

BitDefender for MS Exchange 2000

QUICK START

How does it work?

BitDefender for MS Exchange 2000 is the perfect solution BitDefender offers you in order to keep the mail server FREE from viruses & spam. The product is designed and implemented in a modular manner, thus it can easily adapt to any work environment.

The schema below shows the way BitDefender works

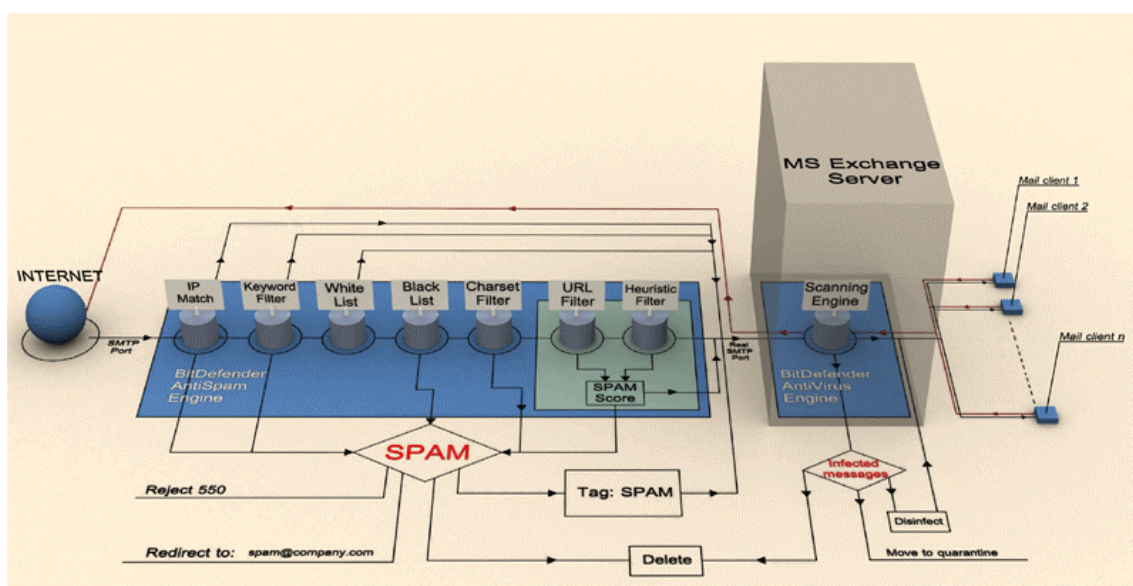


Figure 1

BitDefender for MS Exchange 2000 includes two engines: **BitDefender AntiSpam Engine** and **BitDefender AntiVirus Engine**.

BitDefender AntiSpam Engine

Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving questionable content in your office mail) and you can't stop people from sending it. The next best to that is, obviously, to stop receiving it. Unfortunately, spam comes in a wide range of shapes and sizes, and there's a lot of it.

The **BitDefender AntiSpam Engine** incorporates seven different filters: **IPMatch**, **Keyword filter**, **White list**, **Black list**, **Charset filter**, **URL filter** and **Heuristic filter**.

IP Match

Spammers often try to "spoof" the sender's e-mail address to make the email appear as if it is being sent by someone in your domain. To prevent this, enter a specific e-mail address to a specific IP address.

If the message appears to be from a domain that you have specified in your **IP Match** setting (such as your own company domain), BitDefender checks to see if the IP address of the sender matches the IP address entered for the specified domain. If the sender's domain address, match the IP address, the message will be delivered directly to the mail server. Otherwise the message will be tagged as SPAM.

Keyword filter

Relevant categories are message subject, headers and body. A set of explicit allow / don't allow rules must be defined.

White list / Black list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **White/Black lists**, the admin can set a list of trusted and un-trusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

We recommend that you add the trusted addresses to the **White List**. **BitDefender** does not block messages from those on the list; therefore, adding them helps ensure that legitimate messages get through.

Charset filter

The **Charset filter** helps you block all the e-mail messages written in Cyrillic and / or Asian charsets.

URL filter

Most of the spam messages contain links to various web locations (which contain more advertising and the possibility to buy things, usually). BitDefender has a database, which contains links to these kinds of sites. Every URL link in an e-mail will be checked against the URL database. If it will be found, +45 will be added to the spam score.

Heuristic filter

BitDefender checks all the message components against many rules, (i.e. not only the header but also the message body in either HTML or text format), using the **Heuristic filter**. Each rule is given a numerical value and the aggregate of these values is an overall spam score that ranges from 0-100. The overall spam score is measured against the desired level of spam sensitivity (threshold), and a decision is made whether the message is spam or is valid.

BitDefender AntiVirus Engine

The **BitDefender AntiVirus Engine** will check the e-mail for viruses with the BitDefender powerful scanning engines (**ICSA Labs-**, **Checkmark-** and **VB-**certified).

It will identify the viruses presents in the message body or attachment, including RAR, ZIP, ARJ, LZH, LHA, ACE, GZIP, TARGZ, JAR, UUE, MIME or CAB archives, no matter how they were created (self-extractable, multivolume, etc). Depending on the BitDefender actions, the infected messages can be disinfected, deleted or moved to quarantine and alarm messages (by e-mail or through NetSend) can be sent to the persons in charge with the administration and the protection of the network.

SYSTEM REQUIREMENTS

- ➔ Minimum 20 MB available hard disk space (50 MB Recommended)
- ➔ Windows 2000 SP3 or Windows Server 2003 ; MS Exchange 2003

Best practices

1. After the installation process is over, please register the product.
2. You must specify the proxy settings for the SMTP server. Access the **SMTP Proxy** section and introduce the proxy settings.
3. In the same window you must type the local domain (in order to receive all the incoming e-mails) and the network address (in order to send all the outgoing e-mails through proxy). For local domain you must click the **Add E-mail Domain** button and type in it. For network address you must click the **Add Net Domain** button and type in the network address and mask.
4. Select the action to be taken on infected messages (**AntiVirus Engine** section).
5. Select the action to be taken on spam messages (**MS Exchange AntiSpam** section).
6. In the same window, select the **Add header** check box. The result is that the header of all the messages (spam or not) will be modified. If you receive an e-mail that you think is spam, but BitDefender didn't tag it you can check the spam score in the e-mail properties.
7. Verify that BitDefender is working with the GTUBE & EICAR tests.

The GTUBE test consists in entering the `XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X` line in the body of an e-mail and send it to an user that has the e-mail on the server protected by BitDefender. BitDefender must tag as spam any message that contains this string.

The EICAR test consists in creating a file using a text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a CR/LF at the end. The file must contain the following single line: `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`.

Save the file to any name with COM extension, for example EICAR.COM and send it as attachment to an user that has the e-mail on the server protected by BitDefender. BitDefender must treat this message as an infected one.



The string must be reproduced on a single line.

After sending those messages, access the **Statistics** section, where you can see if BitDefender is actually working.

8. Configure the AntiSpam filters: **IPMatch**, **Keyword filter**, **White list**, **Black list**, **Charset filter**, **URL filter** and **Heuristic filter**.
9. If a virus is detected or an unexpected situation appears, there is the possibility of sending alarm messages by e-mail (**Mail Notification** section) or by net send (**NetSend Notification** section).
10. Configure the update. Enter the **BitDefender Update** section and if you are using a proxy check **Use Proxy** and type in the settings. You can change the update interval (the default interval is 8 hours).

Configure the update pushing feature. Click **Update now** in order to update the BitDefender AntiSpam & AntiVirus engines.