We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies

Accept    Reject    Manage cookies

# Microsoft Ignite

Nov 19–22, 2024

Register now >

Learn    Discover ∨    Product documentation ∨    Development languages ∨    Topics ∨    Sign in

Microsoft 365    Solutions and architecture ∨    Apps and services ∨    Training ∨    Resources ∨    Free Account

**Version**

Windows 11 and Windows Server 2022 PowerShell

Search

Learn / Windows / PowerShell / Defender /

# Set-MpPreference

Reference                                                      Feedback

Module: Defender

## In this article

Syntax

Description

Examples

Parameters

Related Links

Configures preferences for Windows Defender scans and updates.

# Syntax

PowerShell                                                      Copy

```powershell
Set-MpPreference
    [-AllowDatagramProcessingOnWinServer <Boolean>]
    [-AllowNetworkProtectionDownLevel <Boolean>]
    [-AllowNetworkProtectionOnWinServer <Boolean>]
    [-AllowSwitchToAsyncInspection <Boolean>]
    [-AsJob]
    [-AttackSurfaceReductionOnlyExclusions <String[]>]
    [-AttackSurfaceReductionRules_Actions <ASRRuleActionType[]>]
    [-AttackSurfaceReductionRules_Ids <String[]>]
    [-CheckForSignaturesBeforeRunningScan <Boolean>]
    [-CimSession <CimSession[]>]
    [-CloudBlockLevel <CloudBlockLevelType>]
    [-CloudExtendedTimeout <UInt32>]
    [-ControlledFolderAccessAllowedApplications <String[]>]
    [-ControlledFolderAccessProtectedFolders <String[]>]
    [-DefinitionUpdatesChannel <UpdatesChannelType>]
    [-DisableArchiveScanning <Boolean>]
    [-DisableAutoExclusions <Boolean>]
    [-DisableBehaviorMonitoring <Boolean>]
    [-DisableBlockAtFirstSeen <Boolean>]
    [-DisableCacheMaintenance <UInt32>]
    [-DisableCatchupFullScan <Boolean>]
    [-DisableCatchupQuickScan <Boolean>]
    [-DisableCpuThrottleOnIdleScans <Boolean>]
    [-DisableDatagramProcessing <Boolean>]
    [-DisableDnsOverTcpParsing <Boolean>]
    [-DisableDnsParsing <Boolean>]
    [-DisableEmailScanning <Boolean>]
```

Download PDF

```
[-DisableFtpParsing <Boolean>]
[-DisableGradualRelease <Boolean>]
[-DisableHttpParsing <Boolean>]
[-DisableIOAVProtection <Boolean>]
[-DisableInboundConnectionFiltering <Boolean>]
[-DisableNetworkProtectionPerfTelemetry <Boolean>]
[-DisablePrivacyMode <Boolean>]
[-DisableRdpParsing <Boolean>]
[-DisableRealtimeMonitoring <Boolean>]
[-DisableRemovableDriveScanning <Boolean>]
[-DisableRestorePoint <Boolean>]
[-DisableScanningMappedNetworkDrivesForFullScan <Boolean>]
[-DisableScanningNetworkFiles <Boolean>]
[-DisableScriptScanning <Boolean>]
[-DisableSmtpParsing <Boolean>]
[-DisableSshParsing <Boolean>]
[-DisableTlsParsing <Boolean>]
[-EnableControlledFolderAccess <ControlledFolderAccessType>]
[-EnableDnsSinkhole <Boolean>]
[-EnableFileHashComputation <Boolean>]
[-EnableFullScanOnBatteryPower <Boolean>]
[-EnableLowCpuPriority <Boolean>]
[-EnableNetworkProtection <ASRRuleActionType>]
[-EngineUpdatesChannel <UpdatesChannelType>]
[-ExclusionExtension <String[]>]
[-ExclusionIpAddress <String[]>]
[-ExclusionPath <String[]>]
[-ExclusionProcess <String[]>]
[-ForceUseProxyOnly <Boolean>]
[-Force]
[-HighThreatDefaultAction <ThreatAction>]
[-IntelTDTEnabled <UInt32>]
[-LowThreatDefaultAction <ThreatAction>]
[-MAPSReporting <MAPSReportingType>]
[-MeteredConnectionUpdates <Boolean>]
[-ModerateThreatDefaultAction <ThreatAction>]
[-OobeEnableRtpAndSigUpdate <Boolean>]
[-PUAProtection <PUAProtectionType>]
[-PlatformUpdatesChannel <UpdatesChannelType>]
[-ProxyBypass <String[]>]
[-ProxyPacUrl <String>]
[-ProxyServer <String>]
[-QuarantinePurgeItemsAfterDelay <UInt32>]
[-RandomizeScheduleTaskTimes <Boolean>]
[-RealTimeScanDirection <ScanDirection>]
[-RemediationScheduleDay <Day>]
[-RemediationScheduleTime <DateTime>]
[-ReportingAdditionalActionTimeOut <UInt32>]
[-ReportingCriticalFailureTimeOut <UInt32>]
[-ReportingNonCriticalTimeOut <UInt32>]
[-ScanAvgCPULoadFactor <Byte>]
[-ScanOnlyIfIdleEnabled <Boolean>]
[-ScanParameters <ScanType>]
[-ScanPurgeItemsAfterDelay <UInt32>]
[-ScanScheduleDay <Day>]
[-ScanScheduleOffset <UInt32>]
[-ScanScheduleQuickScanTime <DateTime>]
[-ScanScheduleTime <HH:MM:SS>]
[-SchedulerRandomizationTime <UInt32>]
[-ServiceHealthReportInterval <UInt32>]
[-SevereThreatDefaultAction <ThreatAction>]
[-SharedSignaturesPath <String>]
[-SignatureAuGracePeriod <UInt32>]
[-SignatureBlobFileSharesSources <String>]
[-SignatureBlobUpdateInterval <UInt32>]
[-SignatureDefinitionUpdateFileSharesSources <String>]
[-SignatureDisableUpdateOnStartupWithoutEngine <Boolean>]
[-SignatureFallbackOrder <String>]
[-SignatureFirstAuGracePeriod <UInt32>]
[-SignatureScheduleDay <Day>]
[-SignatureScheduleTime <DateTime>]
[-SignatureUpdateCatchupInterval <UInt32>]
[-SignatureUpdateInterval <UInt32>]
[-SignaturesUpdatesChannel <UpdatesChannelType>]
[-SubmitSamplesConsent <SubmitSamplesConsentType>]
[-ThreatIDDefaultAction_Actions <ThreatAction[]>]
[-ThreatIDDefaultAction_Ids <Int64[]>]
[-ThrottleLimit <Int32>]
```

```
    [-UILockdown <Boolean>]
    [-UnknownThreatDefaultAction <ThreatAction>]
    [<CommonParameters>]
```

