information for each module listed in the table below is also updated after the key is validated.

To update the modules

1. Click **Settings**; then, **Updates & Licensing** in the left pane. The **Licensing** tab opens.
2. Click the **Updates** tab.
3. Make a selection:

To schedule a regular date and time to update the module:

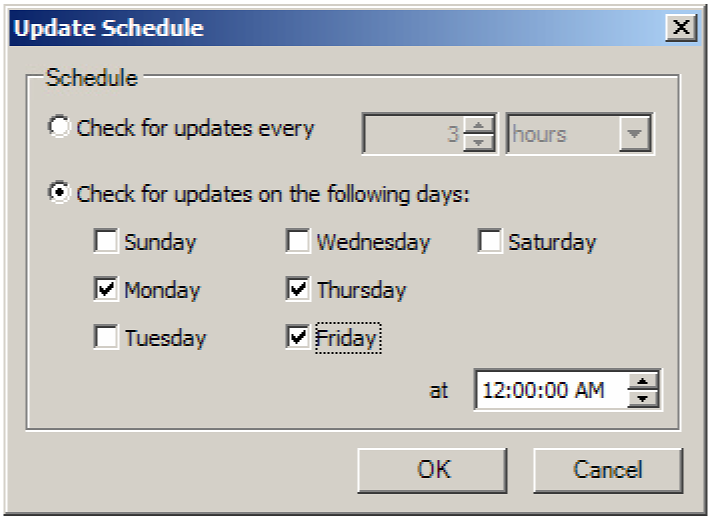
a. Click **Schedule**. A dialog box opens.
b. Select a date and time
c. Click **OK**.

To update the module immediately:

- Click **Update Now**.

To set the update schedule

1. Click **Settings**; then, **Updates & Licensing** in the left pane. The **Licensing** tab opens.
2. Click the **Updates** tab.
3. Click **Schedule**. The **Update Schedule** dialog box opens.



Update Schedule

Schedule

○ Check for updates every 3 hours

● Check for updates on the following days:

□ Sunday □ Wednesday □ Saturday

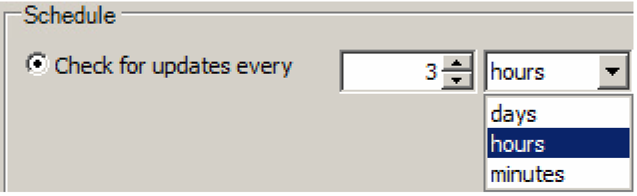
☑ Monday ☑ Thursday

□ Tuesday ☑ Friday

at 12:00:00 AM

Screenshot 15: Updates Tab - Update Schedule Dialog Box

4. To check for updates every number of days, hours, or minutes, select **Check for updates every**; then select the number and unit (**days**, **hours**, or **minutes**) from the drop-list.

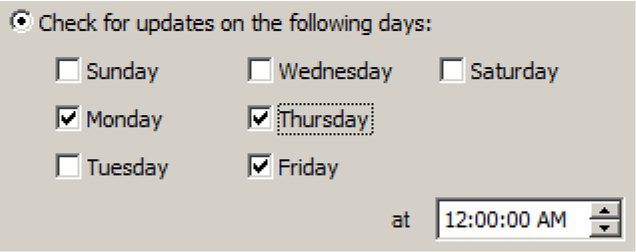


Schedule

● Check for updates every 3 hours

Screenshot 16: Update Schedule Dialog Box - Check for Updates Every Selection

5. To check for updates on specific days at a specific time, select **Check for updates on the following days** then select the day(s) and time VIPRE will check for updates.
6. Click **OK**. You return to the **Updates** tab.



● Check for updates on the following days:

□ Sunday □ Wednesday □ Saturday

☑ Monday ☑ Thursday

□ Tuesday ☑ Friday

at 12:00:00 AM

Screenshot 17: Update Schedule Dialog Box - Check for Updates on the Following Days Schedule

To configure a proxy server

1. Click **Settings**; then, **Updates & Licensing** in the left pane.
2. Click the **Proxy** tab.
3. You must the select the **Use proxy server when communicating with update and license servers** check box to use a proxy server to communicate with VIPRE.
4. Make a selection:

> You must select the **Use proxy server when communicating with update and license servers** check box to enable the remainder of the fields on this tab.

5. Make a selection:

To use an automatic configuration script:

a. Select the **Use automatic configuration script** check box
b. Type the IP address and port from which the configuration script will be accessed in the **Address** and **Port** fields.

To require authentication when using the proxy server:

a. Select the **Requires authentication** check box
b. Type the username, password and domain that will be used for the authentication in the **Username**, **Password**, and **Domain** fields.

3.7 Managing Quarantine and Reporting Security

Use this section to specify which users and/or groups are permitted to access and view items in the quarantine store and view reports.

To manage quarantine and reporting security

1. Click **Settings**; then, **Security**. The **Quarantine and Reporting** tab opens in the right pane.
2. Make a selection:

To add a user to the list of individuals and groups that are allowed to use the quarantine store and report viewer:

- Click **Add User**. The **Select Users** dialog box opens. Go to To Add a secure user.

To add a group to the list of individuals and groups that are allowed to use the quarantine store and report viewer:

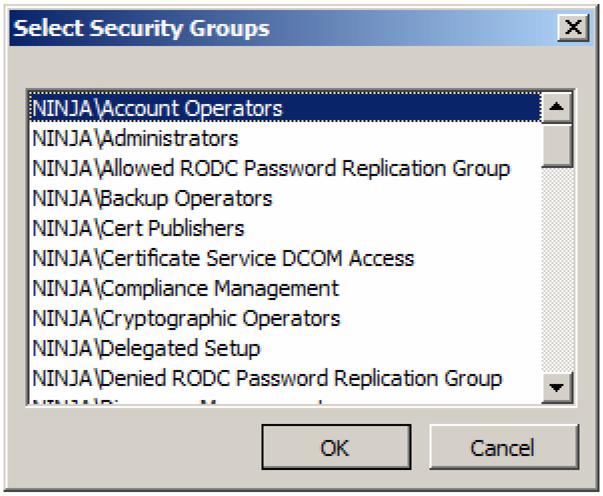
- Click **Add Group**. The **Select Groups** dialog box opens. Go to To add a secure group.

To delete a user or group from the list:

- Click **Remove**. The user or group is deleted.

To add a secure group

1. Click **Settings**; then, **Security**. The **Quarantine and Reporting** tab opens in the right pane.
2. Click **Add Group**. The **Select Security Groups** dialog box opens.



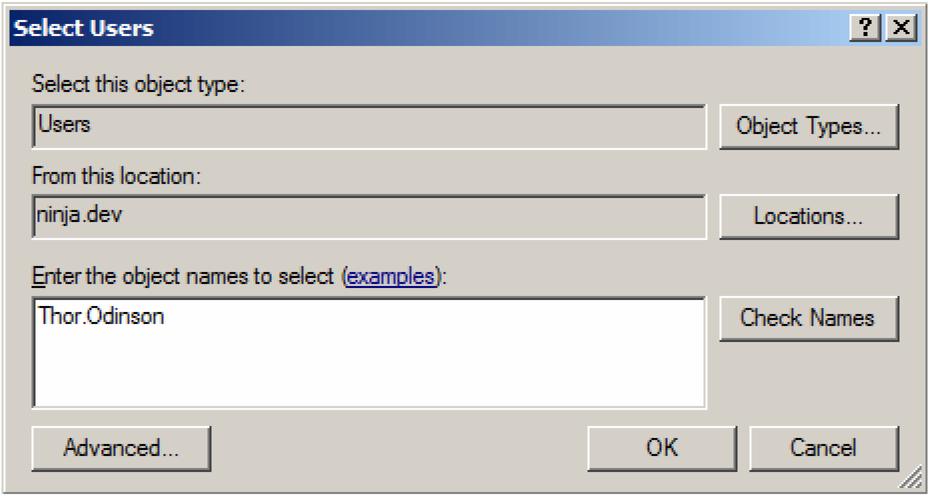
NINJA\Account Operators
NINJA\Administrators
NINJA\Allowed RODC Password Replication Group
NINJA\Backup Operators
NINJA\Cert Publishers
NINJA\Certificate Service DCOM Access
NINJA\Compliance Management
NINJA\Cryptographic Operators
NINJA\Delegated Setup
NINJA\Denied RODC Password Replication Group

Screenshot 18: Select Security Groups Dialog Box

3. Select a group from the list; then, click **OK**.

To Add a secure user

1. Click **Settings**; then, **Security**. The **Quarantine and Reporting** tab opens in the right pane.
2. Click **Add User**. The **Select Users** dialog box opens.



Select this object type: Users

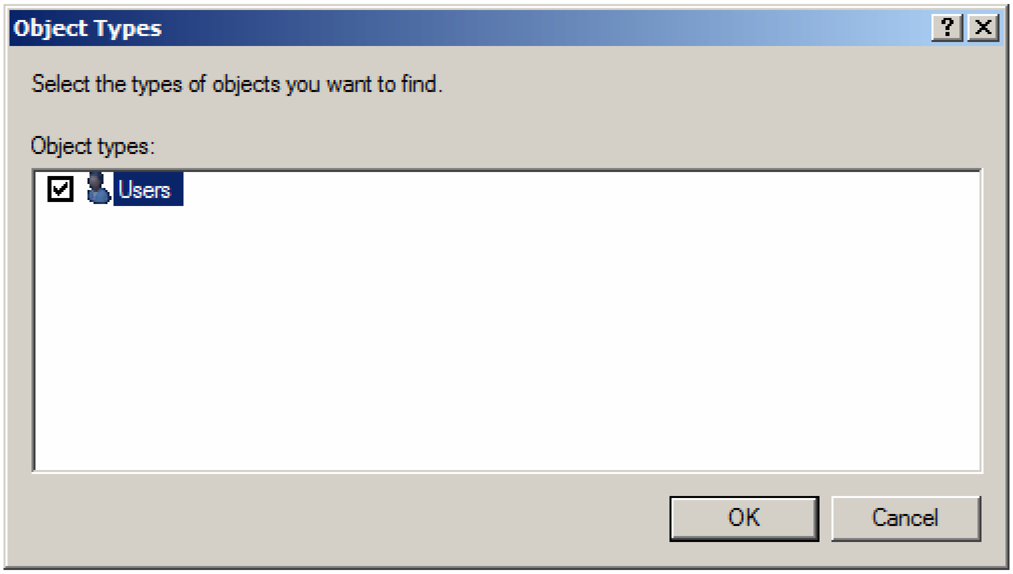
From this location: ninja.dev

Enter the object names to select (examples): Thor.Odinson

Screenshot 19: Select Users Dialog Box

3. To select a different object type, click **Object Types**, select an object type from the **Object Types** dialog box; then click **OK**. You return to the **Select Users** dialog box.

Caution: Steps 3 and 4 tell you how to select a different object type and location. However, We recommend that you leave the **Select this object type** and **From this location** fields at the default settings.


Object Types

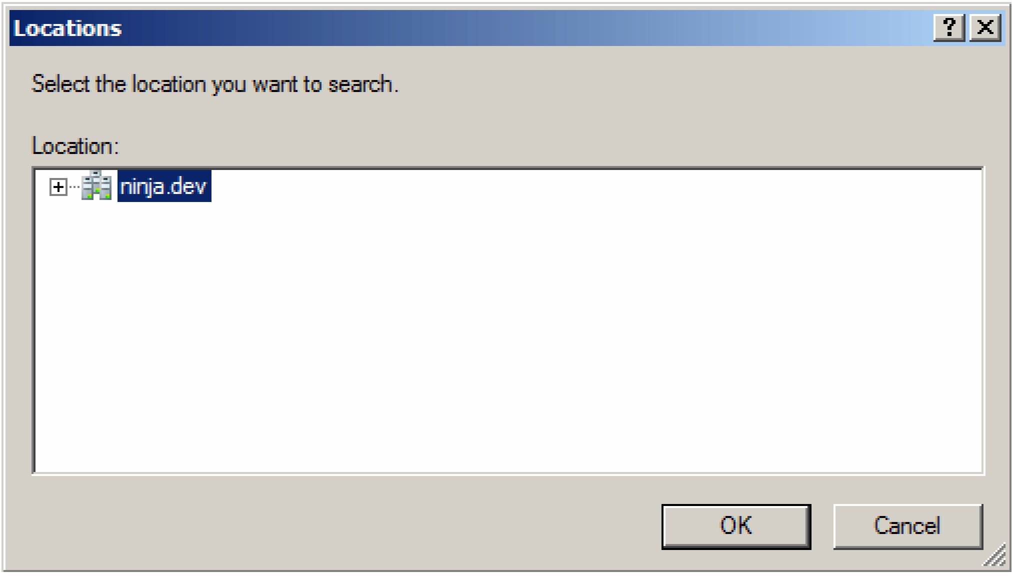
Select the types of objects you want to find.

Object types:

☑ Users

Screenshot 20: Object Types Dialog Box

4. To select a different location, click **Locations**, select a location from the **Locations** dialog box; then click **OK.** You return to the **Select Users** dialog box.


Locations

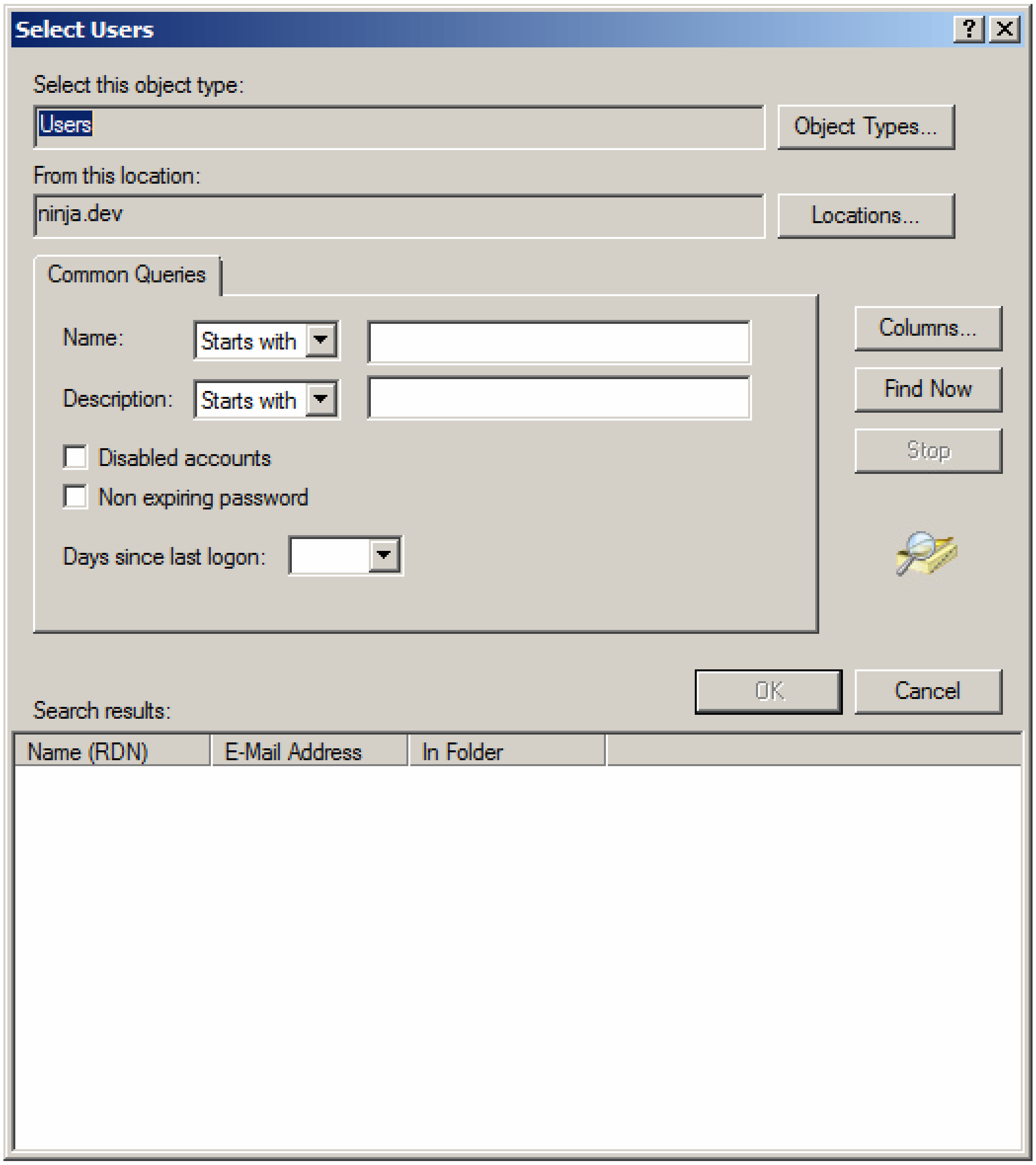
Select the location you want to search.

Location:

⊞ ninja.dev

Screenshot 21: Locations Dialog Box

5. If you want to search for a specific name, type the name in the **Enter the object names to select (examples)** box; then click **Check Names**. Click the blue "examples" text to see examples of object names.
6. To perform an more advanced search, click **Advanced...**. The **Select Users** dialog box opens.



Select Users

Select this object type: Users

From this location: ninja.dev

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

□ Non expiring password

Days since last logon:

Search results:

Name (RDN)	E-Mail Address	In Folder

Screenshot 22: Select Users (Advanced) Dialog Box

7. Make a selection under the Common Queries section:

To Search for a name that starts with a specific letter or an exact name:

- Select **Starts with or Is exactly** from the **Name** drop-list, then click **Find Now**.

To search for a description that starts with a specific letter or an exact name:

- Select **Starts with** or **Is exactly**, from the **Description** drop-list, then click **Find Now**.

To include disabled user accounts in the search:

- Select the **Disabled** accounts check box before clicking **Find Now**.

To include users with passwords that do not expire:

- Select the **Non expiring password** check box before clicking **Find Now**.

To expand the search to a specific amount of day since the user last logged on to the network:

- Select the number of days since the last log on (up to 180) from the **Days since last logon** drop-list.

8. To stop a search that is in progress, click **Stop**.
9. To add a column to the Search results table, click **Columns....** The **Choose Columns** dialog box opens. Select a column name from the **Columns** available list, click add to add it to the **Columns shown** list; then, **click** OK. The column is added to the **Search** results table.
10. After a name is found, select it from the list; then, click **OK**. You return to the **Select Users** dialog box. The name is listed in the **Enter the object names to select (examples)** box.
11. Click **OK**. The **Select Users** dialog box closes and the name is added to the list on the **Quarantine and Reporting** tab. A dialog drops down at the top of the tab.

3.8 Managing Archives Settings

Use this section to specify limits on maximum file sizes to process, how many nested levels of an archive to process, and the actions to take if those limits are reached.

To adjust the limits for archive settings

1. Click **Settings**; then, **Archives**. The **Archive** tab opens in the right pane.
2. To change the limit on the maximum archive file sizes, click the arrows on the **Maximum uncompressed file size to process** box, or manually enter a value in KB.
3. To change the limit on the maximum nested files, click the arrows on the **Maximum nested files/attachments to process** box, or manually enter a value.
4. For either limit, select the "if reached" action to take should these values be reached. You may choose from **Deliver**, **Quarantine**, **Delete**, **Quarantine Email**, or **Delete Email**. By default, the action is set to *Quarantine*.

4 Working with Policies and Recipients

Use this chapter to customize actions for recipients, configure global antispam, antivirus, and attachment filter activity, manage antispam and attachment filter policies, manage disclaimers, and manage quarantined viruses and attachments intended for recipients.

This chapter covers the following topics:

4.1 Policies and Recipients 42

4.2 Working with Recipients 42

4.3 Managing Global Antispam Activity 43

4.4 Managing Antispam Policies 57

4.5 Managing Global Antivirus Activity 65

4.6 Managing Global Attachment Filtering 69

4.7 Managing Attachment Filtering Policies 74

4.8 Managing Global Disclaimer Settings 78

4.9 Managing Disclaimer Policies 82

4.10 Managing the Quarantine Store 83

4.1 Policies and Recipients

A policy is a group of recipients that share the same settings and configurations. Policies help administrators customize actions for recipients. All recipients are automatically assigned to a “default Policy” for a particular plug-in until they are assigned to a different policy.

There are four types of policies that you can assign:

- **Antispam** – policies that help manage Antispam activity for email recipients
- **Antivirus** - policies that help manage Antivirus settings and Quarantined items
- **Attachment Filter** – policies that help manage attachment filters for email recipients
- **Disclaimer** – policies that help manage disclaimers for email recipients

Use the same procedure to add a new Antispam, Antivirus or Attachment Filter policy.

To add a new policy

1. Expand **Policies & Recipients** in the left pane; then, right-click one of the following:
   - Antispam
   - Antivirus
   - Attachment Filter
   - Disclaimer
2. Select **Add New Policy**. The **Add New Policy** window opens.
3. Type a name for the new policy in the **Policy Name** field.
4. Click **OK**. The new policy is added under **Antispam**, **Antivirus**, **Attachment Filter**, or **Disclaimer**.

4.2 Working with Recipients

Use the recipients section to browse recipient assignments, and assign or reassign recipients from one plug-in or policy to another.

To search for all recipient assignments

1. Select **Policies & Recipients**; then, **Recipients** from the left pane. The **Recipients** tab opens in the right pane.
2. Click **Search**. VIPRE searches for all recipient assignments; then, lists the results in a table below.

To search for specific recipient assignments

1. Select **Policies & Recipients**; then, **Recipients** from the left pane. The **Recipients** tab opens in the right pane.
2. Select the criteria by which you want to list the search results from the **Search Field** drop-list. The **Search Type** drop-list and **Search Value** field become active.
3. Make a selection:

To perform a search that contains some or all of the text typed in the Search Value field:

- Select **Contains from the Search Type** drop-list.

To perform a search that exactly matches the text typed in the Search Value field:

- Select **Equals from the Search Type** drop-list.

4. Type a value In **the Search Value** field that will contain or exactly match your search criteria.
5. Make a selection:

To search recipients by policy type:

- Select the policy type from the **Policy Type** drop-list.

To search recipients by the name of the policy:

- Select the name of the policy from the **Policy Name** Drop-list.

