LepideAuditor

Enable Logon/Logoff Events Monitoring

Table of Contents

1. Introduction
2. Issue
3. Manage Logon/Logoff Audit Module
3.1 Install Logon/Logoff Audit Module4
3.2 Stop Logon/Logoff Module
3.3 Uninstall Logon/Logoff Audit Module
4. Generate Logon.exe file
5. Create Group Policy Object at Server
5. Conclusion
7. Support19
3. Copyright19
9. Warranty Disclaimers and Liability Limitations20
10. Trademarks

1. Introduction

This helpful guide takes you through the necessary steps to enable the auditing of logon/logoff events. In both agentless and agent-based auditing, the following steps must be completed:

- Generate "Logon.exe" from the software, while adding or modifying the domain, and create a Group Policy on the server to assign it. It will collect logon and logoff events and passes them to Logon/Logoff Audit Module.
- Install Logon/Logoff Audit Module on any of the domain controllers of the domain, which will process logon/logoff events and send it to the software for display.

Both of these modules should run continuously at the server for collecting logon/logoff events. The following items will not be generated if the above steps are not performed.

- "Successful User Logon/Logoff" and "Domain Controller Logon/Logoff" Reports
- Custom Reports, LiveFeed, alerts, and scheduled reports for above reports

2. Issue

If you have neither installed Logon/Logoff Audit Module nor generated "logon.exe" nor linked it with the server, the following error appears onscreen while generating "Successful User Logon/Logoff" or "Domain Controller Logon/Logoff".



Figure 1: Error while generating logon/logoff reports

You have to generate logon.exe, link it with a Group Policy, and install Logon/Logoff Audit Module to enable the auditing of logon/logoff events to fix this issue.

3. Manage Logon/Logoff Audit Module

The steps to install, manage, and uninstall the logon/logoff Audit Module are listed here.

3.1 Install Logon/Logoff Audit Module

To audit logon/logoff events, you will need to install LepideAuditor Logon/Logoff Audit Module on any of the domain controllers of the domain to collect logon/logoff events. The installer file for this module will come with setup file, which you can download from http://www.lepide.com/lepideauditor/download.html. After downloading this installer file, execute the following steps to install the Logon/Logoff Audit Module.

- 1. Double-click the downloaded installer file to start theinstallation.
- 2. Click "Next" to proceed to the next step of the license agreement.
- 3. It is recommended to read the license agreement carefully before installing the software.
- 4. If you agree to the license agreement and want to continue with the installation, check "I accept the agreement" and click "Next".
- 5. The next step lets you customize the location of the shortcuts folderin the Start Menu.
- 6. Click "Browse" and select a different location to modify the location of the shortcuts folder in the Start Menu.
- 7. Click "Next" to use the default or customized shortcuts folder.
- 8. Check the boxes titled "Create a desktop icon" and/or "Create a Quick Launch icon", if you want.
- 9. Click "Next" to proceed further. The software is now readyto be installed.
- 10. Click "Install" to begin the installation procedure.
- 11. Once installed, the following page comes in the wizard. It asks for the login credentials of a user having administrative privileges.

🚻 Setup - LepideAuditor Lo	gon/Logoff Module	
Create service wizard It is recommended to run account must have "logor	the services under administrator account and given n as service rights".	***
User Account : Password :	Administrator	
Domain Name :	[COD]	
	Next >	Cancel
	Town >	Cancol

Figure 2: Asking for login credentials of an administrator to create the service

12. Enter the login credentials of a local administrator, domain administrator or a Managed Service Account object on this page. Please leave the password text box blank when you select to enter the name of a Managed Service Account object.

NOTE: You should use any of the following account or object.

- 1. A local system administrator
- 2. A member of Domain Admins Group
- 3. Manage Service Account object
- 13. Click "Next" after entering the login credentials of an administrator. The next page displays the message of successful installation of the module.
- 14. Click "Finish" to complete the process.

3.2 Stop Logon/Logoff Module

You may have to stop the app server either to stop receiving logon/logoff events or to uninstall the Module. Perform the following steps.

