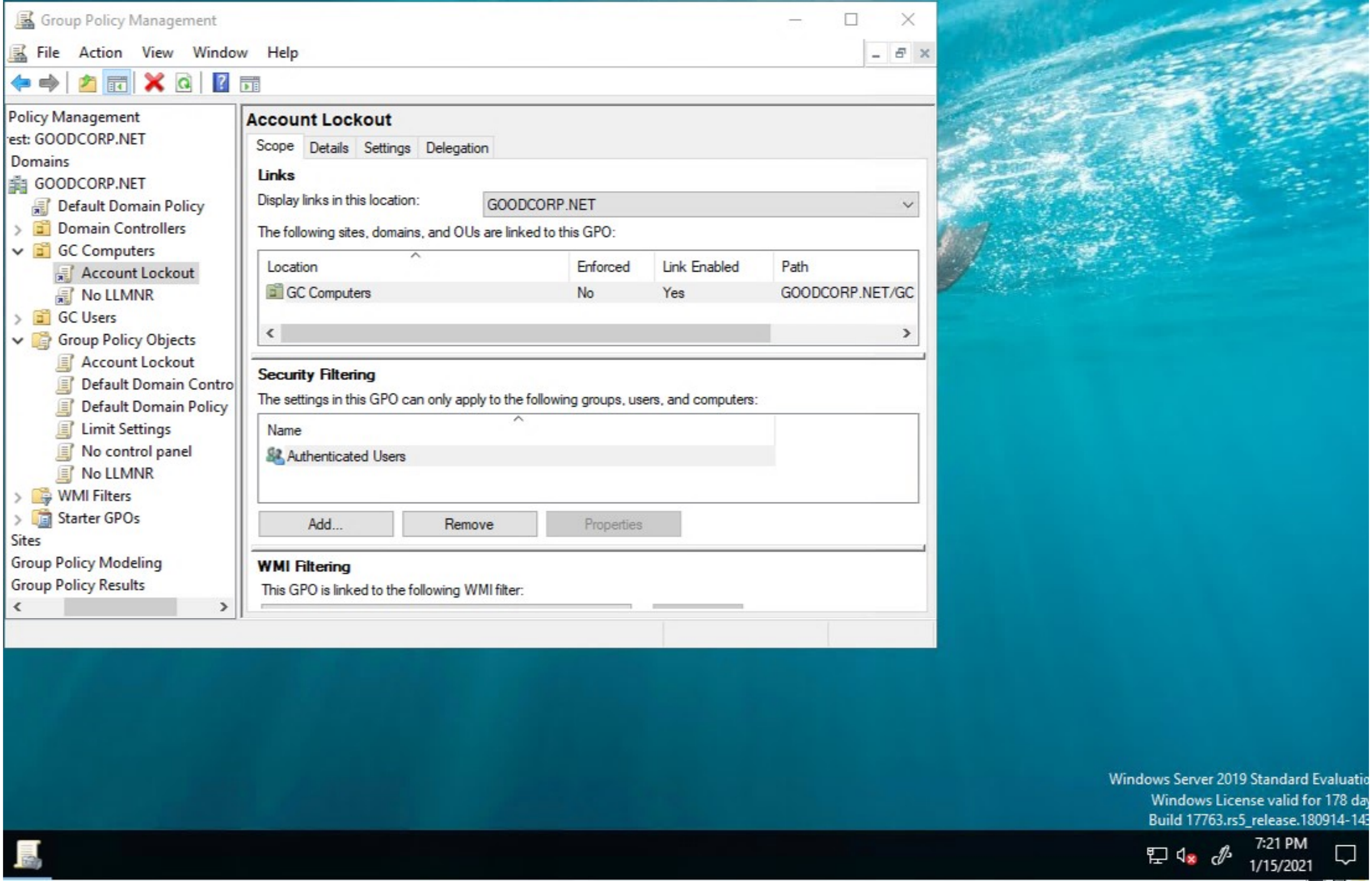
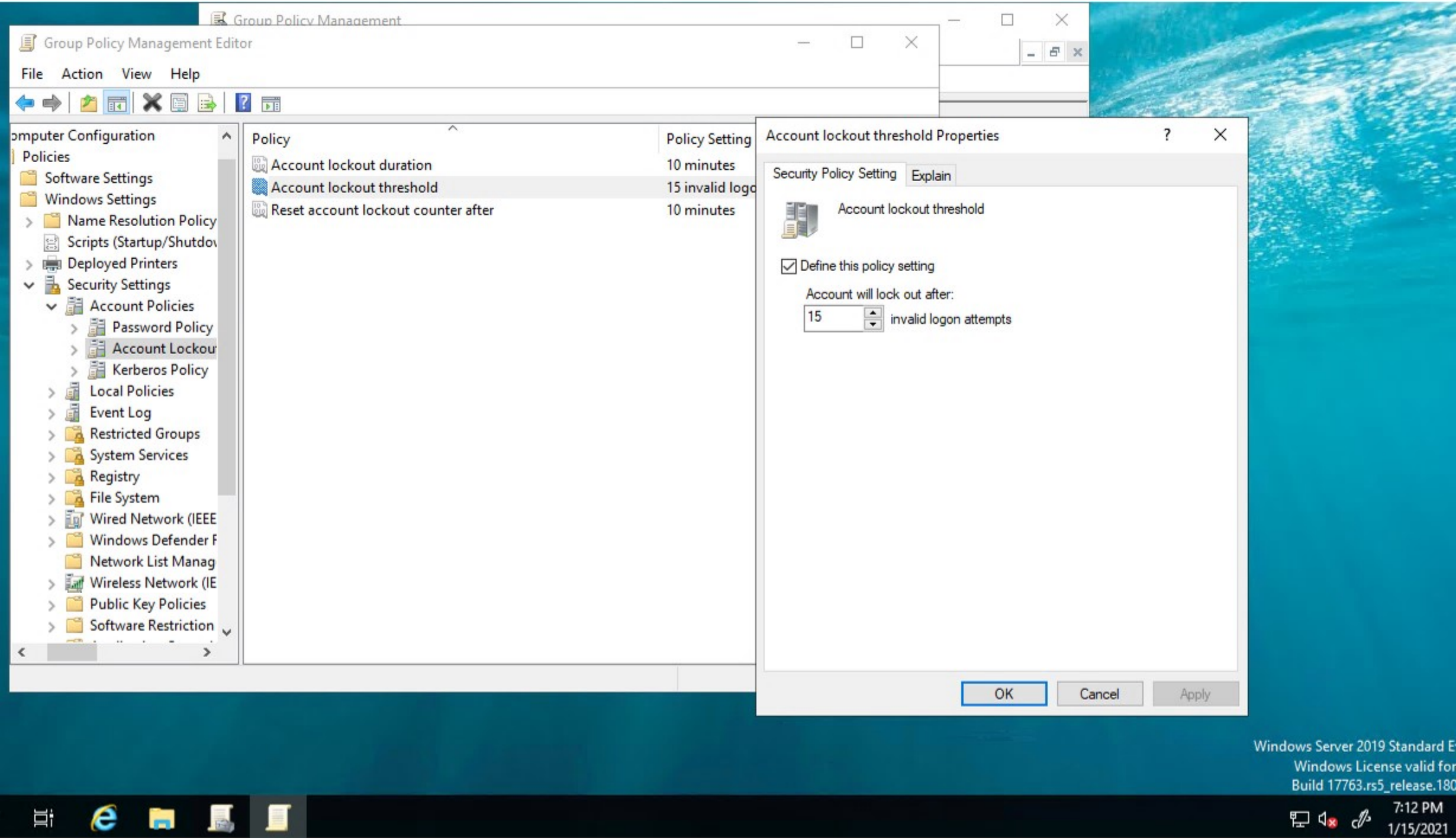
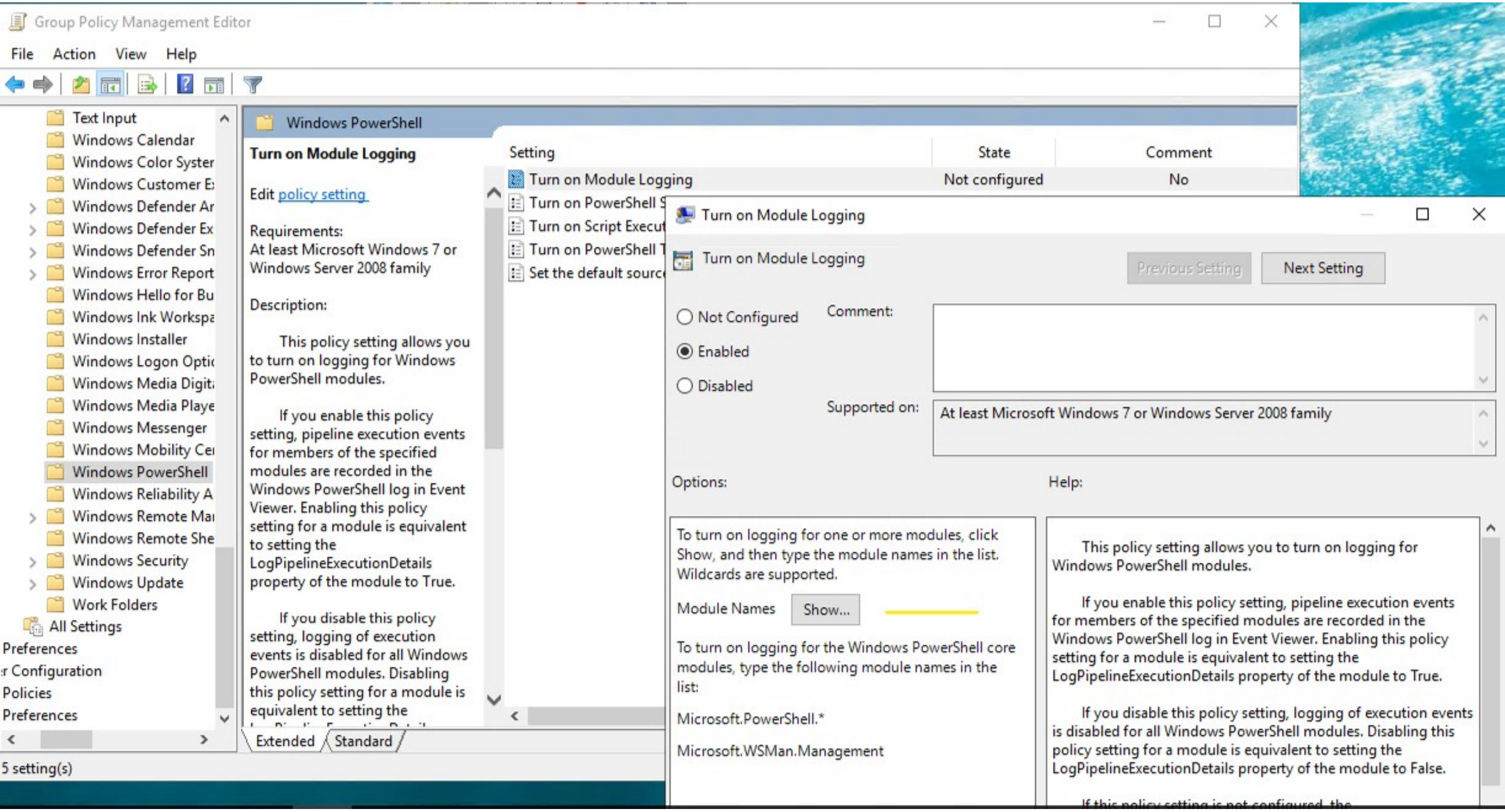
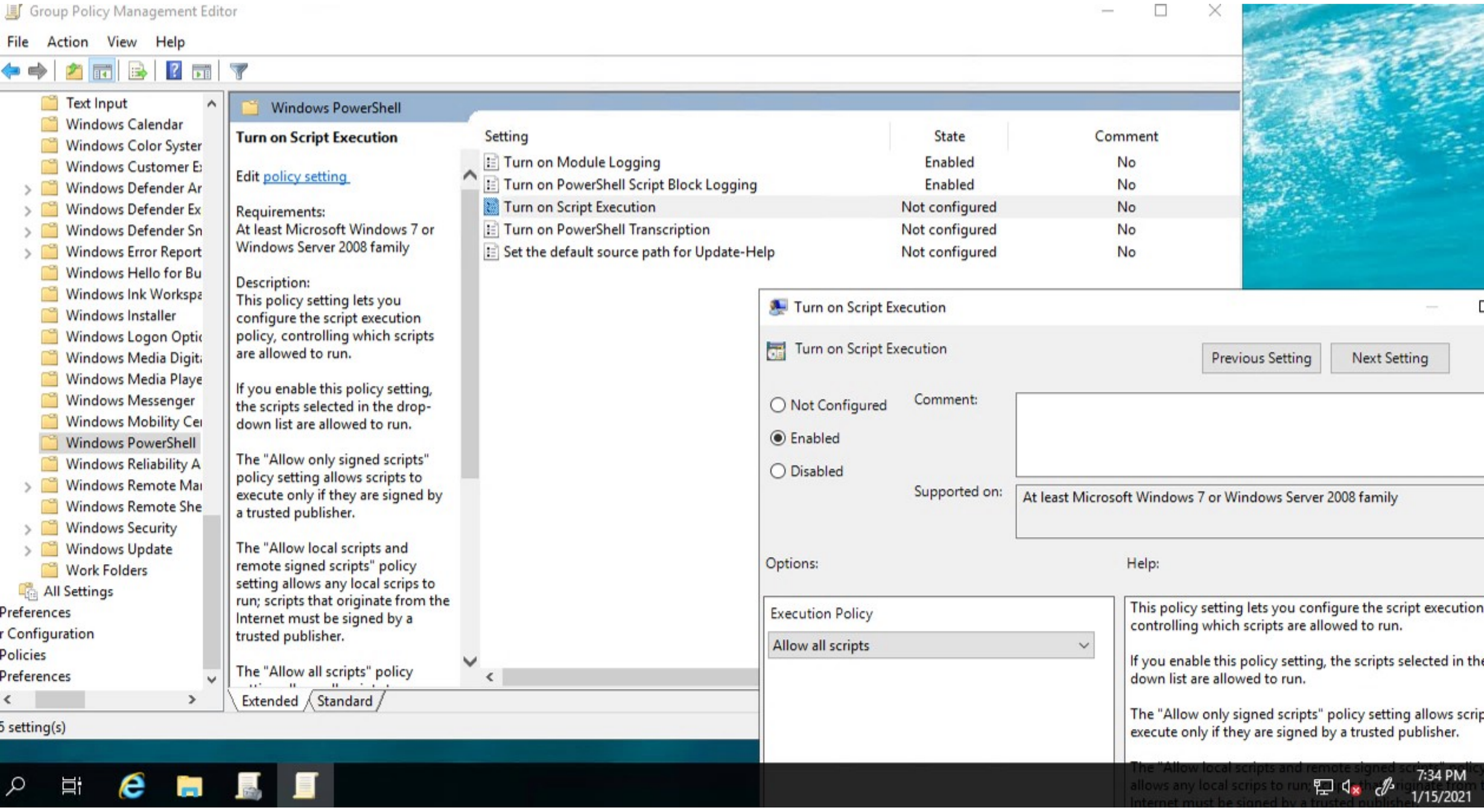
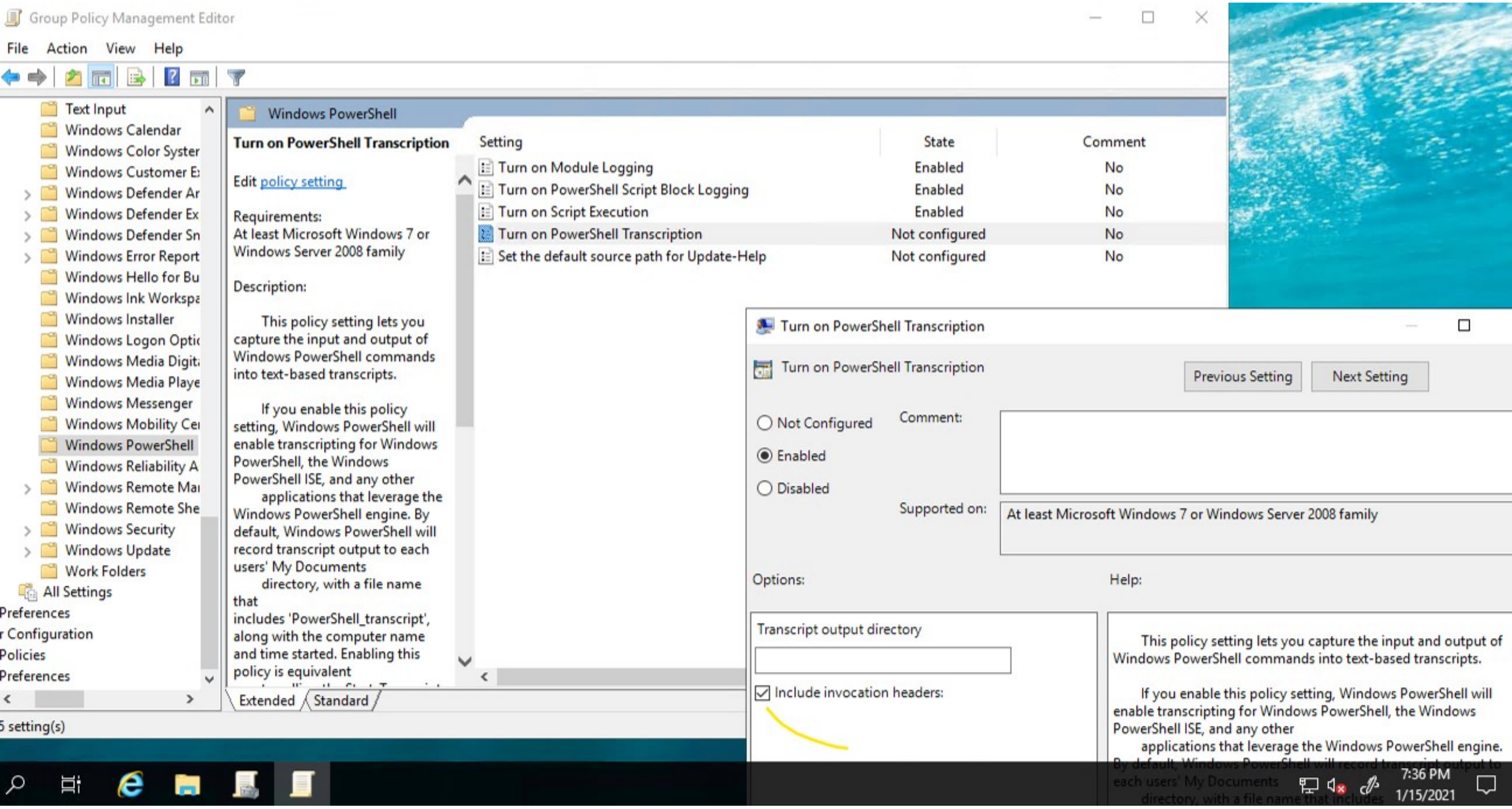
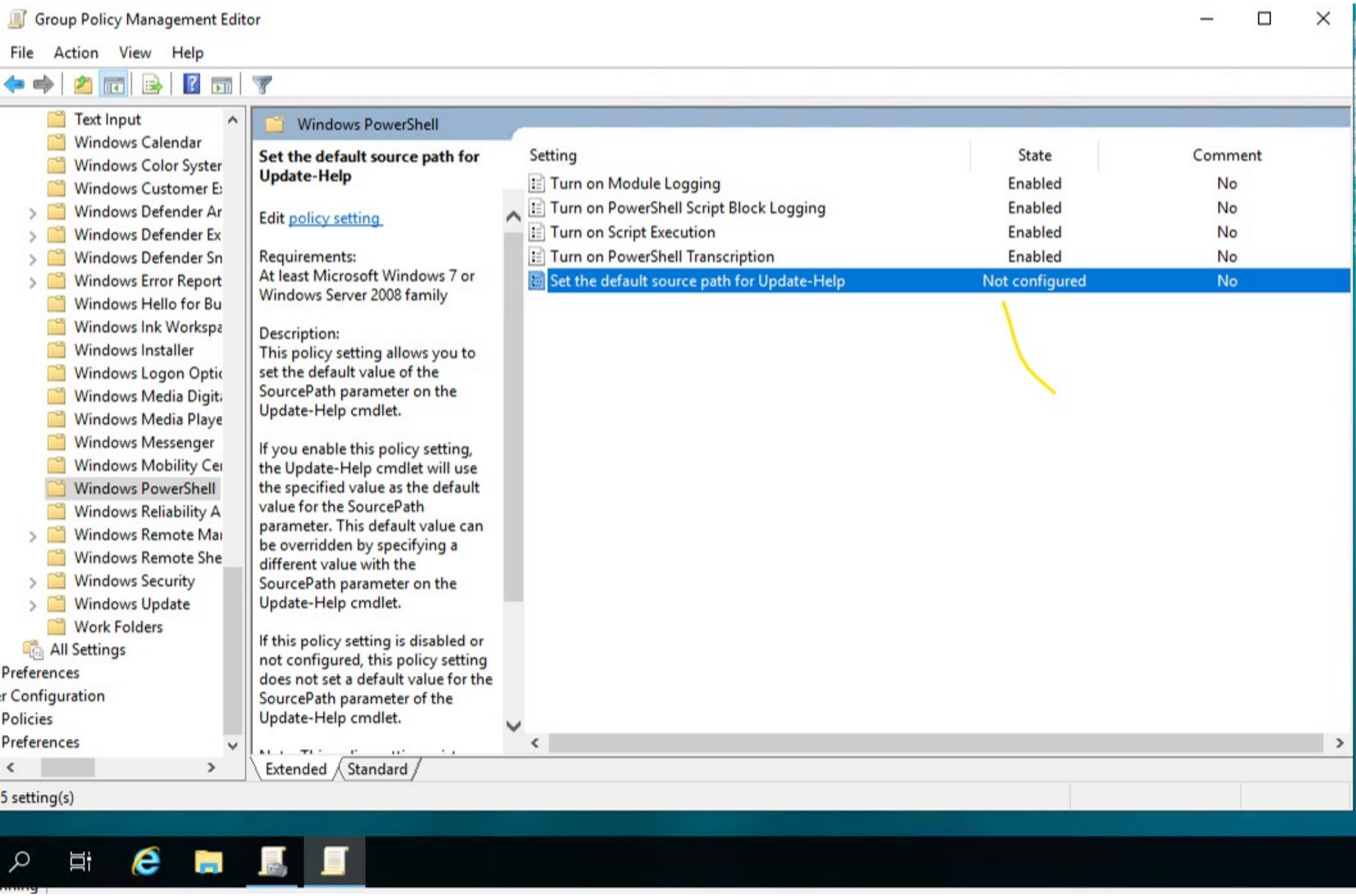

Group Policy Management
File Action View Window Help
Policy Management
est: GOODCORP.NET
Domains
GOODCORP.NET
Default Domain Policy
Domain Controllers
GC Computers
Account Lockout
No LLMNR
GC Users
Group Policy Objects
Account Lockout
Default Domain Contro
Default Domain Policy
Limit Settings
No control panel
No LLMNR
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Account Lockout
Scope Details Settings Delegation
Links
Display links in this location: GOODCORP.NET
