LepideAuditor

Enable Auditing Manually

Contents

1. Introduction

Welcome to the Installation and Configuration Guide for LepideAuditor. This solution provides a comprehensive means of auditing Active Directory, Group Policy, Exchange Server, SharePoint, SQL Server, and File Server.

This guide helps you manually enable domain auditing. If you have any questions at any point in the process, you can contact our Support Team. The contact details are mentioned at the end of this document.

2. Enable Auditing Automatically

While adding a domain, after you provide the appropriate details, LepideAuditor shows the following dialog box to enable auditing at the domain level automatically.

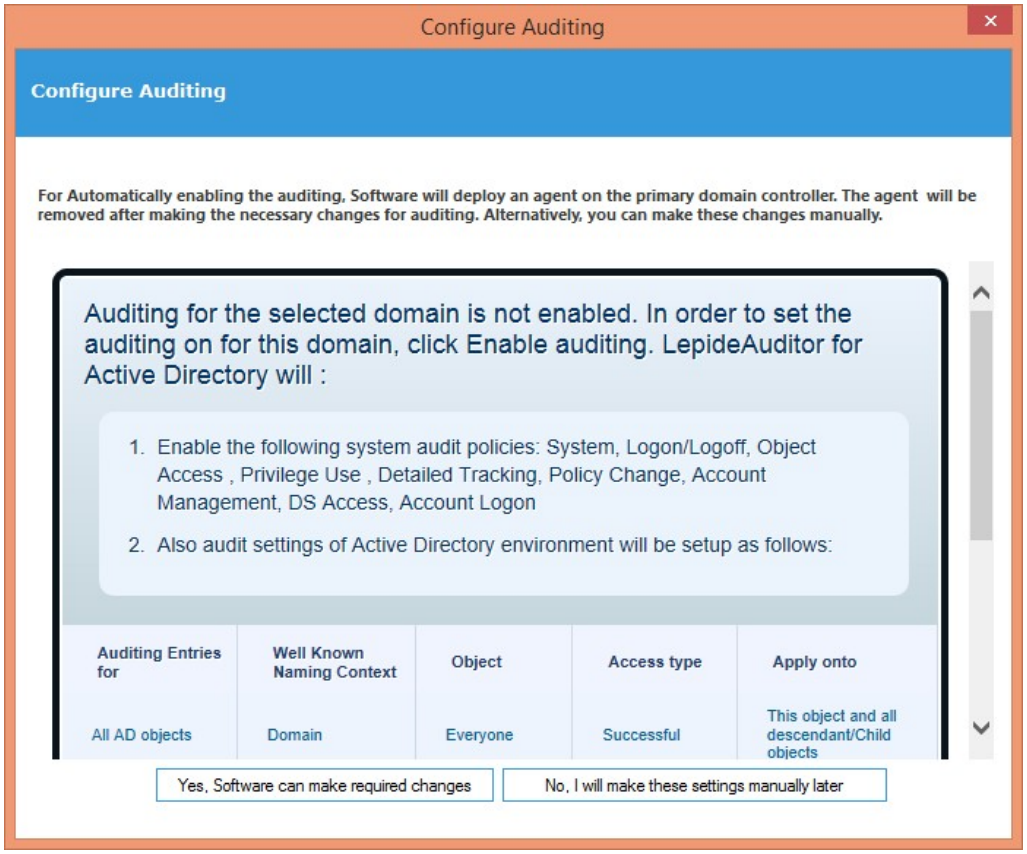

Figure 1: Option to enable auditing automatically

While modifying the properties of an already added domain, "Enable Audit" option appears for "Domain Credentials" property.

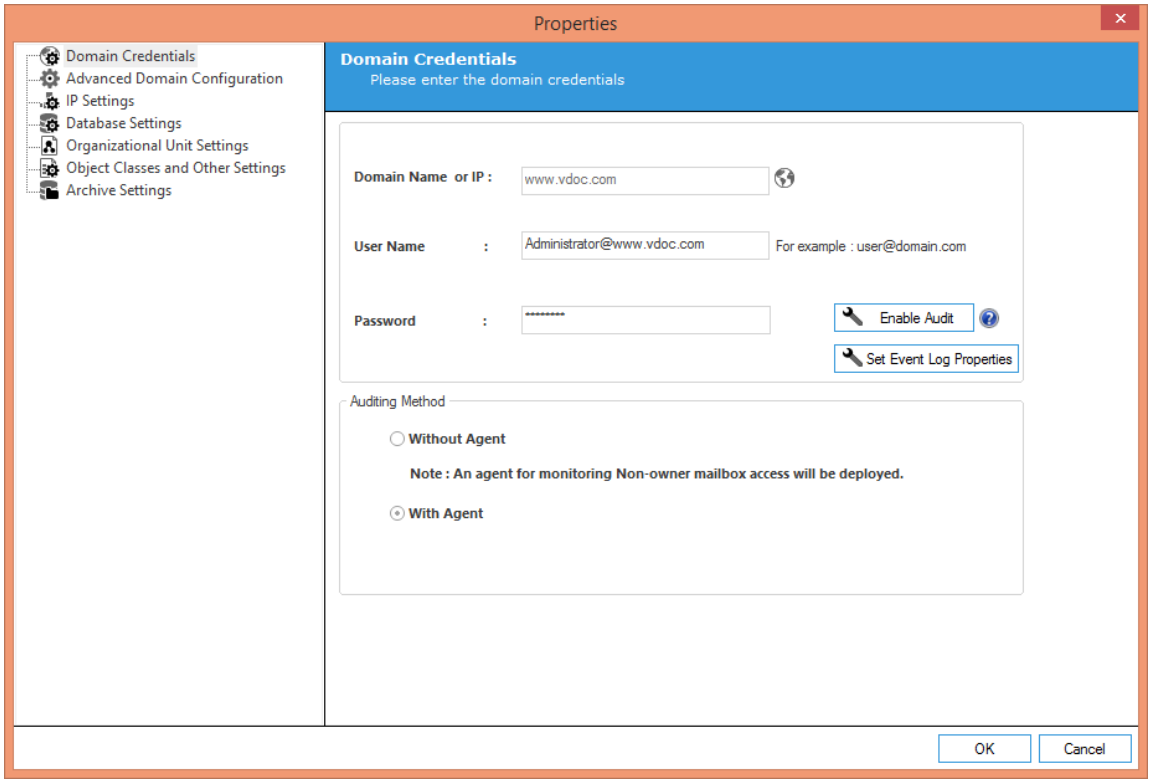

Figure 2: Modifying an already added domain

You can click Yes, Software can make required changes button. It displays the following dialog box.

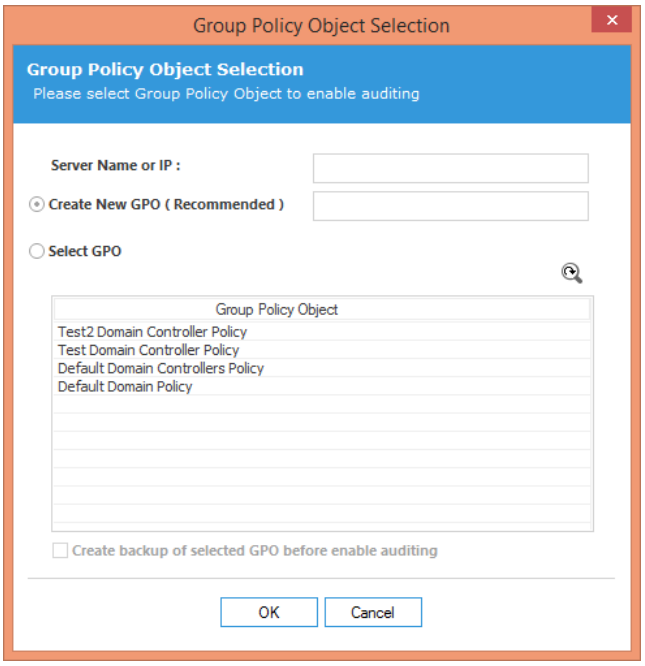

Figure 3: Enable Auditing

Enter either IP Address of the primary domain controller or name of the domain. Select any of the following options.

1. Create New Policy (Recommended): Select it to create a new Domain Controller Policy. Once selected, you have to provide the name of new Group Policy to be created.

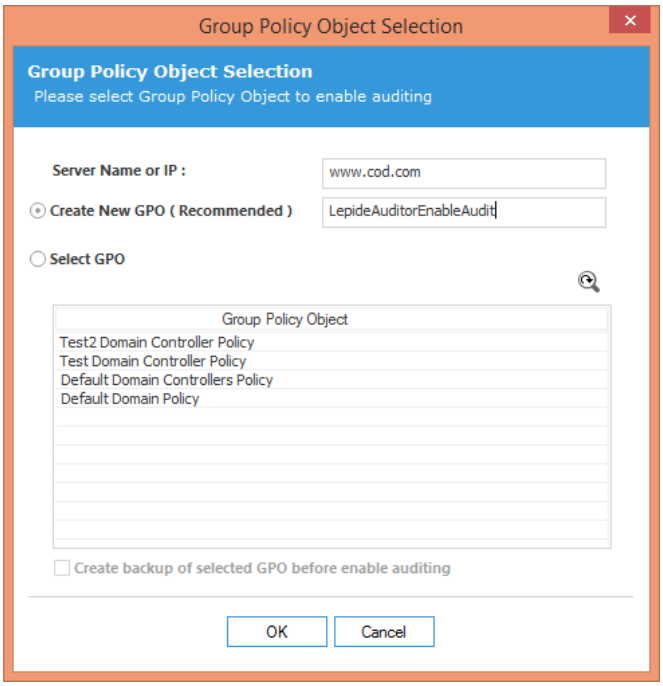

Figure 4: Creating new Group Policy

   Click "OK" to create a new Group Policy at the domain to enable the auditing.

2. Use Selected Domain Controller Policy: This option lets you select a domain controller policy to enable the auditing. Select this option to enable its section.

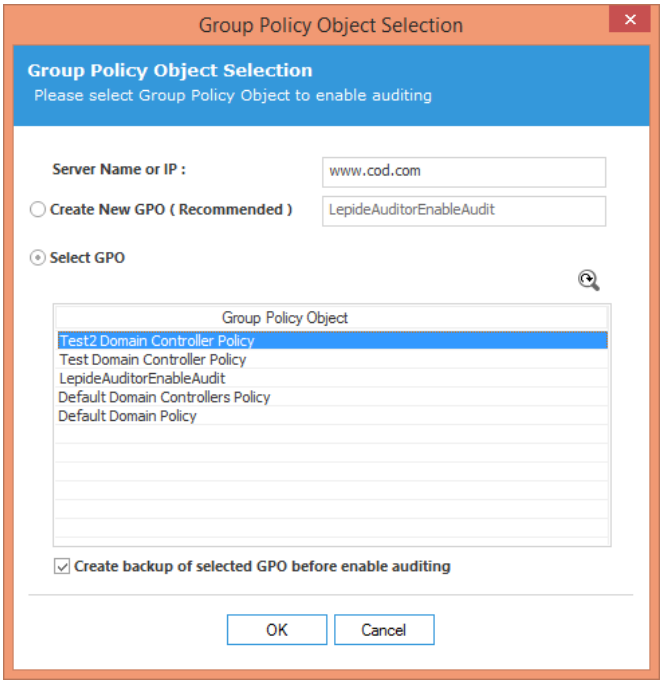

Figure 5: Select a GPO

Perform the following steps to select an existing Group Policy.

A. If a Group Policy is not listed here, you can click icon to rescan the domain for listing the updated set of Group Policies.

B. You cannot select "Default Domain Controller Group Policy" or "Default Domain Group Policy" to enable the auditing using LepideAuditor. If you try, the following error message appears on the screen.

