2013

fort systems ltd

white and black listing

documentation for system and domain administrators

BarricadeMX Plus

This short document will show you how to configure White and Black Listing for System and Domain Administrators using the BarricadeMX Plus web interface. White Listing for End users is covered in the **barricademx end user interface** document.

The BarricadeMX Plus interface is accessed using a Web Browser window. We currently support the latest versions of Internet Explorer on Windows, Safari on Mac OS X and Firefox on Windows, Mac OS X and Linux systems. You will need to have login credentials supplied to you by the administrator of the BarricadeMX system to be able to use this interface.

Why Blacklisting Seldom Works

Blocking senders by using a Blacklist sounds like a useful anti-spam tool, but it rarely is. In reality, Blacklisting is practically useless since spammers change their purported "address" with almost every message. Blacklisting is only really effective if you know that the “From” address or “From Domain” will not change. Examples of this occurring would be:

- You know the sender and simply do not want to receive correspondence from them.
- A commercial site does not have a “Can-Spam” compliant unsubscribe button. Typically this occurs with email from companies not based in the US.
- You can stop email from any unwanted source that consistently uses the same email address.

So Blacklisting obvious spam is almost always a waste of time and other methods must be employed.

Why White Listing Can Be Effective

White listing is necessary if you want to receive email from sites that:

- Have been blacklisted. Periodically sites are black listed by mistake.
- Have not been properly configured to send email in accordance with the Internet protocols for sending email
- Often send emails that trip typical anti-spam tests.
- Are temporarily blacklisted because spammers compromised the site.

White and Blacklisting levels for Domain Administrators

When an **End User** logs in to BarricadeMX Plus or uses the Quarantine Report email to White or Black list a message, that White or Blacklist entry will be applied only to the end users primary email address and any aliases associated with their primary email address.

When a **Domain Administrator** logs in to BarricadeMX to add white or Black list entries, the White or Blacklist entries they make may be applied to one or all of the domains they administer. If they only administer a single domain or want to apply the White and Black lists to all the domains they administer, they should use the web interface to access **Lists -> Blacklist -> 1. Global Blacklist** or **Lists -> Blacklist -> Global Whitelist:**

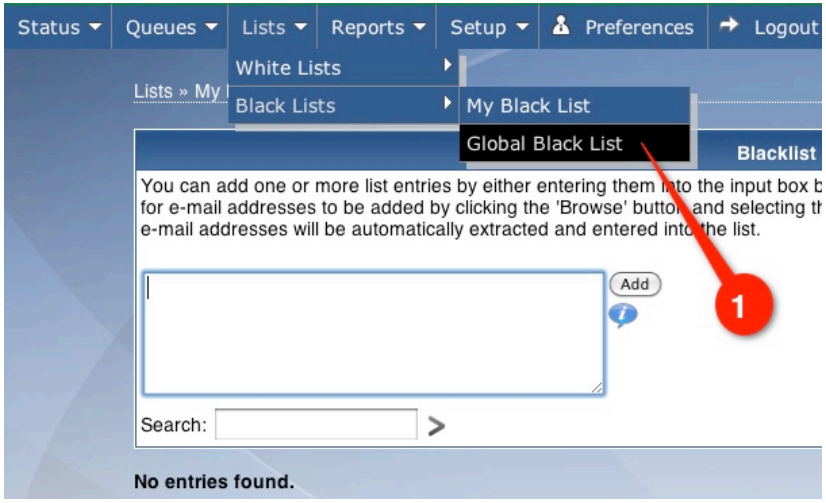

Figure 1. White - Black Listing

Important: Note that selecting either the **Lists -> Blacklist -> My Blacklist** or **Lists -> Blacklist -> My Whitelist** menu choices would apply any added White or Black list entries **ONLY** to the email address that the Domain Administrator used as the login username.

