

# DefenderMX QuickStart Guide

## Initial Web Screens

When you start the DefenderMX web interface for the first time, you will see the **Login:** screen.

Please use:

**Email Address:** administrator

**Password:** password

To authenticate and login.

You will next see the **users-administrator preferences** screen.

Please enter a new password for the administrator and the First and Last names of the DefenderMX administrator and select **UPDATE**.

You will next see the **domain management - my domains** screen. Please add at least one domain. Please fill in:

<b>domain:</b>	enter the name of a domain for which you will receive email. This should be the Fully Qualified Domain Name, i.e. mycompany.com
<b>destination mail server:</b>	enter the name or IP address of the mail hub where the mail for this domain should be delivered. Note that this mail hub must be configured to accept mail from the DefenderMX system or mail will NOT be delivered.

At least one domain should be entered at this time and additional domains may be configured later. When you are finished, please select **UPDATE**.

You will see the **Login:** screen again. Please use:

Email Address: administrator

Password: <your-new-password>

To authenticate, login and begin configuring the system. The most commonly changed configuration parameters are listed below. They are intended to get your system up and running with basic configuration for your site and your system. They are not a substitute for reading the manual. To fully use the power and flexibility of DefenderMX, you must read the manual. To start configuring your system, please select:

scanner configuration

### scanner configuration - general:

Selection made in the scanner configuration sections will affect site-wide settings. For modification of domain and user settings, please see [domain management - my domains - preferences](#) (by domain) and [users - user management - preferences](#) (by user)

### Scanner Processes Per CPU (Max Children):

This depends of the number of processors installed in your system. Typical settings are:

Single processor w/ 1 GB memory: 5

Single Dual Core processor w/ 2 GB memory: 10

Dual processors w/ 2 GB of memory: 10

Note that each Scanner Process uses between 60 to 70 MB of RAM. So the number of Scanner Process should never exceed  $[70\% \text{ of available RAM (MB) } / 70 \text{ MB}]$ .

### Sign Clean Messages:

If you change this to yes, the system will append a signature message to the end of clean messages indicating that the message was scanned and found to be clean. Please see: [scanner configuration -notification - notices editor - inline.sig\(1\) and inline.sig\(2\)](#)

### Find Phishing Fraud:

Phishing fraud messages are attacks that look like a genuine email message from your bank and contain a link to the web site where you will be asked to type in personal information such as your account number or credit card details. This fraud can be detected because the real address of the link in the message is not the same as the text that appears to be the link. Setting this option to yes will reveal the real, previously hidden, destination of the counterfeit link.

### Also find Numeric Phishing

If this option is set to yes, setting this option to yes will point out links to numeric IP addresses. Genuine links to totally numeric IP addresses are very rare, so this option is set to "yes" by default. If a numeric IP address is found in a link, the same phishing warning message is used as in the Find Phishing Fraud option above.

### Expand TNEF:

This should be "yes" unless the scanner you are using Sophos or McAfee virus scanners

## scanner configuration - spam:

### Spam Actions:

Typical selections are "deliver" or "attachment deliver".

- Selecting Deliver will deliver spam to the recipient with the Subject: line modified as defined in [High Scoring Spam Modify Subject](#): (see above)
- Selecting "attachment deliver" will deliver spam to the recipient with the Subject: line modified as defined in [High Scoring Spam Modify Subject](#): (see above). The original spam message will be included as an attachment to a warning message. Please see [scanner configuration -notification - notices editor - inline.spam.warning](#)

### High Scoring Spam Actions:

Typical selections are "store", "attachment deliver" or delete

- Selecting "store" will quarantine the spam. Use [MailWatch](#) to release messages from quarantine. Messages are typically kept in quarantine for 30 days.
- Selecting "attachment deliver" will deliver spam to the recipient with the Subject: line modified as defined in [High Scoring Spam Modify Subject](#): (see above). The original spam message will be included as an attachment to a warning message. Please see [scanner configuration -notification - notices editor - inline.spam.warning](#)
- Selecting "delete" will delete the spam from the system. Many Sites prefer to change this setting to delete seeing that no "real" email is ever marked as "High Scoring Spam"

## scanner configuration - virus:

### Virus Scanners:

Select your virus scanner. ClamAV called by the clamavmodule is installed as the default. If you install additional virus scanner(s) please note that this virus scanner must be installed before selecting it from the list. Please see [Installing Virus Scanners](#) in the [DefenderMX Manual Manual](#).

