ZLD Series - Anti-Spam

Anti-Spam Setup for 4.XX Firmware version and higher

What is Anti-Spam

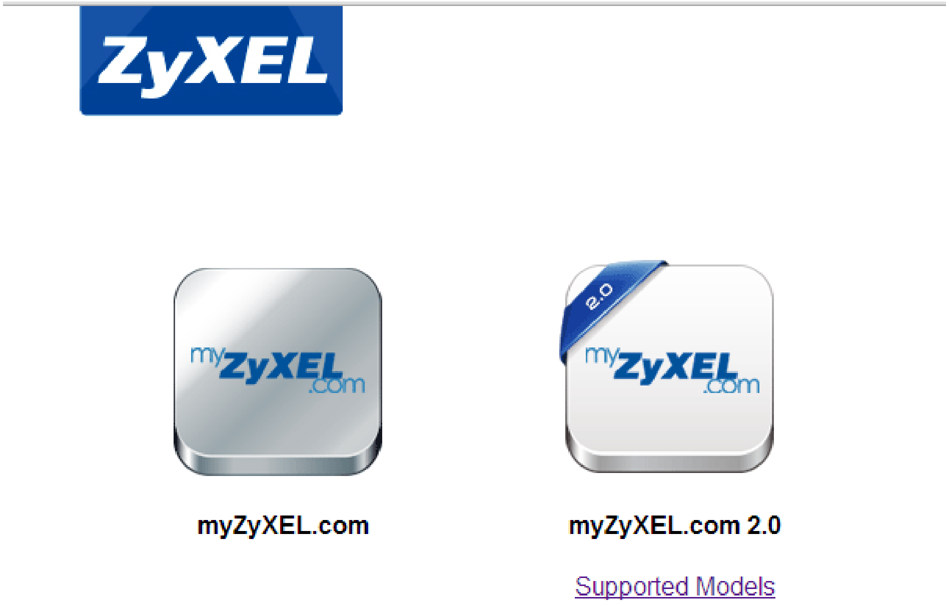
Anti-Spam is a feature that allows the USG to check incoming mail and mark it as spam . This is a licensed service that can be purchased for the USG series firewalls. In addition to signature based detection, the USG can rely on a DNS Blacklist for reputation and then flag the email header as spam so that when it reaches your inbox it can be sent directly to the folder you wish

When to use it

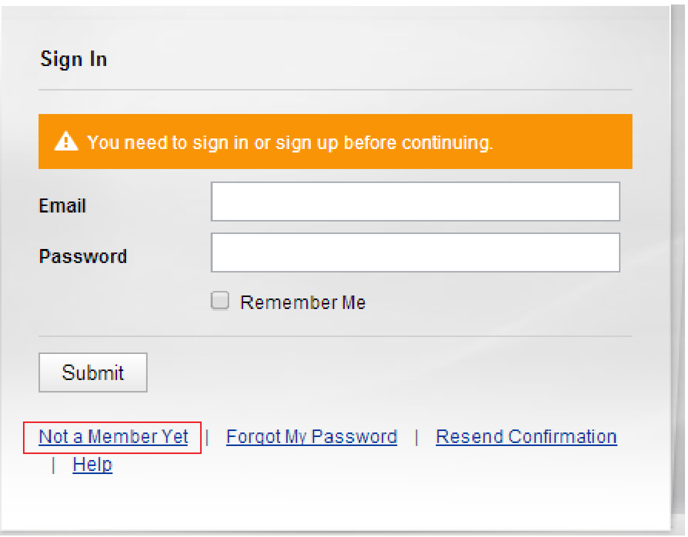
Anti-Spam is useful when you have an internal mail server that is exposed to the outside. Oftentimes outside users can get a hold of your email domain and constantly send spam mail. In some instances, an email server can receive up 1000 spam emails a day. With Anti-Spam you can send flagged email messages to a specific folder

How to Register Anti-Spam

In order to use Anti-Spam, you first need to purchase a Anti-Spam. The license is an alphanumeric key that is purchased from our resellers. First you will need to link your device to a MyZyXEL account. A MyZyXEL account is used to manage and update subscription services on the USG. In order to get the device registered, go to http://www.myzyxel.com and click on MyZyXEL 2.0



You will be prompted with the login screen and an option at the bottom to create a new account by clicking on "Not a Member Yet"



Sign In

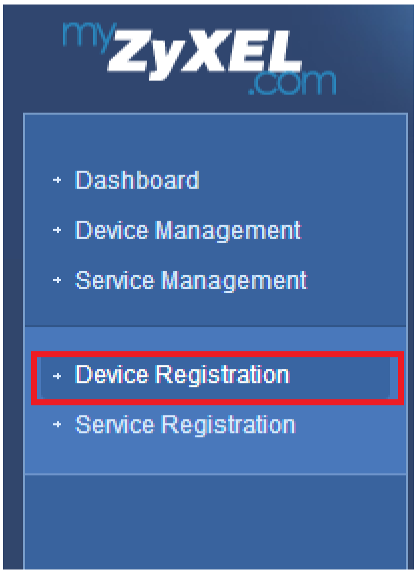
You need to sign in or sign up before continuing.