# Description

The **Set-MpPreference** cmdlet configures preferences for Windows Defender scans and updates. You can modify exclusion file name extensions, paths, or processes, and specify the default action for high, moderate, and low threat levels.

REMEDIATION VALUES

The following table provides remediation action values for detected threats at low, medium, high, and severe alert levels.

⌞ ⌝ Expand table

| Value | Action | |
|-------|--------|---|
| 1 | Clean the detected threat. | |
| 2 | Quarantine the detected threat. | |
| 3 | Remove the detected threat. | |
| 6 | Allow the detected threat. | |
| 8 | Allow the user to determine the action to take with the detected threat. | |
| 9 | Don't take any action. | |
| 10 | Block the detected threat. | |
| 0 | (NULL) | Apply action based on the Security Intelligence Update (SIU). This is the default value. |

# Examples

## Example 1: Schedule to check for definition updates everyday

PowerShell          📋 Copy

```
PS C:\> Set-MpPreference -SignatureScheduleDay Everyday
```

This command configures preferences to check for definition updates every day.

## Example 2: Schedule a time of day to check for definition updates

PowerShell          📋 Copy

```
PS C:\> Set-MpPreference -SignatureScheduleTime 02:00:00
```

This command configures preferences to check for definition updates 120 minutes after midnight on days when it's scheduled to check.

# Parameters

**-AllowDatagramProcessingOnWinServer**

Specifies whether to disable inspection of UDP connections on Windows Server.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | adpows |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-AllowNetworkProtectionDownLevel**

Specifies whether to allow network protection to be set to Enabled or Audit Mode on Windows versions before 1709.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | anpdl |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-AllowNetworkProtectionOnWinServer**

Specifies whether to allow network protection to be set to Enabled or Audit Mode for Windows Server.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | anpws |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-AllowSwitchToAsyncInspection**

Specifies whether to enable a performance optimization that allows synchronously inspected network flows to switch to async inspection once they have been checked and validated.

⧉ Expand table

| Type: | Boolean |
|---|---|
| Position: | Named |
| Default value: | Enabled |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-AsJob**

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

The cmdlet immediately returns an object that represents the job and then displays the command prompt. You can continue to work in the session while the job completes. To manage the job, use the `*-Job` cmdlets. To get the job results, use the Receive-Job⧉ cmdlet.

For more information about Windows PowerShell background jobs, see about_Jobs⧉ .

⧉ Expand table

| Type: | SwitchParameter |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-AttackSurfaceReductionOnlyExclusions**

Specifies the files and paths to exclude from Attack Surface Reduction (ASR) rules. Specify the folders or files and resources that should be excluded from ASR rules. Enter a folder path or a fully qualified resource name. For example, ""C:\Windows"" will exclude all files in that directory. ""C:\Windows\App.exe"" will exclude only that specific file in that specific folder.

For more information about excluding files and folders from ASR rules.

⧉ Expand table

| Type: | String[] |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-AttackSurfaceReductionRules_Actions**

Specifies the states of attack surface reduction rules specified by using the **AttackSurfaceReductionRules_Ids** parameter. If you add multiple rules as a comma-separated list, specify their states separately as a comma-separated list.

⛶ **Expand table**

| | |
|---|---|
| Type: | ASRRuleActionType[] |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -AttackSurfaceReductionRules_Ids

Specifies the states of attack surface reduction rules specified by using the **AttackSurfaceReductionRules_Ids** parameter. If you add multiple rules as a comma-separated list, specify their states separately as a comma-separated list.

⛶ **Expand table**

| | |
|---|---|
| Type: | String[] |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -CheckForSignaturesBeforeRunningScan

Indicates whether to check for new virus and spyware definitions before Windows Defender runs a scan. If you specify a value of $True, Windows Defender checks for new definitions. If you specify $False or don't specify a value, the scan begins with existing definitions. This setting applies to scheduled scans, but it has no effect on scans initiated manually from the user interface or on scans started from the command line using "mpcmdrun -Scan".

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | csbr |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -CimSession

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession ⬈ or Get-CimSession ⬈ cmdlet.

The default is the current session on the local computer.

⛶ **Expand table**

| Type: | CimSession[] |
|---|---|
| Aliases: | Session |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -CloudBlockLevel

Specifies a cloud block level. This value determines how aggressive Microsoft Defender Antivirus is in blocking and scanning suspicious files.

⛶ **Expand table**

| Type: | CloudBlockLevelType |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -CloudExtendedTimeout

Specifies the amount of extended time to block a suspicious file and scan it in the cloud. Standard time is 10 seconds. Extend by up to 50 seconds.

⛶ **Expand table**

| Type: | UInt32 |
|---|---|
| Aliases: | cloudextimeout |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ControlledFolderAccessAllowedApplications

Specifies applications that can make changes in controlled folders.

⛶ **Expand table**

| Type: | String[] |
|---|---|
| Position: | Named |
| Default value: | None |

| Required: | False |
|---|---|
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ControlledFolderAccessProtectedFolders

Specifies more folders to protect.