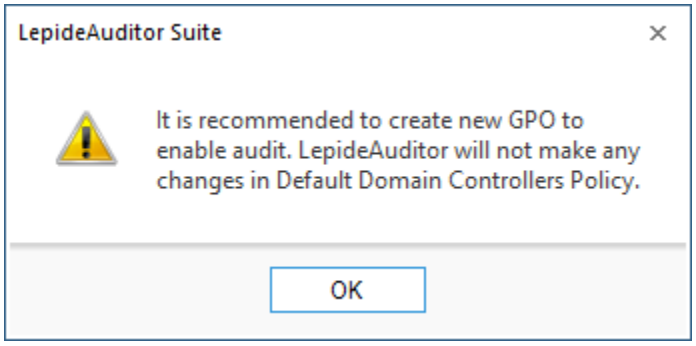

Figure 6: Error message while enabling auditing at Default Domain Controller Policy

C. Select a custom Group Policy created at the Domain Level or Domain Controller Level upon which the auditing setting has to be applied.

D. Please make sure to check "Create backup of selected GPO before enable auditing" box if you are enabling the auditing on an existing Group Policy. This backup allows you to restore the previous default Domain Controller Policy if any issue persists after enablingthe auditing.

It is recommended to create a new Domain Controller Policy to enable the auditing to avoid any such issue.

E. Click "OK." The software tries to enable the auditing and create the backup of the selected group policy 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.

   If you face any issue in future, you can use this backup to restore the policy to the earlier state. Please refer to Section 5 of this document restore the group policy.

F. You have to wait until the auditing is enabled.

3. Issue

If LepideAuditor faces any problem in enabling the auditing, it displays the following error message while adding/modifying the domain.

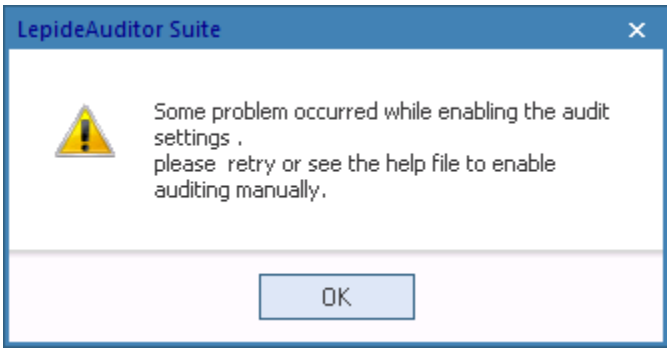

Figure 7: Error message for problem in enabling the auditing

In such cases, you have to enable the auditing settings manually on the Windows Server.

4. Solution

Auditing settings of the Active Directory environment could be setup as follows:

Auditing Entries for	AD Forest Partition for	Object	Access type	Apply onto
All AD objects	Domain naming context	Everyone	Successful	This object and all descendant or child objects.
AD Configuration Objects	Configuration context	Everyone	Successful	This object and all descendant or child objects.

AD Schema Objects	Schema Context	Everyone	Successful	This object and all descendant or child objects.

Table 1: Auditing Settings

If LepideAuditor displays any error message or does not enable the auditing, then you have to enable the auditing manually at the domain in both Group Policy Management Console and ADSIEdit Console. The steps to be performed in both consoles are listed below.

4.1 Enable Auditing in Group Policy Management Console

You have to enable the local and advanced auditing policies in the Group Policy Management Console.

4.1.1 Enable Local Audit Policies

Follow the steps below to configure the Audit Polices for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

1. Go to "Start Menu" → "All Programs" → "Administrative Tools" → "Group Policy Management". It opens "Group Policy Management."

NOTE: You can also type "GPMC.msc" in "Run" and press "Enter" key to access it.

2. Navigate to "Forest: domain.com" → "Domains" → "domain_controller.com" → "Domain Controllers".

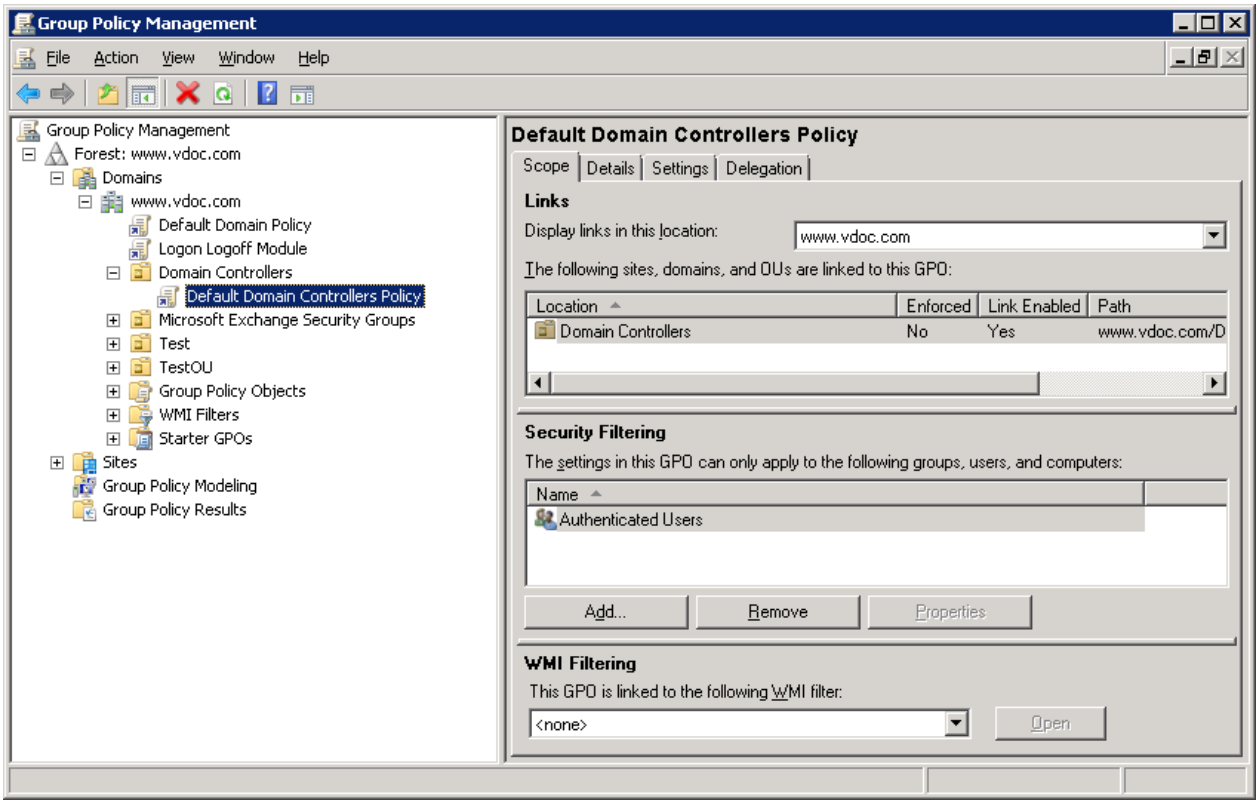

Figure 8: Group Policy Management Console

3. Select "Default Domain Controller Policy" or another policy, which is active and enabled on the domain controller organizational unit.

NOTE: It is recommended to select "Default Domain Controller Policy".

4. Right click on the policy to show the following context menu.

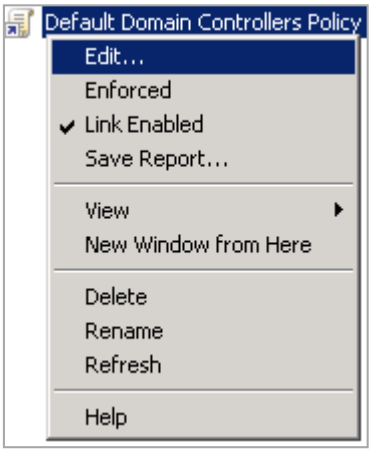

Figure 9: Option to edit Group Policy

5. Click "Edit" to access "Group Policy Management Editor" for the selected policy.
6. Browse to "Computer Configuration" → "Policies" → "Windows Settings" → "Security Settings" → "Local Policies" → "Audit Policy". It displays the policies in the Right Panel.

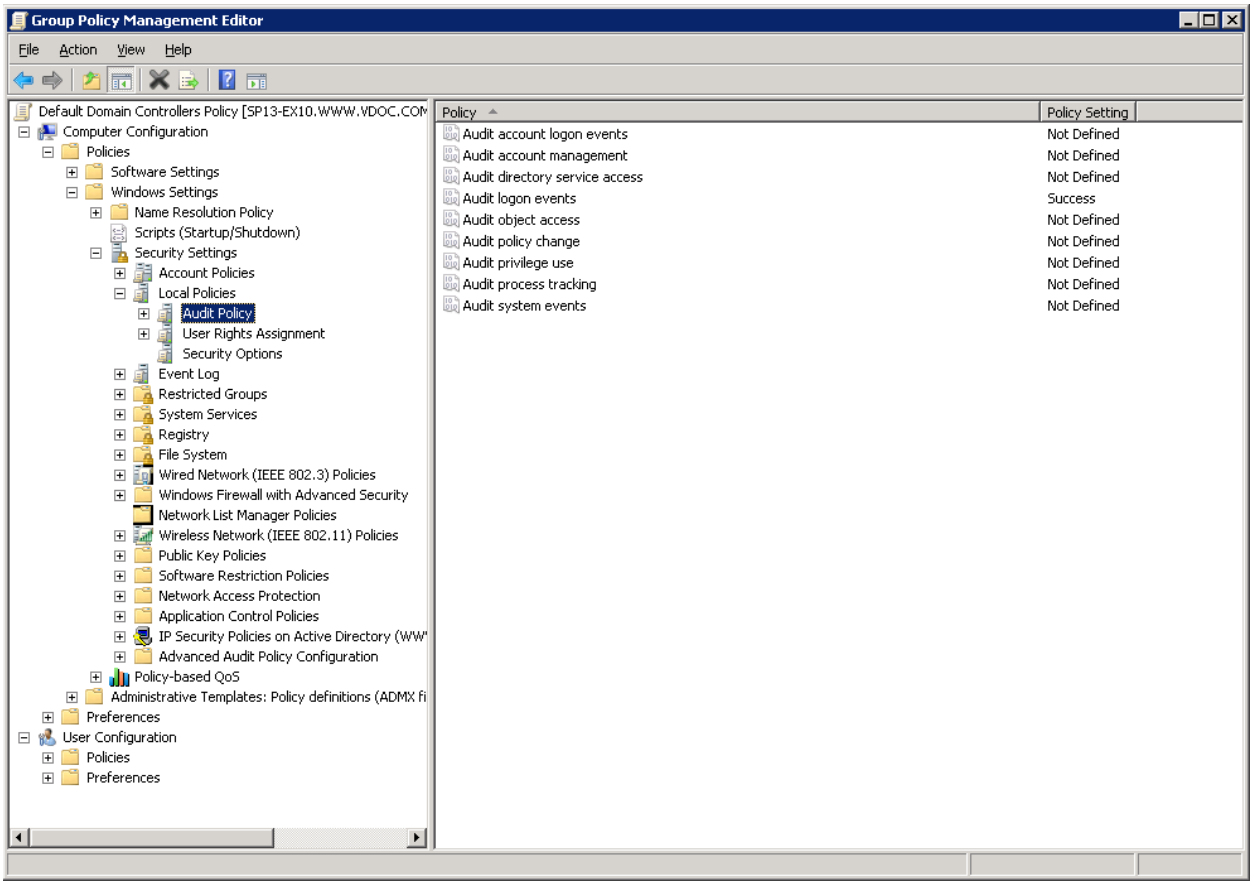

Figure 10: Group Policies

7. Here, you have to configure the following policies
    a. Audit account logon events
    b. Audit account Management
    c. Audit directory service access
8. Double-click "Audit account logon events" policy to access its properties.

