

E-Mail Anti-Spam Settings

- Using Only SmarterMail Anti-Spam Tools – Rev 4.0066: 28-Mar-2013

UPDATE SUMMARY:

Since the production of the original SmarterMail Anti-Spam Tools document in 2009, much has changed in the fight against spam. SPF has finally started to become more widely used, and even mandated by some ISPs. rDNS, originally a “strongly suggested” lookup tool has, albeit not officially per the IETF, become mandatory lookup match for e-mail to be accepted by most large ISPs and many smaller providers have also adopted those same requirements. With the addition of DOMAIN KEYS, DKIM, the DMARC protocol, those three tests, along with SPF, can be used to tie them all together and provide almost proof positive evidence that an e-mail either did, or didn’t actually originate from a stated MX server.

This document has not only been updated to show the changes included in SmarterMail 11.X, but also to provide additional information on correct SPF records. Most DNS admins setup their SPF to use “~all” or “?all” at the end of their records and that makes them little more than meaningless placeholders when it comes to authenticating messages from the domain. For an SPF record to take a firm stance on authenticating against the data in the record, it should only have a “-all” [minus all] at the end. That indicates that messages can ONLY originate via the name MX server(s) or IP ADDRESS(s) contained in the SPF record. [See: http://www.openspf.org/SPF_Record_Syntax]

This document will also touch on the basics of why the RBL and URIBL settings indicated work. In the past there has been some confusion about what were acceptable responses from RBL databases and some have stated that the “only acceptable response” was “127.0.0.2.” That’s not true. Many different responses can be returned by RBL and URIBL database providers and the RBL and URIBL tests listed in this document have been have been updated to reflect those newly known results.

By updating RBL and URIBL “multi” response query results to query for individual positive spam results, these new individual tests will also ignore results which are now being pushed by the RBL and URIBL database providers which indicate when “too many queries” have been received from a group of DNS servers. In many cases, those “too many queries” results were improperly interpreted as positive spam results.

Many SmarterMail users have also realized issues with rDNS reporting as negative when outside tests clearly showed valid rDNS servers were available for incoming e-mail which was being tested. The testing we have run over the last several months has indicated that DNS servers used for SmarterMail must be extremely fast.

This also leads to recommending that the DNS server entries in SmarterMail no longer be left blank, meaning that SmarterMail will use the DNS of the server on which it is installed. I am, therefore, recommending that anyone who installs SmarterMail also designate the DNS servers which will be used to query rDNS, RBL, and URIBL as well as the routing to all external locations.

SmarterMail version 11.X also adds some extremely powerful protection tools, brings incredible speed to a product which is almost completely re-written, and brings ActiveSync to more devices than any previous version. The newly re-written code and protection tools, outlined under Abuse Detection beginning on page 51, outline those abuse detection tools.

History:

Beginning with SmarterMail 6, SmarterTools began incorporating some very powerful tools into the SmarterMail e-mail server software which made the control of undesired SPAM much easier.

Prior to version 6 of the SmarterMail software, it was necessary to maintain blacklists, build complicated tables of undesired words, phrases, IP address, e-mail addresses, and domains – all of which changed almost every hour.

The spammers knew the ISPs and e-mail server operators were up against a wall and, in spite of new state and federal regulations being put into place almost daily, continued to churn out ever more junk mail because they were unconcerned with being stopped or caught. With the introduction of SmarterMail version 6, the tide began to turn in favor of the e-mail server operators. A chart showing both the EU and US Antispam requirements is included in Section L, beginning on page 59 of this document.

Between the more frequent adaptation of SPF, the general requirement of large ISPs that mail server operators have both rDNS [reverse DNS / IN-ARPA] AND PTR records pointing back at the HOST and MX records of their respective mail servers, and the new tools being coded into the SmarterMail e-mail server system, e-mail server operators finally began to accumulate an arsenal in the war of the spammers vs the mail server operators.

In July 2009, ChicagoNetTech converted from IMail to SmarterMail version 5. Within a week of our purchase and conversation, SmarterTools introduced the BETA of SmarterMail version 6, and with SmarterMail Version 6 BETA, a powerful new set of anti-spam tools which would change our relationship with our customers significantly.

As ChicagoNetTech began to work with SmarterMail version 6 BETA, and experimented with various anti-spam configurations, we soon found the tools introduced with SmarterMail version 6 BETA allowed some very powerful capabilities in the fight against spammers.

After testing with one of our minor domains, we decided to “flip the switch” and ran the new anti-spam settings we were using on just one domain on all of the domains. Suddenly, instead of complaints about the large quantities of spam users previously received in their in-boxes, we were receiving compliments about how pleasant it was to open their e-mail in the morning and find that everything in those boxes was 100% related to business.

The spam was gone, the customers were extremely happy, and we have not looked back since then.

In July of 2009, after assisting many SmarterMail admins on the SmarterMail forum with anti-spam issues, I decided to publish my settings for the benefit of everyone's SmarterMail installations.

Since then many have adopted and, to their surprise, have had similar results to those we experienced from the beginning.

Unfortunately the software used for the SmarterMail forums allows for a limited number of characters in each post. Thus it was necessary split the original post into two sections. The forum software also limits the number of images in any given post and that has resulted in many questions as to the implementation of specifics relating to the anti-spam settings effectively implemented on our and other SmarterMail server operators.

This newly updated document will restate those settings, in somewhat greater detail, along with IETF specifications relating to why they work and why you should make certain you are in full compliance with both IETF requirements and recommendations.

The antispam settings listed below are the settings currently used by ChicagoNetTech Inc, an ISP in Chicago Illinois, with client base consisting primarily of not-for-profit agencies, healthcare facilities, and small businesses. ChicagoNetTech runs SmarterTool's SmarterMail Enterprise version 11.0 – latest available software release.

These settings are based on SmarterMail Enterprise Edition, Version 11.0. SmarterMail owners who run the Professional version of SmarterMail, as well as versions earlier than 11.0 may have slightly different settings or screens. More information about the differences in SmarterMail versions is available on the [SmarterMail Version Comparison Page](#). [Note that the LITE version has been eliminated with SmarterMail 11.0]

1. Setup your primary GREYLISTING settings:

To do this, login as the primary ADMIN for the SmarterMail server and goto:

SECURITY → GREYLISTING → OPTIONS

- **SELECT ENABLE GREYLISTING**
- **UNSELECT ENABLE USERS TO OVERRIDE GREYLISTING**
- **SET your BLOCK PERIOD – we use 4 minutes**
- **SET your PASS PERIOD – we use 360 minutes**
- **SET your RECORD EXPIRATION – we use 36 days –this can be longer if you desire**
- **Set APPLY TO EVERYONE EXCEPT SPECIFIED COUNTRIES / IP ADDRESSES**

The screenshot shows the 'Greylisting' configuration page in SmarterMail. At the top is a blue header with a back arrow and the title 'Greylisting'. Below the header is a light blue bar with a 'Save' button. The main content area has two tabs: 'Options' (selected) and 'Filters'. Under the 'Options' tab, there are four settings: 'Block Period' set to 4 Minute(s), 'Pass Period' set to 360 Minute(s), 'Record Expiration' set to 36 Day(s), and 'Apply To' set to 'Everyone except specified countries / IP addresses' via a dropdown menu. Below these settings are three checkboxes: 'Enable greylisting' (checked), 'Enable users to override greylisting' (unchecked), and 'Greylist if the country for the IP Address is unknown' (unchecked).

We seriously considered, and experimented with, setting "APPLY TO" to "EVERYONE," but realized that this superseded the FILTERS list and caused delays with eBay. As an eBay user I am normally sitting on top of any auction I am monitoring, but realize I might be dependant upon a notification for payment or other purposes. I could also care less about Gmail and Yahoo's poor

handling of 421 Greylisted responses – they're big players and need to get their servers setup properly, but also realize I need to include them to make concessions otherwise some of my customers might start screaming.

The Greylisting settings shown above reject an e-mail sent to your mail server by anyone who has not sent e-mail to your server for the past 36 days with a notification to the sending e-mail server that the message was GREYLISTED, in accordance with [RFC 821](#). The Greylisting rejection message will include a notification that the sending server should RETRY the message again after a specific number of seconds.

In our case the GREYLISTING BLOCK PERIOD is 4 minutes or 240 SECONDS. Some versions of SmarterMail were installed with longer greylisting initial block periods of up to 15 minutes. This is way too long a time frame as users now think of e-mail as instant messaging. Check your GREYLISTING BLOCK PERIOD and, if it is longer than 4 minutes, reduce it to between 4 and 2 minutes.

When someone who has not sent an e-mail to someone hosted on our SmarterMail server SmarterMail checks to see if they have e-mailed the intended recipient previously. If they have, and the previous delivery timeframe falls within the record expiration period, the message is allowed to be delivered, provided it does not meet other anti-spam measures.

If not, the initial Greylisting rejection response issued by SmarterMail is:

"rsp: 451 Greylisted, please try again in 240 seconds"

If the sending mail server attempts to resend the original message prior to the 240 second wait period expiring, they will receive another *"rsp: 451 Greylisted, please try again in XXX seconds"*, where XXX is the difference between the initial send time and XXX is the time remaining until the 240 second wait time has expired.

If they send the same message after 240 seconds, but do not wait longer than 360 minutes, then the mail server white lists the sending mail server's ability to send to the e-mail address the message was originally sent to for a period of 36 days.

Greylisting works for two reasons:

- A. Because most spammers attempt to send an e-mail message only one time. They have so many spam messages in their outbound queue that they want to send them out as quickly as possible, and;
- B. Because the [International Engineering Task Force \[IETF\]](#) states that all e-mail server must retry to send an e-mail message for up to a minimum of four [4] days if the message is not deliverable the first time.

The specific IETF rules concerning redelivery attempts are located at:
<http://www.ietf.org/rfc/rfc2821.txt> <http://www.ietf.org/rfc/rfc3261.txt> and
<http://www.ietf.org/rfc/rfc3265.txt>

For more information about [Greylisting](#), please see www.Greylisting.org

NOTE: GREYLISTING WORKS ON A PER USER E-MAIL ACCOUNT BASIS. Just because jimbeam@sendingdomain.com has been Greylisted for jackdaniels@receivingdomain.com does not mean that jimbeam@sendingdomain.com is now Greylisted for oldfitz@receivingdomain.com.

Each time a sending e-mail address sends to a receiving e-mail address on your server which has not received e-mail from the sending e-mail address within the timeframe of the Greylisting table established for your server, they will have to be Greylisted for the receiving e-mail address to which they are sending a message.

Some users will balk at the initial delay imposed on the receipt of messages from “new” senders. Remind them that e-mail is not instant messaging and Greylisting is only a momentary delay – amounting to a mere 4 minutes, under the settings used in our example. You can also remind them that Greylisting plays an important roll in ensuring their e-mail box is not overflowing with junk mail every morning. They will get over it.

To make certain your SmarterMail server installation is properly trying to resend messages which may be Greylisted by receiving mail servers, or otherwise non-deliverable on a temporary basis, you can check your RETRY INTERVAL settings.

SmarterMail’s RETRY INTERVAL SETTINGS are located under:

SETTINGS → GENERAL SETTINGS → SPOOL

IMPORTANT NOTE: YOUR SPOOL PATH MAY BE DIFFERENT THAN THE ONE SHOWN IN THE EXAMPLE BELOW. NEVER ATTEMPT TO CHANGE A SPOOL PATH ON A FUNCTIONING MAIL SERVER!

The screenshot displays the 'General Settings' window with the 'Spool' tab selected. The 'Spool Path' is set to 'd:\SmarterMail\Spool\'. 'SubSpools' is set to 10. 'Delivery Delay' is 3 seconds. 'Retry Intervals' are set to 5, 15, 30, 60, 90, 120, and 24 minutes. 'Bounce DNS errors after' and 'Notify senders of delay after' are both set to 2 attempts. 'Command-Line File' is empty, and 'Command-Line Timeout' is 5 seconds. The 'Enabled' checkbox for the Command-Line File is unchecked.

Setting	Value	Unit/Label
Spool Path	d:\SmarterMail\Spool\	
SubSpools	10	
Delivery Delay	3	Second(s)
Retry Intervals	5, 15, 30, 60, 90, 120, 24	Minute(s) (separated by commas)
Bounce DNS errors after	2	Attempt(s)
Notify senders of delay after	2	Attempt(s)
Command-Line File		<input type="checkbox"/> Enabled
Command-Line Timeout	5	Second(s)

[IETF retry requirements](#) call for “shall retry for up to 4 days”, but they do not specify the frequency of the retry attempts. This goes back to the days of e-mail actually being two different programs: sendmail and readmail. When the first e-mail experiments were developed by DARPA and the universities authorized to work on the projects, the networks were not constantly

connected and the e-mail servers connected every few days to transfer files, send and receive messages.

Based on the demands of today's power e-mail users, the sooner a message is delivered, the better. In reality however, technology does break down and is not always repaired immediately. Attempting to retry delivery too quickly might not allow a message to be delivered at all, so most ISPs have opted to try several times within the first couple of hours and then retry at longer intervals to allow the receiving ISP time to resolve non-receipt issues.

ChicagoNetTech has opted to run the following *retry interval schedule*: 5, 15, 30, 60, 90, 120, 240, 480, 960, 1440, 2880 minutes after the initial attempt. The addition of the first retry attempt of 5 minutes was added to help push through any Greylisted e-mail – based on my suggested greylisting time of 4 minutes.

The above listed retry interval schedule sets the first retry time for 5 minutes after the initial delivery attempt. If still not deliverable, message delivery is reattempted at 15, 30, 60, 90, and then 120 minutes. After the initial schedule, the amount of time doubles for each successive retry attempt.

In all, the server attempts to retry the delivery for a little more than four days. This satisfies the IETF retry requirement of four days.

Conversely, not all MX server operators are aware of the keep trying to send e-mail for up to four-days rule and, therefore, not all MX servers are properly setup. This can cause e-mail non-delivery issues if there is a loss of connectivity in the network between you and an originating MX SERVER.

Remember, the general rule of thumb is: *If you loose an incoming e-mail message because a server does not retry their deliveries after the first delivery attempt they are a SPAMMER. If a server does not continue to re-try for up to four [4] days, they are non-compliant with the retry delivery rules as specified by the IETF.*

No one owns the Internet. The Internet is technically a network of private networks, each of which is expected to abide by the [policies and standards established by the International Engineering Taskforce \[IETF\]](#), but that does not mean the individual networks which are interconnected to form the Internet actually abide by those policies. Each network operator sets their own parameters, and many times those parameters are incorrectly set – making their portion of the network non-compliant. **If a sending mail server is non-compliant, you do not have an obligation to whitelist them because of their ignorance.**

If the receipt of a blocked e-mail is important to you, and/or your client, you may want to try to figure out what caused the problem and notify the sending mail server administrator.

Two new items have been added to the GENERAL SETTINGS => SPOOL tab in recent SmarterMail revisions:

BOUNCE DNS ERRORS AFTER X ATTEMPTS

"Bounce DNS Errors After X Attempts" will automatically bounce an e-mail if the intended recipient's MX server cannot be found in DNS after the number of attempts listed in the count box. This will prevent an e-mail which is addressed to a non-existent MX server from taking up space and CPU cycles as re-delivery is continuously reattempted. This frequently happens when someone spells a domain incorrectly or uses a bad TLD extension. EXAMPLE: Someone attempts to send a message to CHICAGONETTECH@COMCAST.COM it will never be delivered because

"comcast.com" will not accept e-mail of any kind.

Comcast's public domain extension is .NET, so the correct address would be CHICAGONETTECH@COMCAST.NET. In the case of the wrong example, SmarterMail will abort the message after two attempts because COMCAST.COM will not be found.

Beginning with SmarterMail 11.0 the ability to **NOTIFY SENDERS OF DELAY AFTER [X number of attempts]** was also added:

Notify Senders of Delay After will automatically notify the sender that his or her e-mail has been delayed after the number of attempts listed in the count box, but will also include a message that the message will be retried based on the number of retries set in the RETRY INTERVALS BOX. Yes, SmarterMail developers taught SmarterMail how to count, and it works well!

Because so many MX servers still configure 15 minutes as the default for their greylisting delay, I see frequent notifications of delays cause by my 5 minute second attempt at delivery.

The message returned to the sender is straight forward, does not give a reason for the delay, stating the following:

"The server(s) that the message "Updates to SmarterMail Anti-Spam Settings Released: 24 March, 2013" is attempting to be sent to has temporarily delayed the delivery for the following recipient(s):

username@receivingdomain.tld

There will be up to 9 more delivery attempt(s) of this message. Do not re-send your message until there are no more delivery attempt(s) and the messages bounces back to you."