To receive only up to a specific number of results:

- Select or type the number in the **Maximum Results** box.

6. Click **Search**. VIPRE searches the active directory based on the selected criteria; then, returns the results in the table below.

To edit policy assignments for a recipient

1. Select **Policies & Recipients**; then, **Recipients** from the left pane. The **Recipients** tab opens in the right pane.
2. Select your search criteria; then, search for recipients. See To search for specific recipient assignments.
3. Select one or multiple recipients from the list.
4. Click **Edit Recipient**. The **Modify Recipient Policy Assignments** dialog box opens.
5. Select the policy type from which you want to change from the **Policy type to change**: drop-list.
6. Select the new policy type to which you want to assign the recipient(s) from the **Assign these recipients to:** drop-list.
7. Click **OK**.

4.3 Managing Global Antispam Activity

Use this section to do the following:

- Configure options that affect all recipients configured for spam filtering,
- Create a list of blocked or allowed senders for recipients configured for spam filtering,
- Create custom rules to modify the spam score based on specific criteria,
- Enable reverse DNS,
- Configure RBLs (Real-time Black hole Lists) and SPFs (Sender Policy Framework),
- View antispam policy members and assign or reassign recipients to other antispam policies,
- Enable Greylisting.

To manage global antispam settings

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Global Settings** tab.
3. Make a selection:

To enable global spam filtering for all antispam policies:

- Select the **Enable Spam Filtering** check box.

To add headers for all antispam policies:

- Select the **Add X-Headers** check box.

To filter bounce messages for all antispam policies:

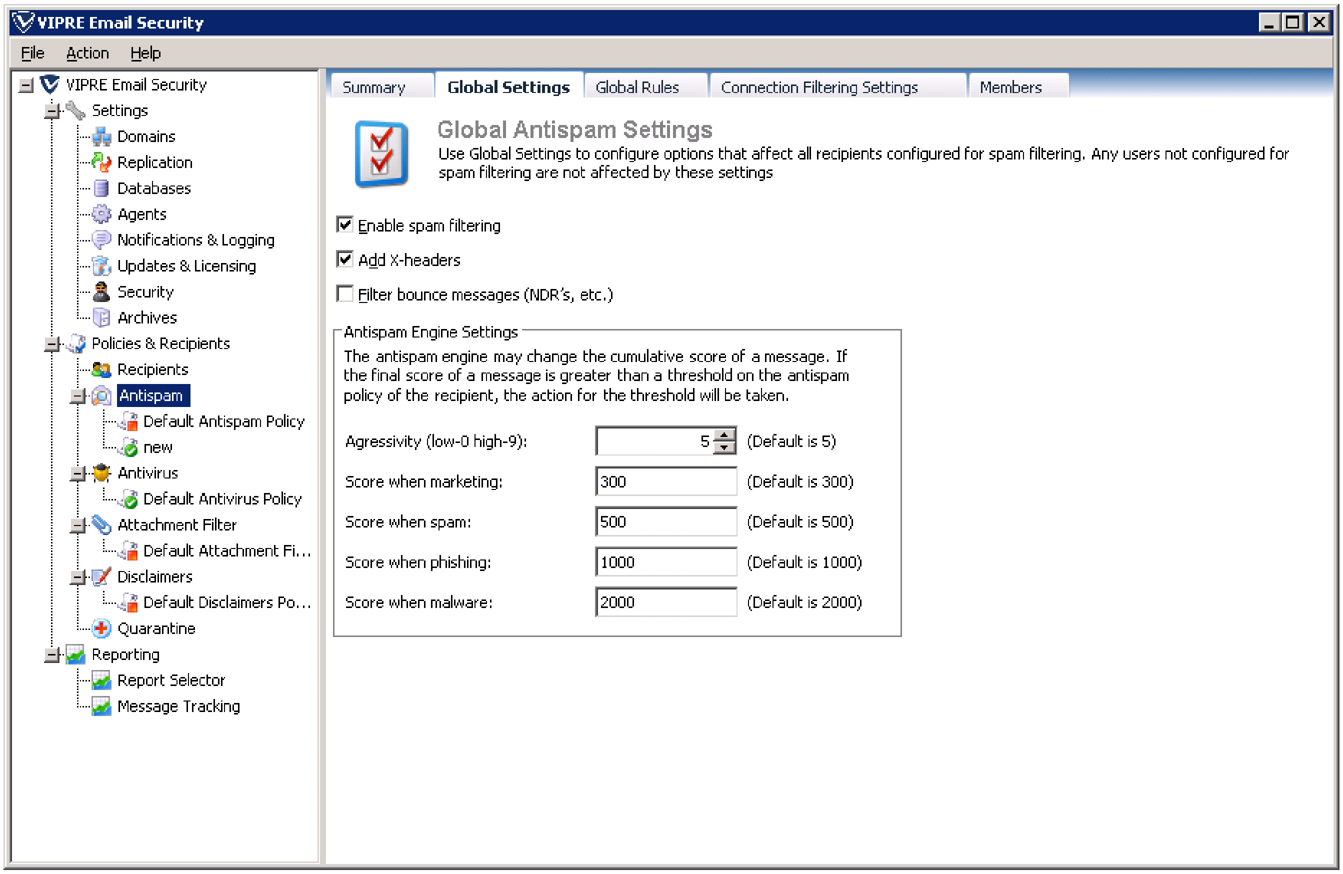
- Select the **Filter Bounce Messages (NDRs, etc.)** check box.

Antispam Engine settings

The Aggressivity level adjusts how *aggressive* the Antispam Engine is. You can tailor this setting to suit your environment depending on what your organization values more (spam vs. false positives).

By default, Aggressivity is set to 5, with a range of 0–9.

- **Higher** = More spam will be caught by the engine, at the risk of increased false positives
- **Lower** = Some spam will be let through, but decreases the change of false positives



Global Antispam Settings

Use Global Settings to configure options that affect all recipients configured for spam filtering. Any users not configured for spam filtering are not affected by these settings

☑ Enable spam filtering

☑ Add X-headers

☐ Filter bounce messages (NDR's, etc.)

Antispam Engine Settings

The antispam engine may change the cumulative score of a message. If the final score of a message is greater than a threshold on the antispam policy of the recipient, the action for the threshold will be taken.

Agressivity (low-0 high-9): 5 (Default is 5)

Score when marketing: 300 (Default is 300)

Score when spam: 500 (Default is 500)

Score when phishing: 1000 (Default is 1000)

Score when malware: 2000 (Default is 2000)

If the text of a message is flagged as spam, the Antispam Engine will identify it as one of four categories: marketing, spam, phishing, and malware. You can adjust how many points are assigned on each category.

The default points assigned per category are

- Marketing - 300
- Spam - 500
- Phishing - 1000
- Malware - 2000

If the total points assigned to a message exceed either the quarantine threshold or delete thresholds, that action will be taken on the message.

Example: The quarantine threshold is 1200, and the delete threshold is 1800. Sample message number 1 gets assigned 1300 total points; it is quarantined. Sample message number 2 gets assigned 2300 total points; it is deleted.

X-Headers

X-Headers are a way to insert user-defined header fields into an e-mail message. These X-Header fields are preserved but ignored by messaging servers and applications that don't use X-Header fields. These X-Header fields can actually set delivery information that exists in the P1 header, such as the sender, recipients, source IP address, and HELO domain. X-Headers are required to preserve original message information when you use the Replay directory to process exported messages from another Exchange server.

Regular Expressions

A regular expression (RE) is a search string that uses special characters to match patterns of text. You can use them with the Find, Find in Files commands, and with the Replace command in conjunction with replacement expressions. Replacement expressions are used to substitute text in conjunction with Tagged Regular Expressions, when using the Replace command. An RE is made up of ordinary characters, some of which take on the special meanings described below.

Ordinary Characters

An ordinary character is an RE that matches itself. It can be any character, except <newline> and the special characters listed below. An ordinary character preceded by a backslash is treated as the ordinary character itself, except when the character is (,), <, >, or the letters f, n, t and x, or the letters f, n, t and x, or the digits 1 through 9.

Hex Characters

Any character can be represented by its hex value. This is specified with the pattern \xdd, where dd is any 2-digit hexadecimal number, excluding zero.

Tabs

A tab character is represented by the pattern \t.

Page Breaks

A page break (form feed) character is represented by the pattern \f.

Line Breaks

A line break is represented by the pattern \n. This matches carriage return and line feed characters. Note that these cannot be combined with repetition operators (see below), so you can only match an exact number of them (e.g. \n\n will match a single blank line.) Do not use this for constraining matches to the end of a line, as it's much more efficient to use "$" (see Expression Anchoring below). This pattern should only be used to match text that spans line boundaries.

Special Characters

These special characters can be rendered ordinary by preceding them with a backslash (\), if they are single special characters, or removing the preceding backslash if they are compound special characters.

Wildcard Character

The period (.), when used outside of a class expression, matches any character except newline.

Repetition Operators

The asterisk (*) matches zero or more occurrences of the smallest possible preceding regular expression, while the question mark (?) matches zero or one, and the plus sign (+) matches at least one occurrence. For example, A*b+ matches zero or more A's followed by one or more B’s.

Interval Operator

Repeats the smallest possible preceding regular expression the given number of times. The options are:

- \{count\} Matches exactly count times.
- \{min,\} Matches at least min times.
- \{min,max\} Matches between min and max times.

Alternation Operator

The alternation operator (\|) matches either the expression to its left or the one to its right. It has a lower precedence of any other regular expression operator, so the surrounding RE's must be bracketed with \(...\) if only a part of them is to be matched.

Class Expressions

A class expression is a RE, enclosed in square brackets ([…]), that matches any one of the elements contained in the brackets.

Simple Characters

These are single characters that match themselves. To match a right square bracket (]), it must be the first character of the class expression, after any initial circumflex (see Negated Class Expressions). To match a hyphen, it must be either the first or the last character of the class expression. For example [AaBb] matches upper or lower case A or B.

Negated Class Expressions

If the first character of a class expression is the circumflex (^), the expression matches any character not in the class. For example [^AB^] matches any character except A, B and the circumflex itself.

Range Expressions

A range expression is two characters separated by a hyphen (-). It matches any characters with code points between those of the two characters. For example, [A-Za-z0-9-] matches any upper or lower case letter or digit, or the hyphen itself. Note that [a-z] also matches upper case letters, unless the option to match case is selected.

Character Class Operators

These can be used as an alternative way of representing classes of characters. For example, [a-z] is equivalent to [[:lower:]] and [a-z0-9] is equivalent to [[:lower:][:digit:]]. (Note the extra pairs of brackets.)

Expression Anchoring

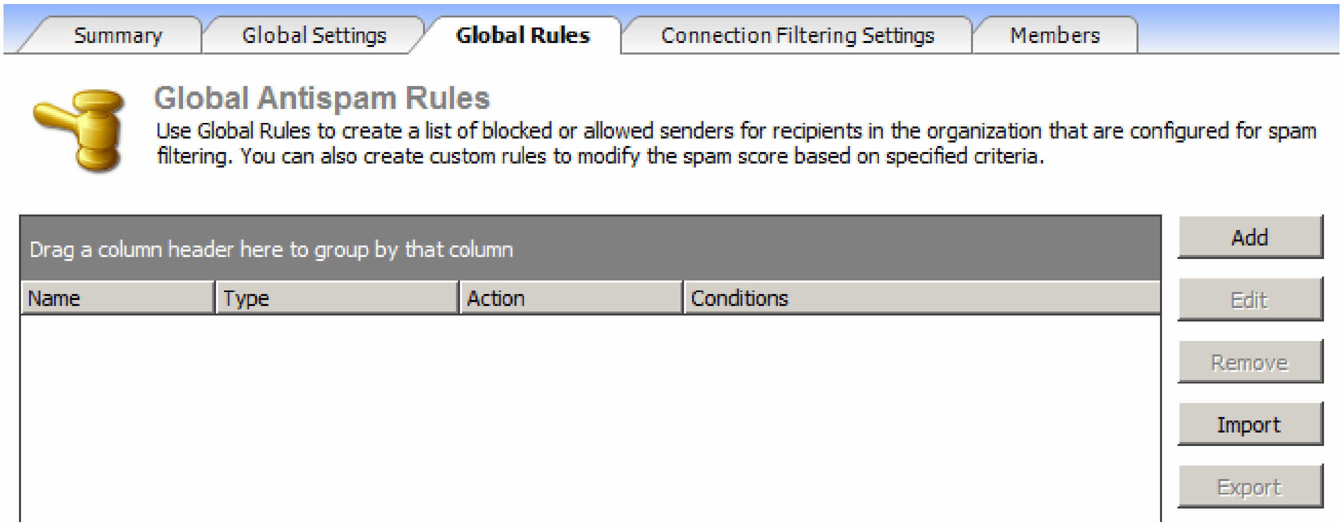
An RE can be restricted to matching strings that begin or end a line or word, as follows: ^ A circumflex as the first character of an RE anchors the expression to the beginning of the line. $ A dollar sign as the last character of an RE anchors the expression to the end of the line. \< The character pair \< anchors the next RE to the start of a word. \> The character pair \> anchors the previous RE to the end of a word.

Tagged Expressions

A tagged expression is an RE that starts with the pair \(and ends with the pair \). There can be up to nine such expressions in a complete RE. Such an expression matches the same as the expression without the surrounding \(and \). The first expression defined in this way can be referenced as \1 later in the RE, and so on up to \9 for the ninth tagged expression. Each such reference matches the same string as its original tagged expression. For example \(tu\) \1 matches the string "tu tu".

To manage global rules for antispam policies:

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Rules tab**.



Global Antispam Rules

Use Global Rules to create a list of blocked or allowed senders for recipients in the organization that are configured for spam filtering. You can also create custom rules to modify the spam score based on specified criteria.

Screenshot 23: Global Rules

3. Make a selection:

To add an allowed or blocked sender, blocked character set, or custom rule:

- Click **Add**. The **Rule Wizard** opens. See To add a rule using the Rule Wizard.

To edit the name or email address for a rule in the list:

- Click **Edit**. The **Rule Wizard** opens. You can only edit the name and/or the email address/character set.

To delete a rule:

- Click **Remove**. The rule is removed from the list.

To import a rule:

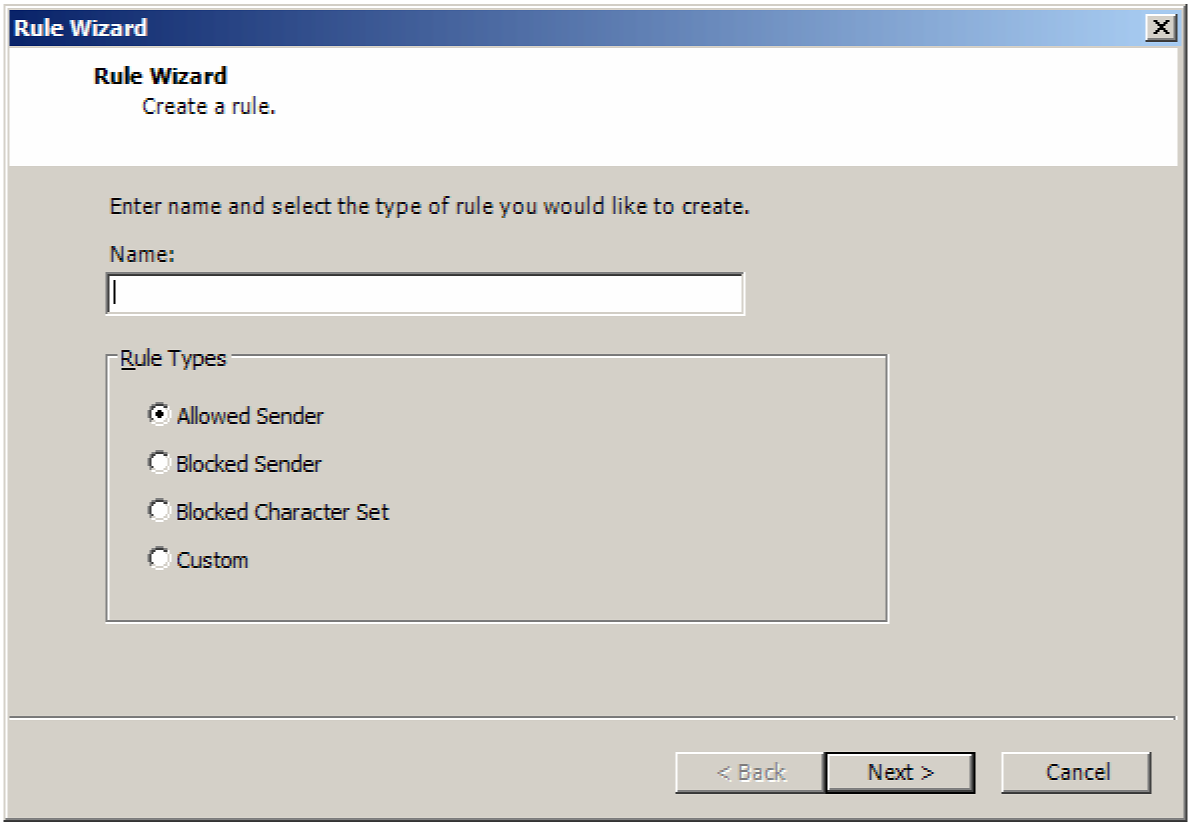
- Click **Import**. For example, if VIPRE creates a rule for our customers, we can place it in a centralized location from which they can import it.

To export a rule:

- Click **Export**.

To add a rule using the Rule Wizard

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Rules tab**.
3. Click **Add**. The **Rule Wizard** opens.



Screenshot 24: Rules Wizard

4. Type a name for the new rule in the Name field.
5. Make a selection:

To allow mail from the email address specified on the next wizard dialog box:

- Click **Allowed Sender**.

To block mail from the email address specified on the next wizard dialog box:

- Click **Blocked Sender**.

To block mail using a specific character set (i.e. Russian, Chinese, etc.):

- Click Blocked Character Set.

To create a custom filter rule:

- Click Custom.

6. Click **Next**.
7. Make a selection:

If you selected Allowed Sender in the previous dialog box:

- Type the email address(es) from which you want to receive email in the **Allowed Senders** box.

If you selected Blocked Sender in the previous dialog box:

- Type the email address(es) from which you do not want to receive email in the **Blocked Senders** box, click **Next**; then, select whether the emails will be quarantined or deleted.

If you selected Blocked Character Set in the previous dialog box:

- Click **Add**, select the character set(s) from the **Add Blocked Character Sets** dialog box, click **Next**; then, select whether the emails containing the selected character sets will be quarantined or deleted.

If you selected Custom in the previous dialog box:

- Select the search parameters that the rule will apply to the policy from the **Fields**, **Search Type**, and **Value** fields; then, select the action to apply to the rule.

8. Click **Finish**. The rule is added to the table.

To edit a rule using the Rule Wizard:

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Rules tab**.
3. Click **Edit**. The **Rule Wizard** opens. Only the **Name** field is editable on the first page.
4. Click **Next**.
5. Edit the parameters as necessary.
6. Click **Finish**.

Connection Filtering

Real-time Black hole Lists (RBLs) list ISP addresses that are known sources of spyware and spam. A network uses this list to filter out undesirable traffic. After the IP addresses are filtered, traffic coming from or going to an IP address that is on the list is blocked.

Sender Policy Framework (SPF) authenticates the Internet domain of a person sending email. This action discourages spam mailers who routinely disguise the origin of their e-mail, a practice known as “spoofing”. SPF makes it easier for a mail server to determine when a message came from a domain other than the one claimed.

The SPF specification defines a policy framework, an authentication scheme, and a machine readable language. Each participating domain declares attributes that uniquely describe their mail, including authorized senders. This description is represented in an SPF record, which is published in DNS (domain name system) records. An SPF client program performs a query searching for the correct SPF record, in order to determine whether a message comes from an authorized source.

If “Enable Sender Policy Framework” is checked, there will be an “X-Ninja-Spf” header added to every received message. This header will contain the result of the SPF check. Possible results are: Pass, None, SoftFail, Fail, TempError, PermError, Neutral (Fail is the same thing as HardFail).

Reverse DNS confirms that the sending IP address has both forward and reverse Domain Name System (DNS) entries that match each other; used to confirm the sender’s IP and domain match.

Greylisting is a feature that will help verify that a sending mail server is a real mail server instead of a spammer. When an email is received from a domain that has not recently sent an email to your domain, the Greylisting module will request a resend from the sending mail server. SMTP rules dictate that all mail servers are required to resend the message(the default for Microsoft Exchange is 5 minutes). Spammers do not use mail servers, and will not resend the message. Legitimate mail servers will resend the message.

Greylist connection filter also supports multiple hub role configurations. If multiple installs all use the same SQL database, the Greylist and Delaylist filters will also share their database. This allows a connection to be made on server A and then retried on server B. Server B would then allow the connection, because it is aware of the first attempt on server A.

How Connection Filtering helps You

RBLs help you reduce the amount of spam by looking at the IP address of an email's source and comparing it to a list of known spamming IP addresses. If the IP addresses matches any addresses on the list, it is blocked. SPF allows you to specify which IP addresses are authorized to transmit email for specific domain. This helps you block spam and potentially harmful mail.

Greylisting will prevent many spam emails from being downloaded by the server, reducing the amount of emails that need to be processed by VIPRE.

Allowed IPs

The addresses listed under Allowed IPs are the IP addresses that are allowed even if the Connection Filtering settings would normally block them.

To manage the Allowed IP list

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. To enable the allowed IP address list so your network can use to filter out spam, select the **Enable allowed IP list** check box.
4. To edit an IP address in the list, select an address in the list; then, click **Edit**. Go to To edit an IP address on the Allowed IP list.
5. Make a selection:

To add an IP address to the Allowed IP list:

- Click **Add**. Go to To add an IP address to the Allowed IP list.

To remove an IP address from the list:

- Click **Remove**. Go to To remove an IP address from the Allowed IP list.

To import an IP address:

- Click **Import**. Go to To import an IP address to the Allowed IP list.

To export an IP address:

- Click **Export**. Go to To export an IP address from the Allowed IP list.

To configure RBL settings:

- Click **RBL Settings...**. Go to To configure RBL settings.