Email

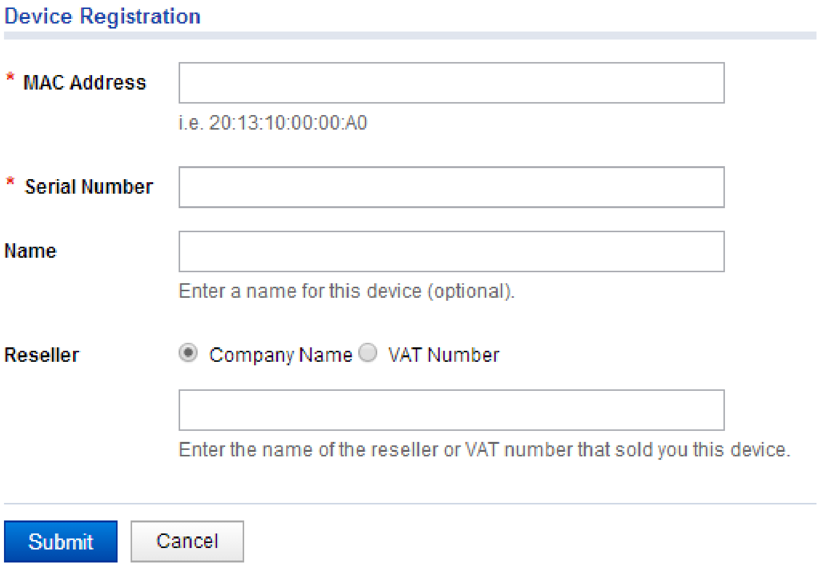
Password

□ Remember Me

Once the information is filled out, log into your myzyxel account.
On the left hand side you will find different menu options. Clicking on "Device Registration" will allow you to enter in the information of your USG to link it to your myzyxel account.



Enter in the first Mac Address that is found on the unit. The Mac Address can be found on the bottom of the USG or on the USG's Dashboard. Make sure to only enter in the First Mac Address of the Mac Address range for the unit. The Serial number can also be found on the bottom of the unit and on the USG's admin dashboard. For the Name, enter in the name of the USG to help differentiate the device from other units you may register, such as Los Angeles USG. Reseller information is not necessary unless you are a reseller so that field can be skipped. Select Submit when finished and the device will be registered.



Device Registration

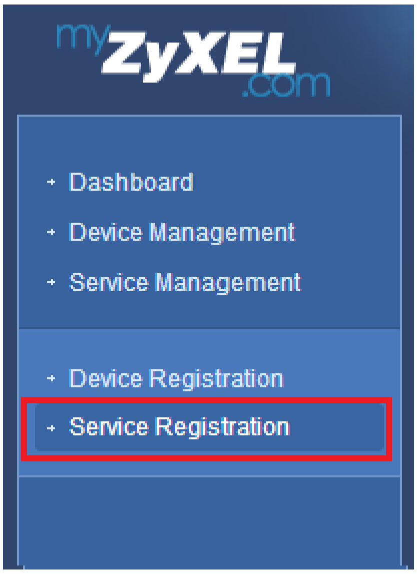
* MAC Address
i.e. 20:13:10:00:00:A0

* Serial Number

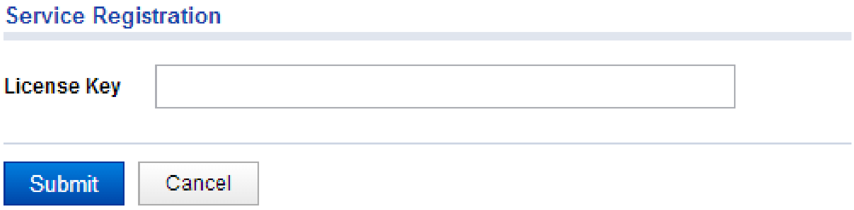
Name
Enter a name for this device (optional).

Reseller ● Company Name ○ VAT Number
Enter the name of the reseller or VAT number that sold you this device.

