 Filter by title

Configure Microsoft Defender Antivirus

Defender Antivirus detections

> Configure Microsoft Defender Antivirus scans

Use limited periodic scanning in Microsoft Defender Antivirus

Protect Dev Drive using performance mode

Compatibility with other security products

Find malware detection names for Microsoft Defender for Endpoint

> Microsoft Defender Antivirus security intelligence and product updates

> Manage Microsoft Defender Antivirus for your organization

> Deploy and report on Microsoft Defender Antivirus

> Scans and remediation

> Microsoft Defender Antivirus exclusions

> Troubleshooting mode for Defender for Endpoint

> Diagnostics and performance for Microsoft Defender Antivirus

▼ Troubleshooting Microsoft Defender Antivirus

Review event logs and error codes to troubleshoot issues with Microsoft Defender Antivirus

Troubleshoot Microsoft Defender Antivirus while migrating from a third-party solution

> Behavioral blocking and containment

UEFI scanning in Defender for Endpoint

Run Microsoft Defender Antivirus in a sandbox

Early Launch Antimalware (ELAM) and Microsoft Defender Antivirus

Hardware acceleration and Microsoft Defender Antivirus


Address false positives/negatives in Microsoft Defender for Endpoint

> Manage device configuration

> Investigate and respond to threats

> Reference

> Microsoft Defender XDR docs

 **Download PDF**

# Review event logs and error codes to troubleshoot issues with Microsoft Defender Antivirus

FAQ • [4 contributors](#)

 [Feedback](#)

## In this article

- [How do I view a Microsoft Defender Antivirus event?](#)
- [Event ID 1000](#)
- [Event ID 1001](#)
- [Event ID 1002](#)
- [Show 108 more](#)

If you encounter a problem with Microsoft Defender Antivirus, you can search the below sections in this article to find a matching issue and potential solution.

### Applies to:

- [Microsoft Defender for Endpoint Plan 1](#)
- [Microsoft Defender for Endpoint Plan 2](#)
- Microsoft Defender Antivirus

## How do I view a Microsoft Defender Antivirus event?

- Open **Event Viewer**.
- In the console tree, expand **Applications and Services Logs > Microsoft > Windows > Windows Defender**.
- Double-click on **Operational**.
- In the details pane, view the list of individual events to find your event.
- Select the event to see specific details about an event in the lower pane, under the **General** and **Details** tabs.

## 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. Examples: Antivirus, Antispyware, or Antimalware
- Scan Parameters: Scan parameters. Examples: Full scan, Quick scan, or 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. Examples: Antivirus, Antispyware, or Antimalware
- Scan Parameters: Scan parameters. Examples: Full scan, Quick scan, or 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. Examples: Antivirus, Antispyware, or Antimalware
- Scan Parameters: Scan parameters. Examples: Full scan, Quick scan, or 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. Examples: Antivirus, Antispyware, or Antimalware
- Scan Parameters: Scan parameters. Examples: Full scan, Quick scan, or 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. Examples: Antivirus, Antispyware, or Antimalware
- Scan Parameters: Scan parameters. Examples: Full scan, Quick scan, or 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. Examples: Antivirus, Antispyware, or Antimalware
- Scan Parameters: Scan parameters. Examples: Full scan, Quick scan, or Custom 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 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:

Copy

- Run the scan again.
- If it fails in the same way, go to the [Microsoft Support site](https://support.microsoft.com/).
- Contact [Microsoft Technical Support](/microsoft-365/admin/get-help-support).

## 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 details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description. Examples: Any threat or malware type.
- Path: File path
- Detection Origin: Detection origin. Examples: Unknown, Local computer, Network share, Internet, Incoming traffic, or Outgoing traffic
- Detection Type: Detection type. Examples: Heuristics, Generic, Concrete, or 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 source 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.
- 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 took action to protect this machine from malware or other potentially unwanted software. For more information, see the following details:

- User: Domain\User
- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Action: Action. Examples:
  - 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's typically from this list of actions specified by the user.
  - 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 encountered an error when taking action on malware or other potentially unwanted software. For more information, see the following details:

- User: Domain\User
- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Path: File path
- Action: Action. Examples:
  - 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's typically from this list of actions specified by the user.
  - 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 restored an item from quarantine. For more information, see the following details:

- Name: Threat name

- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or 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 couldn't restore an item from quarantine.

