CIS Benchmarks

CIS Microsoft Windows Benchmark Build Kit ReadMe

ReadMe

v1.2.0

August 30, 2019

Table of Contents

Introduction

The purpose of this document is to describe the components of the CIS Microsoft Windows Build Kit and provide instruction on how to implement it within your environment. The Build Kit is designed to cover the majority of the benchmark settings, excluding only certain settings that cannot be managed though group policy. These templates are to be modified in alignment with your organization's defined policies.

Note: Prior to applying a Build Kit, verify that the most recent Microsoft Windows Administrative Templates have been downloaded directly from Microsoft and applied to the system.

WARNING: Reviewing the content within the corresponding Benchmark PDF is imperative for an overall successful application of the Build Kit, as there may be some settings that your organization needs to exempt itself from, due to unique operational requirements. Applying the Build Kit to a system without proper testing and review may result in a negative impact within your environment. It is acceptable if 100% of the benchmark is not applied, as it is the responsibility and decision of each organization to determine which settings are applicable to their unique needs. Please make note that you will need to make adjustments for use with Cloud and Standalone versions of Windows.

Build Kit Contents and Application

Inside each Build Kit you will find folders containing broken out GPO settings and custom templates for settings not covered by the standard Microsoft Windows Administrative Templates package.

DC = Domain Controller computer settings
MS = Member Server computer settings
BITLOCKER = BitLocker settings
Next Generation Windows Security = NGWS settings
COMP = Workstation computer settings
USER = User settings (all platform types)
SERVICES-L1= Contains all of the Services settings for Level 1 (only applies to Workstations)
SERVICES-L2= Contains all of the Services settings for Level 2 (only applies to Workstations)
L1 = Level 1 profile
L2 = Level 2 profile
<*Name*> Template – Custom GPO Template

Depending on which profile you decide to apply (L1 or L2) and which platform type (Workstation, Member Server or Domain Controller) here are the GPOs you will want to use:

CIS Group Policy Object (GPO) Name → Use case ↓	COMP-L1	COMP-L2	USER-L1	USER-L2	BITLOCKER	SERVICES-L1	SERVICES-L2	Next Generation Windows Security	DC-L1	DC-L2	MS-L1	MS-L2
Level 1 Workstation	X		X			X						
Level 2 Workstation	X	X	X	X		X	X					
Bitlocker					X							
Next Generation Window Security (DC,MS,WS)								X				
Level 1 Domain Controller			X						X			
Level 2 Domain Controller			X	X					X	X		
Level 1 Member Server			X								X	
Level 2 Member Server			X	X							X	X

Note: It may be helpful to think as "Level 1" as a foundation and the other profiles (Level 2) as "add-ons" to Level 1. For example, if you intend to harden a system to Level 2, then you need to apply ***both*** Level 1 and Level 2 GPOs in order to be L2 compliant. Bitlocker and Next Generation Windows Security are **ONLY** to be applied if you will be using them within an organization. Also, note that the User settings within a profile are identical across all platform types (Workstation, Member Server, Domain Controller) because they are really to be applied to user accounts, not to computer accounts – so the user values are the same, and only vary by profile (L1 or L2).

Application for Domain-joined Systems

The Benchmarks are designed to support domain-joined enterprise systems; as such you will be importing the GPOs contained in the Build Kit into your group policy of your domain controller.

To import these settings into Active Directory group policy environment, perform the following:

1) Unzip the GPO of your choice to a local folder on the computer you plan to import from.
2) Run `gpmc.msc` on the computer.
3) Go to the `Group Policy Object` and/or create a new `Group Policy Object`.
4) Right click on the selected Group Policy Object and click on "`import settings`".
5) Click `Next`.
6) Click `Next`.
7) Click `Browse` and select the folder that is holding the CIS GPO.
8) Click `Next`.
9) Click `Next`.
10) Click `Finish`, at this point the GPO should be imported.

Once imported, edit the GPOs accordingly before applying to any system. Once the GPOs are tailored to the organization's needs and properly tested, begin rollout to a small group of systems.

Application for Standalone Systems & Cloud Systems

Since our guidance is developed for enterprise domain-joined systems, certain settings will need to be tailored to your organizational need before applying to a standalone system.

