Controlling spam: Advanced SMTP settings in Lotus Domino (Part 2)

Edmund Stanton

May 09, 2006
(First published October 11, 2004)

Find out how to control spam mail using the Server document and Notes.ini variables. Then preview the anti-spam controls in Lotus Notes/Domino 7 and see whatâ##s ahead. This article is part two in a series about Lotus Domino methods of spam control.

In the ongoing battle to control unwanted and unsolicited emails, corporations are spending millions, even billions, of dollars for technology to prevent spam mail from infiltrating their users' inboxes. While spam mail may no be preventable, Lotus Notes and Domino has been implementing measures that assist organizations in controlling it. In part one of this article series, we discussed the Configuration Settings document, server mail rules, and inbound SMTP commands and extensions. Each of these measures can help you to prevent unwanted email from reaching your users. In the final part of this series, we look at settings in the Server document and at Domino server Notes.ini variables that affect SMTP and the mail router. Last, we look ahead at Lotus Notes/Domino 7 anti-spam features, such as whitelists, server mail rule enhancements, and more.

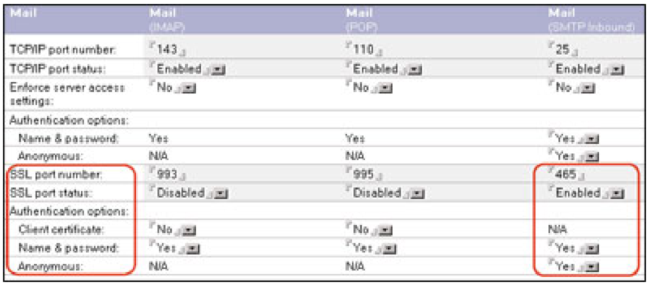
This article series is intended for experienced Domino administrators. If you have not already, read part one of this series.

Server document

In the previous article, we covered the Configuration Settings document inbound relay controls, DNS blacklist filters, and other SMTP controls. But the Configuration Settings document isn't the only document to help you control spam mail. The Server document SSL settings can also help.

SMTP sessions conducted over a standard TCP/IP channel are vulnerable to eavesdropping because the uuencoded transmission can be easily intercepted. To protect SMTP communications, servers can use transport-layer security (TLS), more commonly known as SSL encryption, to provide privacy and authentication. Enabling SSL is done through the Server document Ports - Internet Ports - Mail tab as shown in Figure 1.

Figure 1. Enabling SSL for SMTP Inbound



Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)
TCP/IP port number:	143	110	25
TCP/IP port status:	Enabled	Enabled	Enabled
Enforce server access settings:	No	No	No
Authentication options:			
Name & password:	Yes	Yes	Yes
Anonymous:	N/A	N/A	Yes
SSL port number:	993	995	465
SSL port status:	Disabled	Disabled	Enabled
Authentication options:			
Client certificate:	No	No	N/A
Name & password:	Yes	Yes	Yes
Anonymous:	N/A	N/A	Yes

Some servers support SSL for SMTP communications by sending and receiving SMTP traffic through the SSL port (port 465 by default) only. However, because this requires that both the sending and receiving servers support SMTP over SSL, this solution isn't always practical.

To provide SSL security for SMTP transfers over TCP/IP, Lotus Domino supports the use of negotiated SSL. In a negotiated SSL scheme, the sending and receiving hosts each use the SMTP STARTTLS extension, defined in RFC 2487 and RFC 3207, to signal their readiness to negotiate an SSL connection. The receiving server displays the STARTTLS keyword in response to the sending server's EHLO command. The sending server issues the STARTTLS command to request the creation of a secure connection. After the initial TLS handshake completes successfully, the two parties proceed to set up an SSL channel between them. Both the sending and receiving server must possess SSL certificates.

Above the SSL port information is also a setting called the "Enforce server access settings" field. When this field is enabled, access to the SMTP listener is controlled by the server access settings on the Security tab of the Server document. Users and servers that are not allowed to access the server cannot send mail to the SMTP port. For this option to be effective, you must enable authentication for the port.

Notes.ini variables

Along with configuring SMTP through a Notes GUI, some SMTP settings can be applied through server Notes.ini variables. The following section lists some Notes.ini variables that you can use to help prevent spam mail and to configure SMTP and Router restrictions. All the Notes.ini settings listed in this article apply to the Domino server only.