- 1. Go to "Start Menu" \rightarrow "Administrative Tools" \rightarrow "Services" to access the services.
- 2. Locate "Lepide Logon Logoff Service". Right-click on it to access the context menu.
- 3. Click "Stop" to stop the service.

3.3 Uninstall Logon/Logoff Audit Module

Execute the following steps.

- 1. There are two ways to start the uninstallation.
 - a. Go to Start → All Programs → "LepideAuditor Logon/Logoff Audit Module", click "Uninstall LepideAuditor Logon/Logoff Audit Module".
 - b. Go to Start → Control Panel → "Add/Remove Programs" or "Programs". Select "LepideAuditor Logon/Logoff Audit Module" and click "Remove".

Following any of the above methods displays a warning message.

- 2. Click "Yes" to uninstall the module. After completing the uninstallation, the message boxappears.
- 3. Click "OK" to complete the process.

4. Generate Logon.exe file

Perform the following steps on software to generate "logon.exe" file.

1. Use any of the following methods to start with this process.

A. While adding a domain with Advanced Configuration, you arrive at the following step.

Add Domain	×
Object Classes and Other Settings Please select object classes and other settings to be audited	
Audit : All Object Classes -	
Active Directory Object Classes Exchange Server Object Classes	Q
More Audit Settings ✓ Audit Failed Logon ✓ Audit Successful User Logon/Logoff	
< <u>B</u> ack <u>N</u> ext >	Cancel

Figure 3: Advanced Domain Configuration

B. In domain properties, go to "Object Class and Other Settings" to access the following settings.

	Properties	x
- 🚱 Domain Credentials - 😳 Advanced Domain Configuration - 🖧 IP Settings	Object Classes and Other Settings Please select object classes and other settings to be audited	
Database Settings Organizational Unit Settings Object Classes and Other Settings Archive Settings	Audit : Al Object Classes Active Directory Object Classes Exchange Server Object Classes P P More Audit Settings Audit Failed Logon Audit Successful User Logon/Logoff	
	ОК	Cancel

Figure 4: Modifying Object Class and other Settings

- 2. Check "Audit Successful User Logon/Logoff" option.
- 3. Click icon to access the following dialog box.

Create Logon/Logoff Script	×
Create Logon/Logoff Script	
Enter IP address of domain controller : 127 . 0 . 0 . 1 NOTE : Logon.exe will be linked to the specified IP Address and will run only on the above mentioned IP Address. Enter path for saving file : \\LOCAL_COD\Shared OK Cancel	0
Figure 5: Dialog box to create logon/logoff script	

- 4. Enter the IP Address of the domain controller, where Logon/Logoff Audit Module has been installed.
- 5. Click icon to select the location on the server to the save this executable file.

Browse For Folder	×
Select location to save logon script file	
⊿ 📮 LOCAL COD	~
Address	
Image: BroupMetrics	
▷ 👱 netlogon	
🖳 Shared	
sysvol	
▷ 🖳 SERVER2M	~
Eolder: Shared (\\LOCAL_COD)	
Make New Folder OK Cancel	

Figure 6: Browse for Server

It is recommended to save the executable file in the shared folder on the server, of which logon/logoff events you want to monitor.

- 6. Select the folder.
- 7. Click "OK" to go back to the previous dialog box, which now shows the selected folder.
- 8. Click "OK" to generate and save the executable file to the specified location. The following message appears on the screen to confirm the same.

LepideAuditor Sui	te ×
Successfully generated script file (Logon.exe).	Please follow the link
ОК	

Figure 7: Successfully generated executable file

9. Click hyperlink titled "Please follow the link" to know the steps to be performed at the server. It opens an HTML file in the default Web Browser.

