



# HCL Domino

Understanding SMTP authentication,  
securing your Domino server from spam,  
and using DKIM and SPF to secure  
Domino



## HCL Software Academy for HCL Digital Solutions

Creating a new generation of experts

## Table of Contents

Authors.....	3
Introduction .....	4
Overview of the SMTP process .....	4
SMTP procedures .....	5
Overview of SMTP authentication .....	6
Open relay.....	6
SMTP Authentication .....	7
Determining whether HCL Domino is open relay or closed relay.....	8
Making HCL Domino a closed-relay server .....	9
Setting inbound relay controls.....	9
Enabling SMTP Authentication on the Domino server .....	11
Configuring SMTP-AUTH options on a server that does NOT use an internet Site document.....	11
Configuring SMTP-AUTH options on servers that use Internet Site documents .....	14
SMTP authentication between HCL Domino and IMAP/POP3 clients .....	15
Using the Mozilla Thunderbird client.....	16
Using the Microsoft Outlook client.....	17
Avoiding address spoofing when relaying email from authenticated users.....	19
Inbound anti-relay settings and message transfer to external internet domains .....	21
DKIM signing for outbound SMTP mails and signature verification for inbound SMTP mails .....	22
What is DKIM? .....	22
Configuring DKIM signing for messages routed to external internet domains. ....	24
DKIM signature verification for inbound SMTP mails.....	31
Sender Policy Framework (SPF) to reduce spam. ....	33
What is SPF?.....	33
Configuring the Domino server to use the SPF protocol. ....	34
Conclusion.....	38
Appendix A: SMTP Notes.ini variables .....	38
Resources .....	42
Legal statements.....	43
Disclaimer.....	43

## Authors

This document was created by the following Subject Matter Expert (team of Subject Matter Experts):



**Shrikant Jamkhandi**  
Company: HCL

### Bio

Shrikant Jamkhandi is a Group Technical Specialist at the HCL Software & Digital Solutions Pune, India, facility. He has worked with Notes Domino support since 2005, has more than 21 years of experience working in the Domino environment, and is a Certified ND Professional (CLP).

**Contact: [Shrikant.jamkhandi@pnp-hcl.com](mailto:Shrikant.jamkhandi@pnp-hcl.com)**

---



**Aniket Salve**  
Company: HCL

### Bio

Aniket Salve is a Lead Software Engineer at the HCL Software & Digital Solutions Pune, India, facility. He has worked with Notes Domino support since 2018, has more than 21 years of experience working in the Domino environment, and is a Certified ND Professional (CLP).

**Contact: [aniket-s@pnp-hcl.com](mailto:aniket-s@pnp-hcl.com)**

---



**Jessie Jeffrey Matias**  
Company: HCL

### Bio

Jessie Jeffrey Matias is a Senior Technical Support Engineer at the HCL Software & Digital Solutions Manila, Philippines, facility. He has worked with Notes Domino support since 2012, has more than 10 years of experience working in the Domino environment, and is a Certified ND Professional (CLP).

**Contact: [jjmatias@pnp-hcl.com](mailto:jjmatias@pnp-hcl.com)**

---



**Suraj Joshi**  
Company: HCL

### Bio

Suraj Joshi is a Lead Software Engineer at the HCL Software & Digital Solutions Pune, India, facility. He has worked with Notes Domino support since 2018, has more than 15 years of experience working in the Domino environment, and is a Certified ND Professional (CLP).

**Contact: [suraj.j@pnp-hcl.com](mailto:suraj.j@pnp-hcl.com)**

---



**Xiao Yun Gu**  
Company: HCL

### Bio

Xiaoyun Gu is a Senior Technical Support Engineer at the HCL Software & Digital Solutions Beijing, China, facility. She has worked with Notes Domino support since 1997, has more than 20 years of experience working in the Domino environment, and is a Certified ND Professional (CLP).

**Contact: [xiaoyun.gu@pnp-hcl.com](mailto:xiaoyun.gu@pnp-hcl.com)**

---

## Introduction

Simple Mail Transfer Protocol (SMTP) is a 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. 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.

In this whitepaper, you will learn how the SMTP protocol and SMTP authentication process works, how to verify whether the HCL® Domino® server is open relay, how to make HCL Domino obey the SMTP authentication, and how to use DKIM/SPF for securing the server against spammers.

## Overview of the SMTP process

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

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 might 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. The client may also choose to send more than one email message on the same connection – this is known as pipelining, which improves the performance by not having to establish a new TCP/IP connection every time.

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

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

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

**RCPT TO:** <destination email address>. 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.** 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 can be queued or sent immediately when the "." is entered; however, it cannot be reset at this stage.

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

**QUIT:** Ends the session. Commits the message and closes the channel.

## 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. In this case, the server can terminate the connection and the client wouldn't be allowed to transmit any data.
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.

## Overview of SMTP authentication

SMTP is the widely used protocol for sending email from a mail client such as HCL Notes®, Domino® Web Access, Thunderbird 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 from the outside that was destined for the organization. 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 include 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.

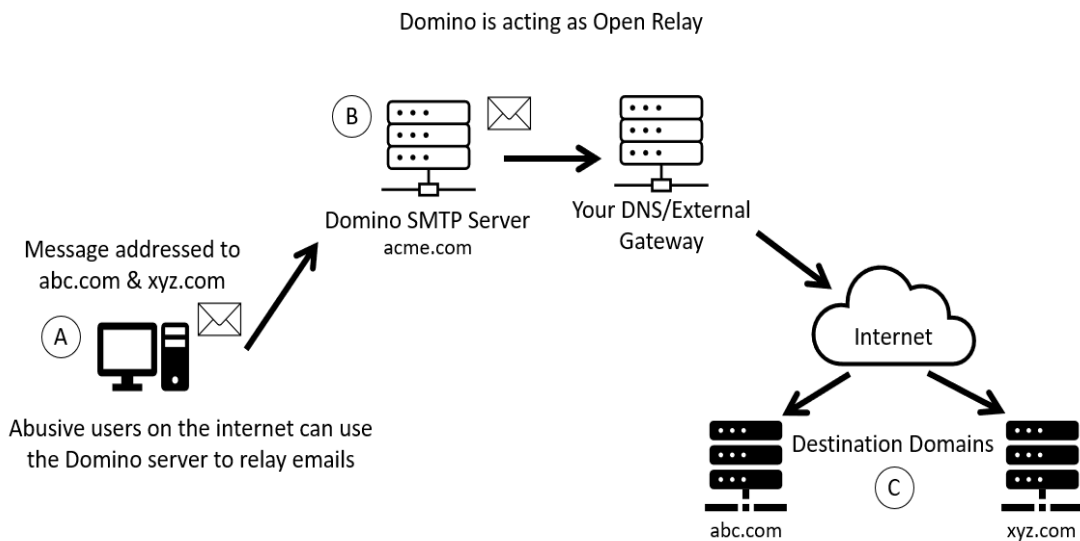
## Open relay

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 3.1).

Spammers can 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 can 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 3.1. 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 mail 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 being becoming abused.

## 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, 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 send mail, 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 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 to a 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 Framework (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).

## Determining whether HCL 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 server1.example.com 25 OR Telnet 192.168.0.107 25)

3. Telnet window will open as shown in figures 4.1 and 4.2.

**Figure 4.1. Telnet window for server1.example.com**

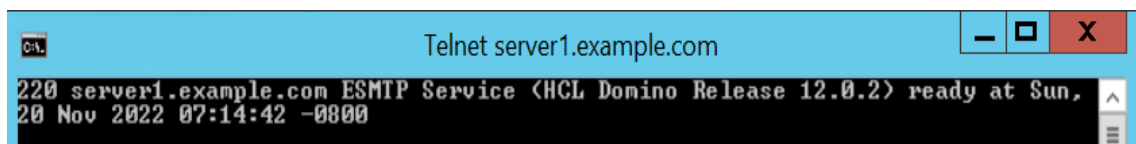
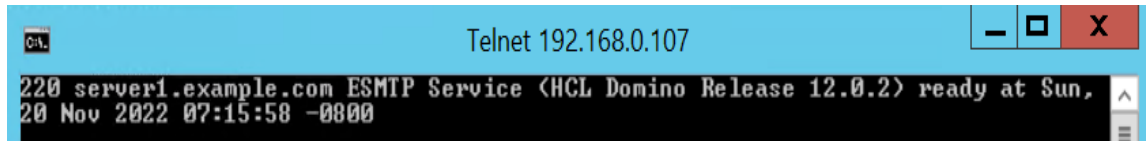




Figure 4.2. Telnet window for 192.168.0.107



4. Now type the commands as indicated below:

**220 server1.example.com** ESMTP Service (HCL Domino Release 12.0.2) ready at Sun, 20 Nov 2022 07:15:58 -0800

**helo abc.com** → Press Enter key

250 server1.example.com Hello abc.com ([192.168.0.107]), pleased to meet you

**mail from:bogus.user@bogus.com** → Press Enter key

250 bogus.user@bogus.com... **Sender OK**

**rcpt to:john.doe@gmail.com** → Press Enter key

250 john.doe@gmail.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.