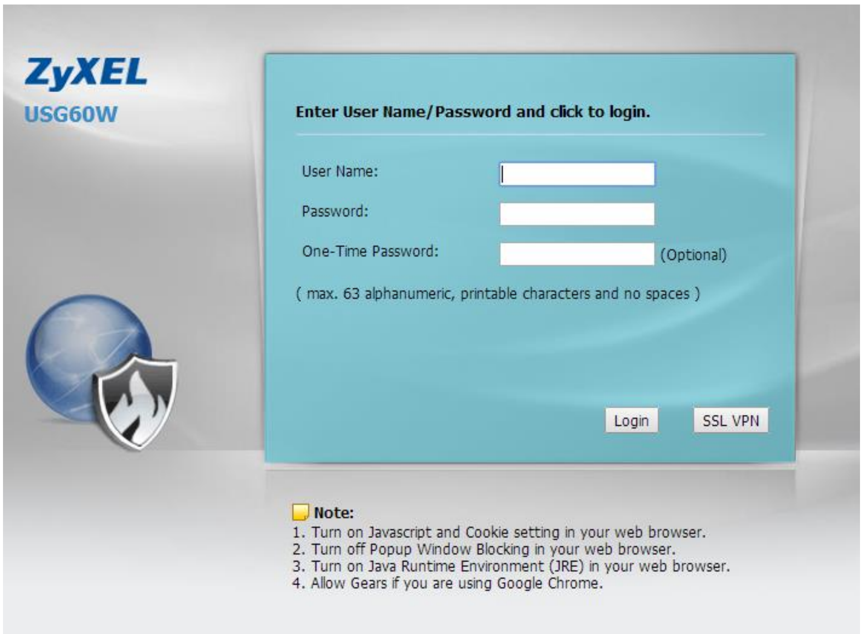
After the device is registered, you will need to apply a license to the device. While in your account, click on "Service Registration"



Enter in the license key in order to register the license to the account. You will be given the option later to link the key to the USG of your choice



Once the device is linked, you can begin to setup Anti-Spam.
For the final step, you will need to sync your USG with the MyZyXEL account so that the registration settings match up. Log into your USG's Administration Page



Enter User Name/Password and click to login.

User Name:

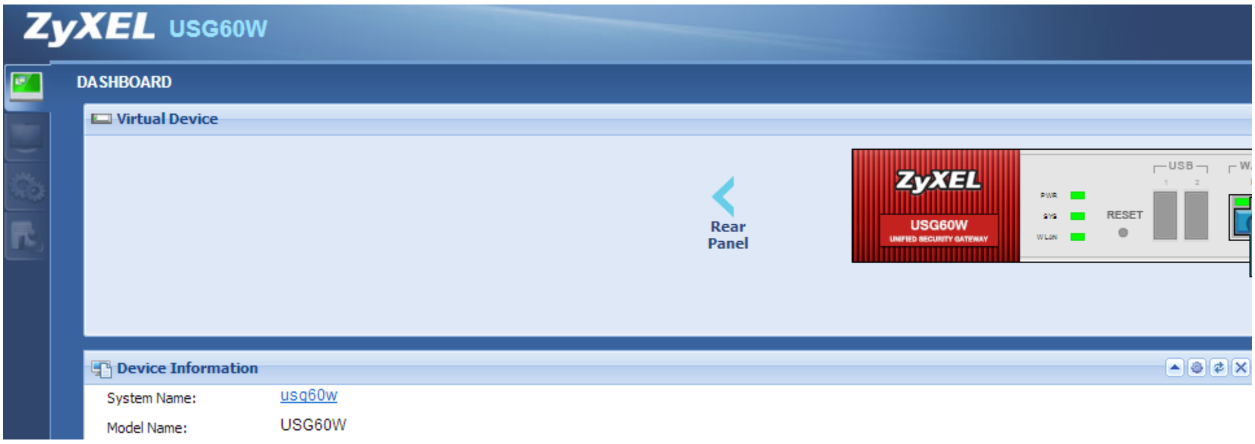
Password:

One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

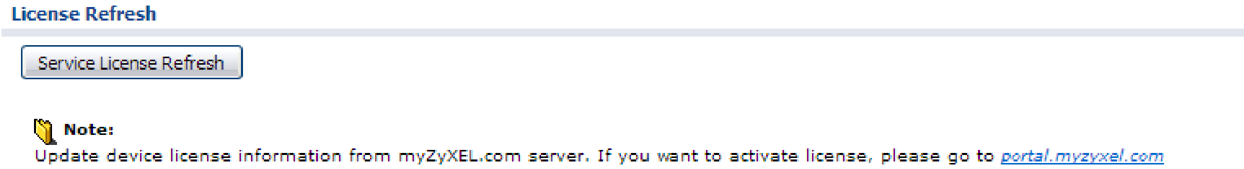
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

