CIS Microsoft Windows Server Stand-alone Benchmark Build Kit ReadMe

V3.0.0 – 06/10/2025

Table of Contents

Introduction

The purpose of this document is to describe the components of the CIS Microsoft Windows Build Kit and provide instructions on how to implement it. Build Kits are designed to cover most of the benchmark recommended settings. **These templates can be modified in alignment with organizational defined policies.**

Note: Prior to applying a Build Kit, ensure that the most recent Microsoft Windows 11 Administrative Templates (applicable to both workstation and server OS versions) have been downloaded directly from Microsoft and installed on the system.

WARNING: Reviewing the content within the corresponding Benchmark PDF or Word document is imperative for an overall successful application of the Build Kit. Some settings may need an exception due to unique operational requirements.

Applying the Build Kit to a system without proper testing and review may result in a negative impact within the 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.

This CIS Benchmark is written for stand-alone systems **only**. Adjustments/tailoring to the benchmark recommendations can be done a number of ways including Local Group Policy Editor, Group Policy Management Console on Windows Server (GPMC), and Microsoft's Local Group Policy Object tool (LGPO).

Build Kit Contents and Application

Inside each Build Kit are folders containing Group Policy Objects (GPOs) and custom templates for settings not covered by the standard Microsoft Windows Administrative Templates package.

Custom ADMX/ADML Template

This custom template (`Configure-IPv6-Components-KB929852.ADMX` and `Configure-IPv6-Components-KB929852.ADML`) must be added to the Central Store, or the Policy Definitions folder. It will then appear in Group Policy Management Editor under

```
Computer Configuration\Policies\Administrative Templates\Center for Internet Security (CIS)\Additional Benchmark Settings
```

Prior to applying a Build Kit, ensure that the most recent version of the Microsoft Windows 11 Administrative Templates (applicable to both workstation and server OS versions) has been downloaded directly from Microsoft and installed on the system.

*Thank you to Aaron Margosis for building the template for CIS.

Profiles and Compliance

Comp = Computer settings
User = User Settings (all platform types)
Next Generation = Next Generation Windows Security (NGWS) settings
Services = Computer Service Settings
MS = Member Server
L1 = Level 1 profile
L2 = Level 2 profile

Depending on which profile is being applied (L1, L2, NGWS etc.), the following GPOs are needed to comply with the benchmark:

CIS Group Policy Object (GPO) Name → **Use case ↓**	**L1**	**L2**	**User-L1**	**User-L2**	**L1 - Servies**	**NGWS**
Level 1 Member Server (MS)	X		X			
Level 2 Member Server (MS)	X	X	X	X	X	
Next Generation Window Security Member Server (MS)						X

Note: Think of Level 1 as foundational 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 to be L2 compliant. The Next Generation Windows Security GPOs are hardware dependent and should **ONLY** be applied if the proper hardware is present.

Application for Stand-alone & Cloud Systems

Certain settings will need to be tailored to your organizational need before applying to a standalone system.

It is imperative appropriate tailoring is done before applying build kits to systems, they should not be applied out of the box. The stand-alone benchmark build kit can be managed and applied using a variety of methods, however 3 example methods are shown here. This document will only cover them at a high level with the LGPO usage being covered in more detail below. It is up to the organization's systems administrator to decide how to automate and deploy with the tools they may uniquely have access to.

1. Import Group Policies into a test/sandbox Domain Controller, tailor as needed, then export using the backup function.
    a. Apply to production stand-alone systems using LGPO manually or through automation (more detail below on LGPO)
2. Apply chosen profiles to a Windows 10 reference machine using LGPO, tailor as needed using local group policy editor, then image and deploy as desired with your software of choice.
3. Apply chosen profiles to a Windows 10 reference machine using LGPO, tailor as needed using local group policy editor, then use LGPO to backup settings to later be deployed to production systems via LGPO.

The default 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 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 to. If hardware-based, take a full image backup that will be ready to be restored quickly.

LGPO usage and examples

1. Download and prep the CIS Build Kit for the O/S. i.e. Windows 10, Windows 11.
    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.

Example:

- C:\CIS\Win10\Computer L1\{Actual GUID}
    - e.g. C:\CIS\Win10\Computer L1\{1CF79D2C-7EF9-4B79-81DF-39E865439DB6}
- C:\CIS\Win10\User L1\{Actual GUID}
    - e.g. C:\CIS\Win10\User L1\{44A16D69-5D67-453F-98FE-9880ADD6E7E3}

2. Download LGPO and install LGPO
    a. Install LGPO.zip from this link: https://www.microsoft.com/en-us/download/details.aspx?id=55319
    b. Unzip it to a directory such as C:\CIS\LGPO\.
    c. Read the included manual LGPO.pdf this includes details on the full functionality, syntax and use cases of the tool.
3. Running LGPO as an example
    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 L1 Profile settings:
        LGPO.exe /g “C:\CIS\Win10\Computer L1\{GUID}” /v > LGPO-CL1.out 2> LGPO-CL1.err

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

        ii. This will install the User settings:

        LGPO.exe /g “C:\CIS\Win10\User L1\{GUID}” /v > LGPO-UL1.out 2> LGPO-UL1.err

        iii. Lastly open the output and error files (e.g. LGPO-CL1.out and LGPO-CL1.err) in a notepad and ensure there aren’t any errors and the setting applied properly.

4. Reboot
5. Login with a local Administrator account
6. 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 somewhere like C:\CIS\
    c. Change to the above directory and type GPOReport.html and press [Enter] to view the file.
    d. Analyze the results.

Support

CIS offers free support to our SecureSuite members. If you have an issue with Build Kits or any of the other products, please use the links below for assistance.

For typos, bugs or incorrect settings within a Build Kit, Benchmark, or assessment content, please create a ticket in the Microsoft Windows Benchmark Community.

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 Discussion area of the Microsoft Windows Community. One of the community subject matter experts will respond.

For support with the Benchmark's Assessment or Remediation content working within the environment, contact our Support Center. A support representative will reach out quickly to help resolve the issue. Please make sure to provide as much information as possible to help expedite support.