## Making HCL Domino a closed-relay server

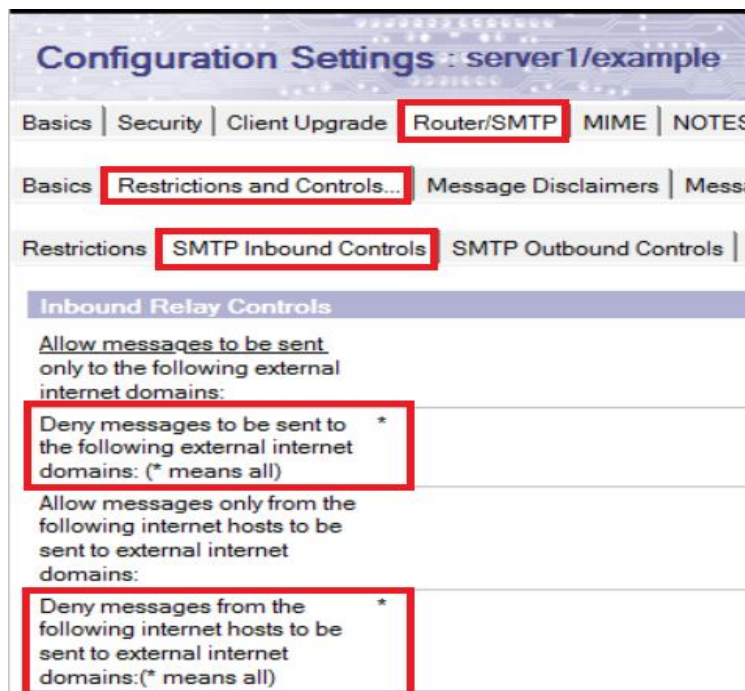
To protect SMTP servers from unauthorized relaying, HCL Domino provides inbound relay controls used to define the hosts to which and from which a server can relay messages. The Domino SMTP listener denies requests to relay messages to or from unauthorized hosts.

### 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 or servers you want to administer; click **Edit Configuration**.
4. Select the **Router/SMTP > Restrictions and Controls > SMTP Inbound Controls** tabs (see figure 5.1).

Figure 5.1. 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.

<b>Tell router update config</b>	(updates the routing tables)
<b>Tell SMTP update config</b>	(updates SMTP tables)

**Deny messages to be sent to the following external internet domains:** This field specifies the internet domains to which HCL 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, HCL 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 server1.example.com ESMTP Service (HCL Domino Release 12.0.2) ready at Sun, 20 Nov
2022 07:25:54 -0800
helo abc.com → Press Enter key
250 mail1.v1202.com Hello abc.com ([192.168.0.107]), pleased to meet you
mail from:bogus.user@bogus.com → Press Enter key
250 bogus.user@bogus.com... Sender OK
rcpt to:john.doe@gmail.com → Press Enter key
554 Relay rejected for policy reasons.
```

## 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 for 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.

## 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 Notes.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 this information. Use the Notes.ini variable SMTPGreeting to customize the SMTP service greeting.

To change inbound SMTP TCP/IP port settings:

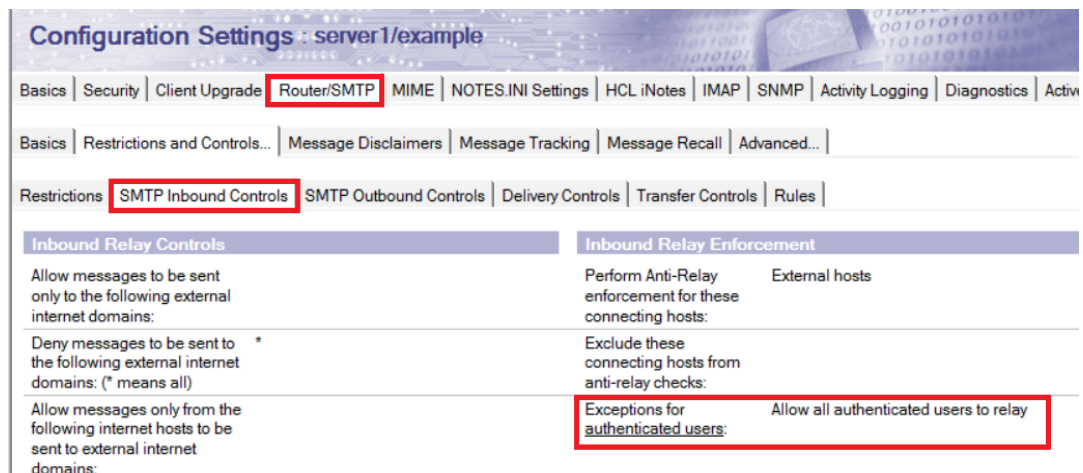
1. From the Domino Administrator, click the **Configuration** tab and open the Server document for the server that runs the SMTP service.
2. Select the **Ports > Internet Ports > Mail** tab.
3. In the Mail (SMTP Inbound) column, set the **Authentication options: Name & password** field to **Yes** (see figure 6.1). Click **Save & Close**.

Figure 6.1. SMTP Inbound authentication options

Web	Directory	Mail	DIOP	Remote Debug Manager	Server Controller
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	No		

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 or servers that 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 6.2) make sure the field **Exceptions for authenticated users** is set to **Allow all authenticated users to relay**.

Figure 6.2. 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 for external hosts only, leave the default **External hosts** 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 **server1.example.com 25** → Press Enter

**Telnet 192.168.0.107 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 server1.example.com ESMTP Service (HCL Domino Release 12.0.2) ready at Mon, 21
Nov 2022 02:09:45 -0800
ehlo abc.com                → Press Enter key
250-server1.example.com Hello abc.com ([192.168.0.105]), pleased to meet you
250-TLS
250-HELP
250-AUTH LOGIN
250-STARTTLS
250-SIZE
250 PIPELINING
```

## 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, 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 6.3):

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

Figure 6.3. Basics tab of SMTP Inbound Site document

Site Information	
Descriptive name for this site:	SMTP Inbound Site
Organization:	example
Host names or addresses mapped to this site:	server1.example.com
Domino servers that host this site:	server1/example

- Now, moving to the **Security** tab, in the **TCIP Authentication** section, select **Yes** for the **Name & Password** field (see figure 6.4).

Figure 6.4. Name and password field

TCP Authentication	
Anonymous:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name & password:	<input checked="" type="radio"/> Yes <input type="radio"/> No

- Click **Save and Close** to save the SMTP Inbound document.
- Restart the SMTP task on the server by issuing the command **Restart Task SMTP**, so the new settings take effect.

## SMTP authentication between HCL Domino and IMAP/POP3 clients

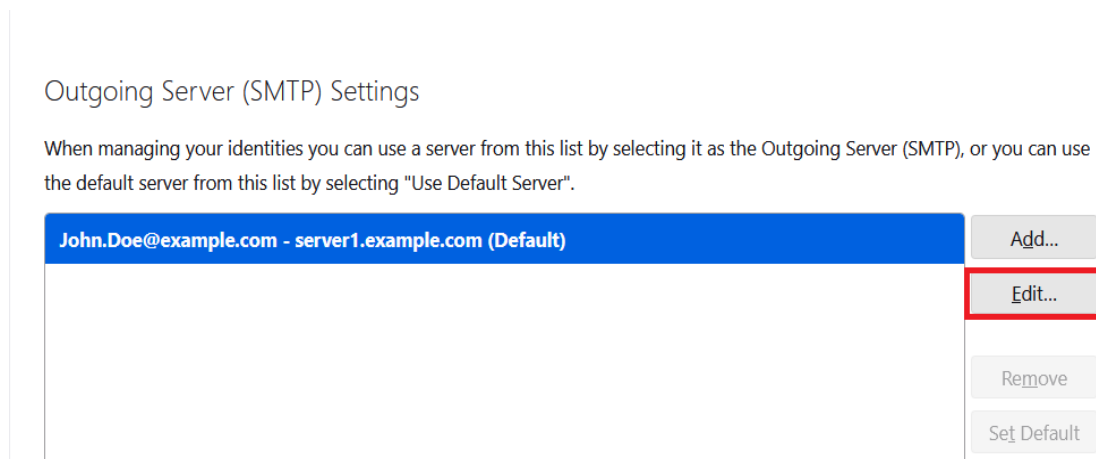
When Mozilla Thunderbird / Microsoft Outlook users send and receive mail from a Domino server from their internal networks or from the internet, SMTP authentication plays a major security role for allowing users to relay the email through the Domino server.

