Understanding SMTP authentication and securing your IBM Lotus Domino 8 server from spam

Shrikant Jamkhandi
IBM Software Group
Senior Software Engineer
Pune, India

September 2009

Summary: Learn how the SMTP protocol and SMTP authentication process works, how to verify whether the IBM® Lotus® Domino® 8 server is open relay, and how to make Lotus Domino obey the SMTP authentication for securing the server from spammers.

Table of Contents

1 Introduction

Simple Mail Transfer Protocol (SMTP) is widely used standard e-mail protocol on the Internet and part of the TCP/IP protocol suite. SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail. SMTP uses TCP port 25.

The primary purpose of SMTP is to transfer email between mail servers. However, it is critical for email clients as well. In order to send email, the client sends the message to an outgoing mail server, which in turn contacts the destination mail server for delivery. For this reason, it is necessary to specify an SMTP server when configuring an email client.

One important point to make about the SMTP protocol is that by default it does not require authentication. This allows anyone on the Internet to send email to anyone else or even to large groups of people. It is this characteristic of SMTP that makes junk email or spam possible.

2 Overview of the SMTP process

When an SMTP client has a message to transmit, it establishes a two-way transmission channel to an SMTP server. The responsibility of an SMTP client is to transfer mail messages to one or more SMTP servers.

Once the transmission channel is established and initial handshaking completed, the SMTP client normally initiates a mail transaction. Such a transaction consists of a series of commands to specify the originator and destination of the mail and the transmission of the message content (including any headers or other structure) itself.

The server responds to each command with a reply; replies may indicate that the command was accepted, that additional commands are expected, or that a temporary or permanent error condition exists. Once a given mail message has been transmitted, the client may either request that the connection be shut down or may initiate other mail transactions.

Basic commands SMTP defines a small required command set, with several optional commands included for convenience purposes. The minimal set required for an SMTP sending client is:

HELO: Greet the mail server. Used once per session, at the beginning of the session.

MAIL FROM: <source email address>. Announce who the sender is. Used once per mail, before specifying any recipients for each mail, or after a RSET.

RCPT TO: < destination email address >. This identifies the recipient of the email message. Multiple recipients are allowed, and each must have its own **RCPT TO:** entered immediately after a **MAIL FROM:**

SIZE=numberofbytes. The size command tells the remote send-mail system the size of the attached message in bytes.

DATA. Starts mail entry mode. Everything entered on the lines following DATA is treated as the body of the message and is sent to the recipients. The DATA terminates with a "**.**" (period) on a

line by itself. A mail message may be queued or sent immediately when the "**.**" is entered; however, it cannot be reset at this stage.

RSET. Reset the state of the current transaction. The MAIL FROM: and RCPT TO: for the current transaction are cleared.

QUIT. End the session. Commit Message and Close Channel.

2.1 SMTP procedures

There are three steps for SMTP mail transactions:

1. The transaction is started with a MAIL command, which gives the sender identification. If accepted, the receiver-SMTP returns a 250 OK reply.

2. A series of one or more RCPT commands follows, which give the receiver information. If accepted, the receiver-SMTP returns a 250 OK reply and stores the forward-path. If the recipient is unknown, the receiver-SMTP returns a 550 Failure reply.

3. Then, a DATA command gives the mail data. If accepted, the receiver-SMTP returns a 354 Intermediate reply and considers all succeeding lines to be the message text. Finally, the end-of-mail data indicator confirms the transaction. When the end of text is received and stored, the SMTP-receiver sends a 250 OK reply.

Example of the SMTP procedure

This SMTP example shows mail sent by Smith at host Alpha.ARPA to Jones, Green, and Brown at host Beta.ARPA. Here we assume that host Alpha contacts host Beta directly.

S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK
S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK
S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here
S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK
S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

The mail has been accepted for Jones and Brown. Green did not have a mailbox at host Beta.

3 Overview of SMTP authentication

SMTP is the widely used protocol for sending email from a mail client such as Lotus Notes®, Domino Web Access, Microsoft® Outlook Express, and Microsoft Outlook. The SMTP protocol listens on port 25 or, more precisely, the SMTP server listens for client connections on port 25.

Originally, SMTP was anonymous as to its origins, with authentication implemented during its evolution. SMTP servers were typically internal to an organization, receiving mail that was destined for the organization from the outside. These servers were also responsible for relaying messages from the organization to the outside.

With time SMTP servers evolved to become message submission agents for email user agents, some of which were now relaying mail from the outside of an organization; for instance when a company mobile worker wants to send email while on a trip, using the corporate SMTP server.

This meant that the SMTP protocol had to include specific rules and methods for relaying mail and authenticating users to prevent abuses such as spam relaying.

SMTP Authentication is a scheme introduced in 1999 by J. Myers of Netscape Communications. It was finally released as RFC 2554 ("SMTP Service Extension for Authentication"), which is obsolete and currently defined in RFC 4954.

Most modern SMTP implementations support SMTP Authentication, and most Mail User Agents (MUAs), which includes the SMTP client, make SMTP Authentication available (for example, Outlook, Eudora, Netscape, and Mozilla.)

SMTP Authentication is advertised by the SMTP Authentication server and requires a client to authenticate and that both parties mutually accept and support the chosen authentication procedure.

With SMTP Authentication, originally invented as a Host-to-Host protocol, *users* must identify themselves and after successful authentication, reception/transmission of their emails is granted.

