Defender Antivirus Logging Definitions

Windows Event Logs

# Defender Antivirus Logs

There is one primary event log source for Microsoft Defender AV and most of its related features including Attack Surface Reduction rules, Controlled Folder Access, and Network Protection. Volume will be low if filtering out healthy state messages and intelligence update information.

## Defender Antivirus Events

### Microsoft-Windows-Windows Defender/Operational (Windows 10) Microsoft-Windows-Windows Defender/WHC (Legacy Operating Systems)

|  |
| --- |
| **Event ID: 1000**  Symbolic name: MALWAREPROTECTION\_SCAN\_STARTED  Message: An antimalware scan started.  Description:  Scan ID: <ID number of the relevant scan.>  Scan Type: <Scan type>, for example: Antivirus, Antispyware, Antimalware  Scan Parameters: <Scan parameters>, for example: Full scan, Quick scan, Customer scan  Scan Resources: <Resources (such as files/directories/BHO) that were scanned.>  User: <Domain>\<User> |
| **Event ID: 1001**  Symbolic name: MALWAREPROTECTION\_SCAN\_COMPLETED  Message: An antimalware scan finished.  Description:  Scan ID: <ID number of the relevant scan.>  Scan Type: <Scan type>, for example: Antivirus, Antispyware, Antimalware  Scan Parameters: <Scan parameters>, for example: Full scan, Quick scan, Customer scan  User: <Domain>\<User>  Scan Time: <The duration of a scan.> |
| **Event ID: 1002**  Symbolic name: MALWAREPROTECTION\_SCAN\_CANCELLED  Message: An antimalware scan was stopped before it finished.  Description:  Scan ID: <ID number of the relevant scan.>  Scan Type: <Scan type>, for example: Antivirus, Antispyware, Antimalware  Scan Parameters: <Scan parameters>, for example: Full scan, Quick scan, Customer scan  User: <Domain>\<User>  Scan Time: <The duration of a scan.> |
| **Event ID: 1003**  Symbolic name: MALWAREPROTECTION\_SCAN\_PAUSED  Message: An antimalware scan was paused.  Description:  Scan ID: <ID number of the relevant scan.>  Scan Type: <Scan type>, for example: Antivirus, Antispyware, Antimalware  Scan Parameters: <Scan parameters>, for example: Full scan, Quick scan, Customer scan  User: <Domain>\<User> |
| **Event ID: 1004**  Symbolic name: MALWAREPROTECTION\_SCAN\_RESUMED  Message: An antimalware scan was resumed.  Description:  Scan ID: <ID number of the relevant scan.>  Scan Type: <Scan type>, for example: Antivirus, Antispyware, Antimalware  Scan Parameters: <Scan parameters>, for example: Full scan, Quick scan, Customer scan  User: <Domain>\<User> |
| **Event ID: 1005**  Symbolic name: MALWAREPROTECTION\_SCAN\_FAILED  Message: An antimalware scan failed.  Description:  Scan ID: <ID number of the relevant scan.>  Scan Type: <Scan type>, for example: Antivirus, Antispyware, Antimalware  Scan Parameters: <Scan parameters>, for example: Full scan, Quick scan, Customer scan  User: <Domain>\<User>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  User action: The antivirus client encountered an error, and the current scan has stopped. The scan might fail due to a client-side issue. This event record includes the scan ID, type of scan (Microsoft Defender Antivirus, antispyware, antimalware), scan parameters, the user that started the scan, the error code, and a description of the error. To troubleshoot this event: Run the scan again. If it fails in the same way, go to the [Microsoft Support site](https://go.microsoft.com/fwlink/?LinkId=215163), enter the error number in the Search box to look for the error code. Contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 1006**  Symbolic name: MALWAREPROTECTION\_MALWARE\_DETECTED  Message: The antimalware engine found malware or other potentially unwanted software.  Description: For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Detection Origin: <Detection origin>, for example: Unknown, Local computer, Network share, Internet, Incoming traffic, Outgoing traffic  Detection Type: <Detection type>, for example: Heuristics, Generic, Concrete, Dynamic signature  Detection Source: <Detection source> for example: User: user initiated, System: system initiated, Real-time: real-time component initiated, IOAV: IE Downloads and Outlook Express Attachments initiated, NIS: Network inspection system, IEPROTECT: IE - IExtensionValidation; this protects against malicious webpage controls, Early Launch Antimalware (ELAM). This includes malware detected by the boot sequence, Remote attestation</ul>Antimalware Scan Interface (AMSI). Primarily used to protect scripts (PowerShell, VBS), though it can be invoked by third parties as well, UAC.  Status: <Status>  User: <Domain>\<User>  Process Name: <Process in the PID>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1007**  Symbolic name: MALWAREPROTECTION\_MALWARE\_ACTION\_TAKEN  Message: The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.  Description: Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information, see the following:  User: <Domain>\<User>  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Action: <Action>, for example: Clean: The resource was cleaned, Quarantine: The resource was quarantined, Remove: The resource was deleted, Allow: The resource was allowed to execute/exist, User defined: User-defined action that is normally one from this list of actions that the user has specified, No action: No action, Block: The resource was blocked from executing  Status: <Status>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1008**  Symbolic name: MALWAREPROTECTION\_MALWARE\_ACTION\_FAILED  Message: The antimalware platform attempted to perform an action to protect your system from malware or other potentially unwanted software, but the action failed.  Description: Microsoft Defender Antivirus has encountered an error when taking action on malware or other potentially unwanted software. For more information, see the following:  User: <Domain>\<User>  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Action: <Action>, for example: Clean: The resource was cleaned, Quarantine: The resource was quarantined, Remove: The resource was deleted, Allow: The resource was allowed to execute/exist, User defined: User-defined action that is normally one from this list of actions that the user has specified, No action: No action, Block: The resource was blocked from executing  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Status: <Status>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1009**  Symbolic name: MALWAREPROTECTION\_QUARANTINE\_RESTORE  Message: The antimalware platform restored an item from quarantine.  Description: Microsoft Defender Antivirus has restored an item from quarantine. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  User: <Domain>\<User>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1010**  Symbolic name: MALWAREPROTECTION\_QUARANTINE\_RESTORE\_FAILED  Message: The antimalware platform could not restore an item from quarantine.  Description: Microsoft Defender Antivirus has encountered an error trying to restore an item from quarantine. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  User: <Domain>\<User>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1011**  Symbolic name: MALWAREPROTECTION\_QUARANTINE\_DELETE  Message: The antimalware platform deleted an item from quarantine.  Description: Microsoft Defender Antivirus has deleted an item from quarantine. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  User: <Domain>\<User>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1012**  Symbolic name: MALWAREPROTECTION\_QUARANTINE\_DELETE\_FAILED  Message: The antimalware platform could not delete an item from quarantine.  Description: Microsoft Defender Antivirus has encountered an error trying to delete an item from quarantine. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  User: <Domain>\<User>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version> |
| **Event ID: 1013**  Symbolic name: MALWAREPROTECTION\_MALWARE\_HISTORY\_DELETE  Message: The antimalware platform deleted history of malware and other potentially unwanted software.  Description: Microsoft Defender Antivirus has removed history of malware and other potentially unwanted software.  Time: The time when the event occurred, for example when the history is purged. This parameter is not used in threat events so that there is no confusion regarding whether it is remediation time or infection time. For those, we specifically call them as Action Time or Detection Time.  User: <Domain>\<User> |
