Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Set-ProcessMitigation'

PS C:\Users\wahid> Get-Help Set-ProcessMitigation

NAME

Set-ProcessMitigation

SYNOPSIS

Commands to enable and disable process mitigations or set them in bulk from an XML file.

SYNTAX

Set-ProcessMitigation [[-Name] <String>] [-Disable {DEP | EmulateAtlThunks | SEHOP | ForceRelocateImages | RequireInfo | BottomUp | HighEntropy | StrictHandle | DisableWin32kSystemCalls | AuditSystemCall | DisableExtensionPoints | BlockDynamicCode | AllowThreadsToOptOut | AuditDynamicCode | CFG | SuppressExports | StrictCFG | MicrosoftSignedOnly | AllowStoreSignedBinaries | AuditMicrosoftSigned | AuditStoreSigned | EnforceModuleDependencySigning | DisableNonSystemFonts | AuditFont | BlockRemoteImageLoads | BlockLowLabelImageLoads | PreferSystem32 | AuditRemoteImageLoads | AuditLowLabelImageLoads | AuditPreferSystem32 | EnableExportAddressFilter | AuditEnableExportAddressFilter | EnableExportAddressFilterPlus | AuditEnableExportAddressFilterPlus | EnableImportAddressFilter | AuditEnableImportAddressFilter |

EnableRopStackPivot | AuditEnableRopStackPivot | EnableRopCallerCheck |
AuditEnableRopCallerCheck | EnableRopSimExec | AuditEnableRopSimExec | SEHOP |
AuditSEHOP | SEHOPTelemetry | TerminateOnError | DisallowChildProcessCreation
| AuditChildProcess}] [-EAFModules <String[]>] [-Enable {DEP |
EmulateAtlThunks | SEHOP | ForceRelocateImages | RequireInfo | BottomUp |
HighEntropy | StrictHandle | DisableWin32kSystemCalls | AuditSystemCall |
DisableExtensionPoints | BlockDynamicCode | AllowThreadsToOptOut |
AuditDynamicCode | CFG | SuppressExports | StrictCFG | MicrosoftSignedOnly |
AllowStoreSignedBinaries | AuditMicrosoftSigned | AuditStoreSigned |
EnforceModuleDependencySigning | DisableNonSystemFonts | AuditFont |
BlockRemoteImageLoads | BlockLowLabelImageLoads | PreferSystem32 |
AuditRemoteImageLoads | AuditLowLabelImageLoads | AuditPreferSystem32 |
EnableExportAddressFilter | AuditEnableExportAddressFilter |
EnableExportAddressFilterPlus | AuditEnableExportAddressFilterPlus |
EnableImportAddressFilter | AuditEnableImportAddressFilter |
EnableRopStackPivot | AuditEnableRopStackPivot | EnableRopCallerCheck |
AuditEnableRopCallerCheck | EnableRopSimExec | AuditEnableRopSimExec | SEHOP |
AuditSEHOP | SEHOPTelemetry | TerminateOnError | DisallowChildProcessCreation
| AuditChildProcess}] [-Force {on | off | notset}] [-Remove] [-Reset]
[<CommonParameters>]

Set-ProcessMitigation [-Disable {DEP | EmulateAtlThunks | SEHOP |
ForceRelocateImages | RequireInfo | BottomUp | HighEntropy | StrictHandle |
DisableWin32kSystemCalls | AuditSystemCall | DisableExtensionPoints |
BlockDynamicCode | AllowThreadsToOptOut | AuditDynamicCode | CFG |
SuppressExports | StrictCFG | MicrosoftSignedOnly | AllowStoreSignedBinaries |
AuditMicrosoftSigned | AuditStoreSigned | EnforceModuleDependencySigning |
DisableNonSystemFonts | AuditFont | BlockRemoteImageLoads |
BlockLowLabelImageLoads | PreferSystem32 | AuditRemoteImageLoads |
AuditLowLabelImageLoads | AuditPreferSystem32 | EnableExportAddressFilter |
AuditEnableExportAddressFilter | EnableExportAddressFilterPlus |
AuditEnableExportAddressFilterPlus | EnableImportAddressFilter |
AuditEnableImportAddressFilter | EnableRopStackPivot |

