VIPRE Email Security
Server Edition

Quick Start Guide

Document Version: VESS-QSG-10.3.1

Last updated: Friday, September 3, 2021

Contents

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 **Quick Start Guide** will step you through installing the product and provide a general overview of the Settings, Policies and Recipients, Disclaimers, The Quarantine Store, and Reports.

2 Installation and the Welcome Wizard

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; then, make a selection:

    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. Install VIPRE on your computer.

3. After the installation is complete, the **InstallShield Wizard Completed** window opens.

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

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

6. Complete the wizard.

> If you need to launch the Welcome Wizard separately, click **Start** > **VIPRE** > **Welcome Wizard**.

3 Settings

Use the Settings section to set the parameters for VIPRE. The Settings are divided into seven groups:

- Domains
- Replication
- Databases
- Agent Registration
- Notifications and Logging
- Updates and Licensing
- Security

To configure VIPRE settings

1. Click **Settings** in the left pane.
2. Select a group. A tab or series of tabs opens in the right pane.
3. Click a tab and configure the settings for that tab.
4. On most of the tabs, if you made a change, a dialog box drops down at the top of the tab. Click **Apply** to accept the change, or **Discard** to cancel it

4 Policies and Recipients

Use the Policies and Recipients 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.

4.1 Policies

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 three types of policies that you can assign:

- **Antispam** – policies that help manage Antispam activity for email recipients.
- **Attachment Filter** – policies that help manage attachment filters for email recipients.
- **Disclaimer** – policies that help manage disclaimers for email recipients

You can also use this section to manage Antivirus settings and quarantined items. Use the same procedure to add a new Antispam 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**, or **Attachment Filter**.
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**, **Attachment Filter**, or **Disclaimers**.

4.2 Recipients

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.

1. Type a value In the **Search Value** field that will contain or exactly match your search criteria.
2. 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.

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

4.3 Antispam

You can assign policies to help manage antispam activity for users receiving email on your network.

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.

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.
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 number of spam messages that can be 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 per spam message the engine has to accumulate in order to break the "Is Spam" threshold. The 6000 value means that messages scoring 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 the **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.

> ℹ️ 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 **Like any other external message. Let the Antispam Engine decide.**

To quarantine the spoofed messages:

- Select **Quarantine them.**

To delete the spoofed messages:

- Select **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, select the Antispam policy you want to manage from the left pane. The **Summary** tab opens in the right pane. Click the **Rules** tab; then, make a selection:

To add a new rule:

- Click **Add**. The **Rule Wizard** opens. See the VIPRE User Guide for more detailed information.

To edit an existing rule:

- Click **Edit**. The **Rule Wizard** opens. See the VIPRE User Guide for more detailed information.

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 we 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 view a 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; 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; then, 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.

3. Type a value In the **Search Value** field that will contain or exactly match your search criteria; then, 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.

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

Antivirus

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.

To manage global antivirus settings

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

2. Click the **Global Settings** tab; then, make a selection:

To enable global antivirus filtering:

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

To activate an antivirus engine:

- Select an engine from the list under **Antivirus Engines**; then, click **Activate**.

To deactivate an antivirus engine:

- Select an engine from the list under **Antivirus Engines**; then, click **Deactivate**.

3. Make a selection:

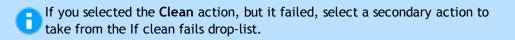**To set the limit of the uncompressed file size to process:**

- Type the Maximum size in the **maximum uncompressed files size to process** field; then, select the action to take after the file size is reached from the **If reached** drop-list.

To set the maximum number of nested files or attachments to process:

- Type the maximum number in the **Maximum nested files/attachments to process** field; then, select the action to take after the number is reached from the **If reached** drop-list.

4. Make a selection:

To select an action to take against infected items:

- Select the action from the Action drop-list.

> ℹ️ If you selected the **Clean** action, but it failed, select a secondary action to take from the If clean fails drop-list.

To replace any quarantined or deleted items with text explaining the action that was taken against them:

- Select the **Replace quarantined/deleted items with this text** check box.

> ℹ️ You can change the text in the box below, however we recommend that you use the default text.

5. Click **Configure** to configure the actions to take against specific types of infected items that cannot be handled by the general antivirus settings. The **Exception Handling** dialog box opens. Select an action to take against one or all of the specific types of infections from the available drop-lists.

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

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

3. To enable notifications for this antivirus policy, select the **Enable notifications for this policy** 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.

Attachment filter

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, allowing you to assign different Active Directory Users, Distribution lists, and mail-enabled public folders to specific policies. Use this section to customize recipient attachment filtering settings.

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.
3. 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-Header** check box.

   To determine which set of rules will be applied to attachments first:
   - Select the **Global rules** or **Policy rules** button.

4. Make a selection:

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

   To set the limit of the uncompressed file size to process:
   - Type the maximum size in the Maximum uncompressed file size to process field; then, select the action to take after the file size is reached from the If reached: drop-list.

   To set the maximum number of nested files/attachments to process:
   - Type the maximum number in the Maximum nested files/attachments to process field; then, select the action to take after the number is reached from the If reached: drop-list.

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. See *X-Headers* in the VIPRE User Guide.
3. Make a selection:

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

- Select the rule; then, click **Edit**. The **Attachment Filter Rule** dialog box opens.

To delete a rule:

- Select the rule; then, click **Remove**. The rule is removed from the list.

4. Make a selection:

To import a rule:

- Click **Import**. For example, if we 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**.

5. If you made a change, a dialog box drops down at the top of the tab. Click **Apply** to accept the change, or **Discard** to cancel it.

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.

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 set alternative actions for messages that cannot be processed, click **Configure**.
6. To specify the text that replaces quarantine or deleted attachments, type the replacement text in the box labeled **Replacement text for quarantined items**.
7. If you made a change, a dialog box drops down at the top of the tab. Click **Apply** to accept the change, or **Discard** to cancel it.

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 add a rule for a file extension:
   - **Click** Add. The **Attachment Filter Rule** dialog box opens.

   To edit the name or email address for a rule in the list:
   - Click **Edit**. The **Attachment Filter Rule** dialog box opens.

   To delete a rule:
   - Click **Remove**. The rule is removed from the list.

   To import a rule:
   - Click **Import**. For example, if we 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 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 the selection from the **Notifications** check box list. For example, if you selected **Notify Postmaster**, verify or edit the information in the **From**, **To**, **Subject**, and **Body** fields.

To view a 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.

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

5 Disclaimers

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.

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. See *Add a disclaimer template* in the VIPRE User Guide.

4 Make a selection:

   To edit a template:
   - Select a template from the list; then click **Edit**. See *Edit a disclaimer template* in the VIPRE User Guide.

   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 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.**

6 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...**.

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

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

To send a notification for quarantined items to authorized individuals.

- Click **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 Settings** tab opens in the right pane.
2. Click **Settings...**. The **Quarantine Store Settings** dialog box opens.
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.

7 Reports

Reports are another tool that provide detailed information on threats to your system. You can use the reports to review various aspects of messaging data. Reports can be exported in six formats:

- Crystal Reports (.rpt)
- Adobe Acrobat (.pdf)
- Microsoft Excel (.xls)
- Microsoft Excel Data Only (.xls)

- Microsoft Word (.doc)
- Rich Text Format (.rtf)

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**.

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