

# Full Access Administration – Is it a threat in your Domino Environment?

Find out how you can use SecurTrac to monitor usage of Full Access Administration in HCL Domino.

## Full Access Administration – Is it a threat in your Domino Environment?

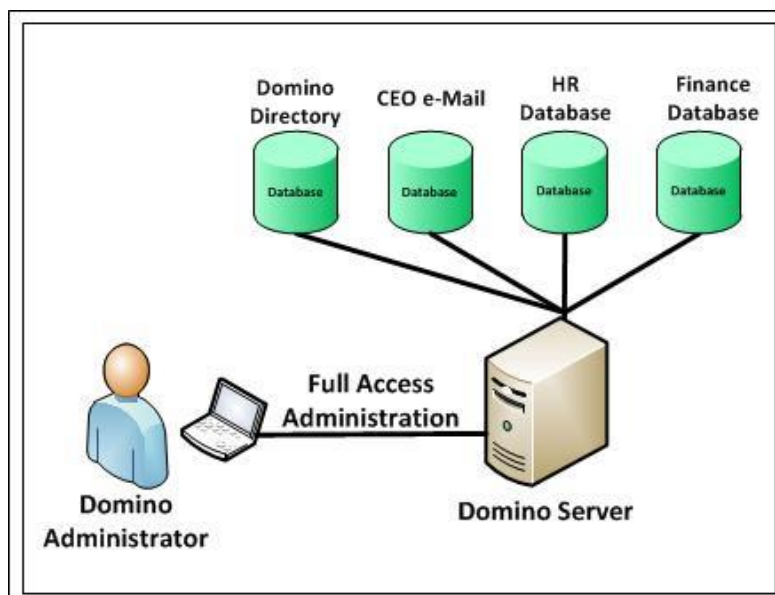
The Full Access Administration privilege is a very useful and powerful security privilege which allows HCL Domino Administrators to correct many administration related problems such as misconfigured database ACLs, Domino Directory issues and user mail database problems. The Full Access Administration privilege is so powerful in fact; that it can actually be used to circumvent HCL Domino server security and allow Domino Administrators to access and possibly make changes to Domino server configurations and even user mail database and/or application database content, without authorization.

With corporate governance and regulatory compliance being more prominent in companies, is yours able to account for each administrator's actions while the Full Access Administration privilege is active? If an audit was to be performed, are you able to provide detailed logging of everyone's activity? How can we control and audit this very powerful tool?

Have you ever wondered what exactly your Domino Administrators are doing when they invoke the powerful Domino server Full Access Administration privilege? Though every IT employee likely has a clause in their employment contract which states that they will never abuse their powers which might allow them to access information for which they are not authorized, how do you really know if employees are complying? Companies put a trust into their employees, fully expecting them to comply with company data access policies. Even with employment contracts and employee trust, this brings to light some very important questions:

### **Could they be using Full Access Administration to .....**

- 1) access the e-mail database of the CEO or another high profile executive? What are they doing while they are in there? Reading confidential email?, Deleting e-mail? Sending e-mail? or even altering the content of existing e-mails?
- 2) access the Domino Directory and make unauthorized changes to Person documents, Group documents or even Server configurations?
- 3) get access to Domino applications databases to Create, Open, Update or even worse Delete documents without authorization?
- 4) make unauthorized database ACL changes?



The fact of reality is in many cases who really knows what it is that they are doing when using Full Access Administration?

While HCL Domino does allow you to log every time someone invokes the Full Access Administration privilege, what the basic logging mechanism does not provide is a full audit trail of the specific actions that were invoked while the Full Access Administration privilege was activated.

Extracomm's SecurTrac product fills this void and provides detailed audit trail logging of what exactly the Domino Administrator did while the Full Access Administration privilege was being used.

With SecurTrac you can.....

- Log Full Access Administration activity in Mail databases, Domino application databases as well as the Domino Directory for Create, Open, Update & Delete actions.
- Log the simple fact that a database was opened, even if no documents were ever accessed. This is especially important since every database has a default view, where document information is displayed in view columns, potentially exposing confidential information without someone ever needing to open a database document.
- Log exactly which database views were accessed in a particular database while using Full Access Administration.

### SecurTrac Monitor Configuration

**Database Monitor**  
Created: 10/31/2012 08:16:54 AM EDT

Basics | Monitor | Report | Administration

**Database to Monitor**

File/Folder name: Employee.nsf

Exclude File(s)/Folder name(s):

**People to Monitor**

Monitor the following people's action only: (e.g. User1/Extracomm, \*/Extracomm, GroupA)

People: Administrators

AND the people are using Full Access Administration privilege

Server(s):

All in the domain

Only the following:

Server01/Thunder Servers...

**Description**

Description (Optional):

Monitor HR Database

## SecurTrac Log - Detected Usage of Full Access Administration

### Action Details

<b>Initiator :</b>	Billy Black/Thunder	<b>Time :</b>	04/28/2022 03:19:44 PM EDT
<b>Short Name:</b>	BBlack	<b>Database Path:</b>	Employee.nsf
<b>Database Title:</b>	Employee Record Database	<b>Action :</b>	Open
<b>Form :</b>	FEmployee	<b>Last Updated Time :</b>	04/28/2022 03:19:41 PM EDT
<b>Document ID :</b>	OFC98660F:EE0BD196-ON852579F8:005D01C3	<b>Used Full Access Admin privilege:</b>	Yes
<b>Last Updated By :</b>	Billy Black/Thunder		
<b>Triggered by Monitor :</b>	Monitor HR Database		

### Connection Details

<b>Service :</b>	nserver	<b>Address :</b>	192.168.2.133:61045
<b>Port Name :</b>	TCPIP		

### Document Details

Monitor Fields | RichText | Attachment

Field Name	Value
Comments	New VP of Sales
EmpDateOfBirth	11/08/1990
EmpDateOfHire	05/08/2012
EmpLeave	0
EmpName	Paul Waters
EmpNo	43563
EmpSalary	99000
EmpSickLeave	0
Form	FEmployee
RichText	
RichText2	

To learn more about how SecurTrac can help monitor the use of Full Access Administration within your Domino environment, please visit our web site <http://www.extracomm.com/SecurTrac/>.



Extracomm Inc.

1730 McPherson Court Unit 6

Pickering, Ontario

Canada, L1W 3E6

Tel: 905-709-8602

Fax: 905-709-8604

<http://www.extracomm.com>

*Product names, logos, brands, and other trademarks featured or referred to within this document are the property of their respective trademark holders.*