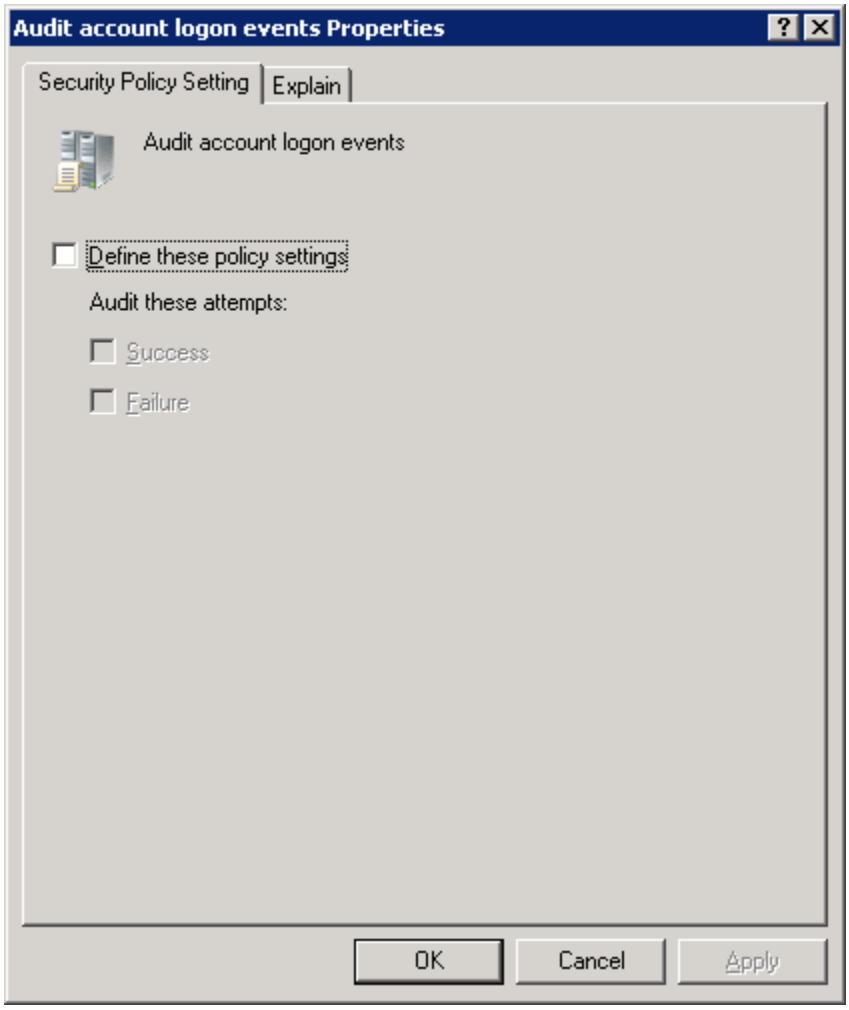

Figure 11: Properties of "Account Logon Events."

9. Check "Define these policysettings" box. It enables the subsequent section.
10. Check both "Success" and "Failure" boxes under "Audit theseattempts."

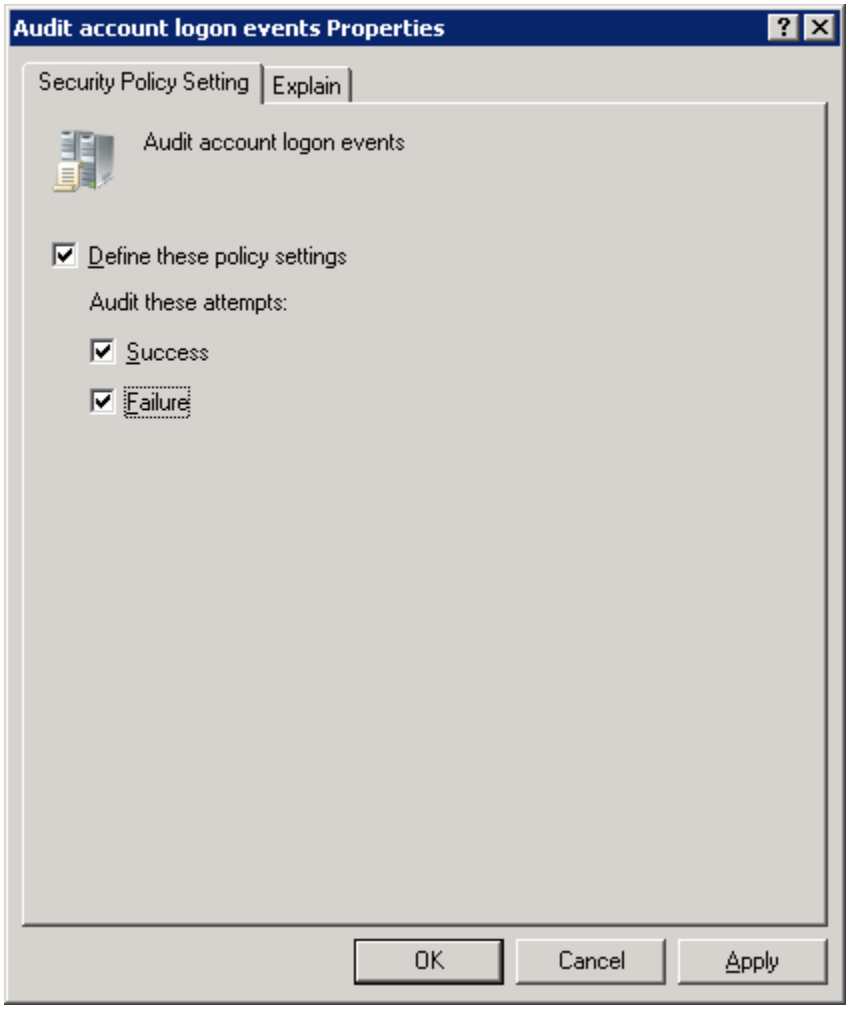

Figure 12: Configured "Account Logon Events"

11. Click "Apply" and "OK." It takes you back to "Group Policy Management Editor", which now shows the configured policy.
12. Follow the same steps to configure the following policies.
    a. Audit Account Management
    b. Audit directory service access

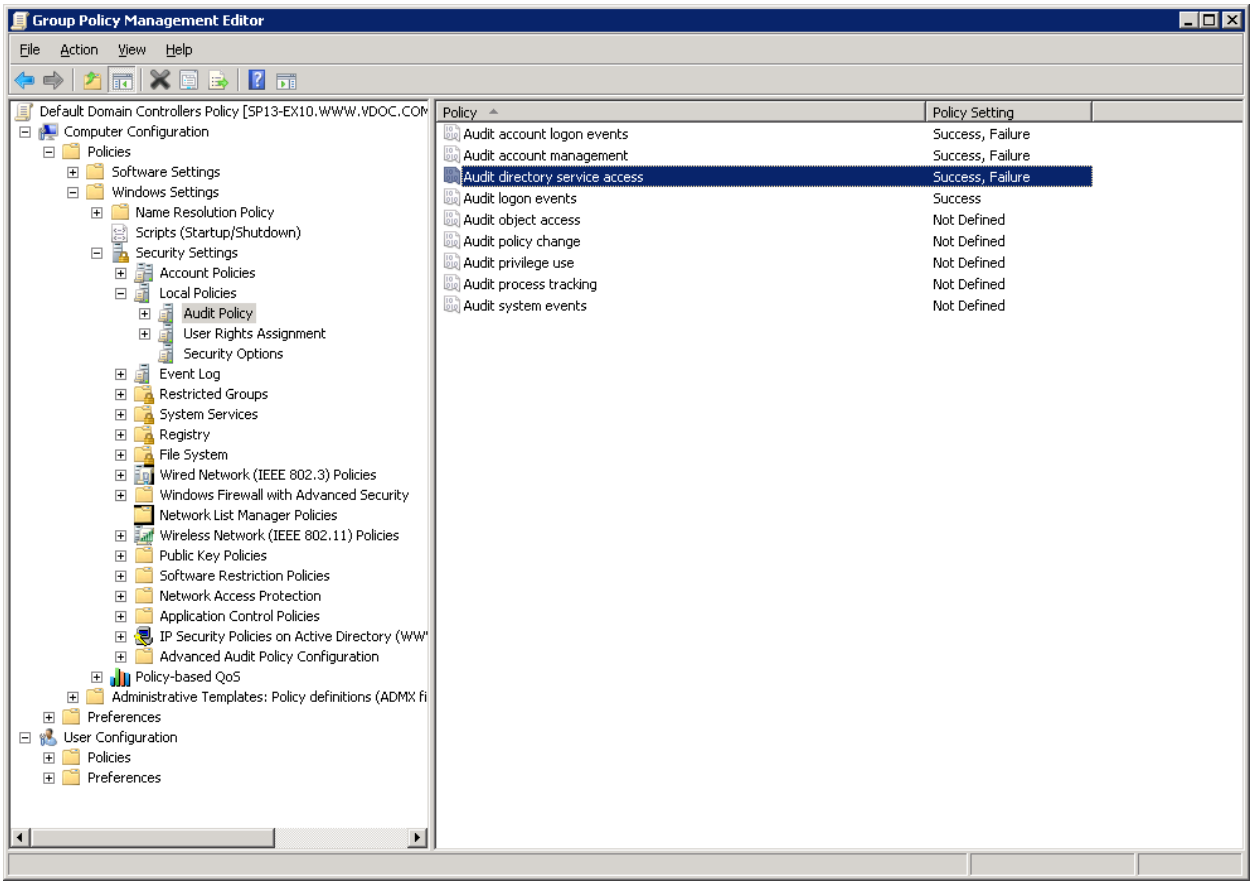

Figure 13: Configured the required policies

13. Close "Group Policy Management Editor."
14. Close "Group Policy Management Console".
15. In "Run" box or at "Command Prompt", execute the following command to apply the above change.

```
gpupdate /force
```

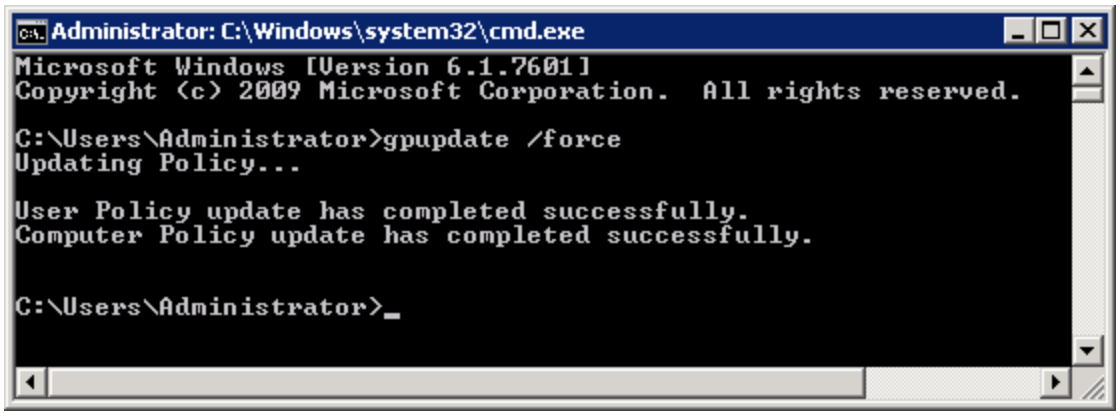

Figure 14: Updating Group Policy

4.1.2 Enable Advanced Audit Policies

There are three different methods for Windows Servers to enable the advanced auditing options in Group Policy Management Console. You have to run the commands on Command Prompt for Windows Server 2008, whereas you have to use Group Policy Management Console for Windows 2008 R2 and above.

4.1.2.1 Steps to Enable Advanced Audit Policies at Windows Server 2008 Only

Start the Command Prompt using Administrator privileges and execute the following commands one by one.

1. `Auditpol /set /category:"Account Logon" /success:enable /failure:enable`
2. `Auditpol /set /category:"Account Management" /success:enable /failure:enable`
3. `Auditpol /set /category:"DS Access" /success:enable /failure:enable`
4. `Auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable`
5. `Auditpol /set /category:"Object Access" /success:enable /failure:enable`
6. `Auditpol /set /category:"Policy Change" /success:enable /failure:enable`

4.1.2.2 Steps to Enable Advanced Audit Policies at Windows Server 2008 R2 and above versions

1. Go to "Start Menu" → "All Programs" → "Administrative Tools" → "Group Policy Management". It opens "Group Policy Management".