AuditEnableRopStackPivot | EnableRopCallerCheck | AuditEnableRopCallerCheck |
EnableRopSimExec | AuditEnableRopSimExec | SEHOP | AuditSEHOP | SEHOPTelemetry
| TerminateOnError | DisallowChildProcessCreation | AuditChildProcess}]
[-EAFModules <String[]>] [-Enable {DEP | EmulateAtlThunks | SEHOP |
ForceRelocateImages | RequireInfo | BottomUp | HighEntropy | StrictHandle |
DisableWin32kSystemCalls | AuditSystemCall | DisableExtensionPoints |
BlockDynamicCode | AllowThreadsToOptOut | AuditDynamicCode | CFG |
SuppressExports | StrictCFG | MicrosoftSignedOnly | AllowStoreSignedBinaries |
AuditMicrosoftSigned | AuditStoreSigned | EnforceModuleDependencySigning |
DisableNonSystemFonts | AuditFont | BlockRemoteImageLoads |
BlockLowLabelImageLoads | PreferSystem32 | AuditRemoteImageLoads |
AuditLowLabelImageLoads | AuditPreferSystem32 | EnableExportAddressFilter |
AuditEnableExportAddressFilter | EnableExportAddressFilterPlus |
AuditEnableExportAddressFilterPlus | EnableImportAddressFilter |
AuditEnableImportAddressFilter | EnableRopStackPivot |
AuditEnableRopStackPivot | EnableRopCallerCheck | AuditEnableRopCallerCheck |
EnableRopSimExec | AuditEnableRopSimExec | SEHOP | AuditSEHOP | SEHOPTelemetry
| TerminateOnError | DisallowChildProcessCreation | AuditChildProcess}]
[-Force {on | off | notset}] [-Remove] [-Reset] [-System] [<CommonParameters>]

Set-ProcessMitigation [-IsValid] -PolicyFilePath <String> [<CommonParameters>]

DESCRIPTION

Used to turn on and off various process mitigation settings. Can also apply an
XML file to apply settings for many processes at once.

PARAMETERS

-Disable <String[]>

Comma separated list of mitigations to disable. Disable list takes
priority over enable list. If specified in both, it will be disabled.

-EAFModules <String[]>

Modules to be added to the EAF+ mitigation.

-Enable <String[]>

Comma separated list of mitigations to enable. Disable list takes priority over enable list. If specified in both, it will be disabled.

-Force <String>

Overrides a system setting either on or off depending on the level this is set at. Will force "on"/"off" all mitigations provided in the -Enable list

-IsValid [<SwitchParameter>]

Set to check the given XML file for validity. Requires local .xsd

-Name <String>

Name of the process to apply mitigation settings to. Can be in the format "notepad" or "notepad.exe"

-PolicyFilePath <String>

Path to XML file containing mitigation settings.

-Remove [<SwitchParameter>]

Removes a mitigation entry from the registry.

-Reset [<SwitchParameter>]

Resets a specific mitigation entry to defer.

-System [<SwitchParameter>]

Used to configure system defaults rather than individual apps.

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

---------- Example 1 ----------

PS C:\> Set-ProcessMitigation -Name Notepad.exe -Enable SEHOP -Disable ForceRelocateImages

Gets the current process mitigation for "notepad.exe" from the registry and then enables SEHOP, and disables ForceRelocateImages.

---------- Example 2 ----------

PS C:\> Set-ProcessMitigation -PolicyFilePath settings.xml

Applies all settings inside settings.xml

---------- Example 3 ----------

PS C:\> Set-ProcessMitigation -System -Enable DEP

Applies DEP at the system level. To disable mitigations, you can replace `-Enable` with `-Disable`. However, for app-level mitigations, this will force the mitigation to be disabled only for that app.

---------- Exmaple 4 ----------

PS C:\> Set-ProcessMitigation -System -Remove -Disable DEP

If you need to restore the mitigation back to the system default, you need to include the `-Remove` cmdlet as well, as in the above example:

---------- Example 5 ----------

PS C:\> Set-ProcessMitigation -System -Enable SEHOP

Enable SEHOP Component at the system level.

-------------------------- Example 6 --------------------------

PS C:\> Set-ProcessMitigation -System -Disable SEHOP

Disable SEHOP Component at the system level.

-------------------------- Example 7 --------------------------

PS C:\> Set-ProcessMitigation -System -Reset

Reset Mitigation at the system level.

REMARKS

To see the examples, type: "get-help Set-ProcessMitigation -examples".

For more information, type: "get-help Set-ProcessMitigation -detailed".

For technical information, type: "get-help Set-ProcessMitigation -full".

For online help, type: "get-help Set-ProcessMitigation -online"