



CONFIGURATION GUIDE

ENABLE LOGON/LOGOFF EVENTS

Table of Contents

- 1. Introduction..... 3
- 2. Manage Logon/Logoff Audit Module 3
 - 2.1. Install Logon/Logoff Audit Module 3
- 3. Generate Logon.exe file..... 4
- 4. Create Group Policy Object at Server..... 6
- 5. Support 17
- 6. Trademarks 17

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.

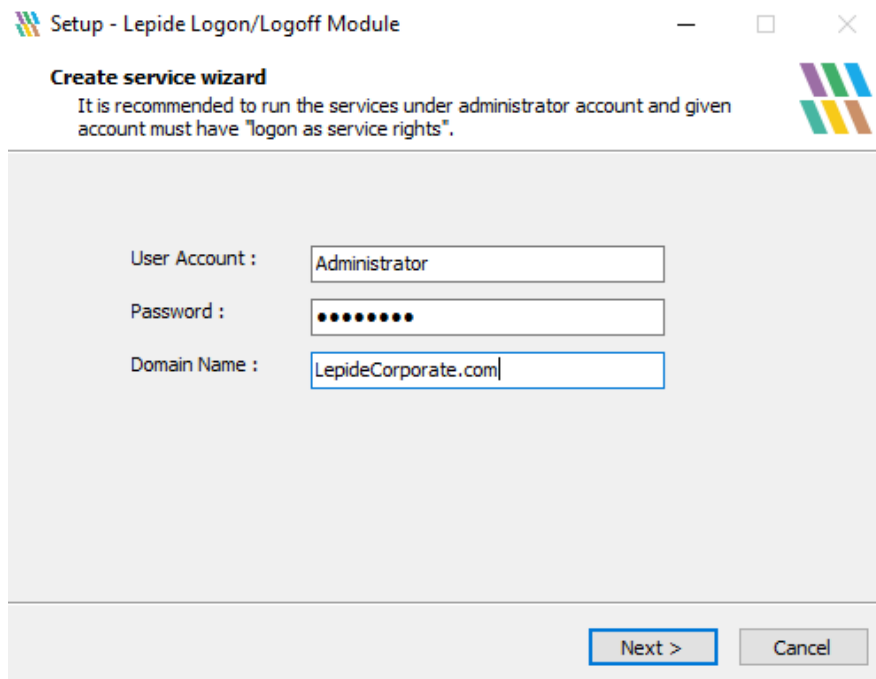


Figure 1: Add Login Credentials of an Administrator to Create the Service

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.