NOTE: You can also type "GPMC.msc" in "Run" and press "Enter" key to access it.

2. Navigate to "Forest: domain.com" → "Domains" → "domain_controller.com" → "Domain Controllers".

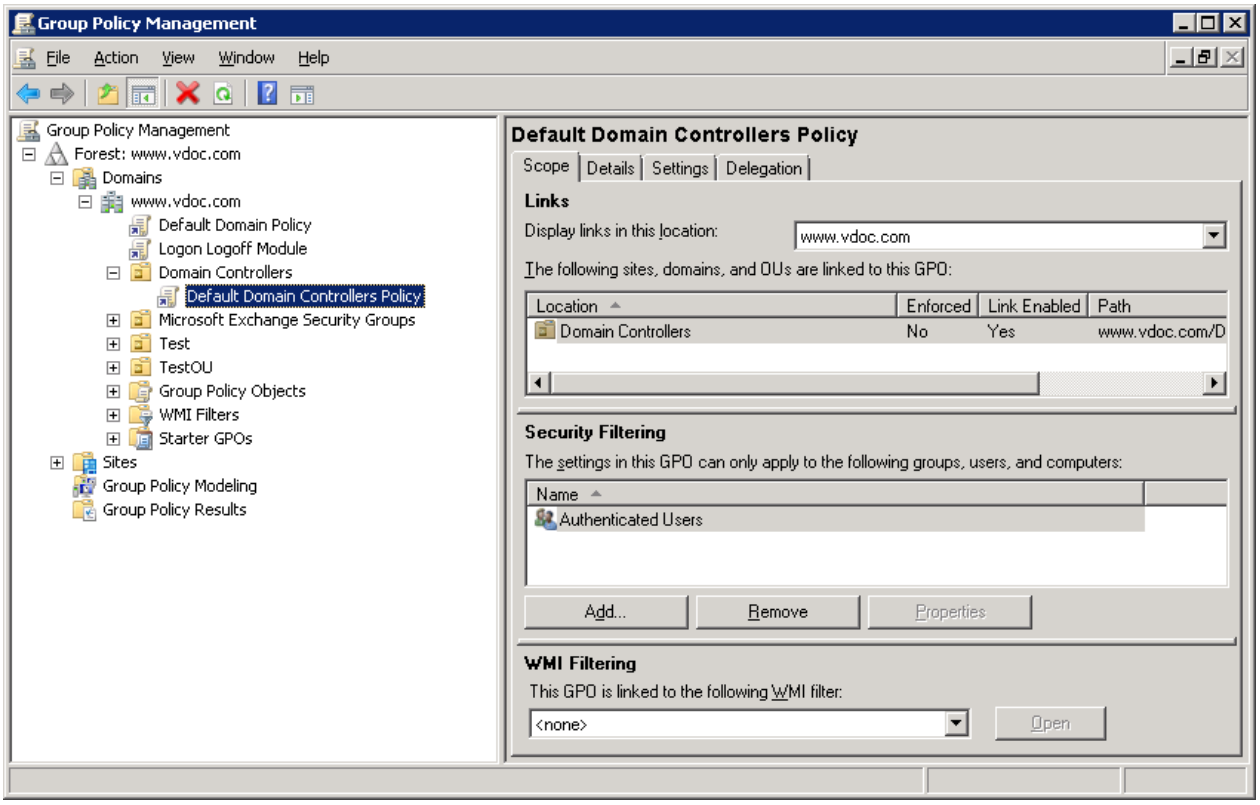

Figure 15: Group Policy Management Console

3. Select "Default Domain Controller Policy" or another policy, which is active and enabled on the domain controller organizational unit.

NOTE: It is recommended to select "Default Domain Controller Policy".

4. Right click on the policy to show the following context menu.

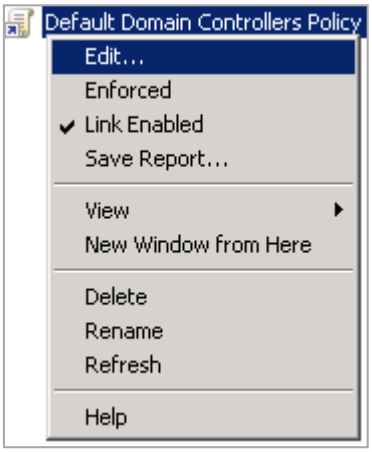

Figure 16: Option to edit Group Policy

5. Click "Edit" to access "Group Policy Management Editor" for the selected policy.
6. Browse "Computer Configuration" → "Policies" → "Windows Settings" → "Security Settings" → "Advanced Audit Policy Configuration" → "Audit Policies." It displays the different policy categories in the Right Panel.

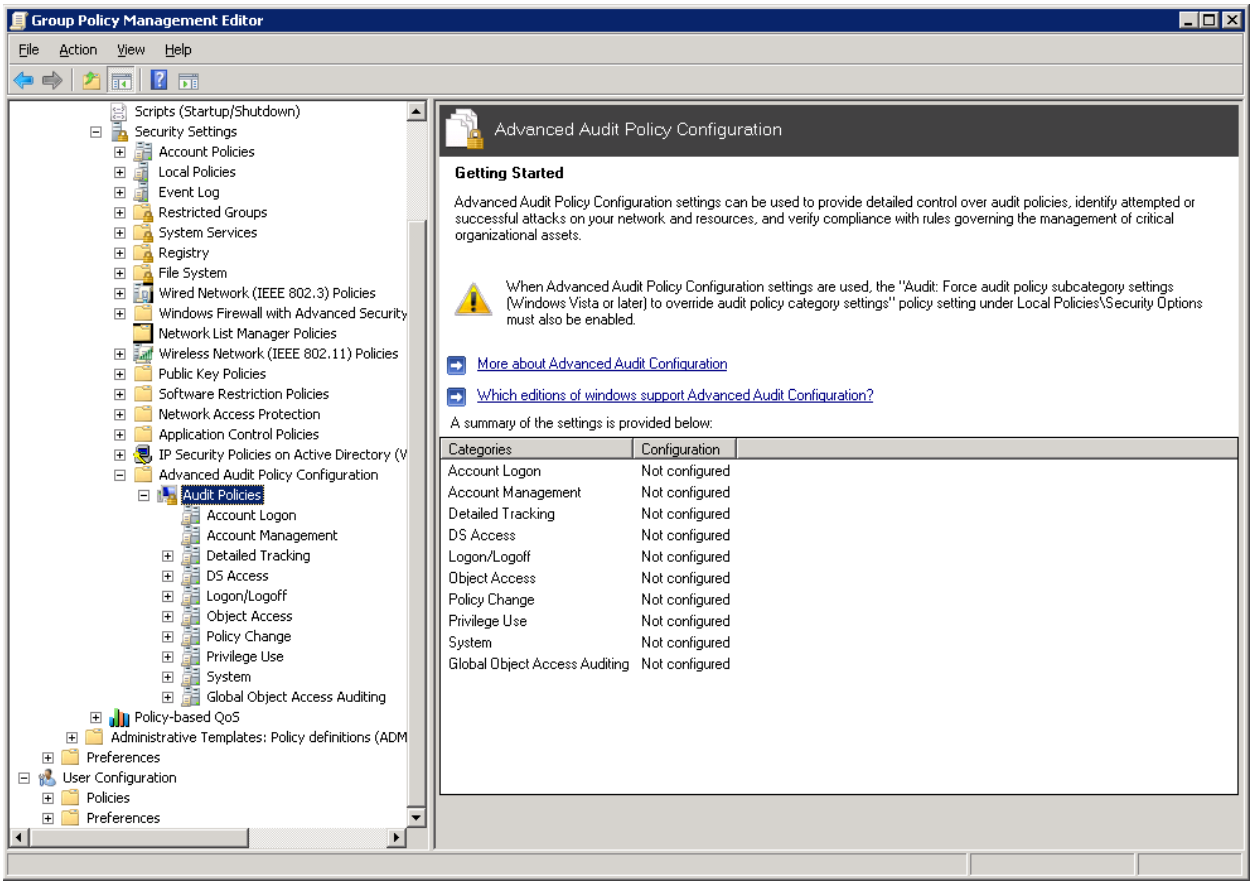

Figure 17: Editor of Group Policy Objects

7. You have to configure all policies of the following categories.
   I. Account Logon
      a. Audit Credential Validation
      b. Audit Kerberos Authentication Service
      c. Audit Kerberos Service Ticket Operations
      d. Audit Other Account Logon Events
   II. Account Management
      a. Audit Application Group Management
      b. Audit Computer Account Management
      c. Audit Distribution Group Management

d. Audit Other Account Management Events
e. Audit Security Group Management
f. Audit User Account Management

III. DS Access
a. Audit Detailed Directory Service Replication
b. Audit Directory Service Access
c. Audit Directory Service Changes
d. Audit Directory Service Replication

IV. Logon/Logoff
a. Audit Account Lockout
b. Audit IPsec Extended Mode
c. Audit IPsec Main Mode
d. Audit IPsec Quick Mode
e. Audit Logoff
f. Audit Logon
g. Audit Network Policy Server
h. Audit Other Logon/Logoff Events
i. Audit Special Logon

V. Object Access
a. Audit Application Generated
b. Audit Certification Services
c. Audit Detailed File Share
d. Audit File Share
e. Audit File System
f. Audit Filtering Platform Connection
g. Audit Filtering Platform Packet Drop
h. Audit Handle Manipulation
i. Audit Kernel Object
j. Audit Other Object Access Events
k. Audit Registry
l. Audit SAM