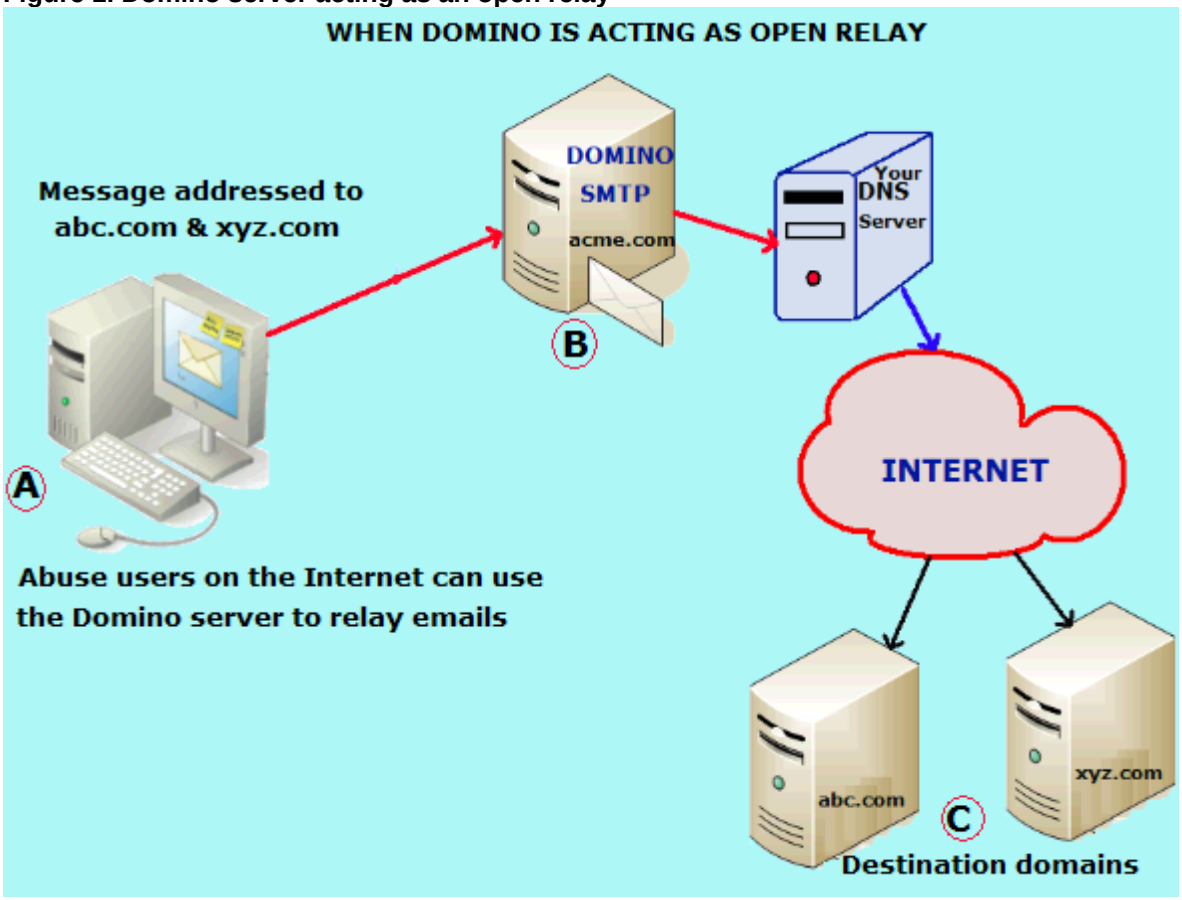
3.1 Open relay

An open mail relay is an SMTP server configured in such a way that it allows anyone on the Internet to send email through it, not just mail destined to or originating from known users (see figure 1).

Spammers are able to locate accessible open-relay servers by using automated tools that are readily available on the Internet. By relaying mail through several open-relay mail servers at the same time, they are able to quickly flood the Internet with large amounts of junk mail before being detected.

Spammers who use third-party mail relays not only damage the reputation of those whose servers they’ve hijacked, clog networks with junk mail, and frequently crash servers, they also are guilty of breaking the law because technically they are stealing services.

Figure 1. Domino server acting as an open relay



The figure illustrates what happens when abusers exploit your Domino server as an open relay:

- Host A is the abuser's system and has no relationship with Host B, your Domino SMTP server, which will be used as a relay.
- A message arriving to unsecured Host B is relayed out on behalf of the (hit-and-run) abuser directly to the Destination Domains C, abc.com and xyz.com.
- Understandably, people receiving such unsolicited junk get annoyed and take action against the abuser's and the open-relay servers.

In all cases, if your system has the misfortune of being a globally reachable open-relay, then your system resources are in danger of becoming abused.

3.2 SMTP Authentication

SMTP Authentication (SMTP-AUTH) is generally a security improvement over unauthenticated SMTP; however, it can also introduce a weakness. If authenticated users are allowed to submit messages from IP addresses, and unauthenticated users are not, then an attacker who manages to get the credentials of one user's account is then able to use the authenticated server as an open mail relay.

Therefore, every user's password now becomes a key to the mail system's security. A good password policy can effectively prevent such an attack.

Having SMTP Authentication in place on your mail server has a number of benefits. It can add another layer of security to sendmail, and it provides mobile users who switch hosts with the ability to use the same mail server without needing to reconfigure their mail client settings each time.

The SMTP-AUTH extension provides an access control mechanism. It consists of an authentication step through which the client effectively logs in to the mail server during the process of sending mail. Servers that support SMTP-AUTH can usually be configured to require clients to use this extension, ensuring that the true identity of the sender is known. The SMTP-AUTH extension is defined in RFC 4954.

SMTP-AUTH can be used to let legitimate users relay mail while denying relay service to unauthorized users, such as spammers. It does not necessarily guarantee the authenticity of either the SMTP envelope sender or the RFC 2822 "From:" header.

For example, spoofing, in which a sender masquerades as someone else, is still possible with SMTP-AUTH, unless the server is configured to limit message from-addresses to only addresses for which the AUTH'ed user is authorized.

The SMTP-AUTH extension also allows one mail server to indicate to another that the sender has been authenticated when relaying mail. Generally this requires the recipient server to trust the sending server, meaning that this aspect of SMTP-AUTH is rarely used on the Internet. The recipient of an email message cannot tell whether the sender was authenticated, so use of SMTP-AUTH is at best only a partial solution to the spam problem.

Proper use and checking of RFC 4408 Sender Policy Frame (SPF) records helps, as does the use of the RFC 4408 SUBMISSION protocol for mail submission from the user agent (as opposed to mail transport from foreign mail servers).

4 Determining whether Lotus Domino is open relay or closed relay

You can use the TELNET utility from the Command Prompt window to determine whether your Domino server is open relay or closed relay. To do this, follow these steps:

1. Open the Command Prompt window on the operating system.

2. Type the command below and press Enter:

   Telnet "Fully qualified hostname/IP address of the domino server" "SMTP port number"
   (For example, Telnet Domino-704.acme.com 25 OR Telnet 192.168.1.4 25)