SMTPStrict821AddressSyntax=value

This variable lets you define whether or not the SMTP task requires addresses that appear in MAIL FROM commands or RCPT TO commands must conform to the 821 standard (must contain <>). Set this to 1 to enforce the 821 standard; the default setting of 0 does not enforce the standard.

SMTPGreeting=string

This variable lets you compose the text message that is sent to SMTP clients when they connect to the SMTP server. You must include the string "%s" within the message. (This string is replaced with the current date/time when the connection is made.) By default, the SMTPGreeting is "host-name ESMTP Service (Lotus Domino build-name) ready at %s".

SMTPStrict821LineSyntax=value

If you set this variable to 1, the SMTP task requires all protocol text be terminated by carriage return and line feed (CRLF) as defined by the 821 standard. If you set this variable to 0 (the default setting), the 821 standard is not enforced, and line feed (LF) is accepted as a line terminator.

SMTPNonStandardLineTermination=value
The SMTP listener task conforms to RFC 2821, requiring a carriage return and a line feed. You can change this functionality with the SMTPNonStandardLineTermination variable. If you set the variable to 0, the SMTP listener task requires a carriage return and line feed (CRLF). If you set it to 1, the SMTP listener task requires a carriage return (CR) or a line feed (LF).

SMTPNotesPort=portname
This variable forces SMTP to bind to a specific TCP/IP port other than the first port listed in the PORTs variable of the server's Notes.ini file, which is the default behavior. You may want to use this variable with a server that has multiple network interface cards.

SMTP_Config_Update_Interval=value
This variable allows you to define how frequently (in minutes) Domino checks the Configuration Settings document for updates. The default value is 2.

SMTPAllowConnectionsAnonymous=value
This determines how the SMTP task handles connections if authentication is required and populates the hosts in the "Allow connections only from the following SMTP internet hostnames/IP addresses" field. If you specify 0, the SMTP task requires authentication, and hosts in the "Allow connections only from the following SMTP internet hostnames/IP addresses" field are denied. If you specify 1, the SMTP task requires authentication, and hosts in the "Allow connections only from the following SMTP internet hostnames/IP addresses" field are exceptions that are allowed to connect.

SMTPTimeoutMultiplier=value
Each SMTP protocol exchange has a timeout wait value. If a client doesn't respond within this period, the connection terminates. You can increase the timeout period by defining a multiplier value with the SMTPTimeoutMultiplier variable. For example, if you set this to 5, all timeout periods are increased by a factor of 5. The default is 1.

RouterDSNForNULLReversePath=value
This variable lets you determine whether or not the Router returns delivery status notifications (DSNs) for messages received over SMTP with null RFC 821 reverse paths. By default, this is set to 0, which tells the Router not to return a failed DSN. In this case, the Router creates the nondelivery report, but marks it as DEAD. (You can later delete or release these messages.) If you set this variable to 1, the Router creates and sends the delivery status notification. In addition, if you set this variable to 2, the Router does not create a delivery status notification.

SMTPVerifySendersDomainTimeout=value
This variable lets you set the default timeout (in seconds) for SMTP Inbound Sender Control in the "Verify Sender's Domain in DNS" field. By default the timeout value is 30 seconds.

SMTPErrorLimit=value
This variable tells SMTP to drop a connection when the error count for that connection exceeds an administrator-defined number of errors. If SMTP sessions are opened by clients that fail to acknowledge a close command, this variable lets the session terminate. The default depends on available resources and the number of SMTP connections.

RouterDisableDSNRelayReports=value
The Router generates SMTP DSN Relay reports when it is unable to forward delivery confirmation requests to the next SMTP hop, including when the current Router has outbound DSN disabled in the Configuration Settings document. To disable SMTP DSN Relay reports, set the variable to 1. The default is 0, letting the Router send a relay report if outbound DSN has been disabled.

RouterDisableMailToGroups=value
This variable determines whether the Router allows or denies mail addressed to a group. The default value of 0 allows the Router to expand groups and forward email to group members. To keep the Router from expanding groups, set this variable to 1. The Router returns the message as a failure report to the sender, stating that the message was rejected for policy reasons.