| **Event ID: 1014**  Symbolic name: MALWAREPROTECTION\_MALWARE\_HISTORY\_DELETE\_FAILED  Message: The antimalware platform could not delete history of malware and other potentially unwanted software.  Description: Microsoft Defender Antivirus has encountered an error trying to remove history of malware and other potentially unwanted software.  Time: The time when the event occurred, for example when the history is purged. This parameter is not used in threat events so that there is no confusion regarding whether it is remediation time or infection time. For those, we specifically call them as Action Time or Detection Time.  User: <Domain>\<User>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error. |
| **Event ID: 1015**  Symbolic name: MALWAREPROTECTION\_BEHAVIOR\_DETECTED  Message: The antimalware platform detected suspicious behavior.  Description: Microsoft Defender Antivirus has detected a suspicious behavior. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Detection Origin: <Detection origin>, for example: Unknown, Local computer, Network share, Internet, Incoming traffic, Outgoing traffic  Detection Type: <Detection type>, for example: Heuristics, Generic, Concrete, Dynamic signature  Detection Source: <Detection source> for example: User: user initiated, System: system initiated, Real-time: real-time component initiated, IOAV: IE Downloads and Outlook Express Attachments initiated, NIS: Network inspection system, IEPROTECT: IE - IExtensionValidation; this protects against malicious webpage controls, Early Launch Antimalware (ELAM). This includes malware detected by the boot sequence, Remote attestation</ul>Antimalware Scan Interface (AMSI). Primarily used to protect scripts (PowerShell, VBS), though it can be invoked by third parties as well, UAC.  Status: <Status>  User: <Domain>\<User>  Process Name: <Process in the PID>  Signature ID: Enumeration matching severity.  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version>  Fidelity Label:  Target File Name: <File name> Name of the file. |
| **Event ID: 1116**  Symbolic name: MALWAREPROTECTION\_STATE\_MALWARE\_DETECTED  Message: The antimalware platform detected malware or other potentially unwanted software.  Description: Microsoft Defender Antivirus has detected malware or other potentially unwanted software. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Detection Origin: <Detection origin>, for example: Unknown, Local computer, Network share, Internet, Incoming traffic, Outgoing traffic  Detection Type: <Detection type>, for example: Heuristics, Generic, Concrete, Dynamic signature  Detection Source: <Detection source> for example: User: user initiated, System: system initiated, Real-time: real-time component initiated, IOAV: IE Downloads and Outlook Express Attachments initiated, NIS: Network inspection system, IEPROTECT: IE - IExtensionValidation; this protects against malicious webpage controls, Early Launch Antimalware (ELAM). This includes malware detected by the boot sequence, Remote attestation, Antimalware Scan Interface (AMSI). Primarily used to protect scripts (PowerShell, VBS), though it can be invoked by third parties as well, UAC.  User: <Domain>\<User>  Process Name: <Process in the PID>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version>  User action: No action is required. Microsoft Defender Antivirus can suspend and take routine action on this threat. If you want to remove the threat manually, in the Microsoft Defender Antivirus interface, click Clean Computer. |
| **Event ID: 1117**  Symbolic name: MALWAREPROTECTION\_STATE\_MALWARE\_ACTION\_TAKEN  Message: The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.  Description: Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Detection Origin: <Detection origin>, for example: Unknown, Local computer, Network share, Internet, Incoming traffic, Outgoing traffic  Detection Type: <Detection type>, for example: Heuristics, Generic, Concrete, Dynamic signature  Detection Source: <Detection source> for example: User: user initiated, System: system initiated, Real-time: real-time component initiated, IOAV: IE Downloads and Outlook Express Attachments initiated, NIS: Network inspection system, IEPROTECT: IE - IExtensionValidation; this protects against malicious webpage controls, Early Launch Antimalware (ELAM). This includes malware detected by the boot sequence, Remote attestation</ul>Antimalware Scan Interface (AMSI). Primarily used to protect scripts (PowerShell, VBS), though it can be invoked by third parties as well, UAC.  User: <Domain>\<User>  Process Name: <Process in the PID>  Action: <Action>, for example: Clean: The resource was cleaned, Quarantine: The resource was quarantined, Remove: The resource was deleted, Allow: The resource was allowed to execute/exist, User defined: User-defined action that is normally one from this list of actions that the user has specified, No action: No action, Block: The resource was blocked from executing  Action Status: <Description of additional actions>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version>  NOTE: Whenever Microsoft Defender Antivirus, Microsoft Security Essentials, Malicious Software Removal Tool, or System Center Endpoint Protection detects a malware, it will restore the following system settings and services that the malware might have changed: Default Internet Explorer or Microsoft Edge setting, User Access Control settings, Chrome settings, Boot Control Data, Regedit and Task Manager registry settings, Windows Update, Background Intelligent Transfer Service, and Remote Procedure Call service, Windows Operating System files.  The above context applies to the following client and server versions: Windows Vista (Service Pack 1, or Service Pack 2), Windows 7 and later, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016  User action: No action is necessary. Microsoft Defender Antivirus removed or quarantined a threat. |
| **Event ID: 1118**  Symbolic name: MALWAREPROTECTION\_STATE\_MALWARE\_ACTION\_FAILED  Message: The antimalware platform attempted to perform an action to protect your system from malware or other potentially unwanted software, but the action failed.  Description: Microsoft Defender Antivirus has encountered a non-critical error when taking action on malware or other potentially unwanted software. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Detection Origin: <Detection origin>, for example: Unknown, Local computer, Network share, Internet, Incoming traffic, Outgoing traffic  Detection Type: <Detection type>, for example: Heuristics, Generic, Concrete, Dynamic signature  Detection Source: <Detection source> for example: User: user initiated, System: system initiated, Real-time: real-time component initiated, IOAV: IE Downloads and Outlook Express Attachments initiated, NIS: Network inspection system, IEPROTECT: IE - IExtensionValidation; this protects against malicious webpage controls, Early Launch Antimalware (ELAM). This includes malware detected by the boot sequence, Remote attestation</ul>Antimalware Scan Interface (AMSI). Primarily used to protect scripts (PowerShell, VBS), though it can be invoked by third parties as well, UAC.  User: <Domain>\<User>  Process Name: <Process in the PID>  Action: <Action>, for example: Clean: The resource was cleaned, Quarantine: The resource was quarantined, Remove: The resource was deleted, Allow: The resource was allowed to execute/exist, User defined: User-defined action that is normally one from this list of actions that the user has specified, No action: No action, Block: The resource was blocked from executing  Action Status: <Description of additional actions>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version>  User action: No action is necessary. Microsoft Defender Antivirus failed to complete a task related to the malware remediation. This is not a critical failure. |
