%Lepide

CONFIGURATION GUIDE

ENABLE LOGON/LOGOFF EVENTS

Table of Contents

IIIt oduction	3
Manage Logon/Logoff Audit Module	3
2.1. Install Logon/Logoff Audit Module	3
Generate Logon.exe file	4
Create Group Policy Object at Server	6
Support1	7
Trademarks 1	7
	Manage Logon/Logoff Audit Module

1. Introduction

This 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 the application server which will process logon/logoff events and send it to the software for display.

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 schedules for above reports.

NOTE: This module is not supported in the Least Privilege Model.

2. Manage Logon/Logoff Audit Module

The steps to install, manage, and uninstall the logon/logoff Audit Module are explained as follows:

2.1. Install Logon/Logoff Audit Module

To audit logon/logoff events, you will need to install the **Lepide Data Security Platform Logon/Logoff Audit Module** on the application server to collect logon/logoff events. The installer file for this module will come with setup file, which you can download from our website. 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 the installation.
- 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 folder in 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.
- 9. Click **Next** to proceed further. The software is now ready to be installed.

- 10. Click **Install** to begin the installation procedure.
- 11. Once installed, the following page is displayed. It asks for the login credentials of a user with administrative privileges.

💥 Setup - Lepide Logon/Log	_		\times	
Create service wizard It is recommended to run account must have logon				
User Account :	Administrator			
Password :	•••••			
Domain Name :	LepideCorporate.com			
		Next >	Ca	incel

Figure 1: Add Login Credentials of an Administrator to Create the Service

- 12. Click **Next** after entering the login credentials of an administrator. The next page displays the message of successful installation of the module.
- 13. Click **Finish** to complete the process.

3. Generate Logon.exe file

Perform the following steps to generate the **logon.exe** file.

- 1. Use any of the following methods to start with this process.
 - a. Click on the domain on the settings page and go to the properties.
 - b. In domain properties, go to **Object Class and Other Settings** to access the following settings.

		×
Organizational Unit Settings	Object Classes and Other Settings Please select object classes and other settings to be aut Audit: All Object Classes	dited
Object Classes and Other Settings	Active Directory Object Classes	Exchange Server Object Classes
Archive Settings	2	م م
	More Audit Settings Audit Failed Logon Audit Successful User Logon/Logoff	
		OK Cancel

Figure 2: Modifying Object Class and Other Settings

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

	×
Create Logon/Logoff Script	
Enter IP address of machine where Logon/Logoff Server is installed	
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 :	
C: \Users\frank\Documents\	?
OK Cancel	

Figure 3: Dialog box to Create Logon/Logoff Script

4. Enter the IP Address of the application server, where Logon/Logoff Audit Module has been installed.

- 5. Click icon to select the location on the server to the save this executable file.
- 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.



Figure 4: Successfully Generated Executable File

4. Create Group Policy Object at Server

Execute the steps below at the domain, of which logon/logoff monitoring you want to enable. (This can be done by opening **gpmc.msc** on the application server as well)

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



Figure 5: Group Policy Management

2. Right click on the node of the domain to access the following context menu:

📓 Group Policy Management		-	- 🗆 🗙
📓 File Action View Window	Help		_ 8 ×
🗢 🔿 📅 🧟 🕅			
Group Policy Management Composition Compos	Group Policy Management Contents Name Create a GPO in this domain, and Link it here Link an Existing GPO Block Inheritance Group Policy Modeling Wizard New Organizational Unit Search Change Domain Controller Remove Active Directory Users and Computers New Window from Here Refresh Properties Help	^	

Figure 6: Context Menu for a Domain in Group Policy Management

3. 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).

New GPO	×
Name:	
Lepide Logon Logoff	
Source Starter GPO:	
(none)	~
	OK Cancel

Figure 7: Providing a Name for the GPO

- 4. Provide a name for the new Group Policy e.g, Lepide Logon Logoff.
- 5. Click **OK**. It creates the new GPO and shows it in the **Group Policy Management** window.



Figure 8: Figure 9: Showing the Newly Created GPO

- 6. Right click on the newly created GPO and click Edit to access Group Policy Management Editor console.
- 7. In the left panel, go to Lepide Logon Logoff, User Configuration, Policies, Windows Settings, Scripts (Logon/Logoff). It displays two policies Logon and Logoff in the right-hand panel.