## scanner configuration - notification:

While you might want to edit the defaults in this section, the default settings are sufficient for many sites. To view and edit these files please select the

**NOTICES EDITOR**

Button at the bottom of the page. This will bring up the notices editor. Clicking on a report name will bring up the report in a simple text editor. Edit each report and save.

**IMPORTANT:** When you have reached this point please select the

commit changes

Button at the bottom of the screen. This will record and propagate your configuration changes.

Next select:

## scanner configuration - attachments:

Carefully review the data on this page for conformance with your sites security policies. Attachments may be blocked based on either filename, the [Attachment File Name Filters](#) list or the file type, [Attachment File Type Filters](#) list.

Rules may be enforced by selecting “allow” or “deny” at the left side of each rule. Additional rules may be added at the end of the [Attachment File Name Filters](#) list and the end of the [Attachment File Type Filters](#) list.

## Domain management - my domains:

For each domain, please select the **preferences** button at the far right of the screen. This will bring up the Editing <domain\_name> screen. On this screen you should:

- Add white and Black list entries specific to this domain.
- Select the desired spam score level for the domain
- Select whether milter-ahead should be used for the domain.
- Select the authentication type for the domain. This is the method that will be used when a user logs in to set individual preferences. Users login by using their email address, i.e. [username@mydomain.com](#) at the login prompt. If they are a locally authenticated user, (one added by using the [users - user management](#) function in SMGateway), they must supply their local password. If they do not have a local account on the SMGateway system they will supply the password that is normally used for them to authenticate against their mail hub. They will then be authenticated by the method you select at the bottom of this screen. Please fill in:

## MILTER AHEAD SETTINGS

For each POP, IMAP and Exchange 2003 domain, please click on the check box in front of

Use milter-ahead filtering on this domain

To enable the DefenderMX to validate that the email address is valid on the destination mailhub BEFORE accepting the email at the gateway.

**Please Note** – in order to successfully authenticate using Milter-Ahead on an Exchange 2003 server, you must ensure that Exchange has been configured to reject email for invalid users. This is not the default Exchange 2003 behavior. Please see the SMGateway Manual for detailed instructions or download the instructions from:

<http://www.fsl.com/support/Milter-Ahead-Exchange-Settings.pdf>

Since it is not possible to configure Exchange 5.5 or Exchange 2000 to reject email for invalid users, do not enable Milter-Ahead for Exchange 5.5 or Exchange 2000 destination mailhubs.

## AUTHENTICATION SETTINGS

- authentication host:** enter the name or IP address of the mail hub that can authenticate the user. This should be IP address or the Fully Qualified Domain Name, i.e. mail.mycompany.com
- authentication type:** Enter the type of authentication used on the mail hub. Select from:  
--- NO AUTHENTICATION – No local user logins  
Active Directory - Microsoft Exchange  
POP- Post Office Protocol  
IMAP - Internet Message Access Protocol  
Local - User has account on SMGateway system

SMGateway provides 4 different ways in which users are authenticated.

- Active – Microsoft Active Directory
- POP – Post Office Protocol
- IMAP – Internet Message Access Protocol
- Local – User has an account on SMGateway

Select the authentication type for the domain. This is the method that will be used when a user logs in to set individual preferences. Users login by using their email address, i.e. [username@mydomain.com](mailto:username@mydomain.com) at the login prompt. If they are a locally authenticated user, one added by using the **users – user management** function in DefenderMX, they must supply their local password. If they do not have a local account on the DefenderMX system they should supply the password that is normally used for them to authenticate against their mail hub. They will then be authenticated by the method selected for **authentication type**.