3. Telnet windows will open as shown in figures 2 and 3.

Figure 2. Telnet window for 704.acme.com

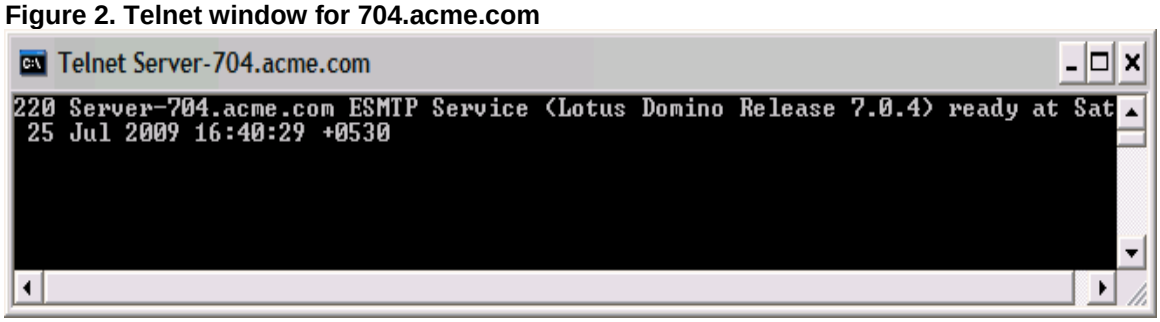
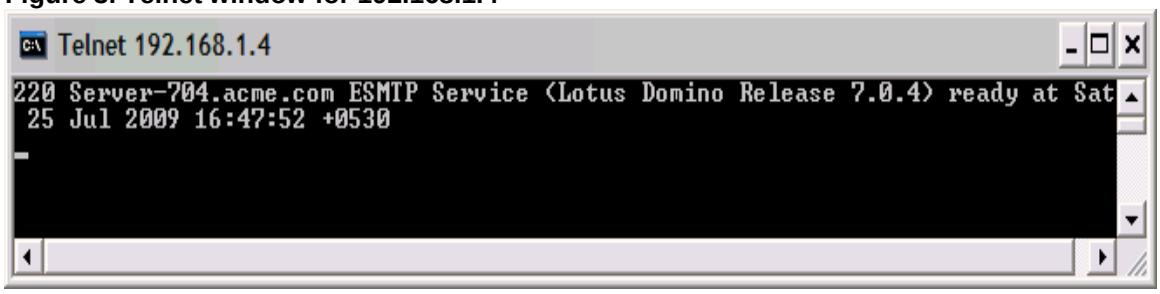


Figure 3. Telnet window for 192.168.1.4



4. Now type the commands as indicated below:

   220 Server-704.acme.com ESMTP Service (Lotus Domino Release 7.0.4) ready at Sat, 25 Jul 2009 16:51:40 +0530
   helo abc.com **-> Press Enter key**
   250 Server-704.acme.com Hello abc.com ([10.10.1.8]), pleased to meet you
   mail from:bogus.user@bogus.com **-> Press Enter**
   250 bogus.user@bogus.com... Sender OK
   rcpt to:john.doe@ibm.com **-> Press Enter**
   250 john.doe@ibm.com... Recipient OK

"Recipient OK" means your Domino server is open relay, and anyone can relay email to the Internet using your Domino SMTP server.

5 Making Lotus Domino a closed-relay server

To protect SMTP servers from unauthorized relaying, Lotus Domino provides inbound relay controls used to define the hosts to which and from which a server can relay messages. The Domino SMTP listener denies requests to relay messages to or from unauthorized hosts.

5.1 Setting inbound relay controls

To set inbound relay controls, follow these steps:

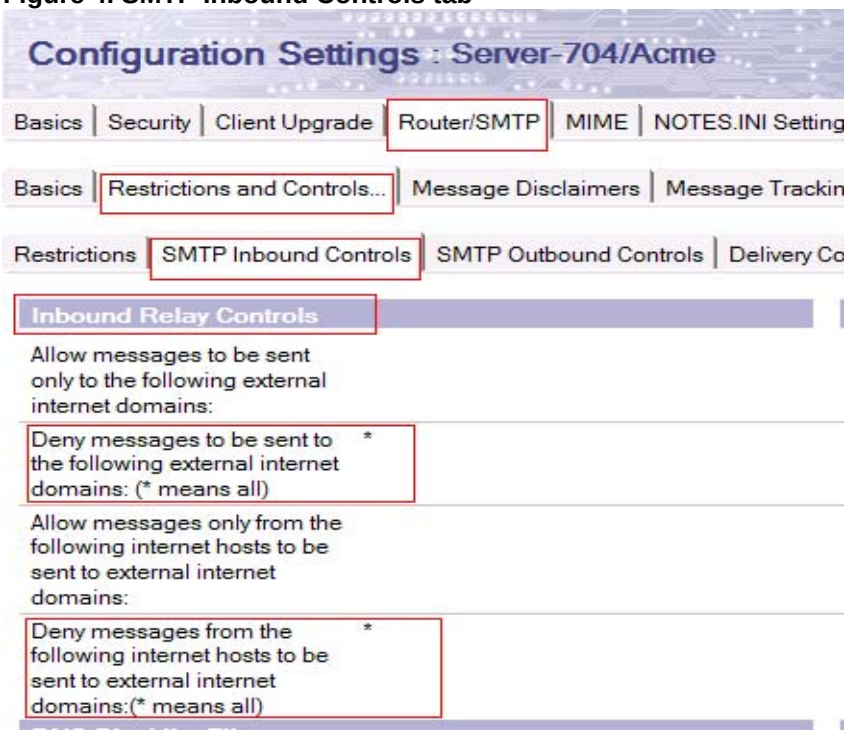
1. Make sure you already have a Configuration Settings document for the SMTP server to be configured.

2. From the Domino Administrator, click the Configuration tab and expand the Messaging section.

3. Click Configurations, and select the Configuration Settings document for the mail server(s) you want to administer; click Edit Configuration.

4. Select the Router/SMTP > Restrictions and Controls > SMTP Inbound Controls tabs (see figure 4).

Figure 4. SMTP Inbound Controls tab



5. Set the following fields to an asterisk (*):

   - Deny messages to be sent to the following external Internet domains
   - Deny messages from the following Internet hosts to be sent to external Internet domains

6. Click “Save and Close” to save the changes.

7. Issue the commands below on the server console, for the changes to take effect immediately; otherwise, the routing table will update the changes after 5 minutes.

   Tell router update config (updates the routing tables)
   Tell SMTP update config (updates SMTP tables)

Deny messages to be sent to the following external Internet domains. This field specifies the Internet domains to which Lotus Domino will not relay messages. An asterisk (*) in this field prevents the Domino server from relaying messages to any external Internet domain.

Deny messages from the following Internet hosts to be sent to external Internet domains. This field specifies the hosts or domains that the Domino SMTP service does not allow to relay outbound Internet mail.

If this field contains valid entries, Lotus Domino denies message relays from servers matching those entries and allows message relays from all other servers. You can specify individual host names or a group name. An asterisk (*) in this field prevents the Domino server from relaying messages from any host subject to the relay controls.

So now, if you telnet to your Domino SMTP server and then attempt to relay email to the Internet, you'll receive the message "554 Relay rejected for policy reasons":

220 Server-704.acme.com ESMTP Service (Lotus Domino Release 7.0.4) ready at Sat, 25 Jul 2009 16:51:40 +0530
helo abc.com **-> Press Enter key**
250 Server-704.acme.com Hello abc.com ([10.10.1.8]), pleased to meet you
mail from:bogus.user@bogus.com **-> Press Enter**
250 bogus.user@bogus.com... Sender OK
rcpt to:john.doe@in.ibm.com **-> Press Enter**
554 Relay rejected for policy reasons.

6 Enabling SMTP Authentication on the Domino server

You can use SMTP sender authentication to ensure that the sender of a message is a legitimate user of an SMTP server. SMTP sender authentication requires an account name and password for the destination SMTP server. The account name you use must be an account on the relay host SMTP server to which a specific Domino server routes messages.

