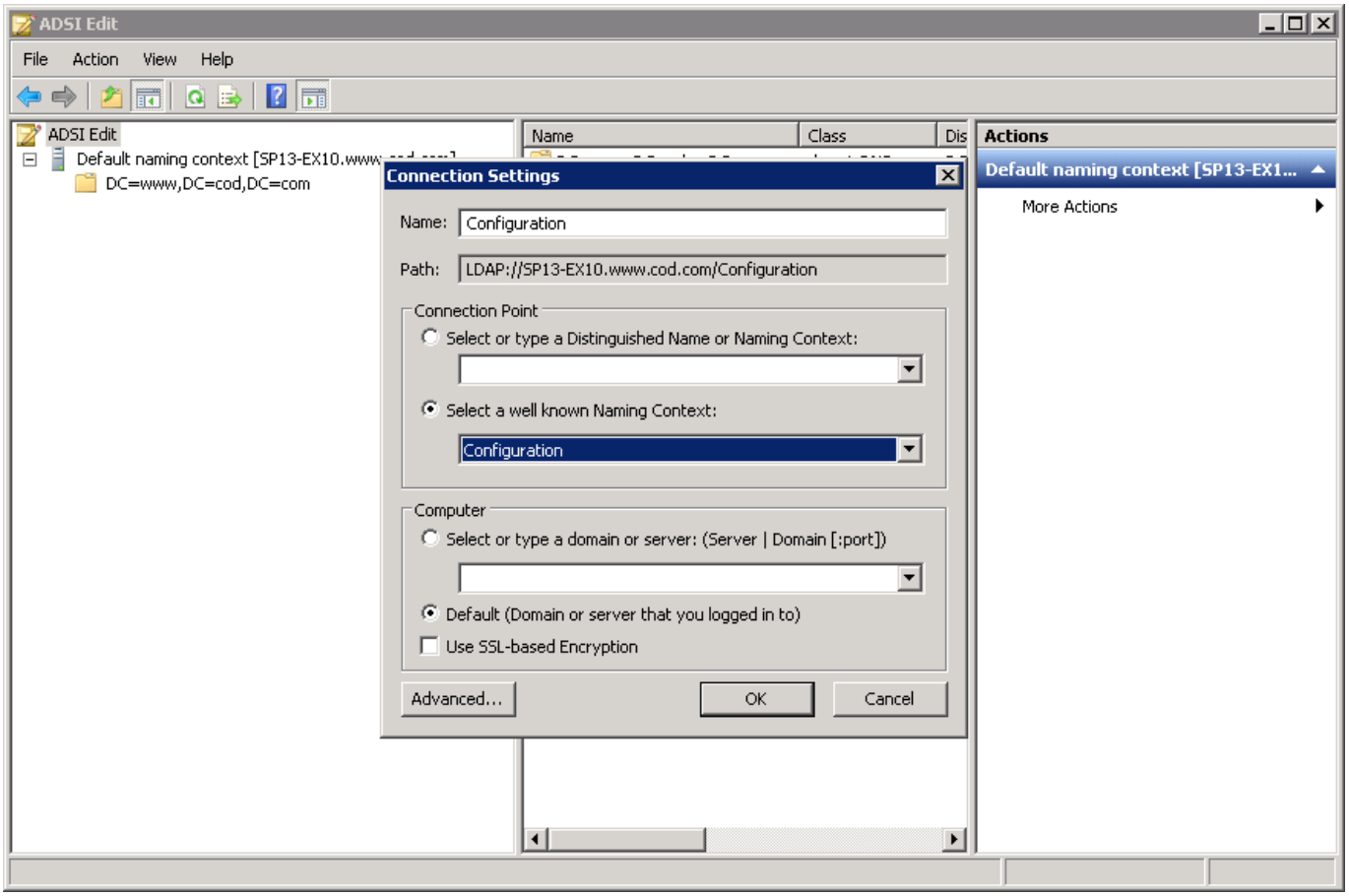

Figure 21: Connecting to Root Configuration

10. It connects ADSI Edit to the Domain Configuration and displays its root node in the Left Panel.
11. Expand the node to access "CN=Configuration,DC=www,DC=domain,DC=com".
12. Right click on "ADSI Edit" parent node and select "Connect To".
13. Select "Schema" as the naming context and click "OK" to connect to it.