⌞⌝ **Expand table**

| Type: | String[] |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableArchiveScanning

Indicates whether to scan archive files, such as .zip and .cab files, for malicious and unwanted software. If you specify a value of $False or do not specify a value, Windows Defender scans archive files.

⌞⌝ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | darchsc |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableAutoExclusions

Indicates whether to disable the Automatic Exclusions feature for the server. If you specify a value of $False or do not specify a value, Windows Defender enables the Automatic Exclusions feature for the server.

⌞⌝ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | dae |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableBehaviorMonitoring**

Indicates whether to enable behavior monitoring. If you specify a value of $False or do not specify a value, Windows Defender enables behavior monitoring.

⌗ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | dbm |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableBlockAtFirstSeen**

Indicates whether to enable block at first seen. If you specify a value of $False or do not specify a value, Windows Defender enables block at first seen.

⌗ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | dbaf |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableCacheMaintenance**

Defines whether the cache maintenance idle task will perform the cache maintenance or not. Allowed values are 1 - cache maintenance is disabled, and 0 - cache maintenance is enabled (default).

⌗ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | dcm |
| Position: | Named |
| Default value: | 0 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableCatchupFullScan**

Indicates whether Windows Defender runs catch-up scans for scheduled full scans. A computer can miss a scheduled scan, usually because the computer is turned off at the

scheduled time. If you specify a value of $False, after the computer misses two scheduled full scans, Windows Defender runs a catch-up scan the next time someone logs on to the computer. If you specify a value of $True, the computer does not run catch-up scans for scheduled full scans.

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dcfsc |
| Position: | Named |
| Default value: | 0 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableCatchupQuickScan

Indicates whether Windows Defender runs catch-up scans for scheduled quick scans. A computer can miss a scheduled scan, usually because the computer is off at the scheduled time. If you specify a value of $False, after the computer misses two scheduled quick scans, Windows Defender runs a catch-up scan the next time someone logs onto the computer. If you specify a value of $True, the computer does not run catch-up scans for scheduled quick scans.

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dcqsc |
| Position: | Named |
| Default value: | True |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableCpuThrottleOnIdleScans

Indicates whether the CPU will be throttled for scheduled scans while the device is idle. This parameter is enabled by default, thus ensuring that the CPU won't be throttled for scheduled scans performed when the device is idle, regardless of what **ScanAvgCPULoadFactor** is set to. For all other scheduled scans, this flag does not have any impact and normal throttling will occur.

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | None |
| Position: | Named |
| Default value: | True |
| Required: | False |
| Accept pipeline input: | False |

| Accept wildcard characters: | False |
| --- | --- |

### -DisableDatagramProcessing

Specifies whether to disable inspection of UDP connections.

⛶ **Expand table**

| Type: | Boolean |
| --- | --- |
| Aliases: | ddtgp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableDnsOverTcpParsing

Specifies whether to disable inspection of DNS traffic that occurs over a TCP channel.

⛶ **Expand table**

| Type: | Boolean |
| --- | --- |
| Aliases: | ddnstcpp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableDnsParsing

Specifies whether to disable inspection of DNS traffic that occurs over a UDP channel. Network protection inspects DNS traffic that occurs over a TCP channel to provide metadata for anti-malware behavior monitoring or to allow for DNS sink holing if the "-EnableDnsSinkhole" configuration is set. This can be disabled by setting this value to "$true".

⛶ **Expand table**

| Type: | Boolean |
| --- | --- |
| Aliases: | ddnsp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableEmailScanning

Indicates whether Windows Defender parses the mailbox and mail files, according to their specific format, in order to analyze mail bodies and attachments. Windows Defender supports several formats, including .pst, .dbx, .mbx, .mime, and .binhex. If you specify a value of $False or do not specify a value, Windows Defender performs email scanning. If you specify a value of $True, Windows Defender does not perform email scanning.

⛶ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | demsc |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableFtpParsing

Specifies whether to disable FTP parsing for network protection.

⛶ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | dfp |
| Position: | Named |
| Default value: | 0 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableGradualRelease

Specifies whether to disable gradual rollout of monthly and daily Windows Defender updates. If you enable this option, devices are offered all updates after the gradual release cycle finishes. Consider this option for datacenter computers that only receive limited updates.

This setting applies to both monthly and daily updates. It overrides configured channel selections for platform and engine updates.

If you disable or do not configure this policy, the device remains in Current Channel (Default) unless specified otherwise in specific channels. The device stays up to date automatically during the gradual release cycle, which is suitable for most devices.

This policy is available starting with platform version 4.18.2106.5 and later.

⛶ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | dgr |
| Position: | Named |
| Default value: | None |

| | |
|---|---|
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableHttpParsing

Specifies whether disable inspection of HTTP traffic. If **EnableNetworkProtection** has the value `Enabled`, HTTP connections to malicious websites can be blocked.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dhttpp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableInboundConnectionFiltering

Specifies whether to inspect only outbound connections. By default, Network Protection inspects both inbound and outbound connections.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dicf |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableIOAVProtection

Indicates whether Windows Defender scans all downloaded files and attachments. If you specify a value of $False or do not specify a value, scanning downloaded files and attachments is enabled.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dioavp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |

| | |
|---|---|
| Accept wildcard characters: | False |

**-DisableNetworkProtectionPerfTelemetry**

This setting disables the gathering and sending of performance telemetry from network protection. The accepted values are 0 and 1.

- 1- Network protection telemetry is disabled.
- 0 (Default) - Network protection telemetry is enabled.

⌟⌞ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dnpp |
| Position: | Named |
| Default value: | 0 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisablePrivacyMode**

**This is a legacy setting that does not have any affect on current platforms**. The intent of this parameter was to disable privacy mode, which prevented users, other than administrators, from displaying threat history. When this parameter was in use, if you specified a value of $False or did not specify a value, privacy mode was enabled.