Description: Microsoft Defender Antivirus encountered an error trying to restore an item from quarantine. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or 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 deleted an item from quarantine. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or 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 couldn't delete an item from quarantine.

Description: Microsoft Defender Antivirus encountered an error trying to delete an item from quarantine. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or 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 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 isn't used in threat events so that there's no confusion regarding whether it's remediation time or infection time. For such events, 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 couldn't delete history of malware and other potentially unwanted software.

Description: Microsoft Defender Antivirus 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 isn't used in threat events so that there's no confusion regarding whether it's remediation time or infection time. For such events, 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 detected a suspicious behavior. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Path: File path
- Detection Origin: Detection origin. Examples: Unknown, Local computer, Network share, Internet, Incoming traffic, or Outgoing traffic
- Detection Type: Detection type. Examples: Heuristics, Generic, Concrete, or 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 source protects against malicious webpage controls.
  - Early Launch Antimalware (ELAM). This source 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
- 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 detected malware or other potentially unwanted software. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Path: File path
- Detection Origin: Detection origin. Examples: Unknown, Local computer, Network share, Internet, Incoming traffic, or Outgoing traffic
- Detection Type: Detection type. Examples: Heuristics, Generic, Concrete, or 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, select **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 took action to protect this machine from malware or other potentially unwanted software. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Path: File path
- Detection Origin: Detection origin. Examples: Unknown, Local computer, Network share, Internet, Incoming traffic, or Outgoing traffic
- Detection Type: Detection type. Examples: Heuristics, Generic, Concrete, or 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 source 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
- Action: Action. Examples:
  - 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's typically from this list of actions specified by the user.
  - No action: No action
  - Block: The resource was blocked from executing.
- Action Status: Description of other 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, Malicious Software Removal Tool, or System Center Endpoint Protection detects a malware, it restores the following system settings and services that might have been changed by the malware:

Copy

```
- 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
- Windows Operating System files
```

The above context applies to the following client and server versions:

Copy

```
- Operating system: Client Operating System
    Operating system version: Windows Vista (Service Pack 1, or Service Pack 2), Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
- Operating system: Server Operating System
    Operating system version: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
```

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 encountered a noncritical error when taking action on malware or other potentially unwanted software. For more information, see the following details:

- Name: Threat name
- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Path: File path
- Detection Origin: Detection origin. Examples: Unknown, Local computer, Network share, Internet, Incoming traffic, or Outgoing traffic
- Detection Type: Detection type. Examples: Heuristics, Generic, Concrete, or 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
- Action: Action. Examples:
  - 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's typically from this list of actions specified by the user.
  - 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 isn't 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 encountered a critical error when taking action on malware or other potentially unwanted software. For more information, see the following details:

- Name: Threat name

- ID: Threat ID
- Severity: Severity. Examples: Low, Moderate, High, or Severe
- Category: Category description, for example, any threat or malware type.
- Path: File path
- Detection Origin: Detection origin. Examples: Unknown, Local computer, Network share, Internet, Incoming traffic, or Outgoing traffic
- Detection Type: Detection type. Examples: Heuristics, Generic, Concrete, or 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
- Action: Action. Examples:
  - 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's typically from this list of actions specified by the user.
  - No action: No action
  - Block: The resource was blocked from executing.
- Action Status: Description of other 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.

- Action: Remove User action: Update the definitions then verify that the removal was successful.
- Action: Clean User action: Update the definitions then verify that the remediation was successful.
- Action: Quarantine User action: Update the definitions and verify that the user has permission to access the necessary resources.
- Action: Allow User action: Verify 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](#), enter the error number in the **Search** box to look for the error code.
- Contact [Microsoft Technical Support](#).

## Event ID 1120

Symbolic name: `MALWAREPROTECTION_THREAT_HASH`

Message: Microsoft Defender Antivirus 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 1121

Message: Event when an attack surface reduction rule fires in block mode.