The purpose of SMTP sender authentication is to authenticate the connection between a Domino router and an SMTP server. Use this feature with SMTP servers that do not allow Anonymous connections, or with SMTP servers that allow both authenticated and non-authenticated connections.

There are two scenarios in configuring the SMTP-AUTH on the Domino server, depending on whether or not it uses an Internet Site document. Let's now examine these two scenarios.

6.1 Configuring SMTP-AUTH options on a server that does NOT use an Internet Site document

On Domino servers that do not use Internet Site documents, the SMTP service obtains port authentication settings from the Server document, to honor the SMTP ports access restrictions.

Changing the default port number

By default, after you enable the SMTP task, it "listens" for client connections on TCP/IP port 25 on the Domino server. The default SMTP SSL port is port 465. In some cases—for example, on partitioned servers—you might need to specify a port number other than the default, to avoid conflicts.

You might also need to change the default port to a nonstandard port number, to "hide" it from clients attempting to connect to the default port, or if another application uses the default port on the server.

Disabling the SMTP Inbound TCP/IP port or SSL port prevents other servers from accessing the SMTP Listener on that port.

NOTE: On servers with multiple TCP/IP ports, by default the SMTP service uses the port listed first in the Note.ini file as the preferred path. You can configure the service to use a different port, if desired.

Changing the default SMTP greeting

You can modify the default reply that the SMTP service sends in response to a connecting host. By default, the Domino SMTP server reveals its host name and software version to connecting clients.

For security reasons, you can change the default greeting so that the server does not disclose essential information. Use the Notes.ini variable SMTPGreeting to customize the SMTP service greeting.

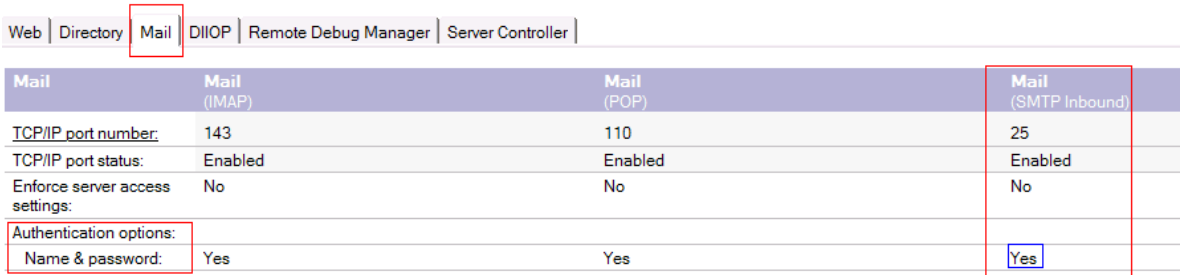
To change inbound SMTP TCP/IP port settings:

1. From the Domino Administrator, click the Configuration tab and open the Server document for the server that runs the SMTP service.

2. Select the Ports > Internet Ports > Mail tabs.

3. In the Mail (SMTP Inbound) column, set the “Authentication options: Name & password” field to “Yes” (see figure 5). Click Save & Close.

Figure 5. SMTP Inbound authentication options



4. Restart the SMTP task on the Domino server, for the changes to take effect, by issuing the command “**Restart Task SMTP.”**

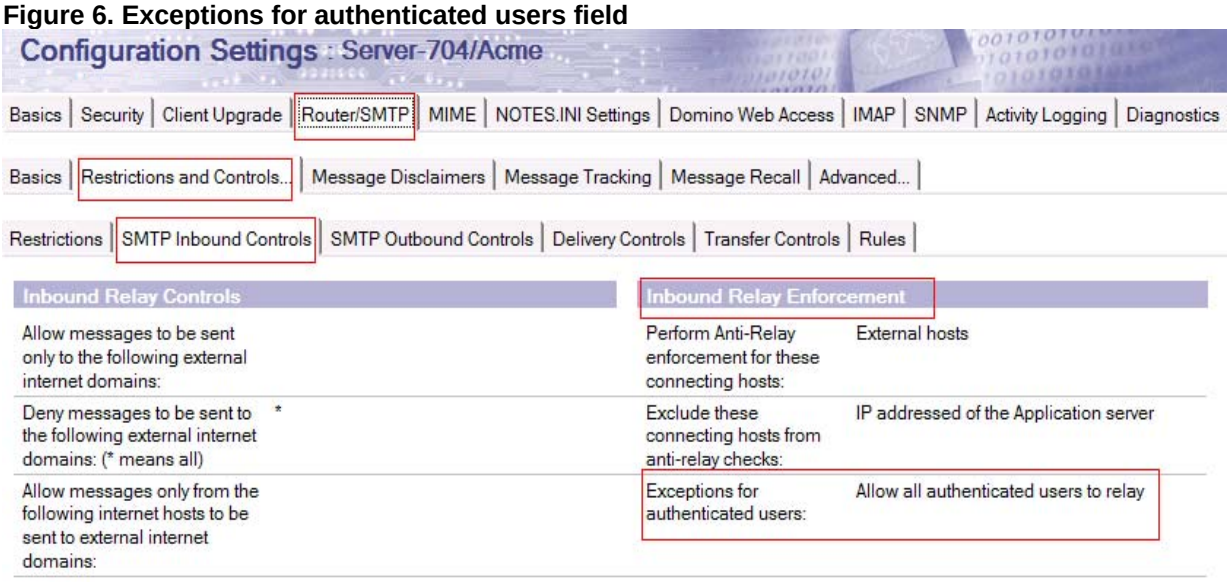
5. Again from the Domino Administrator, click the Configuration tab and expand the Messaging section; click Configurations.

6. Select the Configuration Settings document for the SMTP mail server(s) you want to administer and click Edit Configuration.

7. Select the Router/SMTP > Restrictions and Controls > SMTP Inbound Controls tabs.

8. In the Inbound Relay Enforcement section (see figure 6) make sure the field “Exceptions for authenticated users” is set to “Allow all authenticated users to relay”.

Figure 6. Exceptions for authenticated users field



NOTE: The “Perform Anti-relay enforcement for these connecting hosts” field has the following three options, so make sure you select the proper one:

External hosts (default). The server applies the inbound relay controls only to hosts that connect to it from outside the local Internet domain. Hosts in the local Internet domain are exempt from anti-relay restrictions. The local Internet domain is defined by either a Global Domain document, if one exists, or as the Internet domain of the host server.

All connecting hosts. The server applies the inbound relay controls to all hosts attempting to relay mail to external Internet domains.

None. The server ignores the settings in the inbound relay controls. All hosts can always relay.

If you want to enforce only for external hosts, then leave the default External host setting. If you want to enforce for internal as well as external, then select the All connecting hosts option.