SMTPLookupNoDircat=value
This variable determines whether or not SMTP uses directory catalog lookups. This prevents users listed in the directory from receiving inbound Internet mail on this server. The default value of 0 enables the Router to use any of the Extended Directory Catalogs referenced in its configuration. If you set this variable to 1, the Router cannot use any of the Extended Directory Catalogs referenced in its configuration when doing lookups for inbound Internet mail.

SMTPMaxCommandLength=value
This variable sets the maximum number of characters the SMTP task accepts. The default is 1,200 characters.

SMTPMaxForRecipients=value
This variable determines how many addresses can be added when the SMTP task adds received headers to messages received. The default is based on available resources.

SMTPMaxSessions=value
This variable specifies the number of allowed inbound SMTP connections. After this value has been reached, Domino returns an error 421 message. The default value is based on available resources.

SMTPVerifyAuthenticatedSender=value
This variable lets you determine if mail sent during an authenticated SMTP session is issued from that user's Internet address. The default value of 0 instructs Domino not to check the Internet address of authenticated SMTP sessions. If you set this variable to 1, Domino determines if mail sent during an authenticated SMTP session is issued from that user's Internet address.

SMTPSmartHostAllDisableGroupExpansion=value

This variable disables group expansion when Smarthost is enabled for all recipients in the local Internet domain. If you set it to 0, group expansion occurs when Smarthost is enabled for all local Internet domain recipients. If you set the value to 1, it disables group expansion when Smarthost is enabled for all local Internet domain recipients. The default is 0.

SMTPNoVersionInRcvdHdr=value
When you set this variable to 1, it prevents Domino server product information from being disclosed in the SMTP Received headers. The default is 0.

SMTPMaxRecipientCount=value
This variable can control the number of recipients during the SMTP protocol RCPT TO command. After that value has been reached, Domino will issue an error 552 message. The default is based on available resources.

SMTPTranslateAddresses=value
When messages are received through SMTP by the SMTP task, no change is made to any of the addresses. Some sites may prefer to have the Internet addresses of the local Notes users converted to Notes addresses (hierarchical). To convert the addresses, set this variable to one of the following values: 0 - (default) No translation; 1 - Translate only the from item; or 2 - Translate all address items.

SMTPTranslateLookupFullThenLocal=value
If you have the previous variable SMTPTranslateAddresses set to either 1 or 2, you can use this variable to override the Configuration Setting document for Address lookup. To override the Configuration Setting document, set SMTPTranslateLookupFullThenLocal to 1. When you do, Lotus Domino translates the full name then local part. The default is 0.

SMTPTranslateAddressLookup=value
If you have the variable SMTPTranslateAddresses set to either 1 or 2, you can use this variable to perform a lookup even if the address doesn't appear to be a local address. Set SMTPTranslateAddressLookup to 1 to enable it to perform an address lookup. The default is 0.

SMTPTranslateAddressesPreserve822=value
This variable preserves the original Internet address in Inetxxx items. Lotus Notes/Domino 6.5.2 and later maintain Inet items in the RFC821 form, which is the preferred form for Inet items. Set this variable to 1 to revert to previous behavior and to preserve any RFC822 addresses translated in the Inetxxx items.

SMTPRelayHostsandDomain=value
If you set this variable to 1, entries in the Deny fields of the SMTP inbound relay controls take precedence over entries in the Allow fields in the event of a conflict. The default is 0.

SMTP_RIGHT_DOT_NEVER_NOTESDOMAIN=value
When set to 1, SMTP_RIGHT_DOT_NEVER_NOTESDOMAIN corrects a problem when addressing messages to user@notes.domain.com, where hostname notes matches the Notes domain name. It prevents the router from attempting to delivery the message locally.

RouterUseFromAsSMTPOriginator=value
This variable causes the RFC821 reverse path MAIL FROM command to be based on the value in the From field when set to 1. The default is 0.

RouterLanguageVisibleNDRStatus=value
If you have language packs installed, you can use this variable to enable translation of non-delivery messages. Set this value to 1 to enable this feature. Lotus Domino will translate certain English messages returned in NDRs by the router.