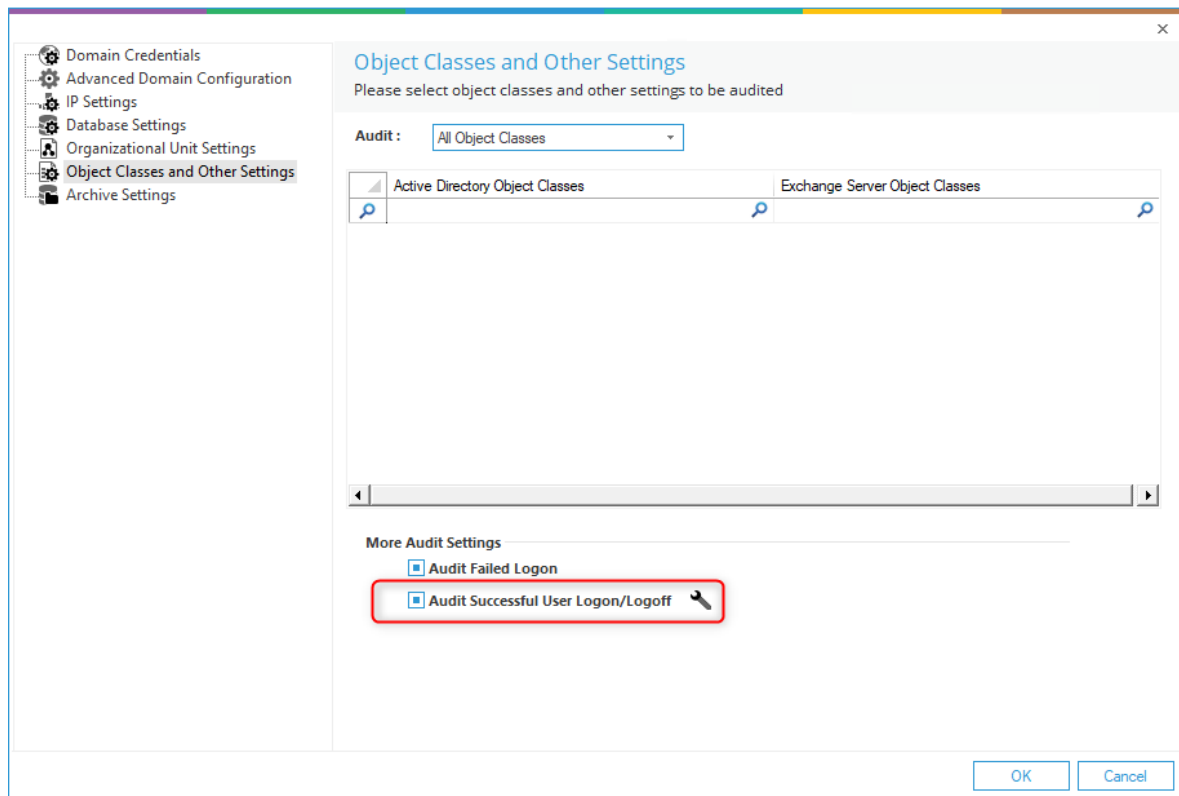



Figure 2: Modifying Object Class and Other Settings

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

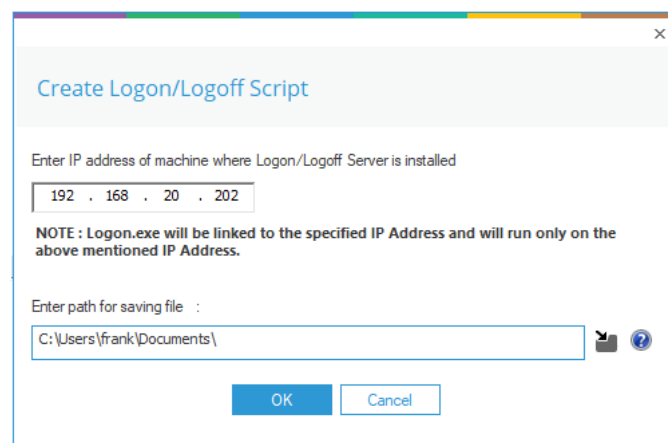



Figure 3: Dialog box to Create Logon/Logoff Script

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 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.

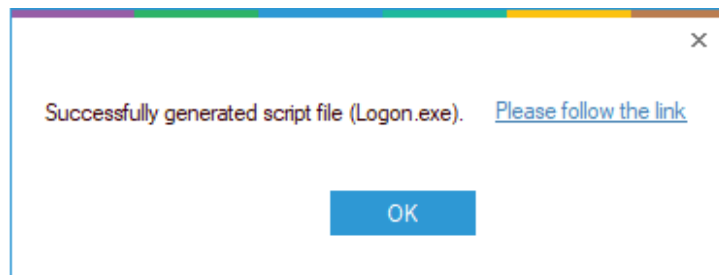


Figure 4: Successfully Generated Executable File

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**.