## Using the Mozilla Thunderbird client

To enable the SMTP authentication, follow these steps:

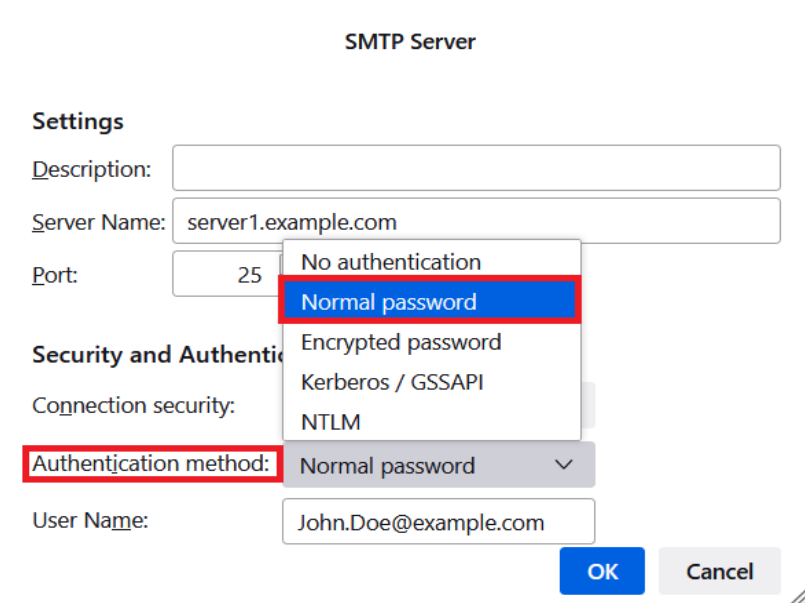
1. Go to **Settings > Account Settings**, and under configured account select **Outgoing Server (SMTP)**.
2. Select your Mail account and then click the **Edit** button (see figure 7.1).

**Figure 7.1. Mozilla Thunderbird Outgoing Server setting**



3. Under **Authentication method** select **Normal Password**. (see figure 7.2).

**Figure 7.2. Mozilla Thunderbird Authentication method**



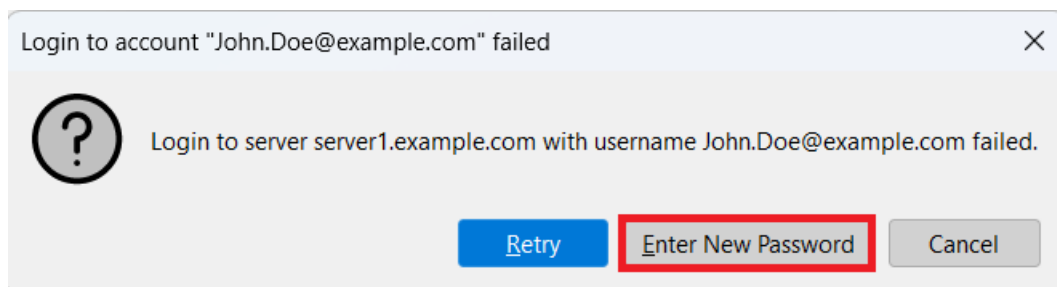
4. Click the **OK** button to save the changes, and then click **Close** to return to Thunderbird.



Now, when users send email from the Mozilla Thunderbird 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 a “[Login to account... failed](#)” error message. On the Thunderbird client, you will be prompted with “[Enter New Password](#)” as shown in figure 7.3.

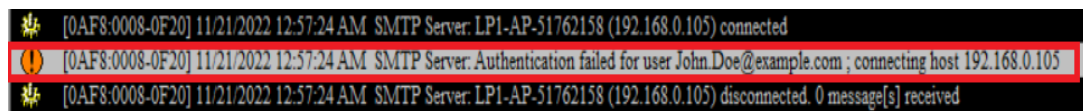
**Figure 7.3. Enter New Password prompt**



On the Domino server you see the following message (see figure 7.4):

*[0AF8:0008-0F20] 11/21/2022 12:57:24 AM SMTP Server: Authentication failed for user John.Doe@example.com ; connecting host 192.168.0.105*

**Figure 7.4. Authentication failed message on the Domino server**

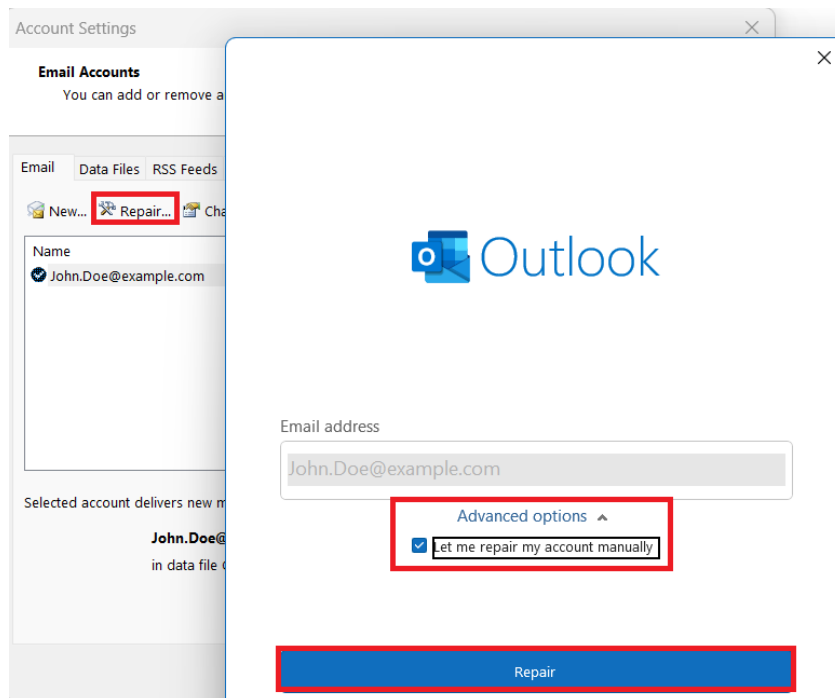


## Using the Microsoft Outlook client

To enable the SMTP authentication, follow these steps:

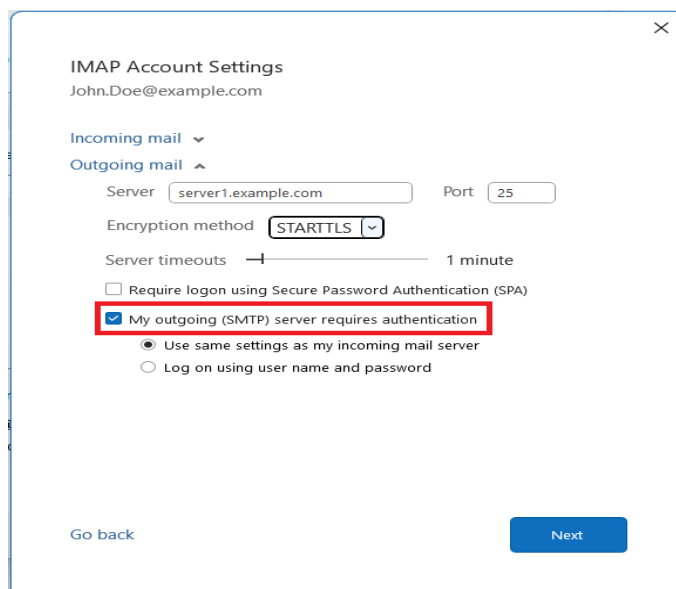
1. Go to **File > Account Settings Account Settings → Email** and select **Repair**.
2. Click Advanced options, select the account and click [Let me repair my account manually](#), and then click **Repair**. (see figure 7.5).

Figure 7.5 Microsoft Outlook Advanced options



3. Select the **Outgoing Server** tab, and enable the option **My outgoing server (SMTP) requires authentication** (see figure 7.6).

Figure 7.6 Outlook Outgoing Server tab



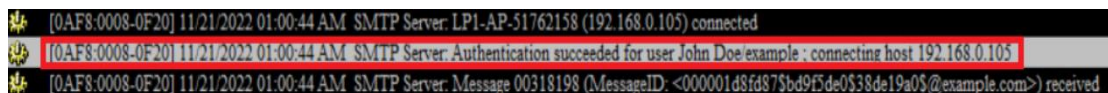
4. Select **Use same settings as my incoming mail server**.
5. Click **Next** and then click the **Finish** button to complete the settings for authentication. Restart your Outlook client.