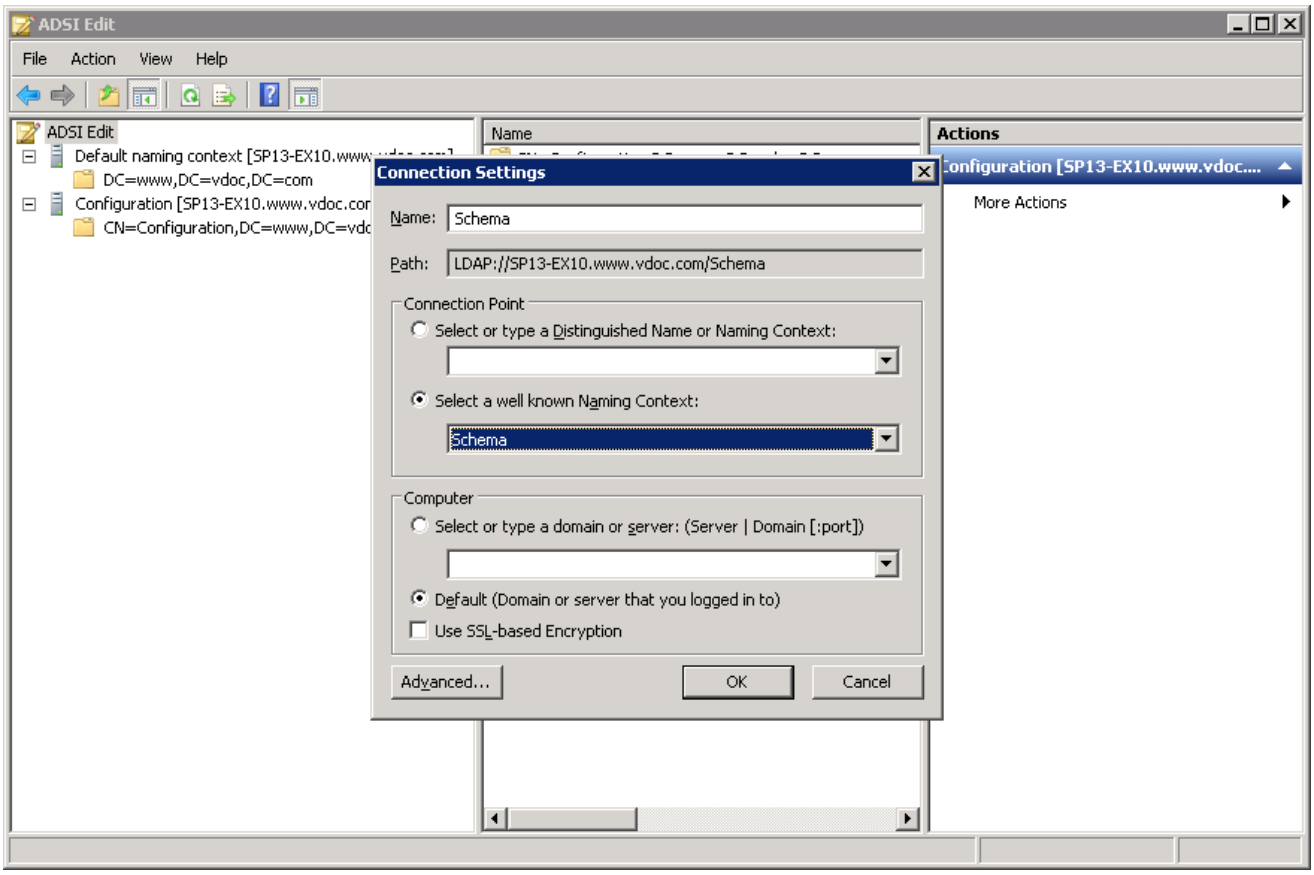

Figure 22: Connecting to Schema

14. It connects ADSI Edit to the Schema and displays its root node in the Left Panel.
15. Expand its node to access "CN=Schema,CN="Configuration,DC=www,DC=domain,DC=com".
16. Now, it is required to enable the auditing settings for the following four root nodes of different naming contexts.
    a. DC=www,DC=domain,DC=com
    b. CN=Configuration,DC=www,DC=domain,DC=com
    c. CN=Schema,CN=Configuration,DC=www,DC=domain,DC=com
17. The user has to perform the following steps one by one for each of the above nodes.
    a. Right click on "DC=www,DC=domain,DC=com" under "Default Naming Context".