Once inside on the main admin page, look on the left hand side for the menu



System Name:	usg60w
Model Name:	USG60W

Click on the Configuration Gears > Licensing > Registration > Service and click on “Service License Refresh” at the bottom:



License Refresh

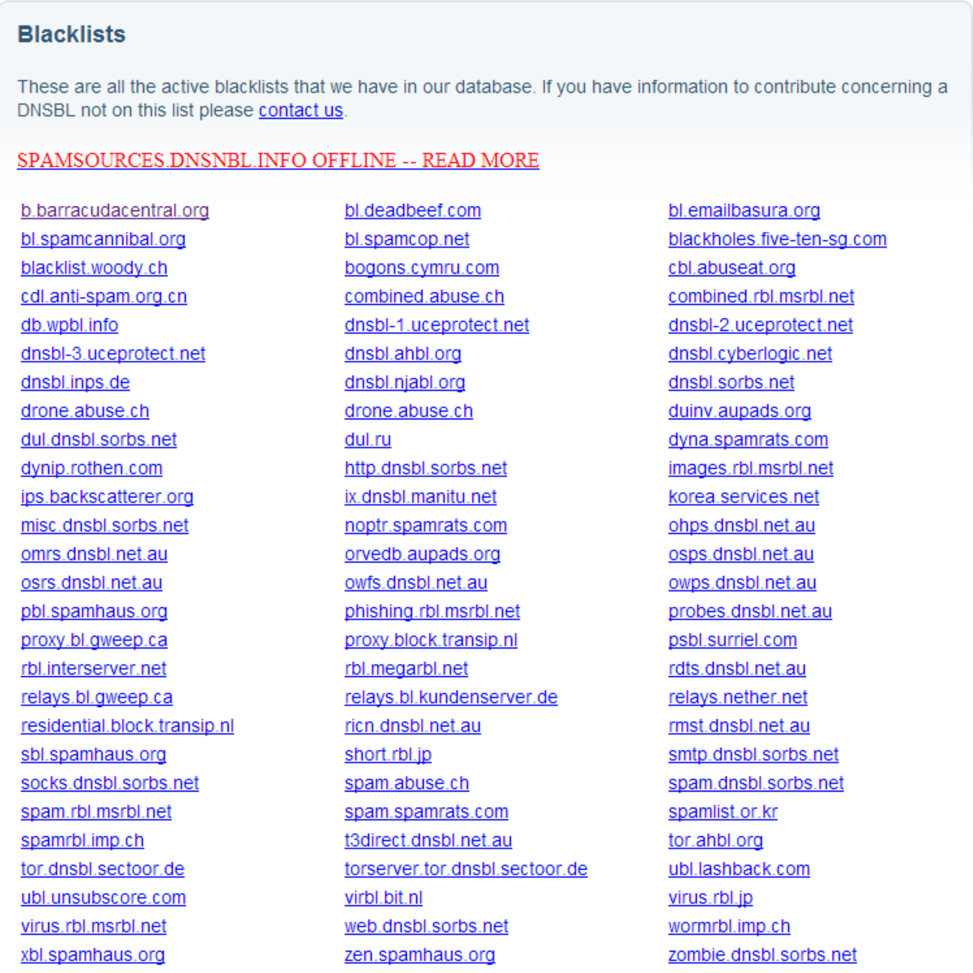
Note:
Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com

This will sync the USG to the MyZyXEL Account and update the expiration dates on the licenses. Once this is completed, click on the configuration gears to enter into the USG configuration settings. Click on UTM Profile > Anti Spam.