In our case, we attempt to deliver up to 11 times, based on the following schedule: 5, 15, 30, 60, 90, 120, 240, 480, 960, 1440, 2880 minutes. After the first two attempts there are 9 left so the notification states the message will be retried up to 9 additional times. There is no capability to modify the text of the delayed message response.

DON'T GET CAUGHT UP IN THE AUTOMATIC WHITELISTNG TRAP!

If a valid ISP has a problem sending e-mail to your server, take the time to find out what the problem is. Your logs will reveal many of the issues for you. You can also use outside DNS testing tools to make certain the sender's DNS is properly configured.

ISPs and e-mail server operators have an obligation to know how to properly configure both their e-mail server software, firewalls, server operating system software and their DNS records.

NOTES:

- DNS records include "A" or "HOST" records, "MX" records, "rDNS" [IN-ARPA] records, and "PTR" records. **CNAMES ARE NOT PERMITTED FOR MX SERVERS**
- PTR is always setup on the LOCAL DNS server.
- rDNS record mapping to the e-mail host must always be done by the INTERNET SERVICE or "bandwidth" PROVIDER – the company who provides the connectivity and IP ADDRESS range assignment to the ISP.

- You should also setup rDNS mappings for any e-mail domains on your local DNS server(s) by creating PTR records in the reverse DNS mappings for your IP ADDRESS range on your DNS servers.
- [RFC974](#), [RFC1034](#) 3.6.2, [RFC1912](#) 2.4, and [RFC2181](#) 10.3 prohibit the use of C-NAME records in MX or mail server host names. **All MX records must be mapped to "A" or "HOST" records directly.**
- ALL IP ADDRESSES ASSIGNED TO PUBLIC E-MAIL SERVERS MUST BE PUBLIC AND AVAILABLE ON THE INTERNET!
- Avoid using the new "musical public IP addresses" which are now being assigned by some Amazon accounts. They wreck havoc with MX DNS records – they don't work and cause confusion in locating MX servers because the transactions between MX servers are so fast on the modern Internet.

EXAMPLE: The only issue we have ever encountered because of GREYLISTING was with a vendor who does shredding for medical companies who was trying to send an e-mail to one of our customers. The vendor's e-mail server was configured to attempt to send messages only once. It was not configured to retry if a message was non-deliverable.

When the sending e-mail server encountered the *"rsp: 451 Greylisted, please try again in 240 seconds"* message, they aborted the process and never resent the message.

When the client complained they had not received the message, we checked the logs and found the problem. The customer asked me to whitelist the domain and IP address and I said no, the vendor needed to fix the configuration of their mail server. I also told our customer I would work with their vendor to resolve the mail server's configuration so it would not happen in the future.

After contacting our customer's vendor and explaining the how Greylisting works, along with the requirements that their server must be compliant, the vendor resolved the issues with their mail server's retry times and we have had no problems with delivery of their e-mail since. The customer's vendor was unaware of the issue and glad to learn of the problem so it could be corrected.

Because our customer's vendor's mail server never attempted to resend the message never got past the greylisting.

For a more complete explanation about Greylisting, see <http://www.greylisting.org/>

2. Once you have configured the GREYLISTING SETTINGS, it is time to configure your ANTI SPAM according to the following settings.

These settings work because they IMMEDIATELY DELETE any incoming message which is found to be from a server that DOES NOT HAVE an IN-ARPA or REVERSE DNS ENTRY.

Messages received from any of the RBL or URIBL are IMMEDIATELY DELETED if they are on one of those lists. If you UNCHECK the column labeled ENABLE FOR SMTP BLOCKING, the CENTER column in the main antispam section, and run according to weights, these settings WILL NOT WORK and you will be back to fighting with spammers.

Protecting your e-mail server from spam depends on total server lockdown.

A. SETUP AN ACCOUNT WITH BARRACUDA CENTRAL and ADD THE BARRACUDA REPUTATION BLOCK LIST to your ANTISPAM settings.

Before you can begin to use the Barracuda Reputation Block List, you will need to setup an account at Barracuda Central. That account must be linked to the DNS SERVERS which will be to query Barracuda by your SmarterMail MX which receives the actual e-mail.

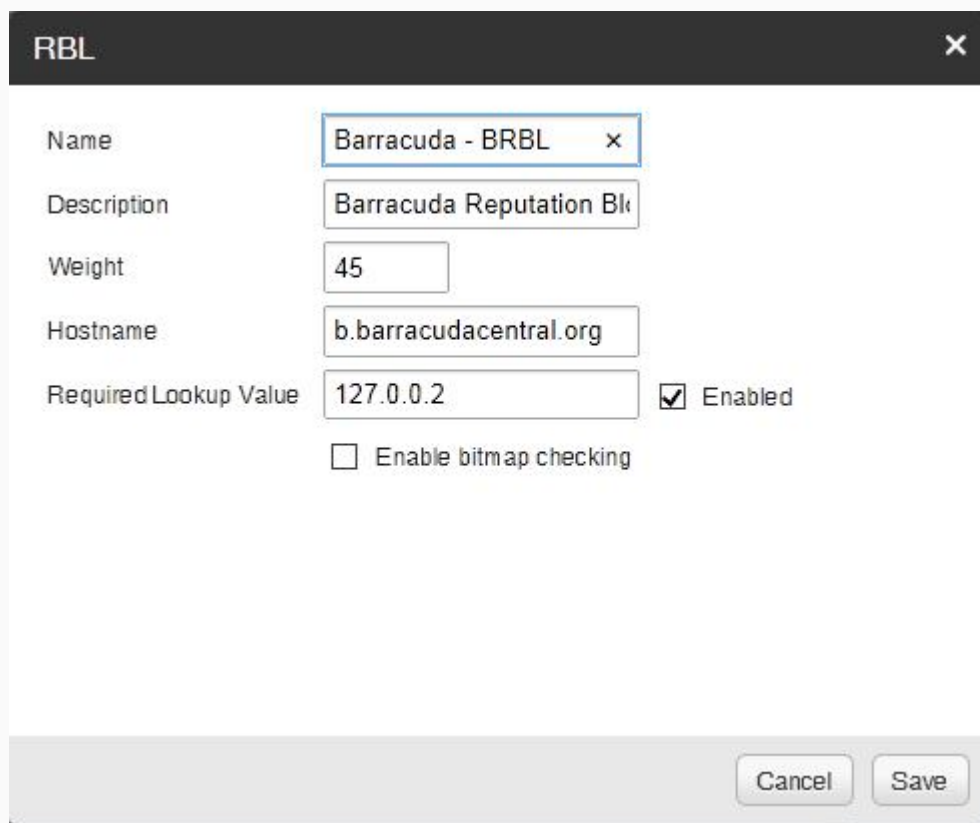
DO NOT USE PUBLIC DNS SERVERS – there is a limit on the number of queries which will now be accepted by any RBL or URIBL. That limit is between 200,000 and 300,000 queries per day, per DNS SERVER.

To setup your account go to <http://www.barracudacentral.org/>. Then go to the TOP OF THE PAGE and click on **REQUEST ACCESS**. This links to <http://www.barracudacentral.org/account/register>

Once you setup your Barracuda account you will need to configure your SmarterMail server to use it. To add your BRBL listing configuration goto:

SECURITY → ANTISPAM ADMINISTRATION → ADD RBL.

Configure your new BARRACUDA RBL listing as follows. Note the high weight score. This is only checked if you are NOT checking the ENABLE FOR INCOMING SMTP BLOCKING box in your antispam settings. If ENABLE FOR INCOMING SMTP BLOCKING is checked, any messages which turns up as a POSITIVE query on this list will be blocked and not accepted:



The screenshot shows a window titled "RBL" with a close button (X) in the top right corner. The window contains the following fields and options:

- Name:** A text box containing "Barracuda - BRBL" with a small 'x' icon to its right.
- Description:** A text box containing "Barracuda Reputation Blk".
- Weight:** A text box containing the number "45".
- Hostname:** A text box containing "b.barracudacentral.org".
- Required Lookup Value:** A text box containing "127.0.0.2".
- Enabled:** A checkbox that is checked, followed by the text "Enabled".
- Enable bitmap checking:** An unchecked checkbox followed by the text "Enable bitmap checking".

At the bottom right of the window, there are two buttons: "Cancel" and "Save".

Once you have entered all of your data into the configuration box, then click SAVE and you have added your new BRBL too to your list of Antispam measures.

B. NOW TURN ON the ANTI-SPAM SETTINGS per the SCREEN CAPTURES SHOWN BELOW:

Your SPAM CHECKS TAB is located at: **SECURITY → ANTISPAM ADMINISTRATION → SPAM CHECKS**

Notes about the settings for each of the line items below:

- ❖ Depending on the version of SmarterMail you have, you may not have some of the items in the tabs shown below;
- ❖ To ADD an RBL, click on AddRBL;
- ❖ To ADD a URIBL, click on AddURIBL;
- ❖ To delete an item, right click on the line and select DELETE from the pop-up menu:

Antispam Administration				
Save	Add RBL	Add URIBL	Edit	Delete
Wizard				
Spam Checks ⁴¹	Filtering	SMTP Blocking	Options	Bypass Gateways
<input type="checkbox"/> Spam Check	Weight	Enable for Filtering	Enable for Incoming SMTP blocking	Enable for Outgoing SMT
<input type="checkbox"/> Declude	0-30	<input type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/> Spam Assassin-Based Pattern Matching	0-30	<input type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/> Remote SpamAssassin	0-30	<input type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/> Commtouch Premium Antispam (Not Licensed)	0-30	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input checked="" type="checkbox"/>
<input type="checkbox"/> Custom Rules	0-0	<input type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/> Bayesian Filtering	10	<input type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/> DomainKeys	0-5	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A
<input type="checkbox"/> DKIM	0-5	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A
<input type="checkbox"/> SPF	0-30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Reverse DNS	35	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> RBL: Barracuda - BRBL	45	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> RBL: CBL - Abuse Seat - DO NOT CHECK OUTGOING	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> RBL: HostKarma - Blacklist	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> RBL: HostKarma - Brownlist	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

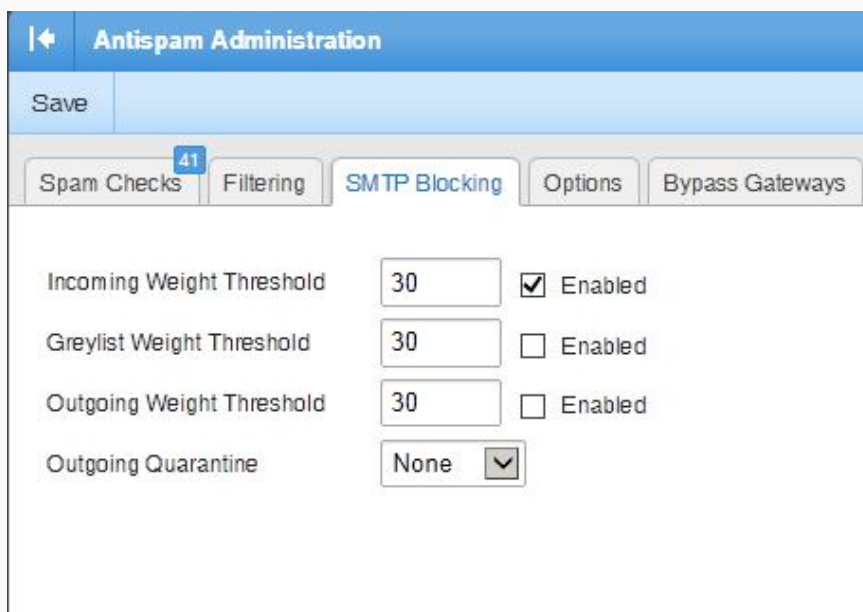
<input type="checkbox"/>	RBL: Hostkarma - NOBLACKLIST	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: HostKarma - Whitelist	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: HostKarma - Yellowlist	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: SORBS - Abuse	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: SORBS - Dynamic IP	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: SORBS - Proxy	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: SORBS - SMTP	20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: SORBS - SOCKS	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: Spamhaus - CBL	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: Spamhaus - CSS	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: Spamhaus - PBL	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: Spamhaus - PBL2	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: Spamhaus - SBL	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: SURBL - Abuse Buster	10	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: SURBL - JWSpamSpy	10	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: SURBL - Malware	10	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: SURBL - Phishing	10	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: SURBL - SpamAssassin	10	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: SURBL - SpamCop	10	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	RBL: UCEProtect Level 1	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: UCEProtect Level 2	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RBL: UCEProtect Level 3	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: URIBL - Black	5	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: URIBL - Grey	5	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: URIBL - Multi	5	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	URIBL: URIBL - Red	5	<input checked="" type="checkbox"/>	<input type="checkbox"/> N/A	<input type="checkbox"/>
<input type="checkbox"/>	RBL: VIRUS RBL - MSRBL	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

NOTES: The settings listed above contain major changes to previous versions of this document. Therefore, the individual settings for each of the line-items shown above are included below.

When you update to these settings you will need to delete several "wild card" responses which were previously included. Failure to delete these can result false positive responses.

ADDITIONAL NOTES:

- ❖ By checking the *ENABLE FOR SMTP BLOCKING* [center] column above, all weights are overridden and the message is deleted immediately
- ❖ This is also moderated by the settings for SMTP BLOCKING shown below:
- ❖ Enabling the GREYLIST Threshold box negates greylisting and makes it ineffective for spam control.



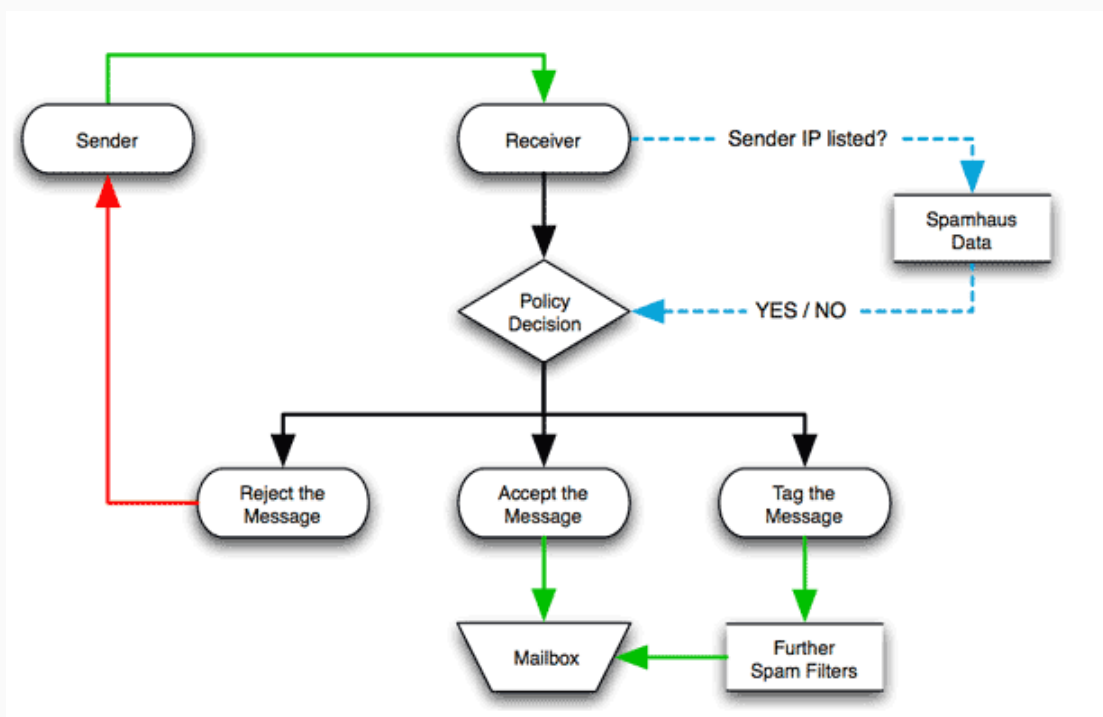
The screenshot shows the 'Antispam Administration' window with a 'Save' button at the top left. Below the title bar are five tabs: 'Spam Checks', 'Filtering', 'SMTP Blocking' (which is selected and highlighted in blue), 'Options', and 'Bypass Gateways'. A small blue square with the number '41' is positioned above the 'Filtering' tab. The 'SMTP Blocking' tab contains four settings:

Incoming Weight Threshold	30	<input checked="" type="checkbox"/> Enabled
Greylist Weight Threshold	30	<input type="checkbox"/> Enabled
Outgoing Weight Threshold	30	<input type="checkbox"/> Enabled
Outgoing Quarantine	None	<input type="button" value="v"/>

- ❖ Several of the settings listed in prior versions of this list have been significantly modified or deleted. In some cases, this is because of issues with too many queries returning a status which can mark something spam when it was not. This was particularly true of URIBL – MULTI which has now been broken out to URIBL – Black, Grey, Red and Multi – each of which returns a unique response and only that response.
- ❖ **blackholes.five-ten-sg.com** is no longer providing spam database lookups and has been removed.
- ❖ **MULTI SURBL.ORG** has been removed and replaced with individual responses to prevent negative responses being triggered on legitimate e-mail. These are now: *SURBL - Abuse Buster*; *SURBL - JWSpamSpy*; *SURBL - Malware*; *SURBL - Phishing*; *SURBL - SpamAssassin*; and *SURBL - SpamCop*.
- ❖ CBL Abuse Seat and VIRUS RBL are both new. ***In the case of CBL Abuse Seat, if you start checking outgoing messages with the RBL they will blacklist your server so don't even consider using CBL Abuse Seat to check outgoing messages.***
- ❖ There is no need to check OUTBOUND messages for spam unless you have known spammers on your server, in which case you have a much bigger problem. Most outbound spam is caused by someone hacking your server and sending via one of your hosted accounts. Secure passwords can go a long way toward preventing having your server hacked and hijacked by spammers and are discussed elsewhere in this document.