| **Event ID: 1119**  Symbolic name: MALWAREPROTECTION\_STATE\_MALWARE\_ACTION\_CRITICALLY\_FAILED  Message: The antimalware platform encountered a critical error when trying to take action on malware or other potentially unwanted software. There are more details in the event message.  Description: Microsoft Defender Antivirus has encountered a critical error when taking action on malware or other potentially unwanted software. For more information, see the following:  Name: <Threat name>  ID: <Threat ID>  Severity: <Severity>, for example: Low, Moderate, High, Severe  Category: <Category description>, for example, any threat or malware type.  Path: <File path>  Detection Origin: <Detection origin>, for example: Unknown, Local computer, Network share, Internet, Incoming traffic, Outgoing traffic  Detection Type: <Detection type>, for example: Heuristics, Generic, Concrete, Dynamic signature  Detection Source: <Detection source> for example: User: user initiated, System: system initiated, Real-time: real-time component initiated, IOAV: IE Downloads and Outlook Express Attachments initiated, NIS: Network inspection system, IEPROTECT: IE - IExtensionValidation; this protects against malicious webpage controls, Early Launch Antimalware (ELAM). This includes malware detected by the boot sequence, Remote attestation</ul>Antimalware Scan Interface (AMSI). Primarily used to protect scripts (PowerShell, VBS), though it can be invoked by third parties as well, UAC.  User: <Domain>\<User>  Process Name: <Process in the PID>  Action: <Action>, for example: Clean: The resource was cleaned, Quarantine: The resource was quarantined, Remove: The resource was deleted, Allow: The resource was allowed to execute/exist, User defined: User-defined action that is normally one from this list of actions that the user has specified, No action: No action, Block: The resource was blocked from executing  Action Status: <Description of additional actions>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version>  User action: The Microsoft Defender Antivirus client encountered this error due to critical issues. The endpoint might not be protected. Review the error description then follow the relevant User action steps below.  RemoveUpdate the definitions then verify that the removal was successful.  CleanUpdate the definitions then verify that the remediation was successful.  QuarantineUpdate the definitions and verify that the user has permission to access the necessary resources.  AllowVerify that the user has permission to access the necessary resources.  If this event persists: Run the scan again. If it fails in the same way, go to the [Microsoft Support site](https://go.microsoft.com/fwlink/?LinkId=215163), enter the error number in the Search box to look for the error code. Contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 1120**  Symbolic name: MALWAREPROTECTION\_THREAT\_HASH  Message: Microsoft Defender Antivirus has deduced the hashes for a threat resource.  Description: Microsoft Defender Antivirus client is up and running in a healthy state.  Current Platform Version: <Current platform version>  Threat Resource Path: <Path>  Hashes: <Hashes>  Note: This event will only be logged if the following policy is set: ThreatFileHashLogging unsigned |
| **Event ID: 1127**  Symbolic name: MALWAREPROTECTION\_FOLDER\_GUARD\_SECTOR\_BLOCK  Message: Controlled Folder Access (CFA) blocked an untrusted process from making changes to the memory.  Description: Controlled Folder Access has blocked an untrusted process from potentially modifying disk sectors. For more information about the event record, see the following:  EventID: <EventID>, for example: 1127  Version: <Version>, for example: 0  Level: <Level>, for example: win:Warning  TimeCreated: <SystemTime>, time when the event was created  EventRecordID: <EventRecordID>, index number of the event in the event log  Execution ProcessID: <Execution ProcessID>, process that generated the event  Channel: <Event channel>, for example: Microsoft-Windows-Windows Defender/Operational  Computer: <Computer name>  Security UserID: <Security UserID>  Product Name: <Product Name>, for example: Microsoft Defender Antivirus  Product Version: <Product Version>  Detection Time: <Detection Time>, time when CFA blocked an untrusted process  User: <Domain>\<User>  Path: <Device name>, name of the device or disk that an untrusted process accessed for modification  Process Name: <Process path>, the process path name that CFA blocked from accessing the device or disk for modification  Security Intelligence Version: <Security intelligence version>  Engine Version: <Antimalware Engine version>  User action: The user can add the blocked process to the Allowed Process list for CFA, using Powershell or Windows Security Center. |
| **Event ID: 1150**  Symbolic name: MALWAREPROTECTION\_SERVICE\_HEALTHY  Message: If your antimalware platform reports status to a monitoring platform, this event indicates that the antimalware platform is running and in a healthy state.  Description: Microsoft Defender Antivirus client is up and running in a healthy state.  Platform Version: <Current platform version>  Signature Version: <Definition version>  Engine Version: <Antimalware Engine version>  User action: No action is necessary. The Microsoft Defender Antivirus client is in a healthy state. This event is reported on an hourly basis. |
| **Event ID: 1151**  Symbolic name: MALWAREPROTECTION\_SERVICE\_HEALTH\_REPORT  Message: Endpoint Protection client health report (time in UTC)  Description: Antivirus client health report.  Platform Version: <Current platform version>  Engine Version: <Antimalware Engine version>  Network Realtime Inspection engine version: <Network Realtime Inspection engine version>  Antivirus signature version: <Antivirus signature version>  Antispyware signature version: <Antispyware signature version>  Network Realtime Inspection signature version: <Network Realtime Inspection signature version>  RTP state: <Realtime protection state> (Enabled or Disabled)  OA state: <On Access state> (Enabled or Disabled)  IOAV state: <IE Downloads and Outlook Express Attachments state> (Enabled or Disabled)  BM state: <Behavior Monitoring state> (Enabled or Disabled)  Antivirus signature age: <Antivirus signature age> (in days)  Antispyware signature age: <Antispyware signature age> (in days)  Last quick scan age: <Last quick scan age> (in days)  Last full scan age: <Last full scan age> (in days)  Antivirus signature creation time: ?<Antivirus signature creation time>  Antispyware signature creation time: ?<Antispyware signature creation time>  Last quick scan start time: ?<Last quick scan start time>  Last quick scan end time: ?<Last quick scan end time>  Last quick scan source: <Last quick scan source> (0 = scan didn't run, 1 = user initiated, 2 = system initiated)  Last full scan start time: ?<Last full scan start time>  Last full scan end time: ?<Last full scan end time>  Last full scan source: <Last full scan source> (0 = scan didn't run, 1 = user initiated, 2 = system initiated)  Product status: For internal troubleshooting |
| **Event ID: 2000**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_UPDATED  Message: The antimalware definitions updated successfully.  Description: Antivirus signature version has been updated.  Current Signature Version: <Current signature version>  Previous Signature Version: <Previous signature version>  Signature Type: <Signature type>, for example: Antivirus, Antispyware, Antimalware, Network Inspection System  Update Type: <Update type>, either Full or Delta.  User: <Domain>\<User>  Current Engine Version: <Current engine version>  Previous Engine Version: <Previous engine version>  User action: No action is necessary. The Microsoft Defender Antivirus client is in a healthy state. This event is reported when signatures are successfully updated. |
| **Event ID: 2001**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_UPDATE\_FAILED  Message: The security intelligence update failed.  Description: Microsoft Defender Antivirus has encountered an error trying to update signatures.  New security intelligence version: <New version number>  Previous security intelligence version: <Previous version>  Update Source: <Update source>, for example: Security intelligence update folder, Internal security intelligence update server, Microsoft Update Server, File share, Microsoft Malware Protection Center (MMPC)  Update Stage: <Update stage>, for example: Search, Download, Install  Source Path: File share name for Universal Naming Convention (UNC), server name for Windows Server Update Services (WSUS)/Microsoft Update/ADL.  Signature Type: <Signature type>, for example: Antivirus, Antispyware, Antimalware, Network Inspection System  Update Type: <Update type>, either Full or Delta.  User: <Domain>\<User>  Current Engine Version: <Current engine version>  Previous Engine Version: <Previous engine version>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  User action: This error occurs when there is a problem updating definitions. To troubleshoot this event: [Update definitions](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide) and force a rescan directly on the endpoint. Review the entries in the %Windir%\WindowsUpdate.log file for more information about this error. Contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 2002**  Symbolic name: MALWAREPROTECTION\_ENGINE\_UPDATED  Message: The antimalware engine updated successfully.  Description: Microsoft Defender Antivirus engine version has been updated.  Current Engine Version: <Current engine version>  Previous Engine Version: <Previous engine version>  Engine Type: <Engine type>, either antimalware engine or Network Inspection System engine.  User: <Domain>\<User>  User action: No action is necessary. The Microsoft Defender Antivirus client is in a healthy state. This event is reported when the antimalware engine is successfully updated. |