How to Setup Anti-Spam

DNSBL

The DNSBL option on Anti-spam allows you to enter in the server that contains a list of blacklisted DNS host addresses. Normally you can find such providers at http://dnsbl.info



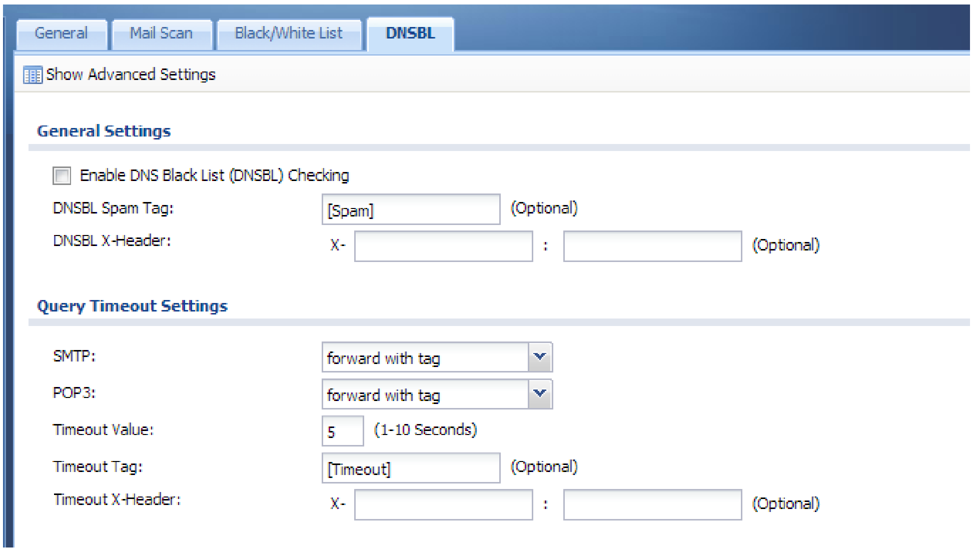
Blacklists

These are all the active blacklists that we have in our database. If you have information to contribute concerning a DNSBL not on this list please contact us.

SPAMSOURCES.DNSNBL.INFO OFFLINE -- READ MORE

b.barracudacentral.org
bl.spamcannibal.org
blacklist.woody.ch
cdl.anti-spam.org.cn
db.wpbl.info
dnsbl-3.uceprotect.net
dnsbl.inps.de
drone.abuse.ch
dul.dnsbl.sorbs.net
dynip.rothen.com
ips.backscatterer.org
misc.dnsbl.sorbs.net
omrs.dnsbl.net.au
osrs.dnsbl.net.au
pbl.spamhaus.org
proxy.bl.gweep.ca
rbl.interserver.net
relays.bl.gweep.ca
residential.block.transip.nl
sbl.spamhaus.org
socks.dnsbl.sorbs.net
spam.rbl.msrbl.net
spamrbl.imp.ch
tor.dnsbl.sectoor.de
ubl.unsubscore.com
virus.rbl.msrbl.net
xbl.spamhaus.org
bl.deadbeef.com
bl.spamcop.net
bogons.cymru.com
combined.abuse.ch
dnsbl-1.uceprotect.net
dnsbl.ahbl.org
dnsbl.njabl.org
drone.abuse.ch
dul.ru
http.dnsbl.sorbs.net
ix.dnsbl.manitu.net
noptr.spamrats.com
orvedb.aupads.org
owfs.dnsbl.net.au
phishing.rbl.msrbl.net
proxy.block.transip.nl
rbl.megarbl.net
relays.bl.kundenserver.de
ricn.dnsbl.net.au
short.rbl.jp
spam.abuse.ch
spam.spamrats.com
t3direct.dnsbl.net.au
torserver.tor.dnsbl.sectoor.de
virbl.bit.nl
web.dnsbl.sorbs.net
zen.spamhaus.org
bl.emailbasura.org
blackholes.five-ten-sg.com
cbl.abuseat.org
combined.rbl.msrbl.net
dnsbl-2.uceprotect.net
dnsbl.cyberlogic.net
dnsbl.sorbs.net
duinv.aupads.org
dyna.spamrats.com
images.rbl.msrbl.net
korea.services.net
ohps.dnsbl.net.au
osps.dnsbl.net.au
owps.dnsbl.net.au
probes.dnsbl.net.au
psbl.surriel.com
rdts.dnsbl.net.au
relays.nether.net
rmst.dnsbl.net.au
smtp.dnsbl.sorbs.net
spam.dnsbl.sorbs.net
spamlist.or.kr
tor.ahbl.org
ubl.lashback.com
virus.rbl.jp
wormrbl.imp.ch
zombie.dnsbl.sorbs.net

Choose the DNSBL servers you would like to import into the USG, then go to the DNSBL tab



General Settings

□ Enable DNS Black List (DNSBL) Checking

DNSBL Spam Tag: [Spam] (Optional)

DNSBL X-Header: X- _____ : _____ (Optional)