Preview of Lotus Domino 7

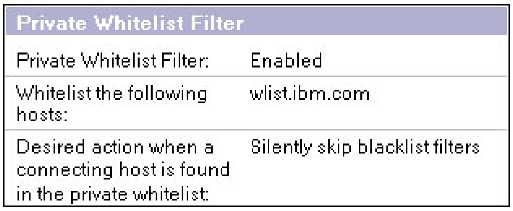
This section describes some new features that are in Lotus Domino 7. The features described below reflect the ones available in the Beta 2 release of Lotus Notes and Domino 7. However, these features may not appear in the final release of these products. Also, the user interface for these features is subject to change, so the illustrations in this article may not exactly match what appears on your screen.

DNS whitelist filters

Lotus Domino 7 has extended its spam control to include DNS whitelist filters. Whitelists allow messages from specified domains to be received. IBM supports both private blacklist and whitelist filters. With these new configuration settings, it is important to understand how you can reduce spam and to know the order that Domino will check when blacklist and whitelist filters are enabled.

If you enable private whitelist filters, when Domino receives an SMTP connection, it compares the IP address/host name against this list. The field "Whitelist the following hosts" should be used to enter the IP addresses or host names of systems that you want to whitelist. You can also use an asterisk (*) as a wild card. Members of the private whitelist are still subjected to connection, relay, sender, and recipient controls. Being whitelisted does not guarantee that the message will be delivered to the recipient.

Figure 2. Private Whitelist Filters



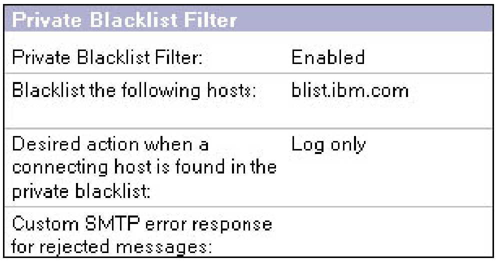
Private Whitelist Filter	
Private Whitelist Filter:	Enabled
Whitelist the following hosts:	wlist.ibm.com
Desired action when a connecting host is found in the private whitelist:	Silently skip blacklist filters

You can also set the "Desired action when a connecting host is found in the private whitelist" field. You can choose to skip all the blacklist filters to avoid any excess lookups. When this action is configured, Domino does not record any additional logging. Prior to the introduction of private whitelist filters, to exclude a host from blacklist filter processing, you had to define the client's mail server as a relay exception.

Another option is to log the connecting IP address/host name that was found in the private whitelist. The last option is to log and tag the message. Tagging the message adds the note $DNSWLSite to the message, which can be used to further filter the message.

If the connecting host was not listed in the private whitelist, Domino searches private blacklist filters if enabled. Domino compares the IP address/host name with this list. You also have the option to log the message or log and tag the message with the note $DNSBLSite. There is a third option to log and reject the message. When configured, if Domino finds that a connecting host is on the private blacklist, it rejects the connection and returns a custom SMTP error message to the host.

Figure 3. Private Blacklist Filter



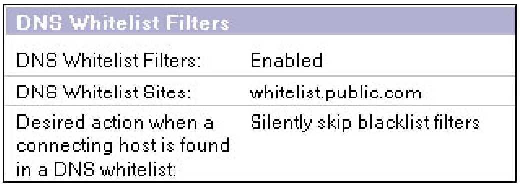
Private Blacklist Filter

Private Blacklist Filter:	Enabled
Blacklist the following hosts:	blist.ibm.com
Desired action when a connecting host is found in the private blacklist:	Log only
Custom SMTP error response for rejected messages:	

After Domino has checked the private filters, it compares the IP address against DNS filters. Administrators should use DNS whitelist filters as a means to help identify legitimate email. The Bonded Sender Program proposed by IronPort Systems allows originators of legitimate email to post a financial bond to ensure the integrity of their email campaign. Recipients who feel that they have received an unsolicited email from a bonded sender can complain to their ISP, enterprise, or IronPort, and a financial charge is debited from the bond. This market-based mechanism allows email senders to ensure their message gets to their end user and provides corporate IT managers and ISPs with an objective way to ensure only unwanted messages get blocked. The Bonded Sender Program operates as a DNS whitelist. There are other programs similar to the Bonded Sender Program that are outside the scope of this article. You can search the Web for additional programs.