- ❖ Note that we ENABLE REVERSE DNS FILTERING. This checks to see if the sending e-mail server has a public rDNS [also known as IN-ARPA or REVERSE DNS] entry which maps to the sending e-mail server's HOST NAME and IP ADDRESS.
- ❖ While not REQUIRED by the IETF, [RFC1912](#) section 2.1 says you SHOULD HAVE a reverse DNS for all your mail servers. It is strongly urged that you have them, as many mailservers will no longer accept mail from mailservers with no reverse DNS entry.
- ❖ With ENABLE REVERSE DNS checked in the ENABLE FOR INCOMING SMTP BLOCKING column, anyone who does not have BOTH an IN-ARPA or REVERSE DNS AND a PTR entry associated with the IP ADDRESS of their primary mail server will be unceremoniously disconnected and their message will not be accepted by your mail server. This is an extremely important antispam setting as most spammers will not make the effort to, or will be blocked from, setting up an IN-ARPA address.
- ❖ Anything checked in the "ENABLE FOR INCOMING SMTP BLOCKING" column will UNCEREMONIOUSLY DELETE an incoming message which meets the criteria. Mail Servers are notified you are using SMTP Blocking with the following message: "554 Sending address not accepted due to spam filter"
- ❖ These settings do not use content filtering. I strongly suggest you do not use content filtering in addition to these settings because the maintenance of any content filtering is a maintenance intensive, self-loathing task which is never done.

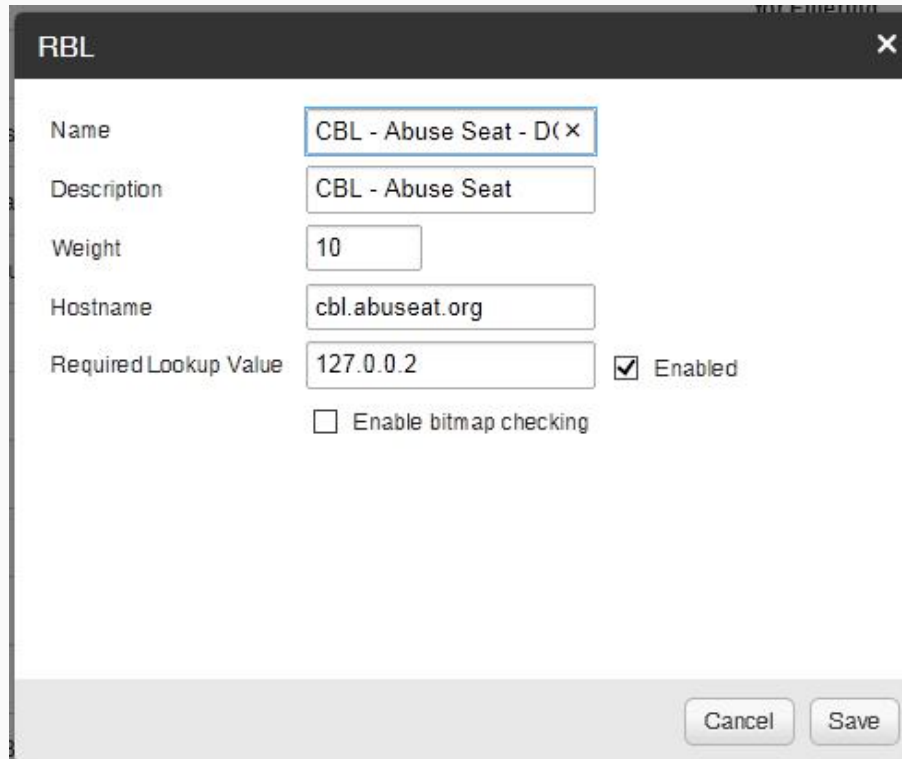
RBL and URIBL queries work based on the polling of spam databases and decisions made by the RECEIVING MX server. Here is a flowchart showing the basic process of those tests, queries and decisions:



While the above image is courtesy of [Spamhaus](#), all RBL / URIBL queries work basically the same way. **NOTE: in order to prevent BACKSCATTER, ChicagoNetTech DOES NOT notify the sender when a message is rejected as spam.**

The individual settings for each of the individual tests listed chart shown on pages 10 and 11 are shown on the following pages, along with specifics relating to the individual RBL / BRBL databases:

RBL CBL ABUSE SEAT:



Name	CBL - Abuse Seat - D(x)
Description	CBL - Abuse Seat
Weight	10
Hostname	cbl.abuseat.org
Required Lookup Value	127.0.0.2
	<input checked="" type="checkbox"/> Enabled
	<input type="checkbox"/> Enable bitmap checking

Cancel Save

More information on CBL ABUSE SEAT can be found at: <http://cbl.abuseat.org/> The only response for a positive e-mail from cbl.abuseat.org is 127.0.0.2

HOST KARMA JUNKMAIL FILTERS:

The next five entries are for HOSTKARMA Junkmail filters. There are a total of five different results which can be returned by the "hostkarma.junkmailfilter.com" RBL

They are:

- 127.0.0.1 - whitelist - trusted nonspam
- 127.0.0.2 - blacklist - block spam
- 127.0.0.3 - yellowlist - mix of spam and nonspam
- 127.0.0.4 - brownlist - all spam - but not yet enough to blacklist
- 127.0.0.5 - NOBL - This IP is not a spam only source and no blacklists need to be tested

The RBL HOST KARMA NOBLACKLIST entry is included below is included only as an example, and not necessary to include for proper antispam performance.

They are included to further substantiate the example that the Required Lookup Value does not always return the value of 127.0.0.2 and that it is important to get the correct "Required Lookup Value" into the Required Lookup Value box and check the Enabled box.

If included and checked, it will be listed in the DELIVERY LOGS when DELIVERY LOGS are set to DETAILED.

You can read more information about HOSTKARMA junkmail filtering here:

http://wiki.junkemailfilter.com/index.php/Spam_DNS_Lists

RBL: HOST KARMA BLACKLIST:

RBL

Name: HostKarma - Blacklist

Description: HostKarma - Blacklist

Weight: 10

Hostname: hostkarma.junkemailfilter

Required Lookup Value: 127.0.0.2 ☒ Enabled

☐ Enable bitmap checking

Cancel Save

RBL: HOST KARMA BROWNLIST:

RBL [X]

Name	HostKarma - Brownlist X
Description	HostKarma - Brownlist
Weight	5
Hostname	hostkarma.junkemailfilter
Required Lookup Value	127.0.0.4 <input checked="" type="checkbox"/> Enabled
	<input type="checkbox"/> Enable bitmap checking

Cancel Save

RBL: HOST KARMA NOBLACKLIST:

RBL [X]

Name	Hostkarma - NOBLACKL
Description	Hostkarma - NOBLACKL
Weight	0
Hostname	hostkarma.junkemailfilter
Required Lookup Value	127.0.0.5 <input checked="" type="checkbox"/> Enabled
	<input type="checkbox"/> Enable bitmap checking

Cancel Save

RBL: HOST KARMA WHITELIST:

RBL

Name

HostKarma - Whitelist

×

Description

HostKarma - Whitelist

Weight

0

Hostname

hostkarma.junkemailfilter

Required Lookup Value

127.0.0.1

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: HOST KARMA YELLOWLIST:

RBL

Name

HostKarma - Yellowlist

Description

HostKarma - Yellowlist

Weight

10

Hostname

hostkarma.junkemailfilter

Required Lookup Value

127.0.0.3

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

SORBS DNS BLACKLIST: <http://www.us.sorbs.net/>

The SORBS DNS BLACKLIST also has the capability of returning more than a single response of 127.0.0.2. The currently available DNS blacklists from SORBS are as follows:

- http.dnsbl.sorbs.net 127.0.0.2
- socks.dnsbl.sorbs.net 127.0.0.3
- misc.dnsbl.sorbs.net 127.0.0.4
- smtp.dnsbl.sorbs.net 127.0.0.5
- new.spam.dnsbl.sorbs.net 127.0.0.6
- recent.spam.dnsbl.sorbs.net 127.0.0.6
- old.spam.dnsbl.sorbs.net 127.0.0.6
- spam.dnsbl.sorbs.net 127.0.0.6
- escalations.dnsbl.sorbs.net 127.0.0.6
- web.dnsbl.sorbs.net 127.0.0.7
- block.dnsbl.sorbs.net 127.0.0.8
- zombie.dnsbl.sorbs.net 127.0.0.9
- dul.dnsbl.sorbs.net 127.0.0.10 [<http://www.us.sorbs.net/delisting/dul.shtml> for explanation of origin and name]
- badconf.rhsbl.sorbs.net 127.0.0.11
- nomain.rhsbl.sorbs.net 127.0.0.12

We are running FIVE different SORBS queries. **ABUSE:** aka "WEB," with a return code of 127.0.0.7. **DYNAMIC IP:** aka *DUL*, with a return code of 127.0.0.10. **PROXY:** with a return of 127.0.0.4. **SMTP:** with a return of 127.0.0.5. **SOCKS:** with a return code of 127.0.0.3.

See <http://www.us.sorbs.net/using.shtml> for more information on SORBS RBL use and lists.

RBL: SORBS ABUSE:

The screenshot shows a configuration window titled "RBL" with a close button (X) in the top right corner. The window contains the following fields and options:

- Name:** A dropdown menu showing "SORBS - Abuse" with a small 'x' icon to its right.
- Description:** A text box containing "SORBS - Abuse".
- Weight:** A text box containing the number "5".
- Hostname:** A text box containing "dnsbl.sorbs.net".
- Required Lookup Value:** A text box containing "127.0.0.7".
- Enabled:** A checkbox that is checked, with the label "Enabled" next to it.
- Enable bitmap checking:** An unchecked checkbox with the label "Enable bitmap checking" next to it.

At the bottom right of the window are two buttons: "Cancel" and "Save".

RBL: SORBS DYNAMIC IP:

RBL

Name

SORBS - Dynamic IP

Description

SORBS - Dynamic IP

Weight

3

Hostname

dnsbl.sorbs.net

Required Lookup Value

127.0.0.10

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: PROXY:

RBL

Name

SORBS - Proxy

Description

SORBS - Proxy

Weight

10

Hostname

dnsbl.sorbs.net

Required Lookup Value

127.0.0.4

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: SORBS SMTP

RBL

Name

SORBS - SMTP

Description

Sorbs SMTP Database

Weight

20

Hostname

smtp.dnsbl.sorbs.net

Required Lookup Value

127.0.0.5

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: SORBS SOCKS

RBL

Name

SORBS - SOCKS

Description

SORBS - SOCKS

Weight

10

Hostname

dnsbl.sorbs.net

Required Lookup Value

127.0.0.3

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

ZEN SPAMHAUS RBL: <http://www.spamhaus.org/zen/>

ZEN is a subset of SPAMHAUSE, and has several different code returns which are possible.

Return Codes	Data Source	Contains
127.0.0.2		Direct UBE sources, spam operations & spam services
127.0.0.3		Direct snowshoe spam sources detected via automation
127.0.0.4-7		CBL (3rd party exploits such as proxies, trojans, etc.)
127.0.0.10-11		End-user Non-MTA IP addresses set by ISP outbound mail policy

- PBL ADVISORY, consisting of 127.0.0.10 and 127.0.0.11, is further broken out as: 127.0.0.10 *ISP Maintained*, and 127.0.0.11 as *Spamhaus maintained*.
- *In the past, 127.0.0.5 was assigned to NJABL listings and 127.0.0.6 to OPM listings; these codes are no longer in use at this time. 127.0.0.5, 127.0.0.6 and 127.0.0.7 remain allocated to XBL for possible future use.*

RBL: SPAMHAUS – CBL

RBL

Name

Spamhaus - CBL

Description

Spamhaus - CBL

Weight

10

Hostname

zen.spamhaus.org

Required Lookup Value

127.0.0.4

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: SPAMHAUS – CSS

RBL

Name

Spamhaus - CSS

Description

Spamhaus - CSS

Weight

10

Hostname

zen.spamhaus.org

Required Lookup Value

127.0.0.3

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: SPAMHAUS – PBL

RBL

Name

Spamhaus - PBL

Description

Spamhaus - PBL

Weight

10

Hostname

zen.spamhaus.org

Required Lookup Value

127.0.0.10

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: SPAMHAUS – PBL2

RBL

Name

Spamhaus - PBL2

Description

Spamhaus - PBL2

Weight

10

Hostname

zen.spamhaus.org

Required Lookup Value

127.0.0.11

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: SPAMHAUS – SBL

RBL

Name

Spamhaus - SBL

Description

Spamhaus - SBL

Weight

10

Hostname

zen.spamhaus.org

Required Lookup Value

127.0.0.2

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

The next several entries are not composed of RBL [REAL TIME BLACK LISTS] or know MX servers which spam, but **SURBLs** which are lists of *web sites* that have appeared in unsolicited messages. Unlike most lists, SURBLs are **not** lists of message senders. An SURBL is added as a URIBL entry.

SURBL: <http://www.surbl.org/>

The SURBL lists support the following queries and return lookup values:
[<http://www.surbl.org/lists>]

- [SC - SpamCop web sites](#) returns: 127.0.0.4
- [WS - sa-blacklist web sites](#) returns: 127.0.0.2
- [OB - Outblaze URI blacklist](#) formerly: 127.0.0.16
(*deprected 22 October 2012 and- reassigned to malware 2013*)
- [AB - AbuseButler web sites](#) returns: 127.0.0.32
- [PH - Phishing sites](#) returns: 127.0.0.8
- [MW - Malware sites](#) returns: 127.0.0.16
(**active as of 1 May 2013 and included as built in this document**)
- [JP - jwSpamSpy + Prolocation sites](#) returns: 127.0.0.64
- [multi.surbl.org - Combined SURBL list](#) – broken out individually above

URIBL: SURBL – ABUSE BUSTER

The screenshot shows a configuration window titled "URIBL" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Name:** SURBL - Abuse Buste x
- Description:** SURBL - Abuse Buster
- Weight:** 10
- Hostname:** multi.surbl.org
- Required Lookup Value:** 127.0.0.32
- Enabled:** ☒ Enabled
- Enable bitmap checking:** ☐ Enable bitmap checking

At the bottom right of the window are two buttons: "Cancel" and "Save".