Query Timeout Settings

SMTP: forward with tag

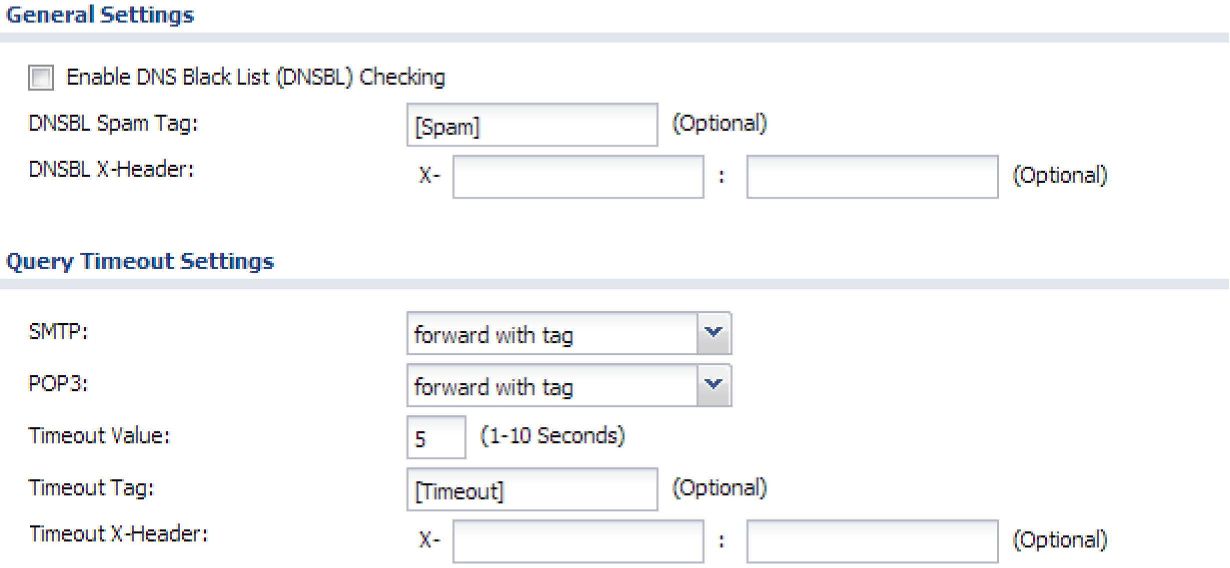
POP3: forward with tag

Timeout Value: 5 (1-10 Seconds)

Timeout Tag: [Timeout] (Optional)

Timeout X-Header: X- _____ : _____ (Optional)

Scroll down to the bottom and click on Add under the DNSBL Domain List to add the DNSBL hosts that you would like to have check. Also do not forget to enable DNSBL checking



General Settings

□ Enable DNS Black List (DNSBL) Checking

DNSBL Spam Tag: [Spam] (Optional)

DNSBL X-Header: X- _____ : _____ (Optional)

Query Timeout Settings

SMTP: forward with tag

POP3: forward with tag

Timeout Value: 5 (1-10 Seconds)

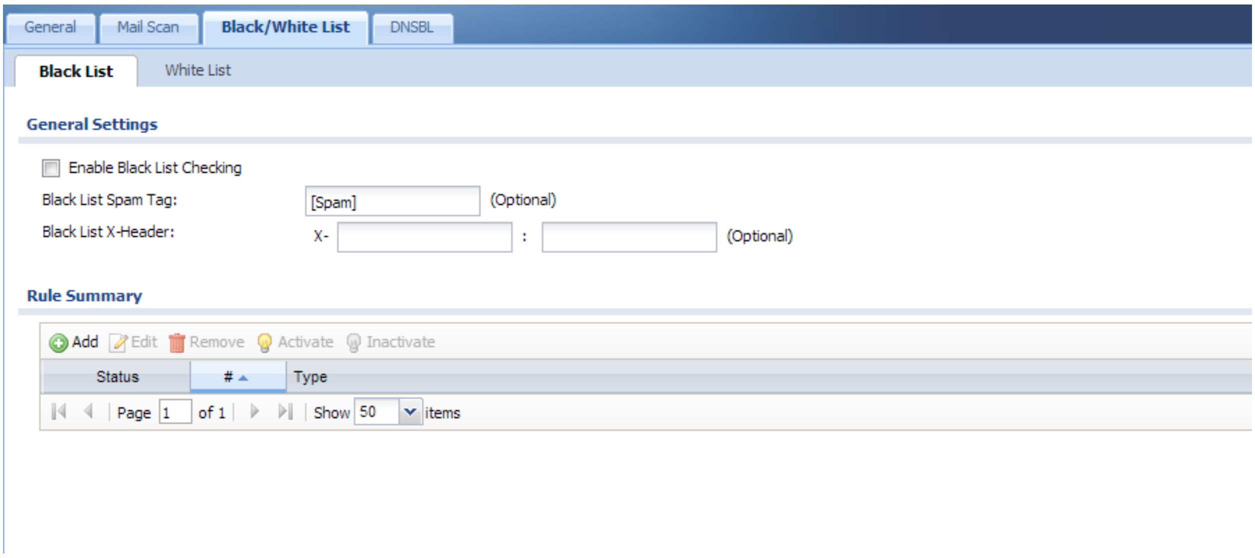
Timeout Tag: [Timeout] (Optional)