When a **Domain Administrator** user logs in to BarricadeMX Plus and wants to apply White or Black list entries **ONLY** to one of two or more domains they administer, they should use the **Setup -> Domains menus**

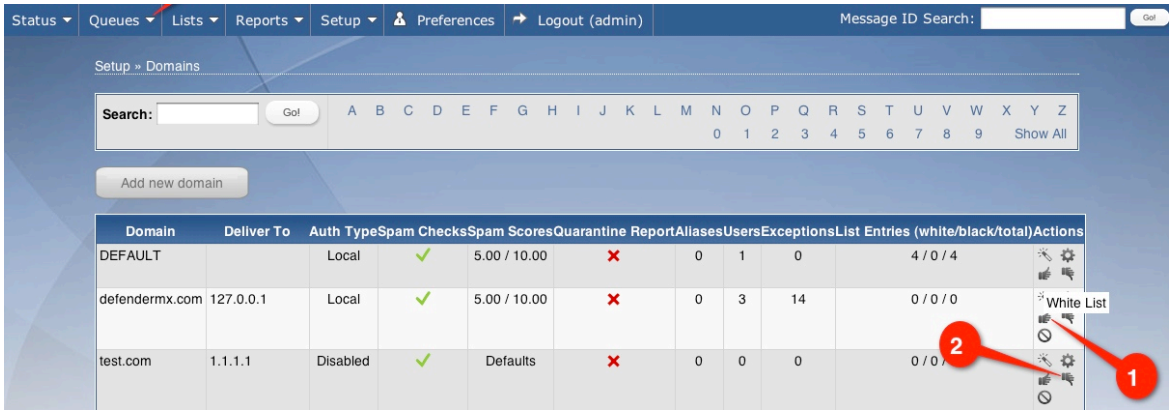

Figure 2. White - Black Listing

Selecting **1**., The White List icon for the defendermx.com domain, will add the new White List entries only to mail sent to the defendermx.com domain.

Selecting **2**., The Blacklist icon for the test.com domain, will add the new Blacklist entries only to mail sent to the test.com domain.

Adding Entries – Domain Administrator

The Screen for adding White or black list entries is shown below.

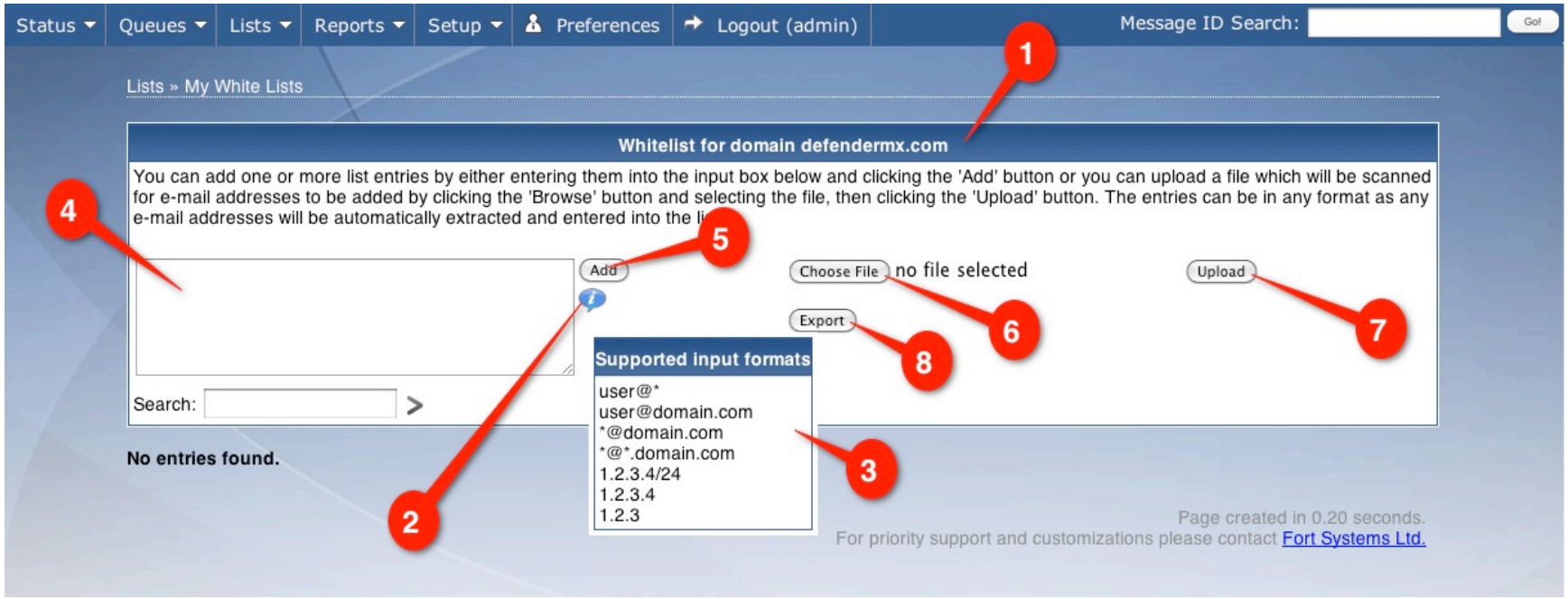

Figure 3. White - Black Listing

The **1**. **Title** of the screen will always show the address or domain scope and type (White or Blacklist) of the entries.