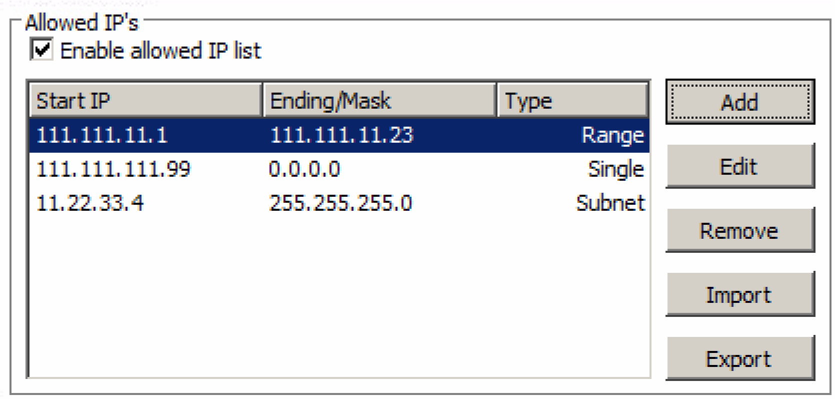
To enable SPF:

- Click **SPF Settings...**. Go to To enable SPF.

6. To determine when records are purged from the cache, select the time frame from the **Purge records from cache**: drop-list. You can also perform a cache dump manually by clicking **Perform Cache Dump**.

To add an IP address to the Allowed IP list:

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Under **Allowed IPs**, select the **Enable allowed IP list** check box.



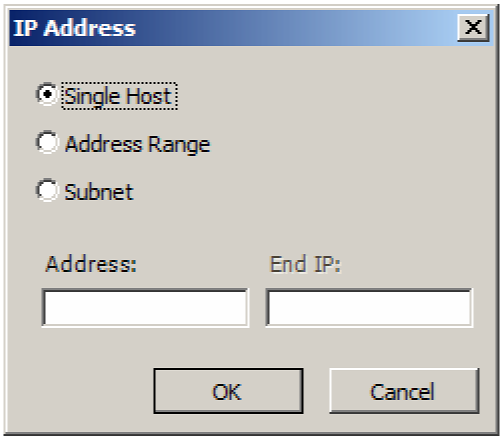
Allowed IP's

☑ Enable allowed IP list

Start IP	Ending/Mask	Type
111.111.11.1	111.111.11.23	Range
111.111.111.99	0.0.0.0	Single
11.22.33.4	255.255.255.0	Subnet

Screenshot 25: Allowed Hosts

4. Click **Add**. The IP Address dialog box opens.



IP Address

● Single Host

○ Address Range

○ Subnet

Address:

End IP:

Screenshot 26: IP Address

5. Make a selection:

To add the address for a single host IP address:

- Select **Single Host**; then, type the address in the **Address** field.

To add the IP addresses in a specific range:

- Select **Address Range**; then, the address and range in the **Address** and **Range** fields.

To add the IP address for a subnet:

- Select **Subnet**; then, type the addresses in the **Address** and **Mask** fields.

6. Click **OK**.

To edit an IP address on the Allowed IP list

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click **the Connection Filtering Settings** tab.
3. Under **Allowed Hosts**, select the **Enable allowed IP list check** box.
4. Click **Edit**. The **IP Address** dialog box opens.
5. Update the relevant information; then, click **OK**.

To remove an IP address from the Allowed IP list

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Under **Allowed Hosts**, select the **Enable allowed IP list** check box; then, click **Remove**. The IP address is removed.

To import an IP address to the Allowed IP list

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Under **Allowed Hosts**, select the **Enable allowed IP list** check box; then, click **Import**. The explorer window opens.
4. Select an XML file to import; then, click **Open**. The IP address is imported to the list.

To export an IP address from the Allowed IP list

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Under **Allowed IP's**, select the **Enable allowed IP list** check box.
4. Click **Export**. The explorer window opens.
5. Select a location in which to save the exported XML file; then, click **Save**. The XML file is exported to the folder.

To enable reverse DNS

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Select the **Enable reverse DNS** check box.

To add a header instead of rejecting connection

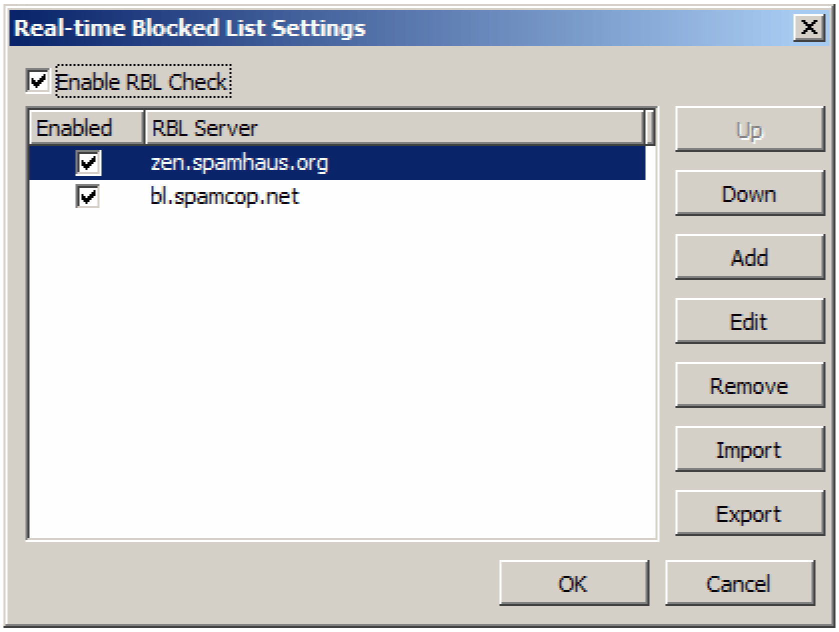
Enabling *Add header* allows rules to be created, in order to assign points or quarantine the message.

Note: This makes False Positives more tolerable since the message can be recovered from the spam folder, as opposed to never receiving it because the connection was dropped.

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Select the **Add Header instead of rejecting connection** check box.
4. Click **Apply**.

To configure RBL settings

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Under **Real-time Blocked List**, click **RBL Settings....** The **Real-time Blocked Settings** dialog box opens.



☑ Enable RBL Check

Enabled	RBL Server
☑	zen.spamhaus.org
☑	bl.spamcop.net

Screenshot 27: RBL Settings

4. Select the **Enable RBL Check** check box.
5. Make a Selection:

To add an RBL server:

- Click **Add**. Go to To add an RBL server.

To edit an RBL setting:

- Click a setting from the list; then, click **Edit**. Update the information.

To remove an RBL setting:

- Click **Remove**. The setting is removed from the list.

To import an RBL setting:

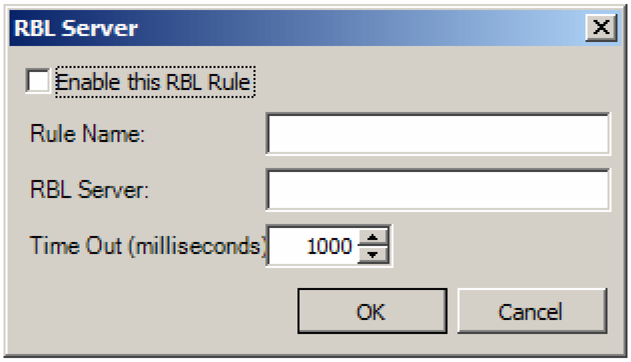
- Click **Import**.

To export an RBL setting:

- Click **Export**.

To add an RBL server

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Under **Real-time Blocked List**, click **RBL Settings...**. The **Real-time Blocked Settings** dialog box opens.
4. Click **Add**. The **RBL Server** dialog box opens.



Time Out (milliseconds) 1000

Screenshot 28: Add RBL Server

5. Select the **Enable this RBL Rule** check box.
6. Type a name for the rule in the **Rule Name** field.
7. Type a name for the server in the **RBL Server** field.
8. Type the number of milliseconds before the server times out in the **Time Out** field.
9. Click **OK**.

To enable SPF

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.

3. Under **Sender Policy Framework**, select the **Enable Sender Policy Framework** check box.
4. Select either the **Block soft fail** or **Block hard fail** check boxes:
   a. Select the **Block soft fail** check box to allow the message
   b. Select the **Block hard fail** check box to reject the message
5. Click **Apply**.

> We do not recommend enabling **Block hard fail** because a hard failed message is virtually guaranteed to be spam. A hard fail indicates that the address does not reside on the SPF record and should not be sending email.

To enable Greylisting

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Click the **Greylisting Settings.**
4. Click the **Enable Greylisting** check box.
5. In the **Allowed Domains:** box, list the domains to include, one per line.
6. Click **OK**.

Additional "distinguishers" enable you to control how aggressively Greylisting filters emails. When enabled, the following options specify how Greylisting determines the source of the email. You can enable or disable these by selecting the check box next to each item in the **Distinguish Connections By:** box.

- Sender Local Part
- Sender Domain
- Sender IP
- Recipient Local Part
- Recipient Domain

It is also possible to exclude specific domains from Greylisting (see below).

Excluding domains from Greylisting

It is possible to exclude specific domains from Greylisting. Exclusions can be used to allow emails from domains that may attempt to resend the email using several different severs.

When a domain is excluded from Greylisting, the greylist connection filter will not temporarily reject new connections for any sender from that domain.

Emails from a greylist-excluded domain will still be subjected to RBL, Reverse DNS, and SPF checking (if they are enabled). All plug-ins, including antispam, may still quarantine the email.

To exclude one or more domains from greylisting:

1. Select **Policies & Recipients**; then, **Antispam**. The Summary tab opens in the right pane.
2. Click the **Global Rules** tab.
3. Click the **Add** button.

4. Write in the name of the rule and select what type of rule you want to create.
5. Write in the domain to be specified, only one domain per line.
   Messages can still be filtered by other components.
6. Click **Finish**.
7. Click **Apply**.

To enable Delaylisting

1. Select **Policies & Recipients**; then, **Antispam**. The **Summary** tab opens in the right pane.
2. Click the **Connection Filtering Settings** tab.
3. Click **Delaylisting Settings**
4. Click the **Enable Delaylist** check box.

To view a global list of antispam policy members

1. Select **Policies & Recipients**; then, **Antispam** from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Members** tab.
3. Select the criteria by which you want to list the search results from the **Search Field** drop-list. The **Search Type** drop-list and **Search Value** field become active.
4. Make a selection:

   To perform a search that contains some or all of the text typed in the Search Value field:

   - Select **Contains** from the **Search Type** drop-list.

   To perform a search that exactly matches the text typed in the Search Value field:

   - Select **Equals** from the **Search Type** drop-list.

5. Type a value In the Search Value field that contains or exactly matches your search criteria.
6. Make a selection:

   To search for members by policy type:

   - Select the policy type from the Policy Type drop-list.

   To search for members by the name of the policy:

   - Select the name of the policy from the Policy Name Drop-list.

   To receive only up to a specific number of results:

   - Select or type the number in the Maximum Results box.

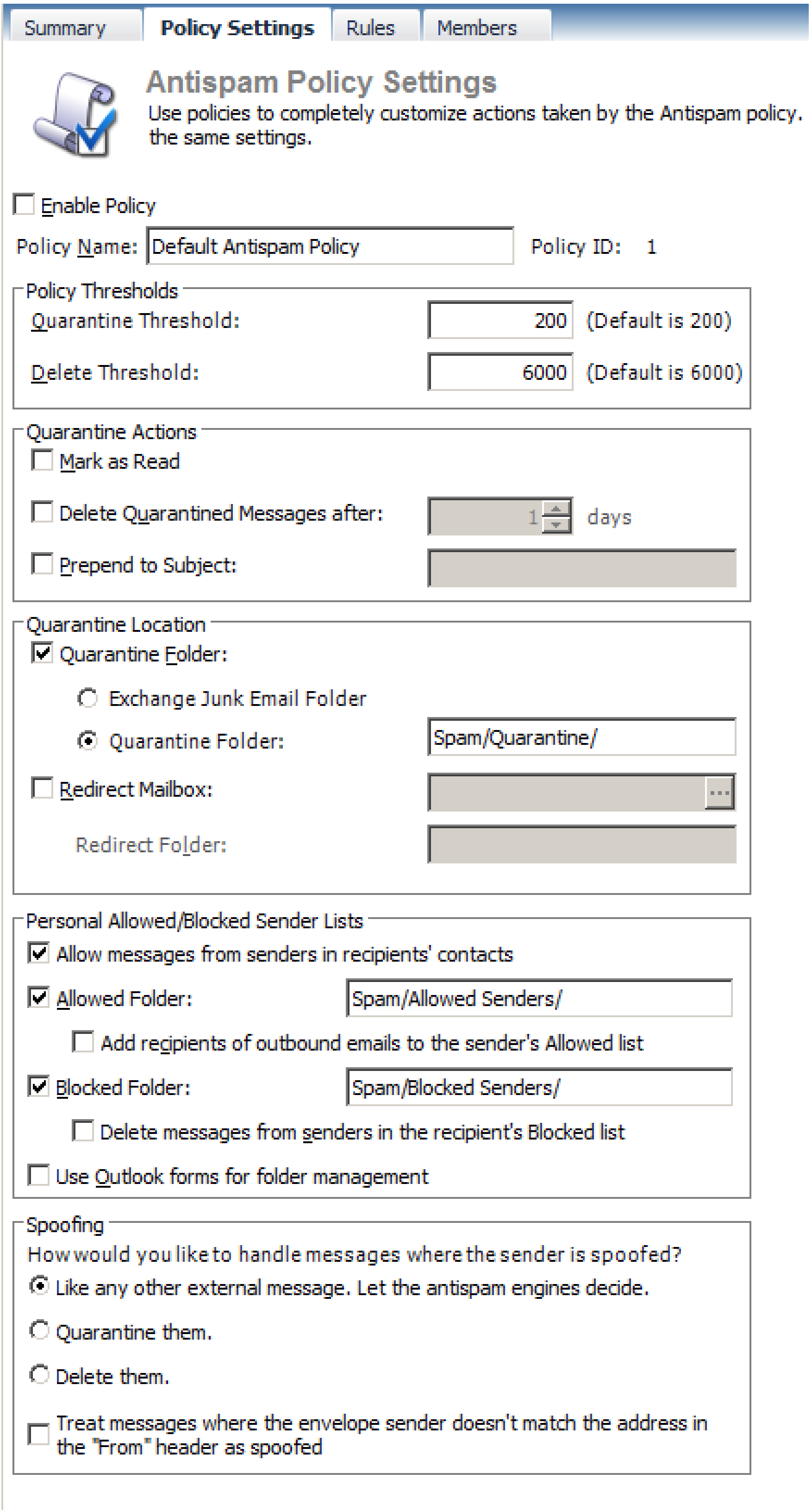
7. Click **Search**. VIPRE searches the member database based on the selected criteria; then, returns the results in the table below.

4.4 Managing Antispam Policies

A policy is a group of recipients who share the same settings and configurations. Use this section to customize individual antispam policies. All recipients are assigned to a default policy until they are re-assigned to a new one.

To configure individual Antispam policy settings

1. Select **Policies & Recipients**; then, the antispam policy you want to manage from the left pane. The Summary tab opens in the right pane.
2. Click the **Policy Settings** tab.



Antispam Policy Settings

Use policies to completely customize actions taken by the Antispam policy.
the same settings.

□ Enable Policy

Policy Name: Default Antispam Policy   Policy ID: 1

Policy Thresholds

Quarantine Threshold: 200 (Default is 200)

Delete Threshold: 6000 (Default is 6000)

Quarantine Actions

□ Mark as Read

□ Delete Quarantined Messages after: 1 days

□ Prepend to Subject:

Quarantine Location

☑ Quarantine Folder:

○ Exchange Junk Email Folder

● Quarantine Folder: Spam/Quarantine/

□ Redirect Mailbox:

Redirect Folder:

Personal Allowed/Blocked Sender Lists

☑ Allow messages from senders in recipients' contacts

☑ Allowed Folder: Spam/Allowed Senders/

□ Add recipients of outbound emails to the sender's Allowed list

☑ Blocked Folder: Spam/Blocked Senders/

□ Delete messages from senders in the recipient's Blocked list

□ Use Outlook forms for folder management

Spoofing

How would you like to handle messages where the sender is spoofed?

● Like any other external message. Let the antispam engines decide.

○ Quarantine them.

○ Delete them.

□ Treat messages where the envelope sender doesn't match the address in the "From" header as spoofed

Screenshot 29: Antispam Policy Settings

3. To enable the policy, select the **Enable Policy** check box.
4. Type the name of the policy in the **Policy Name** field.
5. Under **Policy Thresholds**, type the maximum spam score messages can attain before they are quarantined and deleted in the **Quarantine** and **Delete Threshold** fields.

The defaults are 200 and 6000 respectively. The value of 200 is how many points on a spam message it has to accumulate in order to break the "Is Spam" threshold. The 6000 value means that message that get scored that high will be completely deleted instead of being quarantined.

6. Make a selection under **Quarantine Actions**:

To show the quarantined email as having been read:

- Select the **Mark as Read** check box.

To delete quarantined messages after a certain number of days:

- Select the **Delete Quarantined Messages after...days** check box; then, type the number of days in the available field.

To add a text tag to the beginning of the quarantined message subject line:

- Select **Prepend to Subject** check box; then, type the text in the available field.

7. Make a selection under **Quarantine Location**:

To set a specific folder for quarantined messages:

- Select the **Quarantine Folder** check box; then type the folder in the available field.

To redirect quarantined messages to another mailbox:

- Select the **Redirect Mailbox** check box; then, type the name of the mailbox in the available field.

To redirect mail to a specific folder with in a redirected mailbox:

- Select the **Redirect Mailbox** check box, type the name of the mailbox; then, type the name of the folder in the **Redirect Folder** box.

8. Make a selection under **Personal Allowed/Blocked Sender Lists**:

To allow messages from senders in recipients' contacts:

- Select the **Allow messages from senders in recipients' contacts** check box.

To set a folder for allowed senders:

Select the **Allowed Folder** check box; then type the name and location for the folder in the available field.

To automatically add recipients of outbound emails to the Allowed senders list:

Select the **Add recipients of outbound messages to the sender’s Allowed list** check box.

To set a folder for allowed senders:

Select the **Blocked Folder** check box; then type the name and location for the folder in the available field.

To automatically delete messages from addresses in the Blocked Senders list:

Select the **Delete messages from senders in users' Blocked lists** check box.

To use Outlook forms to manage your folders:

Select the **Use Outlook forms for folder management** check box.

> Out of office replies written in English are not added to the Allowed Senders list.

9. Make a selection under **Spoofing** for how you would like to handle messages where the sender is spoofed:

To treat it like any other external message and let the antispam engine decide:

- Select the Like any other external message. Let the antispam engine decide.

To quarantine the spoofed messages:

- Select the Quarantine them.

To delete the spoofed messages:

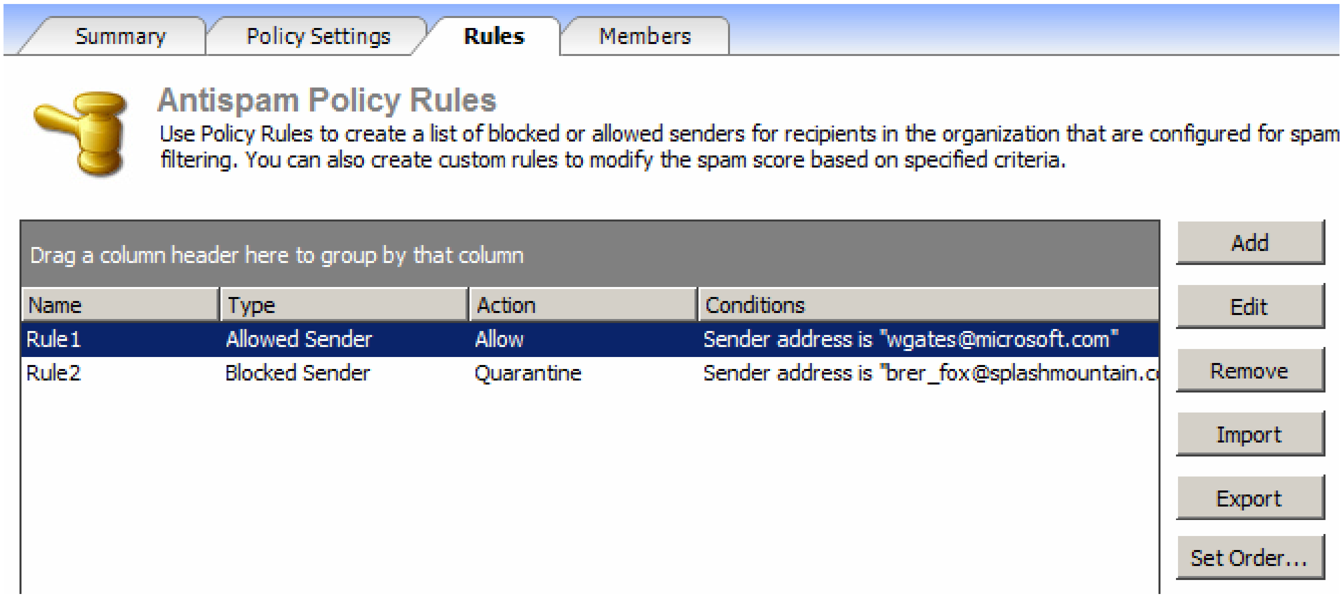
- Delete them.

To treat a mismatched envelope sender and From header as spoofed:

- Select the **Treat messages where the envelope sender doesn't match the address in the "From" header as spoofed** check box.

To manage individual Antispam policy rules

1. Select **Policies & Recipients**; then, the **Antispam** policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Rules** tab.



Antispam Policy Rules

Use Policy Rules to create a list of blocked or allowed senders for recipients in the organization that are configured for spam filtering. You can also create custom rules to modify the spam score based on specified criteria.

Drag a column header here to group by that column

Name	Type	Action	Conditions
Rule1	Allowed Sender	Allow	Sender address is "wgates@microsoft.com"
Rule2	Blocked Sender	Quarantine	Sender address is "brer_fox@splashmountain.c

Screenshot 30: Antispam Policy Rules

3. Make a selection:

To add a new rule:

- Click **Add**. The **Rule Wizard** opens. Go to To add a policy rule using the Rule Wizard.