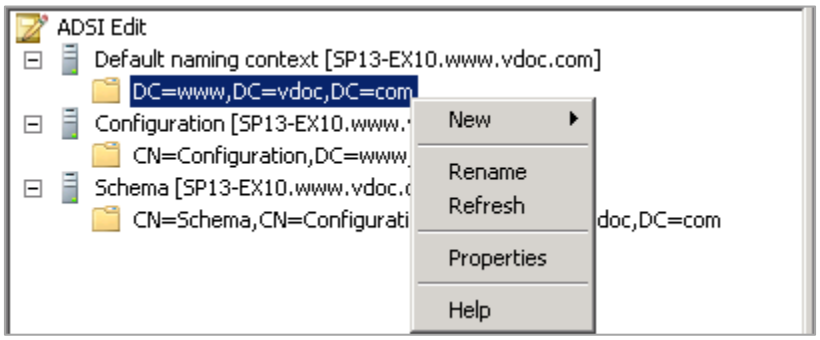

Figure 23: Right click on root node of Default Naming Context

b. Select "Properties" option to access its properties.

c. Switch to "Security" tab.

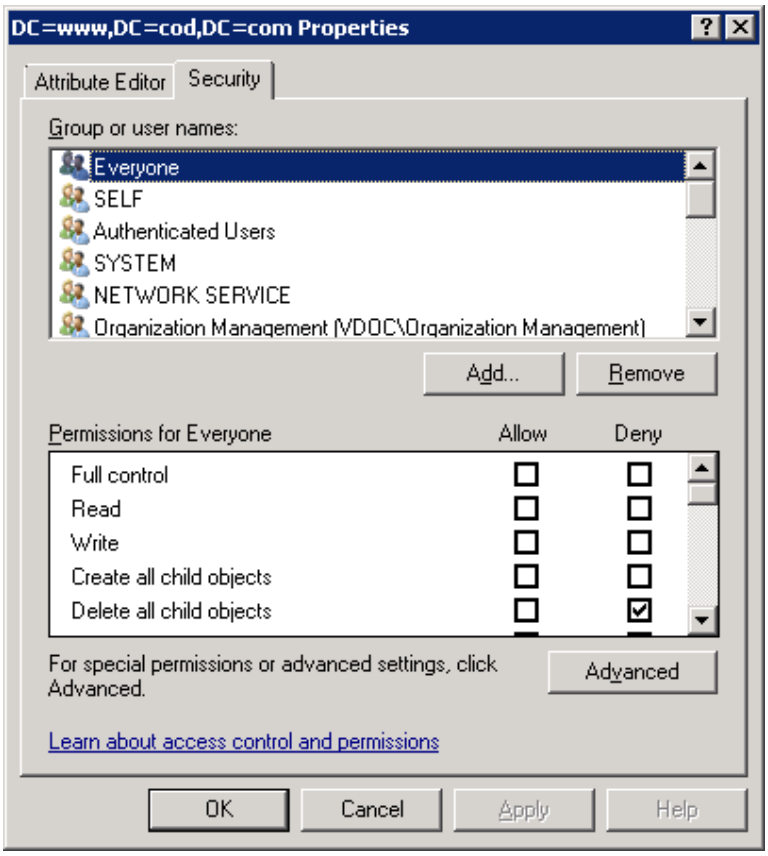

Figure 24: Security Tab of Node Properties

d. Click "Advanced" button to access the Advanced Security settings.

e. Switch to "Auditing" tab in "Advanced Security Settings".