Clicking on the  button will show the permitted formats for entering white or black list entries.

There are two ways to add white or black list entries:

1. The entries in the permitted formats may be manually added in the **4. Text Box**. When all the entries have been added, select the **5**. **Add** button.
2. A plain text file can be created on your local computer. This text file should contain the White or Blacklist entries, one per line, in the permitted formats. Selecting **7**. **Upload**, will upload and add the entries in the text file.

Selecting **8**. **Export** will export the White or Blacklist entries for the scope described in the **1**. **Title**.

White and Blacklisting levels for System Administrators

When a **System Administrator** logs in to BarricadeMX to add white or Black list entries, the White or Blacklist entries they make may be applied to one or all of the domains they administer. If they want to apply the White and Black lists to all the domains they administer, they should use the web interface to access **Lists -> Blacklist ->** 1. **Global Blacklist** or **Lists -> Blacklist -> Global Whitelist:**

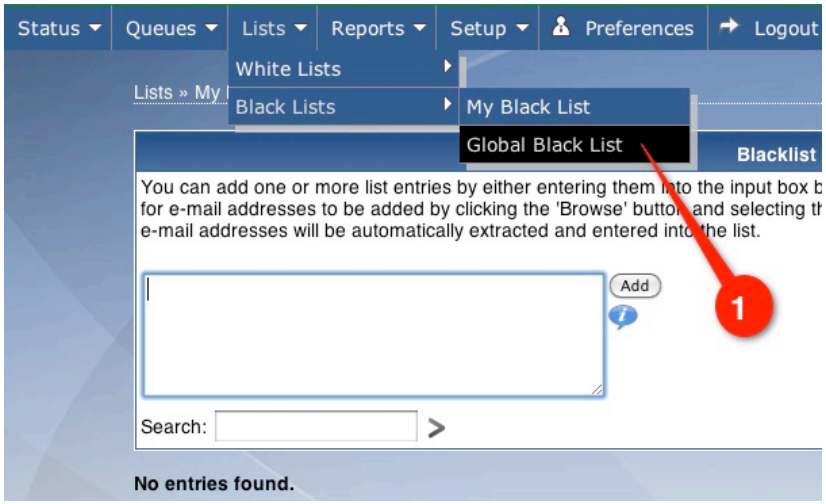

Figure 1. White - Black Listing

Important: Note that selecting either the **Lists -> Blacklist -> My Blacklist** or **Lists -> Blacklist -> My Whitelist** menu choices would apply any added White or Black list entries **ONLY** to the email address associated System Administrator's login username.

When a **System Administrator** user logs in to BarricadeMX Plus and wants to apply White or Black list entries **ONLY** to one of domains they administer, they should use the **Setup -> Domains menus**

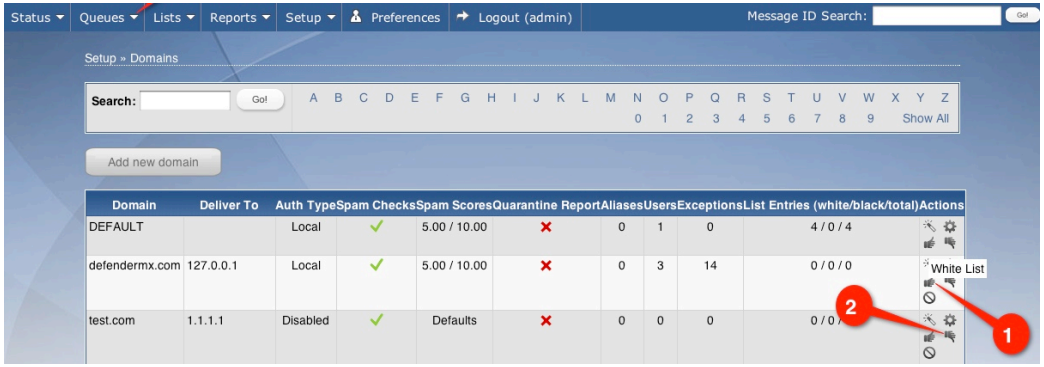

Figure 2. White - Black Listing

Selecting 1., The White List icon for the defendermx.com domain, will add the new White List entries only to mail sent to the defendermx.com domain.