⌟⌞ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dpm |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableRdpParsing**

This setting controls whether to parse RDP traffic to look for malicious attacks using the RDP protocol.

⌟⌞ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | drdpp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |

| | |
|---|---|
| Accept wildcard characters: | False |

### -DisableRealtimeMonitoring

Indicates whether to use real-time protection. If you specify a value of $False or do not specify a value, Windows Defender uses real-time protection. We recommend that you enable Windows Defender to use real-time protection.

⧉ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | drtm |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableRemovableDriveScanning

Indicates whether to scan for malicious and unwanted software in removable drives, such as flash drives, during a full scan. If you specify a value of $False or do not specify a value, Windows Defender scans removable drives during any type of scan. If you specify a value of $True, Windows Defender does not scan removable drives during a full scan. Windows Defender can still scan removable drives during quick scans or custom scans.

⧉ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | drdsc |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -DisableRestorePoint

Indicates whether to disable scanning of restore points. If you specify a value of $False or do not specify a value, Windows Defender restore point is enabled.

⧉ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | drp, dsnf |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |

| | |
|---|---|
| Accept wildcard characters: | False |

**-DisableScanningMappedNetworkDrivesForFullScan**

Indicates whether to scan mapped network drives. If you specify a value of $False or do not specify a value, Windows Defender scans mapped network drives. If you specify a value of $True, Windows Defender does not scan mapped network drives.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dsmndfsc |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableScanningNetworkFiles**

Indicates whether to scan for network files. If you specify a value of $False or do not specify a value, Windows Defender scans network files. If you specify a value of $True, Windows Defender does not scan network files.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dsnf |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableScriptScanning**

Specifies whether to disable the scanning of scripts during malware scans. If you specify a value of $False or do not specify a value, Windows Defender does not scan scripts.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | dscrptsc |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableSmtpParsing**

This setting disables SMTP parsing for network protection. The accepted values are 0 and 1.

- 1 - SMTP parsing is disabled.
- 0 (Default) - SMTP parsing is enabled.

⛶ Expand table

| Type: | Boolean |
|---|---|
| Aliases: | dsp |
| Position: | Named |
| Default value: | 0 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableSshParsing**

Specifies whether to disable inspection of SSH traffic. By default, Network Protection inspects SSH traffic.

⛶ Expand table

| Type: | Boolean |
|---|---|
| Aliases: | dsshp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-DisableTlsParsing**

Specifies whether to disable inspection of TLS traffic. Network protection inspects TLS traffic (also known as HTTPS traffic) to see if a connection is being made to a malicious website, and to provide metadata to behavior monitoring. TLS connections to malicious websites can also be blocked if "-EnableNetworkProtection" is set to enabled. HTTP inspection can be disabled by setting this value to "$true". By default, network protection inspects TLS traffic.

⛶ Expand table

| Type: | Boolean |
|---|---|
| Aliases: | dtlsp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-Enable UdpReceiveOffload:**

Specifies whether UDP receive offload support in Network Protection is enabled, resulting in potentially higher UDP bandwidth in the inbound direction. Starting with platform version `4.18.24030`, Microsoft will gradually move this support default from disabled to enabled. This setting can be manually controlled by setting it to `1` to enable and `0` to disable.

⤢ Expand table

| Type: | ASRRuleActionType |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-Enable UdpSegmentationOffload:**

Specifies whether UDP segmentation offload support in Network Protection is enabled, resulting in potentially higher UDP bandwidth in the outbound direction. Starting with platform version `4.18.24030`, Microsoft will gradually move this support default from disabled to enabled. This setting can be manually controlled by setting it to `1` to enable and `0` to disable.

⤢ Expand table

| Type: | ASRRuleActionType |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-EnableControlledFolderAccess**

Specifies the state for the controlled folder access feature. Valid values are Disabled, Enabled, and Audit Mode.

⤢ Expand table

| Type: | ControlledFolderAccessType |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-EnableConvertWarnToBlock**

This setting controls whether network protection blocks network traffic instead of displaying a warning. This setting can be manually controlled by setting it to `1` to enable and `0` to disable.

⌭ **Expand table**

| Type: | ASRRuleActionType |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -EnableDnsSinkhole (Deprecated)

Specifies whether to examine DNS traffic to detect and sinkhole DNS exfiltration attempts and other DNS based malicious attacks. Network protection can inspect the DNS traffic of a machine and, in conjunction with behavior monitoring, detect and sink hole DNS exfiltration attempts, and other DNS based malicious attacks. Set this configuration to "$true" to enable this feature.

⌭ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | ednss |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -EnableFileHashComputation

Specifies whether to enable file hash computation. When this feature is enabled, Windows Defender computes hashes for files it scans.

⌭ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | efhc |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -EnableFullScanOnBatteryPower

Specifies whether Windows Defender does a full scan while on battery power.

⌭ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | efsobp |

| Position: | Named |
|---|---|
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

## -EnableLowCpuPriority

Specifies whether Windows Defender uses low CPU priority for scheduled scans.

⛶ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | elcp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

## -EnableNetworkProtection

Specifies how the network protection service handles web-based malicious threats, including phishing and malware. Possible values are Disabled, Enabled, and AuditMode.

⛶ **Expand table**

| Type: | ASRRuleActionType |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

## -EngineUpdatesChannel

Specifies when devices receive Microsoft Defender engine updates during the monthly gradual rollout.

Valid values are:

- NotConfigured. Devices stay up to date automatically during the gradual release cycle. This value is suitable for most devices.
- Beta. Devices are the first to receive new updates. Select Beta Channel to participate in identifying and reporting issues to Microsoft. Devices in the Windows Insider Program are subscribed to this channel by default. This value is for use in manual test environments only and a limited number of devices.
- Broad. Devices are offered updates only after the gradual release cycle completes. This value is suggested for a broad set of devices in your production population, from 10 to 100 percent.
- Preview. Devices are offered updates earliest during the monthly gradual release cycle. This value is suggested for pre-production or validation environments.