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

When the authentication from the client is successful, you see an “Authentication succeeded...” message on the server console (see figure 7.7), and the message is relayed successfully to the destination domain:

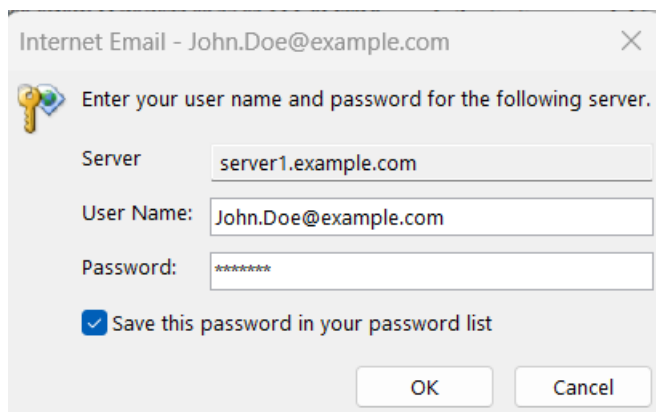
```
[0AF8:0008-0F20] 11/21/2022 01:00:44 AM SMTP Server: Authentication succeeded for user John Doe/example ; connecting host 192.168.0.105
```

Figure 7.7. Authentication succeeded message



If the name and password are not correct, on the client and on the server you will see the same “**Authentication failed**” error as for the Mozilla Thunderbird client and a similar log-in prompt screen (see figure 7.8).

Figure 7.8. Log-in screen if authentication failed



## 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 the 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@example.com](mailto:John.Doe@example.com), but the "From" email address is incorrect, say [bogus.user@example.com](mailto:bogus.user@example.com) (see figure 8.1).

**Figure 8.1. Outlook: File>Account Settings >Account Settings >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 8.2):

*[0820:0008-10E8] 11/21/2022 01:21:25 AM SMTP Server: Message rejected. Authenticated user [John.Doe@example.com](mailto:John.Doe@example.com) from host 192.168.0.105 sending mail from [bogus.user@example.com](mailto:bogus.user@example.com) failed to match directory address [John.Doe@example.com](mailto:John.Doe@example.com)*

**Figure 8.2. 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 be used with only single-address entries in the From or Sender field.

## 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, HCL 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 HCL Domino closes the session if authentication is not successful, HCL Domino does not need to determine whether a host that could not authenticate should 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 matches 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 HCL 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.

## DKIM signing for outbound SMTP mails and signature verification for inbound SMTP mails

### What is DKIM?

Domain-Keys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in email (email spoofing), a technique often used in phishing and email spam.

DKIM allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It achieves this by affixing a digital signature, linked to a domain name, to each outgoing email message. The recipient system can verify this by looking up the sender's public key published in the DNS. A valid signature also guarantees that some parts of the email have not been modified since the signature was affixed.

DKIM signing and verification is done by the sending and receiving endpoints and is not generally visible to message recipients while reading a message.

DKIM is an Internet Standard. It is defined in RFC 6376, dated September 2011; with updates in RFC 8301 and RFC 8463.

#### Relationship to SPF and DKIM

SPF allows email senders to define which IP addresses are allowed to send mail for a particular domain. DKIM, on the other hand, provides an encryption key and digital signature that verify that an email message was not forged or altered.

#### Relationship to SPF and DMARC

Both DKIM and SPF provide different measures of email authenticity. Domain-based Message Authentication, Reporting and Conformance (DMARC) provides the ability for an organization to publish a policy that specifies which mechanism (DKIM, SPF, or both) is employed when sending email from that domain; how to check the "From" field presented to end users; how the receiver should deal with failures—and a reporting mechanism for actions performed under those policies.

DMARC is being considered for a future Domino release. Below is the link to this idea/enhancement request:

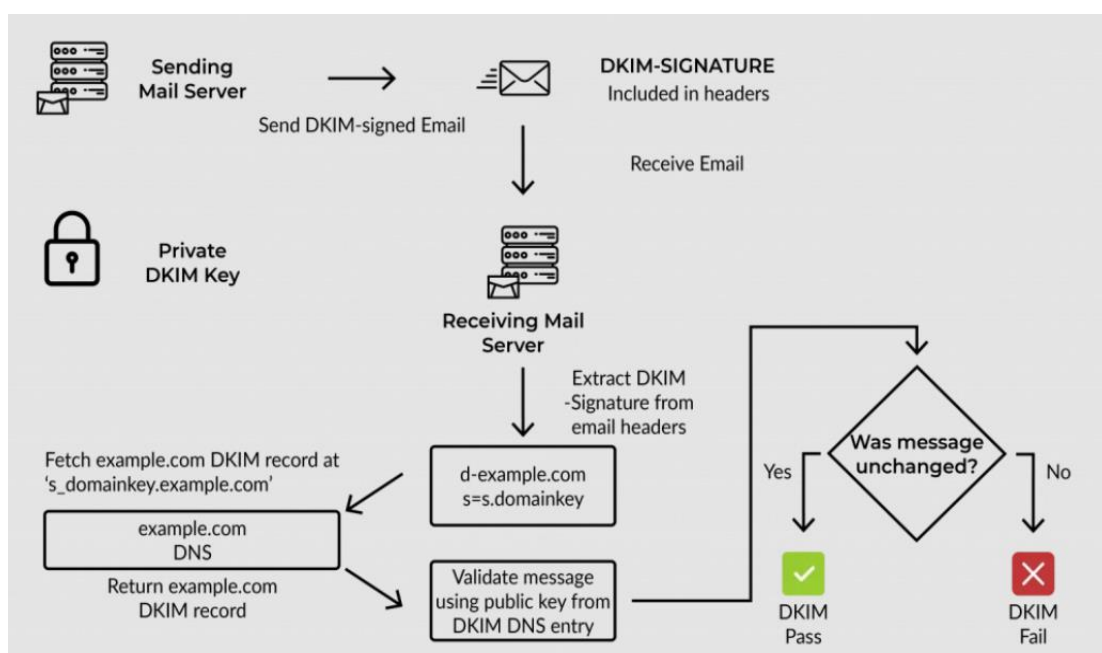
<https://domino-ideas.hcltechsw.com/ideas/IDEAMLCT-I-6>

#### DKIM configuration overview in HCL Domino

- Create key pairs (private key and public key) using **keymgmt** command.
- Create a DNS TXT record that contains the public key and add it to your DNS domain settings.

- Outbound internet mails are DKIM signed by the creation of a hash of certain message headers and their content, the creation of a hash of the message body content, and then the signing the hashes with a digital signature. The sending MTA (Domino in our case) affixes a “DKIM-Signature” header to the message, containing these signed hashes and additional information which allows the verifier (receiving MTA) to locate a public key, which is used to verify the hash.
- When an inbound mail server receives an email, it looks up DNS to find the sender’s (example.com in our case) public DKIM key. This key is used by the inbound server to decrypt the signature and compare it to the newly computed version. If the two values match, the email’s validity and authenticity is proven.
- The verifier will then affix an Authentication-Results header to the message, with its determination of message authenticity.

**Figure 10.1 DKIM Authentication process**



## Configuring DKIM signing for messages routed to external internet domains

To use DKIM to sign messages being routed to the internet, configure DKIM on the Domino servers on the edge of your Domino environment that use SMTP to transfer mail to the internet.

**Note:** DKIM signing requires Domino V12.0.1 and later, and an SMTP server on Linux 64 or Windows 64.

### Steps to configure DKIM signing:

1. Create a credential store for storing DKIM keys on each Domino SMTP that uses DKIM signing.

**Note:** If your SMTP servers already have a credential store, ensure the credential store is using the V12.0.1 websecuritystore.ntf template.

- a. From the server console, use the following command to create a named encryption key (NEK) which is **added** to the server ID file. Domino® uses the key to encrypt the credentials that are stored in the credential store.

Syntax: **keymgmt create nek <nekname>**

This example shows that a NEK named “**credstorekey**” was created (see figure 10.2):

**Figure 10.2. Creating a NEK named “credstorekey”**

```
> keymgmt create nek credstorekey
[0D50:0008-0E8C] 10/22/2022 07:03:49.30 PM NEK > NEK credstorekey - Fingerprint 2D7C 61C2 DB28 7EDB
0AAD E398 BE04 96D9 BCB9 D293
[0D50:0008-0E8C] NEK credstorekey created successfully
```

- b. From the server console, use the following command to create the credential store application and encrypt it using the key you created:

Syntax: **keymgmt create credstore <nekname>**

This example shows that the credential store was created using the key “**credstorekey**” (see figure 10.3):

**Figure 10.3. Creating the credential store database and encrypting it using the key “credstorekey”**

```
> keymgmt create credstore credstorekey
[0CB0:0006-0F04] Credential Store Name : IBM_CredStore\credstore.nsf
[0CB0:0006-0F04] NEK Fingerprint : 84B5 D1E3 8E2A C078 CEF4 0FB0 6D6A 00E0 8937 ADB9
[0CB0:0006-0F04] Credential Store created successfully. The credential store was NOT created in a cluster. If y
ou wish to cluster the current server or move the credential store to another server, see the product documenta
tion
[0CB0:0006-0F04] Nonce Fingerprint : C385 8DB2 B803 D3B3 40C2 BF93 4A1E 3524 778C A7CD
```

The database credstore.nsf is created in the Domino \data\IBM\_CredStore directory.



