

Draft Information - Subject to change. Updated

[Click Here for DRAFT DOCUMENT DISCLAIMER](#)

DRAFT DOCUMENTS ARE NOT COMMERCIALY AVAILABLE, AND HAVE NOT UNDERGONE THE QUALITY ASSURANCE TESTING LOTUS PERFORMS ON THE VERSION OF KNOWLEDGE BASE WHICH LOTUS MAKES AVAILABLE TO THE GENERAL PUBLIC. CUSTOMER SHOULD ALLOW ACCESS TO DRAFT DOCUMENTS ONLY TO KNOWLEDGEABLE AND TRAINED INDIVIDUALS. **IN LIGHT OF THE FOREGOING, CUSTOMER IS REQUIRED TO BACKUP ALL DATA AND PROGRAMS PRIOR TO USING THE DRAFT DOCUMENTS.** LOTUS WILL NOT PROVIDE ANY SUPPORT OR TECHNICAL ASSISTANCE WITH RESPECT TO ITS USE OF THE DRAFT DOCUMENTS. THE DRAFT DOCUMENTS ARE PROVIDED "AS IS" AND LOTUS MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE DRAFT DOCUMENTS INCLUDING QUALITY, PERFORMANCE, MCERHANTIABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. LOTUS WILL NOT HAVE ANY, AND CUSTOMER ACCEPTS ALL, LIABILITY FOR DIRECT, INDIRECT, TORT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH CUSTOMER'S USE OF THE DRAFT DOCUMENTS OR ANY TECHNICAL ASSISTANCE PROVIDED WITH RESPECT TO THE DRAFT DOCUMENTS, INCLUDING, BUT NOT LIMITED TO, DAMAGES OR COSTS INCURRED AS A RESULT OF LOST PROFITS OR REVENUE, LOSS OF USE OF THE DRAFT DOCUMENTS, LOSS OF DATA , THE COST OF RECOVERING THE DRAFT DOCUMENTS OR DATA, THE COST OF SUBSTITUTES OR CLAIMS BY THIRD PARTIES.



Lotus Software Knowledge Base
Technote

Lotus software

Title: **Enabling TLS/SSL for SMTP**

Product: Lotus Domino > Lotus Domino Server > Versions 8.5, 8.0, 7.0, 6.5, 6.0

Platform(s): AIX, i5/OS, Linux, Linux iSeries, Linux zSeries, Solaris, Windows, z/OS

Edition(s): Advanced, Enterprise, Standard

Date: 07/08/2008

Doc Number: New

Abstract

This tech note covers setting up TLS/SSL for SMTP on your Domino server.

Content

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

Note: Port 465 is no longer registered as SMTP-SSL. It has been deprecated in favor of TLS/SSL over port 25. For more information see:

<http://www.iana.org/assignments/port-numbers>

For more information on obtaining server certificates, see the topic [Setting up SSL on a Domino server](#).

http://www-12.lotus.com/ldd/doc/domino_notes/6.5.1/help65_admin.nsf/f4b82fbb75e942a6852566ac0037f284/399db2be0c0ce2eb85256dff004b312c?OpenDocument

Supporting STARTTLS for outbound SMTP sessions

A Domino server configured to use negotiated SSL for outbound mail connects to the receiving server's SMTP TCP/IP port (port 25 by default). If the initial SMTP response from the receiving server indicates that it supports the STARTTLS extension, Domino issues the STARTTLS command to request the use of SSL to encrypt the rest of the session.

If the receiving server did not advertise support for STARTTLS in response to the Domino server's EHLO command, the sending Domino server continues with an unencrypted SMTP TCP/IP session.

To enable outbound STARTTLS support, set the SMTP outbound TCP/IP port status to: Negotiated SSL.

http://www-12.lotus.com/ldd/doc/domino_notes/6.5.1/help65_admin.nsf/f4b82fbb75e942a6852566ac0037f284/3730ca0f6302df2c85256dff004b1f3d?OpenDocument

Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

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

Supporting STARTTLS for inbound SMTP sessions

You can configure Domino to support the STARTTLS command for inbound SMTP transactions. When a Domino SMTP server is set to use negotiated SSL for inbound sessions, the server advertises support for STARTTLS in response to EHLO commands the TCP/IP port receives from connecting hosts. A connecting host can then issue the STARTTLS command to request an encrypted session.

If Domino is configured to require STARTTLS for SMTP sessions over TCP/IP and a connecting host cannot meet this demand, no mail is sent over the connection.

To enable inbound STARTTLS support:

- Enable the SMTP listener task.
http://www.codestore.net/help/help6_admin.nsf/b3266a3c17f9bb7085256b870069c0a9/059f91a614a2f9a885256c1d00395447?OpenDocument
- Enable the SMTP inbound TCP/IP port.
http://www.codestore.net/help/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/15bf31c241ebdbe585256c1d00395b14?OpenDocument
- Enable the STARTTLS ESMTP extension. This causes Domino to advertise STARTTLS as one of its supported extensions in the ESMTP EHLO greeting response.
http://www-12.lotus.com/idd/doc/domino_notes/6.5.1/help65_admin.nsf/b3266a3c17f9bb7085256b870069c0a9/24ea7d6c3dfbcfa185256dff004b1fe3?OpenDocument

[Basics](#) | [Security](#) | [Client Upgrade](#) | [Router/SMTP](#) | [MIME](#) | [NOTES.INI Settings](#) | [Domino Web Access](#) | [IMAP](#) | [SNMP](#) | [Activity Lc](#)

[Basics](#) | [Restrictions and Controls...](#) | [Message Disclaimers](#) | [Message Tracking](#) | [Message Recall](#) | [Advanced...](#)

[Journaling](#) | [Commands and Extensions](#) | [Controls](#)

Inbound SMTP Commands and Extensions		Outbound SMTP Commands and Extensions	
SIZE extension:	Enabled	SIZE extension:	Enabled
Pipelining extension:	Enabled	Pipelining extension:	Enabled
DSN extension:	Enabled	DSN extension:	Enabled
8 bit MIME extension:	Enabled	8 bit MIME extension:	Enabled
HELP command:	Disabled		
VRFY command:	Disabled		
EXPN command:	Disabled		
ETRN command:	Disabled		
SSL negotiated over TCP/IP port:	Enabled		

Note: Setting the SSL negotiated over TCP/IP port to required would force any sending server to use only TLS/SSL. It is suggested to set this setting to Enabled. This feature may not be enabled on sending servers and could result in a loss of incoming mail to your Domino server.

© 2008 IBM Corporation. All rights reserved.
 Material may not be reproduced or distributed in any form without permission.