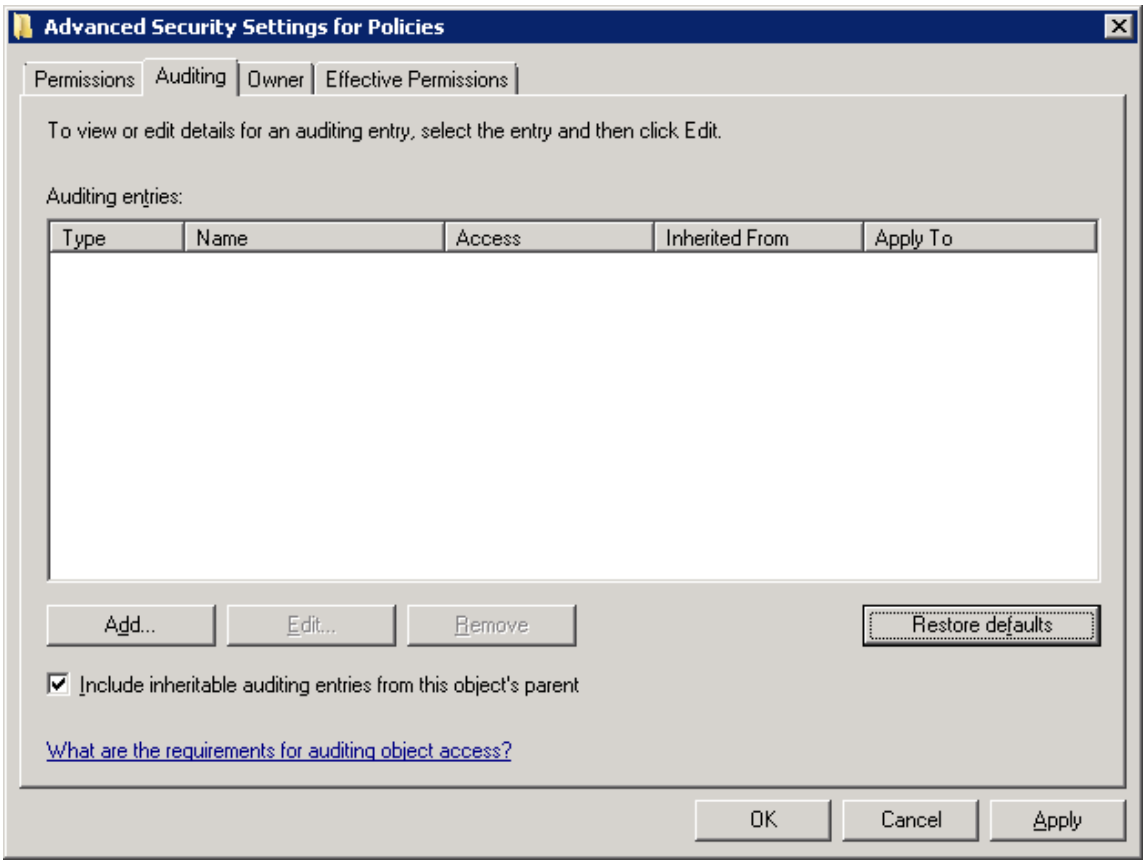

Figure 25: Auditing tab

f. Click "Add" to add "Everyone" for auditing using the following box:

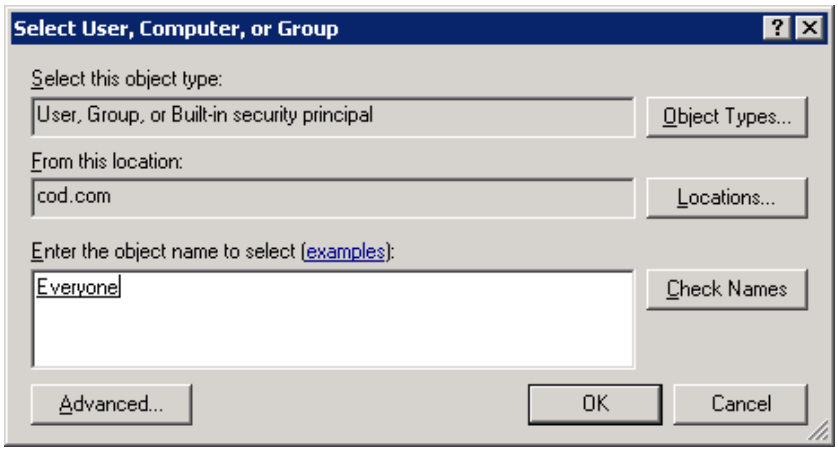

Figure 26: Add User

g. Type “Everyone” to audit the changes made by all objects.

h. Click “Check Names” to verify the username.

i. Click “OK” to add the user. It shows “Auditing Entry” dialog box.