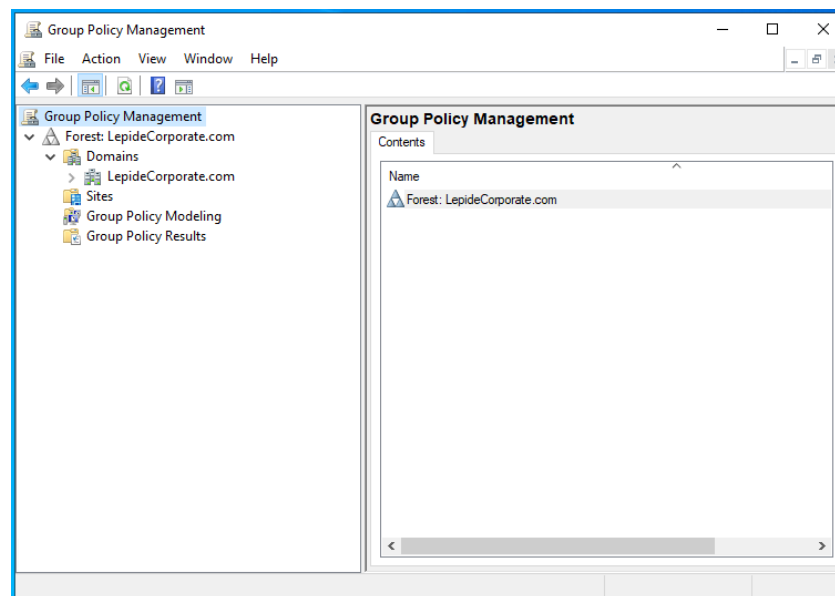


Figure 5: Group Policy Management

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

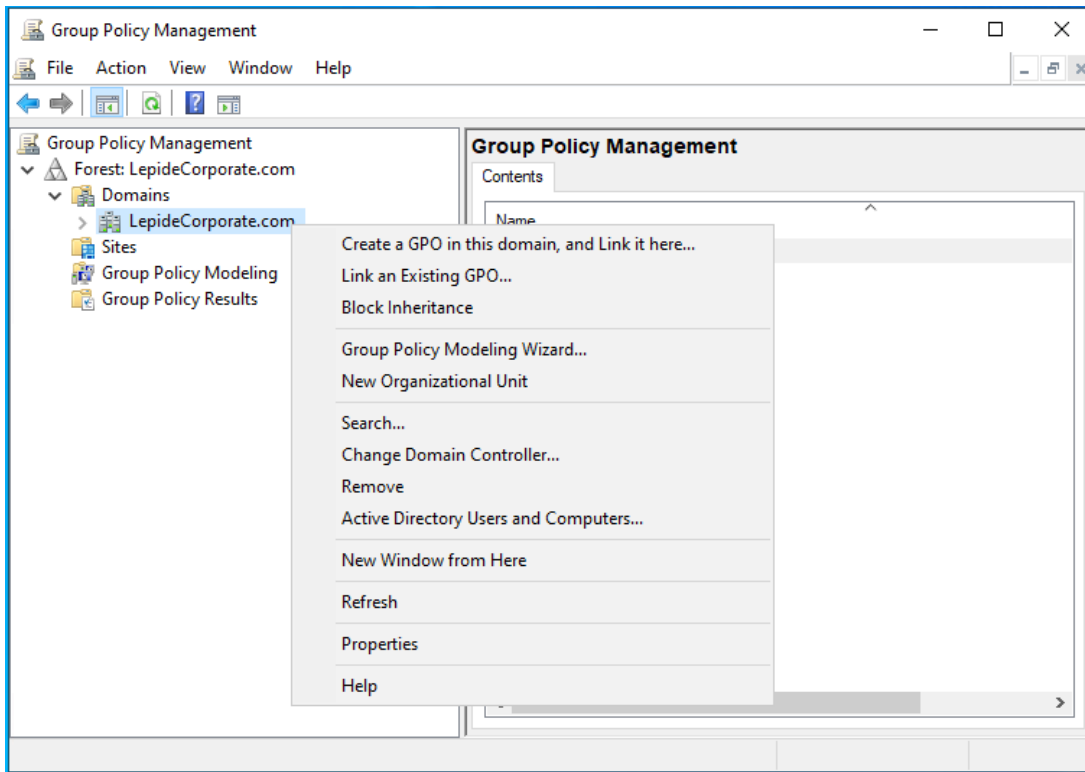


Figure 6: Context Menu for a Domain in Group Policy Management

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).

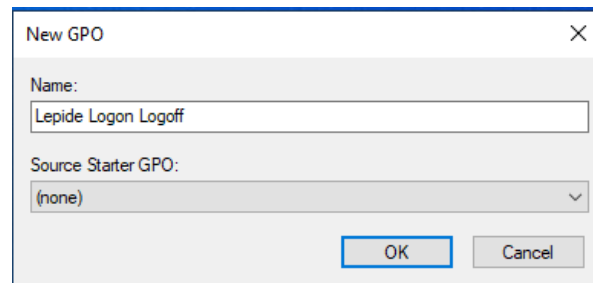


Figure 7: Providing a Name for the GPO

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.

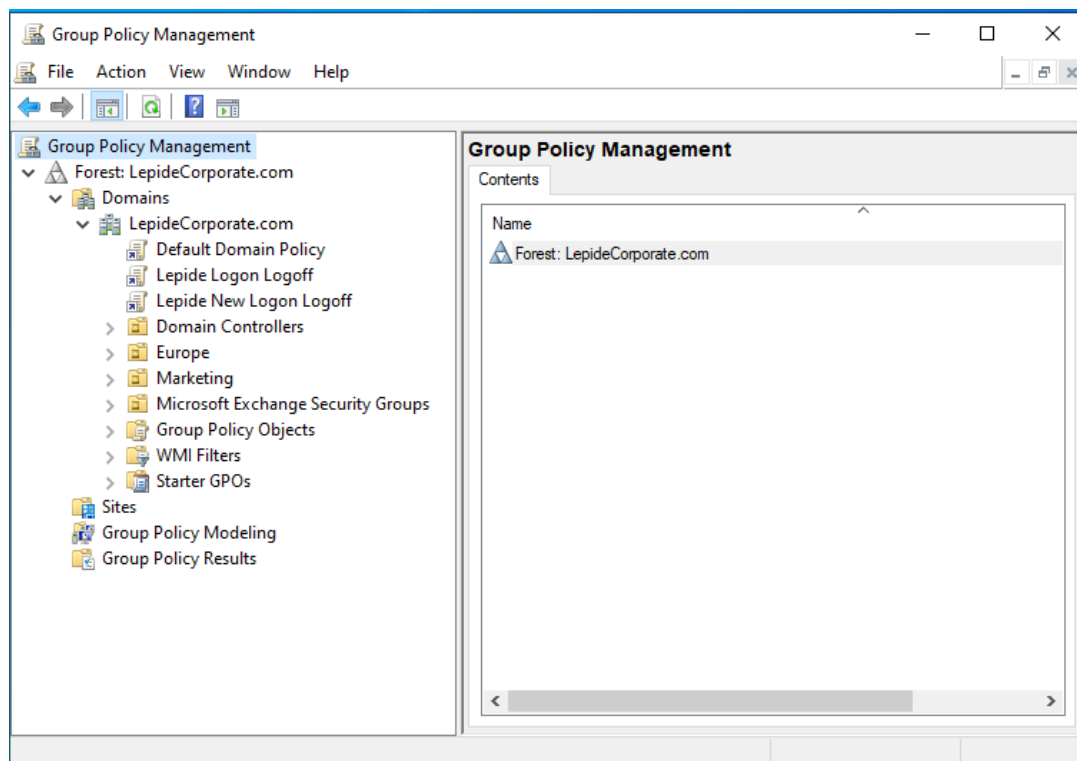


Figure 8: Figure 9: Showing the Newly Created GPO

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.