Selecting 2., The Blacklist icon for the test.com domain, will add the new Blacklist entries only to mail sent to the test.com domain.

Adding Entries – System Administrator

The Screen for adding White or black list entries is shown below.

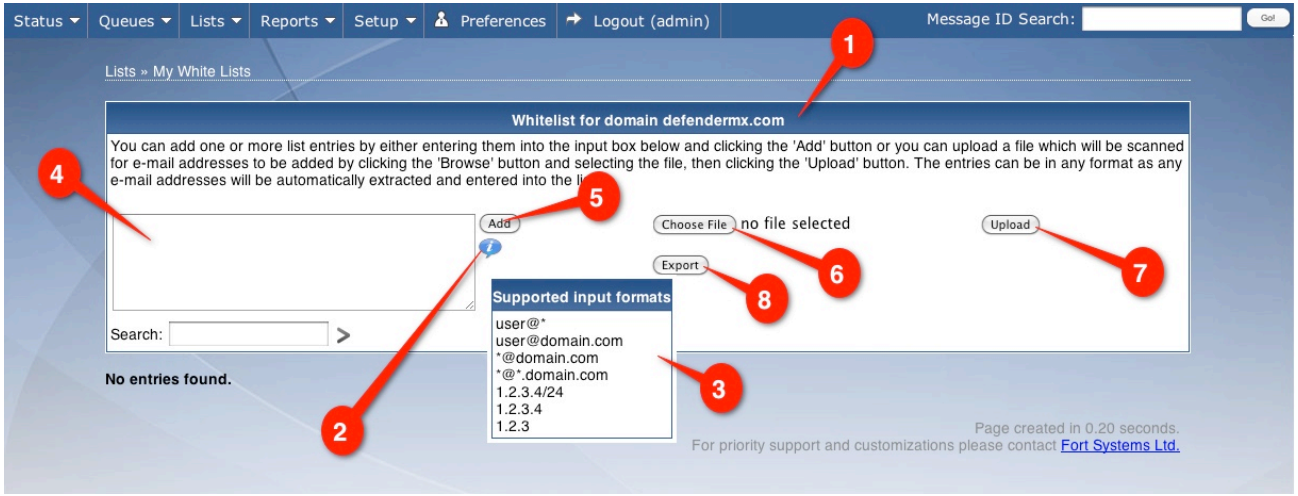

Figure 3. White - Black Listing

The 1. **Title** of the screen will always show the address or domain scope and type (White or Blacklist) of the entries.

Clicking on the  button will show the permitted formats for entering white or Black list entries.

There are two ways to add white or black list entries:

1. The entries in the permitted formats may be manually added in the **4. Text Box**. When all the entries have been added, select the 5. **Add** button.
2. A plain text file can be created on your local computer. This text file should contain the White or Blacklist entries, one per line, in the permitted formats. Selecting 7. **Upload**, will upload and add the entries in the text file.

Selecting **8. Export** will export the White or Blacklist entries for the scope described in the 1. **Title**.

What to White List or Blacklist

Exactly what to White or Black list may not be obvious since it's trivial to forge the "From" or Reply to" of the sender on an email. Since all spam is sent from Forged addresses it is useless to Blacklist the domain or email address found in a spam message.

When Whitelisting email to insure delivery, typically you will want to White List the email address or Domain name of the sender in the formats:

Email Address	steve@fsl.com
Domain Name:	*@fsl.com

Or if you know the IP address or ALL of the IP addresses of the servers that send mail for a domain that you want to whitelist, you can use the formats:

IP Address:	63.69.123.1
CIDR Notation:	63.69.123.1/24

How White and Blacklists are Applied

BarricadeMX Plus provides two levels of email filtering. The first filtering occurs at the MTA level, before accepting an email, using the BarricadeMX /smtpf application. The second level occurs after the email has been accepted; using the BarricadeMX Plus/MailScanner application. (Please refer to the introduction to barricadeMX section of this documentation for a description of how **Two Level** filtering works.)