If DNS whitelist filters are enabled, as shown in Figure 4, Domino compares the IP address/host name with the DNS whitelist sites listed. You can also specify the action when a connecting host is found in the DNS whitelist. You can choose to skip all the blacklist filters to avoid any excess lookups. When this action is configured, Domino does not record any additional logging.

Figure 4. DNS Whitelist Filters

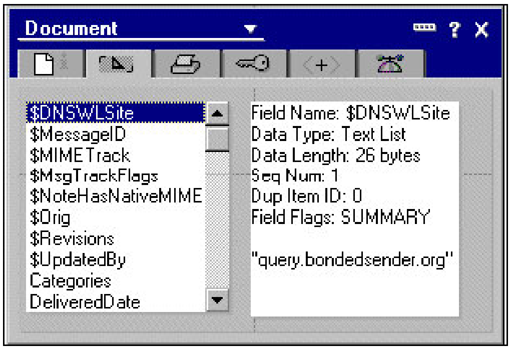


DNS Whitelist Filters

DNS Whitelist Filters:	Enabled
DNS Whitelist Sites:	whitelist.public.com
Desired action when a connecting host is found in a DNS whitelist:	Silently skip blacklist filters

You also have the option to log the connecting IP address/host name that was found in the private whitelist. The last option is to log and tag the message. Tagging the message adds the note $DNSWLSite to the message which can be used to further filter the message.

Figure 5. Document properties for $DNSWLSite



$DNSWLSite
$MessageID
$MIMETrack
$MsgTrackFlags
$NoteHasNativeMIME
$Orig
$Revisions
$UpdatedBy
Categories
DeliveredDate

Field Name: $DNSWLSite
Data Type: Text List
Data Length: 26 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY

"query.bondedsender.org"

The SMTP task maintains statistics to keep a cumulative count of the total number of hits (SMTP.DNSWL.TotalHits) as well as per-whitelist site hits (SMTP.DNSWL.<WhitelistSite>.Hits). The statistics are part of the SMTP stat package and can be viewed through either the Domino Administrator client or server console via the show stat SMTP command. You can further expand the statistics to learn the number of times a given IP address is found in one of the configured DNSWLs (SMTP.DNSWL.<WhitelistSite>.[IP address].Hits). To collect the expanded information, enable the Notes.ini variable:

```
SMTPExpandDNSWLStats=value
```

Use this setting to generate DNS and private whitelist filter statistics for each connecting host found in a DNS or private blacklist site. If you set this variable to 0, the SMTP server does not generate host specific DNS/private blacklist filter statistics. If you set this variable to 1, the SMTP server generates host specific DNS/private blacklist filter statistics that indicate the total number of hits per DNSWL site, per connecting host's IP address.

In the absence of this setting, the SMTP task maintains statistics that track the total number of connecting hosts that were found on the combined DNSBL of all sites combined, as well as how many were found on the DNSBL of each configured site.

Server mail rules enhancements

Lotus Domino 7 has also made some new enhancements for configuring server mail rules. IBM has added two new conditions to search for to identify specific mail messages. Lotus Domino 7 has the ability to filter mail based on blacklist tags and whitelist tags. When a connecting host is found in a blacklist or whitelist, there is an option to tag the messages. Now you can quarantine messages that have a blacklist tag or journal messages that have a whitelist tag.

A new action has also been added for configuring server mail rules. You can specify an action of stop processing. The stop processing action stops the processing of all rules that follow the rule containing the stop processing action. You can use the stop processing action alone--that is, as the only action in a server mail rule--or you can use it with another action in a rule. This is especially useful when more than one rule could apply to a message, but you want execution of mail rules to stop after the first action is executed.

