

2013

fort systems ltd 

adding and deleting domains and routes
documentation for system and domain administrators

BarricadeMX Plus

This short document will show you how to add or delete domains and servers to route email via the BarricadeMX Plus System and Domain Administrators' interface.

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.

Adding Domains to BarricadeMX Plus

You should correctly configure the BarricadeMX Plus server(s) to scan email for a domain **before** you set the domain's DNS MX records to direct email for the domain to the BarricadeMX Plus server(s).

IMPORTANT: All email servers should have a DNS A record that matches its FQDN fully and DNS PTR record that corresponds with the IP address of the DNS A record if that server is to RELAY email to other systems on the internet.

To add a domain that BarricadeMX Plus will receive and process email for, you will need to assemble certain information for the domain. At a minimum you will need to know:

- The name of the domain
- The FQDN or IP address of the mail hub where messages will be forwarded after scanning
- How the mail hub authenticates users, typically POP, IMAP Active Directory or SMTP authentication.

When you have this information, you can login to the BarricadeMX Plus Web Interface and navigate to **Setup -> 1. Domains**. This will bring up the **Domain Information** form.

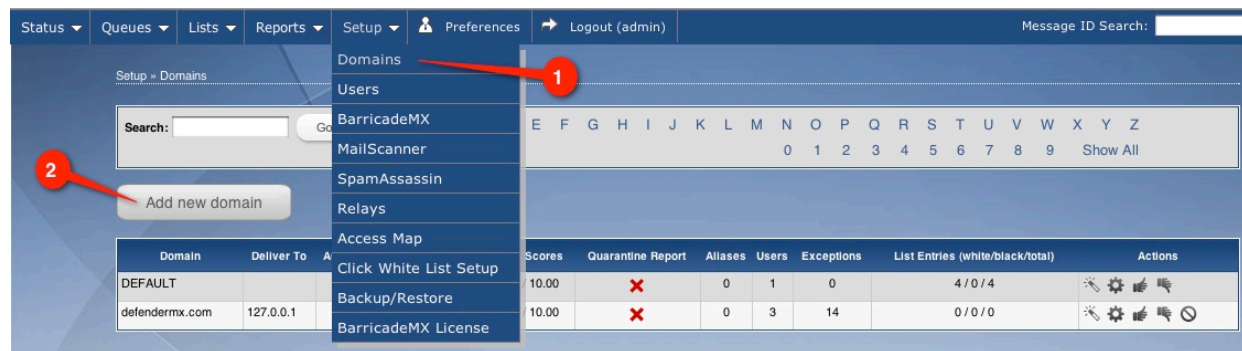


Figure 1. BarricadeMX Setup - Domains screen

Where you should select **2. Add new domain**. This will bring up the **Domain Information** screen:

Domain Information

Domain:

Message Delivery
Mail for this domain should be delivered to the following list of hosts. Delivery will be attempted to the first responding host in order.

This list can contain Hostname or IP addresses. Entries should be made one per line.

Allow host(s) to relay mail through this system

Authentication

Type:

Host:

Port:

AD Domain:

Security:

Cache passwords from non-local authentication

Defaults

Spam Checks:

Spam Scores: Low: High: Use Defaults:

Quarantine Report:

Figure 2. BarricadeMX Domain Information screen

You will need to fill in:

1. The name of the Domain
2. The IP address or FQDN of the mail hub(s)
3. Should the mail hub be allowed to relay mail out through the BarricadeMX Plus server(s)
4. User Login Authentication Type; Disabled, Local, POP3, IMAP, SMTP or Active directory (see below)
5. The IP address or FQDN of Authentication server.
6. The port number for the Authentication Service on the Authentication Server
7. Security type used; None, TLS or SSL
8. Should Spam Checks be enabled for this domain; Checked (on) or Blank (off)
9. Spam Scores; Set Low Scoring SpamAssassin and High Scoring SpamAssassin
10. Or Checked (use defaults)
11. Send Users Quarantine Reports; Checked (on) or Blank (off)
12. Select Save when the Form is completed to add the new domain

User Authentication Type

Disabled: No User Authentication will take place

Local: Local users may be created manually and will be authenticated against the credentials stored in the BarricadeMX Plus database

POP3, IMAP, SMTP: The users email address will be used to authenticate against the user's POP, IMAP or SMTP credentials on specified Authentication host

Active Directory: Please see the **Exchange Authentication** section at the end of this document

Removing Domains from BarricadeMX Plus

To remove a domain from BarricadeMX Plus scanning, use the web interface to navigate to **Setup -> Domains:**