For more information on creating a credential store if you don't already use one, see [Using a credential store to store credentials](#).

## 2. Create DKIM signing keys in the credential store.

Create one or more keypairs in a credential store to use for DKIM signing. To create a DKIM signing keypair document in the credential store, run the following command from the console of a Domino server that has the credential store:

Syntax: **keymgmt create DKIM <domain> <selector> RSA [<keySize>]**

where:

- <domain> is the name of the Domino internet domain
- <selector> is the name of your choice for the DKIM selector. The selector is specified in the DKIM-Signature header and indicates where the public key portion of the DKIM keypair exists in DNS.
- <keySize> is the specified size for the DKIM key. Size can be 1024, 2048 or 4096.

This example shows a created DKIM key where domain is **example.com**, selector is **12345** and keySize is **2048** by issuing the following Domino server console command:

**keymgmt create DKIM example.com 12345 RSA 2048** (see Figure 10.4):

**Figure 10.4: Using keymgmt to create DKIM key**

```
> keymgmt create DKIM example.com 12345 RSA 2048
[0CB0:0006-0F04] Created DKIM key 12345._domainkey.example.com
```

To know configured DKIM keys on the Domino server, you can use command “**keymgmt show dkim ALL**” to show all DKIM keys (see figure 10.5):

**Figure 10.5. Using the command “keymgmt show dkim ALL” to show all DKIM keys**

```
> keymgmt show dkim ALL
[0CB0:0006-0F04] DKIM : Selector: 12345, Domain: example.com, Fingerprint 8F47 98D6 F2CE 273C A579 D6BA 9994 0
0FF 1678 3290 7DA9 FC62 4794 7D8D CC37 FC22
[0CB0:0006-0F04] Show All DKIM Keys succeeded.
```

## 3. Create a **DNS TXT** record that contains the key and add it to your DNS domain settings.

After you create the DKIM signing keys in the credential store, run the following command to create a .txt file in the Domino data directory that contains the contents of a **DNS TXT** record for the specified key:

Syntax: **keymgmt export DKIM DNS <domain> <selector> <dkimdnsfile>**

where:

- <domain> is the name of the Domino internet domain that you specified for the key.
- <selector> is the DKIM selector you specified for the key.
- <dkimdnsfile> is the name of the .txt file to create in the Domino data directory that contains the DNS TXT record.

In the example, we created **dkimdns.txt** file that contains a **DNS TXT** record for the DKIM key (**domain=example.com**, **selector=12345**) (see figure 10.6).

**Figure 10.6: Exporting DNS TXT record to a file**

```
> keymgmt export DKIM DNS example.com 12345 dkimdns.txt
[0CB0:0006-0F04] Parse domain example.com
[0CB0:0006-0F04] Parse selector 12345
[0CB0:0006-0F04] Parse filename dkimdns.txt

[0CB0:0006-0F04] Get DKIM key d=example.com, s=12345, No error

[0CB0:0006-0F04] Get Key as PEM No error

[0CB0:0006-0F04] Get Key as DNSKey v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAswSos/X0KgQgAxp2pwhL48s88wYKav1u4K4Yi293NiOq2eFAFQgds2U0k2BMcXgcmOk61ii+ALerWxBj1St2rRp6QuugTv97cspqdWoe3soBYkctzZ93fgg8iNtZVDAVgZXMMDRwusp533smRHLStpYq3vUHZ7rvsDyOE9UfrKEgdy
[0CB0:0006-0F04] Exported DKIM key to DNS file c:\Domino\Data\dkimdns.txt, No error
```

When you open the exported file **dkimdns.txt**, it looks like this:

```
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAswSos/X0KgQgAxp2pwhL48s88wYKav1u4K4Yi293NiOq2eFAFQgds2U0k2BMcXgcmOk61ii+ALerWxBj1St2rRp6QuugTv97cspqdWoe3soBYkctzZ93fgg8iNtZVDAVgZXMMDRwusp533smRHLStpYq3vUHZ7rvsDyOE9UfrKEgdyx3+eAGhnXRFEuT1ovVEis1ib2Ik6sdWtR1HB5Dqgetwzp4XuDoCilvtWP8jNg5E226ju7aUbXITxxZug9QzdrGtTar3x/z7CM/pDN/xqR+tTG9IZhf7drjGlF33/p/7eNtb8ke3y434/Vrggqy4bAXp/zpY4ZwZlbtmsFylQIDAQAB;
```

Your DNS provider can provide instructions for adding this record to your DNS domain settings. Below is a sample **DNS TXT** record on Windows DNS server (see Figure 10.7):

Figure 10.7. Sample DNS TXT record

**Note:** Be careful with RSA keys that are 2048-bit and larger. DNS is limited to 255-byte strings, so the key ("p=") needs to be split into multiple lines. Exact steps to do this will be vendor specific.

After adding DNS TXT to your DNS domain, you can verify it using **nslookup**, (see figure 10.8):

**nslookup -type=txt 12345.\_domainkey.example.com**

Figure 10.8. Verify DNS TXT record added in DNS domain using nslookup

```
C:\>nslookup -type=txt 12345._domainkey.example.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 192.168.3.252

12345._domainkey.example.com    text =

        "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
X0KgQgAxp2pwhL48s88wYKav1u4K4Yi293Ni0q2eFAFQgds2"
        "U0k2BMcXgcmOk61ii+ALerWxBj1St2rRp6QuugTv97cspqdWoe3soBYkctzZ93fgg8iN
tZVDAVgZXMMDRWusp533smRHLStpYq3vUHZ7rvsDyOE9UfrKE"
        "gdyx3+eAGhnXRFEuT1ovVEis1ib2Ik6sdWtR1HB5Dqgetwzp4DoCilvtWP8jNg5E226j
u7aUbX1TxxZug9QzdrGtAr3x/z7CM/pDN/xqR+tTG9IZhf7"
        "drjGlf33/p/7eNtb8ke3y434/Vrggqy4bAXp/zpY4ZwZlbtmsFylQIDAQAB; "
```

4. Specify the key(s) to use for DKIM signing (through notes.ini) on the server.

After you add a DNS TXT record for the keys to use for DKIM signing to your DNS domain settings, use the notes.ini setting DKIM\_KEY on a Domino SMTP server to map a domain to a key to use for DKIM signing. The following table describes various options for this setting. If the router is running, restart it for the changes to take effect.

Table 10.1.

Example Setting	Description and Example
DKIM_KEY_<domain>=<selector>	<p>When users send messages from the specified domain or any of its subdomains, the server signs the messages with the key that corresponds to the specified selector.</p> <p><i>DKIM_KEY_&lt;domain&gt;=&lt;selector&gt;</i></p>
DKIM_KEY_<subdomain>=<selector>	<p>When users send messages from the specified subdomain, the server signs the messages with the key that corresponds to the specified selector.</p> <p><i>DKIM_KEY_&lt;subdomain&gt;=&lt;selector&gt;</i></p>
DKIM_KEY_<domain>=<selector>,<selector>	<p>When users send messages from the specified domain, the server signs the messages with both of the keys specified by two selectors. This scenario is useful for:</p> <ul style="list-style-type: none"> <li>Allowing signing by both old and new keys during key rollover transition while a new key propagates to DNS.</li> </ul> <p>Using multiple signing algorithms.</p> <p><i>DKIM_KEY_&lt;domain&gt;=&lt;selector&gt;,&lt;selector&gt;</i></p>
DKIM_KEY_<aliasdomain>=<domain>;<selector>	<p>When users send messages from an alias domain (a domain that is not the primary domain), the messages are signed with the key that corresponds to the selector for the primary domain.</p> <p><i>DKIM_KEY_&lt;aliasdomain&gt;=&lt;domain&gt;;&lt;selector&gt;</i></p>

In this example, we mapped example.com to selector “12345” to use for DKIM signing (see figure 10.9).

**Figure 10.9. Setting DKIM\_KEY and restarting router task**

```
> set config DKIM_KEY_example.com=12345
> restart task router
[0C34:0002-01A8] 23/10/2022 10:51:20 AM Router: Shutdown is in progress
[0C34:0002-01A8] 23/10/2022 10:51:22 AM Router: Mail Router shutdown
[1138:0002-1050] 23/10/2022 10:51:24 AM nrouter: Current Logging Options: NORMAL
[1138:0002-1050] 23/10/2022 10:51:24 AM Router: Mail Router started for domain ABC
[1138:0002-1050] 23/10/2022 10:51:24 AM Router: Internet SMTP host server1 in domain example.com; SMTP display
host name server1.example.com
```

5. Enable DKIM signing (through notes.ini) on the server.

After you configure the DKIM\_KEY settings to map a domain to a key, specify the following additional setting to enable DKIM signing. You can enable or disable DKIM signing while the router is running, and no router restart is required.

