Standalone GPO Backup & Import Guide/Documentation

What is LGPO.exe?

- LGPO.exe is a Tool that is used for Backing-Up and Importing Group Policy Objects to and from Local Machines.
- LGPO.exe is Utilized Directly from the Command Prompt with Flags
- LGPO.exe can Import an Entire Directory of Group Policy Objects.
    - Ex: You can Import the Folders Containing "**Google**", "**Microsoft**", and "**Microsoft Edge**" Group Policy Objects all at Once with LGPO.exe.
    - A .ADMX File is a Group Policy Object File
- This Tool can Save a Significant Amount of Time for the Hardening Process of Standalone Machines

How to Get LGPO.exe

- **Note:** The Target Machine Must Run on a Windows 10 Operating System.
- LGPO.exe is Part of the Microsoft Security Compliance Toolkit 1.0, which can be Downloaded Here: **https://www.microsoft.com/en-us/download/details.aspx?id=55319**
- You Could Also Download the Attached "**LGPO.zip**" File
    - LGPO.zip
- Once you have Downloaded the "**LGPO.zip**" File, Copy it to an External Hard Drive or USB.
- Plug the External Hard Drive or USB into the Target Machine, and Copy the "**LGPO.zip**" File to any Directory of your choice on the Target Machine.
- Open the "**LGPO.zip**" File, on the Target Machine, and Extract the "**LGPO_30**" Folder to any Directory of your choice.
- **Important:** Open File Explorer, Click on "**This PC**", Click on "**Windows (C:)**", and make sure you have a Folder Called "**Temp**". If you Do Not Have this Folder, Make Sure you Create it.
- Once the "**LGPO_30**" Folder has been Extracted, and you Verified that you have the "**C:\Temp**" Folder, you are good to go!

How to Backup GPOs with LGPO.exe

1. Run the Command Prompt as Administrator
2. Type in "**cd [Directory Path for the Extracted LGPO Folder]**" and then Press "**Enter**".
    a. Ex: **"cd C:\Users\Administrator\Desktop\LGPO_30"**
3. Type in "**lgpo.exe /b C:\Temp**" and then Press "**Enter**".
    a. This will Create a Backup of your Local Group Policy Objects, and Store them in the "**C:\Temp**" Folder.
        i. You Should See an Output that Says: **"Creating LGPO backup in "C:\Temp\{347BC0C8-3911-466F-B8C7-5CF2CB741323}""**
    b. **Note:** This **/b** Option will not back up MLGPO Configuration Settings.
4. Open File Explorer, Click on "**This PC**", Click on "**Windows (C:)**", Click on "**Temp**", and if Everything Worked Properly you should see a Folder Similar to this, "**{347BC0C8-3911-466F-B8C7-5CF2CB741323}**".
5. You have Successfully Completed an LGPO Backup!

----------WORK-IN-PROGRESS----------

How to Import GPOs with LGPO.exe (From a GPO Backup)

For this Guide we will be using the **DISA STIG GPOs** as an Example, which can be obtained at: **https://public.cyber.mil/stigs/gpo/**

1. Once you have Downloaded your GPO File ("**LGPO.zip**" or), Copy it to an External Hard Drive or USB.
2. Plug the External Hard Drive or USB into the Target Machine, and Copy the "**LGPO.zip**" File to any Directory of your choice on the Target Machine.
3. Open the "**LGPO.zip**" File, on the Target Machine, and Extract the "**LGPO_30**" Folder to any Directory of your choice.
4. Run the Command Prompt as Administrator
5. Type in "**cd [Directory Path for the Extracted LGPO Folder]**", and then Press "**Enter**".
    a. Ex: **"cd C:\Users\Administrator\Desktop\LGPO_30"**
6. In the command line type lgpo.exe /g "Path of provided GPO"
7. Import is completed.

How to Import GPOs with LGPO.exe (DISA STIG GPOs)

For this Guide we will be using the **DISA STIG GPOs** as an Example, which can be obtained at: **https://public.cyber.mil/stigs/gpo/**

1. Once you have Downloaded your GPO File ("**LGPO.zip**" or), Copy it to an External Hard Drive or USB.
2. Plug the External Hard Drive or USB into the Target Machine, and Copy the "**LGPO.zip**" File to any Directory of your choice on the Target Machine.
3. Open the "**LGPO.zip**" File, on the Target Machine, and Extract the "**LGPO_30**" Folder to any Directory of your choice.
4. Run the Command Prompt as Administrator
5. Type in "**cd [Directory Path for the Extracted LGPO Folder]**", and then Press "**Enter**".
    a. Ex: **"cd C:\Users\Administrator\Desktop\LGPO_30"**
6. In the command line type lgpo.exe /g "Path of provided GPO"
7. Import is completed.

Useful Commands and Options for LGPO.exe

- WIP

----------WORK-IN-PROGRESS----------

What does this GPO Import do?

- This GPO Import will Harden the Following STIG Checklists
  - **Windows 10 V2R5**
  - **Windows Firewall w/ Advanced Security V2R1**
  - **Adobe Acrobat Reader DC Continuous Track V2R2**
  - **MS Edge V1R6**
  - **MS Word 2016 V1R1**
  - **MS Excel 2016 V1R2**
  - **MS Publisher 2016 V1R4**
  - **MS PowerPoint 2016 V1R1**
  - **Google Chrome V2R8**
- This GPO Import Includes the **Auditing Permissions**, and **Security Permissions**, for Security-Relevant Folders (shown in the "**Changing Folder Permissions**" and "**What's Left?**" Sections of the Guide)

Requirements

- Windows 10 Operating System
- **Important:** Make Sure you Have the "**Auditors**" Security Group
  - **Verify:** Open Computer Management, Double Click on "**Local Users and Groups**", and Double Click the "**Groups**" Folder.
  - If you Do Not Have the "Auditors" Security Group
    - Right-Click the Space Below the Names of the Various Groups, and then Click on "**New Group...**".
    - For "**Group name:**" Type in "Auditors" (you could also add a description if you would like), Click "**Create**", and then Click "**Close**".
    - If Done Correctly, the Auditors Group Should Appear in the List (usually at the bottom of the list).
- Symantec, Splunk, WinZip
- Download the Attached "**Standalone GPO.zip**", "**ADMX Templates.zip**" and "**ADMX Templates - en-US.zip**" Files, Copy them to an External Hard Drive or USB, and Copy these Files to the Target Standalone Workstation.

Standalone GPO.zip ADMX Templates.zip ADMX Templates - en-US.zip

- Ensure you put the Files from the "**ADMX Templates.zip**" Folder (**access15.admx**, **access16.admx**... **AcrobatDCContinuous.admx**) into the "**C:\Windows\PolicyDefinitions**" Folder.
  - If you get the prompt "**The destination has # files with the same names**", Click on "**Replace the files in the destination**".
- Ensure you put the Files from the "**ADMX Templates - en-US.zip**" Folder (**access15.adml**, **access16.adml**... **AcrobatDCContinuous.adml**) into the "**C:\Windows\PolicyDefinitions\en-us**" Folder.
  - If you get the prompt "**The destination has # files with the same names**", Click on "**Replace the files in the destination**".

How to Import GPOs with LGPO.exe (Pre-Hardened LGPOs)

For this Guide we will be using the Pre-Hardened LGPOs Created by Arun. This Guide assumes that you have Already Completed the "**Requirements**" Section for this Guide.

1. On the Standalone Machine, Open the "**Standalone GPO.zip**" File, and Extract/Copy the "**{5FB0CED9-04FD-4FD7-A421-94AF7943F509}**" and "**LGPO_30**" Folders to any Directory of your Choice.
2. Run the Command Prompt as Administrator
3. Type in "**cd [Directory Path for the Extracted LGPO_30 Folder]**", and then Press "**Enter**".
   a. Ex: "**cd "C:\Users\Administrator\Desktop\LGPO_30"**"
4. Type in "**lgpo.exe /g [Directory Path for the Extracted Pre-Hardened GPO Folder]**", and then Press "**Enter**".
   a. Ex: "**lgpo.exe /g "C:\Users\Administrator\Desktop\{5FB0CED9-04FD-4FD7-A421-94AF7943F509}"**"
      i. The "**/g**" option imports settings from one or more Group Policy backups.
         1. This option can be used to import Registry Policy (**registry.pol**), Security Templates (**GptTmpl.inf**), Advanced Auditing Backups (**audit.csv**), and **backup.xml** Files.
         2. This option imports only into System-Wide Settings and Does Not Support Configuring MLGPO.
   b. If Done Correctly, you Should See an Output that Looks like this: "**Registering Machine CSE: Unknown GP Extension... SECEDIT.EXE exited with exit code 1**"
      i. "**exit code 1**" Refers to the LGPO Import being Unable to Map the "**Auditors**" Group, from the GPO Import, to the Local "**Auditors**" Group that you have configured.
      ii. Instead of it Saying "**Auditors**", in the "**Advanced Security Settings**" for a Given Folder, for some instances, it will Appear something like: "**Account Unknown(S-1-5-21-2682050080-....)**"
      iii. **IMPORTANT:** The Sections "**Changing Folder Permissions**" and "**What's Left?**", will Address and Fix the "**exit code 1**" Error.
5. This concludes the Import Section for LGPOs, the Sections "**Changing Folder Permissions**" and "**What's Left?**", will Address and Fix the "**exit code 1**" Error.

Changing Folder Permissions

- **For Each Folder Below:** Right Click the Folder (if applicable), Click on **Properties -> Security -> Advanced ->** Double Click "**Account Unknown** " (Or "**S-1-5-21-2682050080-....**") **->** Click "**Select a principle**" **->** In the "**Enter the object name to select (examples):**" Field, Input the Name of your "**Auditors**" Group **->** Press the "**Enter**" Key **->** Click "**OK**" **->** Check the Box that Says, "**Replace all child object permission entries with inheritable permission entries from this object**" **->** Click "**Apply**" **->** for the "**Windows Security**" Prompt, Click "**Yes**" **->** Click "**OK**".
    - **C:\Admin**
    - **C:\Audits**
    - **C:\endpoint_keys**
    - **C:\Ivanti_Deployment_Files**
    - **C:\LES_Deployment_Files**
    - **C:\Scripts**
    - **C:\Security**
    - **C:\Splunk**
    - **C:\SPLUNK_DB**
    - **C:\SplunkDB**
    - **D:\Admin**
    - **D:\Audit**
    - **D:\Audits**
    - **D:\Scripts**
    - **D:\Security**
    - **D:\Splunk**
    - **D:\Splunk_DB**
    - **D:\SplunkDB**
    - **E:\Admin**
    - **E:\Audit**
    - **E:\Audits**
    - **E:\Scripts**
    - **E:\Security**
- For the Folder "**C:\Windows\System32\winevt\Logs**", You Must Manually Change the Permissions
    - Right Click the "**C:\Windows\System32\winevt\Logs**" Folder, Click on **Properties -> Security -> Advanced**
    - Once you are in the "**Advanced Security Settings for Logs**" Window, Click on the "**Add**" Button, "**Select a principle**", In the "**Enter the object name to select (examples):**" Field, Input the Name of your "**Auditors**" Group, and Press the "**Enter**" Key
    - Make Sure "**Type:**" is Set to "**Allow**", "**Applies to:**" is Set to "**This folder, subfolders and files**", and Under "**Basic permissions:**" Check the Box that Says "**Full control**", and Click "**OK**".
    - Under the "**Permission entries:**" Section Double Click ""**Administrators**", Make Sure "**Type:**" is Set to "**Allow**", "**Applies to:**" is Set to " **Subfolders and files only**", and Under "**Basic permissions:**" Un-Check all the Boxes, then Check the Box that Says "**Read & execute**" , and Click "**OK**".
    - Check the Box that Says, "**Replace all child object permission entries with inheritable permission entries from this object**", Click " **Apply**", for the Two "**Windows Security**" Prompts Click "**Yes**", and then Click "**OK**".
- Congratulations! You have Successfully Imported and Configured Pre-Hardened GPOs! Make Sure to Check the "**What's Left**" Section, to See if there are any Files that you, or the GPO Import, may have Missed.

What's Left?

This GPO Import will Add Auditing Permissions to the Following Folders if they are Already Created. Some may even Modify Access Permissions, see the Section Above "**Changing Folder Permissions**" to see which Folders Require Manual Modification. Additionally, you can Double-Check the Permissions for the Folders Listed Below, to See if there are any Files that you, or the GPO Import, may have Missed.

- **%AllUsersProfile%\Symantec**
- **%AllUsersProfile%\Symantec Antivirus**
- **%AllUsersProfile%\Symantec Shared**
- **%AllUsersProfile%\SymEFASI**
- **%ProgramFiles%\Common Files\Symantec Shared**
- **%ProgramFiles%\Ivanti**
- **%ProgramFiles%\Lumension**
- **%ProgramFiles%\Putty**
- **%ProgramFiles%\Splunk**
- **%ProgramFiles%\SplunkUniversalForwarder**
- **%ProgramFiles%\Symantec**
- **%ProgramFiles%\Symantec Antivirus**
- **%ProgramFiles%\Symantec Endpoint Protection**
- **%ProgramFiles%\Symantec Endpoint Protection Manager**
- **%ProgramFiles%\Tenable**
- **%ProgramFiles(x86)%\Common Files\Symantec Shared**
- **%ProgramFiles(x86)%\Ivanti**
- **%ProgramFiles(x86)%\Lumension**
- **%ProgramFiles(x86)%\Putty**
- **%ProgramFiles(x86)%\Splunk**
- **%ProgramFiles(x86)%\SplunkUniversalForwarder**
- **%ProgramFiles(x86)%\Symantec**
- **%ProgramFiles(x86)%\Symantec Antivirus**
- **%ProgramFiles(x86)%\Symantec Endpoint Protection**
- **%ProgramFiles(x86)%\Symantec Endpoint Protection Manager**
- **%ProgramFiles(x86)%\Tenable**
- **%SystemDrive%\Admin**

- **%SystemDrive%\Audits**
- **%SystemDrive%\endpoint_keys**
- **%SystemDrive%\Ivanti_Deployment_Files**
- **%SystemDrive%\LES_Deployment_Files**
- **%SystemDrive%\Scripts**
- **%SystemDrive%\Security**
- **%SystemDrive%\Splunk**
- **%SystemDrive%\SPLUNK_DB**
- **%SystemDrive%\SplunkDB**
- **%SystemRoot%\System32**
- **%SystemRoot%\SysWow64**
- **%Windir%\regedit.exe**
- **D:\Admin**
- **D:\Audit**
- **D:\Audits**
- **D:\Scripts**
- **D:\Security**
- **D:\Splunk**
- **D:\Splunk_DB**
- **D:\SplunkDB**
- **E:\Admin**
- **E:\Audit**
- **E:\Audits**
- **E:\Scripts**
- **E:\Security**