Your Domino server should now be enabled with SMTP Inbound authentication, so that only authenticated users can relay email through it. To verify this, you can perform the following steps:

1. Open the Command Prompt window on the operating system.

2. Type the command below and press Enter:

Telnet “Fully qualified hostname/IP address of the domino server” “SMTP port number”
For example, Telnet Domino-704.acme.com 25 Press Enter
Telnet 192.168.1.4 25 Press Enter

3. The Telnet window opens for your Domino server.

4. Type the command **ehlo abc.com;** you will see **250-AUTH LOGIN,** as shown below:

220 Server-704.acme.com ESMTP Service (Lotus Domino Release 7.0.4) ready at Sat, 25 Jul 2009 16:55:40 +0530
ehlo abc.com **-> Press Enter key**
250 Server-704.acme.com Hello abc.com ([10.10.1.8]), pleased to meet you
250-HELP
250-AUTH LOGIN
250-SIZE
250 PIPELINING

6.2 Configuring SMTP-AUTH options on servers that use Internet Site documents

On Domino servers that use Internet Site documents, the SMTP service obtains port authentication settings from the Security tab of the SMTP Inbound Site document, rather than from the Server document.

As a result, when Internet Site documents are used, you cannot use the Server document to configure TCP/IP and SSL authentication settings for the SMTP port. Settings in the Server document do, however, provide the port numbers and status for the SMTP TCP/IP and SSL ports, as well as enable the SMTP ports to honor server access restrictions.

To determine whether the use of Internet Site documents is enabled for a server, on the Basics tab of the Server document, check the value of the field "Load Internet configurations from Server\Internet Sites documents." If this field is set to "Enabled," the server uses Internet Site documents to configure all of its Internet protocols (SMTP, IMAP, POP3, and so forth).

If the server uses Internet Site documents, then you must use Site documents to configure all Internet protocols on the server. If an SMTP Site document is not present in the Domino Directory, or the authentication options in a configured SMTP Site document are set to No, users cannot connect to the SMTP service.

In either case, SMTP clients receive the following error when attempting to connect to the SMTP service: “This site is not enabled on the server.”

Creating Inbound SMTP Site documents and enabling SMTP-AUTH

To do this:

1. From the Domino Administrator, click the Configuration tab and expand the Web section.

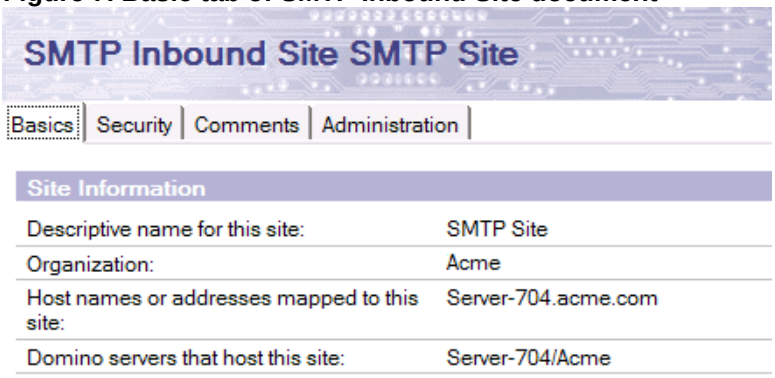
2. Choose Internet Sites.

3. Click “Add Internet Site” and select the SMTP Inbound option. A new SMTP Inbound document opens.

4. Complete the following fields in the Basics tab with your information (see figure 7):

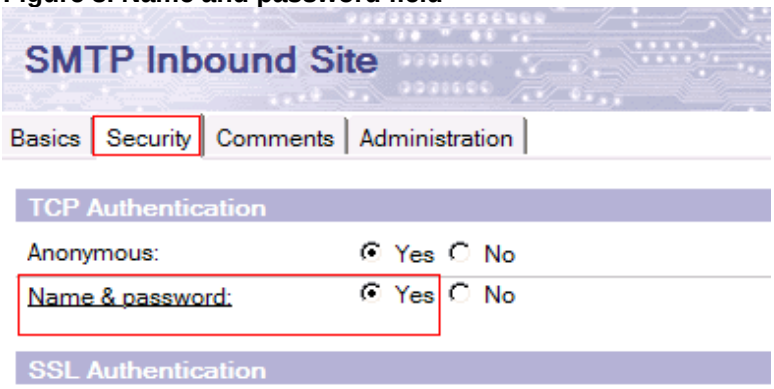
   Descriptive name for this site:
   Organization:
   Host names or addresses mapped to this site:
   Domino servers that host this site:

Figure 7. Basic tab of SMTP Inbound Site document



5. Now, moving to the Security tab, in the TCIP Authentication section, select Yes for the Name & Password field (see figure 8).

Figure 8. Name and password field



6. Click Save and Close to save the SMTP Inbound document.

7. Restart the SMTP task on the server by issuing the command **Restart Task SMTP**, so the new settings take effect.

7 SMTP authentication between Lotus Domino and the Outlook clients

When Outlook Express / Microsoft Outlook / Netscape users send and receive mail from a Domino server from their internal networks or from the Internet, SMTP authentication plays a major security role for allowing users to relay the email through the Domino server.

7.1 Using the Microsoft Outlook Express client

To enable the SMTP authentication, follow these steps:

1. Go to Tools > Accounts, and select the Mail tab.

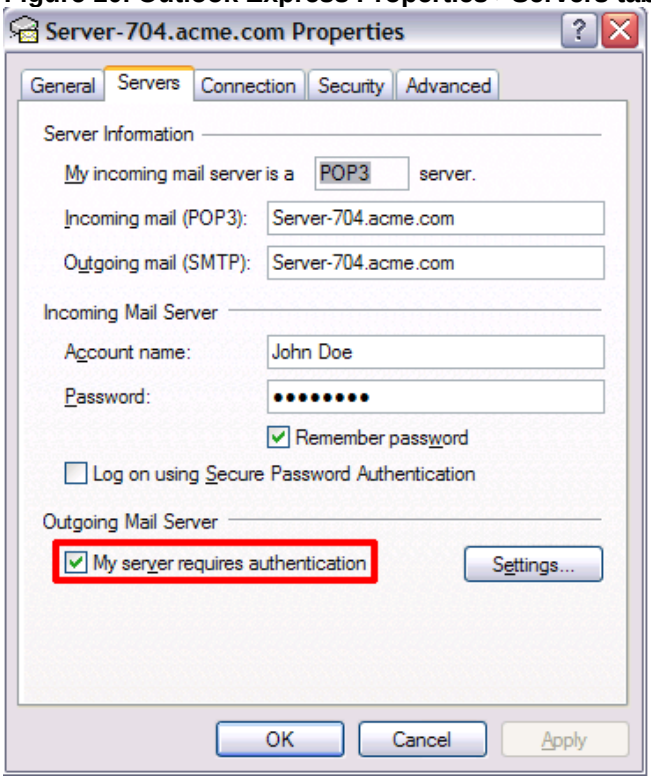
2. Select your Mail account and then click the “Properties” button (see figure 9)

Figure 9. Outlook Express Mail tab

3. Select your Intermedia account and click the Properties button.

4. Go to the Servers tab, and enable the "My server requires authentication" option under Outgoing Mail Server (see figure 10).