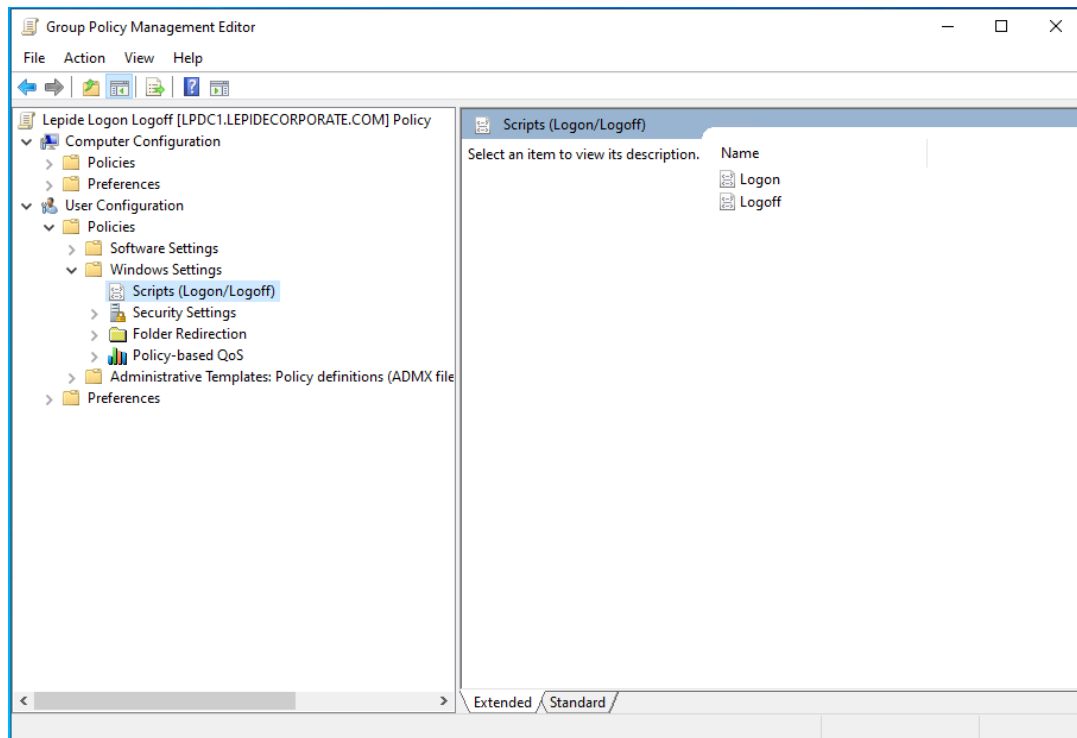


Figure 9: Showing Logon and Logoff Policies

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

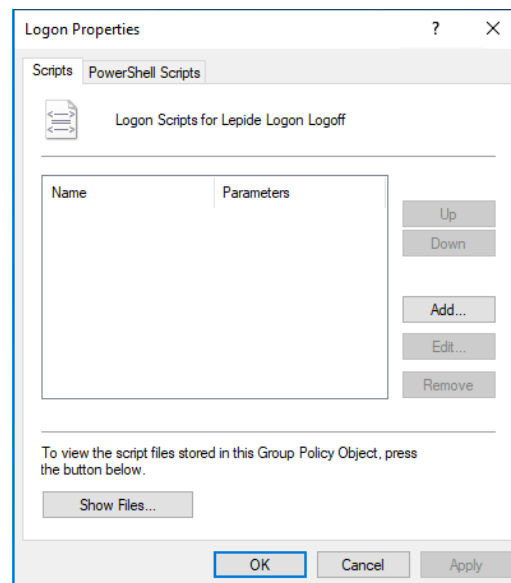


Figure 10: Logon Properties

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

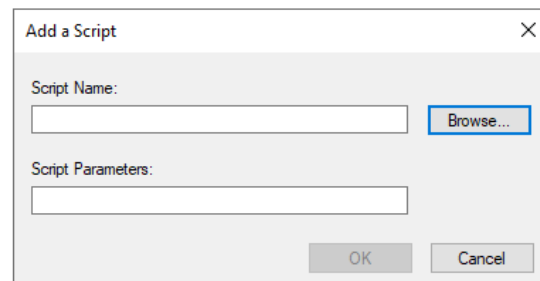


Figure 11: Dialog box to add a logon script

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

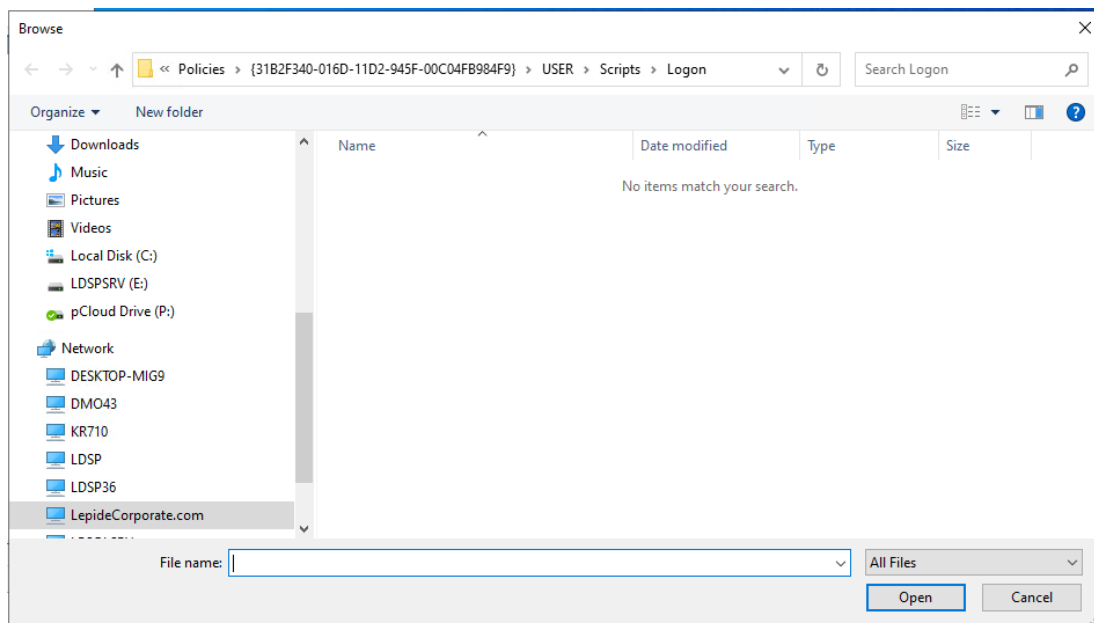


Figure 12: Dialog Box to Open a Logon Script File

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

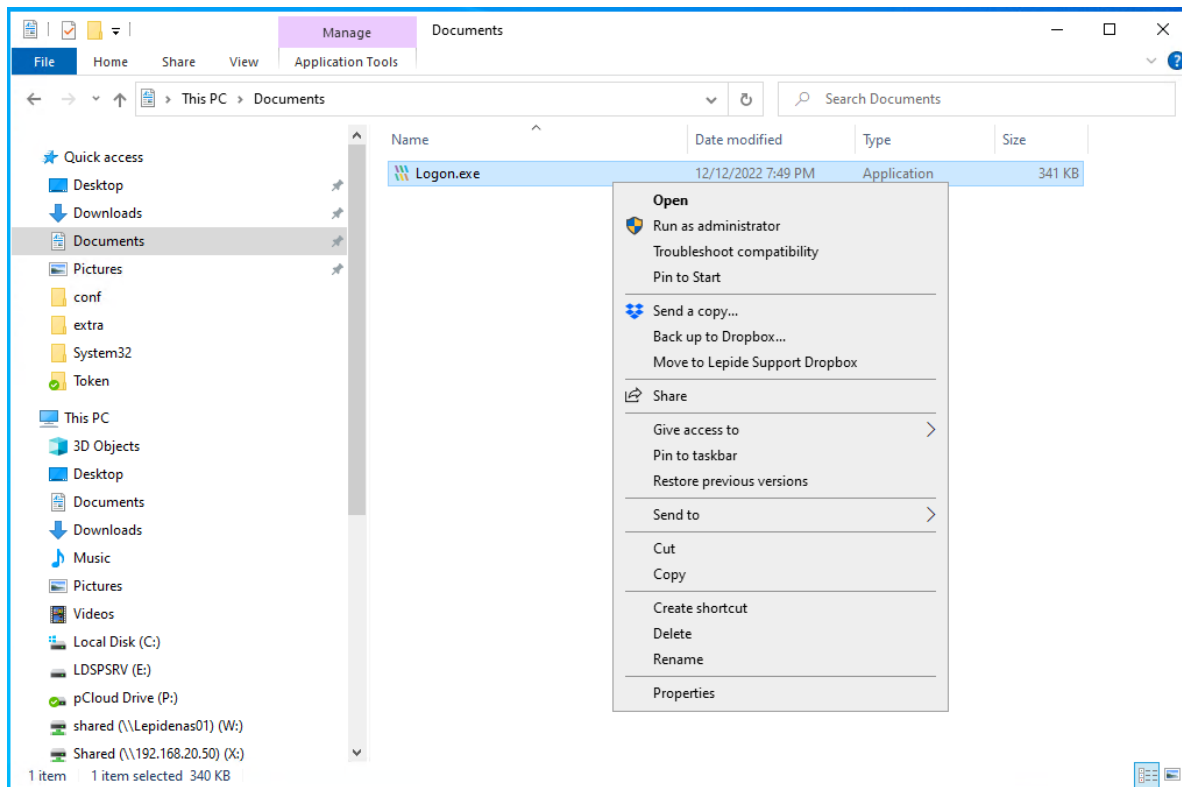


Figure 13: Copying the Logon.exe File

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.