| **Event ID: 2003**  Symbolic name: MALWAREPROTECTION\_ENGINE\_UPDATE\_FAILED  Message: The antimalware engine update failed.  Description: Microsoft Defender Antivirus has encountered an error trying to update the engine.  New Engine Version:  Previous Engine Version: <Previous engine version>  Engine Type: <Engine type>, either antimalware engine or Network Inspection System engine.  User: <Domain>\<User>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  User action: The Microsoft Defender Antivirus client update failed. This event occurs when the client fails to update itself. This event is usually due to an interruption in network connectivity during an update. To troubleshoot this event: [Update definitions](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide) and force a rescan directly on the endpoint. Contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 2004**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_REVERSION  Message: There was a problem loading antimalware definitions. The antimalware engine will attempt to load the last-known good set of definitions.  Description: Microsoft Defender Antivirus has encountered an error trying to load signatures and will attempt reverting back to a known-good set of signatures.  Signatures Attempted:  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Signature Version: <Definition version>  Engine Version: <Antimalware engine version>  User action: The Microsoft Defender Antivirus client attempted to download and install the latest definitions file and failed. This error can occur when the client encounters an error while trying to load the definitions, or if the file is corrupt. Microsoft Defender Antivirus will attempt to revert back to a known-good set of definitions. To troubleshoot this event: Restart the computer and try again. Download the latest definitions from the [Microsoft Security Intelligence site](https://aka.ms/wdsi).  Note: The size of the definitions file downloaded from the site can exceed 60 MB and should not be used as a long-term solution for updating definitions. Contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 2005**  Symbolic name: MALWAREPROTECTION\_ENGINE\_UPDATE\_PLATFORMOUTOFDATE  Message: The antimalware engine failed to load because the antimalware platform is out of date. The antimalware platform will load the last-known good antimalware engine and attempt to update.  Description: Microsoft Defender Antivirus could not load antimalware engine because current platform version is not supported. Microsoft Defender Antivirus will revert back to the last known-good engine and a platform update will be attempted.  Current Platform Version: <Current platform version> |
| **Event ID: 2006**  Symbolic name: MALWAREPROTECTION\_PLATFORM\_UPDATE\_FAILED  Message: The platform update failed.  Description: Microsoft Defender Antivirus has encountered an error trying to update the platform.  Current Platform Version: <Current platform version>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error. |
| **Event ID: 2007**  Symbolic name: MALWAREPROTECTION\_PLATFORM\_ALMOSTOUTOFDATE  Message: The platform will soon be out of date. Download the latest platform to maintain up-to-date protection.  Description: Microsoft Defender Antivirus will soon require a newer platform version to support future versions of the antimalware engine. Download the latest Microsoft Defender Antivirus platform to maintain the best level of protection available.  Current Platform Version: <Current platform version> |
| **Event ID: 2010**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_FASTPATH\_UPDATED  Message: The antimalware engine used the Dynamic Signature Service to get additional definitions.  Description: Microsoft Defender Antivirus used Dynamic Signature Service to retrieve additional signatures to help protect your machine.  Current Signature Version: <Current signature version>  Signature Type: <Signature type>, for example: Antivirus, Antispyware, Antimalware, Network Inspection System  Current Engine Version: <Current engine version>  Dynamic Signature Type: <Dynamic signature type>, for example: Version, Timestamp, No limit, Duration  Persistence Path: <Path>  Dynamic Signature Version: <Version number>  Dynamic Signature Compilation Timestamp: <Timestamp>  Persistence Limit Type: <Persistence limit type>, for example: VDM version, Timestamp, No limit  Persistence Limit: Persistence limit of the fastpath signature. |
| **Event ID: 2011**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_FASTPATH\_DELETED  Message: The Dynamic Signature Service deleted the out-of-date dynamic definitions.  Description: Microsoft Defender Antivirus used Dynamic Signature Service to discard obsolete signatures.  Current Signature Version: <Current signature version>  Signature Type: <Signature type>, for example: Antivirus, Antispyware, Antimalware, Network Inspection System  Current Engine Version: <Current engine version>  Dynamic Signature Type: <Dynamic signature type>, for example: Version, Timestamp, No limit, Duration  Persistence Path: <Path>  Dynamic Signature Version: <Version number>  Dynamic Signature Compilation Timestamp: <Timestamp>  Removal Reason:  Persistence Limit Type: <Persistence limit type>, for example: VDM version, Timestamp, No limit  Persistence Limit: Persistence limit of the fastpath signature.  User action: No action is necessary. The Microsoft Defender Antivirus client is in a healthy state. This event is reported when the Dynamic Signature Service successfully deletes out-of-date dynamic definitions. |
| **Event ID: 2012**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_FASTPATH\_UPDATE\_FAILED  Message: The antimalware engine encountered an error when trying to use the Dynamic Signature Service.  Description: Microsoft Defender Antivirus has encountered an error trying to use Dynamic Signature Service.  Current Signature Version: <Current signature version>  Signature Type: <Signature type>, for example: Antivirus, Antispyware, Antimalware, Network Inspection System  Current Engine Version: <Current engine version>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Dynamic Signature Type: <Dynamic signature type>, for example: Version, Timestamp, No limit, Duration  Persistence Path: <Path>  Dynamic Signature Version: <Version number>  Dynamic Signature Compilation Timestamp: <Timestamp>  Persistence Limit Type: <Persistence limit type>, for example: VDM version, Timestamp, No limit  Persistence Limit: Persistence limit of the fastpath signature.  User action: Check your Internet connectivity settings. |
| **Event ID: 2013**  Symbolic name: MALWAREPROTECTION\_SIGNATURE\_FASTPATH\_DELETED\_ALL  Message: The Dynamic Signature Service deleted all dynamic definitions.  Description: Microsoft Defender Antivirus discarded all Dynamic Signature Service signatures.  Current Signature Version: <Current signature version> |
| **Event ID: 2020**  Symbolic name: MALWAREPROTECTION\_CLOUD\_CLEAN\_RESTORE\_FILE\_DOWNLOADED  Message: The antimalware engine downloaded a clean file.  Description: Microsoft Defender Antivirus downloaded a clean file.  Filename: <File name> Name of the file.  Current Signature Version: <Current signature version>  Current Engine Version: <Current engine version> |
| **Event ID: 2021**  Symbolic name: MALWAREPROTECTION\_CLOUD\_CLEAN\_RESTORE\_FILE\_DOWNLOAD\_FAILED  Message: The antimalware engine failed to download a clean file.  Description: Microsoft Defender Antivirus has encountered an error trying to download a clean file.  Filename: <File name> Name of the file.  Current Signature Version: <Current signature version>  Current Engine Version: <Current engine version>  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  User action: Check your Internet connectivity settings. The Microsoft Defender Antivirus client encountered an error when using the Dynamic Signature Service to download the latest definitions to a specific threat. This error is likely caused by a network connectivity issue. |