Group Policy Management Editor			-	\times
File Action View Help				
🗢 🔿 🚈 🔜 🛛 🖬				
 Policies Policies Policies Policies Software Settings Software Settings Scripts (Logon/Logoff) Security Settings Folder Redirection Ministrative Templates: Policy definitions (ADMX file Preferences 	Scripts (Logon/Logoff) Select an item to view its description.	Name E Logon Logoff		
< >>	\Extended \Standard /			

Figure 9: Showing Logon and Logoff Policies

- 8. Here, you must modify the logon policy.
- 9. Double click **Logon** policy in the right-hand panel to access the following dialog box:

Logon Properties		?	×
Scripts PowerShell Scripts			
Logon Scripts f	or Lepide Logon Logoff		
Name	Parameters	Up Down	
		Add	
		Edit	
		Remove	
To view the script files store the button below. Show Files	ed in this Group Policy Object, p	press	-
	OK Cancel	Apply	

Figure 10: Logon Properties

10. Click **Add** on this tab. It displays the following box to add a script.

Add a Script	×
Script Name:	Browse
Script Parameters:	biowae
ОК	Cancel

Figure 11: Dialog box to add a logon script

11. Click **Browse** in this new box. Leave this box displayed as it is.

Browse					×
\leftrightarrow \rightarrow \checkmark \uparrow \bullet Policies \rightarrow {31B2	F340-016D-11D2-945F-00C04FB984F9} >	USER > Scripts > Logon	5 V	Search Logon	م
Organize 🔻 New folder					
🕂 Downloads	^ Name ^	Date modified	Туре	Size	
👌 Music		No items match your s	earch.		
Pictures		no kens materi yours	concrit		
🗃 Videos					
🏪 Local Disk (C:)					
LDSPSRV (E:)					
🗫 pCloud Drive (P:)					
💣 Network					
DESKTOP-MIG9					
DMO43					
KR710					
LDSP					
LDSP36					
🔜 LepideCorporate.com					
File annual				AUTIM	
File name:			~	All Files	~
				Open	Cancel

Figure 12: Dialog Box to Open a Logon Script File

12. Open the folder where you have saved the **Logon.exe** script file in section 3. Choose **Copy**.



Figure 13: Copying the Logon.exe File

13. Paste this file **logon.exe** in the folder section of the **Browse** window. Copy the path of Logon.exe from the address bar at the top.

Browse								×
	pideCorporate.com\Policies\{E951EF9D-3C26-4295	-8897-EBBC9D961E83}\User	\Scripts\Logon 🗸	ō	Search Logon			Q
Organize 🔻 New folde	er					-		0
System32 ^	Name	Date modified	Туре	Size				
💻 This PC	🚻 Logon	12/12/2022 7:49 PM	Application	3	341 KB			
3D Objects								
E Desktop								
Documents								
🕂 Downloads								
b Music								
E Pictures								
💾 Videos								
🏪 Local Disk (C:)								
LDSPSRV (E:)								
🐅 pCloud Drive (P:								
💣 Network								
~								
File na	ame: Logon			~	All Files			~
	L				Open	(Cancel	

Figure 14: Logon.exe Filename Pasted

14. This process is used to place the **Logon.exe** file in the default **SYSVOL** location of the domain. Click **Cancel** and then exit the window.

Add a Script		×
Script Name:		
		Browse
Script Parameters:		
	OK	Cancel

Figure 15: Add a Script

- 15. Click **OK**. It takes you back to the **Logon Properties**.
- 16. Click **Cancel** and exit the GPO settings.
- 17. In the Group Policy Management Editor, Go to Administrative Templates, System, Logon
- 18. Enable the setting **Run these programs at user logon.** Click on **Show**.

s at user logon	— L X	(
s at user logon	Previous Setting Next Setting	
Comment:	^	
	~	4
Supported on:	At least Windows 2000	
	· · · · · · · · · · · · · · · · · · ·	/
	Help:	
Show	This policy setting specifies additional programs or documents that Windows starts automatically when a user logs on to the system. If you enable this policy setting, you can specify which programs can run at the time the user logs on to this computer that has this policy applied. To specify values for this policy setting, click Show. In the Show Contents dialog box in the Value column, type the name of the executable program (.exe) file or document file. To specify another name, press ENTER, and type the name. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file. If you disable or do not configure this policy setting, the user will have to start the appropriate programs after logon. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the system starts the programs specified in the Computer	<
	s at user logon Comment: Supported on: Show	s at user logon Previous Setting MextSecting Comment:

Figure 16: Run these Programs at User Logon

19. Paste the path in the **Value** field and add **Logon.exe** at the end. Click **OK**. Please see the screenshot below:

how (Contents				_		×
tems	to run at logon						
	Value						
	\Policies\{E951E	F9D-3C26-4295	-8897-EBBC9	D961E83}\U	ser\Scripts\L	ogon\Log	on.exe
					ОК	Canc	el
		Figure 1	7: Show (Contents			

- 20. Click **Apply** and exit the window.
- 21. In the Group Policy Management Editor, Go to **Administrative Templates**, **Windows Components**, **Attachment Manager**.