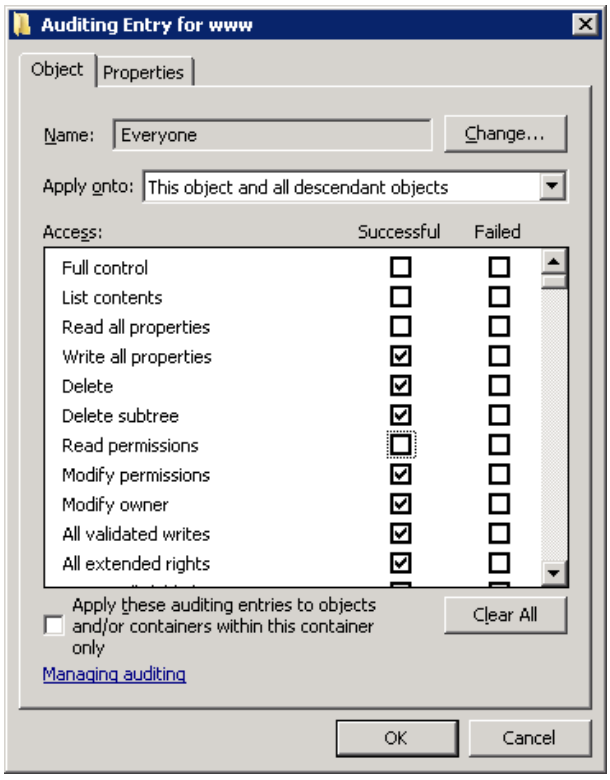

Figure 27: Auditing Entries for www

j. Select "This object and all descendant objects" in "Apply onto" drop-down menu.

k. Click “Full Control” in “Successful” column first.

l. Now, you have to uncheck the following entries in “Successful” column.

- Full Control
- List contents
- Read all properties
- Read permissions

Keep other entries checked in “Successful” column.

m. Make sure all checkboxes in “Failed” column are blank or not checked.

n. Keep "Apply these auditing entries to objects and/or containers within this container only" unchecked.

o. Click “OK” to apply the auditing entries. It takes you back to “Auditing” tab of Advanced Security Settings.

p. Click “Apply” and “OK” to apply the auditing settings.

q. Close “Properties”.

18. Repeat the steps (a) to (q) of Step 17 to enable the auditing of remaining root nodes.

a. CN=Configuration,DC=www,DC=domain,DC=com

b. CN=Schema,CN=Configuration,DC=www,DC=domain,DC=com

19. Close the window of ADSIEdit.msc.

5. Restore Backed up Group Policy

While enabling the auditing, LepideAuditor lets you select an existing Group Policy or create a new one. If you are selecting an existing Group Policy, the solution allows you to take its backup. The backup is created on the server in "%systemdrive%\Windows\Lepide\GPOBKP_24-01-2017 18_13_35\" folder. Here, 24-01-2017 will be replaced with the date and 18_13_35 will be replaced with the time when you have clicked "OK" to enable auditing on the selected policy.
You can perform the following steps to restore the Group Policy using this backup to restore to its earlier state before enabling the auditing.

1. Go to "Start" → "Administrative Tools" → "Group Policy Management Console" to access its console.
2. In the left panel of "Group Policy Management Console", browse to "Forest" → "www.domain.com".
3. Right click on "Group Policy Objects" node and click "Manage Backups" option.

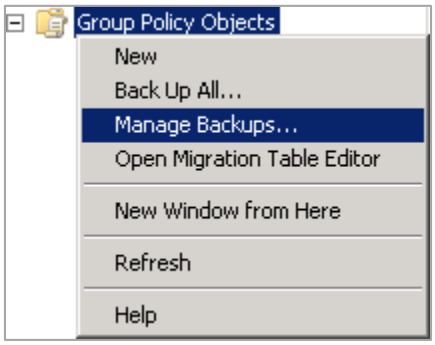

Figure 28: Option to manage the Group Policy Backups

4. "Manage Backups" dialog box appears on the screen.

