Federal Office
for Information Security

Guide to Using Group Policy Objects for Windows 10 Hardening and Logging Configuration

Version: 1.0

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Figures

Tables

1 Introduction

This document outlines the result of work package 12 of the project “SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10” (orig., ger.). This project is being conducted by the company ERNW Enno Rey Netzwerke GmbH on behalf of the German Federal Office for Information Security (orig., ger.: “Bundesamt für Sicherheit in der Informationstechnik” (BSI)).

The goal of this document is to describe the use of the Group Policy objects provided, which were created based on the hardening and logging recommendations for the configuration of Windows 10 components. The description and explanation of the recommended configurations are detailed in the associated result documents of work packages 10 (logging recommendations) and 11 (hardening recommendations).

2 General Concepts

The provided Group Policy objects are divided into the hardening recommendations of work package 11 (see (ERNW_WP11)) and the logging recommendations of work package 10 (see (ERNW_WP10)). In addition, three different use cases for the deployment of Windows 10 were defined in the hardening recommendations:

- Normal protection needs standalone computer
- Normal protection needs domain member
- Increased protection needs domain member

Each specified configuration recommendation was assigned to at least one use case, with the exception of the logging recommendations from work package 10 which apply to all scenarios. Based on the assignment of the recommendation to the use cases, dedicated Group Policy objects were created. This allows for a fine-grained implementation of the hardening recommendations.

Not all settings specified in the hardening and logging recommendations are also configured in the provided Group Policy objects. Some settings require individual consideration or configuration and cannot be universally preconfigured. The following table lists the settings that are not configured in the Group Policy objects:

Hardening Recommendation	Policy Name	Rationale
209	Interactive logon: Message title for users attempting to log on	Setting is company- and language-specific.
231	Interactive logon: Message text for users attempting to log on	Setting is company- and language-specific.
235	Accounts: Rename administrator account	Individual choice of name required.
238	Accounts: Rename guest account	Individual choice of name required.
277-315	User Rights Assignment	Individual role concept required.
323, 326, 328, 331, 341, 342, 348, 356	Disabling system services	Depending on installed roles.

Table 1 Hardening recommendations missing from Group Policy objects

In addition, a larger part of the recommendations from chapter 5 of the hardening recommendations and section 5.6.1.2 of the logging recommendations are not included, since adjustments to the concrete use cases are here likewise necessary and the settings (e.g., due to hardware dependencies, such as in the case of "Virtualization Based Security") must be tested in detail in advance or the concrete configurations cannot be applied via Group Policies (such as the firmware configuration).

Specifically, this means that the recommendations in the following chapters should be implemented manually or only after an evaluation (H - hardening recommendation, P - logging recommendation):

Document	Section Number	Section Header
H	5.1	Windows Defender Application Control Management
H	5.2	Virtualization-Based Security
H	5.3.3	Requirements for the Secure Use of the TPM
H	5.4.1.2	Disabling Autologger-Diagtrack-Listener
H	5.5.1.1	Disabling PowerShell Version 2.0
H	5.5.1.3	Restricting the PowerShell Scripting Language (Local Computer)
H	5.5.1.4	Secure Use of PowerShell Remoting
H	5.5.2	Windows Script Host
H	5.6	Firmware
P	5.6.1.2	Ensure a SACL is Configured for Relevant Registry Objects. *Note: Affects only user-specific registry keys.*

Table 2 Additional setting recommendations to be configured

2.1 Group Policy Objects

The configuration recommendations were divided according to the respective use cases (the abbreviations of the use cases are derived from their German names, see (ERNW_WP11)), section 2.3) on the one hand and the respective setting scope (settings for computers or users) on the other hand. This results in a total of 5 different Group Policy objects that can be used to apply the hardening recommendations. The following tables represent an assignment of the Group Policy objects to the respective use cases:

No.	Name
1	Normal Protection Needs Standalone Computer (NE) - Computer
2	Normal Protection Needs Domain Member (ND) - Computer
3	Increased Protection Needs Domain Member (HD) - Computer

Table 3 Group Policy objects for the computer configuration

The following table lists the provided Group Policy objects for the user configuration:

No.	Name
4	Normal Protection Needs (ND, NE) - User
5	Increased Protection Needs (HD) - User

Table 4 Group Policy objects for the user configuration

For the logging recommendations in work package 10, only one Group Policy object exists, since no distinction needs to be made between different use cases and setting scopes:

Nr.	Name
6	Logging (ND, NE, HD) - Computer

Table 5 Group Policy object for the logging configuration

3 Importing the Group Policy Objects

The following sections describe the procedures to apply the provided Group Policy objects on standalone computers or in the Active Directory in an exemplary way.

3.1 Standalone Computer

Group Policy objects can be exported and imported locally with the tool *Local Group Policy Object Utility* (LGPO) (see (ms_lgpo, 2021)). For this use case, the Group Policy objects *Normal Protection Needs Standalone Computer (NE)* (Group Policy object no. 1), *Normal Protection Needs (NE, ND)* (Group Policy object no. 4) and *Logging (NE, ND, HD)* (Group Policy object no. 6) are relevant. The following are the steps to import the provided Group Policy objects locally:

1. Download the tool *LGPO.exe* from Microsoft.
2. Unzip the folder that contains the file *LGPO.exe* from the downloaded archive.
3. Start an administrative command line:
    a. Start the program *Command Prompt* (cmd.exe) or the program *PowerShell* (powershell.exe).
4. Execute the program *LGPO.exe* with the parameter */g* and the path to the respective Group Policy object, for example:
    a. `C:\>LGPO.exe /g “C:\<Path>\Normal Protection Needs Standalone Computer (NE) – Computer”`
    b. `C:\>LGPO.exe /g “C:\<Path>\Normal Protection Needs (ND, NE) – User”`
    c. `C:\>LGPO.exe /g “C:\<Path>\Logging (ND, NE, HD) – Computer”`
5. Perform a restart to apply the configurations:
    a. `C:\>shutdown.exe /r /t 0`

3.2 Active Directory

In Active Directory environments, Group Policy objects are configured, managed, and assigned to the respective organizational units via the *Group Policy Management* Console (gpmc.msc). The following describes the steps to import the provided Group Policy objects into the Group Policy Management Console:

1. Open the *Group Policy Management Console* in the respective Active Directory domain:
    a. To do this, start the *Group Policy Management Console* (gpmc.msc) program on a Domain Controller or member system.
2. Create a new Group Policy object and name it accordingly:

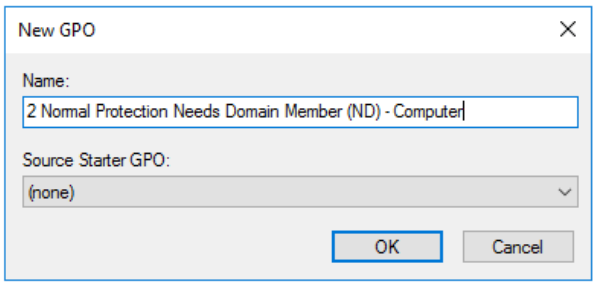

Figure 1 Creating a Group Policy object

3. Right-click the newly created Group Policy object and select the *Import settings...* option:

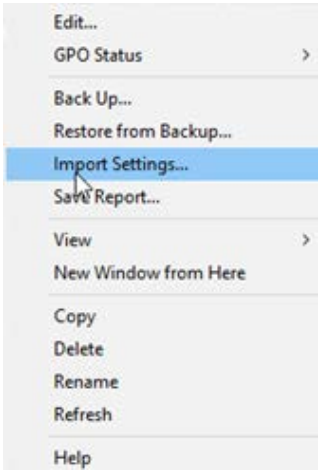

Figure 2 Importing settings

4. Click next until the selection of the backup folder (the folder containing the provided Group Policy object):

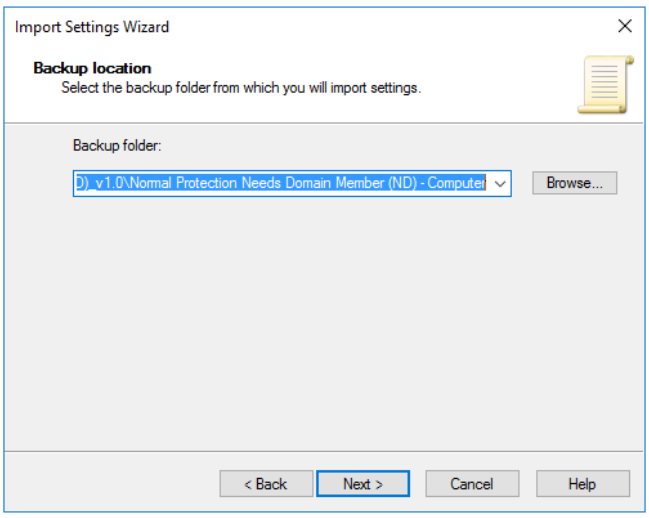

Figure 3 Selecting the backup folder

5. Then select the respective Group Policy object:

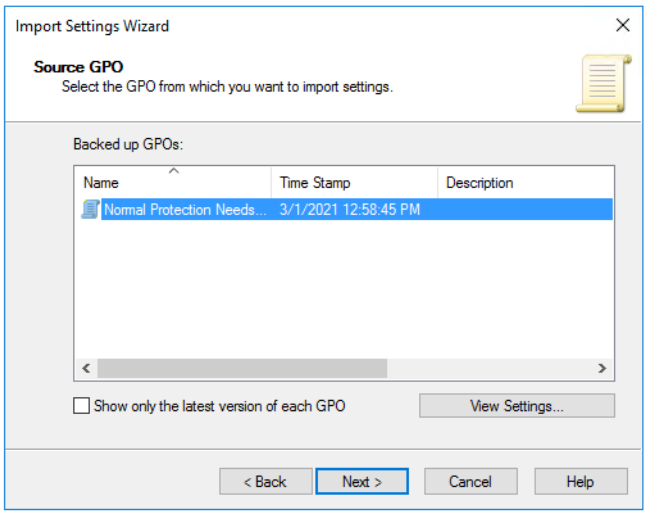

Figure 4 Selecting the Group Policy object to be imported

6. Afterwards, the Group Policy object must still be linked to the corresponding organizational unit.

3.2.1 Linking Group Policy Objects

To effectively apply the Group Policy objects, they still need to be linked to the corresponding objects in Active Directory. For this purpose, individual organizational units are typically created (however, a link to the domain object or so-called *sites* is also possible). These ideally contain either only user or computer objects. For the use case *Normal Protection Needs Domain Member*, this results in at least two organizational units (each containing only users or computers) with a link to the corresponding Group Policy object.

The Group Policy objects for increased protection needs contain dedicated settings for increased protection only. This means that the Group Policy objects of the normal protection needs must also be applied to the organizational units of increased protection needs. Computer and user objects with increased protection needs must be sorted into separate organizational units. The following screenshot shows exemplarily how the Group Policy objects are linked to the two use cases in Active Directory environments:

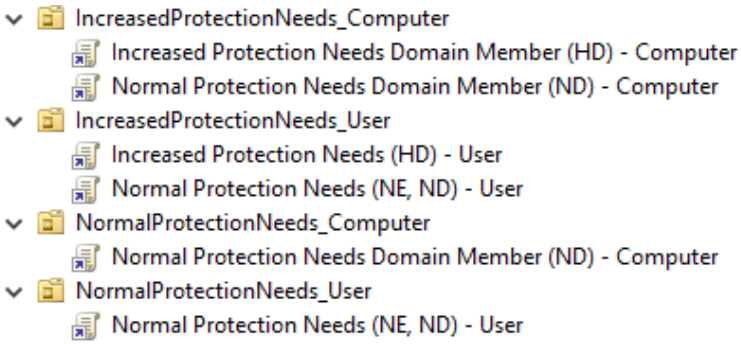

Figure 5 Linking of Group Policy objects

The Group Policy object for logging only affects the computer configuration. Since no distinction is made in terms of protection needs, the imported object can be associated with the computer organizational unit for normal and increased protection needs.

Appendix

Tools Used

Tool	Availability and Description
Local Group Policy Object Utility	*Availability*: Download under https://www.microsoft.com/en-us/download/details.aspx?id=55319 *Description*: Local management of Group Policy objects
Group Policy Management Console	*Availability*: Windows feature that can be activated *Description*: Managing Group Policy Objects in Active Directory Environments

Reference Documentation

ERNW_WP10. (n.d.). SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10): Work Package 10.

ERNW_WP11. (n.d.). SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10): Work Package 11.

ms_lgpo. (2021, March 11). Retrieved from https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319

Abbreviations

TPM: Trusted Platform Module 7