To edit an existing rule:

- Click **Edit**. The **Rule Wizard** opens. Go to To edit a policy rule using the Rule Wizard.

To delete a rule:

- Click **Remove**. The rule is removed from the list.

To import a rule from an XML file:

- Click **Import**. For example, if VIPRE created a rule for our customers, we could place it in a centralized location for them to retrieve it.

To export a rule to an XML file:

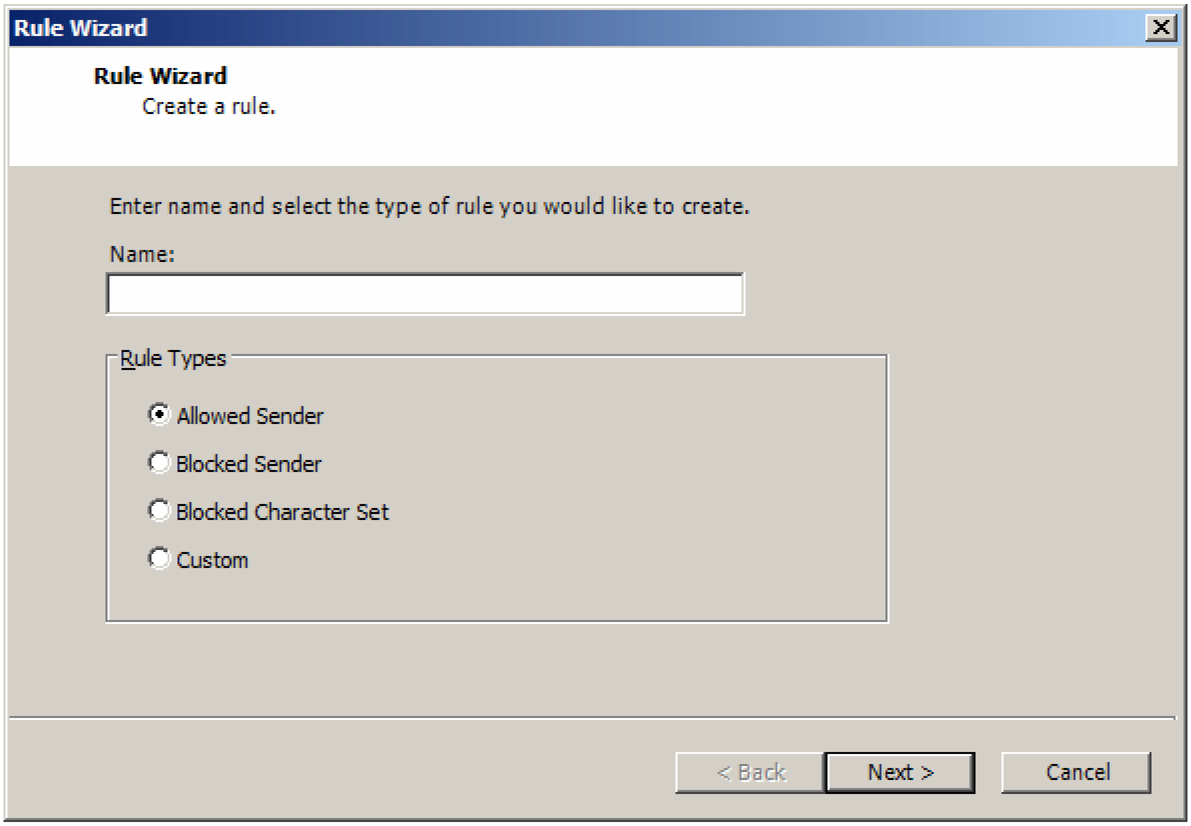
- Click **Export**.

To set the order of the listed rules:

- Click **Set Order...**.

To add a policy rule using the Rule Wizard

1. Select **Policies & Recipients**; then, the **Antispam** policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Rules** tab.
3. Click **Add**. The **Rule Wizard** opens.



Rule Wizard

Rule Wizard

Create a rule.

Enter name and select the type of rule you would like to create.

Name:

Rule Types

● Allowed Sender

○ Blocked Sender

○ Blocked Character Set

○ Custom

Screenshot 31: Rules Wizard

4. Type a name for the new rule in the **Name** field.
5. Make a selection:

To allow mail from the email address specified on the next wizard dialog box:

- Select **Allowed Sender**.

To block mail from the email address specified on the next wizard dialog box:

- Select **Blocked Sender**.

To block mail using a specific character set:

- Select **Blocked Character Set**.

To create a custom filter rule:

- Select **Custom**.

6. Click **Next**.
7. Make a selection:

If you selected Allowed Sender in the first wizard dialog box:

- Type the email address(s) from which you want to receive email in the Allowed Senders box.

If you selected Blocked Sender in the first wizard dialog box:

- Type the email address(s) from which you do not want to receive email in the Blocked Senders box, click Next; then, select whether the emails will be quarantined or deleted.

If you selected Blocked Character Set in the first wizard dialog box:

- Click Add, select the character set(s) from the Add Blocked Character Sets dialog box, click Next; then, select whether the emails containing the selected character sets will be quarantined or deleted.

If you selected Custom in the first wizard dialog box:

- Select the search parameters that the rule will apply to the policy from the Fields, Search Type, and Value fields; then, select the action to apply to the rule.

8. Click **Finish**. The rule is added to the table.

To edit a policy rule using the Rule Wizard

1. Select **Policies & Recipients**; then, the **Antispam** policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Rules** tab.
3. Select a rule.
4. Click **Edit**. The **Rule Wizard** opens. Notice that only the **Name** field is editable on this window.
5. Click **Next**.
6. Edit the parameters as necessary.
7. **Click** Finish.

To view list members for a specific antispam policy

1. Select **Policies & Recipients**; then, the **Antispam** policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Members** tab.
3. Select the criteria by which you want to list the search results from the **SearchField** drop-list. The **Search Type** drop-list and **Search Value** field become active.
4. Make a selection:

To perform a search that contains some or all of the text typed in the Search Value field:

- Select **Contains from the Search Type** drop-list.

To perform a search that exactly matches the text typed in the Search Value field:

- Select **Equals from the Search Type** drop-list.

5. Type a value In the **Search Value** field that will contain or exactly match your search criteria.
6. Make a selection:

To search for members by policy type:

- Select the policy type from the **Policy Type** drop-list.

To search for members by the name of the policy:

- Select the name of the policy from the **Policy Name** Drop-list.

To receive only up to a specific number of results:

- Select or type the number in the **Maximum Results** box.

7. Click **Search**. VIPRE searches the member database based on the selected criteria; then, returns the results in the table below.

4.5 Managing Global Antivirus Activity

Use this section to manage Antivirus activity for users receiving email on your network and configure options that affect all recipients configured for virus filtering. However, before we explain how to manage your antivirus settings and notifications, it is important that you understand how the Antivirus plug-in operates.

The Antivirus Plug-in

The AV Plug-in tests to see if the installation is licensed (including evaluation mode). VIPRE will scan your network in licensed or in evaluation mode.

> If the Antivirus Plug-in is not licensed, the virus definitions will not be updated. In this case, the Antivirus Plug-in is less effective.

Next, VIPRE verifies that the Plug-in is enabled. Enable the Plug-in by selecting the **Enable Antivirus** check box on the Global Settings tab located under the Antivirus section of the Console. If the **Enable Antivirus** check box is not selected, the Plug-in is not enabled and VIPRE does not scan the requested MIME part or attachment from the Store.

If the **Enable Antivirus** check box is selected, the Plug-in scans the MIME part or attachment through each of the active Antivirus Engines. Currently, VIPRE ships with two commercial antivirus engines: Bitdefender and VIPRE. The status of each antivirus engine can be viewed and set in the Antivirus Engines section of the Global Antivirus Settings. Selecting the desired engine; then, click the Activate or Deactivate button to set an antivirus engine to Active or Inactive. Both antivirus engines are active by default.

VIPRE (Virus Intrusion Protection Remediation Engine) is an antivirus and antispyware detection engine that uses a proprietary technology without building on older generation antivirus engines. The engine uses multiple techniques to inspect the characteristics of all types of potentially threatening files. From simple signature-based detection to dynamic, sophisticated analysis of malware files, the engine quickly determines whether a file is good or bad—enabling comprehensive detection of both existing and new unidentified threats.

Managing global antivirus settings

1. Select **Policies & Recipients**; then, **Antivirus**. The **Summary** tab opens in the right pane
2. Click the **Global Settings** tab.

To enable global antivirus filtering:

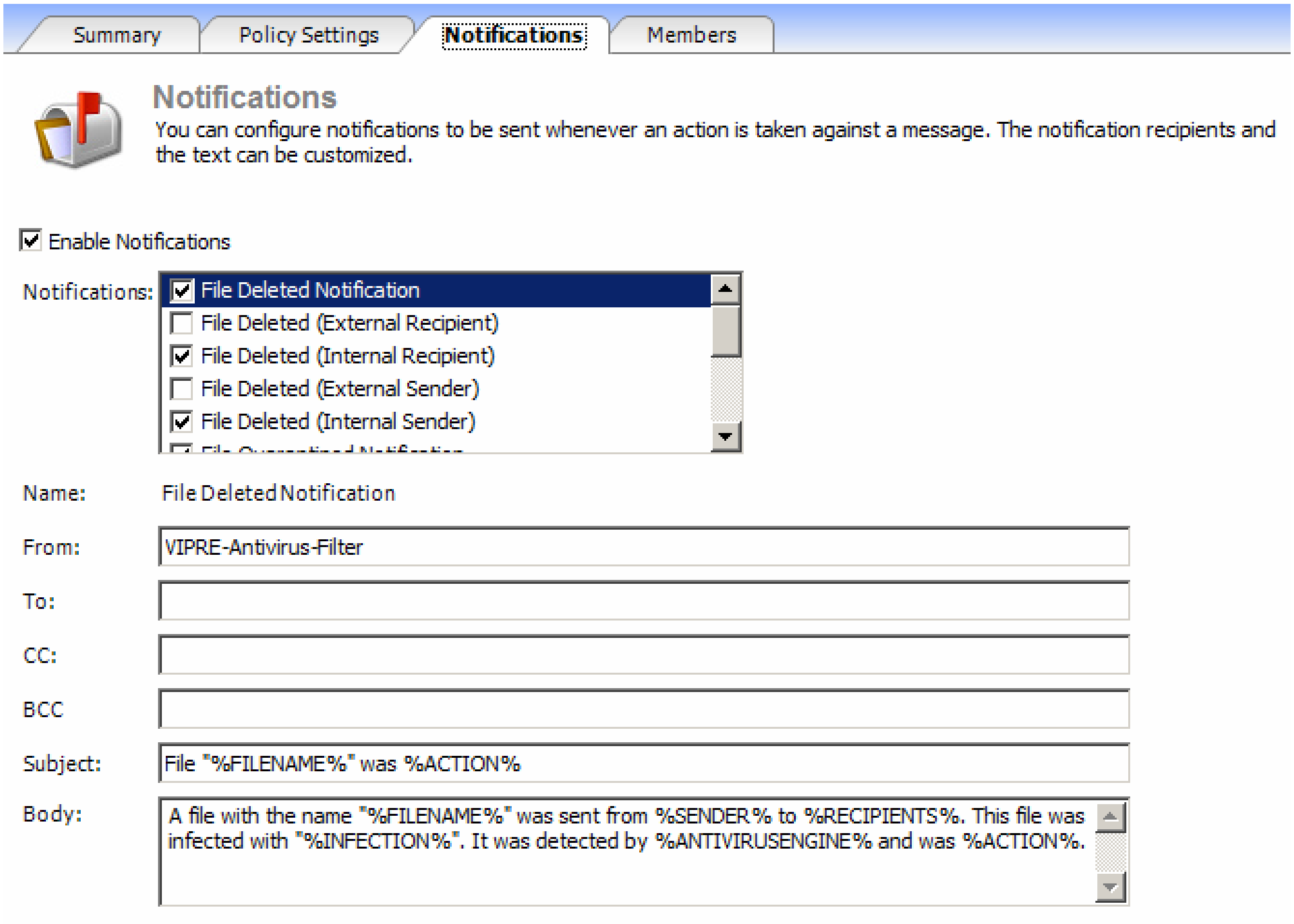
- Select the **Enable Antivirus** check box.

Additionally, you may also enable the following options:

- **Scan all emails from external senders** - enabling this option will apply the default AV policy to emails sent from external senders, regardless of the recipient.
- **Scan all emails to external recipients** - enabling this option will apply the default AV policy to emails sent to external recipients, regardless of the sender.

To set the notifications sent when an action is taken against a message

1. Select **Policies & Recipients**; then, select a policy under **Antivirus** in the left pane. The **Summary** tab opens in the right pane.
2. Click the **Notifications** tab.



Notifications

You can configure notifications to be sent whenever an action is taken against a message. The notification recipients and the text can be customized.

☑ Enable Notifications

Notifications:
☑ File Deleted Notification
☐ File Deleted (External Recipient)
☑ File Deleted (Internal Recipient)
☐ File Deleted (External Sender)
☑ File Deleted (Internal Sender)
☑ File Quarantined Notification

Name: File Deleted Notification

From: VIPRE-Antivirus-Filter

To:

CC:

BCC

Subject: File "%FILENAME%" was %ACTION%

Body: A file with the name "%FILENAME%" was sent from %SENDER% to %RECIPIENTS%. This file was infected with "%INFECTION%". It was detected by %ANTIVIRUSENGINE% and was %ACTION%.

Screenshot 32: Antivirus policy notifications settings

3. To enable notifications for antivirus activity, select the **Enable notifications** check box; then, select the type of notification from the **Notifications** check box list.

4. Verify or edit the information below the **Notifications** check box list. For example, if you selected **Message Body Part Deleted**, verify or edit the information in the **From**, **To**, **Subject**, **CC**, and **BCC**, fields. We recommend that you leave the default text in the **Body** field.

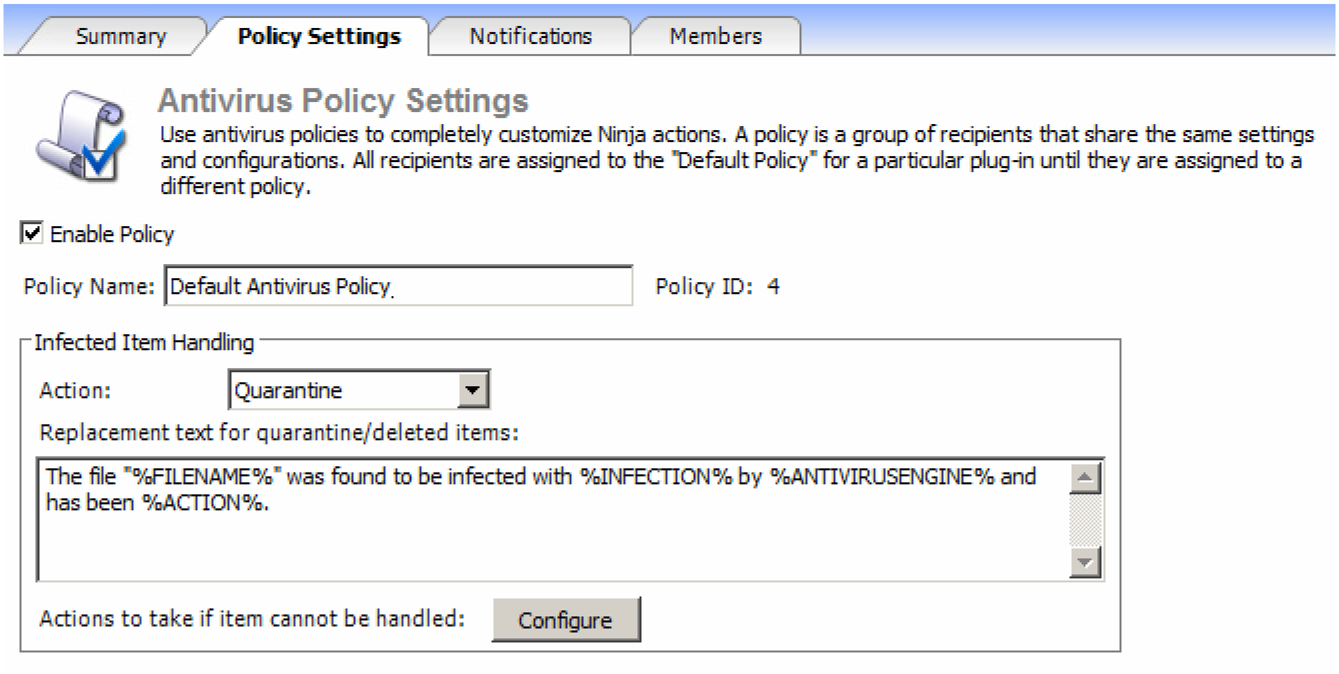
> You must select a check box in the Notifications check box list to enable the fields below.

Managing Antivirus Policies

A policy is a group of recipients who share the same settings and configurations. Use this section to customize individual antivirus policies. All recipients are assigned to a default policy until they are reassigned to a new one.

To configure individual Antispam policy settings

1. Select **Policies & Recipients**; then, the antivirus policy you want to manage from the left pane. The Summary tab opens in the right pane.
2. Click the **Policy Settings** tab.



Antivirus Policy Settings

Use antivirus policies to completely customize Ninja actions. A policy is a group of recipients that share the same settings and configurations. All recipients are assigned to the "Default Policy" for a particular plug-in until they are assigned to a different policy.

☑ Enable Policy

Policy Name: Default Antivirus Policy Policy ID: 4

Infected Item Handling

Action: Quarantine

Replacement text for quarantine/deleted items:

The file "%FILENAME%" was found to be infected with %INFECTION% by %ANTIVIRUSENGINE% and has been %ACTION%.

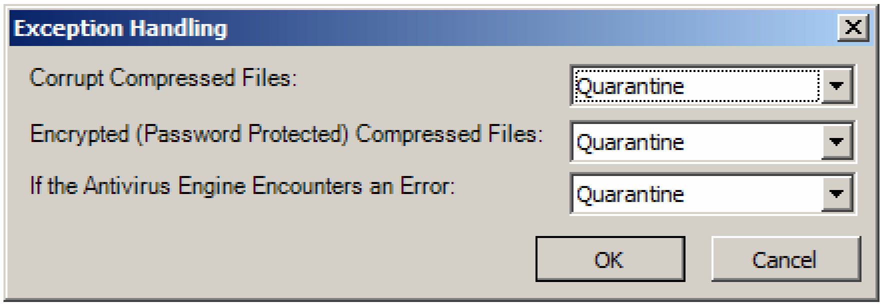
Actions to take if item cannot be handled:

Screenshot 33: Antivirus policy settings tab

3. To enable the policy, select the **Enable Policy** check box.
4. Type the name of the policy in the **Policy Name** field.
5. Under **Infected Item Handling**, select the desired action when a threat is discovered in an email. VIPRE can either quarantine or delete the email. Note: quarantined threats are not delivered to the user’s spam quarantine, but to a central quarantine on the server. This will prevent users from inad-

vertently pulling a threat from the spam quarantine folder, and give the administrator the ability to control the environment.

6. Configure **Actions to take if item cannot be handled**. IF VIPRE cannot scan a file properly, you can choose the action to take. The options are
   - Deliver
   - Quarantine
   - Delete



Exception Handling

Corrupt Compressed Files: Quarantine

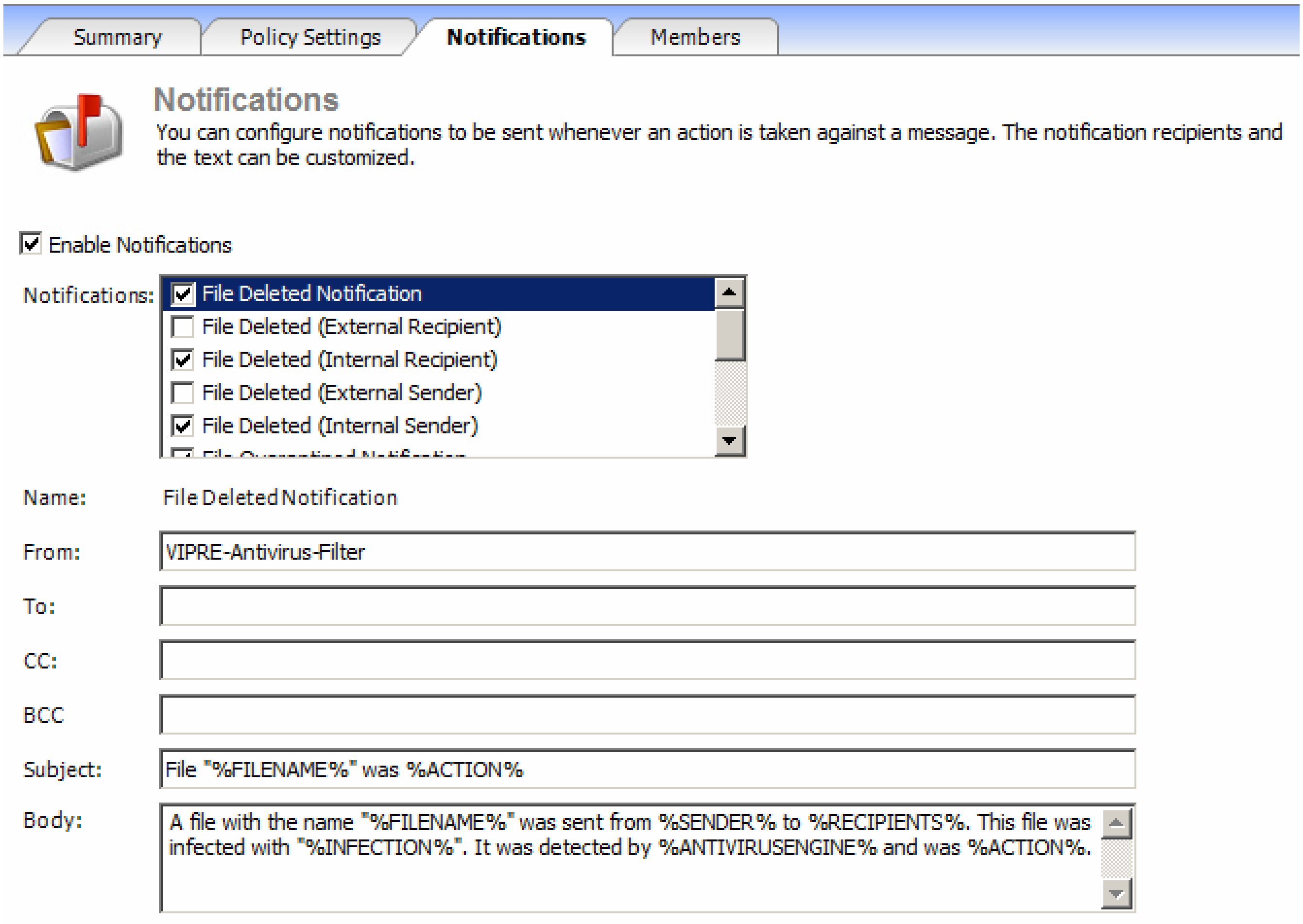
Encrypted (Password Protected) Compressed Files: Quarantine

If the Antivirus Engine Encounters an Error: Quarantine

Screenshot 34: Exception Handling configuration for Antivirus policy

To set the notifications sent when an action is taken against a message

1. Click the **Notifications** tab.



Notifications

You can configure notifications to be sent whenever an action is taken against a message. The notification recipients and the text can be customized.