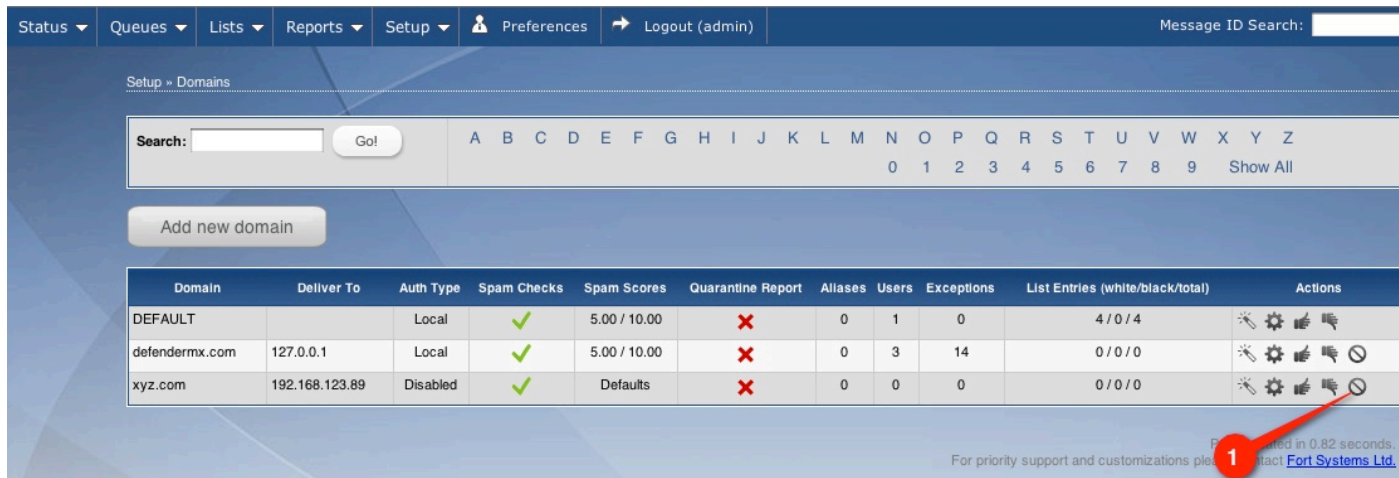


Figure 3. BarricadeMX Remove Domain screen

Then select 1. The **Delete Icon** and respond **Yes** in the pop-up window to confirm that you really want to delete the selected domain.

Allowing Domains to Relay through BarricadeMX Plus Server(s)

To allow a server or a range of IP addresses to use the BarricadeMX Plus servers as “Smart Hosts” and relay mail to the Internet for other servers, use the web interface to navigate to **Setup -> Relays**:

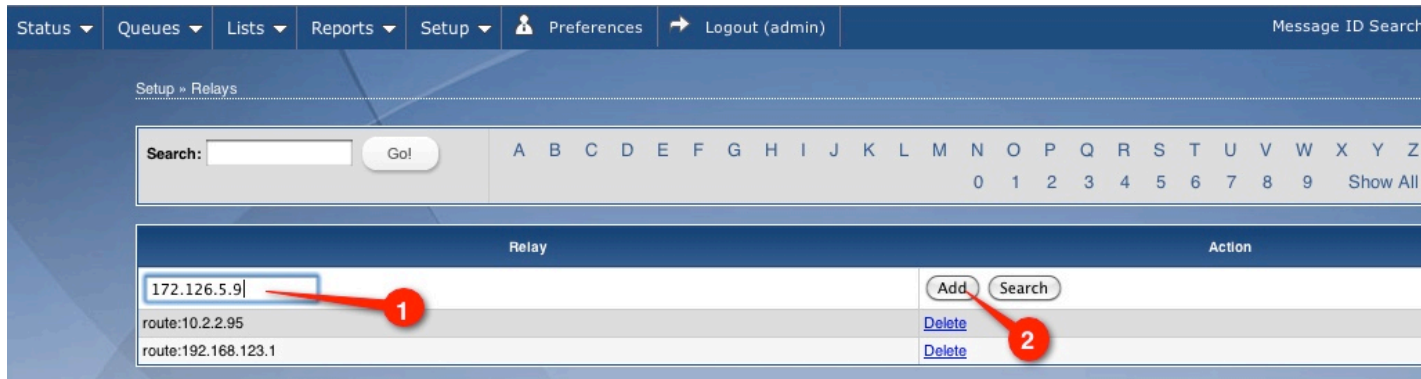


Figure 4. BarricadeMX Allow Relay screen

In the example shown above, The IP Addresses **192.168.123.1** and **10.2.2.95** are already allowed to relay and the **1.** IP Address 172.126.5.9 will be added when the **2. Add** button is selected. Note that a class “C” address can be added as a.b.c, for example 192.168.1.