Enable Logon/Logoff Mo ×
C ③ file:///C:/Program%20Files%20(x86)/LepideAuditor%20Suite/Logon_LogOff/Enable%20Logon%20Logoff%20Monitoring.html
Cepide LepideAuditor Suite
Enable Logon/Logoff Monitoring
LepdieAuditor Suite audit the domain in two different ways - With or Without Agent. Once "Logon.exe" has been generated and stored at Server, after creating Group Policy, it will collect logon and logoff events and pass it to the agent or assigned computer, which will in turn process it and send it to software for display.
Let us have a look at the different steps to be taken in case of both ways.
Steps for Agent-based Auditing
In case of selecting agent-based auditing, the agent to collect logon and logoff events will be installed by default the server. So, there is no additional steps are required to be performed except the default steps illustrated herein below for server.
Steps for Agentless Auditing
In case of agentless auditing, no agent will be installed on server to collect the logon and logoff events. Therefore, it is required to install a module agent on a Domain Controller of the domain, which will collect these events and pass it to software.
A separate installer file to install logon/logoff module will be supplied with the downloaded setup. It is required to run this installer file and install Logon/Logoff Audit module agent on any domain controller of the domain. Please refer to page "Install Logon/Logoff Module" page of Help file to know more about it.

Figure 8: Document showing further steps to be performed

5. Create Group Policy Object at Server

Execute the steps below at the domain, of which logon/logoff monitoring you want to enable.

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

🔜 Group Policy Management	
🛃 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp	_ . .
Group Policy Management Forest: cod.com Forest: cod.com Cod.com	Group Policy Management Contents Name Forest: cod.com

Figure 9: Group Policy Management

- 2 In the left panel, expand the nodes to reach the node of the domain controller.
- 3. Right click on the node of the domain to access the following contextmenu.



Figure 10: Context Menu for a DC in Group Policy Management

- 4. Select the option "Create a GPO in this domain, and Link here...". It displays the following dialog box to create a new Group Policy Object (GPO).
- 5. Provide a name for the new Group Policy e.g. "Logon Logoff byLepideAuditor".

🛃 New GPO		×
<u>N</u> ame:		
Logon Logoff by LepideAuditor		
Source Starter GPO:		
(none)		•
	OK	Cancel

Figure 11: Providing a name for the GPO

6. Click "OK". It creates the new GPO and shows it in the Group Policy Management.



Figure 12: Showing the newly created GPO

7. Right click on this newly created GPO.



Figure 13: Right Click Menu for the new GPO

- 8. Select the option "Edit" in this context menu. Doing this shows "Group Policy Management Editor" console.
- 9. In the left pane, go to "Logon Logoff by LepideAuditor" \rightarrow "User Configuration" \rightarrow "Policies" \rightarrow "Windows Settings" \rightarrow Scripts (Logon/Logoff)". It displays two policies "Logon" and "Logoff" in the Right Panel.



Figure 14: Showing Logon and Logoff Policies

- 10. Here, you have to modify any of these two policies. In this test case, we are modifying the logon policy.
- 11. Double click the "Logon" policy in the Right Panel to access the following dialog box.

ogon Properties		? ×
Scripts PowerShell Scripts		
Logon Scripts fo	r Logon Logoff by LepideAu	ditor
Name	Parameters	I I
		Шр
		Do <u>w</u> n
		A <u>d</u> d
		<u>E</u> dit
		<u>R</u> emove
To view the script files stored the button below. <u>S</u> how Files	d in this Group Policy Object,	press
	OK Cance	Apply

Figure 15: Logon Properties

12. Click "Add" on this tab. It displays the following box to add a script.

Add a Script	×
Script Name:	
	Browse
Script <u>P</u> arameters:	
OK	Cancel

Figure 16: Dialog box to add a logon script

13. Click "Browse" in this new box. Leave this box opened up as it is.

Browse					×
User • So	cripts 👻 Logon	- 🛃	Search Logon		2
Organize 🔻 New folder					
🚖 Favorites	Name *	Date modified	Туре	Size	
🥽 Libraries					
🖳 Computer					
🙀 Network					
File <u>n</u>	ame:	•	All Files		-
			<u>O</u> pen	C	ancel

Figure 17: Dialog box to open a logon script file

14. Open the shared folder where you have copied the "Logon.exe" script file. Copy it.



Figure 18: Copying file "Logon.exe

15. Paste this file "logon.exe" in the folder section of the "Browse" window.

Browse				×
🕞 💮 📕 🕶 User 🕶 So	cripts 👻 Logon	👻 🚱 Search Logon		<u> </u>
Organize 🔻 New folder			:= 🕶 🔳 🔞	
☆ Favorites	Name *	Date modified	Туре	
💻 Desktop 🚺 Downloads 📃 Recent Places	\} Logon	12/26/2016 4:23 PM	Application	
ibraries i Documents i Music i Pictures Videos				
🌉 Computer				
🙀 Network				
	•			▶
File <u>n</u>	ame: Logon	All Files	Cancel	

Figure 19: Pasted the file named "Logon.exe

16. Select the file and click "Open". It opens the file and takes you back to the "Add a Script" box, which now displays the selected file.