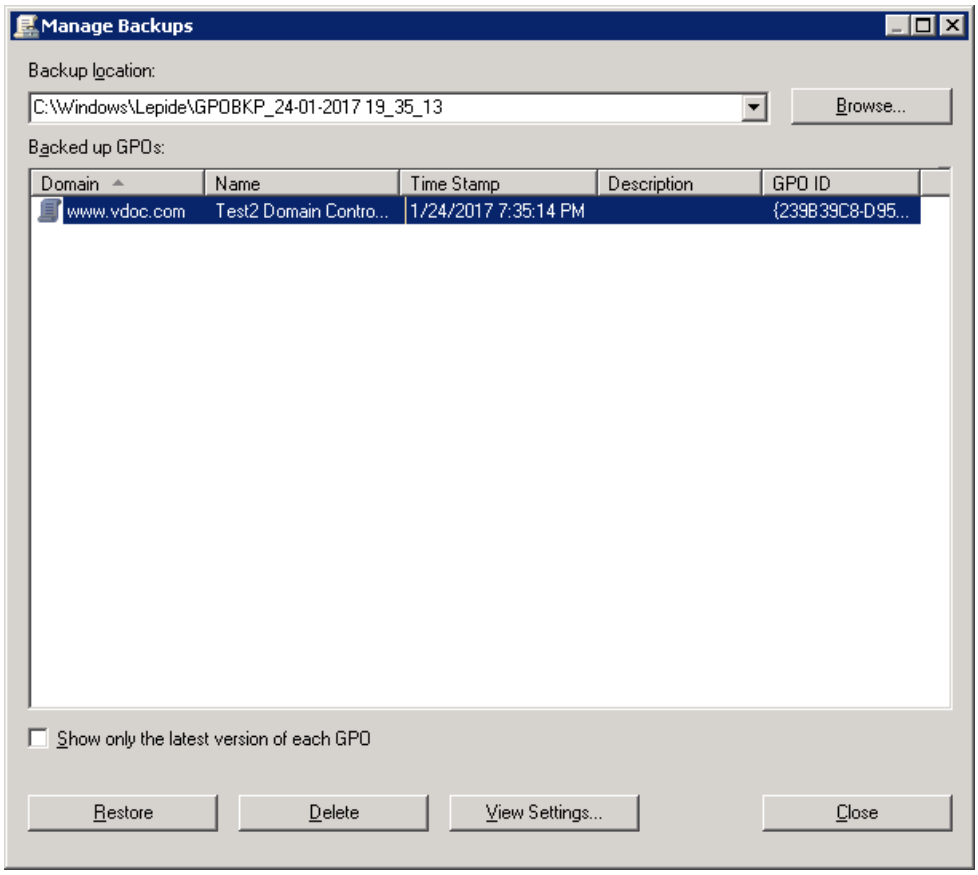

Figure 29: Manage the backups of Group Policies

5. Click "Browse" and open "%systemdrive%\Windows\Lepide" folder.
6. Now select "GPOBKP_*" folder of that date and time when you have selected to create the backup while enabling the auditing.
7. Click "OK". It takes you back to "Manage Backups" dialog box that shows the Group Policy from the selected backup.
8. You can click "Restore" to restore this backup.

6. Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

Product experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit http://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com support@Lepide.com

To read more about the LepideAuditor, visit http://www.lepide.com/lepideauditor/.

7. Copyright

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data and materials, this guide, and other documentation are copyright of Lepide Software Private Limited, with all rights reserved under the copyright laws. This user guide cannot be reproduced in any form without the prior written permission of Lepide Software Private Limited. No Patent Liability is assumed, however, on the use of the information contained herein.

8. Warranty Disclaimers and Liability Limitations

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data, and materials are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where these are installed. You acknowledge that good data processing procedure dictates that any program, listed above, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of LepideAuditor and the above listed accompanying programs covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In no event does Lepide Software Private Limited authorize you or anyone else to use LepideAuditor and the above listed accompanying programs in applications or systems where LepideAuditor and the above-listed accompanying programs' failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

9. Trademarks

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, LepideAuditor for Active Directory, LepideAuditor for Group Policy Object, LepideAuditor for Exchange Server, LepideAuditor for SQL Server, LepideAuditor SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.