Description:

- Current Platform Version: Current platform version
- Threat Resource Path: Path
- Hashes: Hashes

## 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 blocked an untrusted process from potentially modifying disk sectors. For more information about the event record, see the following details:

- EventID: EventID. Examples: 1127

- Version: Version. Examples: 0
- Level: Level. Examples: 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. Examples: Microsoft-Windows-Windows Defender/Operational
- Computer: Computer name
- Security UserID: Security UserID
- Product Name: Product Name. Examples: 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 was updated.

- Current Signature Version: Current signature version
- Previous Signature Version: Previous signature version
- Signature Type: Signature type. Examples: Antivirus, Antispyware, Antimalware, or 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 encountered an error trying to update signatures.

- New security intelligence version: New version number
- Previous security intelligence version: Previous version
- Update Source: Update source. Examples:
  - Security intelligence update folder
  - Internal security intelligence update server
  - Microsoft Update Server
  - File share
  - Microsoft Malware Protection Center (MMPC)
- Update Stage: Update stage. Examples: Search, Download, or 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. Examples: Antivirus, Antispyware, Antimalware, or 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's a problem updating definitions. To troubleshoot this event:

- [Update definitions](#) 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](#).

## Event ID 2002

Symbolic name: MALWAREPROTECTION\_ENGINE\_UPDATED

Message: The antimalware engine updated successfully.

Description: Microsoft Defender Antivirus engine version was 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 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 due to an interruption in network connectivity during an update. To troubleshoot this event:

- [Update definitions](#) and force a rescan directly on the endpoint.
- Contact [Microsoft Technical Support](#).

## Event ID 2004

Symbolic name: MALWAREPROTECTION\_SIGNATURE\_REVERSION

Message: There was a problem loading antimalware definition. The antimalware engine attempts to load the last-known good set of definitions.

Description: Microsoft Defender Antivirus 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 attempts 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](#) .

Note: The size of the definitions file downloaded from the site can exceed 60 MB and shouldn't be used as a long-term solution for updating definitions.

- Contact [Microsoft Technical Support](#).

## 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 loads the last-known good antimalware engine and attempt to update.

Description: Microsoft Defender Antivirus couldn't load antimalware engine because current platform version isn't supported. Microsoft Defender Antivirus reverts 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 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 other definitions.

Description: Microsoft Defender Antivirus used Dynamic Signature Service to retrieve more signatures to help protect your machine.

- Current Signature Version: Current signature version

- Signature Type: Signature type. Examples: Antivirus, Antispyware, Antimalware, or Network Inspection System
- Current Engine Version: Current engine version
- Dynamic Signature Type: Dynamic signature type. Examples: Version, Timestamp, No limit, or Duration
- Persistence Path: Path
- Dynamic Signature Version: Version number
- Dynamic Signature Compilation Timestamp: Timestamp
- Persistence Limit Type: Persistence limit type. Examples: VDM version, Timestamp, or 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.

Change to default behavior: Change to dynamic signature event reporting default behavior.

When a dynamic signature is received by MDE, a 2010 event is reported. However, when the dynamic signature expires or is manually deleted a 2011 event is reported. In some cases, when a new signature is delivered to MDE sometimes hundreds of dynamic signatures expire at the same time; therefore hundreds of 2011 events are reported. The generation of so many 2011 events can cause a Security information and event management (SIEM) server to become flooded.

To avoid the previously described situation - starting with platform version 4.18.2207.7 - by default, Defender for Endpoint doesn't report 2011 events:

- This new default behavior is controlled by registry entry:  
`HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\EnableDynamicSignatureDroppedEventReporting`.
- The default value for `EnableDynamicSignatureDroppedEventReporting` is **false**, which means 2011 *events aren't reported*. If it's set to true, 2011 *events are reported*.

Because 2010 signature events are timely distributed sporadically - and won't cause a spike - 2010 signature event behavior is unchanged.

Description: Microsoft Defender Antivirus used Dynamic Signature Service to discard obsolete signatures.