URIBL: SURBL – JWSpamSpy

URIBL

Name

SURBL - JWSpamSpy x

Description

SURBL - JWSpamSpy

Weight

10

Hostname

multi.surbl.org

Required Lookup Value

127.0.0.64

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: SURBL – MALWARE

URIBL

Name

SURBL - Malware x

Description

SURBL - Malware

Weight

10

Hostname

multi.surbl.org

Required Lookup Value

127.0.0.16

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: SURBL – PHISHING

URIBL

Name

SURBL - Phishing

Description

SURBL - Phishing

Weight

10

Hostname

multi.surbl.org

Required Lookup Value

127.0.0.8

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: SURBL – SPAM ASSASSIN

URIBL

Name

SURBL - SpamAssassin

Description

SURBL - SpamAssassin

Weight

10

Hostname

multi.surbl.org

Required Lookup Value

127.0.0.4

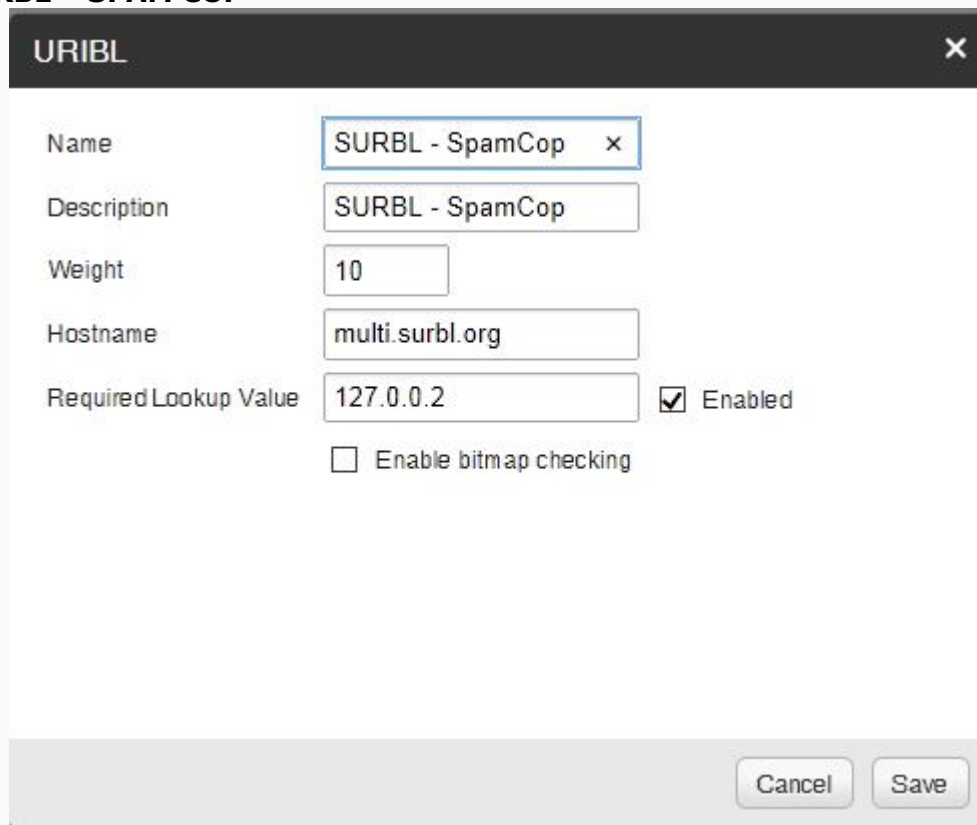
☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: SURBL – SPAM COP



URIBL

Name: SURBL - SpamCop

Description: SURBL - SpamCop

Weight: 10

Hostname: multi.surbl.org

Required Lookup Value: 127.0.0.2 ☒ Enabled

☐ Enable bitmap checking

Cancel Save

UCE PROTECT: <http://www.uceprotect.net/en/index.php>

UCE Protect is run out of the Netherlands and their website is available in both English and Dutch.

UCE Protect uses three separate query addresses for the three different levels of lookups:

- dnsbl-1.uceprotect.net
 - <http://www.dnsbl.info/dnsbl-details.php?dnsbl=dnsbl-1.uceprotect.net>
- dnsbl-2.uceprotect.net
 - <http://www.dnsbl.info/dnsbl-details.php?dnsbl=dnsbl-2.uceprotect.net>
- dnsbl-3.uceprotect.net
 - <http://www.dnsbl.info/dnsbl-details.php?dnsbl=dnsbl-3.uceprotect.net>

All three return a score of 127.0.0.2 when a message is returned as positive by the respective database.

The configurations for each of the respective queries are shown on the next two pages.

RBL: UCE PROTECT LEVEL 1

RBL

Name

UCEProtect Level 1

Description

UCEProtect Level 1

Weight

5

Hostname

dnsbl-1.uceprotect.net

Required Lookup Value

127.0.0.2

☐ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: UCE PROTECT LEVEL 2

RBL

Name

UCEProtect Level 2

Description

UCEProtect Level 2

Weight

5

Hostname

dnsbl-2.uceprotect.net

Required Lookup Value

127.0.0.2

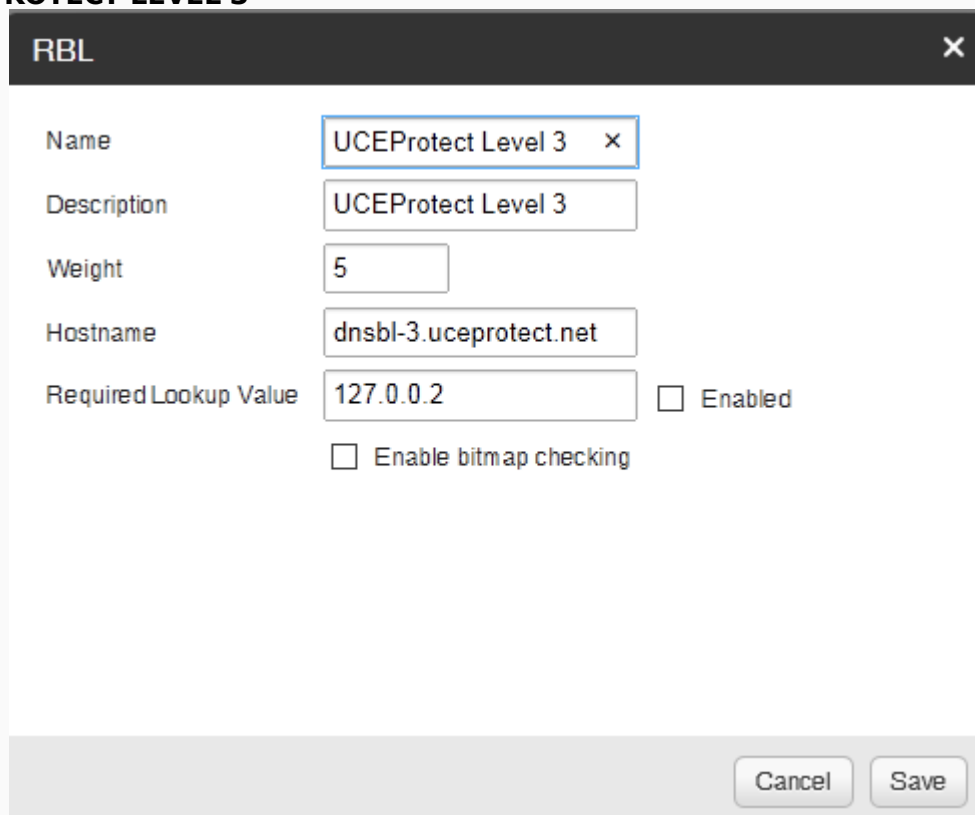
☐ Enabled

☐ Enable bitmap checking

Cancel

Save

RBL: UCE PROTECT LEVEL 3



The screenshot shows a window titled "RBL" with a close button (X) in the top right corner. Inside the window, there are several input fields and checkboxes:

- Name:** A text box containing "UCEProtect Level 3" with a small "X" icon to its right.
- Description:** A text box containing "UCEProtect Level 3".
- Weight:** A text box containing the number "5".
- Hostname:** A text box containing "dnsbl-3.uceprotect.net".
- Required Lookup Value:** A text box containing "127.0.0.2".
- Enabled:** A checkbox that is currently unchecked, followed by the text "Enabled".
- Enable bitmap checking:** A checkbox that is currently unchecked, followed by the text "Enable bitmap checking".

At the bottom right of the window, there are two buttons: "Cancel" and "Save".

URIBL: <http://www.uribl.com/> - goal of zero [False Positives](#) and rebuilds the zone frequently as new data is added.

The public URIBL Lists which can be queried at URIBL are:

- **black.uribl.com** - This list contains domain names belonging to and used by spammers, including but not restricted to those that appear in URIs found in Unsolicited Bulk and/or Commercial Email (UBE/UCE).
- **grey.uribl.com** - This list contains domains found in UBE/UCE who possibly honor opt-out requests. It may include ESPs which allow customers to import their recipient lists and may have no control over the subscription methods. Remember, both the US and EU spam regulations require verified or double opt-in to add an e-mail address to a list.
- **red.uribl.com** - This list contains domains that actively show up in mail flow, are not listed on URIBL black, and are either: being monitored, very young (domain age via whois), or use whois privacy features to protect their identity. This list is automated in nature and primarily based on automated whois queries.
- **white.uribl.com** - This list contains legit domain names which URIBL does not want to show up on any other URIBL lists. This list is mostly static, with only a handful of changes per day. URIBL white is not currently bitmasked into multi.uribl.com. If you want to query it, you must send a separate query. This zone rebuilds as needed. This zone is not included in the ChicagoNetTech antispam query settings.
- **multi.uribl.com** - checks to see if a domain is on any of our lists. This zone rebuilds if any of the above zones are rebuilt, with the exception of white. The multi.uribl.com list is

the basis for all of the queries which have been built in SmarterMail as part of this document.

The query codes returned via multi.uribl.com for each of the query types are as follows:

BLACK: 127.0.0.2
RED: 127.0.0.4
GREY: 127.0.0.8
WHITE: NOT QUERIED – REQUIRES SUBSCRIPTION
MULTI: 127.0.0.16
BLOCKED: 127.0.0.255 – YOUR DNS IS BLOCKED FROM MAKING QUERIES

Additional, subscription based, lists are available for a fee via a private subscription service.

For more information about subscriptions, query types and codes returned by query type, see: <http://www.uribl.com/about.shtml>

URIBL: URIBL BLACK

URIBL

Name

URIBL - Black

Description

URIBL

Weight

5

Hostname

multi.uribl.com

Required Lookup Value

127.0.0.2

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: URIBL GREY

URIBL

Name

URIBL - Grey

Description

URIBL - Grey

Weight

5

Hostname

multi.uribl.com

Required Lookup Value

127.0.0.8

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: URIBL MULTI

URIBL

Name

URIBL - Multi

Description

URIBL - Multi

Weight

5

Hostname

multi.uribl.com

Required Lookup Value

127.0.0.14

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

URIBL: URIBL RED

URIBL

Name

URIBL - Red

Description

URIBL - Red

Weight

5

Hostname

multi.uribl.com

Required Lookup Value

127.0.0.4

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

MSRBL Virus Database: <http://multirbl.valli.org/detail/virus.rbl.msrbl.net.html>

Returns only one Required Lookup Value: 127.0.0.2 – **RBL: VIRUS RBL**

RBL

Name

VIRUS RBL - MSRBL

Description

VIRUS RBL - MSRBL

Weight

10

Hostname

virus.rbl.msrbl.net

Required Lookup Value

127.0.0.2

☒ Enabled

☐ Enable bitmap checking

Cancel

Save

BACKSCATTER has become a huge issue with MX servers which deny receipt of messages because they are spam and then attempt to notify the sender that receipt of the message was denied. This frequently causes MX servers to be listed in BACKSCATTER databases and their reputation is impeded.

To DISABLE BACKSCATTER, goto **SECURITY → ANTISPAM ADMINISTRATION → OPTIONS** and make certain you have set CONTENT FILTER BOUNCING to DISABLED.

It should be configured as follows – Press SAVE when completed:

Save

43 Spam Checks Filtering SMTP Blocking Options Bypass Gateways

When configuring Enable spool proc folder, a 3rd party application must move messages into the spool after processing.

Auto-Responders Require message pass SPF if SPF record exists

Content Filter Bouncing Disabled

Max message size to content scan 1000 KB

☐ Allow domains to override filter weights and actions

☐ Enable bounces for outgoing SMTP blocking

☐ Enable spool proc folder

☐ Disable spam filtering on SMTP whitelisted IP addresses

☐ Enable catch-all accounts to send auto-responders and bounce messages.

☒ Enable SRS when forwarding messages

☒ Enable DMARC policy compliance check

Note that the AUTO-RESPONDER is set to REQUIRE MESSAGE PASS SPF if SPF record exists. This means that if an SPF record is found, and matches the incoming message's domain, then the auto-responder will function normally. If the SPF record is NOT found, the auto-responder will function normally. If the SPF record does NOT match, then the message will NOT be forwarded if a forwarder is enabled.

In the above example CONTENT FILTER BOUNCING is completely DISABLED. This is prevent BACKSCATTER. For more information on why backscatter is bad, see: [http://en.wikipedia.org/wiki/Backscatter_\(email\)](http://en.wikipedia.org/wiki/Backscatter_(email))

- ✓ DomainKeys have been updated to REMOVE NEGATIVE PASS WEIGHTS. If the DomainKey fails, and is not used to trigger an immediate non-acceptance, then it will add a spam weight of 5 to the total spam weight. If there is no DomainKey, there will be no penalty.
- ✓ The maximum size of a message which will be checked is 4096 MB [effectively unlimited]. Setting the max message size to 0 will also check unlimited message sizes.
- ✓ The Max Key Size allowed pertains to the size of the key which can be generated for your OUTBOUND message signing:

DomainKeys



Pass Weight

Fail Weight

None Weight

Max message size to sign MB

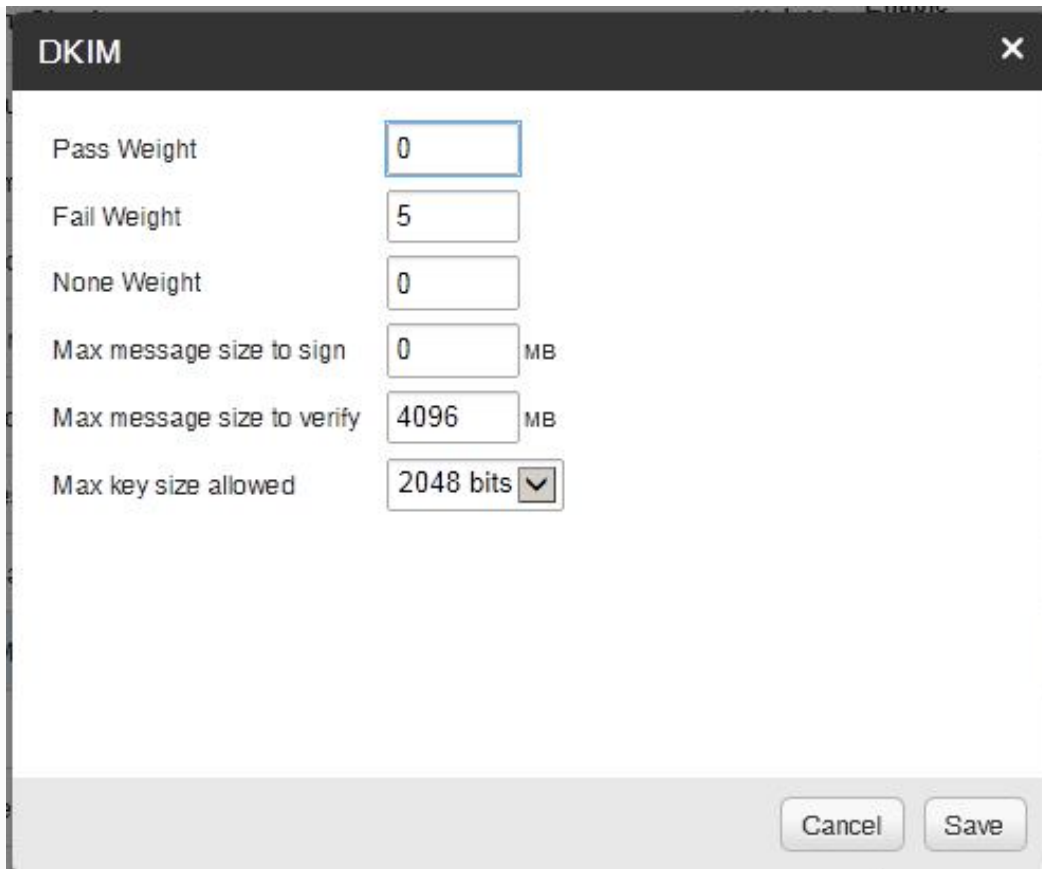
Max message size to verify MB

Max key size allowed

Cancel

Save

- ✓ The DKIM settings shown below have also been updated to remove negative weights on PASS and give no negative weight for not having a DKIM record:
- ✓ The maximum size of a message which will be checked is 4096 MB. Setting the max message size to 0 will check unlimited messages sizes but use more memory.
- ✓ The Max Key Size allowed pertains to the size of the key which can be generated for your OUTBOUND message signing:

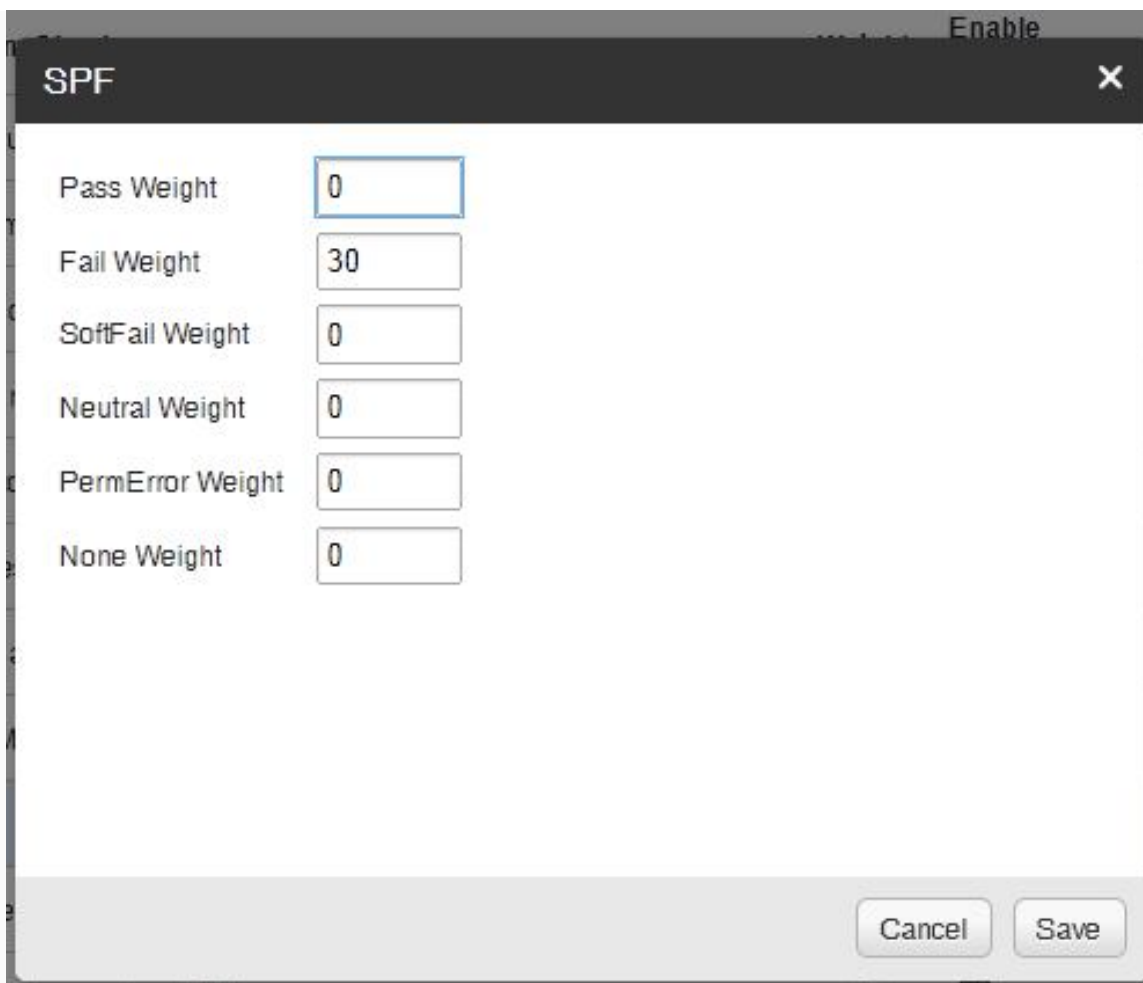


The image shows a screenshot of a 'DKIM' settings dialog box. The dialog has a title bar with the text 'DKIM' and a close button (X). Inside the dialog, there are six settings, each with a text input field and a label to its left:

- Pass Weight: 0
- Fail Weight: 5
- None Weight: 0
- Max message size to sign: 0 MB
- Max message size to verify: 4096 MB
- Max key size allowed: 2048 bits (with a dropdown arrow)

At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Save'.

- ✓ We have initiated some different settings for SPF records. The only score we apply is FAIL, at 30. Everything else is set to ZERO. Our SPF configuration is now set as follows:



The image shows a window titled "SPF" with a close button (X) in the top right corner. Inside the window, there are six rows of settings, each with a label and a text input field:

Setting	Value
Pass Weight	0
Fail Weight	30
SoftFail Weight	0
Neutral Weight	0
PermError Weight	0
None Weight	0

At the bottom right of the window, there are two buttons: "Cancel" and "Save".

C. FILTERING:

The FILTERING settings are available under:

SECURITY → ANTISPAM ADMINISTRATION → FILTERING

We initially set our LOW PROBABILITY to PREFIX SUBJECT WITH TEXT [**** Junk E-Mail ****] to make certain we were not deleting legitimate e-mail.

Once you are comfortable with the new antispam settings, and are convinced you are not turning away legit e-mail, you can change LOW to DELETE if you like. If you are more comfortable with initially setting the MEDIUM or HIGH to PREFIX or MOVE, please feel free to do so.

Again, ANYTIME you make any changes to any of these screens, please remember to SAVE your changes or they will be lost!

Antispam Administration

Save

41

Spam Checks

Filtering

SMTP Blocking

Options

Bypass Gateways

Low Probability of Spam

Weight Threshold

30

Default Action

Prefix subject with text

Text to Add

**** Junk E-Mail ****

Medium Probability of Spam

Weight Threshold

40

Default Action

Move to Junk E-Mail Folder

High Probability of Spam

Weight Threshold

50

Default Action

Move to Junk E-Mail Folder

In order to alleviate any confusion about what we show in the SMTP BLOCKING screen, I have include a capture from our SmarterMail setup below. Your settings may be different.

Antispam Administration

Save

41

Spam Checks

Filtering

SMTP Blocking

Options

Bypass Gateways

Incoming Weight Threshold

30

☒ Enabled

Greylist Weight Threshold

30

☐ Enabled

Outgoing Weight Threshold

30

☐ Enabled

Outgoing Quarantine

None

D. OPTIONS:

The following options are available under:

SETTINGS → DEFAULTS → DOMAIN DEFAULTS → TECHNICAL

The screenshot shows the 'Domain Defaults' configuration window with the 'Technical' tab selected. The 'Save' button is at the top left. Below the tab bar, the following settings are visible:

- Folder Path: d:\SmarterMail\
- Auto-Responder Exclusions: Do not auto-respond to Spam Level Low and above (dropdown)
- Forwarding Exclusions: Do not forward Spam Level Medium and above (dropdown)
- TLS: Enabled (dropdown)
- SRS: Enabled (dropdown)
- Calendar Auto Clean: 12 (dropdown) Month(s)
- ☒ Require SMTP Authentication
- ☒ Restrict auto-responders to once per day per sender
- ☐ Disable greylisting
- ☐ Allow users to opt out of LDAP listings
- ☐ Exclude IP from received line
- ☐ Allow users to override personalization settings

NOTE: The FOLDER PATH is a NON-STANDARD folder path. Yours may be different.

We require SMTP AUTHENTICATION for ALL transactions. No authentication, no message accepted for delivery.

We also force greylisting on all incoming messages. I will loose a non-compliant customer before I will allow a domain to be inundated with junk mail from spammers which can be eliminated by greylisting.

Example: We maintain a SmarterMail server for a major national real estate company in their data center and block more than 1.2 million spam messages via greylisting every month.

E-mail is not instant messaging – delivery is guaranteed in 4 days or less – per the original IETF / DARPA protocol standard which has never been updated.

You will also want to make certain that your PRIMARY IP ADDRESS is properly mapped to your SmarterMail host's server name.

Because we run TLS on the mail server [*available in the Enterprise edition only*], and run SSL, we have ALL of our clients setup to use the IP ADDRESS which is bound to our SSL/TLS.

In the event of a failure of that IP ADDRESS, SmarterMail will automatically pick up with the primary IP ADDRESS of the NIC card, which is also bound to all domains, but not as a primary.

Our two MX records point to:

- ❖ *SECUREMAIL.CHICAGONETTECH.COM, with a PRIORITY of 5, which makes that our PRIMARY e-mail server, running on an IP ADDRESS of 173.165.112.155, and;*
- ❖ *FIFI.CHICAGONETTECH.COM, with a PRIORITY of 10, makes that our SECONDARY e-mail server, running on an IP ADDRESS of 173.165.112.146*

Make certain these are both setup in DNS, with the appropriate HOST NAME records, MX records, and PRT records pointing to the HOST NAME records.

The MX record number which is the LOWEST will always be the first to be attempted when e-mail is delivered to your server from outside your domain.

You will also want to have your internet service bandwidth provider, the company who allocates your static IP ADDRESSES, map rDNS [IN-ARPA or REVERSE DNS] entries back to those HOST NAMES for your MX records.

These settings are available under the SmarterMail primary ADMIN account via:

SETTINGS → PROTOCOL SETTINGS → SMTP OUT:

The screenshot shows the 'Protocol Settings' window with the 'SMTP Out' tab selected. The 'Save' button is at the top left. Below the tab bar, the following settings are visible:

- Outbound IPv4:** 173.165.112.155 (dropdown menu)
- Outbound IPv6:** Use Primary IP on NIC (dropdown menu)
- ☒ **Enable primary IP on failure**
- Command Timeout:** 60 (text input) Second(s)
- Max Spam Check Threads:** 30 (text input)
- Max Delivery Threads:** 50 (text input)
- ☐ **Enable DNS caching**
- ☒ **Enable TLS if supported by the remote server**

NOTES:

- ❖ The OUTBOUND IP is the DEFAULT OUTBOUND IP for all domains hosted on your SmarterMail server. If you host multiple domains with separate IP ADDRESSES assigned to those domains, or you have SSL setup to use a specific IP ADDRESS as would probably be the case if you have enabled TLS, then you may need to change this default IP ADDRESS for specific domains or services.
- ❖ If you run more than one domain on SmarterMail, remember to check the OUTBOUND IP address for each domain you host. This can be found by selecting the domain, EDITING the domain settings and then navigating to the TECHNICAL TAB and selecting the OUTBOUND IP address from the drop down box. If you should ever have to change IP address ranges, or add additional IP ADDRESSES to the server hosting your SmarterMail installation, it will be necessary to change the outbound IP ADDRESS in EVERY domain you host via these settings.
- ❖ DO NOT CHECK the DISABLE GREYLISTING box. If it is checked, UNCHECK it. Allowing users or domains to disable greylisting will override one of the most important aspects of your new anti-spam settings and result in your users, once again, being deluged in spam.
- ❖ The EXCLUDE IP FROM RECEIVED LINE was added in SmarterMail version 9. While this may be something which is perceived as being needed by some admins, I highly recommend NOT checking this box.
- ❖ In our case, we have TLS enabled. TLS is an encryption protocol which became available in SmarterMail 8.
- ❖ Beginning with the most recent versions of SmarterMail 9, TLS is available on a PER DOMAIN basis and is enabled or disabled only after enabling TLS on the SmarterMail server, via the TECHNICAL TAB under EDIT DOMAIN. ***TLS must be enabled in BOTH AREAS for TLS to be available for a domain.***

So, now that I have told you we have TLS enabled, you may wonder, what does TLS do and why is TLS important?

TLS enables the full encryption of e-mail, along every step of the message chain, from the desktop to the recipient, where the inter-transport e-mail servers also support TLS and an SSL encryption is used between the desktop and the SmarterMail server.

- ✓ TLS uses PUBLIC KEY CERTIFICATES to verify the identity of the endpoints;
- ✓ In the case of e-mail servers, these endpoints are the SMTP servers which interconnect to transport the e-mail messages;
- ✓ TLS is the upgrade to the SSL protocol which is now partially depreciated.
- ✓ Both work under SSL certificates;
- ✓ Implementation of SSL in SmarterMail requires you run SmarterMail under IIS and disable the SmarterMail web server;

- ✓ The full benefit of TLS is realized only if e-mail originates either via an SSL web interface or a TLS or SSL encrypted client, whether desktop or SmartPhone;
- ✓ TLS is included only in SmarterMail Enterprise edition;

For more information about SSL/TLS, see: http://en.wikipedia.org/wiki/Transport_Layer_Security.

For information on how to implement SSL/TLS in SmarterMail, see my post at:
[http://forums.smartertools.com/showthread.php/29845-SM-9-x-and-SSL-\(Free-Version\)](http://forums.smartertools.com/showthread.php/29845-SM-9-x-and-SSL-(Free-Version))

If you decide to implement TLS on your SmarterMail server you should then test your server to make certain your implementation is working properly.

To test either your SmarterMail TLS installation, or any other e-mail server which claims to be TLS enabled and capable, you can use the free testing tool at:
<http://www.checktls.com/perl/TestReceiver.pl>

Once you have opened the testing website, use the drop-down and select **CertDetail** after entering a full e-mail address for the server you wish to test. Use the e-mail address of Test@CheckTLS.com to see demonstration output for a properly configured TLS e-mail server.

Here is the summary output for the test e-mail address:

TestReceiver

CheckTLS Confidence Factor for "Test@CheckTLS.com": 100

MX Server	Pref	Connect	Allowed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
mail2.CheckTLS.com [204.225.38.195]	20	OK (1ms)	OK (4ms)	OK (1ms)	OK (1ms)	OK (207ms)	OK (6ms)	OK (78ms)	OK (4ms)
www1.CheckTLS.com [24.123.1.3]	30	OK (117ms)	OK (1,031ms)	OK (88ms)	OK (86ms)	OK (595ms)	OK (251ms)	OK (352ms)	OK (92ms)
Average		100%	100%	100%	100%	100%	100%	100%	100%

In the example above the e-mail address, test@checktls.com shows that the e-mail servers used by checktls.com are both capable of fully supporting the TLS encryption protocol and the SSL certificate is both valid, not expired, and properly installed on the server.

The **CertDetail** level test performed will also generate approximately 5 pages of test data showing all negotiations, results, and certificates used during the testing process.

If this test positively validates a TLS server, then the server is both capable of, and properly configured to use, TLS negotiations and encryption during the process of sending, and receiving, of e-mail messages.

Failure to encrypt e-mail can cause unwanted and undesirable results in today's hacker and corporate raider environment. Every e-mail server operator should consider upgrading their mail server to support TLS and SSL. Read on, McDuff!

RESULTS FROM A NON-TLS COMPLIANT E-MAIL SERVER, or How the FBI and Scotland Yard Shot Themselves In the Foot:

For an interesting sidebar on how the lack of TLS got the FBI and Scotland Yard into trouble with the nefarious group Anonymous, see the following blog:

<http://networkbastion.blogspot.com/2012/02/anonymous-vs-fbi.html>

Here is the FAILED TLS test from the FBI's e-mail server:

TestReceiver

CheckTLS Confidence Factor for "Timothy.Lauster@ic.fbi.gov": 0

MX Server	Pref	Connect	Allowed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
mail.ic.fbi.gov [153.31.119.142]	10	OK (83ms)	OK (2,703ms)	OK (72ms)	FAIL	FAIL	FAIL	OK (2,932ms)	OK (75ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%

It was not just the FBI's e-mail server which failed the TLS testing, but the e-mail servers of other intelligence groups whom the United States deals with on a day-by-day basis as we attempt to prevent infiltration of government, military, corporate and personal e-mail communications and networks.

Had TLS been properly installed and tested on the e-mail servers of the various intelligence communities involved, the incident outlined in the blog would probably never have happened.

Out of the six intelligence agencies involved, only three passed the basic TLS encryption security capabilities on their e-mail servers.

NOTES:

- ❖ E-Mail servers which run Greylisting may require a second test after a few minutes to display completely accurate results.
- ❖ Failure to validate an e-mail address as part of the test does not mean the TLS enabled e-mail server has failed the TLS testing.

E: SETTINGS → PROTOCOL SETTINGS

Make certain you are not an open, or partially open, relay: [Your SMTP BANNER may be different. I keep ours up to date with the current VERSION information whenever we update.]

←

Protocol Settings

Save

POPIMAPLDAPSMTP InSMTP OutXMPPEWEASEAS

Changing the Allow Relay setting to Anyone or Only Local Domains can potentially cause your server to become an open relay.

SMTP Banner

#HostName# #TimeUTC# UTC - SmarterMail Enterprise 11.0.48

Allow Relay

Nobody

Session Timeout

15

Minute(s)

☒ Enabled

Command Timeout

120

Second(s)

Max Bad Commands

4

Max Connections

10000

(0 = unlimited)

Max Hop Count

20

Max Message Size

50

MB (0 = unlimited)

Max Bad Recipients

20

(0 = unlimited)

Append Received Line

All Incoming Messages

Require Auth Match

Email Address

☐ Enable VRFY command

☐ Enable EXPN command

☒ Allow relay for authenticated users

☒ Enable domain's SMTP auth setting for local deliveries

☐ Disable AUTH LOGIN method for SMTP authentication

Autodiscover Host

securemail.chicagonette.com

Autodiscover Port

465

☒ SSL

Settings.aspx#

F: PASSWORDS – the Bane of Every Administrator:

To check your password requirement settings, goto

SECURITY → ADVANCED SETTINGS → PASSWORD REQUIREMENTS

and modify your password settings as necessary.