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
GC Computers No Yes GOODCORP.NET/GC
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
Windows Server 2019 Standard Evaluatio
Windows License valid for 178 da
Build 17763.rs5_release.180914-14
7:21 PM
1/15/2021

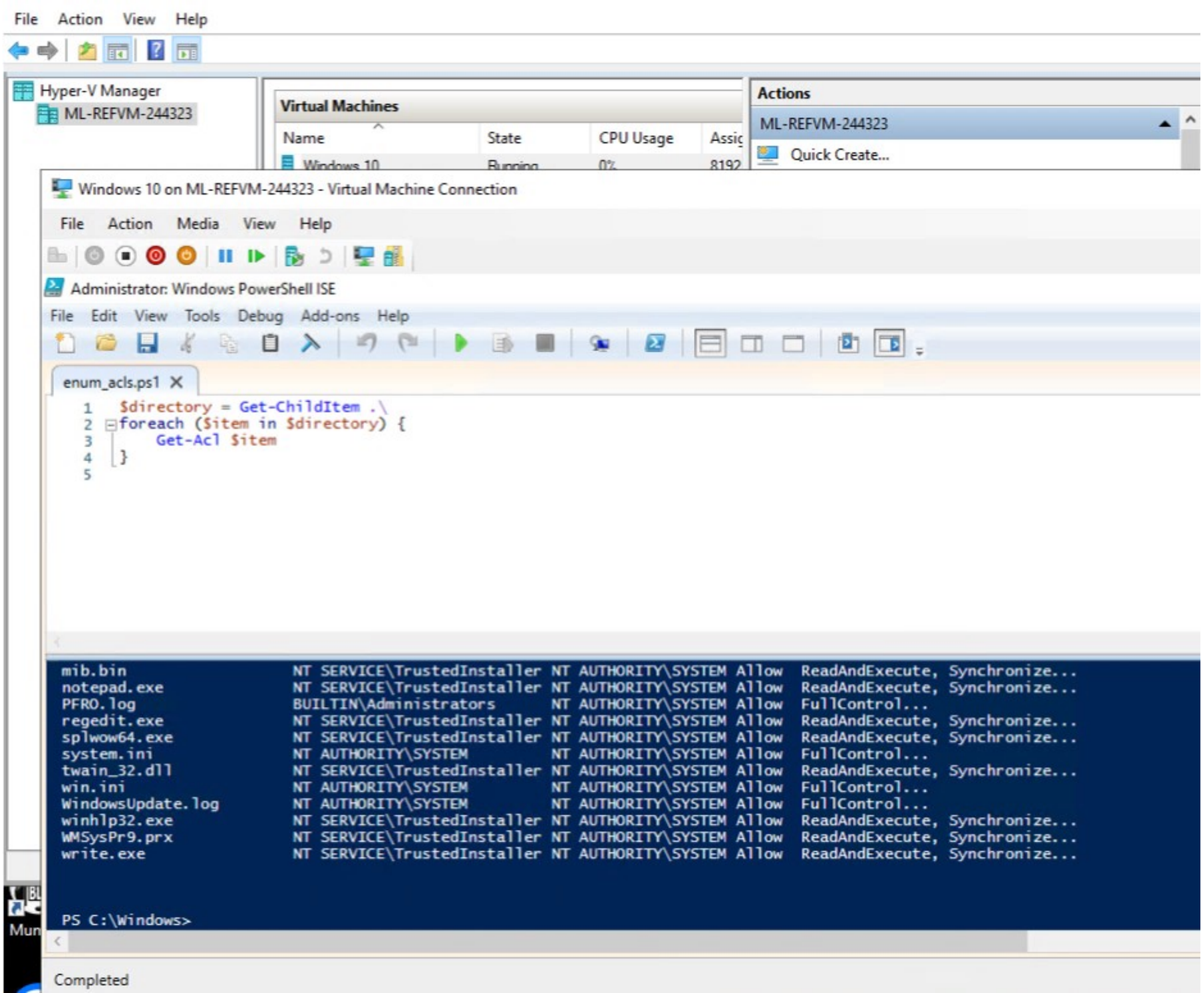

Group Policy Management
Group Policy Management Editor
File Action View Help
omputer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdo
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockou
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Defender F
Network List Manag
Wireless Network (IE
Public Key Policies
Software Restriction
Policy
Policy Setting
Account lockout duration
10 minutes
Account lockout threshold
15 invalid logo
Reset account lockout counter after
10 minutes
Account lockout threshold Properties
Security Policy Setting
Explain
Account lockout threshold
Define this policy setting
Account will lock out after:
15
invalid logon attempts
OK
Cancel
Apply
Windows Server 2019 Standard E
Windows License valid for
Build 17763.rs5_release.180
7:12 PM
1/15/2021

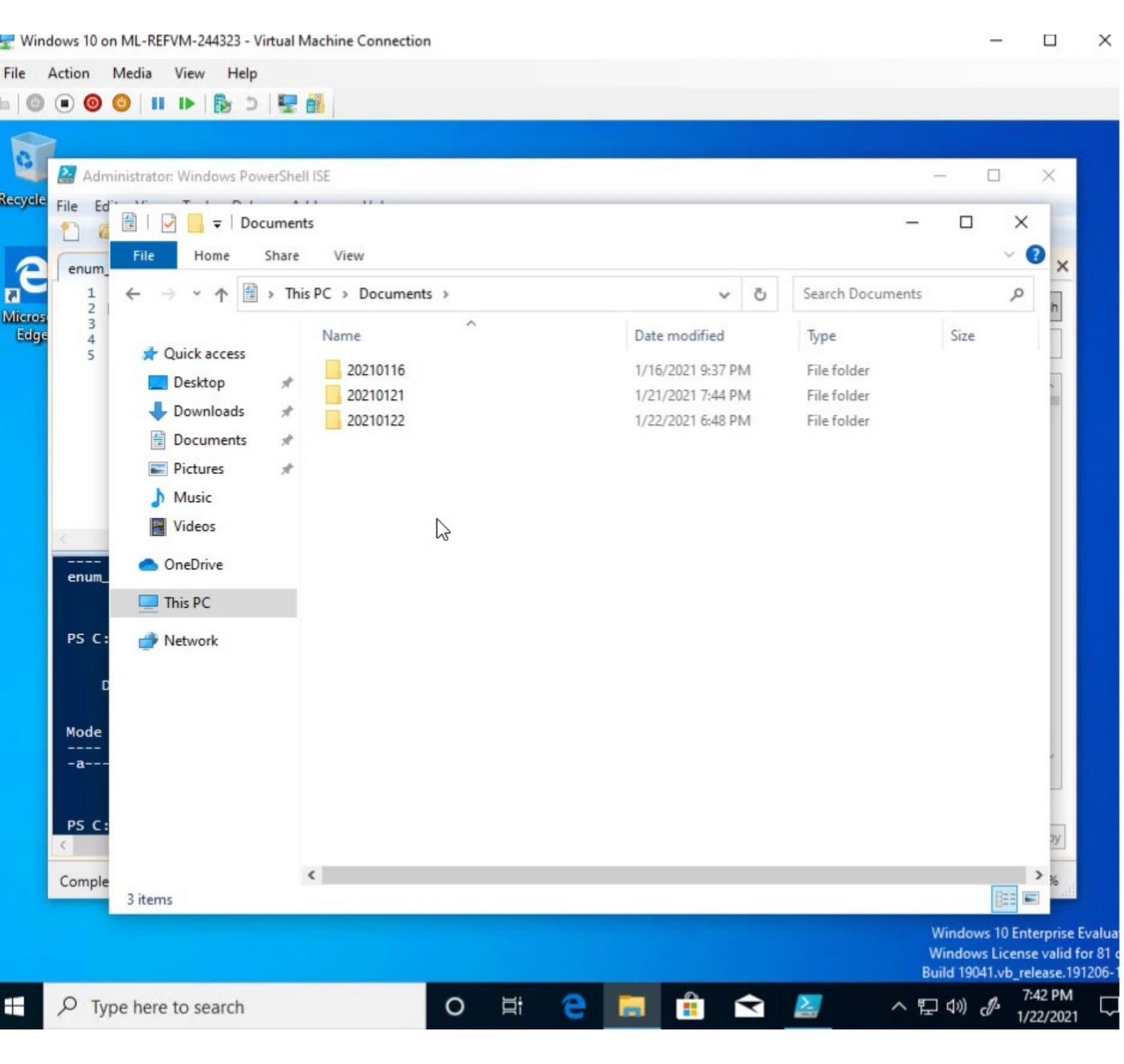

Group Policy Management Editor
File Action View Help
Text Input
Windows Calendar
Windows Color Syster
Windows Customer Ex
Windows Defender Ar
Windows Defender Ex
Windows Defender Sn
Windows Error Report
Windows Hello for Bu
Windows Ink Workspa
Windows Installer
Windows Logon Optic