Timeout X-Header: X- _____ : _____ (Optional)

You also have the option to create a DNSBL tag. This tag will modify the header so that when the offending email comes into the inbox, you can create rules with your email to forward the tag to a specified folder.

Black/White List

The Black/White List will allow you to create specific rules for allowing or blocking specific domains. Click on "add" under rule summary to add addresses to the list. Similarly to the DNSBL list you can create a custom header for sorting purposes.



General Settings

□ Enable Black List Checking

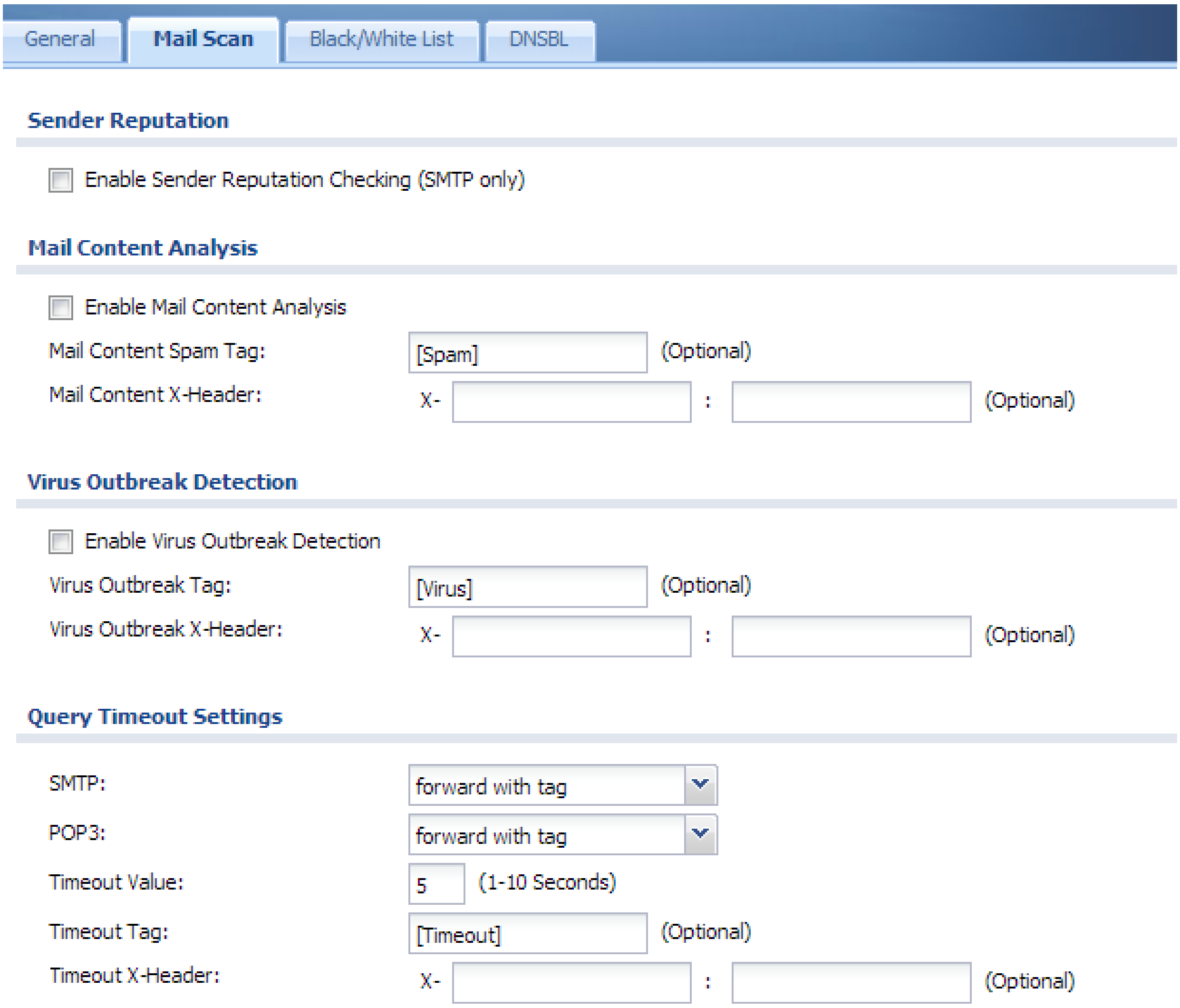
Black List Spam Tag: [Spam] (Optional)