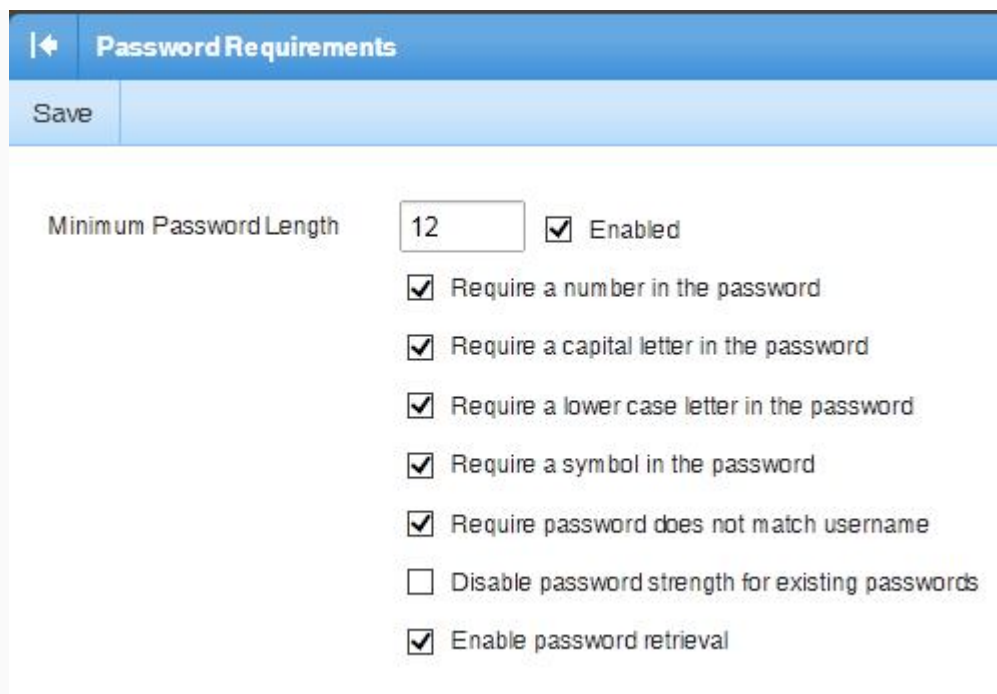
We currently require passwords to be a minimum of TWELVE [12] characters in length with at least ONE UPPERCASE LETTER, 1 NUMBER and 1 SPECIAL CHARACTER in the password.

We do not allow any exceptions to the password rule. This prevents a lot of headaches because it eliminates short and simple passwords and prevents having our mail server hacked.

Note that setting a minimum of 12 characters [up from 8 in prior versions of this document] does not preclude longer passwords as SmarterMail does not check for a maximum password length. This is actually a good thing because it allows your users to use PASS PHRASES.

So, with the settings show above, both: "rG#34_1@4b" and "meYe d0Ggi3 hA\$ f133Z" or "th3 R^1n |n \$pa1N f*Iz Ma|n|y |n T%3 pL^|n" are all acceptable passwords – with the second two examples actually being pass phrases: longer, and easier to remember than the first. They all meet the secure password requirements shown in the password configuration screen below, and they are all secure.

Generally speaking, the longer the password or pass phrase, the more secure it is, and the less likely it is to be hacked by spammers, and the safer your SmarterMail installation will be:



The screenshot shows the 'Password Requirements' configuration window. At the top is a blue header with a back arrow and the title 'Password Requirements'. Below the header is a light blue bar with a 'Save' button. The main area contains the following settings:

- Minimum Password Length:** A text box containing '12' and a checkbox labeled 'Enabled' which is checked.
- ☒ Require a number in the password
- ☒ Require a capital letter in the password
- ☒ Require a lower case letter in the password
- ☒ Require a symbol in the password
- ☒ Require password does not match username
- ☐ Disable password strength for existing passwords
- ☒ Enable password retrieval

NOTE: leaving the DISABLE PASSWORD STRENGTH FOR EXISTING PASSWORDS box checked will allow users to keep passwords which DO NOT meet the defined password requirements.

Leaving this blank will force everyone to change their passwords to meet the new requirements when they next login via the webmail interface.

G: FURTHER PROTECTING YOUR SMARTERMAIL E-MAIL SERVER REPUTATION

To help protect your SmarterMail installation, you can do a couple of additional things:

- **Setup an SPF record** which points ONLY to the IP ADDRESS or IP ADDRESSES authorized to send messages from your e-mail server(s). Do NOT use a range. Setup specifically for the e-mail server, or servers, allowed to send. For more information see: <http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/>

- **Setup both DOMAIN KEY and DKIM signing:**

NOTES:

DOMAIN KEYS ARE SPECIFIC TO THE DOMAIN.

EACH DOMAIN MUST HAVE A UNIQUE DOMAIN KEY CERTIFICATE.

EACH DOMAIN KEY CERTIFICATE MUST BE PLACED INTO THE DNS RECORD OF THE DOMAIN FOR WHICH IT WAS GENERATED

YOU SHOULD ALSO SETUP A DOMAIN KEY POLICY RECORD FOR YOUR DOMAIN

YOU CANNOT PLACE DOMAIN KEYS FOR MULTIPLE DOMAINS INTO OTHER DNS RECORDS

❖ These keys are setup on a PER DOMAIN BASIS via the MANAGE tool for the domain.

❖ To setup DOMAIN KEYS:

- **SELECT THE DOMAIN FOR WHICH YOU WISH TO CREATE THE KEY**
- **SELECT MANAGE**
- **SELECT SETTINGS → DOMAIN SETTINGS → ADVANCED SETTINGS → MAIL SIGNING → OPTIONS.**

❖ Enable BOTH ENABLE DOMAIN KEY SIGNING and ENABLE DKIM SIGNING

Mail Signing [chicagonettech.com]

Save

DNS test was successful.

Options Certificate DomainKeys Signing DKIM Signing

☒ Enable DomainKey signing

☒ Enable DKIM signing

- ❖ Then click on the tabs CERTIFICATES, DOMAIN KEYS SIGNING, and DKIM SIGNING, and complete the forms according to the HELP FOR THIS PAGE from SmarterMail. They have done a pretty good job with this section of the help files.

Here is a picture of the process of generating the certificate required for DOMAIN KEYS. Note that the KEY SIZE can be selected as 512, 768, and 1024. Shorter keys require less work on the part of both the sending and receiving e-mail servers but are less secure.

NOTE: Microsoft officially discontinued support for certificates less than 1024 bits in 2012. The effect of this on Mail Signing is not yet published and will be added when that research is completed.

The longer the Domain Key certificate, the better.

Most modern e-mail servers can handle 1024 bit keys without any problems.

Mail Signing [chicagonettech.com]

Save Generate Key Test DNS

Options Certificate DomainKeys Signing DKIM Signing

Selector CNT

Key Size 1024

Add the following TXT record to DNS

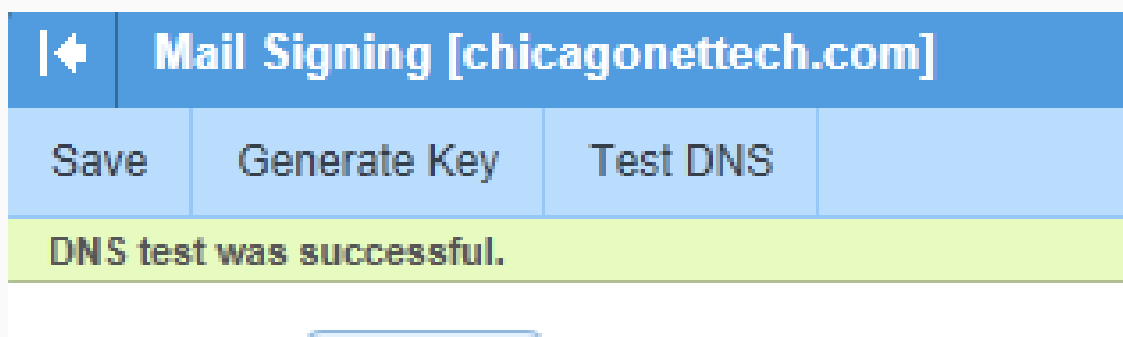
TXT Record Name CNT._domainKey.chicag

TXT Record Value p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa3m0LhcIE...

- ❖ Note the TXT record name? Domain Keys are added to your DNS as TXT records.

- ❖ First enter a SELECTOR to differentiate your domainKey and give it a name.
- ❖ Now Generate Key. This will both create the TXT Record Name and the TXT Record Value.
- ❖ **SAVE YOUR RECORD! If you do not SAVE your record at each step, your tests will fail.**
- ❖ Even though the FQDN of the Key is *CNT._domainKey.chicagonettech.com*, when you add them to the DNS record, the only portion of the TXT RECORD NAME you enter into RECORD NAME portion of the DNS is, according to the example above, is "CNT.domainKey" [without the quotes].
- ❖ The Microsoft GUI DNS tool will automatically append your domain name to the TXT record and create your domainKey certificate record.
- ❖ If you are using DNS other than Microsoft's DNS, consult your DNS to see how to add a TXT record.
- ❖ The TXT Record VALUE is your actual certificate and goes into the TXT box of the TXT record. Save both the new TXT record value in SmarterMail and the newly created TXT record in your DNS for the domain, and you should be able to click on the TEST DNS and receive a PASSED notation at the top.

A test of a successful generation, and DNS install, of your domainKey certificate will look like this:



➤ **Setup a DOMAIN KEY POLICY RECORD**

Once you have setup and tested your DomainKey record, you should also setup a DOMAIN KEY POLICY RECORD.

Using DomainKey Policy records publish policy statements in your DNS that help e-mail receivers understand how they should treat your email. There are three main statements that can be published:

- "t=y" - Which means that your email DomainKeys are in test mode.
- "o=-" - All email from your domain is digitally signed.
- "o=~" - Some email from your domain is digitally signed.
- "n=*" - n stands for notes. Replace the * symbol, with any note you like

The DomainKey Policy is an ADDITIONAL TXT RECORD which is added to into the same DNS container as your DomainKey record.

In the case of chicagonettech.com, our published records look like this:

Here is the additional DNS container shown under the CHICAGONETTECH.COM domain in DNS:



Here are the two records as shown within the actual DNS record:

Backup Zones\chicagonettech.com_domainkey]		
elp		
_domainkey 2 record(s)		
Name	Type	Data
cnt	Text (TXT)	p=MIGfM,
{same as parent folder}	Text (TXT)	o=-

- The DomainKey record is on the first line, beginning with CNT
- The DomainKey Policy record is on the second line and has no name in the record.
- The policy in the DomainKey Policy record is "o-", which tells all receiving e-mail servers that ALL OUTGOING E-MAIL sent from securemail.chicagonettech.com is signed.

A very good explanation of both DOMAINKEY SIGNING, DKIM SIGNING and DOMAINKEY POLICY is available at: <http://www.unlocktheinbox.com/resources/domainkeys/>

An additional explanation of DOMAINKEY SIGNING and DKIM SIGNING can be found in the SmarterMail KB at

<http://help.smartertools.com/SmarterMail/v9/Default.aspx?p=SA&v=9.0.4408&lang=en-US&page=domainadmin%2ffrmdomainkeys>

For more information on DOMAIN KEYS see:

http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail and <http://www.dkim.org/>

H: SETUP DMARC

DMARC was introduced to SmarterMail beginning with Version 9. In the short time since the introduction of DMARC to the e-mail industry, DMARC has been adopted by more than 60% of all e-mail providers.

DMARC, or *Domain-based Message Authentication, Reporting & Conformance*, is an approach designed to help stop or reduce e-mail spam and phishing attacks.

The DMARC specification is based around existing email authentication using SPF or DKIM. This will effectively allow email senders, when sending email to receivers implementing DMARC, to experience more uniform authentication.

DMARC is backed by some very large corporations, including: Google, American Greetings, PayPal, Microsoft, Comcast, FaceBook, LinkedIn, AOL and several others.

To use DMARC, a domain owner publishes a DMARC policy record in their DNS. Once published, any e-mail server which supports DMARC can check e-mail received from the publishing e-mail server to make sure the messages received from the domain are valid.

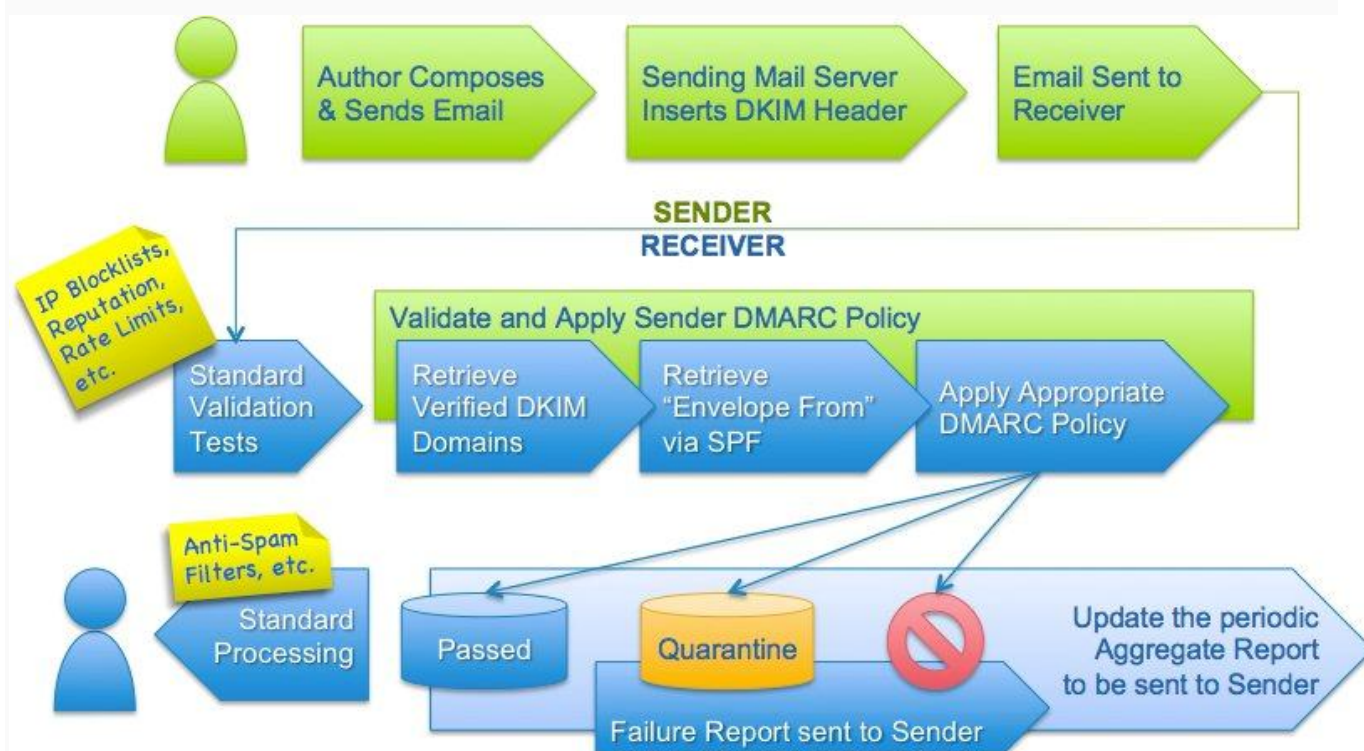
Part of the DMARC specification instructs the receiving e-mail server on how it is to handle messages which do not authenticate against the DMARC record published by the sending e-mail server. This takes the burden off the receiving e-mail server because there are specific instructions about what to do with a message which is determined to be invalid: quarantine, reject, nothing.

DMARC allows the management team of the SENDING DOMAIN to determine how spoofed and unauthorized e-mail is to be handled. DELETE IT, SEQUESTER IT, or IGNORE IT. *The receiving domain MUST abide by the SENDING domain's instructions to be fully DMARC compliant.*

DMARC also adds a provision for AFRF, or Authentication Failure Reporting Format ([RFC 5965](https://tools.ietf.org/html/rfc5965)) - which allows reports to be passed back to the sender containing information about any successes or failures that the receiver may have encountered.

DMARC is not yet a final specification but is already in use by more than 60% of ISPs offering e-mail services throughout the world. For a thorough understanding of DMARC, see: www.dmarc.org.

DMARC.ORG has published a graphic showing how DMARC is to be processed in relation to other antispam and e-mail processing when an e-mail message is received by the server:



Source: <http://dmarc.org/overview.html>

Unfortunately, DMARC.org does not provide an easy to use tool to generate a DMARC record for your e-mail server, but there are other resources available on the internet.