Support for IPv6 for SMTP

Lotus Domino 7 supports IPv6 for SMTP. Support for IPv6 by hardware and operating system suppliers and the Internet is still in the early stages. Moving to the IPv6 standard is a gradual process for most organizations. IPv6 is an emerging standard. Vendors who have implemented (or are implementing) IPv6 have done so in varied ways. How you enable and configure IPv6 in your enterprise depends on the client and server platforms you are using. To enable IPv6, add this setting to the server's Notes.ini file:

```
TCP_EnableIPV6=value
```

You can enable support for IPv6 on a Domino server that runs the IMAP, POP3, SMTP, LDAP, or HTTP service. If you set this variable to 0, Domino uses the IPv4 standard. Set the variable to 1 to enable Domino to use the IPv6 standard. By default, this setting is set to 0.

Even if you enable IPv6 in Lotus Domino, it can continue to connect to IP addresses that use the IPv4 standard. AAAA records store IPv6 addresses in DNS. After you enable IPv6 on a Domino server and add the server's AAAA record to DNS, another IPv6-enabled Domino server can connect to it only over IPv6. Servers that don't support IPv6 can run Lotus Domino with IPv6 support disabled, which is the default. These servers can successfully connect to IPv6-enabled Domino servers only if the DNS for the IPv6 servers contain A records.

Domino Domain Monitoring

Domino Domain Monitoring (DDM), new in Lotus Domino 7, lets you view the status of multiple servers across more than one domain. DDM uses probes that you configure to monitor server activity. One of those probes is a mail probe that monitors local mail routing. It sends a message to a known destination and verifies its delivery. If too much mail is pending or if mail fails to reach its destination, DDM can send you an alert. You can also use an SMTP probe to verify mail delivery to an SMTP recipient. DDM can issue a delivery status notification report. The Event Resolution Center database (Ddm.nsf) consolidates information gathered by the probes in a single repository.

For more information about Domino Domain Monitoring and other new features in Lotus Notes/ Domino 7, see the developerWorks: Lotus article, "New features in Notes/Domino 7."

New Notes.ini variables

Lotus Domino 7 is also introducing some new Notes.ini variable to help prevent spam.

SMTPDenyMailToGroups=value
This variable requires that you have the option "Verify that local domain recipient exist in the Domino Directory" enabled. If you set this variable to 1, all external hosts receive a permanent error after the RCPT TO command when mail is addressed to a group. If you set this to 2, all connecting hosts receive a permanent error after the RCPT TO command when mail is addressed to a group. The default value is 0.

SMTPDenyNotUniqueRCPT=value

This variable requires that you have the option "Verify that local domain recipient exist in the Domino Directory" enabled. If you set this variable to 1, the SMTP task will not except any recipient name that is not unique. The default is 0.

What's coming

IBM research is also working on additional anti-spam technologies that are not in the current releases of Lotus Domino. One such technology framework known as SpamGuru allows one or more of these technologies to be combined to filter mail. One of the technologies being developed in this framework is a Bayesian spam filter. Bayesian filters use a statistical method to determine if a particular message is spam or not. By comparing features of a message with a corpus of previous good and spam messages, the probability of a message being spam is calculated and represented by a "score" that can be used to potentially alter the disposition of the message.

Bayesian filters continue to learn about new spam through a training process. The corpus of good/spam messages can continuously be updated to affect future calculations. This learning is accomplished by allowing users (mail recipients) to provide input to the system by "voting" a particular message as either good or spam. The number of votes for messages with a particular feature is considered during future calculations, allowing the filter to dynamically adapt to new spam content and the users' definition of spam.

See "SpamGuru: An Enterprise Anti-Spam Filtering System" for an overview of the SpamGuru architecture and how Lotus Domino can become an adaptive spam filter. Additional reading material can also be found at IBM Research.

NOTE: Currently IBM has no scheduled timeline for integrating SpamGuru technologies and Lotus Notes and Domino.

Summary

IBM has researched and configured many settings to prevent spam in Lotus Domino 6 and 7. Most users do not understand why or how they are receiving spam messages, which is why preventing spam messages from getting in the front door will ease the amount of time spent by the users managing these messages. IBM continues to enhance Lotus Domino to stay up-to-date with the latest anti-spam techniques.

Related topics

- Read Part 1 of this article series.
- For more about anti-spam controls, see the *LDD Today* articles, "Preventing spam mail in Notes/Domino 6" and "Notes spam mail filtering."
- You may also want to refer to the IBM Redbook, *Lotus Domino 6 spam Survival Guide*.