Syntax: **RouterDKIMSigning=<value>**

where <value> is one of the following values:

- 1 This option makes a best effort to sign a message if a signing key is specified for the sender’s domain. If a signing error occurs, an error is logged but the message is delivered unsigned.
- 2 This option enforces DKIM signing. If a signing key is specified for the sender’s domain and a signing error occurs, the error is logged, and the message isn't sent. The sending user receives a non-delivery report.

In this example, we set **RouterDKIMSigning=2** to enforce DKIM signing (see figure 10.10).

**Figure 10.10. Setting ini RouterDKIMSigning=2 dynamically from Domino console**

```
> set config RouterDKIMSigning=2
[1138:0002-1050] 23/10/2022 10:52:23 AM RouterDKIMSigning changed to 2.
```

Now if you send an email from **example.com** to external internet domains, you will see that Domino appends a “DKIM–Signature” to the header of the message.

You can follow the link below to trap outbound SMTP MIME information on the Domino server.

[https://support.hcltechsw.com/csm?id=kb\\_article&sysparm\\_article=KB0037179](https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0037179)

Below is an example of a DKIM–Signature when it adds to the message header.

**DKIM-Signature:**

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com;
s=12345; t=1666493747;
bh=XXfL04v41isU/a7jpmN3mnXD+y07hioZVtDkkvMzzmY=;
h=To:MIME-Version:Subject:Message-ID:From:Date:Content-Type;
b=RKmoSL4bN66BfTvBjam4reKkD/QBh5BifzuXt7AYts3EFiL7c7Jb0HL+AQlkjpQvB
wfjPI92XW29qLFgvSWxP1H3eEHRA6Bbir5kkZB/6HAVy6CfXAFecXSDeCOAuav7/8DNqhWceTE
7/joHAMhPWYEDo7Ql2s9dIYldZOeyTpfR1U4foY6g5+DAVfO+izS54sPBc