Add a Script		×
Script <u>N</u> ame:		
Logon.exe	Browse.)
Script Parameters:		
	OK Cance	!

Figure 20: File has been selected

17. Click "OK". It takes you back to the "Logon Properties".

Logon Properties	? ×
Scripts PowerShell Scripts	
Logon Scripts for Logon Logoff by LepideAudi	tor
Name Parameters	
Logon.exe	Цр
	Do <u>w</u> n
	Add
	Edit
	<u></u>
	<u>R</u> emove
To view the script files stored in this Group Policy Object, p the button below.	press
Show Files	
<u>3</u> 11044 Files	
OK Cancel	

Figure 21: Required Logon Properties

- 18. Click "Apply" to apply the changes.
- 19. Click "OK" to close the "Logon Properties".
- 20. Close "Group Policy Management Editor" console.
- 21. Come back to "Group Policy Management" console.
- 22. Select the newly created/modified policy in the Left Panel. It shows its details in the Right Panel.

Figure 22: Showing the properties of newly created policy

- 23. In its Right Panel, the "Security Filtering" section lets you select the objects such as users, groups, and computers on which this policy will be applied.
- 24. Click "Add" to display the box to add the objects upon which this policy will be applicable.

Select User, Computer, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	<u>O</u> bject Types
Erom this location:	
cod.com	Locations
Enter the object name to select (<u>examples</u>):	
Everyone	<u>C</u> heck Names
Advanced	OK Cancel

Figure 23: Select the objects to be affected by this policy

- 25. Type "Everyone" in the text box and click "Check Names". It selects all objects.
- 26. Click "OK" to confirm the change. It takes you back to the "Group Policy Management" window, which now displays the newly added object.

🛃 Group Policy Management	
Eile Action View Window Help	_ B ×
(= -) 2 🔐 Q 🔢 🖬	
Group Policy Management A Forest: cod.com God Default Domain Policy Default Domain Policy Default Domain Policy Default Domain Controllers Default Domain Controllers Default Policy Objects Group Policy Objects Sites Group Policy Modeling Group Policy Modeling Group Policy Results	Logon Logoff by LepideAuditor Scope Details Settings Delegation Links Display links in this location: cod.com The following sites, domains, and OUs are linked to this GPO: Ink Enabled Location Enforced Link Enabled Path Enforced Link Enabled Path Enforced Link Enabled Path Inforced Link Enabled Path No Yes doc.com Image: Inforced No Yes Inforced Security Filtering The settings in this GPO can only apply to the following groups, users, and computers: Name Add Bemove Properties MMI Filtering This GPO is linked to the following WMI filter: Inforce Image: Inforced Image: Image

Figure 24: Showing 'Everyone' in Security Filtering

- 27. Close the "Group Policy Management" console.
- 28. Go to Run or Command Prompt and type the command "gpupdate".
- 29. Press Enter to run the "gpupdate" command to update the group policies.



Figure 25: Updated the Group Policies successfully

30. It is required to logoff the current user and then logon again in the Windows Server to run "logon.exe" file.

You can follow the above steps to enable both the collection of logon/logoff events and to generate relevant reports, alerts, and LiveFeed updates.

6. Conclusion

If you have completed these steps successfully then you are ready to start the monitoring of logon/logoff events at the domain level. These events will now be captured and audited by LepideAuditor. To read more about the solution, please visit <u>http://www.lepide.com/lepideauditor/</u>.

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 <u>http://www.lepide.com/contactus.html</u> 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

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.

© Lepide Software Private Limited, All Rights Reserved.

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, 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.

Microsoft®, Windows®, and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