The best resources I have found for generating DMARC records is located on the website [UNLOCK THE INBOX](#).

UNLOCK THE INBOX provides not only a great explanation of how DMARC works, but also provides a tool which will allow you to generate a DMARC record for your domain's DNS records using a step-by-step process. The UNLOCK THE INBOX DMARC RECORD GENERATOR is located here: <http://www.unlocktheinbox.com/dmarcwizard/>

To use the DMARC RECORD GENERATOR, simply enter:

- your DOMAIN NAME;
- the e-mail address where you want to receive AGGRIGATE E-MAIL reports [reports from the ISPs of which messages failed SPF and DKIM checks (DMARC)];
- the e-mail address from where you want to receive FORENSIC E-MAIL [sample messages that are failing SPF and DKIM checks (DMARC)];
- your MAIL RECEIVER POLICY – NONE, QUARANTINE, REJECT [policy that defines how you would like the ISPs to handle messages that failed SPF and DKIM];
- the PERCENTAGE OF MESSAGES you want checked – 0 to 100%;
- click GENERATE DMARC RECORD

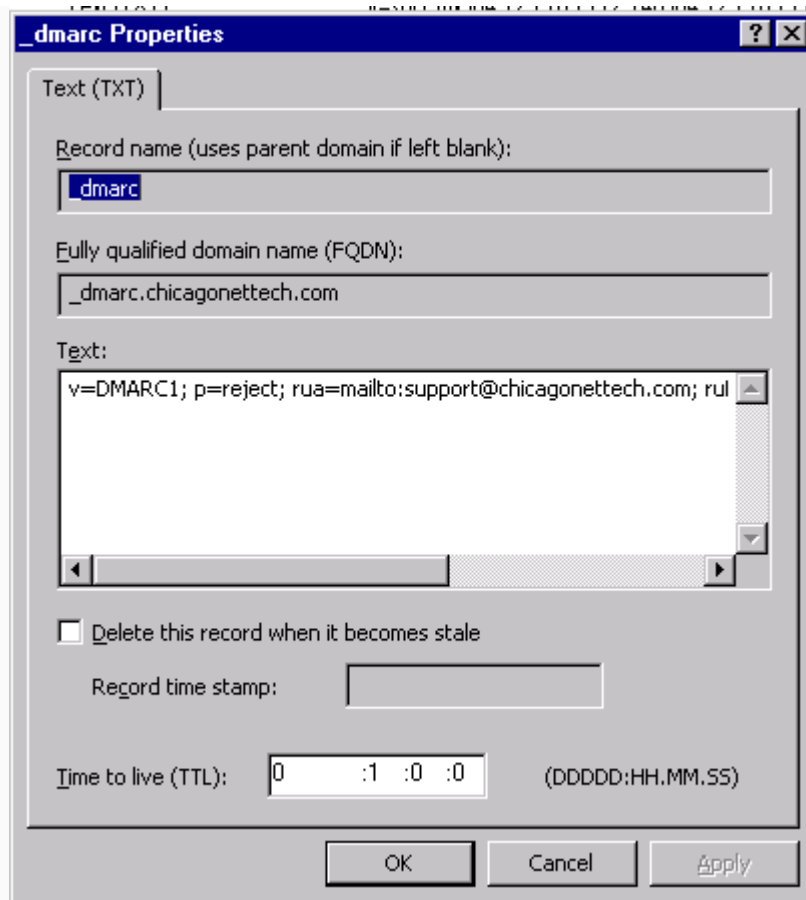
In the case of CHICAGONETTECH.COM, the DMARC RECORD generated by the tool creates:

**"v=DMARC1; p=reject; rua=mailto:support@chicagonettech.com;
ruf=mailto:support@chicagonettech.com; pct=100"**

So using the Microsoft DNS GUI, you would create a new TXT RECORD.

The TXT record MUST have the NAME _DMARC. In our case, ChicagoNetTech's DMARC FQDN is "_dmarc.chicagonettech.com"

Here is a screen capture of our DMARC TXT record from our DNS server. [The actual TEXT of the DMARC record does not wrap when pasted into the TEXT box]



I: Abuse Detection: Protecting your SmarterMail server from DOS attacks, Harvesting Attacks, and Internal Spammers, and Brute Force Protocol Attacks

For several major releases, SmarterMail has had the ability to supplement against DOS, Harvesting and Internal Spammers. Beginning with SmarterMail 11.X, SmarterMail has introduced an extremely powerful tool which allows SmarterMail Administrators to setup parameters against Brute Force attacks on user accounts . . . and the code behind the tool is nothing short of remarkable!

The new PASSWORD BY BRUTE FORCE PROTOCOL literally monitors each username attempting to login to the SmarterMail server according to protocol type based on the IP ADDRESS attempting to do the login.

If an IP ADDRESS is found to be attempting to access an account more than the number of times established in the test, within the time period allocated, access to that user's account, from that IP address is blocked for the specified period of time.

As I have come to understand the PASSWORD BY BRUTE FORCE PROTOCOL detection process, if an IP address appears to be part of an attack against a specific account is denied, only attacks against the specific account are denied. Legitimate attempts to access other accounts from the same IP ADDRESS are allowed and not blocked. Brilliant coding, absolutely brilliant!

The inclusion of this new tool for PASSWORD BY BRUTE FORCE PROTOCOL is, in and of itself, reason to upgrade to SmarterMail 11.X.

The settings for ABUSE DETECTION are found under **SECURITY → ADVANCED SETTINGS → ABUSE DETECTION**. The settings use by ChicagoNetTech, and populated to those servers which we maintain, are show below:

Abuse Detection 13						
New Edit Delete						
<input type="checkbox"/> Detection Type	Service	Time Frame	Count	Block Time	Description	
<input type="checkbox"/> Denial of Service (DOS)	IMAP	10	50	60	Denial of Service - IMAP - 50 in 10 Min	
<input type="checkbox"/> Denial of Service (DOS)	LDAP	10	50	60	Denial of Service - LDAP - 50 in 10 Min	
<input type="checkbox"/> Denial of Service (DOS)	POP	10	50	60	Denial of Service - POP - 50 in 10 Min	
<input type="checkbox"/> Denial of Service (DOS)	SMTP	10	50	60	Denial of Service - SMTP - 50 in 10 Min	
<input type="checkbox"/> Denial of Service (DOS)	XMPP	10	50	60	Denial of Service - XMPP - 50 in 10 Min	
<input type="checkbox"/> Bad SMTP Sessions (Harvesting)		10	50	60	Harvesting: 10 in 50	
<input type="checkbox"/> Bad SMTP Sessions (Harvesting)		5	30	60	Harvesting: 5 in 30	
<input type="checkbox"/> Internal Spammer Notification		5	50		Internal Spammer Notification	
<input type="checkbox"/> Password Brute Force by Protocol	IMAP	5	10	5	IMAP Password Brute Force Protection	
<input type="checkbox"/> Password Brute Force by Protocol	LDAP	5	10	5	LDAP Password Brute Force Protection	
<input type="checkbox"/> Password Brute Force by Protocol	POP	5	10	5	POP Password Brute Force Protection	
<input type="checkbox"/> Password Brute Force by Protocol	SMTP	5	10	5	SMTP Password Brute Force Protection	
<input type="checkbox"/> Password Brute Force by Protocol	XMPP	5	10	5	XMPP Password Brute Force Protection	

Each category of settings can be setup with individual parameters for TIME FRAME, COUNT, and BLOCK TIME. The descriptions are customizable.

The INTERNAL SPAMMER NOTIFICATION sends a notice indication the SENDING E-MAIL ADDRESS, and number of messages sent to a specified e-mail account or accounts. [Multiple recipients should be separated by a semi-colon and space.]

IP ADDRESSES which are temporarily blocked by the settings in the chart above can be seen, in real time by SmarterMail system administrators on the MANAGE [wrench] page, under CURRENT IDS blocks. The cumulative list of all blocks can be seen by selecting ALL BLOCKS or the blocks for the individual protocols can be seen by selecting the specific protocol in the list.

These are extremely powerful protection tools which, along with STRICT and STRONG PASSWORD enforcement, can help protect your SmarterMail server from being compromised and used by spammers.

J: TEACH YOUR USERS NOT TO RESPOND TO PHISHING E-MAIL MESSAGES!

Sorry if I appear to be shouting, but the long, ALL CAPS, bolded title was deliberate.

General rule of thumb: ***If you don't recognize the sender, or were not expecting an attachment, DO NOT OPEN THE MESSAGE – DELETE IT!***

Phishing e-mail responses cause more problems with compromised e-mail accounts, identity theft, and compromised business networks and workstations than all other problems combined.

No matter how much you secure your e-mail server, no matter how well you protect your network, no matter how good the tables in your firewalls are constructed, all it takes is one hair-brained user sharing personal information with a total stranger to undo all of your hard work.

The FTC has published an excellent article on Phishing scams, which is available as a FREE PDF from their website, in both English, and Spanish, that is both well written, and easy to understand.

The FTC's Phishing Scam article is available on the FTC website at:
<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>

A downloadable, and re-distributable, PDF version is available at:
<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf>

If you are an ISP, make this available for download, via a link from your website or on your e-mail FAQ page, so that every person who you provide services for has an opportunity to read it.

For your business customers, you have an excellent opportunity to help them run a tighter workplace by making this available to them for distribution to their employees.

If you are a business, you might consider making the FTC's PDF part of your employment or IT security manual which you distribute to all employees when they are hired.

K: SUMMARY

Once you have your new antispam settings configured you will be able to monitor your server and see the actual results of your efforts.

First, you will have to make certain your logs are set for DETAILED recording of all log data. To do this go to **SETTINGS → LOG SETTINGS** and make certain you have your logs set to DETAILED for both DELIVERY and SMTP.

Once you have your logs set for detailed logging you can search. Logging can only be performed by SmarterMail admins. To view your SmarterMail logs, go to

MANAGE → VIEW LOGS.

- Search both the DELIVERY LOGS and the SMTP logs [be certain to check the ENABLE RELATED TRAFFIC BOX] for

❖ **"rsp: 554 Sending address not accepted due to spam filter".**

- ❖ The results will show you which messages were denied messages because of spam and why they are being denied.

- You will also be able to see both the spam tests, and results, for the delivery of all other messages processed by the server.
- [NOTE: We designed our servers with enough capacity to keep all logs for a minimum of FIVE [5] years because of our medical and healthcare clients. This is in compliance with the new HIPAA / HITECH Agency requirements which were made law in October 2011 and challenges to the laws only served to reinforce the security requirements from both the LOG retention; liability of the contractors and, now subcontractors; and physical server room access controls.]
- By using these settings we have close to ELIMINATED our spam problem. It CAN be done and it does not take a lot of effort or extra cost.
- **Get rid of content filtering.** It is a pain to maintain and will drive you crazy trying to stay ahead of the spammers and hackers as they come up with new ways to get around your content filters.
- **Do not use the antispam wizard.** Use the capabilities of the built in antispam tools in SmarterMail to your advantage. *[NOTE: This is subject to review and modification as SmarterTools did incorporate some of my original document into those filters and has blanket permission to do the same with these suggested settings.]*
- **LIMIT WHITELISTING.** Well created and properly setup e-mail servers should not have to be whitelisted. Poorly designed and improperly setup e-mail servers are not our problem. They are indicative of someone who does not know what they are doing or who should not be running an e-mail server in the first place. It doesn't cost a lot of money to setup an e-mail server properly.
- If you encounter a problem you would normally whitelist, **search out the real problem and inform of the administrators of the domain** with the problem about the issues.
- Ask the administrators with improperly setup e-mail servers and/or DNS servers to correct the problem on their end. There are several free and paid DNS testing tools available via searching the Internet which can assist you in troubleshooting those issues.
- **Run REPORTS:**
 - ❖ Go into **REPORTS → SPAM AND VIRUS REPORTS → GREYLISTING** and set a date range to see how many e-mail servers never re-send because they are spammers.
 - ❖ **Reports can also be created on both a SERVER and DOMAIN LEVEL.** You can also create custom reports and have them e-mailed on a regular schedule.
 - ❖ **Other reports are available as well.** Experiment with what is already built into SmarterMail and see how well your server is doing and what resources your customers are using.

Once you have configured these settings, monitor your server for a while. You should see a huge improvement in the amount of spam you process immediately.

Using these settings provides no guarantee that you will not have any spam.

Spam will never be completely eliminated because the spammers are constantly monitoring what we, as ISPs and providers are doing and adapting to circumvent our tools. Even with these new antispam settings in place on your SmarterMail installation you may, occasionally, see some spam creep through and end up in user's mail boxes.

You can help prevent this from happening by making certain you **do not allow your users to override greylisting or spam settings**. Doing so will both allow spam to start to come through again and will also cause you hours of support headaches and ill will with your customers and users.

Spammers make large amounts of money off the relatively small percentage of people who respond. In the case of identity theft, the result is often years of working to resolve unauthorized charges on credit cards, money stolen from bank accounts, and ruined credit. As SmarterMail operators we have an obligation to protect our users from all kinds of spam.

Much of what you are likely to encounter is [joe-jobbing](#). If you are the victim of joe-jobbing there is nothing which can be done except to ride out the storm, but using DMARC and forcing the SENT FROM to MATCH the REPLY TO e-mail addresses will go a long way to prevent [joe-jobbing](#).

You may also encounter spam from spammers who have setup e-mail servers which meet all of the requirements set forth by the IETF and are not trapped by these filters.

Again, and I cannot repeat this too often, make certain you do not allow your users to override greylisting or spam settings.

Finally, and I cannot impress this frequently enough, **make certain you enforce SECURE passwords**.

Our secure passwords now require passwords which are at least twelve [12] characters in length, and require a combination of UPPER and lower case letters, numbers, and special characters. This will help to eliminate insecure passwords; eliminate the possibility of your users from using the names of family members, pets, and friends; and will also eliminate words which are in the dictionary. The additional security resources provided by SmarterMail 11.X will also help prevent hackers from effecting a dictionary or harvesting attack against your SmarterMail server if configured properly.

L: RESOURCES

RESOURCES: SPF, DMARC, DOMAINKEYS, DKIM, TESTING TOOLS, and STANDARDS . . .

Given the myriad new reputation tools for domains which are now being included in both SmarterMail and other e-mail server software programs, I thought I would post some of the resources which I commonly use for testing, along with some of the standards resources, I commonly use in diagnosing issues which present themselves from time-to-time with my customer networks and by members of these forums who post here. Let's start with [UNLOCK THE IN-BOX](#):

UNLOCK THE IN-BOX

Henry Timmes over at [UNLOCK THE IN-BOX](http://www.unlocktheinbox.com/) has created an incredible website full of tools which are FREE, supported by donations only, and available at: <http://www.unlocktheinbox.com/>

[UnlockTheInBox](http://www.unlocktheinbox.com/) will both discuss the basis for, assist with the proper configuration of, and let you test your settings for:

- [SPF Records;](#)
- [MX Records;](#)
- [PTR Records;](#)
- [DOMAINKEYS;](#)
- [DMARC Records](#)

New features and tests are added to the [UNLOCK THE IN-BOX](http://www.unlocktheinbox.com/) site regularly.

Note that in addition to the DOMAINKEYS TXT record, ADDITIONAL DOMAINKEYS TXT records, called a **DOMAIN KEY POLICY RECORDS [each item must be in a SEPARATE TXT RECORD]**, can be added which allow you to can publish a policy statement in DNS that help email receivers understand how they should treat your email.

The four DOMAINKEYS statements, which can be published IN ADDITION TO the DOMAINKEY certificate, include [remember to OMIT THE QUOTES from the TXT record!]:

- "t=y" - Which means that your email DomainKeys are in test mode
- "o=-" - All email from your domain is digitally signed
- "o=~" - Some email from your domain is digitally signed.
- "n=*" - n stands for notes. Replace the * symbol, with any note you like

NOTE: Be VERY careful about how you configure your DKIM DOMAIN POLICY RECORD!

If you state "o=-" that is 'lowercase o equals minus' [ANOTHER REMINDER: Remember to REMOVE THE QUOTES in the actual record!] in that record, this will indicate that ALL outgoing e-mail in that domain is digitally signed. If you make such a restrictive statement, and then decide to allow any user to override the DKIM policy, their e-mail will probably get rejected as SPAM as the DOMAINKEYS and DKIM policy checking is implemented by more and more e-mail providers.

- DKIM SIGNATURES;
- SENDER ID, and;
- DMARC Records

=====

DMARC

DMARC is a relatively new antispam standard and appears, from both the comments and postings in these and other forums, to confuse a number of those who either have implemented, or are thinking of implementing the protocol.