☑ Enable Notifications

Notifications:

☑ File Deleted Notification
☐ File Deleted (External Recipient)
☑ File Deleted (Internal Recipient)
☐ File Deleted (External Sender)
☑ File Deleted (Internal Sender)
File Quarantined Notification

Name:	File Deleted Notification
From:	VIPRE-Antivirus-Filter
To:	
CC:	
BCC	
Subject:	File "%FILENAME%" was %ACTION%
Body:	A file with the name "%FILENAME%" was sent from %SENDER% to %RECIPIENTS%. This file was infected with "%INFECTION%". It was detected by %ANTIVIRUSENGINE% and was %ACTION%.

Screenshot 35: Notifications configuration for Antivirus policy

2. To enable notifications for antivirus activity, select the **Enable notifications** check box; then, select the type of notification from the **Notifications** check box list.
3. Verify or edit the information below the Notifications check box list. For example, if you selected Message Body Part Deleted, verify or edit the information in the **From**, **To**, **Subject**, **CC**, and **BCC**, fields. We recommend that you leave the default text in the **Body** field.

4.6 Managing Global Attachment Filtering

Use this section to customize recipient attachment filtering settings.

The Attachment Filter Plug-in

VIPRE employs the Attachment Filtering plug-in to administer and control email traffic that contains messages with attachments. This plug-in has a policy based architecture, thus, allowing VIPRE administrators to assign different Active Directory Users, Distribution lists, and mail-enabled public folders to specific policies.

Global Attachment Filter Settings and Rules

Global settings and global rules automatically take effect for all policy members.Global rules provide administrators with control over attachment traffic in the domain for all mail enabled users on all policies listed for the specific plug-in. The important part of global rules is to specify the direction (e-mail path) of the message to which the rule is applicable. Go to To manage global attachment filter settings.

An administrator can also customize filtering by using regular expressions. For example, “[M]” will perform selected actions on all file attachments with a letter “M” in the attachment file name. By creating this global rule all existing policy rules are affected.

> ℹ If a rule is activated for an attachment, no other rules will apply to that attachment.

Policy Settings and Rules

Attachment Filter Policies enable administrators to customize actions for attached files in specific recipient groups assigned to a particular policy. Policy members can be AD Users, Distribution Groups and Mail Enabled Public Folders. Every policy consists of a set of rules and every rule has a custom action for specific email attachments. Policy rules are run in the order they are positioned on the Rules tab. All rules are applied to the members of the policy. When a rule is matched for an attachment, the Attachment Filter stops processing rules for that specific attachment file. The main difference between Policy rules and global rules is that one runs at global level for all polices and policy rules only run for specific groups.

S.M.A.R.T. Detection

The Suspicious Mail Attachment Removal Technology (S.M.A.R.T) filter scans the header of a file to verify that an attachment is what it says it is and has not just been renamed. For example: An administrator creates a new policy called “Quarantine all zip” to quarantine all zip files sent internally; then, selects S.M.A.R.T. Detection. Now, if a user listed on the policy sends a renamed zip file internally, the Attachment Filter plug-in recognizes it as an zip file and applies the specified action to it.

Imbedded Email Attachments

When one email is embedded inside another, attachment filtering treats it as a special attachment by looking at the extension of the email attachment (should have ‘*.eml’ extension). Attachment filtering looks inside the embedded email to see if it meets certain requirements. If an embedded email meets these requirements, Attachment filtering treats it as another email, applying policies and rules to its attachments as it would with a regular email.

Notifications

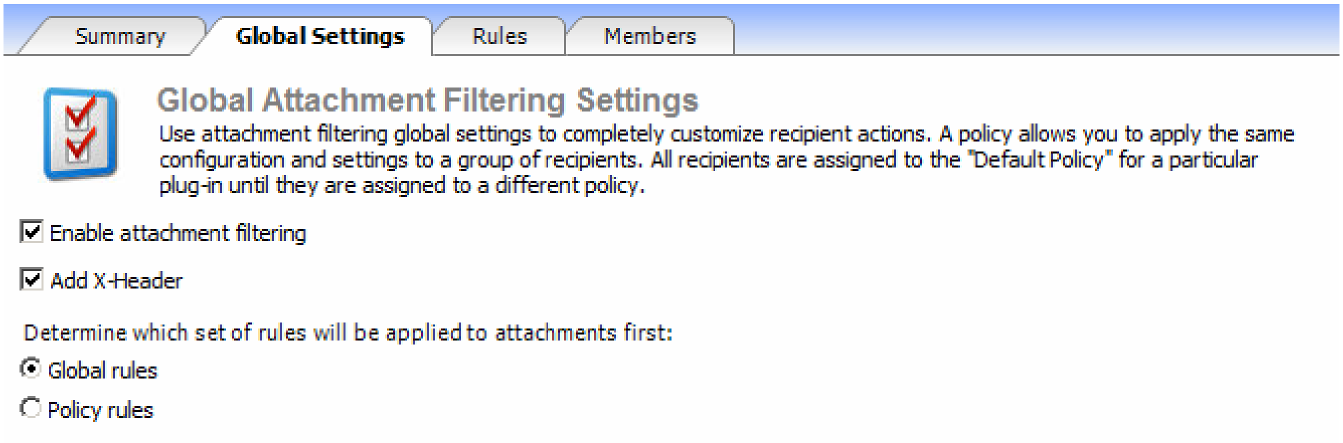
Every time Attachment filtering matches one of the policy rules with an email that contains an attachment, a notification email can be sent to inform recipients about the action taken for that particular rule. Notifications are policy based, meaning that every policy can have its own Notifications configured. Notifications are generated for the first rule that matches the attachment.

X-Headers

X-Headers are used to insert user-defined header fields into an e-mail message. However, they are ignored by messaging servers and applications that don't use them. X-Headers can contain delivery information such as the sender, recipients, and source the IP address.

To manage global attachment filter settings

1. Select **Policies & Recipients**; then, **Attachment Filter**. The **Summary** tab opens in the right pane.
2. Click the **Global Settings** tab.



Global Attachment Filtering Settings

Use attachment filtering global settings to completely customize recipient actions. A policy allows you to apply the same configuration and settings to a group of recipients. All recipients are assigned to the "Default Policy" for a particular plug-in until they are assigned to a different policy.

☑ Enable attachment filtering

☑ Add X-Header

Determine which set of rules will be applied to attachments first:

● Global rules

○ Policy rules

Screenshot 36: Attachment Filter - Global Settings Tab

Make a selection:

To enable global attachment filtering for all policies:

- Select the **Enable Attachment Filtering** check box.

To add headers for all attachment filter policies:

- Select the **Add X-Headers** check box.

To determine which set of rules will be applied to attachments first:

- Select the **Global rules** or **Policy rules** button.

To manage global rules for attachment filters

1. Select **Policies & Recipients**; then, **Attachment Filter**; then, click the **Rules** tab.
2. To add a rule for a file extension, click **Add**. The **Attachment Filter Rule** dialog box opens. Go to Step 4.
3. Make a selection:

To edit the name or email address for a rule in the list:

- Select the rule; then, click **Edit**. Go to To edit a rule.

To delete a rule:

- Select the rule; then, click **Remove**.

4. Make a selection:

To import a rule:

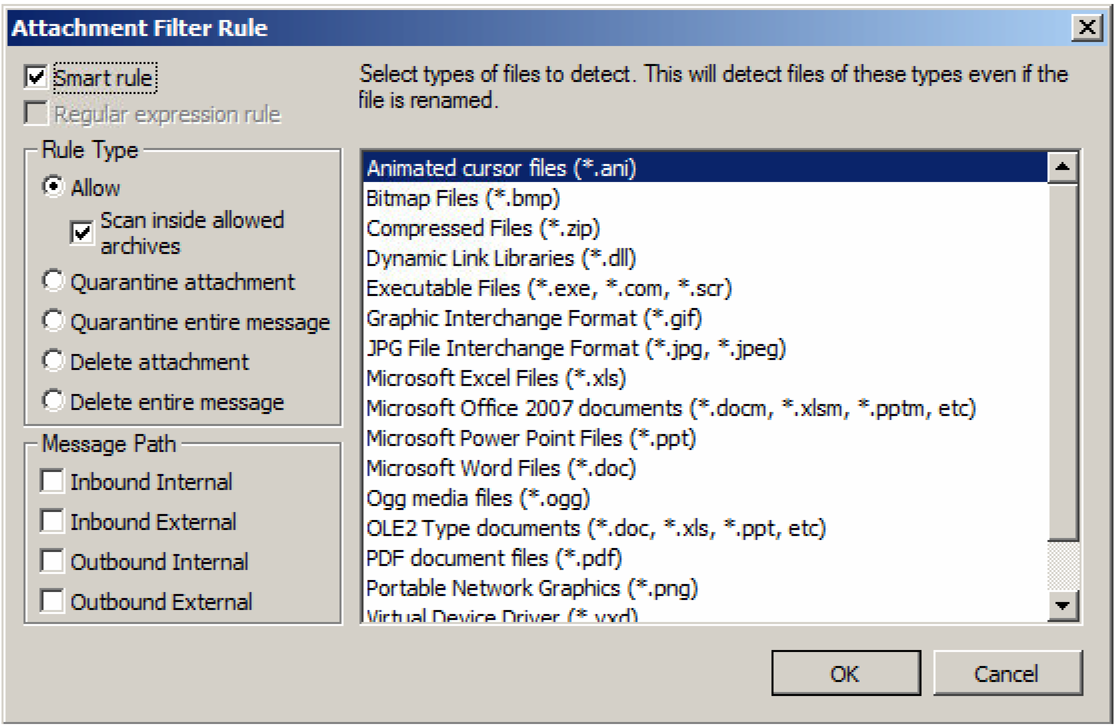
- Click **Import**. For example, if VIPRE created a rule for our customers, we could place it in a centralized location for them to retrieve it.

To export a rule:

- Click **Export**.

To add a rule

1. Select **Policies & Recipients**; then, **Attachment** Filter. The **Summary** tab opens in the right pane.
2. Click the **Rules tab**; then click **Add**. The **Attachment Filter Rule** dialog box opens.



Attachment Filter Rule

☑ Smart rule
□ Regular expression rule

Rule Type
● Allow
☑ Scan inside allowed archives
○ Quarantine attachment
○ Quarantine entire message
○ Delete attachment
○ Delete entire message

Message Path
□ Inbound Internal
□ Inbound External
□ Outbound Internal
□ Outbound External

Select types of files to detect. This will detect files of these types even if the file is renamed.

Animated cursor files (*.ani)
Bitmap Files (*.bmp)
Compressed Files (*.zip)
Dynamic Link Libraries (*.dll)
Executable Files (*.exe, *.com, *.scr)
Graphic Interchange Format (*.gif)
JPG File Interchange Format (*.jpg, *.jpeg)
Microsoft Excel Files (*.xls)
Microsoft Office 2007 documents (*.docm, *.xlsm, *.pptm, etc)
Microsoft Power Point Files (*.ppt)
Microsoft Word Files (*.doc)
Ogg media files (*.ogg)
OLE2 Type documents (*.doc, *.xls, *.ppt, etc)
PDF document files (*.pdf)
Portable Network Graphics (*.png)
Virtual Device Driver (*.vxd)

Screenshot 37: Rules Wizard

Make a selection:

To use S.M.A.R.T. rule filtering:

- Check the **Smart rule** check box.

To use regular expressions:

- Check the **Use regular expressions** check box.

Make a selection under Rule Type:

> ℹ If a rule is activated for an attachment, no other rules will apply to that attachment.

To allow a file attachment:

- Select **Allow**; then, type the character pattern that matches the file name in the box on the right.

To unpack the archived file and to have the rules run against the contents of the archived file:

- Select the **Scan inside allowed archives** check box.

To quarantine attachments:

- Select the **Quarantine attachment** check box.

To quarantine the entire email message:

- Select the **Quarantine entire message** check box.

To delete the attachment:

- Select the **Delete attachment** check box.

To delete the entire message:

- Select the **Delete entire message** check box.

Make a selection under Message Path:

To apply the rule while processing inbound messages sent within the company:

- Select the **Inbound Internal** check box.

To apply the rule while processing inbound messages sent from outside the company:

- Select the **Inbound External** check box.

To apply the rule while processing outbound messages sent within the company:

- Select the **Outbound Internal** check box.

To apply the rule while processing outbound messages sent out of the company:

a. Select the **Outbound External** check box.
b. Click **OK**. The rule is added to the table.

To edit a rule

1. Select **Policies & Recipients**; then, **Attachment Filter**. The **Summary** tab opens in the right pane.
2. Click the **Rules tab**; then, click **Edit**. The **Attachment Filter Rule** dialog box opens.
3. Select the rule.
4. Edit the rule parameters that you want to change; then, click **OK**.

To view a global list of attachment filter policy members

1. Select **Policies & Recipients**; then, **Attachment Filter** from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Members** tab.
3. Select the criteria by which you want to list the search results from the **Search Field** drop-list. The **Search Type** drop-list and **Search Value** field become active.
4. Make a selection:

   To perform a search that contains some or all of the text typed in the Search Value field:

   - Select **Contains from the Search Type** drop-list.

   To perform a search that exactly matches the text typed in the Search Value field:

   - Select **Equals from the Search Type** drop-list.

5. Type a value In the **Search Value** field that will contain or exactly match your search criteria.
6. Make a selection:

   To search for members by policy type:

   - Select the policy type from the **Policy Type** drop-list.

   To search for members by the name of the policy:

   - Select the name of the policy from the **Policy Name** drop-list.

   To receive only up to a specific number of results:

   - Select or type the number in the **Maximum Results** box.

7. Click **Search**. VIPRE searches the member database based on the selected criteria; then, returns the results in the table below.

4.7 Managing Attachment Filtering Policies

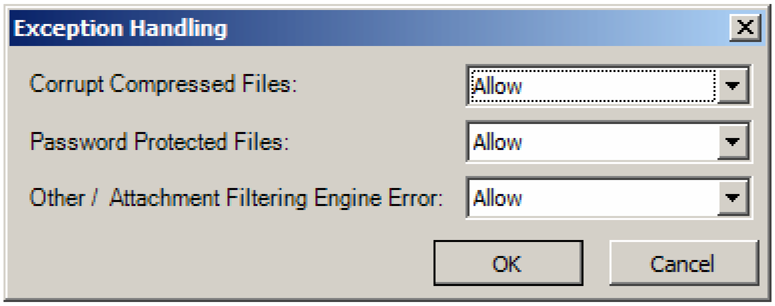
Use this section to learn how to customize attachment filter policies. All recipients are assigned to a default policy until they are re-assigned to a new one.

To configure individual Attachment Filter policy settings

1. Select **Policies & Recipients**; then, an attachment filter policy from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Policy Settings** tab.
3. To enable the policy, select the **Enable Policy** check box.
4. Type the name of the policy in the **Policy Name** field.
5. To specify the text that replaces quarantine or deleted attachments, type the replacement text in the box labeled Replacement text for quarantined items.
6. To set alternative actions for messages that cannot be processed, click **Configure**.

To configure alternative actions for messages that cannot be handled

1. Click the **Policy Settings** tab.
2. To enable the policy, select the **Enable Policy** check box.
3. Click **Configure** next to **Actions to take if message cannot be handled**. The **Exception Handling** dialog box opens.



Exception Handling

Corrupt Compressed Files: Allow

Password Protected Files: Allow

Other / Attachment Filtering Engine Error: Allow

Screenshot 38: Exception Handling

4. Make a selection:

To set an action for compressed files that have been corrupted:

- Select an action from the Corrupt Compressed Files drop-list.

To set an action for files that are protected by a password:

- Select an action from the Password Protected Files drop-list.

To set an action for other types of anomalies, like attachment filtering engine errors:

- Select an action from the Other / Attachment Filtering Engine Error drop-list.

5. Click **OK**.

To manage rules for attachment filter policies

1. Select **Policies & Recipients**; then, an **Attachment Filter** policy. The **Summary** tab opens in the right pane.
2. Click the **Rules** tab.
3. Make a selection:

To move an item up the list:

- Select an item in the list; then click **Up**.

To move an item down the list:

- Select an item in the list; then click **Down**.

4. Make a selection:

To add a rule for a file extension:

- Select **Add**. The **Attachment Filter Rule** dialog box opens. Go to To add an attachment filter rule to a policy.

To edit the name or email address for a rule in the list:

- Select **Edit**. The **Attachment Filter Rule** dialog box opens. Go to To add an attachment filter rule to a policy.

To delete a rule:

- Select **Remove**. The rule is removed from the list.

To import a rule:

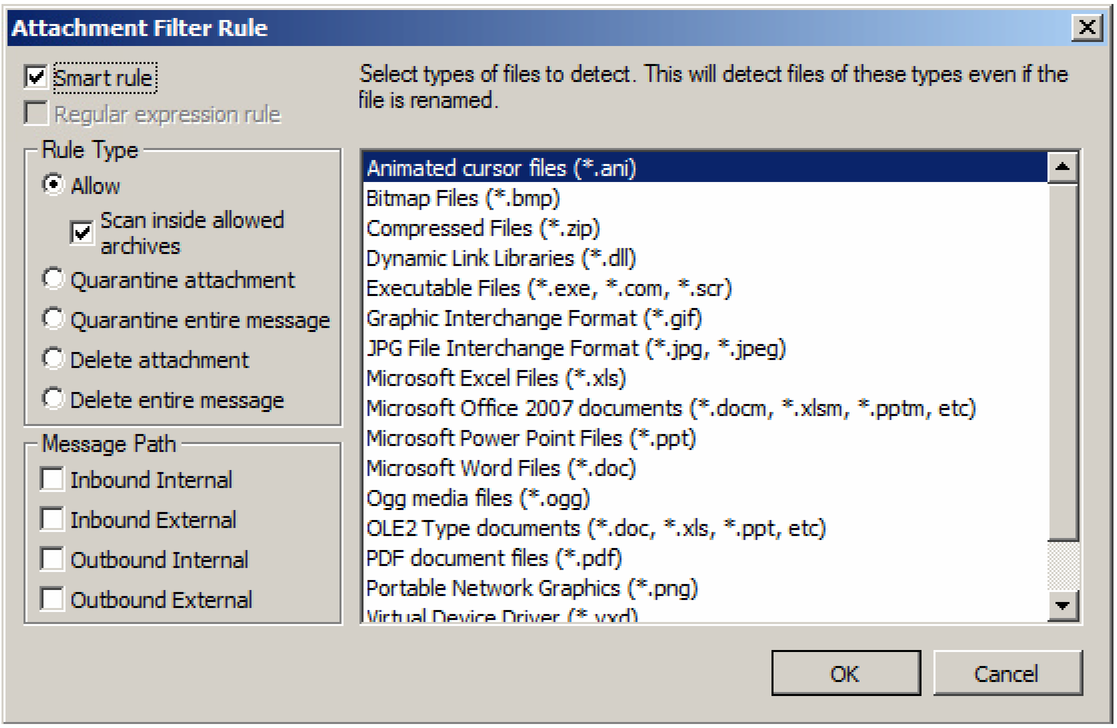
- Select **Import**. For example, if VIPRE created a rule for our customers, we could place it in a centralized location for them to retrieve it.

To export a rule:

- Select **Export**.

To add an attachment filter rule to a policy

1. Select **Policies & Recipients**; then, **Attachment Filter**. The **Summary** tab opens in the right pane.
2. Click the **Rules** tab.
3. Click **Add**. The **Attachment Filter Rule** dialog box opens.



☑ Smart rule

□ Regular expression rule

Select types of files to detect. This will detect files of these types even if the file is renamed.

Rule Type

● Allow

☑ Scan inside allowed archives

○ Quarantine attachment

○ Quarantine entire message

○ Delete attachment

○ Delete entire message

Message Path

□ Inbound Internal

□ Inbound External

□ Outbound Internal

□ Outbound External

Animated cursor files (*.ani)
Bitmap Files (*.bmp)
Compressed Files (*.zip)
Dynamic Link Libraries (*.dll)
Executable Files (*.exe, *.com, *.scr)
Graphic Interchange Format (*.gif)
JPG File Interchange Format (*.jpg, *.jpeg)
Microsoft Excel Files (*.xls)
Microsoft Office 2007 documents (*.docm, *.xlsm, *.pptm, etc)
Microsoft Power Point Files (*.ppt)
Microsoft Word Files (*.doc)
Ogg media files (*.ogg)
OLE2 Type documents (*.doc, *.xls, *.ppt, etc)
PDF document files (*.pdf)
Portable Network Graphics (*.png)
Virtual Device Driver (*.vxd)

Screenshot 39: Attachment Filter Rule selection

4. Select **Smart rule** and select types of files to detect, which will detect files of these types even if the file is renamed.
   -or-
   Select **Regular expression rule** and enter the file names you would like to create rules for.
5. Make a selection under Rule Type:

To allow a file extension:

- Select the **Allow** radio button; then, type the character pattern that matches the file name in the box on the right. Optionally, select the **Scan inside allowed archives** check box to unpack the archived file and to have the rules run against the contents of the archived file.