Figure 10. Outlook Express Properties >Servers tab



5. Click the Settings button and select "Use same settings as my incoming mail server"; click OK twice, to save the changes, and then click Close, to return to Outlook Express.

6. Finally, restart your Outlook Express client.

Now, when users send email from the Outlook Express client to the Internet, the client will first authenticate with the Domino server, using the name & password. If the credentials are correct, then it will allow to the email to be relayed.

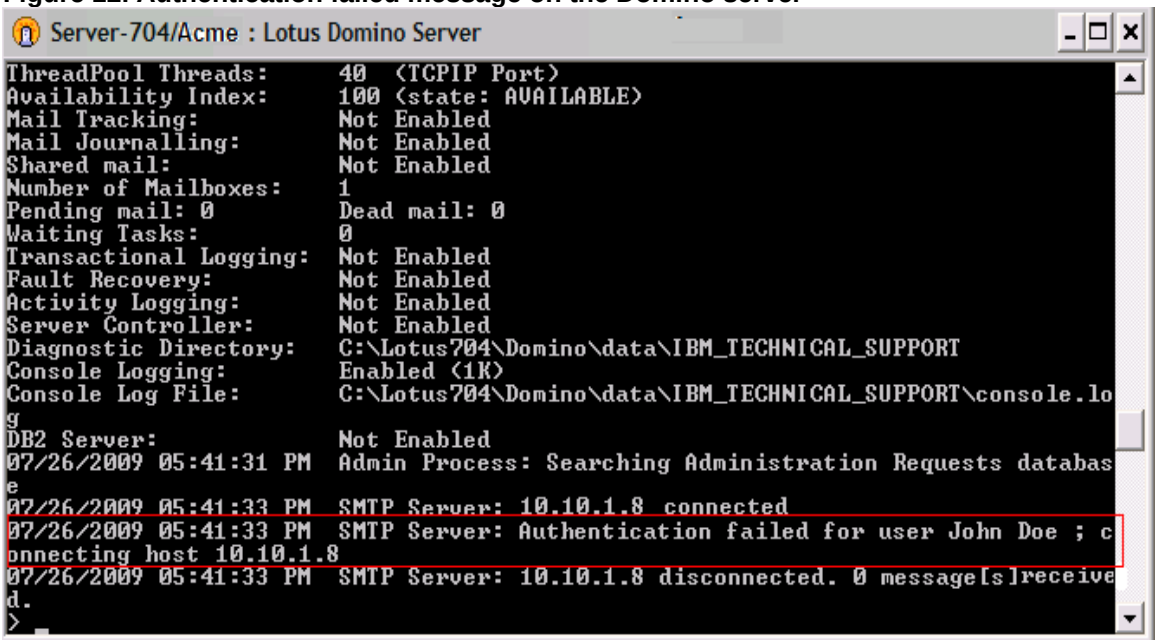
If the name and password are not correct, then on the client and the server, you will see an “Authentication failed…” error message. On the client, you will be prompted with the log-on screen shown in figure 11.

Figure 11. Name and password prompt

On the Domino server you see the following message (see figure 12):

07/26/2009 05:41:33 PM SMTP Server: Authentication failed for user John Doe ; connecting host 10.10.1.8

Figure 12. Authentication failed message on the Domino server



7.2 Using the Microsoft Outlook client

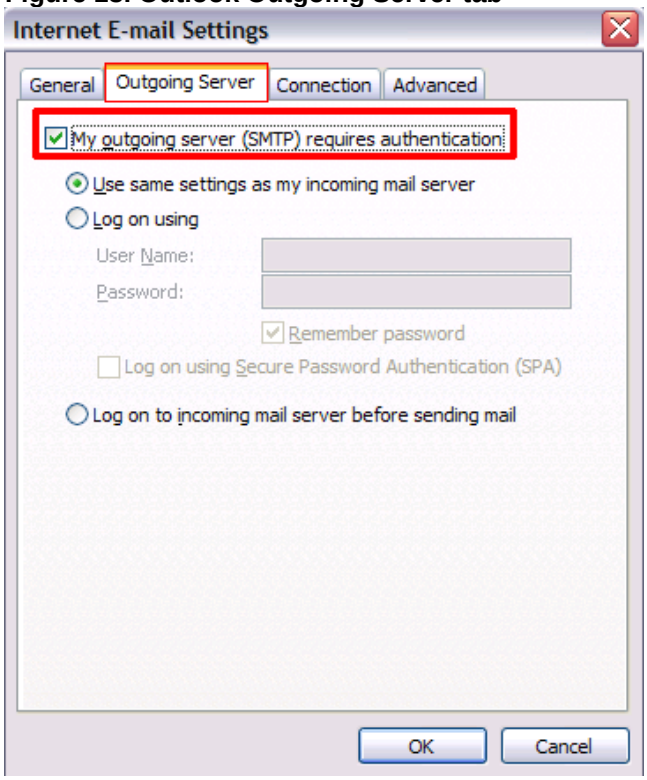
To enable the SMTP authentication, follow these steps:

1. Go to Tools > E-Mail Accounts, and select "View or change existing e-mail accounts".

2. Click Next, and select your Mail Account; then click “Change” button followed by “More Settings” button.

3. Select the Outgoing Server tab, and enable the option "My outgoing server (SMTP) requires authentication” (see figure 13).

Figure 13. Outlook Outgoing Server tab



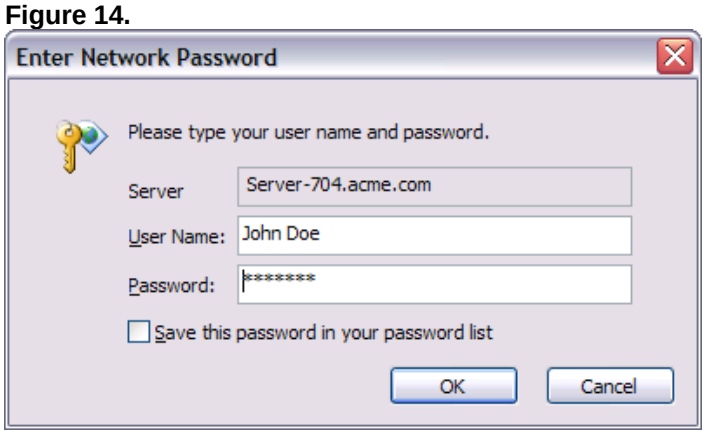
4. Select "Use same settings as my incoming mail server" and click OK.