**Please Note** – in order to successfully authenticate using Active Directory on an Exchange 5.5 server, you must ensure that the Active Directory Connector (ADC) has been successfully implemented; otherwise you may only authenticate using POP or IMAP.

### **Authentication Settings:**

- Authentication type** Enter the type of authentication used on the mail hub. Select from:
- active directory – Microsoft Active Directory

pop – Post Office Protocol  
imap – Internet Message Access Protocol  
local – User has an account on the  
SMGateway system

**If pop or imap is selected:**

**authentication host:** enter the name or IP address of a system that can authenticate the user. This should be the Fully Qualified Domain Name, i.e. mail.mycompany.com

**enable ssl:** Check if ssl is enabled on the authentication host or leave blank if ssl is not used.

**port:** Enter the port number to use on the authentication host. The values listed below are the normal ports used by these services.

pop:	110
pop with ssl:	995
imap:	143
imap with ssl:	993
Active Directory:	389

**leave fields blank:** Please leave the Active Directory Username, Active Directory Password and Active Directory Domain Name fields blank if you are authenticating using POP or IMAP.

**If Active Directory is selected:**

**Authentication host:** Enter the Fully Qualified hostname of the Active Directory Domain Controller

**Active Directory Username:** Enter the username of a user who has at least read permissions on the Active Directory. This must be entered in the form *domain\username* where *domain* is the netbios domain name for your Active Directory domain, and *username* is the name of the account with read access to AD

**Active Directory Password:** Enter the password of the username that you entered above.

**Active Directory Domain:**

Enter the name of the Active Directory domain used for authentication

Next select:

**utilities** > **diagnostics**

Then select:

**Generate Sample Email**  
**Generate Sample Spam**  
**Generate Sample Virus**

To send test messages to DefenderMX

*Please Note - For the **Generate Sample Spam** test to work, your system must have fully qualified DNS "A" and "PTR" records.*

Use **mailwatch** to verify that the results are successful.

## CONFIGURE MTA BLOCKING

Most systems that receive email principally from the United States and Western Europe will want to configure blocking email from domains listed in [sbl-xbl.spamhaus.org](http://sbl-xbl.spamhaus.org). To turn on this blocking

select **utilities** and then select [configure MTA blocking](#) and the select

**TURN ON Spamhaus XBL-SBL MTA-LEVEL BLOCKING**

## FINISHING UP

When you are satisfied with your configuration, the results of the tests and are satisfied that the DefenderMX system is ready for production, you will need to redirect all incoming email to the new DefenderMX. This is typically accomplished by:

- Redirecting port 25 traffic on the firewall from the existing email hub to the new DefenderMX

OR

- Changing the MX records for the domain to point to the new DefenderMX. If this method is to be selected you should shorten the TTL (Time to Live) value in your DNS MX records. Typically this is done a day or two before the actual records are to be changed. A reasonable value is 5 minutes.

Carefully monitor the mail flow through the DefenderMX using the **MailWatch** to monitor Message Flow, Spam Detection, Load Average, inbound and outbound Mail Queues. If any problems occur please see the **Trouble Shooting** section of the **DefenderMX Manual**. If you are still stumped, please file a report at [www.fsl.com/customer\\_support](http://www.fsl.com/customer_support).

## STILL TO DO

Congratulations. Your system is now working with a basic configuration. Please read the **DefenderMX Manual** to start fine tuning your system and adding additional functionality. Please see the **Common Tasks** section of the manual to learn how to:

- Adding a Local User
- Adding a Domain
- Promoting a User to an Administrator

- Creating White and Black List Entries
- Tracking a Message