- Staged. Devices are offered updates after the monthly gradual release cycle. This value is suggested for a small, representative part of your production population, around 10 percent.

⌷ **Expand table**

| | |
|---|---|
| Type: | UpdatesChannelType |
| Aliases: | erelr |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ExclusionExtension

Specifies an array of file name extensions, such as obj or lib, to exclude from scheduled, custom, and real-time scanning.

⌷ **Expand table**

| | |
|---|---|
| Type: | String[] |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ExclusionIpAddress

Specifies an array of IP addresses to exclude from scheduled and real-time scanning.

⌷ **Expand table**

| | |
|---|---|
| Type: | String[] |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ExclusionPath

Specifies an array of file paths to exclude from scheduled and real-time scanning. You can specify a folder to exclude all the files under the folder.

⌷ **Expand table**

| | |
|---|---|
| Type: | String[] |
| Position: | Named |

| Default value: | None |
|---|---|
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ExclusionProcess

Specifies an array of processes, as paths to process images. This cmdlet excludes any files opened by the processes that you specify from scheduled and real-time scanning. Specifying this parameter excludes files opened by executable programs only. The cmdlet does not exclude the processes themselves. To exclude a process, specify it by using the **ExclusionPath** parameter.

⌖ **Expand table**

| Type: | String[] |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -Force

Forces the command to run without asking for user confirmation.

⌖ **Expand table**

| Type: | SwitchParameter |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ForceUseProxyOnly

Specifies whether to force the device to use only the proxy.

⌖ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | fupo |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-HighThreatDefaultAction**

Specifies which automatic remediation action to take for a high level threat. The acceptable
values for this parameter are:

- Quarantine
- Remove
- Ignore

⛶ Expand table

| | |
|---|---|
| Type: | ThreatAction |
| Aliases: | htdefac |
| Accepted values: | Clean, Quarantine, Remove, Allow, UserDefined, NoAction, Block |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-IntelTDTEnabled**

This policy setting configures the Intel TDT integration level for Intel TDT-capable devices.
The acceptable values for this parameter are:

- 0 (Default) - If you don't configure this setting, the default value will be applied. The
  default value is controlled by Microsoft security intelligence updates. Microsoft will
  enable Intel TDT if there is a known threat.
- 1 - If you configure this setting to enabled, Intel TDT integration will turn on.
- 2 - If you configure this setting to disabled, Intel TDT integration will turn off.

⛶ Expand table

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | itdte |
| Accepted values: | 0, 1 and 2 |
| Position: | Named |
| Default value: | 0 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-LowThreatDefaultAction**

Specifies which automatic remediation action to take for a low level threat. The acceptable
values for this parameter are:

- Quarantine
- Remove
- Ignore

⛶ Expand table

| Type: | ThreatAction |
|---|---|
| Aliases: | ltdefac |
| Accepted values: | Clean, Quarantine, Remove, Allow, UserDefined, NoAction, Block |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-MAPSReporting**

Specifies the type of membership in Microsoft Active Protection Service. Microsoft Active Protection Service is an online community that helps you choose how to respond to potential threats. The community also helps prevent the spread of new malicious software. The acceptable values for this parameter are:

- 0: Disabled. Send no information to Microsoft. This is the default value.
- 1: Basic membership. Send basic information to Microsoft about detected software, including where the software came from, the actions that you apply or that apply automatically, and whether the actions succeeded.
- 2: Advanced membership. In addition to basic information, send more information to Microsoft about malicious software, spyware, and potentially unwanted software, including the location of the software, file names, how the software operates, and how it affects your computer.

If you join this community, you can choose to automatically send basic or additional information about detected software. Additional information helps Microsoft create new definitions. In some instances, personal information might unintentionally be sent to Microsoft. However, Microsoft will not use this information to identify you or contact you.

⌞⌝ **Expand table**

| Type: | MAPSReportingType |
|---|---|
| Accepted values: | Disabled, Basic, Advanced |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-MeteredConnectionUpdates**

Specifies whether to update managed devices to update through metered connections. Data charges may apply.

⌞⌝ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | mcupd |
| Position: | Named |
| Default value: | None |

| | |
|---|---|
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ModerateThreatDefaultAction

Specifies which automatic remediation action to take for a moderate level threat. The acceptable values for this parameter are:

- Quarantine
- Remove
- Ignore

⛶ Expand table

| | |
|---|---|
| Type: | ThreatAction |
| Aliases: | mtdefac |
| Accepted values: | Clean, Quarantine, Remove, Allow, UserDefined, NoAction, Block |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -OobeEnableRtpAndSigUpdate

This setting allows you to configure whether real-time protection and Security Intelligence Updates are enabled during Out of Box experience (OOBE).

Valid values are:

- True - If you enable this setting, real-time protection and Security Intelligence Updates are enabled during OOBE.
- False (Default) - If you either disable or don't configure this setting, real-time protection and Security Intelligence Updates during OOBE aren't enabled.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Position: | Named |
| Default value: | False |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -PlatformUpdatesChannel

Specifies when devices receive Microsoft Defender platform updates during the monthly gradual rollout.

Valid values are:

- NotConfigured. Devices stay up to date automatically during the gradual release cycle. This value is suitable for most devices.
- Beta. Devices are the first to receive new updates. Select Beta Channel to participate in identifying and reporting issues to Microsoft. Devices in the Windows Insider Program are subscribed to this channel by default. This value is for use in manual test environments only and a limited number of devices.
- Broad. Devices are offered updates only after the gradual release cycle completes. This value is suggested for a broad set of devices in your production population, from 10 to 100 percent.
- Preview. Devices are offered updates earliest during the monthly gradual release cycle. This value is suggested for pre-production or validation environments.
- Staged. Devices are offered updates after the monthly gradual release cycle. This value is suggested for a small, representative part of your production population, around 10 percent.

⌞⌝ **Expand table**

| | |
|---|---|
| Type: | UpdatesChannelType |
| Aliases: | prelr |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-ProxyBypass**

Specifies proxy bypasses.