5. Click Next and then Finish, completing the settings for authentication and, finally, restarting your Outlook client.

Now if users send mail from the Outlook client to the Internet, the client will first authenticate with the Domino server, using the name & password. If the credentials are correct, then it will allow the sender to relay the emails.

If the name and password are not correct, then on client and on the server you will see the same “Authentication failed” error as for the Express client and a similar log-on prompt screen (see figure 14).

Figure 14.

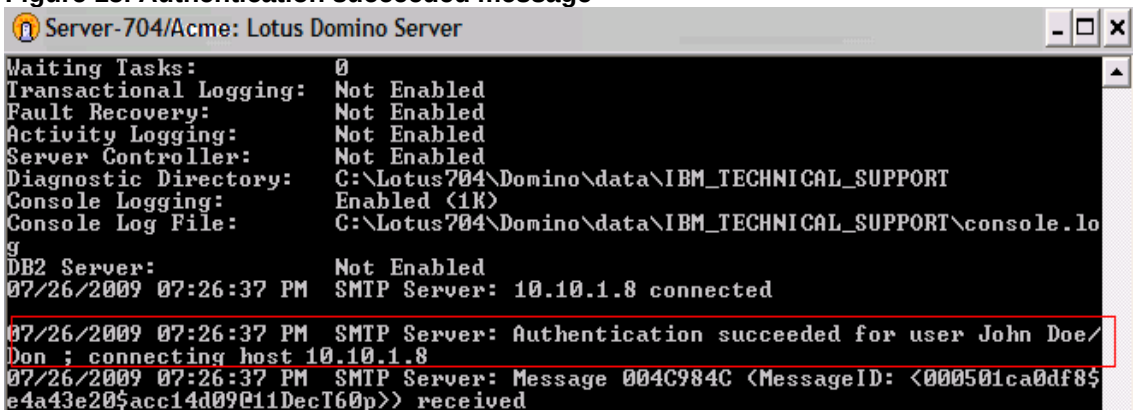


On the Domino server you see the same “Authentication failed..” message as in the case of the Express client.

When the authentication from the client is successful, you see an “Authentication succeeded…” message on the server console (see figure 15), and the message is relayed successfully to the destination domain:

> 07/26/2009 07:26:37 PM SMTP Server: Authentication succeeded for user John Doe/Don ; connecting host 10.10.1.8

Figure 15. Authentication succeeded message



8 Avoiding address spoofing when relaying email from authenticated users

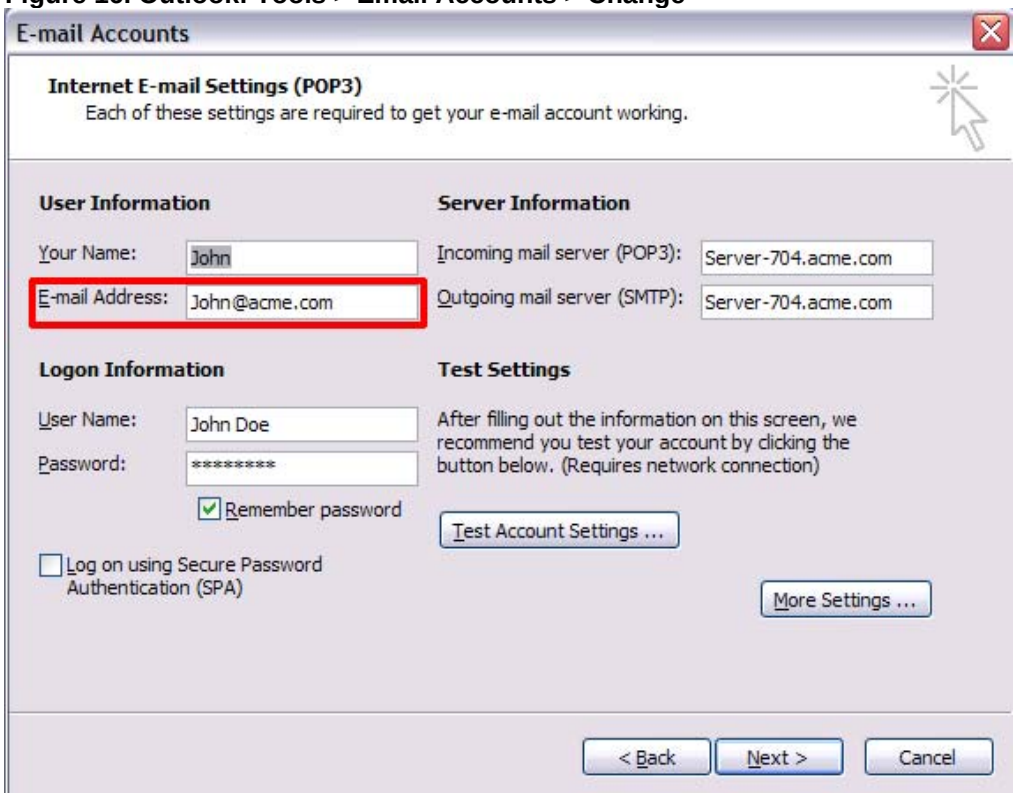
SMTP-AUTH does not necessarily guarantee the authenticity of either the SMTP envelope sender or the RFC 2822 "From:" header. Indeed, spoofing, in which a sender masquerades as someone else, is still possible even with SMTP-AUTH.

On the Domino server you can avoid spoofing of the “From” email address by using the Notes.ini parameter SMTPVerifyAuthenticatedSender. This variable lets you determine whether mail sent during an authenticated SMTP session is issued from that user's Internet address.

> Syntax: **SMTPVerifyAuthenticatedSender=value**
>
> **Description:** Specifies whether the SMTP server requires mail sent during an authenticated session to be from the Internet address of the authenticated user.
>
> **0** - Do not require the sender to use their Internet address
>
> **1** - Require the Sender, or From, if Sender header does not exist, to match the Internet address of the authenticated server.

Basically, it verifies whether the email address of the sender in the Person document matches. For example, suppose the sender is John Doe, whose email address is john.doe@acme.com, but the From email address is incorrect, say John@acme.com (see figure 16).