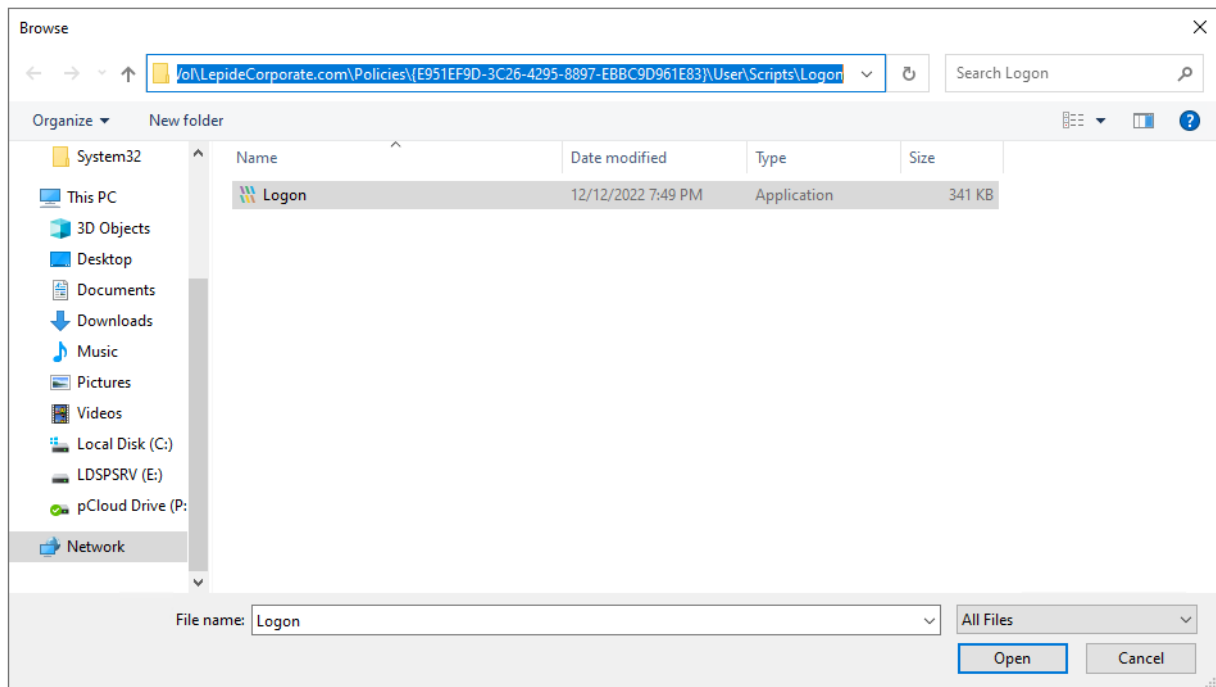


Figure 14: Logon.exe Filename Pasted

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.

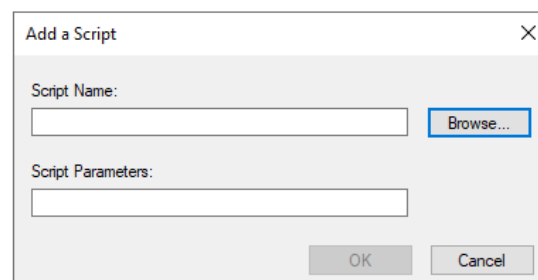


Figure 15: Add a Script

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**.