⌞⌝ **Expand table**

| | |
|---|---|
| Type: | String[] |
| Aliases: | proxbps |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-ProxyPacUrl**

Specifies the Privilege Attribute Certificate (PAC) proxy.

⌞⌝ **Expand table**

| | |
|---|---|
| Type: | String |
| Aliases: | ppurl |
| Position: | Named |
| Default value: | None |
| Required: | False |

| | |
|---|---|
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ProxyServer

Specifies the proxy server.

⬚ **Expand table**

| | |
|---|---|
| Type: | String |
| Aliases: | proxsrv |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -PUAProtection

Specifies the level of detection for potentially unwanted applications. When potentially unwanted software is downloaded or attempts to install itself on your computer, you are warned.

⬚ **Expand table**

| | |
|---|---|
| Type: | PUAProtectionType |
| Accepted values: | Disabled, Enabled, AuditMode |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -QuarantinePurgeItemsAfterDelay

Specifies the number of days to keep items in the Quarantine folder. If you specify a value of zero or do not specify a value for this parameter, items stay in the Quarantine folder indefinitely.

⬚ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | qpiad |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-RandomizeScheduleTaskTimes**

Indicates whether to select a random time for the scheduled start and scheduled update for definitions. If you specify a value of $True or do not specify a value, scheduled tasks begin within 30 minutes, before or after, the scheduled time. If you randomize the start times, it can distribute the impact of scanning. For example, if several virtual machines share the same host, randomized start times prevents all the hosts from starting the scheduled tasks at the same time.

⛶ **Expand table**

| Type: | Boolean |
|---|---|
| Aliases: | rstt |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-RealTimeScanDirection**

Specifies scanning configuration for incoming and outgoing files on NTFS volumes. The acceptable values for this parameter are:

- 0: Scan both incoming and outgoing files. This is the default.
- 1: Scan incoming files only.
- 2: Scan outgoing files only.

Specify a value for this parameter to enhance performance on servers which have a large number of file transfers, but need scanning for either incoming or outgoing files. Evaluate this configuration based on the server role. For non-NTFS volumes, Windows Defender performs full monitoring of file and program activity.

⛶ **Expand table**

| Type: | ScanDirection |
|---|---|
| Aliases: | rtsd |
| Accepted values: | Both, Incoming, Outcoming |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-RemediationScheduleDay**

Specifies the day of the week on which to perform a scheduled full scan in order to complete remediation. Alternatively, specify everyday for this full scan or never. The acceptable values for this parameter are:

- 0: Everyday
- 1: Sunday
- 2: Monday
- 3: Tuesday

- 4: Wednesday
- 5: Thursday
- 6: Friday
- 7: Saturday
- 8: Never

The default value is 8, never. If you specify a value of 8 or do not specify a value, Windows Defender performs a scheduled full scan to complete remediation by using a default frequency.

⛶ Expand table

| | |
|---|---|
| Type: | Day |
| Aliases: | rsd |
| Accepted values: | Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Never |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -RemediationScheduleTime

Specifies the time of day, as the number of minutes after midnight, to perform a scheduled scan. The time refers to the local time on the computer. If you do not specify a value for this parameter, a scheduled scan runs at the default time of two hours after midnight.

⛶ Expand table

| | |
|---|---|
| Type: | DateTime |
| Aliases: | rst |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ReportingAdditionalActionTimeOut

Specifies the number of minutes before a detection in the additional action state changes to the cleared state.

⛶ Expand table

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | raat |
| Position: | Named |
| Default value: | None |
| Required: | False |

| | |
|---|---|
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ReportingCriticalFailureTimeOut

Specifies the number of minutes before a detection in the critically failed state changes to either the additional action state or the cleared state.

⛶ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | rcto |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ReportingNonCriticalTimeOut

Specifies the number of minutes before a detection in the non-critically failed state changes to the cleared state.

⛶ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | rncto |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanAvgCPULoadFactor

Specifies the maximum percentage CPU usage for a scan. The acceptable values for this parameter are: integers from 5 through 100, and the value 0, which disables CPU throttling. Windows Defender does not exceed the percentage of CPU usage that you specify. The default value is 50.

Note: This is not a hard limit but rather a guidance for the scanning engine to not exceed this maximum on average. If ScanOnlyIfIdleEnabled (instructing the product to scan only when the computer is not in use) and DisableCpuThrottleOnIdleScans (instructing the product to disable CPU throttling on idle scans) are both enabled, then the value of ScanAvgCPULoadFactor is ignored.

⛶ **Expand table**

| | |
|---|---|
| Type: | Byte |
| Aliases: | saclf |
| Position: | Named |

| | |
|---|---|
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanOnlyIfIdleEnabled

Indicates whether to start scheduled scans only when the computer is not in use. If you specify a value of $True or do not specify a value, Windows Defender runs schedules scans when the computer is on, but not in use.

⛶ Expand table

| | |
|---|---|
| Type: | Boolean |
| Aliases: | soiie |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanParameters

Specifies the scan type to use during a scheduled scan. The acceptable values for this parameter are:

- 1: Quick scan
- 2: Full scan

If you do not specify this parameter, Windows Defender uses the default value of quick scan.

⛶ Expand table

| | |
|---|---|
| Type: | ScanType |
| Accepted values: | QuickScan, FullScan |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanPurgeItemsAfterDelay

Specifies the number of days to keep items in the scan history folder. After this time, Windows Defender removes the items. If you specify a value of zero, Windows Defender does not remove items. If you do not specify a value, Windows Defender removes items from the scan history folder after the default length of time, which is 15 days.