Group Policy Management Editor					- a ×
File Action View Help					
← → 2 m → 0 m 7					
I Lepide Logon Logoff [LPDC1_LEPIDECORPORATE.COM] Policy	Attachment Manager				
V 👫 Computer Configuration		1			
> Policies	Inclusion list for low file types	Setting	State	Comment	
> C Preferences	Edit policy settion	Notify antivirus programs when opening attachments	Not configured	No	
v 🅵 User Configuration	con princy manny.	Trust logic for file attachments	Not configured	No	
V 🧾 Policies	Requirements:	Do not preserve zone information in file attachments	Not configured	No	
> 📫 Software Settings	At least Windows XP Professional	E Hide mechanisms to remove zone information	Not configured	No	
V 🛄 Windows Settings	with SP2	Default risk level for file attachments	Not configured	No	
Scripts (Logon/Logoff)	Description	😥 Inclusion list for high risk file types	Not configured	No	
> 🔁 Security Settings	This policy setting allows you to	😥 Inclusion list for low file types	Not configured		
> 🤐 Folder Redirection	configure the list of low-risk file	inclusion list for moderate risk file types	Not configured	No	
> III Policy-based QoS	types. If the attachment is in the list				
Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.	of low-risk file types, windows will not promot the user before accession				
> Control Panel	the file, regardless of the file's zone				
> Desktop	information. This inclusion list				
> Network	overrides the list of high-risk file				
Shared Folders	types built into Windows and has a lower precedence than the high-rick				
> Start Menu and laskbar	or medium-risk inclusion lists (where				
) jugarni	an extension is listed in more than				
V windows components	one inclusion list).				
Add features to windows Tu	Management of the section of the sec				
App runtime	can specify file types that pose a low				
Allackment Manager	risk.				
Autofilia Delivier					
Calculater	If you disable this policy setting,				
Cloud Content	Windows uses its default trust logic.				
Credential Unar Interface	If you do not configure this policy				
Data Collection and Deniau Builds	setting, Windows uses its default trust				
Deriton Gednete	logic.				
Desiton Window Manager					
Digital Locker					
Edge III					
> File Explorer					
File Revocation					
IME INE					
Instant Search					
> Calinternet Explorer					
Location and Sensors					
> Microsoft Management Console					
> Microsoft User Experience Virtualization					
Multitasking					
> 🧾 NetMeeting					
Network Sharing					
OOBE					
Presentation Settings					
> 🧱 Remote Desktop Services					
RSS Feeds					
Search					
Sound Recorder					
Store					
> III NDHEPL V	Extended Standard				
8 setting(s)					

Figure 18: Attachment Manager

22. Click on **Inclusion List for Low File Types.** Enable it and type **Logon.exe** in the Options Box.





Figure 19: Inclusion List for Low File Types

- 23. Close the **Group Policy Management Editor** console.
- 24. Come back to Group Policy Management console.
- 25. Select the newly created/modified policy in the Left Panel. It shows its details in the right-hand panel.

📓 Group Policy Management						-	пх
🔜 File Action View Window Help							_ & ×
🗢 🔿 🙍 📰 🗙 🙆 📓 🖬							
Group Policy Management ✓ ▲ Forest: LepideCorporate.com ✓ ➡ Domains ✓ ➡ LepideCorporate.com ➡ LepideLogonLogoff ➡ Lepide New Logon Logoff ➡ Lepide New Logon Logoff ➡ Lepide New Logon Logoff ➡ Europe > ➡ Europe > ➡ Marketing > ➡ Marketing > ➡ Marketing > ➡ Group Policy Objects > ➡ Group Policy Objects > ➡ Stater ∰ Group Policy Modeling ➡ Group Policy Results	Lepide Logon Log Scope Details Settin Links Display links in this locat The following sites, dom Location Location Location LepideCorporate.co Security Filtering The settings in this GPO Name Latherticated User	off ja Delegation on: LepideC ains. and OUs are Inked m can only apply to the fo	orporate.com d to this GPO: Enforced No	Link Enabled Yes	Path LepideCorporate.com		
	Add	Remove	Properties				
	WMI Filtering This GPO is linked to th <none></none>	e following WMI filter:	~	Open			
	1						

Figure 20: Showing the Properties of Newly Created Policy

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



Figure 21: Updated the Group Policies successfully

29. You will need to logoff the current user and then logon again in the Windows Server to run **logon.exe** file.

5. Support

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

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 <u>https://www.lepide.com/contactus.html</u> 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 solution, visit https://www.lepide.com/data-security-platform/.

6. Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform 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.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.