NltV0RbQQkNIFohi3ZrZfFDurwToFFt3teSSOP5+2Jt78jXdqduoP+y133/1lzXObjR6TTiy9CbwcsiH
PSVQip1ZoM6C7K1JQsi1bugG+G+8hPk+DXqXCke2R9RtWDjlCYRKvdOV5lzafQuLg==
```

Where the tags used are:

- v** (required), version
- a** (required), signing algorithm
- c** (optional), canonicalization algorithm(s) for header and body
- d** (required), Signing Domain Identifier (SDID)
- s** (required), selector
- t** (recommended), signature timestamp
- h** (required), header fields - list of those that have been signed
- bh** (required), body hash
- b** (required), signature of headers and body

## DKIM signature verification for inbound SMTP mails

Domino servers which receive SMTP messages directly from the internet may be configured to use DKIM signature verification. They will use DKIM-Signature affixed by the sending server, and public keys published in DNS by the sending domain, to verify that the message was authorized by the domain, and that the contents of the message have not been modified in transit.

Domino records the result of each signature validation in an Authentication-Results header that it affixes to the message.

**Table 10.2 Possible DKIM evaluation results (only one result per signature is recorded)**

Result	Reason	Untrusted?
None	No DKIM signatures were found on the message	No
Neutral	The message was signed, but the signature or signatures contained syntax errors or were not otherwise able to be processed. This result is also used for other failures not covered elsewhere in this list.	No
Pass	The message was signed, the signature was acceptable, and the signature passed verification.	No
Fail	The message was signed and the signature or signatures were acceptable, but they failed verification.	Yes
Temperror	The message could not be verified due to some error that is likely transient in nature, such as a temporary inability to retrieve a public key from DNS. A later attempt may produce a final result.	No
Permerror	The message could not be verified due to some error that is unrecoverable, such as a required header field being absent. A later attempt is unlikely to produce a final result.	No

**Note:**

1. DKIM signature verification requires Domino 12.0.2.
2. DKIM signature verification can result in multiple DNS lookups, and thus can potentially impact SMTP server performance. An internal cache is utilized by Domino to reduce this impact.
3. DKIM signature verification will never cause a message to be rejected for any result.

**Configuring the Domino SMTP server to use DKIM signature verification:**

Open the **Configuration** document and go to **Router/SMTP > Restrictions and Controls > SMTP Inbound Controls**. Locate the **Inbound Sender Domain Authentication Controls** section and change the **DKIM signature verification** field to **Enabled** (see Figure 10.11).

Figure 10.11. DKIM signature verification

Inbound Sender Domain Authentication Controls

DKIM signature verification: ☒ Enabled

Sender Policy Framework check (SPF): ☐ Disabled

Desired action when the sending IP hard fails the SPF check for the sender domain: ☒ Log and tag message

Do not perform an SPF check for the following internet hostnames/IP addresses:

Below are **Authentication-Results** examples after DKIM signature verification enabled (see figure 10.12).

Figure 10.12. DKIM evaluation result is Pass

Advanced Document Properties - enabled DKIM for outbound mail(enabled DKIM... [E33CB1E610...]

Fields Info Attachments

Search: copy

Field Name	Data Type	Size	Value
\$Orig	Notes Refs	20	7F90FFE18DE8F1C
\$Revisions	Time\Date	10	
\$TUA	Notes Refs	20	E33CB1E610C814
\$UpdatedBy	Names	18	CN=server2/O=x
AltFrom	Computed...	4	
Authentication_Re...	RFC 822 Text	154	xyz.com 1; dkim=
BGTableColor	Computed...	8	bg_3
BlindCopyTo	Computed...	4	
Body	Computed...	4	
Categories	Text	2	

Field Name: Authentication\_Results  
Data Type: RFC 822 Text  
Data Length: 154 bytes  
Field Flags: SUMMARY

"xyz.com 1; dkim=pass  
header.s=12345  
header.d=example.com"

panagenda Follow Document Selections Close

Figure 10.13. DKIM evaluation result is Permerror

Advanced Document Properties - enabled DKIM for outbound mail(enabled DKIM... [131F4FA9930AB9...]

Fields Info Attachments

Search: copy

Field Name	Data Type	Size	Value
\$TUA	Notes Refs	20	131F4FA9930AB9!
\$UpdatedBy	Names	18	CN=server2/O=x
Authentication_Re...	RFC 822 Text	236	xyz.com 1; dkim=
Categories	Text	2	
DeliveredDate	Time\Date	10	11/11/2022 07:39:
DKIM_Signature	RFC 822 Text	1,136	v=1; a=rsa-sha25
Form	Text	6	Memo
From	RFC 822 Text	58	admin@example
MIME_Version	RFC 822 Text	38	1.0
PostedDate	RFC 822 Text	61	11/11/2022 07:20:

Field Name: Authentication\_Results  
Data Type: RFC 822 Text  
Data Length: 236 bytes  
Field Flags: SUMMARY

"xyz.com 1;  
dkim=permerror  
reason="unable to  
apply public key"  
header.s=12345  
header.d=example.com"

panagenda Follow Document Selections Close



## Sender Policy Framework (SPF) to reduce spam

### What is SPF?

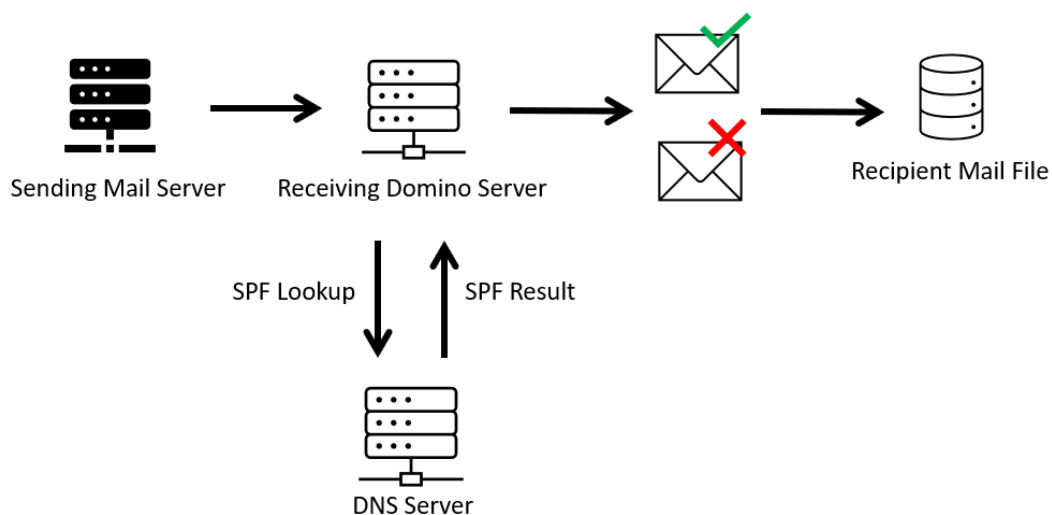
Sender Policy Framework (SPF) is a protocol designed to restrict who can use an organization's domain as the source of an email message. SPF blocks spammers and other attackers from sending email that appears to be from a legitimate organization. SMTP (Simple Mail Transfer Protocol) does not place any restrictions on the source address for emails, so SPF defines a process for the domain owners to identify which IP addresses are authorized to forward email for their domains.

The SPF protocol was published in 2014 by the Internet Engineering Task Force (IETF) in RFC 7208, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1." SPF is an IETF Proposed Standard specification.

### SPF configuration overview in HCL Domino

- Domino servers that receive SMTP messages directly from the internet can be configured to use the SPF protocol to evaluate whether the sending server is an authorized one.
- SPF evaluation should generally not be enabled on servers which are not externally facing as it requires the IP address of the sending server as an input for evaluation.

**Figure 11.1 SPF Authentication Process**

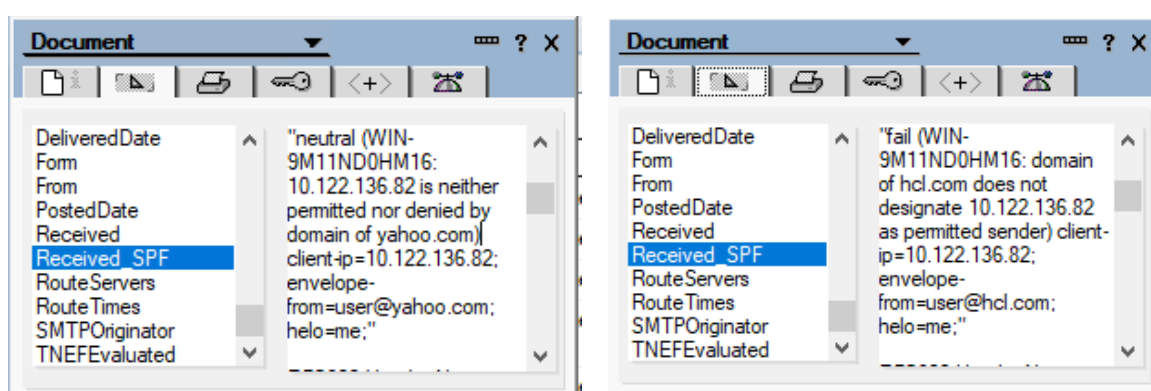


- SPF checking can result in multiple DNS lookups, and thus can potentially impact SMTP server performance. An internal cache is utilized by Domino to reduce this impact.
- A Domino server which does SPF evaluations will add a Received-SPF header to a received message with the results of its evaluation.

**Table 11.1. Possible SPF Evaluation Results**

Result	Reason	Untrusted
None	No syntactically valid SPF policy was found in DNS that could be used to validate the sending server, or no SPF record is published by the domain of the apparent message sender, thus no evaluation is possible.	No
Neutral	The sending domain's SPF policy explicitly states that it is not asserting whether the IP address is authorized.	No
Pass	The IP of the sending SMTP server was validated via the SPF policy published in DNS by the apparent sender's domain.	No
Fail	The IP of the sending SMTP server was not validated through the SPF policy published in DNS by the apparent sender's domain, and the SPF policy explicitly states to treat the sender as not authorized to send mail for the apparent sender's domain.	Yes
Softfail	A "softfail" result is a weak statement by the apparent sender's domain, by means of the SPF policy, that the host is probably not authorized. It did not publish a stronger, more definitive policy that results in a "fail."	No
Temperror	Domino encountered a transient error while performing the check, generally DNS. A later retry might succeed without further action by the apparent sender's domain.	No
Permerror	The apparent sender's domain's published records could not be correctly interpreted. This signals an error condition that requires the apparent sender's domain's intervention to resolve.	Yes