| **Event ID: 2030**  Symbolic name: MALWAREPROTECTION\_OFFLINE\_SCAN\_INSTALLED  Message: The antimalware engine was downloaded and is configured to run offline on the next system restart.  Description: Microsoft Defender Antivirus downloaded and configured offline antivirus to run on the next reboot. |
| **Event ID: 2031**  Symbolic name: MALWAREPROTECTION\_OFFLINE\_SCAN\_INSTALL\_FAILED  Message: The antimalware engine was unable to download and configure an offline scan.  Description: Microsoft Defender Antivirus has encountered an error trying to download and configure offline antivirus.  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error. |
| **Event ID: 2040**  Symbolic name: MALWAREPROTECTION\_OS\_EXPIRING  Message: Antimalware support for this operating system version will soon end.  Description: The support for your operating system will expire shortly. Running Microsoft Defender Antivirus on an out of support operating system is not an adequate solution to protect against threats. |
| **Event ID: 2041**  Symbolic name: MALWAREPROTECTION\_OS\_EOL  Message: Antimalware support for this operating system has ended. You must upgrade the operating system for continued support.  Description: The support for your operating system has expired. Running Microsoft Defender Antivirus on an out of support operating system is not an adequate solution to protect against threats. |
| **Event ID: 2042**  Symbolic name: MALWAREPROTECTION\_PROTECTION\_EOL  Message: The antimalware engine no longer supports this operating system, and is no longer protecting your system from malware.  Description: The support for your operating system has expired. Microsoft Defender Antivirus is no longer supported on your operating system, has stopped functioning, and is not protecting against malware threats. |
| **Event ID: 3002**  Symbolic name: MALWAREPROTECTION\_RTP\_FEATURE\_FAILURE  Message: Real-time protection encountered an error and failed.  Description: Microsoft Defender Antivirus Real-Time Protection feature has encountered an error and failed.  Feature: <Feature>, for example: On Access, Internet Explorer downloads and Microsoft Outlook Express attachments, Behavior monitoring, Network Inspection System  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error.  Reason: The reason Microsoft Defender Antivirus real-time protection has restarted a feature.  User action: You should restart the system then run a full scan because it's possible the system was not protected for some time. The Microsoft Defender Antivirus client's real-time protection feature encountered an error because one of the services failed to start. If it is followed by a 3007 event ID, the failure was temporary and the antimalware client recovered from the failure. |
| **Event ID: 3007**  Symbolic name: MALWAREPROTECTION\_RTP\_FEATURE\_RECOVERED  Message: Real-time protection recovered from a failure. We recommend running a full system scan when you see this error.  Description: Microsoft Defender Antivirus Real-time Protection has restarted a feature. It is recommended that you run a full system scan to detect any items that may have been missed while this agent was down.  Feature: <Feature>, for example: On Access, IE downloads and Outlook Express attachments, Behavior monitoring, Network Inspection System  Reason: The reason Microsoft Defender Antivirus real-time protection has restarted a feature.  User action: The real-time protection feature has restarted. If this event happens again, contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 5000**  Symbolic name: MALWAREPROTECTION\_RTP\_ENABLED  Message: Real-time protection is enabled.  Description: Microsoft Defender Antivirus real-time protection scanning for malware and other potentially unwanted software was enabled. |
| **Event ID: 5001**  Symbolic name: MALWAREPROTECTION\_RTP\_DISABLED  Message: Real-time protection is disabled.  Description: Microsoft Defender Antivirus real-time protection scanning for malware and other potentially unwanted software was disabled. |
| **Event ID: 5004**  Symbolic name: MALWAREPROTECTION\_RTP\_FEATURE\_CONFIGURED  Message: The real-time protection configuration changed.  Description: Microsoft Defender Antivirus real-time protection feature configuration has changed.  Feature: <Feature>, for example: On Access, IE downloads and Outlook Express attachments, Behavior monitoring, Network Inspection System  Configuration: |
| **Event ID: 5007**  Symbolic name: MALWAREPROTECTION\_CONFIG\_CHANGED  Message: The antimalware platform configuration changed.  Description: Microsoft Defender Antivirus configuration has changed. If this is an unexpected event, you should review the settings as this may be the result of malware.  Old value: <Old value number>  Old antivirus configuration value.  New value: <New value number>  New antivirus configuration value. |
| **Event ID: 5008**  Symbolic name: MALWAREPROTECTION\_ENGINE\_FAILURE  Message: The antimalware engine encountered an error and failed.  Description: Microsoft Defender Antivirus engine has been terminated due to an unexpected error.  Failure Type: <Failure type>, for example: Crash or Hang  Exception Code: <Error code>  Resource: <Resource>  User action: To troubleshoot this event: Try to restart the service. For antimalware, antivirus and spyware, at an elevated command prompt, type net stop msmpsvc, and then type net start msmpsvc to restart the antimalware engine. For the Network Inspection System, at an elevated command prompt, type net start nissrv, and then type net start nissrv to restart the Network Inspection System engine by using the NiSSRV.exe file. If it fails in the same way, look up the error code by accessing the [Microsoft Support Site](https://go.microsoft.com/fwlink/?LinkId=215163) and entering the error number in the Search box, and contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491).  User action: The Microsoft Defender Antivirus client engine stopped due to an unexpected error.  To troubleshoot this event: Run the scan again. If it fails in the same way, go to the [Microsoft Support site](https://go.microsoft.com/fwlink/?LinkId=215163), enter the error number in the Search box to look for the error code. Contact [Microsoft Technical Support](https://go.microsoft.com/fwlink/?LinkId=215491). |
| **Event ID: 5009**  Symbolic name: MALWAREPROTECTION\_ANTISPYWARE\_ENABLED  Message: Scanning for malware and other potentially unwanted software is enabled.  Description: Microsoft Defender Antivirus scanning for malware and other potentially unwanted software has been enabled. |
| **Event ID: 5010**  Symbolic name: MALWAREPROTECTION\_ANTISPYWARE\_DISABLED  Message: Scanning for malware and other potentially unwanted software is disabled.  Description: Microsoft Defender Antivirus scanning for malware and other potentially unwanted software is disabled. |
| **Event ID: 5011**  Symbolic name: MALWAREPROTECTION\_ANTIVIRUS\_ENABLED  Message: Scanning for viruses is enabled.  Description: Microsoft Defender Antivirus scanning for viruses has been enabled. |
| **Event ID: 5012**  Symbolic name: MALWAREPROTECTION\_ANTIVIRUS\_DISABLED  Message: Scanning for viruses is disabled.  Description: Microsoft Defender Antivirus scanning for viruses is disabled. |
| **Event ID: 5100**  Symbolic name: MALWAREPROTECTION\_EXPIRATION\_WARNING\_STATE  Message: The antimalware platform will expire soon.  Description: Microsoft Defender Antivirus has entered a grace period and will soon expire. After expiration, this program will disable protection against viruses, spyware, and other potentially unwanted software.  Expiration Reason: The reason Microsoft Defender Antivirus will expire.  Expiration Date: The date Microsoft Defender Antivirus will expire. |
| **Event ID: 5101**  Symbolic name: MALWAREPROTECTION\_DISABLED\_EXPIRED\_STATE  Message: The antimalware platform is expired.  Description: Microsoft Defender Antivirus grace period has expired. Protection against viruses, spyware, and other potentially unwanted software is disabled.  Expiration Reason:  Expiration Date:  Error Code: <Error code> Result code associated with threat status. Standard HRESULT values.  Error Description: <Error description> Description of the error. |