UNLOCK THE INBOX has an excellent tool for creating the DMARC record for your domain(s) at: <http://www.unlocktheinbox.com/dmarcwizard/>

DMARC can be a very confusing protocol because many of those who want to implement DMARC feel the SENDER should be notified when a message is rejected.

DMARC can also be very confusing because it is one of the few antispam protocols which MUST be checked BEFORE a message is actually accepted by the receiving e-mail server. That is counterintuitive to both programmers and e-mail server admins.

More information about the DMARC protocol, the standards upon which it was developed, and the proper implementation, by both programmers and end users, can be found at <http://www.dmarc.org/>.

The complete technical specification for DMARC, which stands for "Domain-based Message Authentication, Reporting and Conformance," is available at: <http://www.dmarc.org/draft-dmarc-base-00-01.html>.

DMARC mandates that the PUBLISHER of the record makes the determination on how malformed e-mail shall be handled. If the DMARC record wants the message discarded, then the receiver must, under the current release of the protocol, discard the message.

Whether you agree with how DMARC works or not, it is a standard which is in the process of being implemented, has been adopted by more than 60% of ISPs worldwide, and, if used, is expected to be implemented and work in the manner specified by [DMARC.ORG](http://www.dmarc.org/).

TLS

TLS is an encryption protocol which is the replacement standard for SSL. TLS capabilities were introduced into SmarterMail 8 ENTERPRISE edition.

More information on the TLS standards, and how TLS works, can be found at: http://www.google.com/support/enterprise/static/postini/docs/admin/en/admin_ee_cu/ib_tls_overview.html

TLS requires:

- an SSL certificate;
- that SmarterMail be setup to run under IIS as SSL cannot be installed under the SmarterMail browser;
 - See: <http://portal.smartertools.com/KB/a1...archID=443848>, for configuring IIS 6;
 - See: <http://portal.smartertools.com/KB/a1...earchID=443848>, for configuring IIS 7;
 - See: <http://portal.smartertools.com/KB/a2814/set-up-smartermail-as-an-iis-site-in-iis-8.aspx?KBSearchID=521653>, for configuring IIS 8.
- TLS requires:
 - proper ports be setup under the newly redesigned port mapping interface in SmarterMail 8 or 9 ENTERPRISE, per the instructions for setting up TLS, located at: <http://portal.smartertools.com/KB/a1...earchID=443847>, are followed TO THE LETTER!
 - you have a SOLID WORKING KNOWLEDGE of IIS host headers in Microsoft Windows;
 - you have a SOLID WORKING KNOWLEDGE of DNS in Microsoft Windows, or with whomever your DNS hosting is provided.
 - NOTE: Some "DNS PORTALS" are not capable of properly setting up the DNS records for some of the new reputation protocols.

Once you have setup TLS on your SmarterMail 8 Enterprise, or SmarterMail 9 Enterprise installation, you can TEST your SmarterMail TLS installation to make certain it is working properly by using the test available at: <http://www.checktls.com/perl/TestReceiver.pl?ASSURETLS>

After opening <http://www.checktls.com/perl/TestReceiver.pl>

You will be on the TEST RECEIVER page of the testing system. This will test the capability of your SmarterMail e-mail server to run TLS for mail delivered to other e-mail servers which also run valid TLS.

- Enter A VALID e-mail address on the SmarterMail server you wish to test;
- Select CERT DETAIL from the drop down menu below the e-mail window;
- Click START TEST;

There will be a short delay, shown by a countdown timer, and your test will begin.

By using the CERT DETAIL test you will see all of the detail, along with any errors which might be reported, in the report window.

NOTE: There was a problem with SmarterMail 9.2.4464, which broke TLS. The errors were showing up as a down-conversion to SSL, along with errors in the SMTP logs in SmarterMail. There were also errors with clients who were trying to use TLS to connect to SmarterMail to send and receive e-mail.

This was resolved with an interim release of SmarterMail 9.2.4469 which fixed the problems.

Again, PLEASE NOTE that TLS ONLY WORKS IN SMARTER MAIL 8.X, 9.X, 10.X, and 11.X ENTERPRISE VERSIONS and requires a very specific set of configurations on the part of the SmarterMail licensee.

You will also see a summary at the top of the window.

NOTE: Greylisted e-mail accounts may show RECEIVER FAIL if they are Greylisted. If that is the case, simply wait the required time stated by your greylisting settings and retry the tests. This will show up in the TLS TEST detail as: "[451 Greylisted, please try again in 240 seconds](#)".

Here is an example of GREYLISTED TLS RESULTS:

TestReceiver

CheckTLS Confidence Factor for "tstest@chicagonettech.com": 98

MX Server	Pref	Connect	Allowed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
securemail.chicagonettech.com [173.165.112.155]	5	OK (8.0ms)	OK (7.4ms)	OK (6.9ms)	OK (6.9ms)	OK (47.8ms)	OK (7.6ms)	OK (8.8ms)	FAIL
fifi.chicagonettech.com [173.165.112.146]	10	OK (9.4ms)	OK (6.9ms)	OK (6.9ms)	OK (7.4ms)	FAIL	OK (8.40ms)	OK (7.5ms)	FAIL
Average		100%	100%	100%	100%	50%	100%	100%	0%

(double click matrix to select all for copy and paste)

Note: Cert failures do not affect TLS encryption, but may mean the site isn't who they say they are.

If you would like to try our chicagonettech.com e-mail server, then use the e-mail address of **TLSTEST@CHICAGONETTECH.COM** to test to our SmarterMail installation so you can see the results of our chicagonettech.com e-mail server.

Here is an example of an e-mail address which has been retried after the greylisting period requirements have been met.:

NOTE THAT THE SECOND LINE WILL INDICATE A FAILURE because the 2nd e-mail server is NOT setup with an SSL certificate:

TestReceiver

CheckTLS Confidence Factor for "tlstest@chicagonettech.com": 98

MX Server	Pref	Connect	Allowed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
securemail.chicagonettech.com [173.165.112.155]	5	OK (81ms)	OK (68ms)	OK (70ms)	OK (74ms)	OK (458ms)	OK (74ms)	OK (88ms)	OK (70ms)
fifi.chicagonettech.com [173.165.112.146]	10	OK (79ms)	OK (68ms)	OK (72ms)	OK (74ms)	FAIL	OK (725ms)	OK (75ms)	OK (75ms)
Average		100%	100%	100%	100%	50%	100%	100%	100%

(double click matrix to select all for copy and paste)

Note: Cert failures do not affect TLS encryption, but may mean the site isn't who they say they are.

You can also test e-mail sent FROM your SmarterMail server by opening the page at <http://www.checktls.com/perl/TestSender.pl> and following the instructions to SEND an e-mail FROM your SmarterMail e-mail account, or any other e-mail account you may have access to, via the link and key provided on that page.

M: ANTI-SPAM LAWS | US and EU

Legal Requirements of MX Hosting Companies in the USA and EU

The purpose of this table is to give an overview of the basic email requirements in the United States and Europe. Always check the best email marketing practices and the national legislation in each country before engaging in bulk email marketing activities.

Requirements	United States	Europe
Type of Email Messages	The CAN-SPAM Act covers commercial email messages, the primary purpose of which is the advertisement or promotion of a commercial product or service.	The EU directive covers all direct email marketing messages, including charitable and political messages.
Permission / Opt-In	No, the CAN-SPAM Act allows direct marketing email messages	Yes, direct marketing email messages may be sent only to subscribers who

Requirement	to be sent to anyone, without permission, until the recipient explicitly requests that they cease ("opt-out").	<p>have given their prior consent ("opt-in"). Prior permission is required for business-to-consumer (B2C) communication covering all "natural persons".</p> <p>Exceptions: A business relationship in which contact information was obtained constitutes prior consent as long as a means to opt out was provided at the same time and continues to be provided with each such message and each message is about similar products or services by the same company.</p> <p>For business-to-business communication (B2B), i.e. "legal persons", EU member states are free to make "opt-out" the minimum legislation. However, national legislation of the member states can require opt-in for B2B email, too.</p>
Unsubscribe / Opt-Out Requirement	<p>Yes, every message must include opt-out instructions. The sender must honor the opt-out requests of recipients within 10 days.</p> <p>New Rule Provision 2008: An email recipient cannot be required to pay a fee, provide information other than his or her email address and opt-out preferences, or take any steps other than sending a reply email message or visiting a single Internet Web page to opt out of receiving future email from a sender.</p>	<p>Yes, every message must include opt-out instructions. The practice of sending email for purposes of direct marketing or without a valid address to which the recipient may send a request that such communications cease, is prohibited.</p> <p>Existing Business Relationship: When the email address is obtained in the context of the sale of a product or service, the natural or legal person may use the email for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.</p>
Sender Identity	The CAN-SPAM Act bans false or misleading header information. The email's "From", "To" and routing information – including the originating domain name and email address – must be accurate and identify the person who	Disguising or concealing the identity of the sender on whose behalf the communication is made is prohibited.

	<p>initiated the email.</p> <p>The Act prohibits open relay abuses, falsifying header information, generating multiple email addresses to send from, deceptive subject headers, address harvesting and dictionary attacks, and other fraudulent ways of sending spam.</p> <p>New Rule Provision 2008: The definition of "sender" was modified to make it easier to determine which of multiple parties advertising in a single email message is responsible for complying with the Act's opt-out requirements.</p> <p>New Rule Provision 2008: A definition of the term "person" was added to clarify that the CAN-SPAM Act's obligations are not limited to natural persons.</p>	
Subject Lines / Labeling	<p>Deceptive subject lines are prohibited. The subject line cannot mislead the recipient about the contents or subject matter of the message. Identification that the message is an advertisement or solicitation is required.</p>	
Contact Information / Postal Address	<p>Yes, a valid physical postal address is required.</p> <p>New Rule Provision 2008: A "sender" of commercial email can include an accurately registered post office box or private mailbox established under United States Postal Service regulations to satisfy the Act's requirement that a commercial email display a "valid physical postal address".</p>	<p>Yes, the same information disclosure requirements apply to business email as to physical business letters. Companies registered or operating in the EU need to state their company details on every electronic business communication sent from their organization. Business email messages sent by a company should include:</p> <ul style="list-style-type: none"> ▪ The full name of the company and its legal form ▪ The place of registration of the company ▪ The registration number ▪ The address of the registered

		<p>office</p> <ul style="list-style-type: none"> The VAT number <p>A valid return address must be always provided.</p>
Legislation	<p>"CAN-SPAM Act"</p> <p>The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM or the Act).</p>	<p>"EU Opt-In Directive"</p> <p>The EU directive 2002/58/EC. The EU directive specifies a minimum legislation for the member states.</p> <p>Directive 2003/58/EC amending Council Directive 68/151/EEC.</p>
Links	<p>FTC's Spam Site: http://www.ftc.gov/spam/</p> <p>15 USC Chapter 103 - Controlling The Assault Of Non-Solicited Pornography And Marketing http://uscode.house.gov/download/pls/15C103.txt</p> <p>FTC Approves New Rule Provision Under The CAN-SPAM Act http://www.ftc.gov/opa/2008/05/canspam.shtm</p> <p>16 CFR Part 316: Project No. R411008: Definitions and Implementation Under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM Act): Final Rule and Statement of Basis and Purpose http://www.ftc.gov/os/2008/05/R411008frn.pdf</p>	<p>European Law: http://eur-lex.europa.eu</p> <p>EU Directive 2002/58/EC Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Article 13 Unsolicited communications http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF</p> <p>Directive 2003/58/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0058:EN:HTML</p> <p>Amending Council Directive 68/151/EEC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31968L0151:EN:HTML</p>
Wikipedia	http://en.wikipedia.org/wiki/CAN-SPAM	http://en.wikipedia.org/wiki/Directive_on_Privacy_and_Electronic_Communications

ChicagoNetTech is a strong proponent of explicit prior recipient permission, opt-in, and strongly recommends double opt-in, even if this is not required by legislation. Here are two quick checklists that can help you comply with email marketing messaging requirements.

Quick Checklist of Legal Requirements

- Do I have prior explicit and verifiable permission, opt-in, from the recipient?
- Does the message have:
 - A clear and accurate sender identity?
 - An accurate subject line?
 - Clear and easy opt-out instructions?
 - A physical postal address and company details?
 - A valid return address?
- Have I tested that the subscription and unsubscription works?
- Have I checked the test messages carefully before posting? Did my colleague do this, too?
- Can I process the replies and any subscriber requests promptly?

Quick Checklist of Email Best Practices

- Obtain prior permission via double opt-in subscription. Send an automated and well thought-out welcome message with key instructions and expectations.
- Test deliverability
 - Use email authentication: Check that SPF, Sender ID, DomainKeys, Make certain your DNS records correctly verify the sender of the message.
 - Use a spam checker: Scan email message to make sure that it is not identified as spam by common spam filtering applications.
- Test readability
 - Check the HTML message design and readability. It must work with blocked images.
 - Use alternative text part for HTML messages.
 - Keep the subject line short and clear. 25 characters display in most clients.
- Provide wanted, expected, relevant and interesting messages to each recipient.
- Provide clear instruction on how the subscribers can automatically unsubscribe (opt out). Send an automated and well thought-out farewell message. This works as a successful confirmation, gives an opportunity to ask for feedback and thank the subscriber.

N: NEED HELP?

IT has changed significantly in the 40-plus years since IBM was kind enough to underwrite the classes I initially attended while in high school. It is no longer about plugging cables into boards on accounting machines or writing code with a 16K limitation on available memory. We no longer enter data via 80 column punched cards and read the results off of printed paper, and we don't have to wait hours or days to see a result.

The best thing about working in IT is the fact that our field is constantly changing – and constantly challenging.

The SmartPhones we now carry around with us have more than 100,000 times the computing power of the computers sent up in the original Mercury and Gemini space programs and 10,000 times the computing power of early mainframes.

Even for an experienced IT tech: someone who has come up through the ranks, answered the calls on the help desk, can troubleshoot PCs, Macs and printers, in his or her sleep, giving tech support via a hands-free cell phone call while driving down a busy expressway; setting up an e-mail server, even an e-mail server with the reliability and integrity of SmarterMail, can be a daunting endeavor.

The devil is always in the detail! The detail required to properly setup modern IT has so many different aspects to it that locating something that is "not quite right" can completely disable the proper operation of many different aspects of a network but improper configurations are especially significant where e-mail is concerned.

A forgotten HOST entry, selecting the wrong IP address, forgetting to map an MX record to a HOST NAME, not mapping DNS to the DNS servers setup when a domain name was purchased, wrangling with DNS for e-mail and IIS when having to maintain the integrity of DNS for Active Directory, failing to setup rDNS [IN-ARPA] – all of these have a potential to disable any e-mail server's ability to send and receive e-mail properly.

SmarterMail users are exceptionally fortunate to have an incredible community of users who participate in the forums provided at:

<http://forums.smartertools.com/forums/smartermail.14/>

If the forums cannot provide everything you need, then the SmarterTools Knowledge Base is available for further research at: <http://portal.smartertools.com/KB/browse.aspx>

Remember, SmarterMail gives two free support tickets with the initial purchase of each product.

Those tickets can be used to open support cases with SmarterMail, and, if your trouble turns out to be a bug, the cost of the ticket is refunded back into your account. This is a HUGE benefit of using SmarterMail over some of the other products on the market.

Finally, if you are just setting up a new SmarterMail installation, you can always request support from one of the members of the forum. Simply click on the member's screen name and select the option to send a private message.

If I can be of service to you whether for problems you encounter with SmarterMail, DNS or other general networking issues, please do not hesitate to contact me using one of the links below.

Support Portal: <http://portal.chicagonettech.com>

Website: <http://www.chicagonettech.com>

E-Mail: bbarnes@chicagonettech.com

Skype: chicagonettech

Blog: <http://networkbastion.blogspot.com/>

Copyright © 2009 – 2013, Bruce Barnes, ChicagoNetTech Inc, All Rights Reserved
Compiled by [Bruce Barnes](#) | [ChicagoNetTech](#) | [ChicagoNetTech](#) on the [SmarterMail forums](#)

VERSION CONTROL:

20130317: 17 Mar 2013	<ul style="list-style-type: none">➤ Update to expand on antispam information, standards and include SmarterMail Versions 10.X and 11.X➤ Include information and documentation regarding extrapolation of “multi” responses into individual checks.➤ Include individual build data for each record for clarification.➤ Redo all images with graphics from Version 11.X
20120519: 19 May 2012:	<ul style="list-style-type: none">➤ Clarified record name for mail signing key➤ Added additional images for DKIM/DomainKeys➤ Added DOMAIN KEY POLICY record section➤ Added DMARC section➤ Added RESOURCES section
20120218: 18 Feb 2012:	➤ Original Version Published