Black List X-Header: X- : (Optional)

Rule Summary

Mail Scan

Mail Scan can be setup to scan for virus outbreaks and flag the header with a custom message. You can also set the query timeout setting for scanning POP and SMTP



Sender Reputation

□ Enable Sender Reputation Checking (SMTP only)

Mail Content Analysis

□ Enable Mail Content Analysis

Mail Content Spam Tag:	[Spam]	(Optional)		
Mail Content X-Header:	X-		:	(Optional)

Virus Outbreak Detection

□ Enable Virus Outbreak Detection

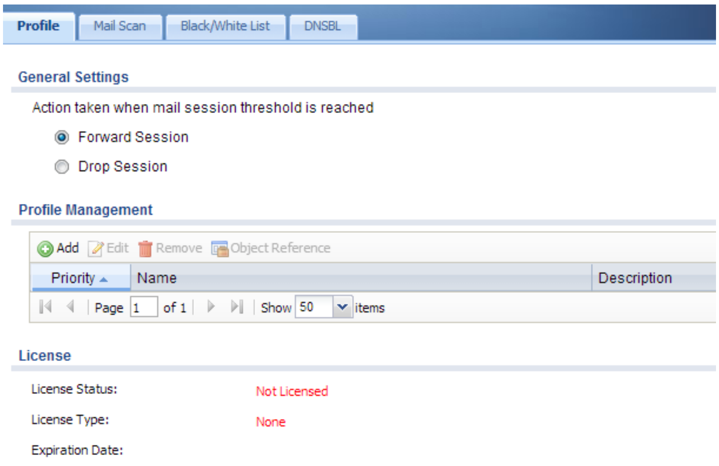
Virus Outbreak Tag:	[Virus]	(Optional)		
Virus Outbreak X-Header:	X-		:	(Optional)

Query Timeout Settings

SMTP:	forward with tag			
POP3:	forward with tag			
Timeout Value:	5	(1-10 Seconds)		
Timeout Tag:	[Timeout]	(Optional)		
Timeout X-Header:	X-		:	(Optional)

Profile

In the Policy section you can setup a policy and select what you would like the Anti-Spam to check as along with the email direction. You will note that there is an option on what to do when the mail session threshold reaches. There is a threshold on each USG as to how many emails the device scan scan. Please refer to the documentation for your specific USG to determine what this number is.



General Settings

Action taken when mail session threshold is reached

● Forward Session

○ Drop Session

Profile Management

Priority ▲	Name	Description

Page 1 of 1 | Show 50 items

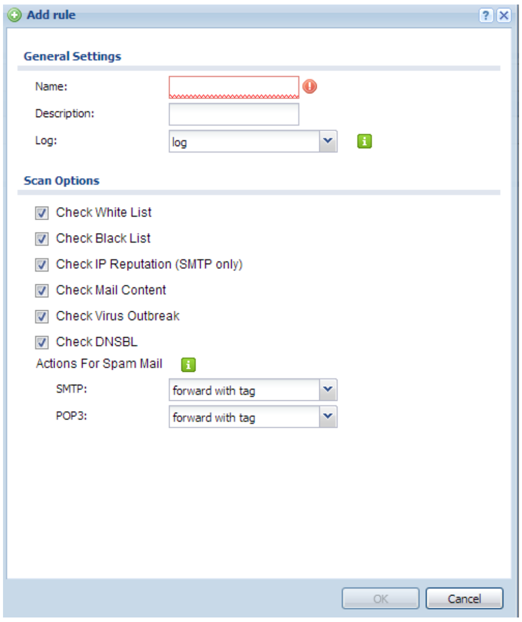
License

License Status: Not Licensed

License Type: None

Expiration Date:

You will be able to set what your scan options for the profile that you set up



General Settings

Name:

Description:

Log: log

Scan Options

☑ Check White List

☑ Check Black List

☑ Check IP Reputation (SMTP only)

☑ Check Mail Content

☑ Check Virus Outbreak

☑ Check DNSBL

Actions For Spam Mail

SMTP: forward with tag

POP3: forward with tag