⛶ Expand table

| | |
|---|---|
| Type: | UInt32 |

| | |
|---|---|
| Aliases: | spiad |
| Position: | Named |
| Default value: | 15 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanScheduleDay

Specifies the day of the week on which to perform a scheduled scan. Alternatively, specify everyday for a scheduled scan or never. The acceptable values for this parameter are:

- 0: Everyday
- 1: Sunday
- 2: Monday
- 3: Tuesday
- 4: Wednesday
- 5: Thursday
- 6: Friday
- 7: Saturday
- 8: Never

The default value is 8, never. If you specify a value of 8 or do not specify a value, Windows Defender does not perform scheduled scans.

⌐⌐ **Expand table**

| | |
|---|---|
| Type: | Day |
| Aliases: | scsd |
| Accepted values: | Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Never |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanScheduleOffset

Configures the number of minutes after midnight to perform a scheduled scan. The time on the endpoint is used to determine the local time. If you enable this setting, a scheduled scan will run at the time specified. If you disable or don't enable this setting, a scheduled scan runs at the default time of two hours (120 minutes) after midnight.

⌐⌐ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | scso |
| Position: | Named |
| Default value: | None |

| | |
|---|---|
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanScheduleQuickScanTime

Specifies the time of day, as the number of minutes after midnight, to perform a scheduled quick scan. The time refers to the local time on the computer. If you do not specify a value for this parameter, a scheduled quick scan runs at the time specified by the **ScanScheduleOffset** parameter. That parameter has a default time of two hours after midnight.

⛶ **Expand table**

| | |
|---|---|
| Type: | DateTime |
| Aliases: | scsqst |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ScanScheduleTime

Specifies the time of day to run a scheduled scan. The time refers to the local time on the computer. Specify the number of minutes after midnight (for example, enter 60 for 1 a.m.). This parameter has a default time of two hours after midnight (2 a.m.).

⛶ **Expand table**

| | |
|---|---|
| Type: | DateTime |
| Aliases: | scsqst |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SchedulerRandomizationTime

Specifies the randomization time for the scheduler.

⛶ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | srt |
| Position: | Named |
| Default value: | None |
| Required: | False |

| | |
|---|---|
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ServiceHealthReportInterval

This policy setting configures the time interval (in minutes) for the service health reports to be sent from endpoints. These are for Microsoft Defender Antivirus events 1150 and 1151. For more information, see Microsoft Defender Antivirus event IDs.

If you do not configure this setting, the default value will be applied. The default value is set at 60 minutes (one hour). If you configure this setting to 0, no service health reports will be sent. The maximum value allowed to be set is 14400 minutes (ten days).

⌗ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | shri |
| Accepted values: | 0-14400 |
| Position: | Named |
| Default value: | 60 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SevereThreatDefaultAction

Specifies which automatic remediation action to take for a severe level threat. The acceptable values for this parameter are:

- Quarantine
- Remove
- Ignore

⌗ **Expand table**

| | |
|---|---|
| Type: | ThreatAction |
| Aliases: | stdefac |
| Accepted values: | Clean, Quarantine, Remove, Allow, UserDefined, NoAction, Block |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SharedSignaturesPath

Specifies the shared signatures path.

⌗ **Expand table**

| | |
|---|---|
| Type: | String |

| Aliases: | ssp, SecurityIntelligenceLocation, ssl |
|---|---|
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-SignatureAuGracePeriod**

Specifies a grace period, in minutes, for the definition. If a definition successfully updates within this period, Windows Defender abandons any service initiated updates.

⛶ **Expand table**

| Type: | UInt32 |
|---|---|
| Aliases: | sigagp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-SignatureBlobFileSharesSources**

Specifies the file shares sources for signatures.

⛶ **Expand table**

| Type: | String |
|---|---|
| Aliases: | sigbfs |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-SignatureBlobUpdateInterval**

Specifies the signature update interval.

⛶ **Expand table**

| Type: | UInt32 |
|---|---|
| Aliases: | sigbui |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |

| Accept wildcard characters: | False |
|---|---|

### -SignatureDefinitionUpdateFileSharesSources

Specifies file-share sources for definition updates. Specify sources as a bracketed sequence of Universal Naming Convention (UNC) locations, separated by the pipeline symbol; for example, { \\Server01\Share01 | \\Server02\Share02 | \\Server03\Share03}. If you specify a value for this parameter, Windows Defender attempts to connect to the shares in the order that you specify. After Windows Defender updates a definition, it stops attempting to connect to shares on the list. If you do not specify a value for this parameter, the list is empty.

⛶ **Expand table**

| | |
|---|---|
| Type: | String |
| Aliases: | sigdufss |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SignatureDisableUpdateOnStartupWithoutEngine

Indicates whether to initiate definition updates even if no antimalware engine is present. If you specify a value of $True or do not specify a value, Windows Defender does not initiate definition updates on startup. If you specify a value of $False, and if no antimalware engine is present, Windows Defender initiates definition updates on startup.

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Aliases: | sigduoswo |
| Position: | Named |
| Default value: | False |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SignatureFallbackOrder

Specifies the order in which to contact different definition update sources. Specify the types of update sources in the order in which you want Windows Defender to contact them, enclosed in braces and separated by the pipeline symbol; for example, { InternalDefinitionUpdateServer | MicrosoftUpdateServer | MMPC }. The values that you can specify in the string are:

- InternalDefinitionUpdateServer
- MicrosoftUpdateServer
- MMPC
- FileShares

MMPC refers to Microsoft Malware Protection Center.

If you specify a value for this parameter, Windows Defender contacts the definition update sources in the specified order. After Windows Defender downloads definition updates from a source, it stops attempting to connect to other sources. If you do not specify a value for this parameter, Windows Defender contacts sources in the default order of { MicrosoftUpdateServer | MMPC }.

⛶ **Expand table**

| Type: | String |
|---|---|
| Aliases: | sfo |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SignatureFirstAuGracePeriod

Specifies a grace period, in minutes, for the definition. If a definition successfully updates within this period, Windows Defender abandons any service initiated updates. This parameter overrides the value of the **CheckForSignaturesBeforeRunningScan** parameter.