VI. Policy Change

a. Audit Audit Policy Change

b. Audit Authentication Policy Change

c. Audit Authorization Policy Change

d. Audit Filtering Platform Policy Change

e. Audit MPSSVC Rule-Level Policy Change

f. Audit Other Policy Change Events

8. Execute the following steps to configure the above policies in the above listed different categories.

A. Click "Account Logon" category in either Left or Right Panel to access its policies.

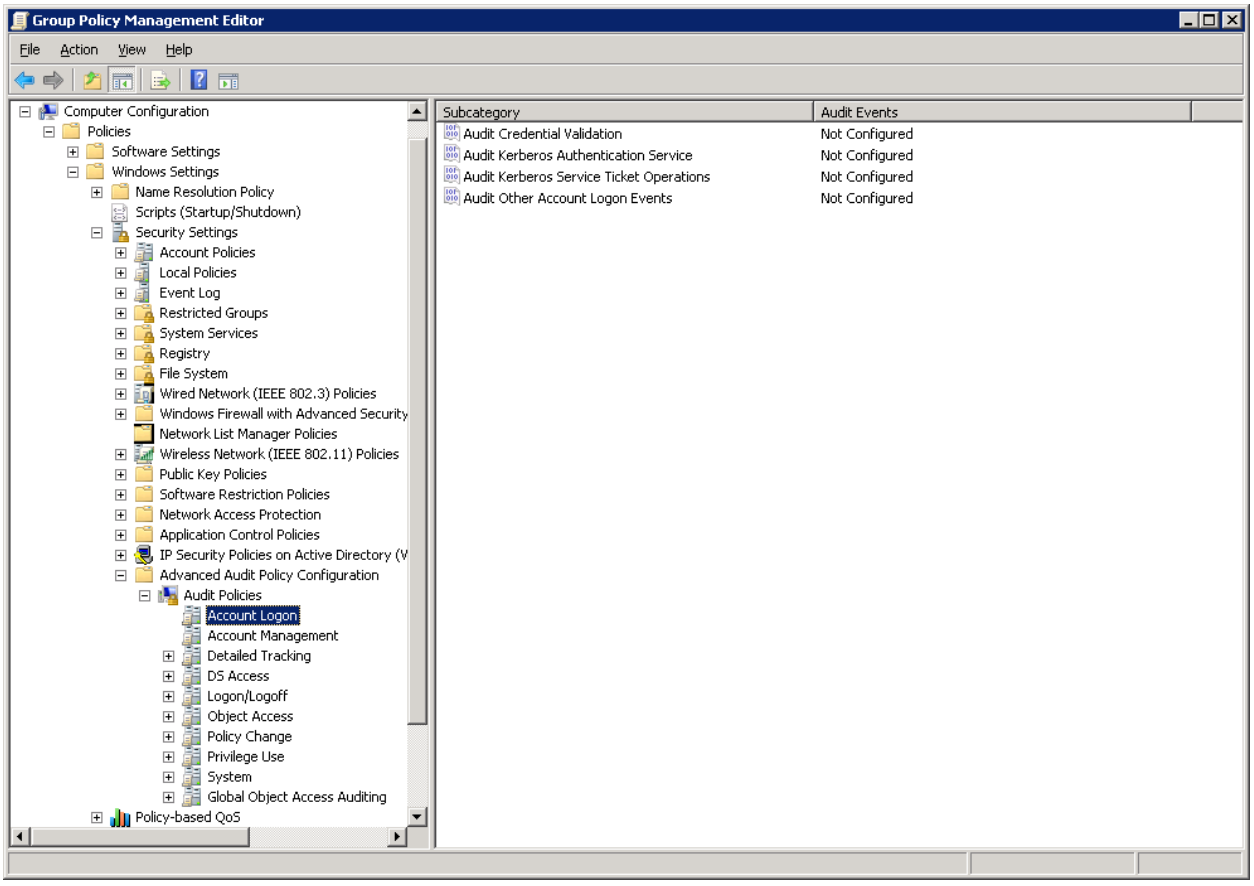

Figure 18: Account Logon Policies

B. In the Right Panel, double-click any policy say "Audit Credential Validation" to access its properties.

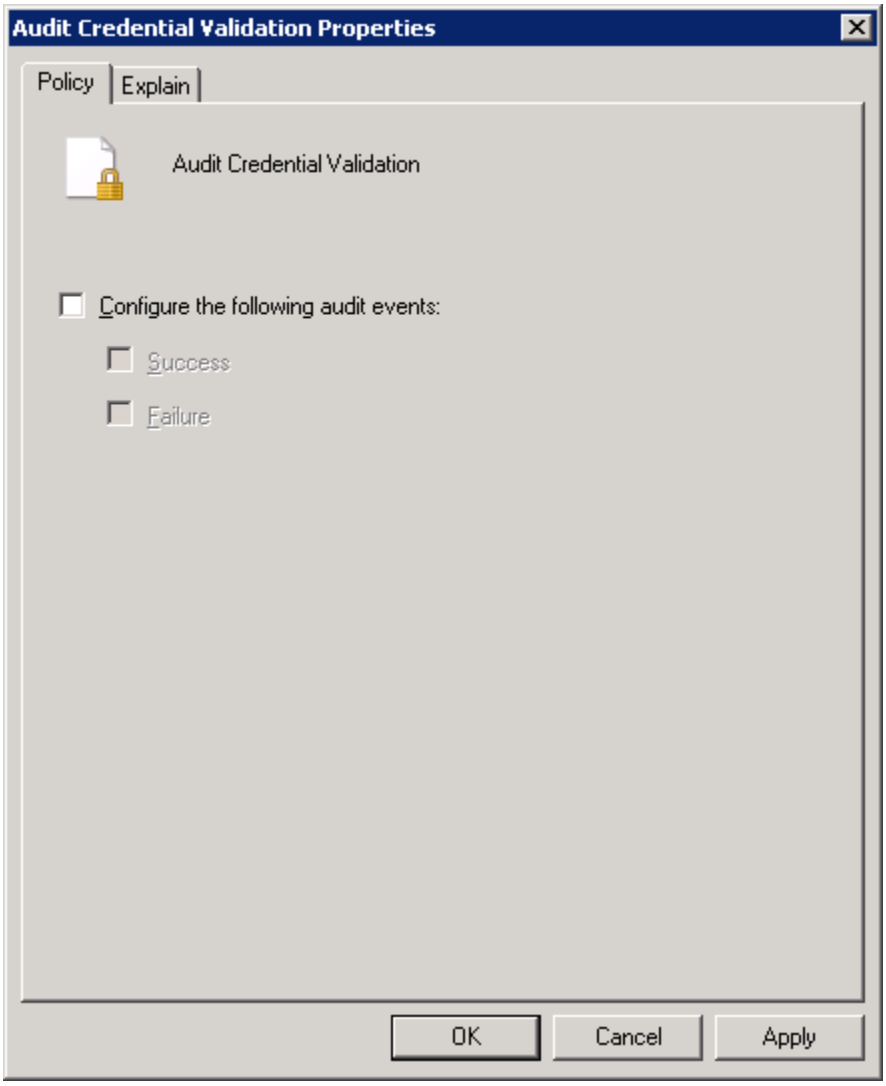

Figure 19: Properties of "Audit Credential Validation"

C. Check "Configure the following audit events" box. It enables the subsequent section.

D. Check both "Success" and "Failure" boxes.

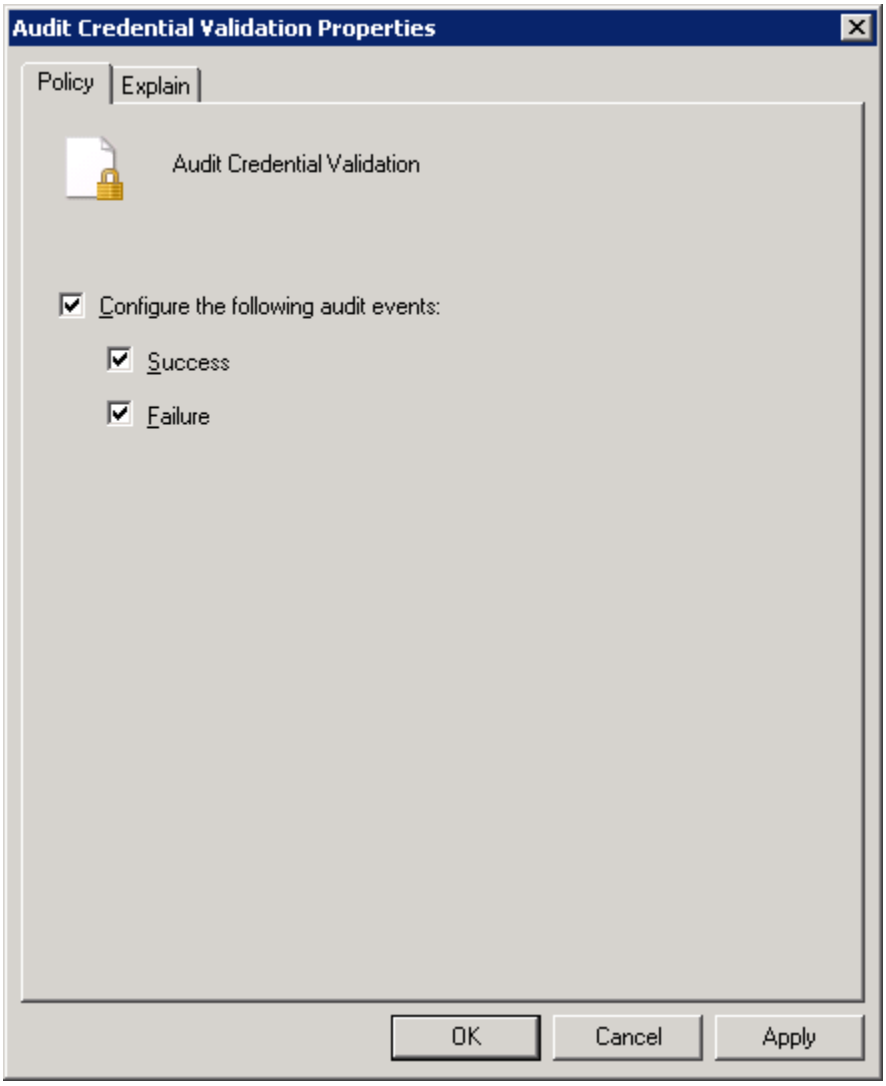

Figure 20: Configured "Audit Credential Validation"

E. Click "Apply" and "OK." It takes you back to "Group Policy Management Editor", which now shows the configured policy.

F. Execute the above steps to configure other policies of "Account Logon" category.

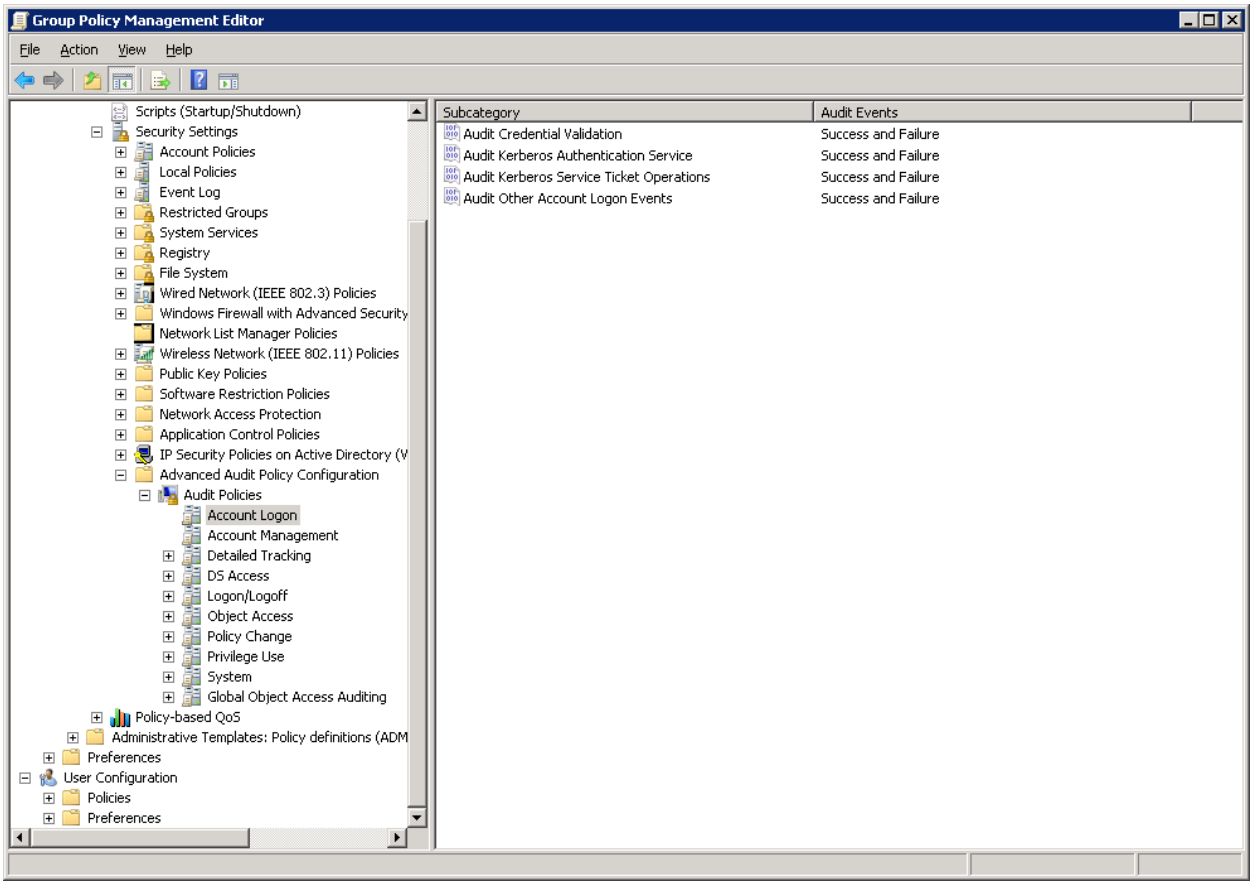

Figure 21: Configured all policies of "Account Logon"

9. Follow the same steps to configure all policies in the above-listed categories.

4.2 Enable Auditing using ADSIEdit.msc

Perform the following audit settings using the ADSIEdit.msc on any Windows Server. Visit http://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx to know more about installing and using ADSIEdit.msc.