White and Blacklist must be applied at both levels of filtering. The **Level One** filtering is provided by the Access Map configuration in the BarricadeMX /smtpf application while the **Level Two** filtering is provided by the White and Blacklisting rulesets used by using BarricadeMX Plus/MailScanner.

When you add a White or Blacklisting entry using the methods described later in this section, that entry is used by the **Level Two** BarricadeMX Plus/MailScanner filtering. Additionally, to ensure that a new listed entry gets through the **Level One** filtering, a corresponding entry is silently added to the Access Map configuration used by the BarricadeMX /smtpf application during the **Level One** filtering.

These added Access Map White and Blacklist entries are automatically kept in sync with the BarricadeMX Plus/MailScanner rulesets and are not displayed in the **Setup -> Access Map** screens in the web interface. Deleting or updating a **Level Two** Filter entry will automatically delete or update the corresponding **Level One** filter.

Using the Access Map to White and Blacklist

When very specific conditions exist, you can and should use the **Setup -> Access Map** function of the web interface for White or Blacklisting. These conditions are:

A site is blacklisted by mistake:

There will be occasions when you will need to accept email from a site that has been blacklisted. This can be accomplished by using the **Setup -> Access Map** function of the web interface to allow the IP address or addresses of the Blacklisted site through the Level One BarricadeMX /smtpf filtering. The following examples will bypass all Level One checks including Virus Checks:

connect:110.123.2	OKPLUSAV
connect:110.123.2	OKPLUSAV
From:somedomain.com	OKPLUSAV
From:user@somedomain.com	OKPLUSAV

The following examples will bypass all Level One checks but NOT Virus Checks:

Connect:110.123.2	OK
Connect:110.123.2	OK
From:somedomain.com	OK
From:user@somedomain.com	OK

The following examples will bypass all Level One checks but NOT Virus Checks, URL checks and Spam Checks. (Spam Checks will only be bypassed if enabled in Level One filtering which is not the default):

connect:110.123.2	CONTENT
connect:110.123.2	CONTENT
From:somedomain.com	CONTENT
From:user@somedomain.com	CONTENT

A spam attack is occurring

If you are experiencing any type of spam attack that can be identified as coming from a single source or limited number of sources you should use **Setup -> Access Map** function of the web interface to block the offending connections as soon as possible. The following examples can be used to immediately block incoming connections:

connect:110.123.2	IREJECT
connect:110.123.2	IREJECT
From:somedomain.com	IREJECT
From:user@somedomain.com	IREJECT

The following examples can be used to Blacklist incoming connections:

connect:110.123.2	REJECT
connect:110.123.2	REJECT
From:somedomain.com	REJECT
From:user@somedomain.com	REJECT

A "Joe Job" attack is occurring

If a hosted email address is used by Spammer as the From: or Reply-to: address on a spam run, your email gateways may be overcome by "bounced" spam messages. This type of attack is referred to as a "Joe Job". These useless connections may be blocked by using the **Setup -> Access Map** function of the web interface to add and entry similar to the following example (0 = zero):

Null-Rate-To:innocent@mydomain.com	0

A spam attack is originating from one of your systems

If a system on you network is compromised and sending out spam or phishing emails through your gateway, these message can be detected and stopped by using Message Limits at the BarricadeMX/ smtpf level. Use the **Setup -> Access Map** function of the web interface to add an entry similar to one of the following examples:

Msg-Limit-Connect:192.168.123.10	1000 / minute
Msg-Limit-Connect:mydomain.com	1000 / minute
Msg-Limit-From:baduser@compromised.com	100 / minute

A messages containing blocked URLS

If wanted messages are being blocked because they contain URLs that are being blocked by DNSBL checks, Use the **Setup -> Access Map** function of the web interface to add examples similar to one of the following examples:

Body: 110.123.2.10	OK
Body:okdomain.com	OK
Body:steve@fsl.com	OK

Messages containing unwanted URLS

If unwanted messages contain URLs that should be blocked at your site, Use the **Setup -> Access Map** function of the web interface to add examples similar to the following:

Body: 110.123.2.10	REJECT
Body:okdomain.com	REJECT
Body:steve@fsl.com	REJECT

The examples used above show a few of the possibilities for using the BarricadeMX/smtpf Access Map configuration to block or allow messages. Many more examples may be found at our partner site: http://www.snertsoft.com/smtp/smtpf/access-map.html.

Additional Support

For additional support please contact the support@fsl.com