Note: If your organization includes a multitude of standalone systems or cloud systems, a beneficial tactic for deployment would be to have a test domain controller VM. The GPOs can be imported into the test domain controller VM, modified appropriately, exported and then applied to the standalone system in accordance with any settings that have been configured to the organization's approved policy. The Administrator and Guest accounts have been renamed within the Build kits so make sure to verify you have tailored these settings as needed before applying to a standalone system or cloud system.

WARNING: The necessary modifications of particular settings will be dependent upon the function of the standalone/cloud system. Most modifications will be conducted in the User Rights section of the appropriate computer settings GPO and within the Remote Access based recommendations. Make sure that you have a backup administrator account created as the built in is disabled with the GPO out of the box. As standalone users are unique to each system, locking a system down by user may result in issues related to local file sharing. Additionally, Remote Desktop settings may be affected as locking down that system may result in insufficient inbound connectivity from another system.

Note: Before you begin, please test the below steps on test system(s). If the test system is a VM, take a snapshot before so you have something to revert back to. If hardware-based, take a full image backup that will be ready to be restored quickly.

1) Download and prep the CIS Build Kit for the particular O/S. i.e. Win2008, Win2008 R2, Win2012, Win2012 R2, Win2016, Win2019, Win7, Win8.1, Win10.
    a. Copy the Build Kit to the standalone system.
    b. Important: Unzip the files to a shorter and much smaller directory structure. An example of this is below. **Note:** The biggest issue people have with the Build Kits is that the files can get corrupted in the unzip process due to the long filenames.

EXAMPLES:

`C:\CIS\Win2008R2\CompSettingsL1\{`*Actual GUID*`}`
`C:\CIS\Win2008R2\UserSettingsL1\{`*Actual GUID*`}`

e.g.
`C:\CIS\Win2008R2\CompSettingsL1\{1CF79D2C-7EF9-4B79-81DF-39E865439DB6}`
`C:\CIS\Win2008R2\UserSettingsL1\{44A16D69-5D67-453F-98FE-9880ADD6E7E3}`

2) Download LGPO and install LGPO
    a. Install `LGPO.zip` from this link: https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/
    b. Unzip it to a directory such as `C:\Utils\LGPO`.

3) Run LGPO
   a. Open a Command Prompt as an Administrator.
   b. Change to the directory where LGPO.exe is unzipped and run the following:
      i. This will install the **Computer** settings:

         `C:\Utils\LGPO\lgpo.exe /g C:\CIS\Win2008R2\ComputerSettingsL1\{Actual GUID}`

         Note: Make sure to use a lowercase **`/g`** in the above command

      ii. This will install the **User** settings:

         `C:\Utils\LGPO\lgpo.exe /g C:\CIS\Win2008R2\UserSettingsL1\{Actual GUID}`

4) BEFORE YOU REBOOT – do the following:

   a. Edit two key local policies:
      i. Run `gpedit.msc` and edit the following two settings, **removing** the items in yellow from each:

         1. ***Configure 'Deny access to this computer from the network' (Scored)***

            a. **Level 1 - Member Server.** The recommended state for this setting is to include: `Guests, Local account and member of Administrators group.`

               Location: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network

         2. ***Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Scored)***

            a. The recommended state for this setting is to include: `Guests, Local account.`

               Location: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally

5) Reboot

6) Login with a local Administrator account

7) Check that the CIS policies have been applied by doing the following:

   a. Run `GPRESULT /H:GPOReport.html` at an Administrative Command Prompt.
   b. Copy the `GPOReport.html` file to `C:\`
   c. Type `GPOReport.html` at the `C:\` Command Prompt, and press [Enter] to view the file.
   d. Analyze the results.

Support

CIS offers free support with our memberships. In the event that you have an issue with our Build Kits or any of the other products, we offer you a few options.

If you notice any typos, bugs or incorrect settings within a Build Kit, Benchmark or assessment content, please create a ticket in the appropriate Benchmark community here: http://workbench.cisecurity.org

If you have any questions about why a given recommendation is contained within a Benchmark or why we decided on checking for a specific setting please feel free to post this question directly within the discussions of the community (http://workbench.cisecurty.org) so that one of the subject matter experts can answer the question.

If you need support getting the benchmarks/assessment/remediation working in your environment you can email support@cisecurity.org. A support representative will reach out quickly to help you resolve your issue. Please make sure to provide as much information as possible to help expedite your support.