You have to perform the following steps for all Windows Server.

1. Open ADSIEdit.msc using the "Run" dialog box. You can also open it from “Start Menu” → “Administrative Tools” → “ADSIEdit”.
2. Connect to the Active Directory. Select any node and perform below steps. Repeat these steps for each root node.
3. Right-click on the root “ADSI Edit” and select “Connect to”.
4. It is required to connect to all four available naming contexts and to turn on their auditing.

a. Default Naming Context

b. Configuration

c. RootDSE

d. Schema

NOTE: We will connect to all these naming contexts one by one and then turn on their auditing.

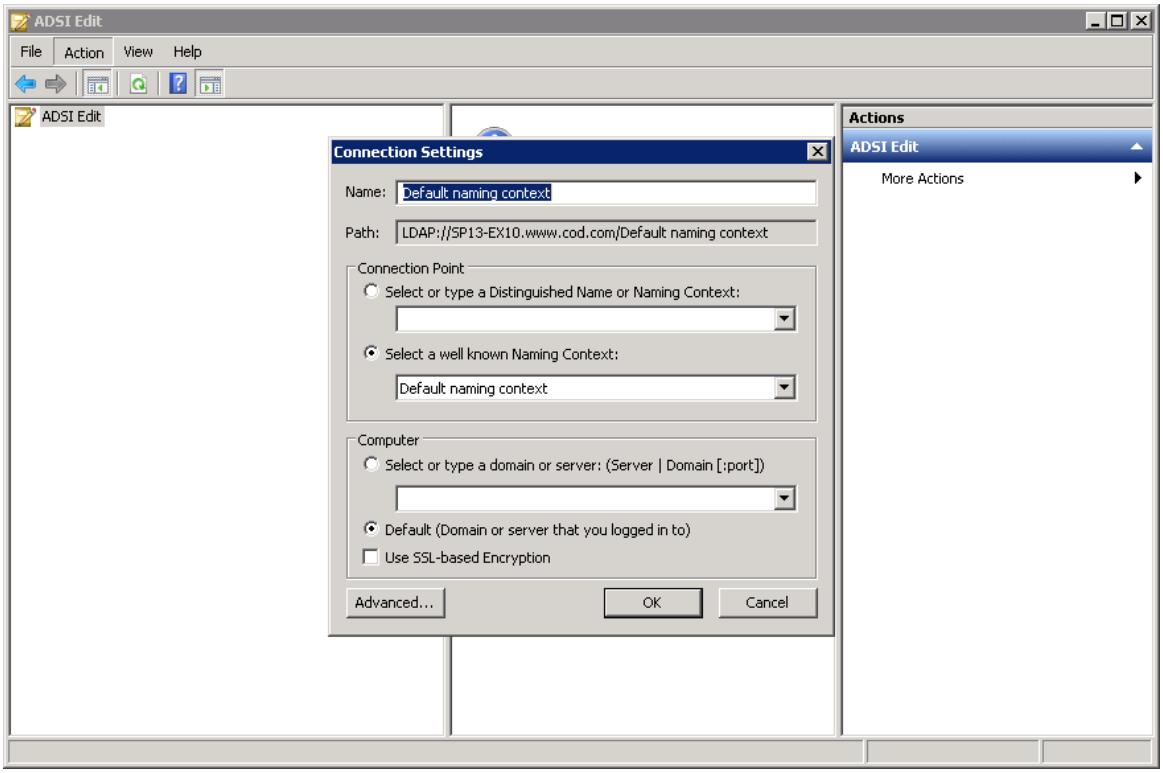

Figure 22: Select the naming context to which you want to connect

5. Select "Default Naming Context".
6. Click "OK" to establish the connection. Default Naming Context will be connected and its root node will be displayed in "Left Panel".
7. Expand the root node to access the domain controller's node –"DC=www,DC=domain,DC=com".
8. Again, right click on "ADSIEdit" parent node and select "Connect To".
9. In "Connection Settings" box, select "Configuration" for naming context and click"OK".

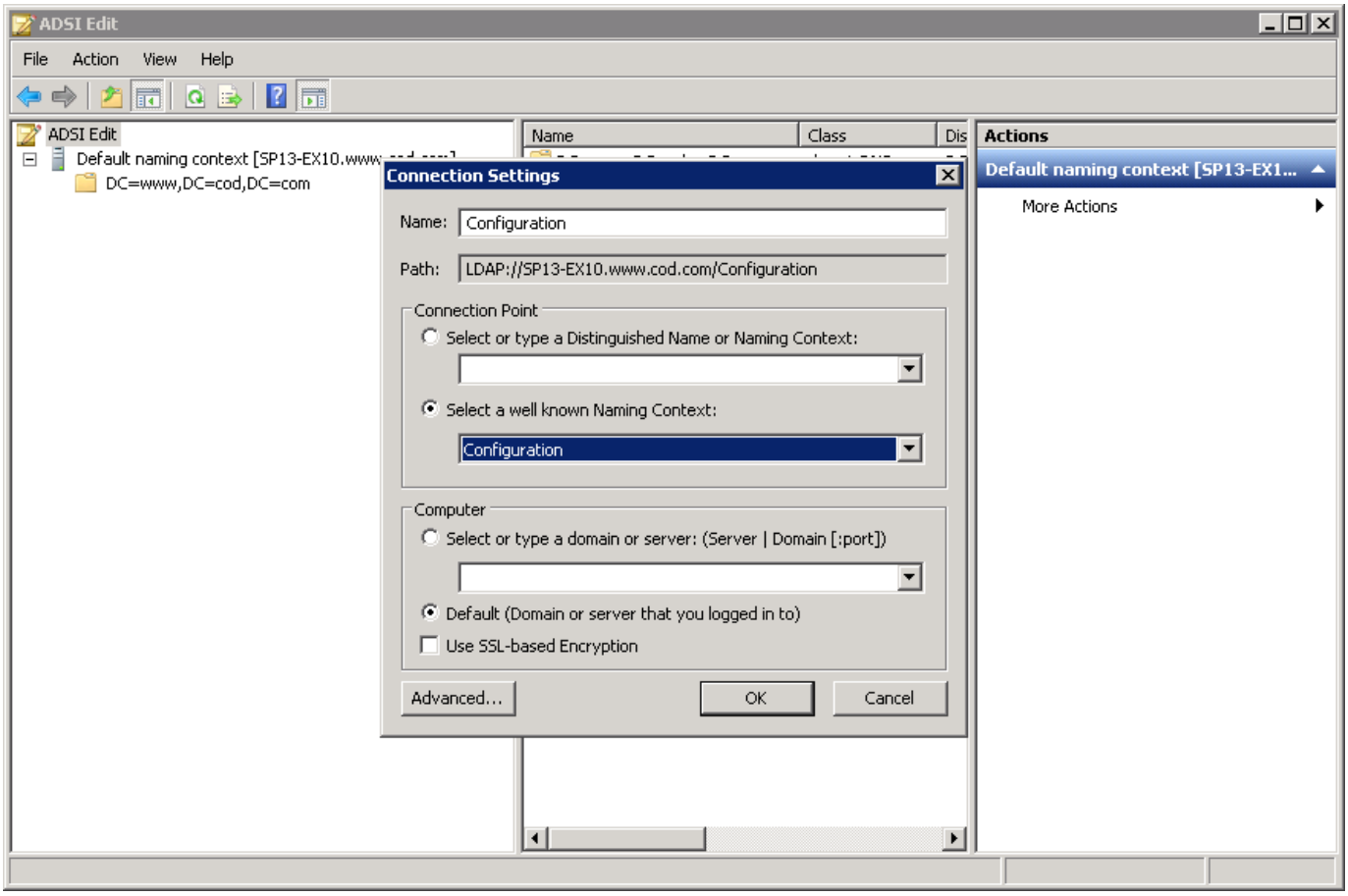

Figure 23: Connecting to Root Configuration

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 "RootDSE" as naming context in "Connection Settings" and click "OK".

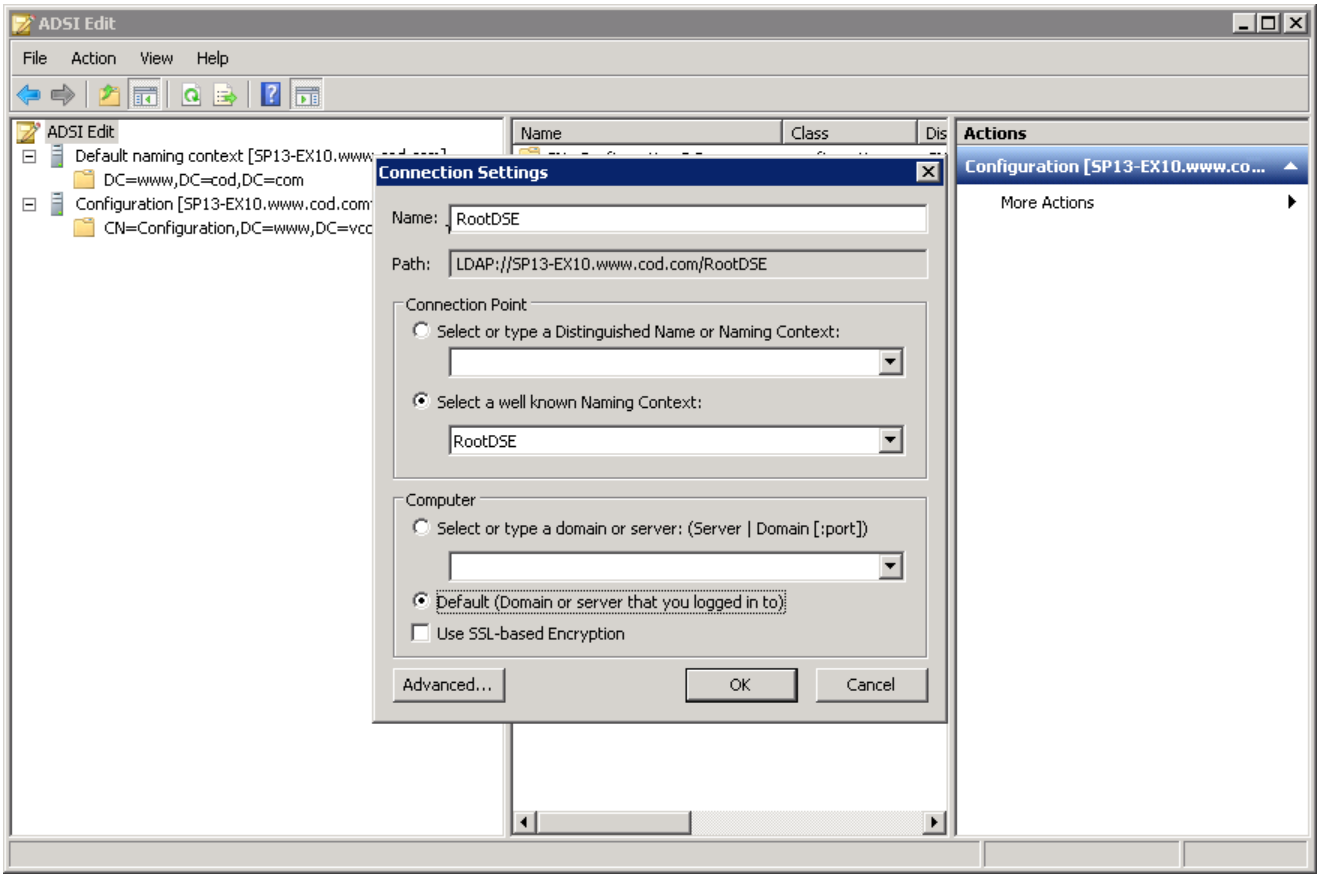

Figure 24: Connecting to RootDSE

14. It connects ADSI Edit to the root of Active Directory (RootDSE) and shows its root node in the Left Panel.
15. Expand root node of RootDSE to access "RootDSE".
16. Again, right-click on "ADSI Edit" parent and select "Connect To".
17. Select "Schema" as the naming context and click "OK" to connect to it.