Removing Relay Permissions for Servers

To stop a server or a range of IP addresses from using the BarricadeMX Plus servers as “Smart Hosts” and prevent them from relaying relay mail to the Internet, use the web interface to navigate to **Setup** -> **Relays**:

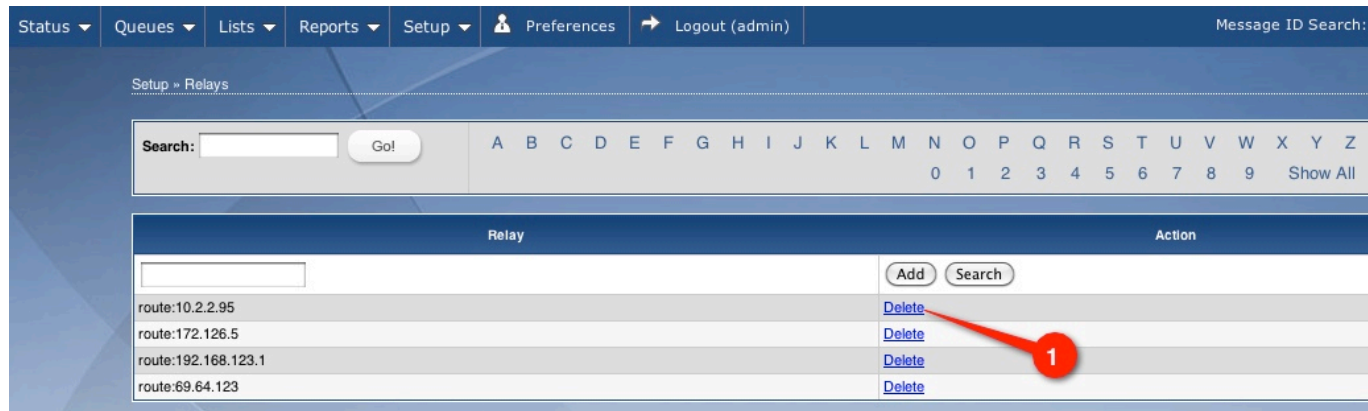


Figure 5. BarricadeMX Remove Relay screen

Selecting **1. Delete**, will remove the RELAY permissions from the server at IP 10.2.2.95.

Exchange Authentication

User logins to BarricadeMX Plus may be configured to authenticate against a mot all version and configurations of Microsoft’s Active Directory service. If you configure BarricadeMX Plus (BMX+) to authenticate against a Microsoft Active Directory or Global Catalogue, when a user logs into the BMX+ system, the system will find and store any email aliases that exist for the user in the Microsoft Directory Services. The BMX+ system will then apply the user’s white and black list preferences against email to the users principal email address and any found aliases.

New Login URLs

Because there are several different schemes used to allow user to authenticate against Microsoft Directory Services, we have made some changes to the BMX+ login page that allow two new GET variables to be supplied. These changes should allow you to configure your system so that users may supply only their email address as the username and the password associated with their User Principal Name (UPN) to login to the BMX+ system.

auth_prepend

This allows a string to be automatically added to the front of the supplied username and is typically used where pre-Windows 2000 NT usernames are used.

Example:

If my username were 'FSL\smf', the URL:

```
http://server/bmxplus/index.php?auth_prepend=FSL\
```

This would allow me to log-in using 'smf' and my AD password since 'smf' would be converted to 'FSL\smf' by the authentication functions.

auth_domain

This allows a default domain to be presumed by the authentication functions. It can be used for any authentication type.

Example:

If my username is 'smf@fsl.com', the URL:

```
http://servername/bmxplus/index.php?auth_domain=fsl.com
```

This would allow me to log-in using 'smf' and my AD password since 'smf' would be converted to 'FSL\smf' by the authentication functions.

auth_domain

This allows a default domain to be presumed by the authentication functions. It can be used for any authentication type.

Example:

If my username is 'smf@fsl.com', the URL:

```
http://servername/bmxplus/index.php?auth_domain=fsl.com
```

This would allow me to log-in as 'smf' which would then be turned into 'smf@fsl.com' by the authentication functions.

So if your domain name was exchange.com, you would supply the end-users with this link on their desktop:

```
http://<dmxplus_hostname>/bmxplus/index.php?auth_domain=exchange.com
```

They then log-in with their AD username: e.g. user@exchange.com along with their AD password; this will then get converted to 'user@exchange.com@exchange.com' correctly by the authentication functions.

Important note: if these functions are used, then the 'admin' (system administrator) user should login just as they do now using the URL:
http://<dmxplus_hostname>

Logout

Select Logout from the Top level Menu to exit the BarricadeMX Plus web interface.

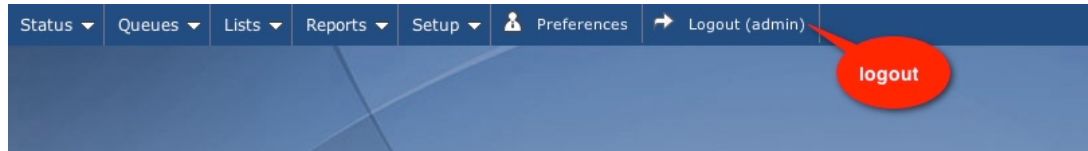


Figure 6. BarricadeMX Logout screen