## Attack Surface Reduction Event ID’s

|  |
| --- |
| **Event ID: 5007**  Description: Microsoft Defender Antivirus configuration has changed. If this is an unexpected event, you should review the settings as this may be the result of malware.  Old value: <Old value number>  Old antivirus configuration value.  New value: <New value number>  New antivirus configuration value. |
| **Event ID: 1121**  Description:  Detection time: <Date in UTC>  User: <Domain>\<User>  Path: <Path>  Process Name: <Full Process Path>  Security intelligence Version: <Security intelligence Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |
| **Event ID: 1122**  Description: <Process Name> has been blocked from modifying <Path> by Controlled Folder Access.  Detection time: <Date in UTC>  User: <Domain>\<User>  Path: <Path>  Process Name: <Full Process Path>  Security intelligence Version: <Security intelligence Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |

## Controlled Folder Access Event ID’s

### Microsoft-Windows-Windows Defender/Operational (Windows 10) Microsoft-Windows-Windows Defender/WHC (Legacy Operating Systems)

|  |
| --- |
| **Event ID: 5007**  Description: Microsoft Defender Antivirus configuration has changed. If this is an unexpected event, you should review the settings as this may be the result of malware.  Old value: <Old value number>  Old antivirus configuration value.  New value: <New value number>  New antivirus configuration value. |
| **Event ID: 1123**  Description:  Detection time: <Date in UTC>  User: <Domain>\<User>  Path: <Path>  Process Name: <Full Process Path>  Security intelligence Version: <Security intelligence Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |
| **Event ID: 1124**  Description: <Process Name> has been blocked from modifying <Path> by Controlled Folder Access.  Detection time: <Date in UTC>  User: <Domain>\<User>  Path: <Path>  Process Name: <Full Process Path>  Security intelligence Version: <Security intelligence Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |

## Network Protection Logs

### Microsoft-Windows-Windows Defender/Operational (Windows 10) Microsoft-Windows-Windows Defender/WHC (Legacy Operating Systems)

|  |
| --- |
| **Event ID: 5007**  Description: Microsoft Defender Antivirus configuration has changed. If this is an unexpected event, you should review the settings as this may be the result of malware.  Old value: <Old value number>  Old antivirus configuration value.  New value: <New value number>  New antivirus configuration value. |
| **Event ID: 1123**  Description:  Detection time: <Date in UTC>  User: <Domain>\<User>  Path: <Path>  Process Name: <Full Process Path>  Security intelligence Version: <Security intelligence Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |
| **Event ID: 1124**  Description: <Process Name> has been blocked from modifying <Path> by Controlled Folder Access.  Detection time: <Date in UTC>  User: <Domain>\<User>  Path: <Path>  Process Name: <Full Process Path>  Security intelligence Version: <Security intelligence Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |

## Defender for Endpoint Event ID’s?

|  |
| --- |
| **Event ID: 1134**  Description: Microsoft Defender Antivirus has audited an operation. For more information please contact your IT administrator.  Policy Version: <Policy Versions>  Policy Rule ID: <Policy Rule ID's>  Enforcement Level: Audit  Audit Reason: 0  Timestamp: <Timestamp>  Action Type: CopyToClipboard  Process: <Source Process>  Source: <Source File Paths>  Target: <Target Process>  Session ID: <Session ID>  User SID: <User SID>  Signature Version: <Signature Version>  Engine Version: <Engine Version>  Product Version: <Product Version> |

# Exploit Protection Logs

There are several sources for Exploit Protection (which replaced and improved on EMET). Volume is highly dependent on mitigations enabled and application usage, but it will still be relatively low. There will be a lot of duplicate data as the same applications will generate the same events.

### Microsoft-Windows-Security-Mitigations/Kernel Mode Microsoft-Windows-Security-Mitigations/UserMode

|  |
| --- |
| **Event ID: 1**  Name: Arbitrary Code Guard (ACG) Auditing  Message: Process '%2' (PID %5) would have been blocked from generating dynamic code. Description: ACG audit |
| **Event ID: 2** Name: Arbitrary Code Guard (ACG) Enforcement  Message: Process '%2' (PID %5) was blocked from generating dynamic code. Description: ACG enforce |
| **Event ID: 3** Name: Audit: Child Process Creation  Message: Process '%2' (PID %5) would have been blocked from creating a child process '%14' with command line '%16'.  Description: Don't allow child processes audit |
| **Event ID: 4**  Name: Enforce: Prevent Child Process Creation  Message: Process '%2' (PID %5) was blocked from creating a child process '%14' with command line '%16'. Description: Don't allow child processes block |
| **Event ID: 5** Name: Audit: Low integrity image load  Message: Process '%2' (PID %5) would have been blocked from loading the low-integrity binary '%14'. Description: Block low integrity images audit |
| **Event ID: 6**  Name: Enforce: Block low integrity image load  Message: Process '%2' (PID %5) was blocked from loading the low-integrity binary '%14'. Description: Block low integrity images block |
| **Event ID: 7** Name: Audit: Log Remote Image Loads  Message: Process '%2' (PID %5) would have been blocking from loading a binary from a remote share. Description: Block remote images audit |
| **Event ID: 8** Name: Enforce: Block Remote Image Loads  Message: Process '%2' (PID %5) was blocked from loading a binary from a remote share. Description: Block remote images block |
| **Event ID: 9** Name: Audit: Log Win32K System Call Table Use  Message: Process '%2' (PID %5) would have been blocked from making system calls to Win32k.sys. Description: Disable win32k system calls audit |
| **Event ID: 10** Name: Enforce: Prevent Win32K System Call Table Use  Message: Process '%2' (PID %5) was blocked from making system calls to Win32k.sys. Description: Disable win32k system calls block |
| **Event ID: 11** Name: Audit: A non-Microsoft-signed binary would have been loaded.  Message: Process '%2' (PID %5) would have been blocked from loading the non-Microsoft-signed binary '%16'. Description: Code integrity guard audit |
| **Event ID: 12** Name: Enforce: A non-Microsoft-signed binary was prevented from loading.  Message: Process '%2' (PID %5) was blocked from loading the non-Microsoft-signed binary '%16'. Description: Code integrity guard block |
| **Event ID: 13** Name: EAF mitigation audited  Message: Process '%2' (PID %3) would have been blocked from accessing the Export Address Table for module '%8'. Description: EAF audit |
| **Event ID: 14** Name: EAF mitigation enforced  Message: Process '%2' (PID %3) was blocked from accessing the Export Address Table for module '%8'. Description: EAF enforce |
| **Event ID: 15** Name: EAF+ mitigation audited  Message: Process '%2' (PID %3) would have been blocked from accessing the Export Address Table for module '%8'.  Description: EAF+ audit |
| **Event ID: 16** Name: EAF+ mitigation enforced  Message: Process '%2' (PID %3) was blocked from accessing the Export Address Table for module '%8'.  Description: EAF+ enforce |
| **Event ID: 17** Name: IAF mitigation audited  Message: Process '%2' (PID %3) would have been blocked from accessing the Import Address Table for API '%10'.  Description: IAF audit |
| **Event ID: 18** Name: IAF mitigation enforced  Message: Process '%2' (PID %3) was blocked from accessing the Import Address Table for API '%10'.  Description: IAF enforce |
| **Event ID: 19** Name: ROP mitigation audited: Stack Pivot  Message: Process '%2' (PID %3) would have been blocked from calling the API '%4' due to return-oriented programming (ROP) exploit indications.  Description: ROP StackPivot audit |
| **Event ID: 20** Name: ROP mitigation enforced: Stack Pivot  Message: Process '%2' (PID %3) was blocked from calling the API '%4' due to return-oriented programming (ROP) exploit indications.  Description: ROP StackPivot enforce |
| **Event ID 21** Name: ROP mitigation audited: Caller Checks  Message: Process '%2' (PID %3) would have been blocked from calling the API '%4' due to return-oriented programming (ROP) exploit indications.  Description: ROP CallerCheck audit |
| **Event ID: 22** Name: ROP mitigation enforced: Caller Checks  Message: Process '%2' (PID %3) was blocked from calling the API '%4' due to return-oriented programming (ROP) exploit indications.  Description: ROP CallerCheck enforce |
| **Event ID: 23** Name: ROP mitigation audited: Simulate Execution Flow  Message: Process '%2' (PID %3) would have been blocked from calling the API '%4' due to return-oriented programming (ROP) exploit indications.  Description: ROP SimExec audit |
| **Event ID: 24** Name: ROP mitigation enforced: Simulate Execution Flow  Message: Process '%2' (PID %3) was blocked from calling the API '%4' due to return-oriented programming (ROP) exploit indications.  Description: ROP SimExec enforce |