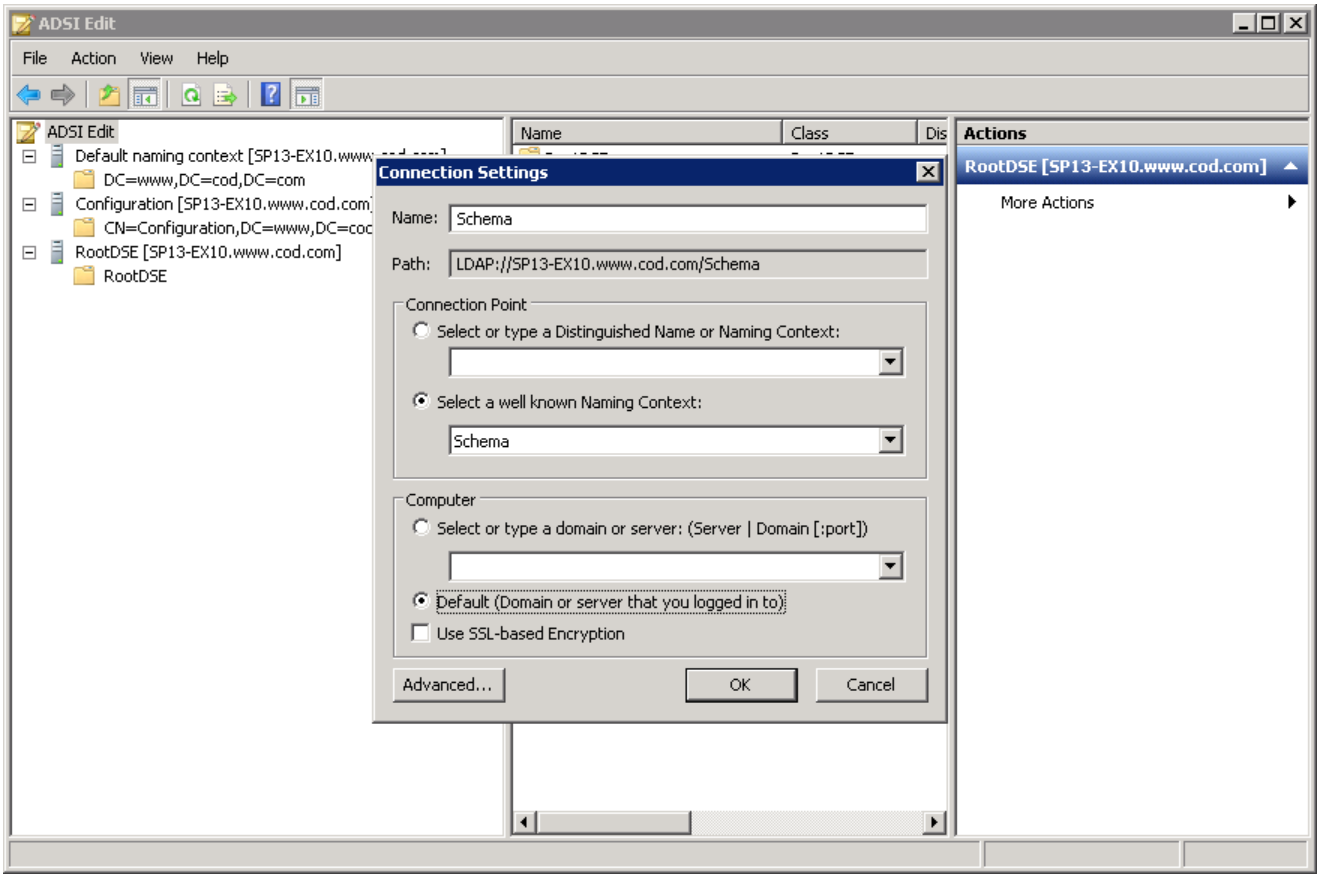

Figure 25: Connecting to Schema

18. It connects ADSI Edit to the Schema and displays its root node in the Left Panel.
19. Expand its node to access "CN=Schema,CN="Configuration,DC=www,DC=domain,DC=com".
20. 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. RootDSE
    d. CN=Schema,CN=Configuration,DC=www,DC=domain,DC=com
21. 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".

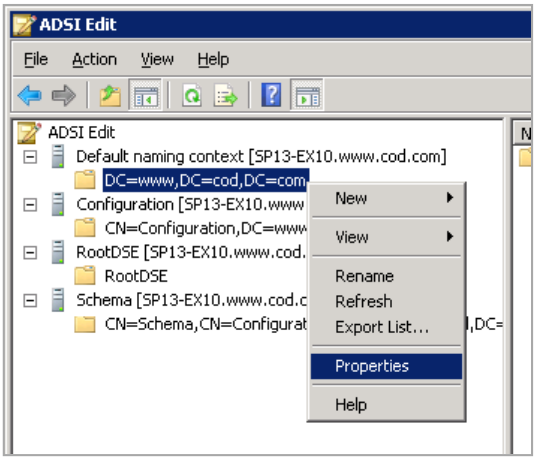

Figure 26: Right click on root node of Default Naming Context

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

c. Switch to "Security" tab.

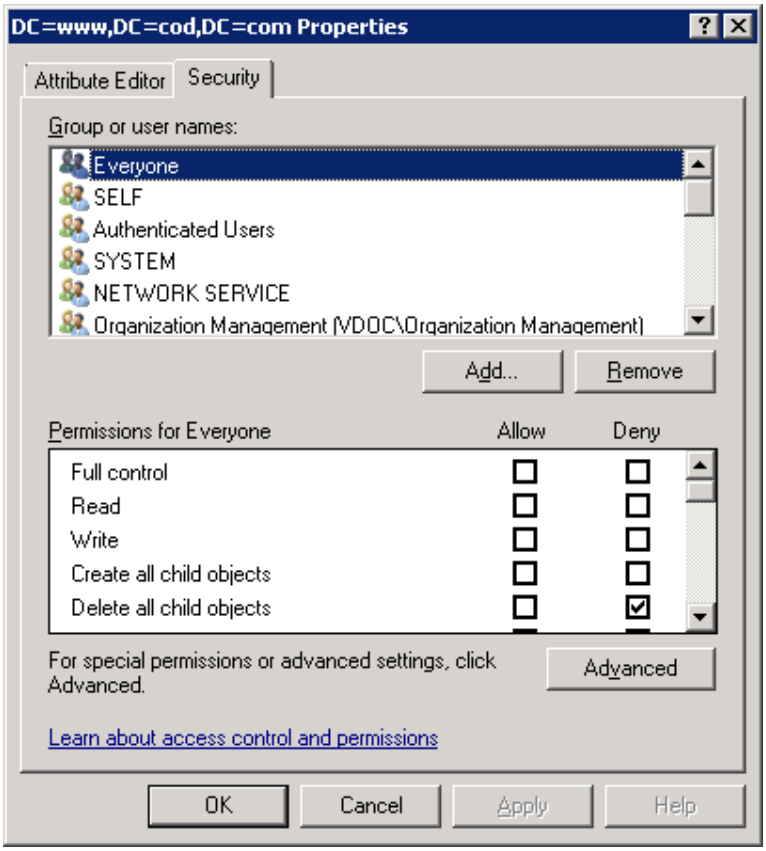

Figure 27: Security Tab of Node Properties

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

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

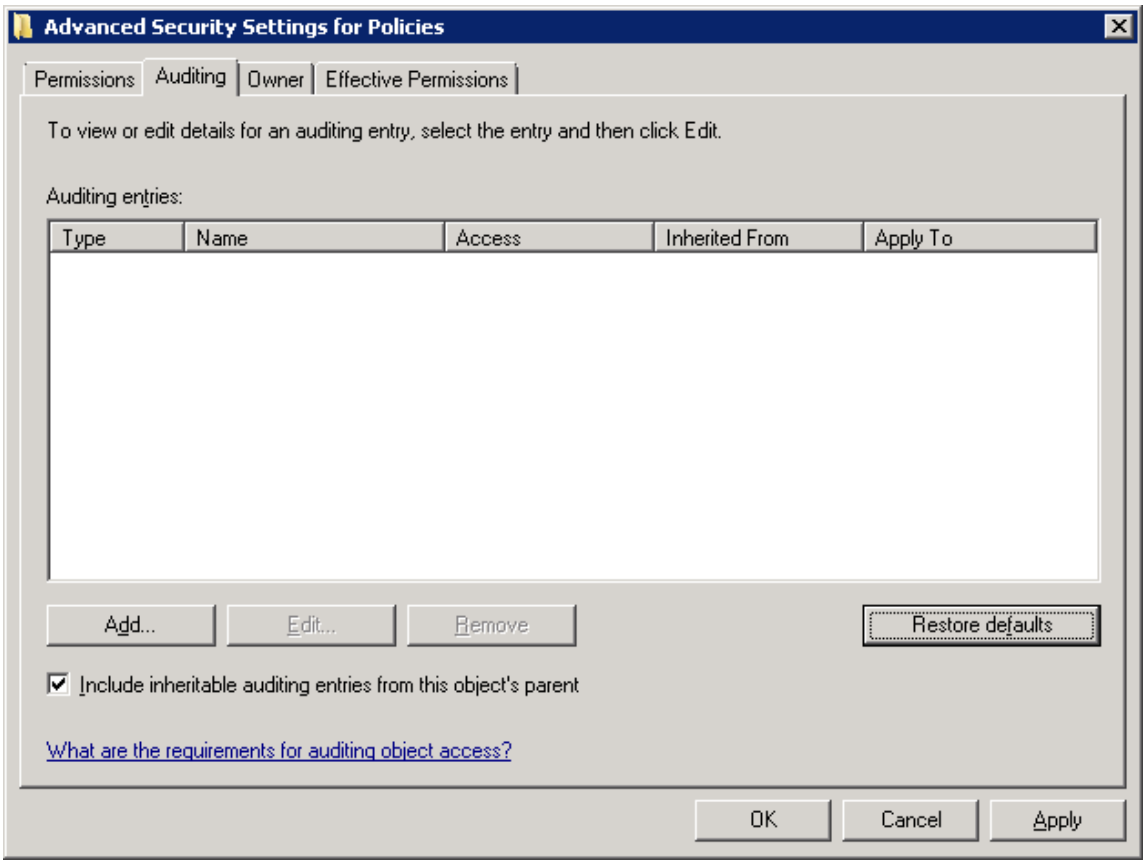

Figure 28: Auditing tab

f. Click "Add" to add the user for whom you want to enable auditing. It shows the following box:

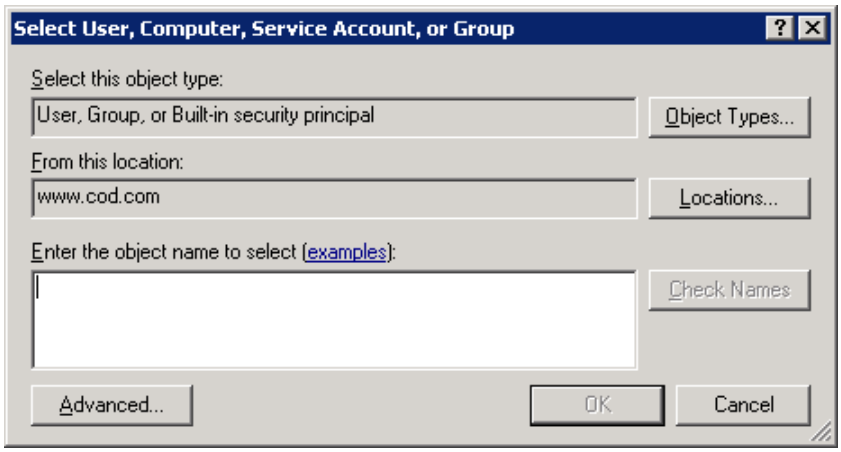

Figure 29: Add User

g. Type the name of a specific user for which you want to enable the auditing. Instead, you can type "Everyone" to audit the changes in Group Policies for all users.

h. Click "Check Names" to verify the username.