To block a file attachment or the entire message:

- Select the either of the two **Quarantine** or **Delete** options for the blocked attachment; then, type the character pattern that matches the file name in the box on the right.

6. Make a selection under Message Path:

To apply the rule while processing inbound messages sent within the company:

- Select the **Inbound Internal** check box.

To apply the rule while processing inbound messages sent from outside the company:

- Select the **Inbound External** check box.

To apply the rule while processing outbound messages sent within the company:

- Select the **Outbound Internal** check box.

To apply the rule while processing outbound messages sent out of the company:

- Select the **Outbound External** check box.

7. Click **OK**. The rule is added to the table.

To edit a rule

1. Select **Policies & Recipients**; then, an **Attachment Filter** policy. The **Summary** tab opens in the right pane.
2. Click the **Rules** tab.
3. Select a rule.
4. Click **Edit**. The **Attachment Filter Rule** dialog box opens.
5. Edit the rule parameters that you want to change.
6. Click **OK**.

To set the notifications sent when an action is taken against a message

1. Select **Policies & Recipients**; then, the attachment filter policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Notifications** tab.

3. To enable notifications for this policy, select the **Enable notifications** check box.
4. Select all the actions that you want to trigger a notification and the recipients of the notifications from the **Notifications** list.
5. Verify or edit the information relating to the selection from the **Notifications** check box list. For example, if you selected *File Deleted (Notify Postmaster)*, verify or edit the information in the **From**, **To**, **Subject**, and **Body** fields.

> You must select a check box in the Notifications check box list to enable the fields below it.

To view a list of attachment filter policy members

1. Select **Policies & Recipients**; then, the attachment filter policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Members** tab.
3. Select the criteria by which you want to list the search results from the **Search Field** drop-list. The **Search Type** drop-list and **Search Value** field become active.
4. Make a selection:

To perform a search that contains some or all of the text typed in the Search Value field:

- Select **Contains** from the **Search Type** drop-list.

To perform a search that exactly matches the text typed in the Search Value field:

- Select **Equals** from the **Search Type** drop-list.

5. Type a value In the **Search Value** field that will contain or exactly match your search criteria.
6. Make a selection:

To search for members by policy type:

- Select the policy type from the **Policy Type** Drop-list.

To search for members by the name of the policy:

- Select the name of the policy from the **Policy Name** drop-list.

To receive only up to a specific number of results:

- Select or type the number in the **Maximum Results** box.

7. Click **Search**. VIPRE searches the member database based on the selected criteria; then, returns the results in the table below.

4.8 Managing Global Disclaimer Settings

Use this section to manage disclaimers and signatures attached to emails for security, compliance, and general informational on incoming and outgoing email. Disclaimers are typically used to provide legal information, warnings about unknown or unverified e-mail senders, or various other reasons as determined by an organization. The following provides an example of a disclaimer:

> *IMPORTANT MESSAGE: This e-mail message is intended to be received only by persons entitled to receive the confidential information it may contain. E-mail messages to clients of VIPRE may contain information that is confidential and legally privileged. Please do not read, copy, forward or store this message unless you are an intended recipient of it. If you have received this message in error, please forward it back to the sender and delete it completely from your computer system.*

VIPRE inserts disclaimers into email messages using the same message format that used when the original message was created. For example, if a message is created in HTML, the disclaimer is added in HTML. If you choose to append a disclaimer to messages, VIPRE appends the disclaimer to the bottom of the message thread. VIPRE can also verify if previous disclaimers have been added to the message.

Tokens

VIPRE uses tokens to allow policy members to manage global disclaimers.

To manage Global Disclaimer Settings

1. Select **Policies & Recipients**; then, **Disclaimers**. The **Summary** tab opens in the right pane.
2. Click the **Global Settings** tab.
3. Make a selection:

   To enable the global disclaimer plug-in:

   - Select the **Enable plug-in** check box.

   To make sure duplicate disclaimer are not added to messages:

   - Select the **Do not add duplicate global disclaimer** check box.

4. To select a global disclaimer to apply to all email messages, click **Select** next to Select the global disclaimer.
5. Make a selection:

   To enable tokens that allow policy members to manage global disclaimers:

   - Select the **Enable tokens** check box; then type the name of the token in the **Token** field.

   To remove a Token from a message:

   - Select the **Remove token from message** check box.

   To only add a disclaimer if a token is found:

   - Select **Only Disclaim if Token found**.

   To only add a disclaimer if a token is not found:

   - Select **Only Disclaim if Token not found**.

To Manage disclaimer templates

1. Select **Policies & Recipients**; then, **Disclaimers**. The **Summary** tab opens in the right pane.
2. Click the **Templates** tab.

3. To add a disclaimer template, click **Add**. The **Template Editor** opens. Go to To add a disclaimer template .
4. Make a selection:

To edit a template:

- Select a template from the list; then click **Edit**. Go to To edit a disclaimer template.

To copy a template:

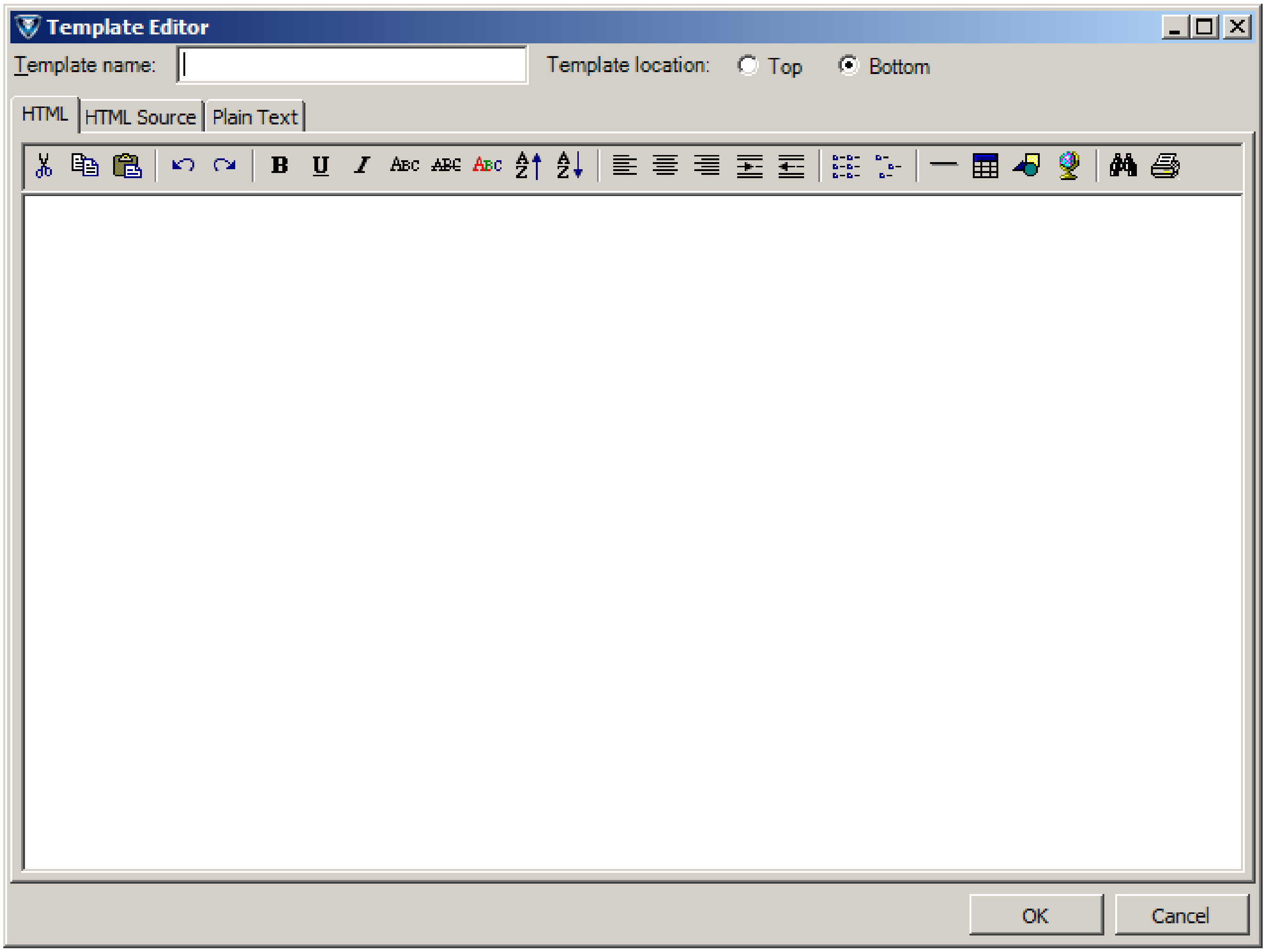
- Select a template from the list; then click **Copy**. The **Template Editor** opens. Change the name of the template; then close the window.

To delete a template :

- Select a template from the list; then click **Delete**. The template is removed from the list.

To add a disclaimer template

1. Select **Policies & Recipients**; then, **Disclaimers**. The **Summary** tab opens in the right pane.
2. Click the **Templates** tab.
3. Click **Add**. The **Template Editor** opens.



Screenshot 40: Disclaimers - Template Editor

4. Type a name for the template in the **Template** name field.
5. Type the text for the disclaimer in the text box under the HTML, HTML Source, or Plain Text tabs in the left pane. Only the HTML tab offers standard formatting tools.
6. Make a selection:

To add an attachment:

- Select **Add**. The attachment is added in the right pane.

To delete an attachment:

- Select **Delete**. The attachment is removed from the right pane.

Close the window.

To edit a disclaimer template

Certain functionality of the template editor relies on Internet Explorer's Enhanced Security Configuration (ESC) being disabled. For full editing ability, please disable Internet Explorer ESC.

1. Select **Policies & Recipients**; then, **Disclaimers**. The **Summary** tab opens in the right pane.
2. Click the **Templates** tab.
3. Select a template from the list; then click **Edit**. The **Template Editor** opens.
4. Edit the template.
5. Close the window.

To view a global list of disclaimer policy members

1. Select **Policies & Recipients**; then, **Attachment Filter** from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Members** tab.
3. Select the criteria by which you want to list the search results from the **Search Field** drop-list. The **Search Type** drop-list and **SearchValue** field become active.
4. Make a selection:

To perform a search that contains some or all of the text typed in the Search Value field:

- Select **Contains** from the **Search Type** drop-list.

To perform a search that exactly matches the text typed in the Search Value field:

- Select **Equals** from the **Search Type** drop-list.

5. Type a value In the **Search Value** field that will contain or exactly match your search criteria.
6. Make a selection:

To search for members by policy type:

- Select the policy type from the **Policy Type** drop-list.

To search for members by the name of the policy:

- Select the name of the policy from the **Policy Name** drop-list.

To receive only up to a specific number of results:

- Select or type the number in the **Maximum Results** box.

7. Click **Search**. VIPRE searches the member database based on the selected criteria; then, returns the results in the table below.

4.9 Managing Disclaimer Policies

Use this section to learn how to customize disclaimer policies. All recipients are assigned to a default policy until they are re-assigned to a new one.

To manage disclaimer policy settings

1. Select **Policies & Recipients**; then, the disclaimer policy you want to manage from the left pane. The **Policy Settings** tab opens in the right pane.
2. To enable the policy, select the **Enable policy** check box.
3. To select the disclaimer that will be applied to messages sent from members of the policy, click **Select** under the **Disclaimer Actions** section.
4. Make a selection:

To enable the global disclaimer plug-in:

- Select the **Enable plug-in** check box.

To make sure duplicate disclaimer are not added to messages:

- Select the **Do not add duplicate global disclaimer** check box.

5. Make a selection under the Token Actions section:

To enable tokens that allow policy members to manage global disclaimers:

- Select the **Enable tokens** check box; then type the name of the token in the **Token** field.

To Remove a Token from a message:

- Select the **Remove token from message** check box.

To only add a disclaimer if a token is found:

- Select **Only disclaim if Token found**.

To only add a disclaimer if a token is not found:

- Select **Only disclaim if token not found**.

To view a list of members using disclaimer policies

1. Select **Policies & Recipients**; then, the disclaimer policy you want to manage from the left pane. The **Summary** tab opens in the right pane.
2. Click the **Members** tab then, select the criteria by which you want to list the search results from the **Search Field** drop-list. The **Search Type** drop-list and **Search Value** field become active.
3. Make a selection:

   To perform a search that contains some or all of the text typed in the Search Value field:

   - Select **Contains from the Search Type** drop-list.

   To perform a search that exactly matches the text typed in the Search Value field:

   - Select **Equals from the Search Type** drop-list.

4. Type a value In the **Search Value** field that will contain or exactly match your search criteria.
5. Make a selection:

   To search for members by policy type:

   - Select the policy type from the **Policy Type** drop-list.

   To search for members by the name of the policy:

   - Select the name of the policy from the **Policy Name** drop-list.

   To receive only up to a specific number of results:

   - Select or type the number in the **Maximum Results** box.

6. Click **Search**. VIPRE searches the member database based on the selected criteria; then, returns the results in the table below.

4.10 Managing the Quarantine Store

Use this section to view, deliver, save, and delete quarantined items from the Quarantine Store.

To manage quarantined items

1. Select **Policies & Recipients**; then, **Quarantine** from the left pane. The **Quarantine Settings** tab opens in the right pane.
2. Make a selection:

   To refresh the list of quarantined items:

   - Click **Refresh**.

   To configure settings for quarantine storage:

   - Click **Settings...**. Go to To configure quarantine settings.

   To save the list of quarantined items under another file name:

   - Click **Save As...**.

To send a notification for quarantined items to authorized individuals:

- Select **Deliver...**.

To delete a quarantined item:

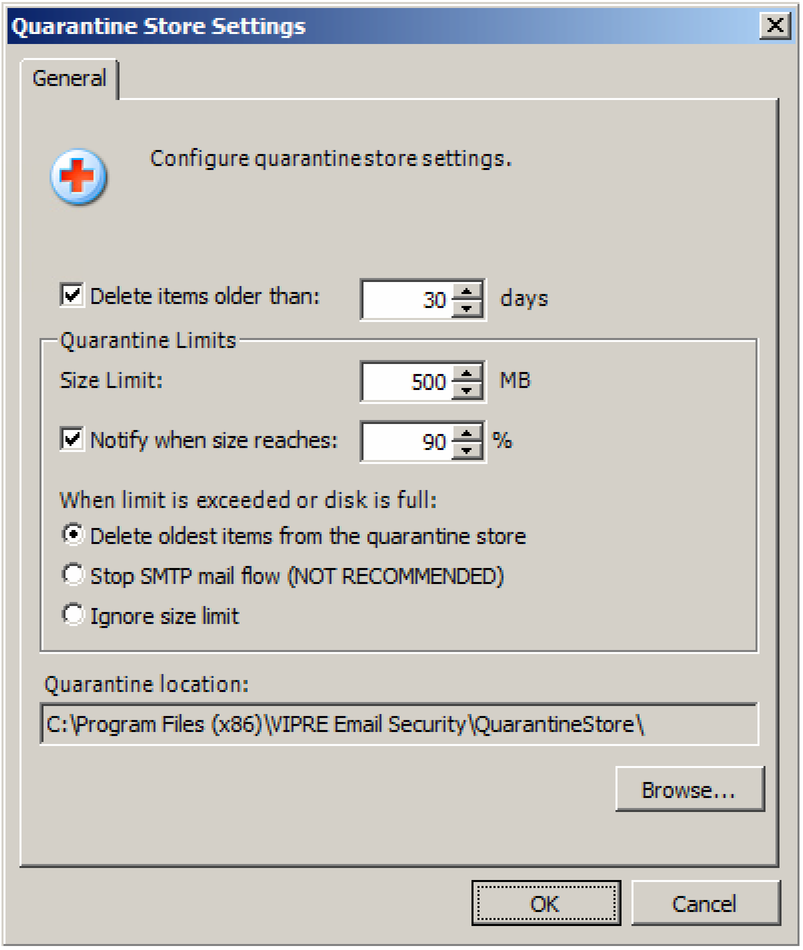
- Click **Delete**.

To purge the list of quarantined items:

- Click **Purge...**.

To configure quarantine settings

1. Select **Policies & Recipients**; then, **Quarantine** from the left pane. The **Quarantine** tab opens in the right pane.
2. Click **Settings...**. The **Quarantine Store Settings** dialog box opens.



Quarantine Store Settings

General

Configure quarantine store settings.

☑ Delete items older than: 30 days

Quarantine Limits

Size Limit: 500 MB

☑ Notify when size reaches: 90 %

When limit is exceeded or disk is full:

● Delete oldest items from the quarantine store

○ Stop SMTP mail flow (NOT RECOMMENDED)

○ Ignore size limit

Quarantine location:

C:\Program Files (x86)\VIPRE Email Security\QuarantineStore\

Screenshot 41: Quarantine Settings

3. Make a selection:

To delete items older than a certain amount of day:

- Select the **Delete items older than:** check box; then, select or type the number of days in the days box.

To set the quarantine storage size limit:

- Select or type the number of Megabytes in the **MB** box.

To have a notification sent what the storage reaches a certain size:

- Select the **Notify when size reaches:** check box; then, select or type the percentage the file size must reach before a notification is sent in the % box.

To set an action for when the storage limit is exceeded or the disk is full:

- Select the appropriate radio button below the heading, **When the limit is exceeded or disk is full:**.

4. If you want to edit the change the location where the quarantined items are stored, click inside the **Quarantine** location field, click **Browse...** to open the explorer, select the new location; then, click **OK**.
5. Click **OK** on the **Quarantine Store Settings** dialog box.

5 Managing Reports

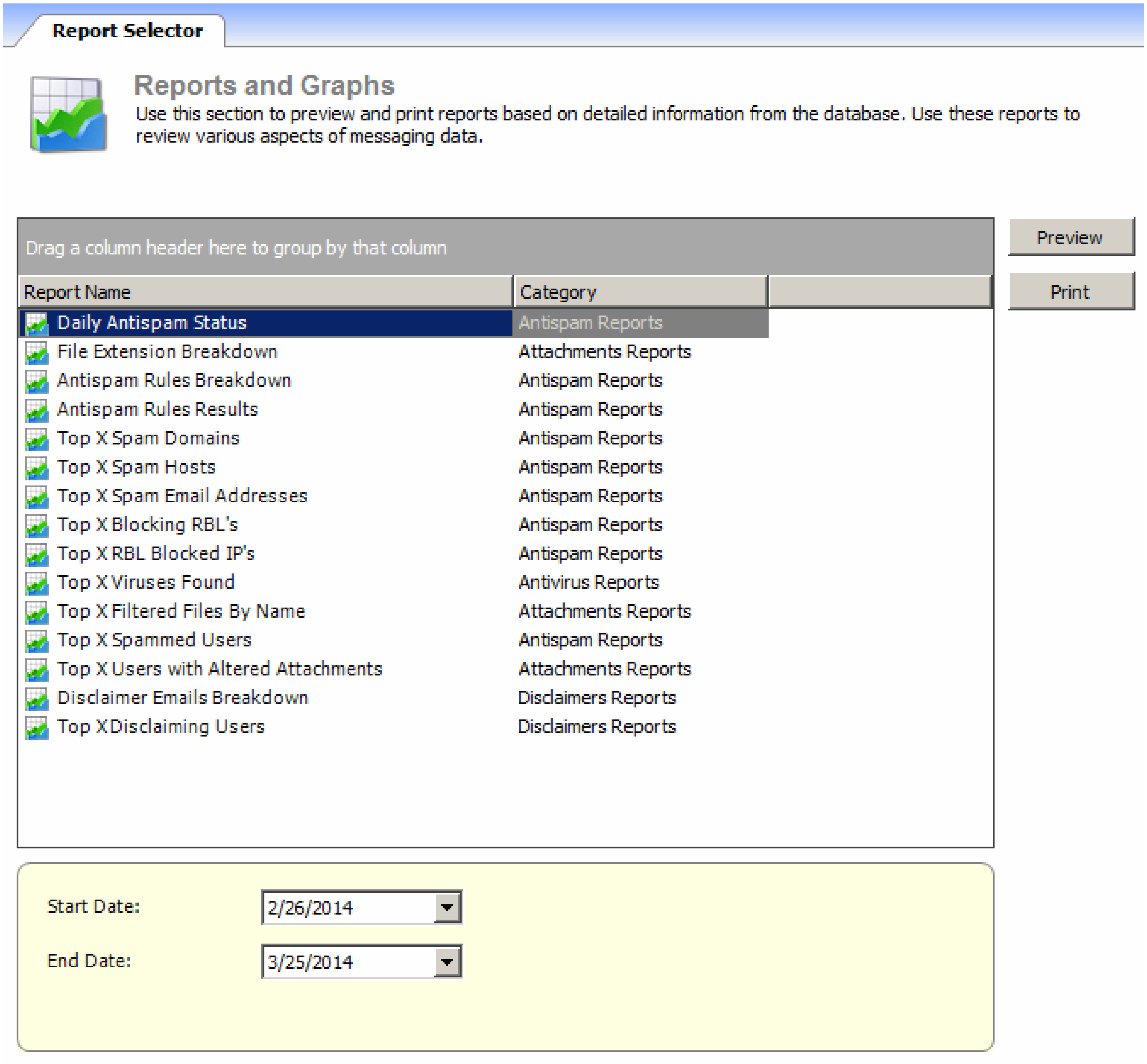
Use this chapter to learn how to customize, preview, and print reports. Reports can be exported in six formats:

- Adobe Acrobat (.pdf)
- Hypertext Markup Language (.html)
- MIME HTML (.mht)
- Rich Text Format (.rtf)
- Microsoft Excel (.xls, .xlsx)
- Comma-Separated Value (.csv)
- Text File
- Image File

5.1 About Reporting

Reports provide detailed information on threats to your system. Use the reports to review various Reporting aspects of messaging data.

To open the Report Selector tab in the right pane, select **Reporting**; then, **Report Selector** in the left pane.



Reports and Graphs

Use this section to preview and print reports based on detailed information from the database. Use these reports to review various aspects of messaging data.