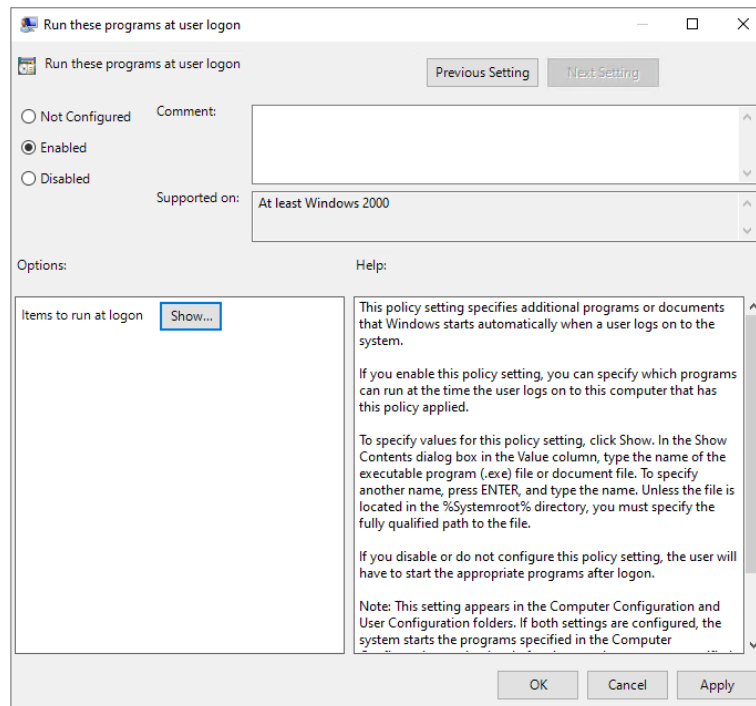


Figure 16: Run these Programs at User Logon

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

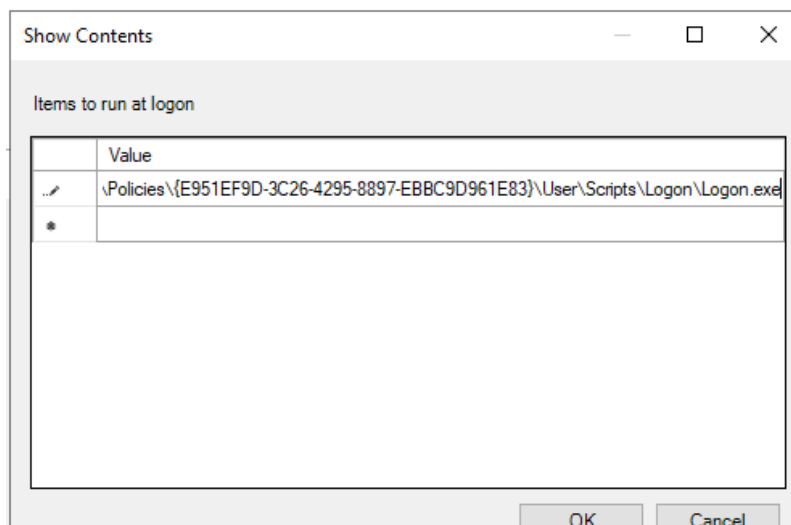


Figure 17: Show Contents

20. Click **Apply** and exit the window.

21. In the Group Policy Management Editor, Go to **Administrative Templates, Windows Components, Attachment Manager**.

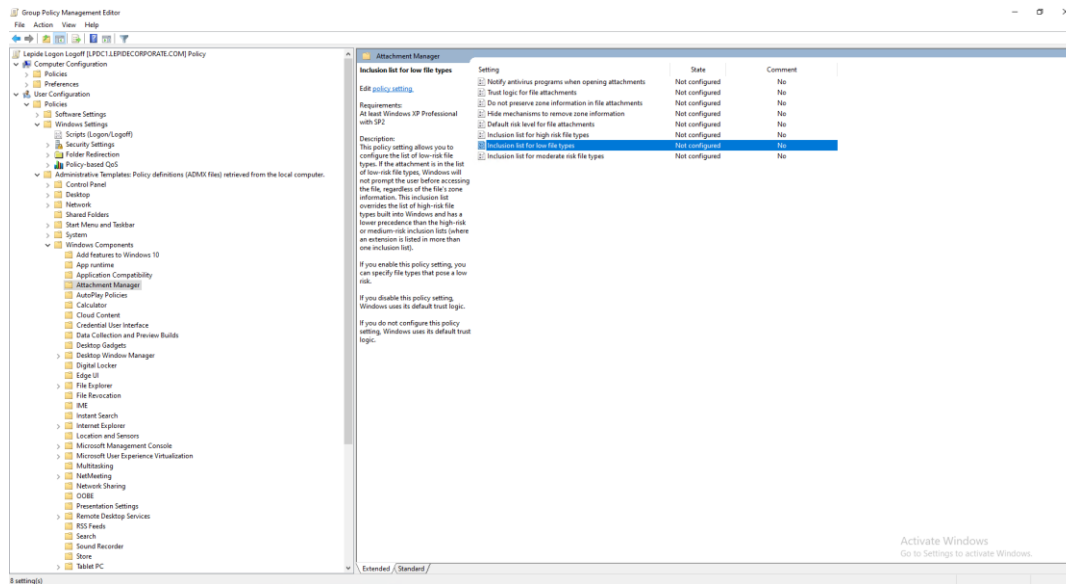


Figure 18: Attachment Manager

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

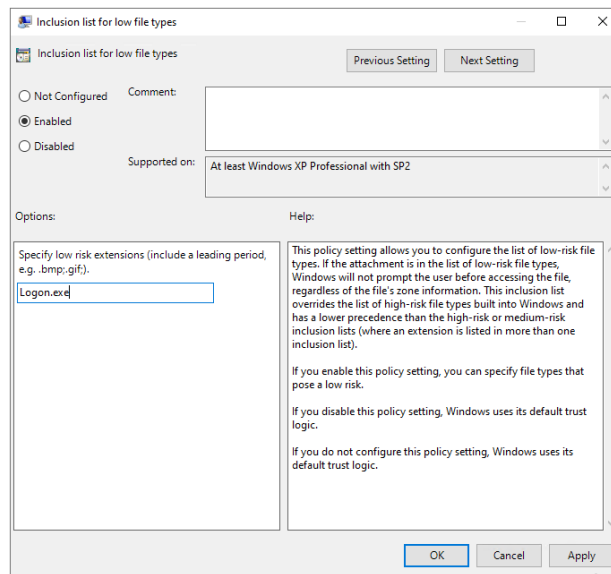


Figure 19: Inclusion List for Low File Types

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.

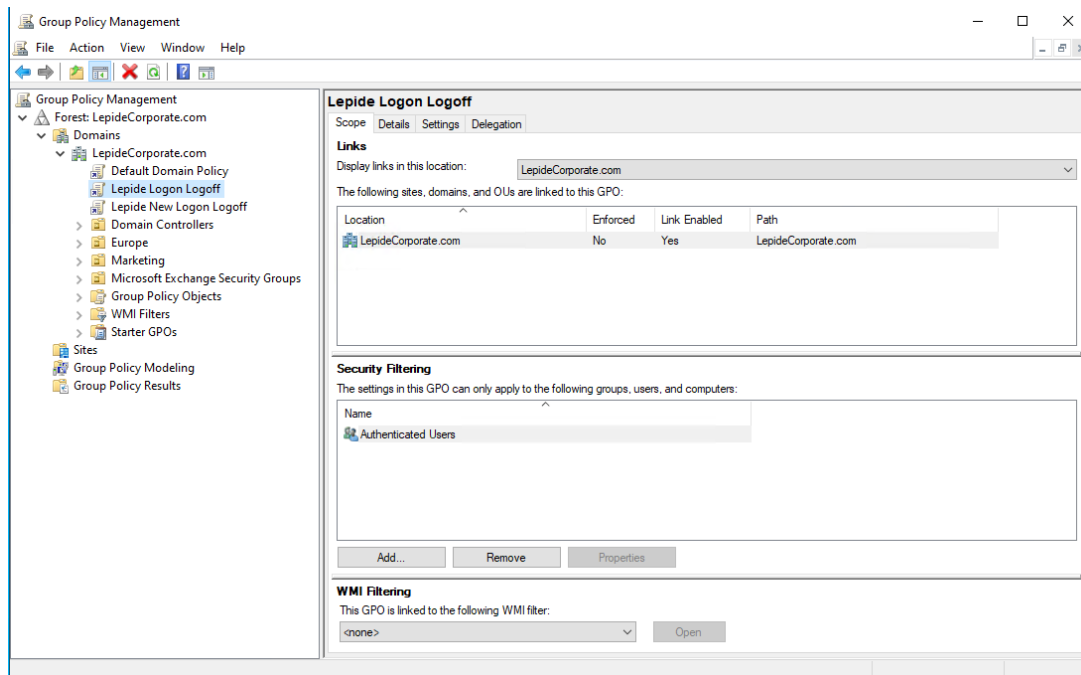


Figure 20: Showing the Properties of Newly Created Policy

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.

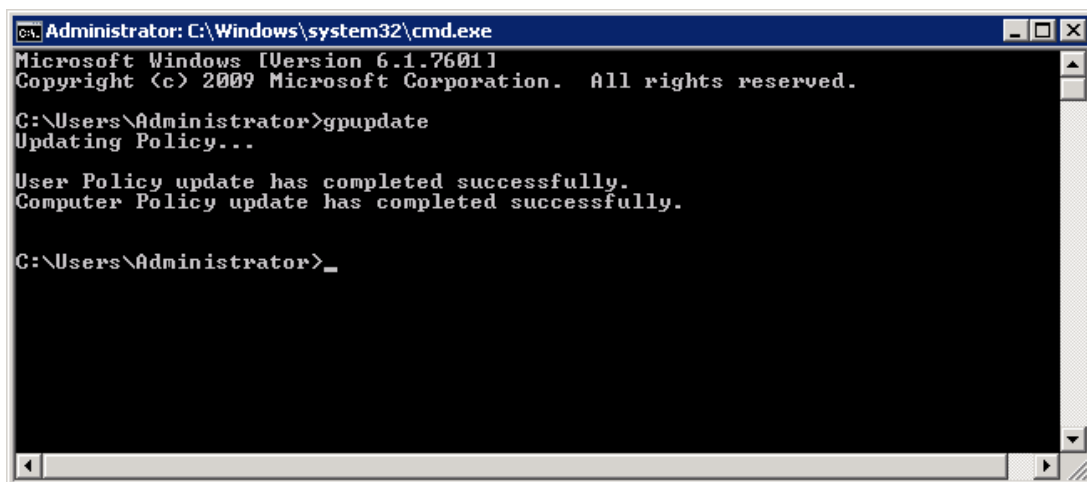


Figure 21: Updated the Group Policies successfully

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 <https://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 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.