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

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

k. Click "Full Control" in "Successful" column to monitor all successful access events.

l. Uncheck "Full Control" in "Failed" column for not monitoring all failed access events.

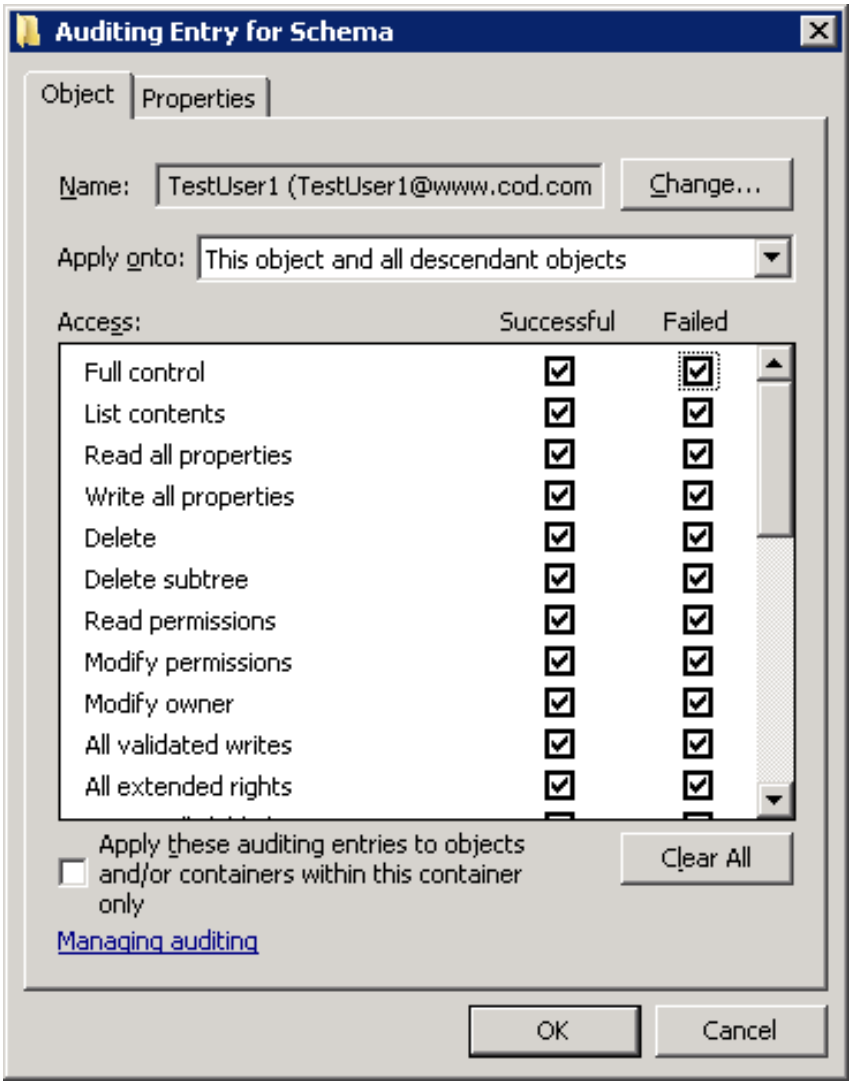

Figure 30: Auditing Entries for www

m. Now, you have to uncheck the following entries in "Successful" column.

- Full Control

- List contents
- Read all properties
- Read permissions

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

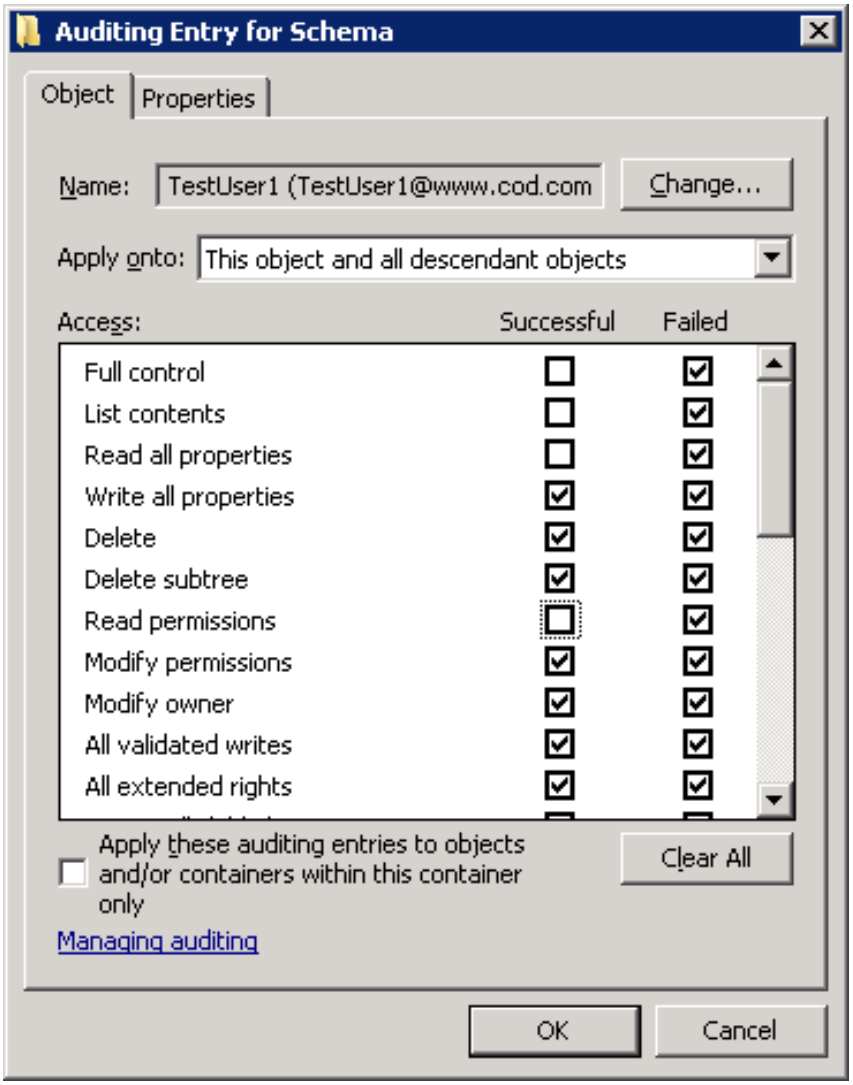

Figure 31: Displaying settings to be unchecked

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".

22. Repeat the steps (a) to (n) of Step 21 to enable the auditing of remaining rootnodes.

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

b. RootDSE

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

23. 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.

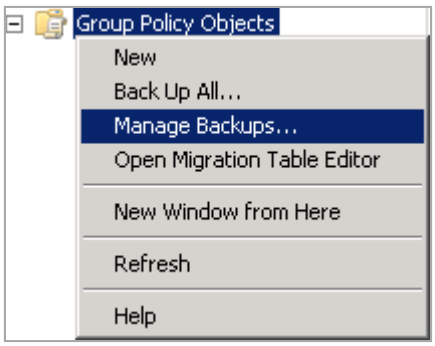

Figure 32: Option to manage the Group Policy Backups

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

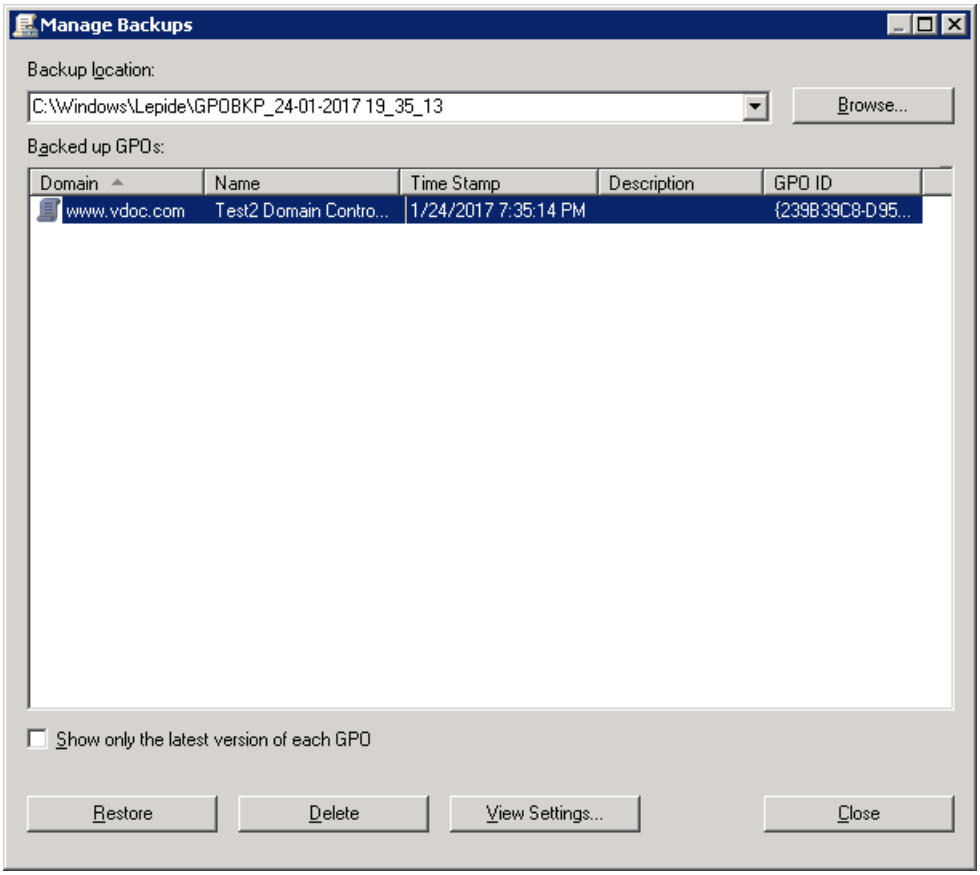

Figure 33: Manage the backups of Group Policies

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. Conclusion

By completing the above steps, you will be able to enable the domain auditing manually. To read more about the LepideAuditor, please visit http://www.lepide.com/lepideauditor/.

7. Support

If you are facing any issue while installing, configuring or using the software or while enabling the auditing, then you can connect with our team.

Product experts

USA/Canada: +1-800-814-0578

UK/Europe: +44 (0) -845-594-3766

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

Technical gurus

USA/Canada: +1-800-814-0578

UK/Europe: +44(0)-800-088-5478

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

You can also visit http://www.lepide.com/contactus.html to chat live with our team and to know more about our support team.

You can email your queries at the following addresses:

sales@Lepide.com for Sales

support@Lepide.com for Support

8. Copyright

9. 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.

10. 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.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only. We have compiled a list of such trademarks, but it may be possible that a few of them are not listed here.

Windows 7®, Windows 8®, Windows 8.1®, Windows 10®, Windows 2000 Server®, Windows 2000 Advanced Server®, Windows Server 2008®, Windows Server 2008 R2®, Windows Server 2012®, Exchange Server 2003®, Exchange Server 2007®, Exchange Server 2010®, Exchange Server 2013®, SharePoint Server®, SharePoint Server 2010®, SharePoint Foundation 2010®, SharePoint Server 2013® SharePoint Foundation 2013®, SQL Server 2005®, SQL Server 2008®, SQL Server 2008 R2®, SQL Server 2012®, SQL Server 2014®, SQL Server 2016®, SQL Server 2005 Express Edition®, SQL Server 2008 Express® SQL Server 2008 R2 Express®, SQL Server 2012 Express®, SQL Server 2014 Express®, .NET Framework 4.0, .NET Framework 2.0, Windows PowerShell® are registered trademarks of Microsoft Corporation.