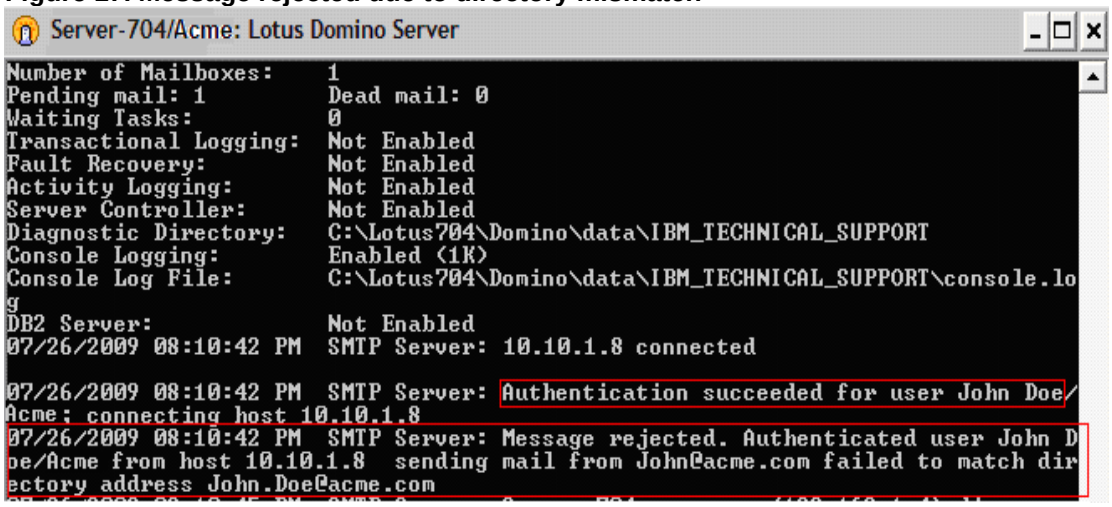
Figure 16. Outlook: Tools > Email Accounts > Change



In that case, the Domino server will not allow email to be relayed, and you see this message on the server console (see figure 17):

> 07/26/2009 08:10:42 PM **SMTP Server**: **Message rejected**. **Authenticated user John Doe/Acme** from host 10.10.1.8 sending mail from **John@acme.com failed to match directory address John.Doe@acme.com**

Figure 17. Message rejected due to directory mismatch



NOTE:

- This setting does not affect the Router, nor does it affect messages that are not submitted via SMTP.
- The SMTPVerifyAuthenticatedSender parameter does not work when SMTPTranslateAddresses is configured. Mail is rejected if addresses are translated because the match fails.
- The feature can only be used with single-address entries in the From or Sender field.

9 Inbound anti-relay settings and message transfer to external Internet domains

The process by which Inbound anti-relay settings control message transfer to external Internet domains is as follows:

1. The SMTP listener receives a connection request.

2. The server performs a reverse DNS lookup, querying DNS to find the host name that matches the connecting host's IP address. If the address resolves to a name in one of the local Internet domains, the host is considered internal. IP addresses that resolve to host names outside the local Internet domains or that do not have DNS entries are considered external.

3. The server checks the setting in the field "Perform Anti-Relay enforcement for these connecting hosts" to determine whether anti-relay controls are enabled and, if so, whether they apply to all hosts or external hosts only. If connections from the sending domain are not subject to inbound relay controls, the server allows relays for this session.

4. If the relay controls apply, Lotus Domino next checks whether the host name appears in the field "Exclude these connecting hosts from anti-relay checks." If the host name is found, the server allows relays for this session.

5. If the relay controls still apply and the connecting host successfully authenticated with the server, the server checks the field "Exceptions for authenticated users" to determine whether authenticated users are exempt from the inbound relay checks. If authenticated users are exempt, the server allows relays for this session.

   NOTE: A connecting host provides authentication credentials only when the Domino server requests them. Because Lotus Domino closes the session if authentication is not successful, there is no case in which Lotus Domino needs to determine whether a host that could not authenticate might be allowed to relay.

6. The SMTP listener receives "RCPT TO" commands from the connecting host.

7. The server examines each recipient address to see if the message would be a relay to an external domain. If so, the server checks the inbound relay controls to determine whether:

   - the connecting host is allowed to relay, or
   - relays are allowed to the target domain

The server performs matching of domains by looking for the restricted domain name as a trailing substring of the recipient's domain. If you deny the domain spamme.com, you also deny the domain you.spamme.com. Rejected recipients receive a failure status in response to the RCPT commands.

Inbound port settings affect how other SMTP hosts connect to Lotus Domino. For inbound connections, you can specify TCP/IP port settings and SSL port settings. For both ports you can define port numbers, port status, and the supported authentication methods.

10 Conclusion

Many 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 lessen the amount of time spent managing these unwanted messages.

You should now have a good understanding of what SMTP authentication is and how you can configure your Domino server with SMTP-AUTH to secure Lotus Domino from spammers.

11 Appendix A: SMTP Notes.ini variables

This 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. (This material is excerpted from the developerWorks® Lotus article, "Controlling spam: Advanced SMTP settings in Lotus Domino, Part 2".)

SMTPStrict821AddressSyntax=value. Lets you define whether or not the SMTP task requires addresses appearing in MAIL FROM commands or RCPT TO commands to 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. 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 this 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. 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. Lets you define how frequently (in minutes) Lotus Domino checks the Configuration Settings document for updates. The default value is 2.

SMTPAllowConnectionsAnonymous=value. 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. Lets you determine whether 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 non-delivery 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; if you set this variable to 2, the Router does not create a delivery status notification.

SMTPVerifySendersDomainTimeout=value. 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. 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. 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. Determines whether 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. Sets the maximum number of characters the SMTP task accepts. The default is 1,200 characters.

SMTPMaxForRecipients=value. 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. 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. 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. 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 set to 1, this variable 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 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 this variable 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, this variable 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 deliver the message locally.

RouterUseFromAsSMTPOriginator=value. 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.

The latest Notes.ini variables to be added were introduced in Lotus Domino 7, as follows:

SMTPDenyMailToGroups=value. 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. 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 accept any recipient name that is not unique. The default is 0.

12 Resources

- developerWorks Lotus Notes and Domino product page: http://www.ibm.com/developerworks/lotus/products/notesdomino/?S_TACT=105AGX13&S_CMP=LP

- Lotus Knowledge Base Technote, “Using Domino authenticated access for SMTP”: http://www-01.ibm.com/support/docview.wss?uid=swg21085735

- Lotus Notes and Domino wiki: http://www-10.lotus.com/ldd/dominowiki.nsf

- Lotus Support Web site: http://www-01.ibm.com/software/lotus/support

- Lotus Notes and Domino forums: http://www.ibm.com/developerworks/lotus/community/index.html?S_TACT=105AGX13&S_CMP=LP

- developerWorks articles, parts 1 &2, “Controlling Spam: Advanced SMTP settings in Lotus Domino”:
  http://www.ibm.com/developerworks/lotus/library/spam-smtp1/
  http://www.ibm.com/developerworks/lotus/library/spam-smtp2/

About the author

Shrikant Jamkhandi is a Senior Software Engineer for Lotus Software at IBM’s Pune, India, facility. He has worked with Lotus Domino since 2005, has more than six years of experience working in the Domino environment, and is a Certified Lotus Professional (CLP).