# Defender Application Control Logs

There are two sources for Defender Application Control logs - CodeIntegrity and AppLocker. Volume will be similar to Application or System logs but will depend on configuration. There will be a lot of duplicate data since the same applications will generate the same events, so filtering out unnecessary and duplicate events will significantly reduce ingested data.

## Microsoft-Windows-CodeIntegrity/Operational

|  |
| --- |
| **Event ID: 3001**  Description: An unsigned driver was attempted to load on the system. |
| **Event ID: 3002**  Description: Code Integrity could not verify the boot image as the page hash could not be found. |
| **Event ID: 3004**  Description: Code Integrity could not verify the file as the page hash could not be found. |
| **Event ID: 3010**  Description: The catalog containing the signature for the file under validation is invalid. |
| **Event ID: 3011**  Description: Code Integrity finished loading the signature catalog. |
| **Event ID: 3012**  Description: Code Integrity started loading the signature catalog. |
| **Event ID: 3023**  Description: The driver file under validation did not meet the requirements to pass the application control policy. |
| **Event ID: 3024**  Description: Windows application control was unable to refresh the boot catalog file. |
| **Event ID: 3026**  Description: The catalog loaded is signed by a signing certificate that has been revoked by Microsoft and/or the certificate issuing authority. |
| **Event ID: 3033**  Description: The file under validation did not meet the requirements to pass the application control policy. |
| **Event ID: 3034**  Description: The file under validation would not meet the requirements to pass the application control policy if the policy was enforced. The file was allowed since the policy is in audit mode. |
| **Event ID: 3036**  Description: The signed file under validation is signed by a code signing certificate that has been revoked by Microsoft or the certificate issuing authority. |
| **Event ID: 3064**  Description: If the policy was enforced, a user mode DLL under validation would not meet the requirements to pass the application control policy. The DLL was allowed since the policy is in audit mode. |
| **Event ID: 3065**  Description: [Ignored] If the policy was enforced, a user mode DLL under validation would not meet the requirements to pass the application control policy. |
| **Event ID: 3074**  Description: Page hash failure while hypervisor-protected code integrity was enabled. |
| **Event ID: 3075**  Description: This event monitors the performance of the Code Integrity policy check a file. |
| **Event ID: 3076**  Description: Audit executable/dll file |
| **Event ID: 3077**  Description: Block executable/dll file |
| **Event ID: 3079**  Description: The file under validation did not meet the requirements to pass the application control policy. |
| **Event ID: 3080**  Description: If the policy was in enforced mode, the file under validation would not have met the requirements to pass the application control policy. |
| **Event ID: 3081**  Description: The file under validation did not meet the requirements to pass the application control policy. |
| **Event ID: 3082**  Description: If the policy was in enforced mode, the non-WHQL driver would have been denied by the policy. |
| **Event ID: 3084**  Description: Code Integrity will enforce the WHQL Required policy setting on this session. |
| **Event ID: 3085**  Description: Code Integrity will not enforce the WHQL Required policy setting on this session. |
| **Event ID: 3086**  Description: The file under validation does not meet the signing requirements for an isolated user mode (IUM) process. |
| **Event ID: 3089**  Description: Signing information event correlated with either a 3076 or 3077 event. One 3089 event is generated for each signature of a file. Contains the total number of signatures on a file and an index as to which signature it is. Unsigned files will generate a single 3089 event with TotalSignatureCount 0. Correlated in the "System" portion of the event data under "Correlation ActivityID". |
| **Event ID: 3090**  Description: Allow executable/dll file |
| **Event ID: 3091**  Description: Audit executable/dll file |
| **Event ID: 3092**  Description: Block executable/dll file |
| **Event ID: 3095**  Description: This Code Integrity policy cannot be refreshed and must be rebooted instead. |
| **Event ID: 3097**  Description: The Code Integrity policy cannot be refreshed. |
| **Event ID: 3099**  Description: Indicates that a policy has been loaded |
| **Event ID: 3100**  Description: The application control policy was refreshed but was unsuccessfully activated. Retry. |
| **Event ID: 3101**  Description: Code Integrity started refreshing the policy. |
| **Event ID: 3102**  Description: Code Integrity finished refreshing the policy. |
| **Event ID: 3103**  Description: Code Integrity is ignoring the policy refresh. |
| **Event ID: 3104**  Description: The file under validation does not meet the signing requirements for a PPL (protected process light) process. |
| **Event ID: 3105**  Description: Code Integrity is attempting to refresh the policy. |
| **Event ID: 3108**  Description: Windows mode change event was successful. |
| **Event ID: 3110**  Description: Windows mode change event was unsuccessful. |
| **Event ID: 3111**  Description: The file under validation did not meet the hypervisor-protected code integrity (HVCI) policy. |

## Microsoft-Windows-AppLocker/MSI and Script

|  |
| --- |
| **Event ID: 8028**  Description: Audit script/MSI file generated by Windows LockDown Policy (WLDP) being called by the script hosts themselves. Note: there is no WDAC enforcement on third-party script hosts. |
| **Event ID: 8029**  Description: Block script/MSI file |
| **Event ID: 8036**  Description: COM object was blocked. To learn more about COM object authorization, see Allow COM object registration in a Windows Defender Application Control policy. |
| **Event ID: 8038**  Description: Signing information event correlated with either an 8028 or 8029 event. One 8038 event is generated for each signature of a script file. Contains the total number of signatures on a script file and an index as to which signature it is. Unsigned script files will generate a single 8038 event with TotalSignatureCount 0. Correlated in the "System" portion of the event data under "Correlation ActivityID". |