Drag a column header here to group by that column

Report Name	Category
Daily Antispam Status	Antispam Reports
File Extension Breakdown	Attachments Reports
Antispam Rules Breakdown	Antispam Reports
Antispam Rules Results	Antispam Reports
Top X Spam Domains	Antispam Reports
Top X Spam Hosts	Antispam Reports
Top X Spam Email Addresses	Antispam Reports
Top X Blocking RBL's	Antispam Reports
Top X RBL Blocked IP's	Antispam Reports
Top X Viruses Found	Antivirus Reports
Top X Filtered Files By Name	Attachments Reports
Top X Spammed Users	Antispam Reports
Top X Users with Altered Attachments	Attachments Reports
Disclaimer Emails Breakdown	Disclaimers Reports
Top X Disclaiming Users	Disclaimers Reports

Start Date: 2/26/2014

End Date: 3/25/2014

Screenshot 42: Report Selector Tab

To preview a report

1. Select the type of report you want to preview from the list; then select a date range the report will cover from the **Start** and **Enddate** drop-lists.
2. To preview a report that lists information about inbound or outbound mail, select **inbound** or **outbound** from the **Direction** drop-list; then, click **Preview**.

To print a report

1. Select a report from the list; then, select the date range the report will cover from the **Start** and **End date** drop-lists.
2. To preview a report that shows information about inbound or outbound mail, select **inbound** or **outbound** from the **Direction** drop-list; then, click **Print**.

5.2 About Message Tracking

Message Tracking simplifies the process of determining why VIPRE has allowed or blocked each message. By providing intricate information on every message handled by VIPRE, admins can now easily review how and why messages were handled, in a single location within the VIPRE application. This feature provides better transparency to the entire messaging process and reduces the need to reach out to VIPRE Support.

Search Query

The most effective way to view processed messages with Message Tracking is via a search query. You may search by:

- Message ID
- Subject
- Sender IP
- To
- From
- date ranges

The query itself uses partial matching, which displays more results. To refine your results, use a column's autofilter, or build a custom filter. See FILTERING, below.

> A blank search query will display the last 100 processed messages.

Results

Searches will display in a new Results tab.

The results are divided into five columns:

- Connected At
- Sender IP
- Subject
- From
- To

By default, results are sorted by **Connected At**, with the most recent messages at the top of the list. Click any column header to change the sort to that column. Click again to reverse sort.

> If your search returns more than 100 results, you will be presented with only the first 100 results. You may narrow your search criteria for more specific results.

Expanding Results

Each result is expanded by clicking the [+] in the leftmost column for that result. Once expanded, the result will now also display:

Date/Time – The time when this filter step was taken.

Component – The component of VIPRE that processed this filter step.

Message – A detailed plain English message explaining the step VIPRE took via this component.

For more information, refer to Appendix 1 - Message Tracking details (page 92).

Filtering Results

You may filter your results using autofiltering or robust custom filters to narrow your search even further.

Hover over a column heading to display the filter icon . Clicking the filter icon will allow you to perform two types of filters: autofiltering, or custom filtering.

Autofiltering

To choose an autofilter, select it from the drop-down. Each autofilter will allow you to select:

All - Shows all search results for the column (this effectively clears the autofilter)

Custom - Allows you to build a custom filter for this column. See Custom Autofilter, below.

Blanks - Shows only empty results for this column.

Non blanks - Shows only results that contain a result for this column.

Specific Results - You may also select an existing result from this column, in order to immediately restrict your filter to that single item.

For example, if your current Sender IP results include three IP addresses:

- 192.168.0.200
- 192.168.0.135
- 10.3.1.20

You may choose to show only the results that matched IP **10.3.1.20**, by selecting that IP from filter drop-down.

> The **Connected At** autofilter functions differently; it allows for a quick selection of a specific calendar day, or today’s date only.

Custom Autofilter

For a more robust autofilter, you may choose Custom from the filter dropdown.

Using the Custom Autofilter window, you can use the following operators to further limit your query results:

- Equals
- Does not equal
- Is like
- Is not like
- Is greater than
- Is greater than or equal to
- Is null
- Is not null
- Is blank
- Is not blank

Custom autofiltering is not available via the **Connected At** column dropdown, but you may still create detailed filters using the **Edit Filter** button (see below).

The Filter String

Once you have selected at least one autofilter, the filter string will display on the bottom of the results tab. The filter string is comprised of all the autofilter options that are currently selected, combined into a single query string.

Using the query string, you may:

Select the Checkbox - to enable or disable the current filter.

Click the dropdown button - for a list of recent filters run. You can clear filters individually from this list by clicking the red X for each item.

Click the Edit Filter button - to display the Filter Editor dialogue. From here, power users can create intricate filters for every column, using the following operands:

- Equals
- Does not equal
- Is greater than
- Is greater than or equal to
- Is less than
- Is less than or equal to
- Is between
- Is not between
- Is null
- Is not null

- Is any of
- Is none of
- Date and time operators:
  - Is beyond this year
  - Is later this year
  - Is next week
  - Is later this week
  - Is tomorrow
  - Is today
  - Is yesterday
  - Is earlier this week
  - Is last week
  - Is earlier this month
  - Is earlier this year
  - Is prior this year
  - Is later this month

Click the X button - to wipe all recent filters with no confirmation.

Message Status

VIPRE allows you to filter results by the selected statuses. By default, all the following statuses are selected. You may toggle any of the statuses on and off by clicking the check box next to it.

- **Delivered** – The message reached the destination mailbox
- **Quarantined(Spam)** – The message was placed in the spam folder for the corresponding antispam policy
- **Quarantined (AV/AF)** – The message was placed in the server’s quarantine store by either the anti-virus or attachment filtering plug-in
- **Deleted** – The message was deleted by either the antivirus, attachment filtering, or antispam plug-in
- **Attachment Quarantined** – At least one attachment on the message was quarantined by antivirus or attachment filtering
- **Attachment Deleted** – At least one attachment on the message was deleted by antivirus or attachment filtering

6 Appendix 1 - Message Tracking details

Reference the table below for more details regarding each "message" provided by VIPRE in the Message Tracking output.

Plug-in	Message	Detail
TransportAgent (Transport Agent)	SMTP Mail From command received on <MachineName>.	A new connection has been established to the mail server specified by <MachineName>. Reverse DNS and RBL checks will be performed as required and the results will be provided back to Exchange so it can allow/block the connection accordingly.
TransportAgent (Transport Agent)	Skipping Reverse DNS and RBL filters because the sender is internal.	The email corresponding to this connection is being sent from a local sender and will not be subject to Reverse DNS and RBL filtering.
TransportAgent (Transport Agent)	Skipping Reverse DNS and RBL filters because the sender IP is not IPv4 or IPv6.	Reverse DNS and RBL filters are only designed to handle IPv4 and IPv6 connections. If the email comes from a different source, these filters must be skipped.
TransportAgent (Transport Agent)	Allowing connection because the sender's IP is whitelisted.	The Allowed IP list is enabled and contains an IP, range, or network that matches the sender's IP address. This will cause the Reverse DNS and RBL checks to be automatically skipped.
TransportAgent (Transport Agent)	Disconnecting SMTP connection and returning error code: <SmtpErrorText>	The connection will be blocked with <SmtpErrorText> as the error text, because either the Reverse DNS or RBL filter indicated that the sender is not valid. Review previous tracking entries to determine which filter and why.
TransportAgent (Transport Agent)	Skipping Reverse DNS and RBL filters because the connection is authenticated.	Authenticated connections automatically bypass the Reverse DNS and RBL checks.
TransportAgent (Transport Agent)	Processing of SMTP Mail From command complete. Returning control to Exchange.	Once the connection is allowed through Reverse DNS and RBL filtering, it is handed back over to Exchange for further processing until the complete email headers have been received.

Plug-in	Message	Detail
TransportAgent (Transport Agent)	Received email headers from Exchange on <MachineName>.	Once a sending MTA has transmitted all the email headers, VIPRE is ready to preform the SPF, Greylisting, and Antispoofing checks on the connection.
TransportAgent (Transport Agent)	Processing of email headers complete. Returning control to Exchange.	Once the SPF, Greylisting and Antispoofing checks are complete, control is given back to Exchange so the rest of the email can be retrieved before AV, AF, and AS filtering can occur.
TransportAgent (Transport Agent)	Sending email to the plug-ins to be scanned for recipient: <RecipientName>	Since an email can address multiple recipients and they may be assigned to different policy combinations, emails will be scanned 1 or more times from the perspective of each policy combination. This entry will be generated for each recipient or group of recipients that have the same policy combination.
TransportAgent (Transport Agent)	Sending email to the plug-ins to be scanned for recipients: <MultipleRecipients>	Since an email can address multiple recipients and they may be assigned to different policy combinations, emails will be scanned 1 or more times from the perspective of each policy combination. This entry will be generated for each recipient or group of recipients that have the same policy combination.
TransportAgent (Transport Agent)	Returning modified message to Exchange for delivery.	The plug ins have made modifications to the message such as adding x-headers, prepending the subject with [SPAM], or replacing an attachment with a text notification. Now that modified email will be processed by Exchange as if it were the original email.
TransportAgent (Transport Agent)	Saving message to the unprocessed folder, it will not be delivered. Please contact support for assistance.	A plug-in encountered an serious error condition and should be analyzed by support staff.

Plug-in	Message	Detail
TransportAgent (Transport Agent)	Queuing message to be resent to the plug-ins.	Only a finite quantity of emails can be scanned simultaneously. If multiple emails are going to the same recipient and it is taking a long time to retrieve that recipients personal allowed/blocked senders lists, it would delay other emails. Instead of waiting for this to happen, the email is placed further back in the queue and emails to other recipients are processed in the meantime.
TransportAgent (Transport Agent)	Queuing message to be resent to the plug-ins in 20 minutes because there is not enough memory to process the message right now.	An out of memory exception occurred while processing the email. Either the server should be configured to use less resources or the hardware should be upgraded.
TransportAgent (Transport Agent)	Returning message to Exchange for delivery.	The original email was not modified or quarantined by the plug-ins and will be delivered as usual by Exchange.
TransportAgent (Transport Agent)	Queuing message to be resent to the plug-ins in 20 minutes because an error occurred handling while handling the return message: <ErrorMessage>	During normal operation, this will never be encountered. Seeing this entry could indicate that there is a real-time AV scanner actively scanning the VIPRE temp directory.
FCrDNS (Reverse DNS)	Allowing connection because Reverse DNS settings failed to load.	connectionfiltering.xml settings file is missing, corrupted, or inaccessible due to incorrect file permissions.
FCrDNS (Reverse DNS)	Allowing connection because Reverse DNS is configured to allow IPv6 connections.	connectionfiltering.XML: FCrDNSCheckSkipIPv6=true. This is an xml only setting that is defaulted to false. This exists in case FCrDNS only works well with IPv4.
FCrDNS (Reverse DNS)	Blocking connection because no PTR record exists for the connecting IP.	Reverse DNS performs a reverse lookup on the connection IP and then verifies that the returned host resolves to that same IP. This entry indicates that the reverse lookup failed because the sender has not registered a PTR record for this IP address. To allow this connection whitelist the sender IP or disable Reverse DNS.

Plug-in	Message	Detail
FCrDNS (Reverse DNS)	Allowing connection because <SenderIP> resolves to <HostName>.	The IP address that made the connection, <SenderIP>, has a PTR record that points to <HostName> and <HostName> resolves back to the <SenderIP>.
FCrDNS (Reverse DNS)	Allowing connection because Reverse DNS confirmed <SenderIP> resolves to <HostName> via MX record.	The IP address that made the connection, <SenderIP>, has a PTR record that points to <HostName> and the MX record for <HostName> contains the <SenderIP>.
FCrDNS (Reverse DNS)	Blocking connection because Reverse DNS was unable to resolve <HostName> to <SenderIP>.	The IP address that made the connection, <SenderIP>, has a PTR record that points to <HostName> but <HostName> does not have an A/AAAA Record or MX Record that resolves to <SenderIP>.
FCrDNS (Reverse DNS)	Blocking connection because Reverse DNS failed. <ErrorMessage>.	An error occurred during the Reverse DNS check. Check the <ErrorMessage> for details.
FCrDNS (Reverse DNS)	Allowing connection because Reverse DNS is disabled.	To enable Reverse DNS go to Policies & Recipients -> Connection Filtering Settings->Enable Reverse DNS
RBL (Real-Time Blocked Lists)	Allowing connection because the RBL settings failed to load.	connectionfiltering.xml settings file is missing, corrupted, or inaccessible due to incorrect file permissions
RBL (Real-Time Blocked Lists)	Allowing connection because the RBL filter is disabled.	To enable the RBL filter, go to Policies&Recipients->Connection Filtering Settings>RBL Settings...
RBL (Real-Time Blocked Lists)	Allowing connection because there are no RBL servers configured.	To configure RBL servers, go to Policies&Recipients->Connection Filtering Settings>RBL Settings...
RBL (Real-Time Blocked Lists)	Allowing connection because the sender IP is not IPv4.	Since RBLs do not include support for IPv6 yet only IPv4 addresses are checked against the block lists.
RBL (Real-Time Blocked Lists)	Blocking connection because RBL server '<ServerName>' returned an A-record.	The connection will be blocked because the sender IP is on the <ServerName> block list. Sometimes a legitimate sender will get on a block list for a short period of time. If the sender should always be allowed add the sender IP to the allowed IP list.
RBL (Real-Time Blocked Lists)	Allowing connection because RBL server '<ServerName>' did not return an A-record.	The sender IP is not on the <ServerName> 's block list. The connection may still be blocked by a different RBL.

Plug-in	Message	Detail
SPF (Sender Policy Framework)	Allowing connection because Sender Policy Framework settings failed to load.	connectionfiltering.xml settings file is missing, corrupted, or inaccessible due to incorrect file permissions
SPF (Sender Policy Framework)	Allowing connection because Sender Policy Framework is disabled.	To enable the SPF filter, go to Policies&Recipients->Connection Filtering Settings>Enable Sender Policy Framework
SPF (Sender Policy Framework)	Allowing connection because the Sender Policy Framework result was Pass.	The sender has configured a SPF record and the sender IP is part of that SPF record.
SPF (Sender Policy Framework)	Allowing connection because the Sender Policy Framework result was None.	The sending domain does not have an SPF record configured.
SPF (Sender Policy Framework)	Allowing connection because the Sender Policy Framework result was Neutral.	The sender has configured a SPF record. Based on this record it can't be determined with certainty if the sender IP is authorized for this domain.
SPF (Sender Policy Framework)	Allowing connection because the Sender Policy Framework result was TempError.	A DNS query failed. This is most likely due to a temporary network issue.
SPF (Sender Policy Framework)	Allowing connection because the Sender Policy Framework result was PermError.	The sender domain has specified a SPF record that is not compliant with the RFC or contains a syntax error. The sender will need to modify their SPF record to resolve this.
SPF (Sender Policy Framework)	Allowing connection because the Sender Policy Framework result was SoftFail.	ConnectionFilteringSettings.xml AllowTypeSoftFail=true
SPF (Sender Policy Framework)	Blocking connection because the Sender Policy Framework result was SoftFail.	ConnectionFilteringSettings.xml AllowTypeSoftFail=false
SPF (Sender Policy Framework)	Blocking connection because the Sender Policy Framework result was Fail.	The sender IP is not authorized to send on behalf of the sending domain. If the sender should always be allowed, add the sender IP to the allowed IP list.
Greylist (Greylisting)	Blocking connection because the Connection IP is NULL.	This message will not be seen during normal operation. Most likely indicates a bug.
Greylist (Greylisting)	Blocking the connection because the sender has attempted the same connection <ConnectionCount> times and has been flagged as a DoS threat.	The sender IP has sent too many emails during the initial rejection period established by greylisting. Greylistsettings.xml has been configured with BlacklistDosConnections=true.

Plug-in	Message	Detail
Greylist (Greylisting)	Temporarily blocking the first connection for this IP, sender, and recipient combination.	Greylisting blocks the first attempt to send email. Many spambots will not try again. Normal MTAs will retry the message. This also gives the Antispam Engine more time to include the spam in its detection signatures.
Greylist (Greylisting)	Allowing the connection because it has been more than <GreylistRejectMinutes> minutes since the initial connection.	The sender has retried correctly and will be allowed.
Greylist (Greylisting)	Continuing to temporarily block the connection because the initial connection occurred within the <GreylistRejectMinutes> minute rejection interval.	The retried too soon or the GreylistRejectMinutes is too large
Greylist (Greylisting)	Allowing connection because the sending IP and domain have previously satisfied the Greylisting requirements.	The sender has been cached as legitimate.
Greylist (Greylisting)	Allowing connection because the sending domain has previously satisfied the Greylisting requirements and the SPF result for this connection was Pass.	The sender domain matches a domain that has already been cached as legitimate but the IP is new. SPF has verified that this IP is authorized for the domain.
Greylist (Greylisting)	Allowing connection because the sending domain has previously satisfied the Greylisting requirements and the IP is contained in the sending domain's MX record.	The sender domain matches a domain that has already been cached as legitimate but the IP is new. The IP has been matched to the domain via the MX record for that domain.
Antispoofing	Skipping spoofing check because the Antispoofing settings could not be loaded.	connectionfiltering.xml settings file is missing, corrupted, or inaccessibility due to incorrect file permissions
Antispoofing	Skipping spoofing check because Antispoofing is disabled.	Settings->Domains->Antispoofing->Enable Antispoofing to enable this feature.
Antispoofing	Skipping spoofing check because sender is internal.	The message has originated from a local MTA. No anti-spoofing check is required.
Antispoofing	Treating sender as not-spoofed because the sender IP is trusted.	The sending domain is local and the IP is in Settings->Domains->Antispoofing->Trusted IP List
Antispoofing	Treating sender as not-spoofed because the sender IP is in a trusted range. Start IP: {0} End IP: {1}.	The sending domain is local and the IP matches a network in Settings->Domains->Antispoofing->Trusted IP List
Antispoofing	Treating sender as not-spoofed because the sender IP is in a trusted network. Network IP: {0} Mask: {1}.	The sending domain is local and the IP matches a range in Settings->Domains->Antispoofing->Trusted IP List

Plug-in	Message	Detail
Antispoofing	Treating sender as spoofed because the sender IP is not trusted to send emails on behalf of the local domain.	The sending domain is local and the IP does not match any IPs, Networks, or Ranges in Settings->Domains->Antispoofing->Trusted IP List
Antispoofing	Skipping spoofing check because the connection was authenticated.	The sending domain is local, the connection was authenticated and Settings->Domains->Antispoofing->Trust authenticated connections is enabled.
Antispoofing	Treating sender as spoofed because the message has been previously flagged as spoofed.	VIPRE on a different MTA has already flagged this message as spoofed.
Antispoofing	Skipping spoofing check because the From address is not local.	The sending domain is different than the internal domain.
Antivirus	Skipping scan because the Antivirus plug-in is disabled.	Policies & Recipients->Antivirus->Global Settings->Enable Antivirus
Antivirus	Skipping scan because there are no Antivirus engines enabled.	Policies & Recipients->Antivirus->Global Settings->Antivirus Engines - All engines are Inactive
Antivirus	Skipping scan because the policy, <PolicyName>, is disabled.	Policies & Recipients->Antivirus->Policy Name->Policy Settings->Enable Policy
Antivirus	Threat definitions may be out of date because the Antivirus plug-in is not licensed.	Either the evaluation is expired or the registration key is no longer valid for the Antivirus plug-in. Messages will still be scanned with whatever the latest definitions are, but new threat definitions will no longer be downloaded. See sales for information on purchasing a new license.
Antivirus	Quarantining email because <EngineName> detected <InfectionName> in the html message body.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
Antivirus	Quarantining email because <EngineName> detected <InfectionName> in the text/plain message body.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
Antivirus	Deleting email because <EngineName> detected <InfectionName> in the html message body.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
Antivirus	Deleting email because <EngineName> detected <InfectionName> in the text/plain message body.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:

Plug-in	Message	Detail
Antivirus	Quarantining attachment <FileName> because <EngineName> detected <InfectionName>.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
Antivirus	Deleting attachment <FileName> because <EngineName> detected <InfectionName>.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
Antivirus	Quarantining email because <EngineName> detected <InfectionName> in <FileName>.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
Antivirus	Deleting email because <EngineName> detected <InfectionName> in <FileName>.	The action taken is configured in Policies & Recipients->Antivirus->Policy Name->Policy Settings->Action:
AttachmentFilter (Attachment Filter)	The message has no attachments to filter.	The attachment filter only filters messages with on or more attachments.
AttachmentFilter (Attachment Filter)	Skipping Attachment Filter check because no policy is assigned.	The recipient is assigned to "No Attachment Filtering Policy". This is changed via Policies & Recipients->Recipients OR Recipients->Attachment Filter->Members.
AttachmentFilter (Attachment Filter)	Skipping Attachment Filter check because the policy is disabled.	Policies & Recipients->Attachment Filter->Policy Name->Policy Settings->Enable policy
AttachmentFilter (Attachment Filter)	Allowing <FileName> because <Reason>.	The specified action is taken because the specified rule matched the specified file name.
AttachmentFilter (Attachment Filter)	Quarantining <FileName> because <Reason>.	The specified action is taken because the specified rule matched the specified file name.
AttachmentFilter (Attachment Filter)	Deleting <FileName> because <Reason>.	The specified action is taken because the specified rule matched the specified file name.
AttachmentFilter (Attachment Filter)	Quarantining the email because <Reason> for attachment <FileName>.	The specified action is taken because the specified rule matched the specified file name.
AttachmentFilter (Attachment Filter)	Deleting the email because <Reason> for attachment <FileName>.	The specified action is taken because the specified rule matched the specified file name.
AttachmentFilter (Attachment Filter)	Skipping Attachment Filter check because the plug-in is disabled.	Policies & Recipients->Attachment Filter->Global Settings->Enable attachment filtering.
AttachmentFilter (Attachment Filter)	Skipping Attachment Filter check because the plug-in is not licensed.	Contact sales for purchase information.

