



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials Bootcamp Style (Security 401)"  
at <http://www.giac.org/registration/gsec>

# Locking Down a Lotus Domino Server

Andrew G. Hargreave, III

December 7, 2000

## Introduction

In the following paper I will be discussing the basics of locking down your Lotus Domino R5 server. I'll discuss access control lists, templates and server databases, internet ports used, and settings on the server configuration document that control access.

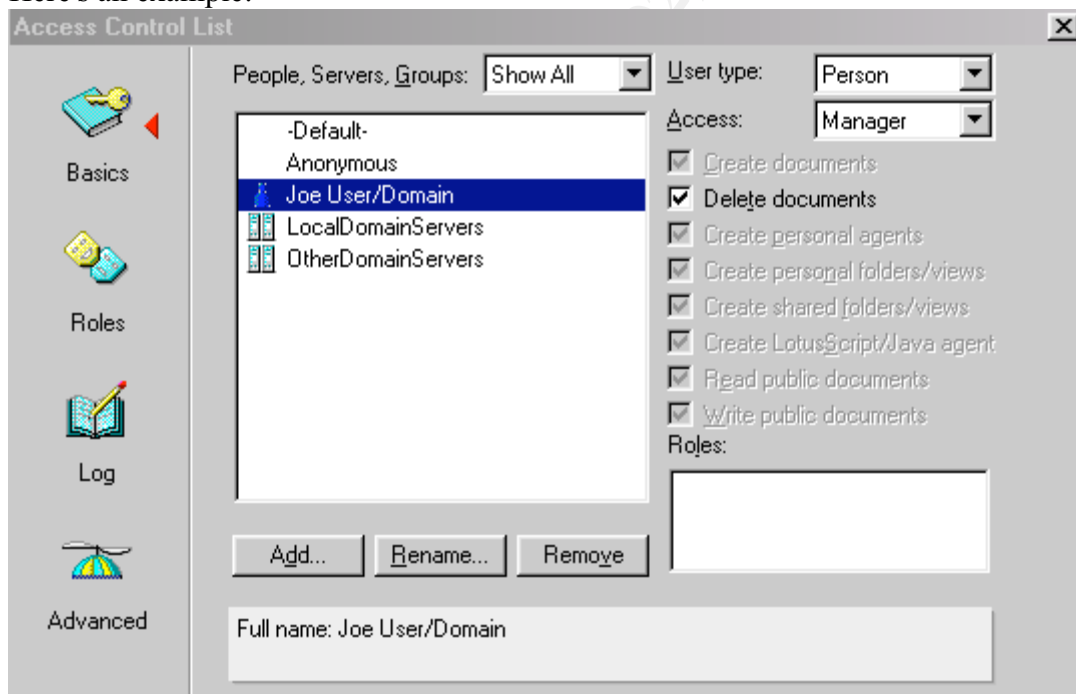
## What is Lotus Domino?

Lotus Domino ([www.lotus.com](http://www.lotus.com)) is the industry leading group collaboration and messaging platform used by over 60 million users around the world. Lotus Notes/Domino has been around since the 1980's and its user base continues to grow at a very brisk pace. Notes/Domino's extreme power comes from its flexibility, programmability, and diverse platform support. However, an incomplete understanding of the architecture of Domino network can leave very severe holes into your network.

## What is an Access Control List?

The Access Control List (or ACL) is what determines who can gain access to a file on the Domino server. ACL's are set on template files and each database on the server.

Here's an example:



The defaults on the template files on a freshly installed Domino server usually have the -Default- access set to Manager or Designer. On newer versions of Domino (Release 5.05 and up), Lotus has started setting them to 'No Access' which is much more secure.

It's important to check the ACL on templates to make sure they contain two users:  
[-Default-] with a setting of 'No Access'.

[Anonymous] set to type 'Person' and 'No Access'

The '[ -- ]' users on template files will be automatically set when new databases are created based on that template. The **Default** is the default access to the database. The proper setup on databases is that you will have Groups setup with your users in them and then you put the group in the ACL and set the -Default- access to 'Access' to ensure the most security. If you have Default set to anything else, then anyone would be able to open the file.

The **Anonymous** user is really only used when you allow your Domino databases to be accessed from a web browser via the HTTP service built into Domino. The **Anonymous** user when set to 'No Access' tells Domino to pop up a user login screen on the browser and the users are required to enter in their Notes user name and internet password to gain access. An important point to note is that in a mixed Notes client/Web browser environment, each user will have two passwords; their Notes User.ID password and a separate internet password that is set on their person record in the Domino Master Address Book. More information can be found in the Domino 5 Administration Help file

(<http://notes.net/notesua.nsf/a08df36b2299a8bc8525665d006dce40/69f5e7de5964365e8525673e00491995?&nDocument>)

### **Important Templates and Databases to secure.**

When Domino is installed, templates and default databases are installed in the "data" directory. Here is a brief list of the files and template that need to have the Default access removed:

- Admin4.ntf / Admin4.nsf (Administration events on your server)
- Catalog.ntf / Catalog.nsf (Catalog of all databases on the system)
- Certlog.ntf / Certlog.nsf (Tracks user & server certifications)
- Csrv50.ntf
- Da50.ntf (Directory Assistance file)
- DecsAdm.ntf / DecsAdm.nsf
- DirCat5.ntf
- DolAdmin.ntf / DolAdmin.nsf (Domino Offline Service Administration)
- DomLog.ntf / DomLog.nsf (web accesses are logged here)
- Events4.ntf / Events4.nsf (server monitoring)
- Log.ntf / Log.nsf (all server events are listed here)
- PubNames.ntf / Names.nsf (Master list of servers, users and groups. The keys to the kingdom.)
- Resrc50.ntf / Resource.nsf
- StatRep50.ntf / Statrep.nsf (Server statistics reporting)
- Webadmin.ntf / Webadmin.nsf

One thing to remember when updating the ACLs on these files: the server usually has these files open when it's running. First, you will have to shut down your server. From a Notes client installed on a workstation, mount a drive to the server and open the files locally to change the ACLs. This is well worth the down time to correct. Access to any of these files by unauthorized users can provide very detailed information about your Domino server and give them a roadmap into your infrastructure.

### **TCP Ports used by Domino.**

Domino offers full internet standards support for all the main protocols and services. Domino supports:  
SMTP for mail delivery – tcp port 25

NNTP for newgroups – tcp port 119  
IMAP & POP3 for mail services – tcp ports 143 and 110 respectively  
LDAP for directory services – tcp port 389  
HTTP for browsers – tcp port 80  
Notes Remote Protocol NRPC for Notes clients connecting to a server – tcp port 1352.  
IIOP – tcp port 63148

Domino also has full SSL support on all the protocols above. As with any server that is on the public internet or a private intranet, only run the services that you actually need. For example, if you don't need LDAP or NNTP don't load them on your server, as they are just one more doorknob for a would-be-cracker to check.

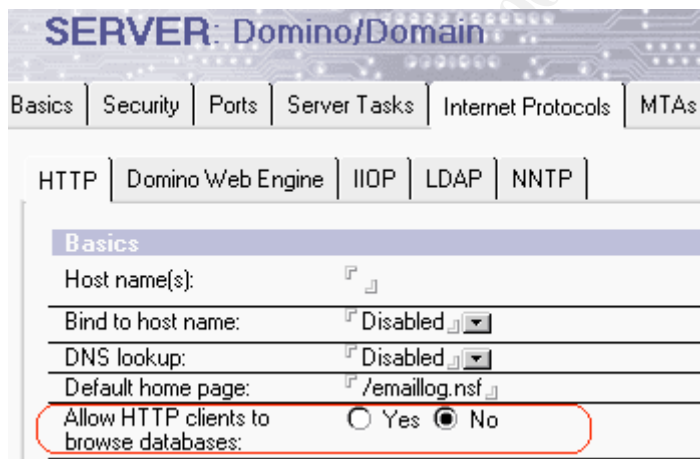
### Security Settings on the Server Configuration Document.

Most of the configuration settings on a Domino server are stored in the server document in the Public Address Book on the server. The key settings to check are circled in red below:

The “Allow anonymous Notes connections” setting prevents unauthorized Notes clients from accessing the server.

The “Only allow server access to users listed in this Directory” setting ensures that only users with valid entries in the directory can access server resources.

ALWAYS create a “Deny Access” group for holding former employees or clients who may have possession of a once valid user.id file. Then put this group name in the “Not access server” field so that they will be locked out.



On the Internet Protocols/HTTP tab, make sure to set “Allow HTTP clients to browse databases” to “No” so that non-authorized users cannot see the file names of the databases on your server.

There are other security measures that can be implemented in the Server Configuration document, but that would require its own whitepaper as they involve settings for lotuscript/javascript, java applets, etc.

This concludes my paper on the basics of locking down a Lotus Domino server. I hope you use the information I have provided to secure your Domino network or at least make you review your settings again. The references below discuss these and other issues in much more detail than I do and deserve your review.

**References:**

"Securing the Domino Environment". Notes Net URL:

<http://notes.net/lbytes.nsf/308c971706adfdef8525640500696fa8/478baef79d90f56d85256817000eb1f5?OpenDocument>

"Implementing and Maintaining Domino Web Servers". Notes Net URL:

<http://notes.net/lbytes.nsf/308c971706adfdef8525640500696fa8/f668d51aaa7db800852568480071482f?OpenDocument>

"Domino 5 Administration Help". Notes Net URL:

<http://notes.net/notesua.nsf/a08df36b2299a8bc8525665d006dce40/69f5e7de5964365e8525673e00491995?CnDocument>

"Falling Dominos": Trust-Factory (July, 2000) URL:

<http://www.trust-factory.com/Falling-Dominos-FAQ-1.0.html>

Lotus Notes and Domino R5.0 Security Infrastructure Revealed. IBM, USA (May, 1999) URL:

<http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245341.pdf>

© SANS Institute 2000 - 2002 Author retains full rights.

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS