Importing DISA STIG Group Policy Objects to Active Directory

|  |  |
| --- | --- |
| The following instructions are to assist an administrator in importing the quarterly DISA STIG GPO Baseline GPOs into an Active Directory environment. The scope of this document is importing domain-based group policy objects (GPOs) into an Active Directory environment. Configuring WMI filters and linking GPO are outside the scope of this document.  The baseline package contains local policies that can be leveraged to apply STIG settings to standalone systems via LGPO. Use of local policies is outside scope of this document. | |
| 1. Download the quarterly baseline package from Cyber.Mil (<https://public.cyber.mil/stigs/gpo>). 2. Copy baseline package compressed file to privileged access workstation. |  |
| 1. Extract files to **C:\Temp.** 2. Browse to location of downloaded GPO package. 3. Right-click zip file and select **Extract All...**   **Note:** In this example the zip file **U\_STIG\_GPO\_Package\_October\_2020.zip** was copied to user’s **Downloads** directory. |  |
| 1. Enter **C:\Temp** in the **Files will be extracted to this folder.** 2. Select **Extract** button. |  |
| 1. Once extraction is complete, a **File Explorer window** will open displaying the extracted STIG Package directory. |  |
| 1. The quarterly DISA STIG GPO Baseline package provides multiple files under the Support Files to assist administrator in importing all or only the updated STIG Baseline GPOs.    1. **DISA\_GPO\_Baseline\_Import.ps1** is a PowerShell script that will request administrator to select import file and migration table to be used during execution. The script will import identified GPOs based on selected import file. If GPO is already present in environment administrator is prompted to overwrite or skip.    2. **DISA\_AllGPO\_Import\_*MMMYYYY*.csv** is used to import all DISA STIG Baseline GPOs into your Active Directory environment. This is intended for new environments or to overwrite existing GPOs.    3. **DISA\_QuarterlyGPO\_*MMMYYYY*\_Import.csv** is used to import only the modified GPOs in the quarterly baseline release.    4. **Importable.migration** is used during import of DISAOS baseline GPOs.    5. **Sample\_LGPO.bat** is a sample batch file that can be used to apply STIG setting via local policy on standalone systems.    6. **Local Policies** contains GPO backups to be used in conjunction with the LGPO. The backup GPOs are copies of the domain STIG baseline operating system GPOs without the required domain settings and remote desktop services setting restricting local account access.   **Note:** Example shows **October 2020 DISA STIG GPO Baseline** package. |  |
| 1. The import CSV files are predefined to locate GPO backup files under **C:\Temp\*DISA Quarterly Baseline Package*\*Product.***   **Note:** If **DISA STIG GPO Baseline package** was extracted to **C:\Temp** there is no need to modify import files. |  |
| 1. To modify import files, open either the **DISA\_AllGPO\_Import\_MMMYYYY.csv** or **DISA\_QuarterlyGPO\_Oct2020\_Import.csv** file. 2. Select **Edit | Replace…** 3. Enter **C:\Temp** in the **Find what** field. 4. Enter the full path to location of extracted DISA STIG Baseline package. 5. Select **Replace All** button. 6. Save file. |  |
| 1. Double-click **importtable.migration** file. 2. Locate line items **ADD YOUR DOMAIN ADMINS** and **ADD YOUR ENTERPRISE ADMINS** under **Source Name** column. 3. Click in the corresponding line item under the **Destination Name** column. 4. Enter Active Directory environment values for Domain Admins and Enterprise Admins groups.   **Note:** This example is for a single forest/domain model with the name of WHFBTEST. |  |
| The following instructions are based on DISA STIG Baseline package copied to local device under C:\TEMP.   1. Open PowerShell. 2. Type **cd \temp\October 2020 DISA STIG GPO Package 1009\Support Files** and press **Enter.**   **Note:** The path is based on October 2020 DISA release. The full path will change with each quarterly or out-of-cycle release. |  |
| 1. Type **.\DISA\_GPO\_Baseline\_Import.ps1** and press **Enter.** |  |
| 1. First action of script will check for logs. If not found, script will create a directory **GPO\_Automation\_Log** under the user’s Documents directory and create **STIG\_GPO\_Import.txt** log file. 2. User will receive message box to ensure required changes to import files were completed. Select **Yes.** If **No** or **Cancel** are selected the script will close with no changes to environment. |  |
| 1. User is prompted to select import file. Browse to **C:\TEMP\October 2020 DISA STIG GPO Package\Support Files** and select ***appropriate import file***. Select **Open.**   **Note:** Support files contains two import CSV files.  **DISA\_AllGPO\_Import\_MMMYYYY.csv** is used to import all DISA STIG Baseline GPOs into your Active Directory environment. This is intended for new environments or to overwrite existing GPOs.  **DISA\_QuarterlyGPO\_MMMYYYY\_Import.csv** is used to import only the modified GPOs in the quarterly baseline release.  In this example we are selecting quarterly updates only. |  |
| 1. User is prompted to select importtable.migration file. Browse to **C:\TEMP\October 2020 DISA STIG GPO Package\Support Files** and select **importtable** file. Select **Open.**   **Note:** Migration table is only required for operating system GPO imports, but user must provide migration table file for execution of script. |  |
| 1. PowerShell will loop through each entry in selected import file. If a GPO with same name located in the environment, user is prompted to with overwrite or skip import of GPO backup. Enter appropriate response **Y** or **N** and press **Enter.**   In this example, the GPO DoD Google Chrome STIG Computer v2r1 was found in environment and we chose to overwrite. The GPO DoD Outlook 2016 STIG User v2r1 was found and we chose not to overwrite.  If GPO is not found in environment, the GPO will be created and settings imported from backup. |  |
| 1. Review **STIG\_GPO\_Import.txt** log under user’s **Document\GPO\_Automation\_Log** directory. 2. GPO will be present in Active Directory environment. Administrators should follow locally established standard operating procedures to apply appropriate WIM filters to newly imported GPOs and link GPOs to appropriate AD objects. |  |