Windows Media Digit
Windows Media Playe
Windows Messenger
Windows Mobility Cer
Windows PowerShell
Windows Reliability A
Windows Remote Mar
Windows Remote She
Windows Security
Windows Update
Work Folders
All Settings
Preferences
r Configuration
Policies
Preferences
Windows PowerShell
Turn on Module Logging
Edit policy setting
Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family
Description:
This policy setting allows you to turn on logging for Windows PowerShell modules.
If you enable this policy setting, pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer. Enabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to True.
If you disable this policy setting, logging of execution events is disabled for all Windows PowerShell modules. Disabling this policy setting for a module is equivalent to setting the
Setting
State
Comment
Turn on Module Logging
Not configured
No
Turn on PowerShell S
Turn on Script Execut
Turn on PowerShell T
Set the default source
Extended
Standard
5 setting(s)
Turn on Module Logging
Turn on Module Logging
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
To turn on logging for one or more modules, click Show, and then type the module names in the list. Wildcards are supported.
Module Names
Show...
To turn on logging for the Windows PowerShell core modules, type the following module names in the list:
Microsoft.PowerShell.*
Microsoft.WSMan.Management
This policy setting allows you to turn on logging for Windows PowerShell modules.
If you enable this policy setting, pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer. Enabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to True.
If you disable this policy setting, logging of execution events is disabled for all Windows PowerShell modules. Disabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to False.


Group Policy Management Editor
File Action View Help
Text Input
Windows Calendar
Windows Color Syster
Windows Customer E
Windows Defender Ar
Windows Defender Ex
Windows Defender Sn
Windows Error Report
Windows Hello for Bu
Windows Ink Workspa
Windows Installer
Windows Logon Optic
Windows Media Digit
Windows Media Playe
Windows Messenger
Windows Mobility Ce
Windows PowerShell
Windows Reliability A
Windows Remote Ma
Windows Remote She
Windows Security
Windows Update
Work Folders
All Settings
Preferences
Configuration
Policies
Preferences
Windows PowerShell
Turn on Script Execution
Edit policy setting
Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family
Description:
This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.
If you enable this policy setting, the scripts selected in the drop-down list are allowed to run.
The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher.
The "Allow local scripts and remote signed scripts" policy setting allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher.