⛶ **Expand table**

| Type: | UInt32 |
|---|---|
| Aliases: | sigfagp |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SignatureScheduleDay

Specifies the day of the week on which to check for definition updates. Alternatively, specify everyday for a scheduled scan or never. The acceptable values for this parameter are:

- 0: Everyday
- 1: Sunday
- 2: Monday
- 3: Tuesday
- 4: Wednesday
- 5: Thursday
- 6: Friday
- 7: Saturday
- 8: Never

The default value is 8, never. If you specify a value of 8 or do not specify a value, Windows Defender checks for definition updates by using a default frequency.

⛶ **Expand table**

| Type: | Day |
|---|---|

| Aliases: | sigsd |
| --- | --- |
| Accepted values: | Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Never |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-SignatureScheduleTime**

Specifies the time of day, as the number of minutes after midnight, to check for definition updates. The time refers to the local time on the computer. If you do not specify a value for this parameter, Windows Defender checks for definition updates at the default time of 15 minutes before the scheduled scan time.

⌞⌝ **Expand table**

| Type: | DateTime |
| --- | --- |
| Aliases: | sigst |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-SignaturesUpdatesChannel**

Specifies when devices receive daily Microsoft Defender definition updates during the monthly gradual rollout.

Valid values are:

- NotConfigured. Devices stay up to date automatically during the gradual release cycle. This value is suitable for most devices.
- Broad. Devices are offered updates only after the gradual release cycle completes. This value is suggested for a broad set of devices in your production population, from 10 to 100 percent.
- Staged. Devices are offered updates after the monthly gradual release cycle. This value is suggested for a small, representative part of your production population, around 10 percent.

This parameter name will be updated to **DefinitionUpdatesChannel** in a future release.

⌞⌝ **Expand table**

| Type: | UpdatesChannelType |
| --- | --- |
| Aliases: | srelr |
| Position: | Named |
| Default value: | None |
| Required: | False |

| | |
|---|---|
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SignatureUpdateCatchupInterval

Specifies the number of days after which Windows Defender requires a catch-up definition update. If you do not specify a value for this parameter, Windows Defender requires a catch-up definition update after the default value of one day.

⛶ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | siguci |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SignatureUpdateInterval

Specifies the interval, in hours, at which to check for definition updates. The acceptable values for this parameter are: integers from 1 through 24. If you do not specify a value for this parameter, Windows Defender checks at the default interval. You can use this parameter instead of the **SignatureScheduleDay** parameter and **SignatureScheduleTime** parameter.

⛶ **Expand table**

| | |
|---|---|
| Type: | UInt32 |
| Aliases: | sigui |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -SubmitSamplesConsent

Specifies how Windows Defender checks for user consent for certain samples. If consent has previously been granted, Windows Defender submits the samples. Otherwise, if the **MAPSReporting** parameter does not have a value of Disabled, Windows Defender prompts the user for consent. The acceptable values for this parameter are:

- 0: Always prompt
- 1: Send safe samples automatically
- 2: Never send
- 3: Send all samples automatically

⛶ **Expand table**

| | |
|---|---|
| Type: | SubmitSamplesConsentType |

| | |
|---|---|
| Accepted values: | AlwaysPrompt, SendSafeSamples, NeverSend, SendAllSamples |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ThreatIDDefaultAction_Actions

Specifies an array of the actions to take for the IDs specified by using the
**ThreatIDDefaultAction_Ids** parameter. The acceptable values for this parameter are:

- 1: Clean
- 2: Quarantine
- 3: Remove
- 6: Allow
- 8: UserDefined
- 9: NoAction
- 10: Block

> ⓘ **Note**
>
> A value of 0 (NULL) applies an action based on the Security Intelligence Update (SIU).
> This is the default value.

⌄⌃ **Expand table**

| | |
|---|---|
| Type: | ThreatAction[] |
| Aliases: | tiddefaca |
| Accepted values: | Clean, Quarantine, Remove, Allow, UserDefined, NoAction, Block |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

### -ThreatIDDefaultAction_Ids

Specifies an array of threat IDs. This cmdlet modifies the default action for the threat IDs
that you specify.

⌄⌃ **Expand table**

| | |
|---|---|
| Type: | Int64[] |
| Aliases: | tiddefaci |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |

| | |
|---|---|
| Accept wildcard characters: | False |

**-ThrottleForScheduledScanOnly**

A CPU usage limit can be applied to scheduled scans only, or to scheduled and custom scans. The default value applies a CPU usage limit to scheduled scans only. The acceptable values for this parameter are:

- 1 (Default) - If you enable this setting, CPU throttling will apply only to scheduled scans.
- 0 - If you disable this setting, CPU throttling will apply to scheduled and custom scans.

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Position: | Named |
| Default value: | 1 |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-ThrottleLimit**

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then Windows PowerShell® calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit applies only to the current cmdlet, not to the session or to the computer.

⛶ **Expand table**

| | |
|---|---|
| Type: | Int32 |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

**-UILockdown**

Indicates whether to disable UI lockdown mode. If you specify a value of $True, Windows Defender disables UI lockdown mode. If you specify $False or do not specify a value, UI lockdown mode is enabled.

⛶ **Expand table**

| | |
|---|---|
| Type: | Boolean |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |

| | |
|---|---|
| Accept wildcard characters: | False |

**-UnknownThreatDefaultAction**

Specifies which automatic remediation action to take for an unknown level threat. The acceptable values for this parameter are:

- Quarantine
- Remove
- Ignore

⬚ Expand table

| | |
|---|---|
| Type: | ThreatAction |
| Aliases: | unktdefac |
| Accepted values: | Clean, Quarantine, Remove, Allow, UserDefined, NoAction, Block |
| Position: | Named |
| Default value: | None |
| Required: | False |
| Accept pipeline input: | False |
| Accept wildcard characters: | False |

## Related Links

- [Add-MpPreference](#)
- [Get-MpPreference](#)
- [Remove-MpPreference](#)

## Feedback

Was this page helpful?   👍 Yes   👎 No

Provide product feedback ⧉