Plug-in	Message	Detail
Antispam	Skipping spam check because the Antispam plug-in is disabled.	Policies & Recipients->Antispam->Global Settings->Enable spam filtering.
Antispam	Adding <Points> points to spam score because the modify points rule <RuleName> was matched.	A custom rule that is configured to modify points matched. Rules can be edited in Policies & Recipients->Antispam->Global Settings->Global Rules AND Policies & Recipients->Antispam->Policy Name->Rules
Antispam	Skipping spam check because the Antispam plug-in is not licensed.	Purchase or renew
Antispam	Skipping spam check because the message direction is outbound only.	Only email from external senders to local recipients are scanned by the antispam plug-in.
Antispam	Skipping spam check because the message is internal.	Only email from external senders to local recipients are scanned by the antispam plug-in.
Antispam	Skipping spam check because no policy is assigned.	The recipient is assigned to "No Antispam Policy". This is changed via Policies & Recipients->Recipients OR Recipients->Antispam->Members.
Antispam	Skipping spam check because the policy, <PolicyName>, is disabled.	Policies & Recipients->Antispam->Policy Name->Policy Settings->Enable Policy
Antispam	Quarantining the email for <Recipient> because the sender, <Sender>, is in their personal blocked senders list.	Policies & Recipients->Antispam->Policy Name->Policy Settings->Blocked Folder is enabled and the recipient has put a message from this sender in their blocked folder.
Antispam	Deleting the email for <Recipient> because the sender, <Sender>, is in their personal blocked senders list.	Policies & Recipients->Antispam->Policy Name->Policy Settings->Delete messages from the senders in the recipient's Blocked list is enabled.
Antispam	Allowing the email for <Recipient> because the sender, <Sender>, is in their personal allowed senders list.	Policies & Recipients->Antispam->Policy Name->Policy Settings->Allowed Folder is enabled and the recipient has put a message from this sender in their Allowed folder.
Antispam	Allowing the email for <Recipients> because the <RuleType> rule, <RuleName>, was matched.	Rules can be edited in Policies & Recipients->Antispam->Global Settings->Global Rules AND Policies & Recipients->Antispam->Policy Name->Rules

Plug-in	Message	Detail
Antispam	Quarantining the email for <Recipients> because the <RuleType> rule, <RuleName>, was matched.	Rules can be edited in Policies & Recipients->Antispam->Global Settings->Global Rules AND Policies & Recipients->Antispam->Policy Name->Rules
Antispam	Deleting the email for <Recipients> because the <RuleType> rule, <RuleName>, was matched.	Rules can be edited in Policies & Recipients->Antispam->Global Settings->Global Rules AND Policies & Recipients->Antispam->Policy Name->Rules
Antispam	Quarantining the email because the sender was spoofed.	Policies & Recipients->Antispam->Policy Name->Spoofing
Antispam	Deleting the email because the sender was spoofed.	Policies & Recipients->Antispam->Policy Name->Spoofing
Antispam	Antispam Engine gave a spam score of <Score>.	The score assigned by the Antispam Engine can be configured in Policies & Recipients->Antispam->Global Settings
Antispam	Deleting the email for <Recipients> because the final score <Score> exceeded the delete threshold <DeleteThreshold>.	Policies & Recipients->Antispam->Policy Name->Delete Threshold
Antispam	Quarantining the email for <Recipients> because the final score <Score> exceeded the quarantine threshold <QuarantineThreshold>.	Policies & Recipients->Antispam->Policy Name->Quarantine Threshold
Antispam	Allowing the email for <Recipients> because the final score <Score> did not exceed the quarantine or delete threshold.	The message is most likely not spam. If the message is spam rules can be added to increase the chance that a message gets a higher score.
Disclaimer (Disclaimers)	Not disclaiming the email because the Disclaimers plug-in is disabled.	Policies & Recipients->Disclaimers->Global Settings->Enable disclaimers plug-in
Disclaimer (Disclaimers)	Not disclaiming the email because the sender is not assigned to a disclaimers policy.	The sender is assigned to "No Disclaimers Policy". This is changed via Policies & Recipients->Recipients OR Recipients->Disclaimers->Members.
Disclaimer (Disclaimers)	Not disclaiming the email because the sender's policy, <PolicyName>, is disabled.	Policies & Recipients->Disclaimers->Policy Name->Policy Settings->Enable policy
Disclaimer (Disclaimers)	Disclaiming the email with policy template <TemplateName>.	Policies & Recipients->Disclaimers->Policy Name->Policy Settings->Disclaimer Actions
Disclaimer (Disclaimers)	Omitting the policy disclaimer because the token, <Token>, was found in the email.	Policies & Recipients->Disclaimers->Policy Name->Policy Settings->Token Actions

Plug-in	Message	Detail
Disclaimer (Disclaimers)	Disclaiming the email with global template <TemplateName>.	Policies & Recipients->Disclaimers->Global Settings->Select the global disclaimer
Disclaimer (Disclaimers)	Omitting the global disclaimer because the token, <Token>, was found in the email.	Policies & Recipients->Disclaimers->Global Settings->Token Actions
Disclaimer (Disclaimers)	Not disclaiming the email because the direction is not outbound.	Disclaimers are only applied to messages that are sent from a local sender to an external recipient.
Disclaimer (Disclaimers)	Not disclaiming the email because the direction is internal.	Disclaimers are only applied to messages that are sent from a local sender to an external recipient.

Glossary

A

ADSI

ADSI (Analog Display Services Interface) is the standard protocol for enabling alternate voice and data services, such as a visual display at the phone, over the analog telephone network. A popular application enabled by ADSI is Call Waiting Deluxe, an application that displays the name and number of an incoming call while you are on the phone. If you have an ADSI screen phone, several options are displayed on your screen including switching to the new call, forwarding the new call to your voice mail, putting the new caller on hold, playing a recorded message, or dropping the current call and switching to the new call.

Algorithm

The term algorithm (pronounced AL-go-rith-um) is a procedure or formula for solving a problem. The word derives from the name of the mathematician, Mohammed ibn-Musa al-Khwarizmi, who was part of the royal court in Baghdad and who lived from about 780 to 850. Al-Khwarizmi's work is the likely source for the word algebra as well. A computer program can be viewed as an elaborate algorithm. In mathematics and computer science, an algorithm usually means a small procedure that solves a recurrent problem.

API

Acronym for Application Programming Interface. A set of routines used by an application program to direct the performance of procedures by the computer’s operating system. An API can be contrasted with a graphical user interface or a command interface (both of which are direct user interfaces) as interfaces to an operating system or a program.

B

Bayesian Filter

A Bayesian filter is a program that uses Bayesian logic, also called Bayesian analysis, to evaluate the header and content of an incoming e-mail message and determine the probability that it constitutes spam. Bayesian filters aren't perfect, but because spam characteristically contains certain types of text, such a program can be amazingly effective when it is fine-tuned over a period of time. A Bayesian filter works by categorizing e-mail into groups such as "trusted" and "suspect," based on a probability number (ranging from 0 or 0% to 1 or 100%). The categories are defined according to user preference. Spammers constantly try to invent new ways to defeat spam filters. Certain words, commonly identified as characteristic of spam, can be altered by the insertion of symbols such as periods, orby the use of non-standard but readable characters such as Â, Ç, Ë, or Í. But as the user instructs a Bayesian filter to quarantine or delete certain messages, the filter incorporates this data into its future actions. Thus a Bayesian filter improves with time, so it becomes more likely to block spam without also blocking desired messages. Bayesian filters are best used in conjunction with antivirus programs. Malicious viruses or worms can occasionally appear as attachments to e-mail messages, even from trusted sources.

Bayesian Logic

Named for Thomas Bayes, an English clergyman and mathematician, Bayesian logic is a branch of logic applied to decision making and inferential statistics that deals with probability inference: using the knowledge of prior events to predict future events. Bayes' theorem provided, for the first time, a mathematical method that could be used to calculate, given occurrences in prior trials, the likelihood of a target occurrence in future trials. According to Bayesian logic, the only way to quantify a situation with an uncertain outcome is through determining its probability. Bayes' Theorem is a means of quantifying uncertainty. Based on probability theory, the theorem defines a rule for refining a hypothesis by factoring in additional evidence and background information, and leads to a number representing the degree of probability that the hypothesis is true.

C

Cluster

In a computer system, a cluster is a group of servers and other resources that act like a single system and enable high availability, and, in some cases, load balancing and parallel processing. In personal computer storage technology, a cluster is the logical unit of file storage on a hard disk; it is managed by the computer's operating system. Any file stored on a hard disk takes up one or more clusters of storage. A file's clusters can be scattered among different locations on the hard disk. The clusters associated with a file are kept track of in the hard disk's file allocation table (FAT). When you read a file, the entire file is obtained for you and you aren't aware in which of the clusters it is stored.

D

Delaylisting

Works similar to Greylisting, except instead of dropping connections it holds the message locally for a specified delay interval. This gives the antispam engines more time to update definitions and increases effectiveness. Can be used on servers that are behind relays.

Directory Service

A directory service is a software application — or a set of applications — that stores and organizes information about a computer network's users and network resources. It allows network administrators to manage users' access to the resources. Additionally, directory services act as an abstraction layer (a way of hiding the implementation details of a particular set of functionality) between users and shared resources. A directory service should not be confused with the directory repository itself; which is the database that holds information about named objects that are managed in the directory service.

DLL

A dynamic link library (DLL) is a collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file). DLL files that support specific device operation are known as device drivers. The advantage of DLL files is that, because they don't get loaded into random access memory (RAM) together with the main program, space is saved in RAM. When and if a DLL file is needed, then it is loaded and run. For example, as long as a user of Microsoft Word is editing a document, the printer DLL file does not need to be loaded into RAM. If the user decides to print the document, then the Word application causes the printer DLL file to be loaded and run. A DLL file is often given a ".dll" file name suffix. DLL files are dynamically linked with the program that uses them during program execution rather than being compile with the main program. The set of such files (or the DLL) is somewhat comparable to the library routines provided with programming languages such as C and C++.

Domain

A Domain is a logical group of computers running versions of the Microsoft Windows operating system that share a central directory database. This central database (known as the Active Directory starting with Windows 2000[1]) contains the user accounts and security information for the resources in that domain. Each person who uses computers within a domain receives his or her own unique account, or user name. This account can then be assigned access to resources within the domain. In a domain, the directory resides on computers that are configured as "domain controllers". A domain controller is a server that manages all security-related aspects of a user and domain interactions, centralizing security and administration.

E

Exchange (Microsoft)

Exchange is a popular Microsoft messaging system that includes a mail server, an e-mail program (e-mail client), and groupware applications. Designed for use in a business setting, the Exchange server is often used in conjunction with Microsoft Outlook to take advantage of Outlook's collaborative features, such as the ability to share calendars and contact lists.

F

Failover

Failover is a backup operational mode in which the functions of a system component (such as a processor, server, network, or database, for example) are assumed by secondary system components when the primary component becomes unavailable through either failure or scheduled down time. Used to make systems more fault-tolerant, failover is typically an integral part of mission-critical systems that must be constantly available. The procedure involves automatically off loading tasks to a standby system component so that the procedure is as seamless as possible to the end user. Failover can apply to any aspect of a system: within an personal computer, for example, failover might be a mechanism to protect against a failed processor; within a network, failover can apply to any network component or system of components, such as a connection path, storage device, or Web server.

FQDN

A fully-qualified domain name (FQDN) is the portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to. The FQDN includes the second-level domain name (such as "sunbelt-software.com") and any other levels (for example, "www.sunbelt-software.com" or "www1.somesite.com"). The prefix "http://" added to the fully-qualified domain name completes the URL.

G

Greylisting

Greylisting is a feature that will help verify that a sending mail server is a real mail server instead of a spammer. When an email is received from a domain that has not recently sent an email to your domain, the Greylisting module will reqeuest a resend from the sending mail server. SMTP rules dictate that all mail servers are required to resend the message (the default for Microsoft Exchange is 5 minutes). Spammers do not use mail servers, and will not resend the message. Legitimate mail servers will resend the message. Greylisting will prevent many spam emails from being downloaded by the server, reducing the amount of emails that need to be processed by VIPRE Email Security.

Group Policy Object

A Group Policy Object (GPO) is a collection of settings that define the appearance of a system and how it will behave for a defined group of users. Microsoft provides a program snap-in that allows you to use the Group Policy Microsoft Management Console (MMC). The selections result in a Group Policy Object. The GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs). The MMC allows you to create a GPO that defines registry-based polices, security options, software installation and maintenance options, scripts options, and folder redirection options.

H

Hashing

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms. The hashing algorithm is called the hash function. The hash function is used to index the original value or key and then used later each time the data associated with the value or key is to be retrieved.

Host File

In computing, a hosts file, stored on the computer's file system, is used to look up the Internet Protocol address of a device connected to a computer network, such as your home computer connected to the Internet. The hosts file describes a many-to-one mapping of device names to IP addresses. When accessing a device by name, the networking system attempts to locate the name within the hosts file if it exists. Typically, this is used as a first means of locating the address of a system, before accessing the Internet domain name system. The reason for this is that the hosts file is stored on the computer itself and does not require any network access to be used, whereas DNS requires access to an external system, which is typically slower.

I

IIS

IIS (Internet Information Server) is a group of Internet servers (including a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with additional capabilities for Microsoft's Windows NT and Windows 2000 Server operating systems.

IMAP

IMAP (Internet Message Access Protocol) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP Version 4) is a client/server protocol in which e-mail is received and held for you by your Internet server. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail. A less sophisticated protocol is Post Office Protocol 3 (POP3). With POP3, your mail is saved for you in a single mailbox on the server. When you read your mail, all of it is immediately downloaded to your computer and, except when previously arranged, no longer maintained on the server. Where IMAP can be thought of as a remote file server, POP3 can be thought of as a "store-andforward" service. POP3 and IMAP deal with the receiving of e-mail from your local server and are not to be confused with Simple Mail Transfer Protocol (SMTP), a protocol used for exchanging e-mail between points on the Internet. Typically, SMTP is used for sending only and POP3 or IMAP are used to read e-mail.

IP Address

An IP address (Internet Protocol Address) is a unique address that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). In simpler terms, it is a computer address. Any participating network device — including routers, computers, time-servers, printers, Internet fax machines, and some telephones — can have their own unique address. Also, many people can find personal information through IP addresses. An IP address can also be thought of as the equivalent of a street address or a phone number (compare: VoIP) for a computer or other network device on the Internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. An IP address can appear to be shared by multiple client devices either because they are part of a shared hosting web server environment or because a proxy server (e.g. an ISP or anonymizer service) acts as an intermediary agent on behalf of its customers, in which case the real originating IP addresses might be hidden from the server receiving a request. The analogy to telephone systems would be the use of predial numbers (proxy) and extensions (shared). IP addresses are managed and created by the Internet Assigned Numbers Authority. IANA generally assigns super-blocks to Regional Internet Registries, who in turn allocate smaller blocks to Internet Service Providers and enterprises. Some portion of the IP address represents the network number or address and some portion represents the local machine address (also known as the host number or address). IP addresses can be one of several classes, each determining how many bits represent the network number and how many represent the host number. The most common class used by large organizations (Class B) allows 16 bits for the network number and 16 for the host number. Using the above example, here's how the IP address is divided: the Network address is 130.5, the Host address is 5.25. If you want to add subnetting to this address, then some portion of the host address could be used for a subnet address. For example: the Network address is 130.5, the Subnet address is 5, and the Host address is 25.

M

Mail Server

A mail server is an application that receives incoming e-mail from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, is an example of a mail server programs. The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an e-mail message, your e-mail program, such as Outlook, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

MAPI

Acronym for Messaging Application Programming Interface. The Microsoft interface specification that allows different messaging and workgroup applications (including e-mail, voice mail, and fax) to work through a single client, such as the Exchange client included with Windows 95 and Windows NT. See also API.

MD5

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is intended for use with digital signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. According to the standard, it is "computationally infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest.

MIME

Acronym for Multipurpose Internet Mail Extensions. A protocol widely used on the Internet that extends the SMTP (Simple Mail Transfer Protocol) to permit data, such as video, sound, and binary files, to be transmitted by Internet e-mail without having to be translated into ASCII format first. This is accomplished by the use of MIME types, which describe the contents of a document. A MIME-compliant application sending a file, such as some e-mail programs, assigns a MIME type to the file. The receiving application, which must also be MIME-compliant, refers to a standardized list of documents that are organized into MIME types and subtypes to interpret the content of the file. For instance, one MIME type is text, and it has a number of subtypes, including plain and html. A MIME type of text/html refers to a file that contains text written in HTML. MIME is part of HTTP, and both Web browsers and HTTP servers use MIME to interpret e-mail files they send and receive.

N

Node

In a network, a node is a connection point; it is either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes.

NTLM

NTLM stands for Windows NT LAN Manager, a name chosen to distinguish this more advanced challenge/response-based protocol from its weaker predecessor LAN Manager (LM). NTLM is the authentication protocol used on networks that include systems running the Windows NT operating system and on stand-alone systems. NTLM authentication is based on the data obtained when a user logs on logon. It consists of a domain name, a user name, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials. Interactive NTLM authentication over a network typically involves two systems: a client system, where the user requests authentication, and a domain controller where information related to the user's password is stored. Non-interactive authentication, which may be required to permit users already logged-on to access a resource such as a server application, typically involves three systems: a client, a server, and a domain controller that does the authentication calculations on behalf of the server.

P

Proxy Server

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion. A proxy server receives a request for an Internet service (such as a Web page request) from a user. If it passes filtering requirements, the proxy server, assuming it is also a cache server, looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user. To the user, the proxy server is invisible; all Internet requests and returned responses appear to be directly with the addressed Internet server. (The proxy is not quite invisible; its IP address has to be specified as a configuration option to the browser or other protocol program.) An advantage of a proxy server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy's cache, which will improve user response time. In fact, there are special servers called cache servers. A proxy can also do logging. The functions of proxy, firewall, and caching can be in separate server programs or combined in a single package. Different server programs can be in different computers. For example, a proxy server may in the same machine with a firewall server or it may be on a separate server and forward requests through the firewall.

R

Real-time Blackhole Lists (RBLs)

RBLs list ISP addresses that are known to be sources of spyware and spam that a network can use to filter out undesirable traffic. After the IP addresses are filtered, traffic coming from or going to an IP address on the list simply disappears, as if it were swallowed by an astronomical black hole. The SPF specification defines a policy framework, an authentication scheme, and a machine-readable language. Each participating domain declares attributes that uniquely describe their mail, including authorized senders. This description is represented in an SPF record, which is published in DNS (domain name system) records. An SPF client program performs a query searching for the correct SPF record, in order to determine whether a message comes from an authorized source.

S

Sender Policy Framework (SPF)

SPF is an antispam approach in which the Internet domain of a person sending email is authenticated for that sender. This action discourages spam mailers who routinely disguise the origin of their e-mail, a practice known as e-mail spoofing. The SPF makes it easier for a mail server to determine when a message came from a domain other than the one claimed.

Subnet

A subnet (short for "subnetwork") is an identifiably separate part of an organization's network. Typically, a subnet represents all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Without subnets, an organization could get multiple connections to the Internet, one for each of its physically separate subnetworks, but this would require an unnecessary use of the limited number of network numbers the Internet has to assign. It would also require that Internet routing tables on gateways outside the organization would need to know about and have to manage routing that could and should be handled within an organization. The Internet is a collection of networks whose users communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address (Internet Protocol address). This 32-bit IP address has two parts: one part identifies the network (with the network number) and the other part identifies the specific machine or host within the network (with the host number). An organization can use some of the bits in the machine or host part of the address to identify a specific subnet. Effectively, the IP address then contains three parts: the network number, the subnet number, and the machine number. The standard procedure for creating and identifying subnets is provided in Internet Request for Comments 950.

Subnet Mask

After an email arrives at an organization's gateway or connection point with its unique network number, it can be routed within the organization's internal gateways using the subnet number. The router knows which bits to look at (and which not to look at) by looking at a subnet mask. A mask is simply a screen of numbers that tells you which numbers to look at underneath. In a binary mask, a "1" over a number says "Look at the number underneath"; a "0" says "Don't look." Using a mask saves the router having to handle the entire 32 bit address; it can simply look at the bits selected by the mask. If you have the job of creating subnets for an organization (an activity called subnetting) and specifying subnet masks, your job may be simple or complicated depending on the size and complexity of your organization and other factors.

T

TNEF (Transport Neutral Encapsulation Format)

A proprietary format of attachment used by Microsoft Outlook. An attached file can be identified to be in this format using the unix "file" command or generally if it is called winmail.dat. Not all winmail.dat files contain useful data (but many do). Some only contain formatting information used by Outlook to generate an HTML-style view of the message, embedded (OLE) documents or Outlook-specific features such as forms, voting buttons, and meeting requests. TNEF attachments contain security sensitive information such as user login name and file paths, from which access controls can be inferred. There are no Internet-standard email functions that require TNEF encoding, and any file that can be sent using this method can also be sent using the MIME standard supported by all mail servers and nearly all mail clients. However, there are some functions of Microsoft's proprietary email infrastructure (see Microsoft Exchange Server) that require TNEF. In VIPRE Email Security, the Attachment Filter plug-in quarantines entire TNEF messages and their attachments, rather than just the attachment, even if the action for the attachment is set to "Delete".

U

UNC

In a network, the Universal Naming Convention (UNC) is a way to identify a shared file in a computer without having to specify the device on which it is storage device. The UNC can be used instead of the local naming system (such as the DOS naming system in Windows). In Windows, operating systems, the UNC name format is: \\servername\sharename\path\filename. The share name is sometimes used to logically identify the volume or device on which the file is stored. However, the idea is to free the user from having to know this. The file name can also exist directly under the sharename. For example: \\sunbelt\devsept\forms\cscug.html might specify on a server in the corporate main office a shared file (cscug.html) kept with other forms that members of a corporation's development department might download and read, or print and use. Printers and other devices can also be addressed using UNC.

Contacting VIPRE Support or Sales

VIPRE Business and Enterprise Support

311 Park Place Blvd, Suite 300, Clearwater, FL, 33759, USA

Telephone: +1 (877) 757-4094

https://businesssupport.vipre.com

VIPRE Sales

311 Park Place Blvd, Suite 300, Clearwater, FL, 33759, USA

Telephone: +1 (855) 885-5566 (+1 727-324-0001)

Email: vipresales@vipre.com