**Figure 11.2. Sample Document Properties**



**NOTE:** This would only cover setting the Domino server to use SPF protocol for inbound SMTP messages. If you want to publish SPF record to the internet, you may reach out to your ISP/DNS vendor for the complete steps.

## Configuring the Domino server to use the SPF protocol.

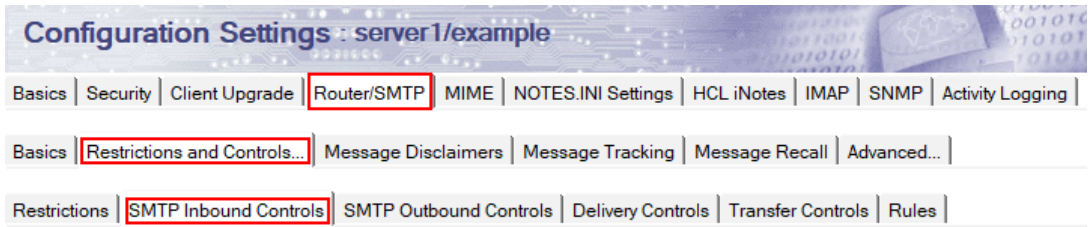
Domino servers that receive SMTP messages directly from the internet can be configured to use the SPF protocol to evaluate whether the sending server is an authorized one.

**Note:** This feature is supported on Windows and Linux.

Steps to configure SPF Evaluation on Domino

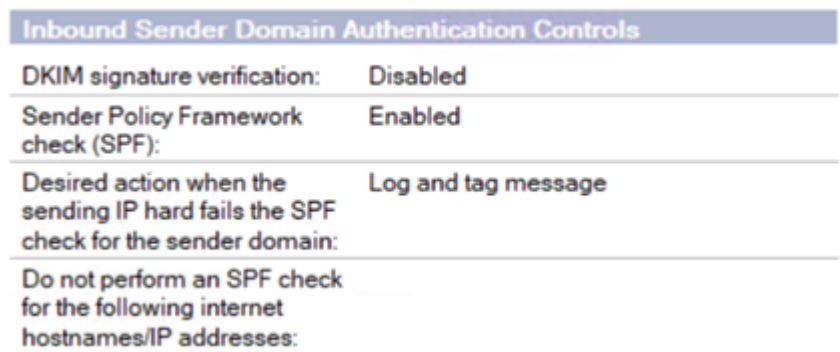
1. Open the SMTP server **Configuration Settings** document, **Router/SMTP** tab > **Restrictions and Controls** tab > **SMTP Inbound Controls** tab.

Figure 11.3. Configuration Settings



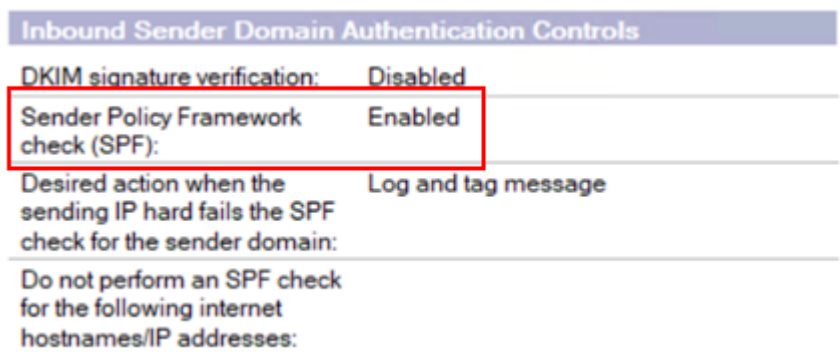
2. Locate the **Inbound Sender Domain Authentication Controls** section (see figure 11.4).

Figure 11.4. Inbound Sender Domain Authentication Controls



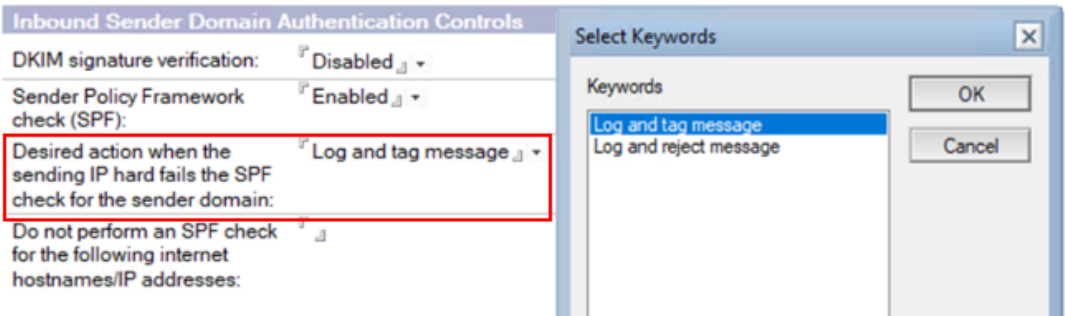
3. In the **Sender Policy Framework check (SPF)** field, change the setting to **Enabled** (see figure 11.5).

Figure 11.5. Inbound Sender Domain Authentication Controls



4. In the **Desired action when the sending IP hard fails the SPF check for the sender domain** field, select the action you wish to take for messages determined to be untrusted as a result of SPF evaluation (see figure 11.6).

Figure 11.6. Inbound Sender Domain Authentication Controls



**Log and tag message** - Outputs a message in the server console, noting the domain and IP address used to determine the failure.

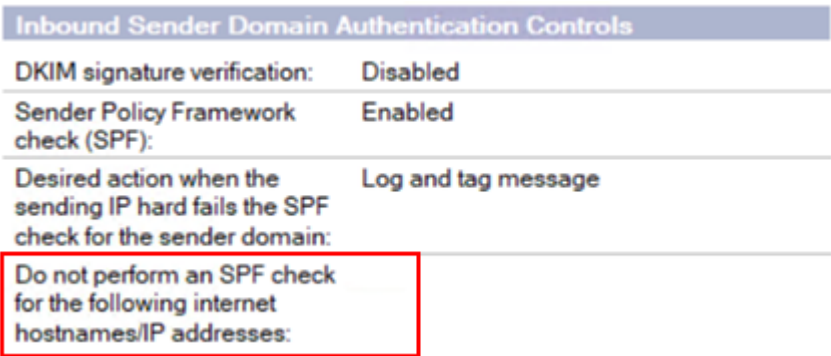
- For example, "SMTP Server: Message will be tagged but allowed. SPF policy for domain example.com does not designate host 10.100.127.35 as a permitted sender." Records the SPF evaluation result status in the Received-SPF header and continues processing the message.

**Log and reject message** - Outputs a message in the server console, noting the domain and IP address used to determine the failure.

- For example, "SMTP Server: Mail rejected for policy reasons. SPF policy for domain example.com does not designate host 10.100.127.35 as a permitted sender."
- Rejects the message in protocol by returning the following message to the sending SMTP server: "554 Mail rejected for policy reasons. SPF policy for domain example.com does not designate host 10.100.127.35 as a permitted sender."

5. If you have internal or trusted external servers from which you receive messages over the SMTP protocol and which you don't want to do SPF checks on, enter the servers in the **Do not perform an SPF check for the following internet hostnames/IP addresses** field (see figure 11.7).

Figure 11.7. Inbound Sender Domain Authentication Controls



## Delivering untrusted mail to the Junk folder

Messages received from external sources can be determined to be untrusted by spam reduction checks such as the Sender Policy Framework (SPF) protocol.

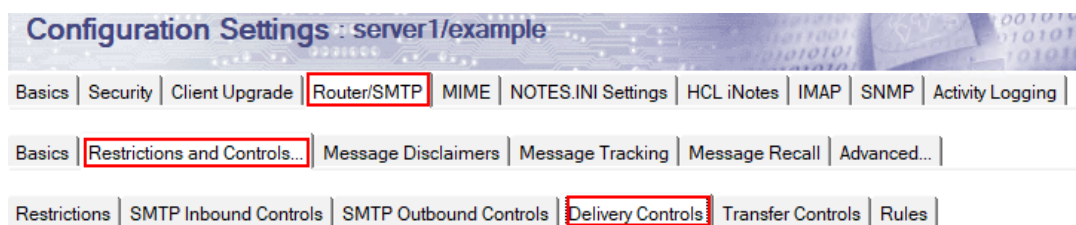
You can choose to send messages that are deemed untrusted as a result of spam reduction checks to the recipient's Junk folder.

All SMTP-inbound Domino edge servers with SPF and/or DKIM enabled must be at 12.0.2 for this feature to work properly.

### Steps:

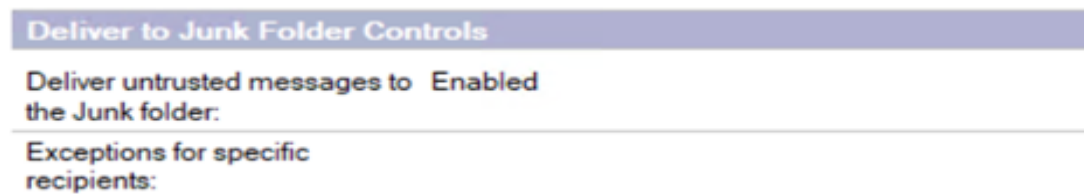
1. Open Domino server **Configuration Document > Router/SMTP > Restrictions and Controls > Delivery Controls**.

**Figure 11.8. Configuration Settings**



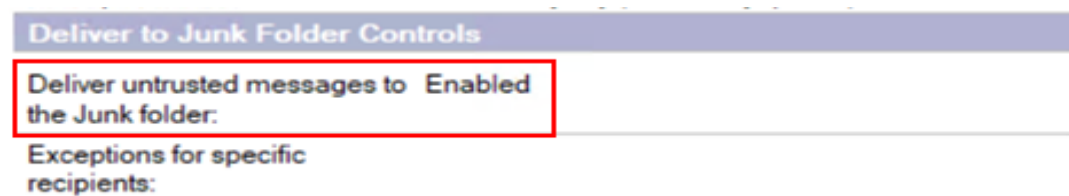
2. Locate the **Deliver to Junk Folder Controls** section.

**Figure 11.9. Deliver to Junk Folder Controls**



3. Set the **Deliver untrusted messages to the Junk folder** field to **Enabled**.

**Figure 11.10. Deliver to Junk Folder Controls**



4. If you have users or groups for whom you don't want to deliver untrusted messages to the Junk folder, enter their Notes names or group names in the **"Exceptions for specific recipients"** field (see figure 11.11).

**Figure 11.11. Deliver to Junk Folder Controls**



**NOTE:** Hard fails are untrusted messages, but if you choose to treat soft fails as untrusted and therefore delivered to the Junk folder, you can enable the following notes.ini on their mail servers:  
**RouterJunkDeliverSoftfail=1**

## 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 HCL Domino from spammers and use DKIM/SPF to make Domino more secure.

## 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.

**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 (HCL 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) HCL 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 might 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, HCL 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. HCL 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. HCL Domino will translate certain English messages returned in NDRs by the router.

The latest Notes.ini variables to be added were introduced in HCL 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.

**RouterJunkDeliverSoftfail=1.** Treats soft fails as untrusted and therefore delivered to the Junk folder.

## Resources

- HCL Software Customer Support Portal:  
<https://support.hcltechsw.com/csm>
- HCL Notes and Domino Community Forums:  
<https://support.hcltechsw.com/community>
- HCL Notes and Domino Fix List:  
[https://ds\\_infolib.hcltechsw.com/ldd/fixlist.nsf](https://ds_infolib.hcltechsw.com/ldd/fixlist.nsf)
- HCL Domino products documentation landing page:  
<https://help.hcltechsw.com/domino/welcome/index.html>

## Legal statements

**This edition applies to version 12.0.2 of HCL Domino and to all subsequent releases and modifications until otherwise indicated in new editions.**

When you send information to HCL Technologies Ltd., you grant HCL Technologies Ltd. a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

**©2023 Copyright HCL Technologies Ltd and others. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with HCL Technologies.

## Disclaimer

**This report is subject to the HCL Terms of Use (<https://www.hcl.com/terms-of-use>) and the following disclaimers:**

The information contained in this report is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied, including but not limited to the implied warranties of merchantability, non-infringement, and fitness for a particular purpose. In addition, this information is based on HCL's current product plans and strategy, which are subject to change by HCL without notice. HCL shall not be responsible for any direct, indirect, incidental, consequential, special, or other damages arising out of the use of, or otherwise related to, this report or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from HCL or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of HCL software.

References in this report to HCL products, programs, or services do not imply that they will be available in all countries in which HCL operates. Product release dates and/or capabilities referenced in this presentation may change at any time at HCL's sole discretion based on market opportunities or other factors and are not intended to be a commitment to future product or feature availability in any way. The underlying database used to support these reports is refreshed on a weekly basis. Discrepancies found between reports generated using this web tool and other HCL documentation sources may or may not be attributed to different publish and refresh cycles for this tool and other sources. Nothing contained in this report is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings, or other results. You assume sole responsibility for any results you obtain or decisions you make as a result of this report. Notwithstanding the HCL Terms of Use (<https://www.hcl.com/terms-of-use>), users of this site are permitted to copy and save the reports generated from this tool for such users own internal business purpose. No other use shall be permitted.