The "Allow all scripts" policy
Setting
State
Comment
Turn on Module Logging
Enabled
No
Turn on PowerShell Script Block Logging
Enabled
No
Turn on Script Execution
Not configured
No
Turn on PowerShell Transcription
Not configured
No
Set the default source path for Update-Help
Not configured
No
Extended
Standard
5 setting(s)
Turn on Script Execution
Turn on Script Execution
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
Execution Policy
Allow all scripts
This policy setting lets you configure the script execution
controlling which scripts are allowed to run.
If you enable this policy setting, the scripts selected in the
down list are allowed to run.
The "Allow only signed scripts" policy setting allows scrip
execute only if they are signed by a trusted publisher.
7:34 PM
1/15/2021


Group Policy Management Editor
File Action View Help
Text Input
Windows Calendar
Windows Color Syster
Windows Customer E:
Windows Defender Ar
Windows Defender Ex
Windows Defender Sn
Windows Error Report
Windows Hello for Bu
Windows Ink Workspa
Windows Installer
Windows Logon Optic
Windows Media Digit
Windows Media Playe
Windows Messenger
Windows Mobility Cer
Windows PowerShell
Windows Reliability A
Windows Remote Mar
Windows Remote She
Windows Security
Windows Update
Work Folders
All Settings
Preferences
r Configuration
Policies
Preferences
Windows PowerShell
Turn on PowerShell Transcription
Edit policy setting
Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family
Description:
This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.
If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other
applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents
directory, with a file name that
includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent
Setting
State
Comment
Turn on Module Logging
Enabled
No
Turn on PowerShell Script Block Logging
Enabled
No
Turn on Script Execution
Enabled
No
Turn on PowerShell Transcription
Not configured
No
Set the default source path for Update-Help
Not configured
No
Extended
Standard
5 setting(s)
Turn on PowerShell Transcription
Turn on PowerShell Transcription
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
Transcript output directory
Include invocation headers:
This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.
If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other
applications that leverage the Windows PowerShell engine.
By default, Windows PowerShell will record transcript output to each users' My Documents
directory, with a file name that includes
7:36 PM
1/15/2021


Group Policy Management Editor
File Action View Help
Text Input
Windows Calendar
Windows Color Syster
Windows Customer E:
Windows Defender Ar
Windows Defender Ex
Windows Defender Sn
Windows Error Report
Windows Hello for Bu
Windows Ink Workspa
Windows Installer
Windows Logon Optic
Windows Media Digit:
Windows Media Playe
Windows Messenger
Windows Mobility Cer
Windows PowerShell
Windows Reliability A
Windows Remote Mar
Windows Remote She
Windows Security
Windows Update
Work Folders
All Settings
Preferences
r Configuration
Policies
Preferences
Windows PowerShell
Set the default source path for Update-Help
Edit policy setting
Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family
Description:
This policy setting allows you to set the default value of the SourcePath parameter on the Update-Help cmdlet.
If you enable this policy setting, the Update-Help cmdlet will use the specified value as the default value for the SourcePath parameter. This default value can be overridden by specifying a different value with the SourcePath parameter on the Update-Help cmdlet.
If this policy setting is disabled or not configured, this policy setting does not set a default value for the SourcePath parameter of the Update-Help cmdlet.
Setting
State
Comment
Turn on Module Logging
Enabled
No
Turn on PowerShell Script Block Logging
Enabled
No
Turn on Script Execution
Enabled
No
Turn on PowerShell Transcription
Enabled
No
Set the default source path for Update-Help
Not configured
No
Extended
Standard
5 setting(s)
Windows Server 2019 Standard Eva
Windows License valid for 1
Build 17763.rs5_release.1809
7:36 PM
1/15/2021


File Action View Help
Hyper-V Manager
ML-REFVM-244323
Virtual Machines
Name State CPU Usage
Windows 10 Running 0%
Actions
ML-REFVM-244323
Quick Create...
Windows 10 on ML-REFVM-244323 - Virtual Machine Connection
File Action Media View Help
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
enum_acls.ps1
1 $directory = Get-ChildItem .\
2 foreach ($item in $directory) {
3 Get-Acl $item
4 }
5
mib.bin NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
notepad.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
PFRO.log BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
regedit.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
splwow64.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
system.ini NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
twain_32.dll NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
win.ini NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
WindowsUpdate.log NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
winhlp32.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
WMSysPr9.prx NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
write.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
PS C:\Windows>
Completed


Windows 10 on ML-REFVM-244323 - Virtual Machine Connection
File Action Media View Help
Administrator: Windows PowerShell ISE
Documents
File Home Share View
This PC › Documents ›
Search Documents
Name
Date modified
Type
Size
20210116
1/16/2021 9:37 PM
File folder
20210121
1/21/2021 7:44 PM
File folder
20210122
1/22/2021 6:48 PM
File folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
3 items
Windows 10 Enterprise Evalua
Windows License valid for 81
Build 19041.vb_release.191206-
Type here to search
7:42 PM
1/22/2021