- Current Signature Version: Current signature version
- Signature Type: Signature type. Examples: Antivirus, Antispyware, Antimalware, or Network Inspection System
- Current Engine Version: Current engine version
- Dynamic Signature Type: Dynamic signature type. Examples: Version, Timestamp, No limit, or Duration
- Persistence Path: Path
- Dynamic Signature Version: Version number
- Dynamic Signature Compilation Timestamp: Timestamp

- Removal Reason:
- Persistence Limit Type: Persistence limit type. Examples: VDM version, Timestamp, or 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 encountered an error trying to use Dynamic Signature Service.

- Current Signature Version: Current signature version
- Signature Type: Signature type. Examples: Antivirus, Antispyware, Antimalware, or 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. Examples: Version, Timestamp, No limit, or Duration
- Persistence Path: Path
- Dynamic Signature Version: Version number
- Dynamic Signature Compilation Timestamp: Timestamp
- Persistence Limit Type: Persistence limit type. Examples: VDM version, Timestamp, or 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 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 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 expires shortly. Running Microsoft Defender Antivirus on an out of support operating system isn't 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 isn't 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 isn't 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 encountered an error and failed.

- Feature: Feature. Examples: On Access, Internet Explorer downloads and Microsoft Outlook Express attachments, Behavior monitoring, or 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 restarted a feature.

User action: You should restart the system then run a full scan because it's possible the system wasn't 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's 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 restarted a feature. It's recommended that you run a full system scan to detect any items that might have been missed while this agent was down.

- Feature: Feature. Examples: On Access, IE downloads and Outlook Express attachments, Behavior monitoring, or Network Inspection System

- Reason: The reason Microsoft Defender Antivirus real-time protection restarted a feature.

User action: The real-time protection feature restarted. If this event happens again, contact [Microsoft Technical Support](#).

## 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 changed.

- Feature: Feature. Examples: On Access, IE downloads and Outlook Express attachments, Behavior monitoring, or Network Inspection System
- Configuration:

## Event ID 5007

Symbolic name: `MALWAREPROTECTION_CONFIG_CHANGED`

Message: The antimalware platform configuration changed.

Description: Microsoft Defender Antivirus configuration changed. If this event is unexpected, you should review the settings as the event might 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 was terminated due to an unexpected error.

- Failure Type: Failure type. Examples: 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](#) and entering the error number in the Search box, and contact [Microsoft Technical Support](#).

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](#), enter the error number in the **Search** box to look for the error code.
- Contact [Microsoft Technical Support](#).

## Event ID 5009

Symbolic name: MALWAREPROTECTION\_ANTISPYWARE\_ENABLED

Message: Scanning for malware and other potentially unwanted software is enabled.

Description: Microsoft Defender Antivirus enabled scanning for malware and other potentially unwanted software.

## 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 enabled scanning for viruses.

## 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 5013

Symbolic name: MALWAREPROTECTION\_SCAN\_CANCELLED

Message: Tamper protection blocked a change to Microsoft Defender Antivirus.

Description: If Tamper protection is enabled then any attempt to change any of Defender's settings is blocked. Event ID 5013 is generated and states which setting change was blocked.

## Event ID 5100

Symbolic name: MALWAREPROTECTION\_EXPIRATION\_WARNING\_STATE

Message: The antimalware platform expires soon.

Description: Microsoft Defender Antivirus 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 expires.
- Expiration Date: The date Microsoft Defender Antivirus expires.

## 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.

- Error Code: Error code Result code associated with threat status. Standard HRESULT values.
- Error Description: Error description Description of the error.

# Microsoft Defender Antivirus client error codes

If Microsoft Defender Antivirus experiences any issues, it will usually give you an error code to help you troubleshoot the issue. Most often an error means there was a problem installing an update. This section provides the following information about Microsoft Defender Antivirus client errors.

- The error code
- The possible reason for the error
- Advice on what to do now

Use the following information to help troubleshoot Microsoft Defender Antivirus error codes.

## Error code 0x80508007

Message: ERR\_MP\_NO\_MEMORY

Possible reason: This error indicates that you might have run out of memory.

Resolution:

- Check the available memory on your device.
- Close any unused applications that are running to free up memory on your device.
- Restart the device and run the scan again.

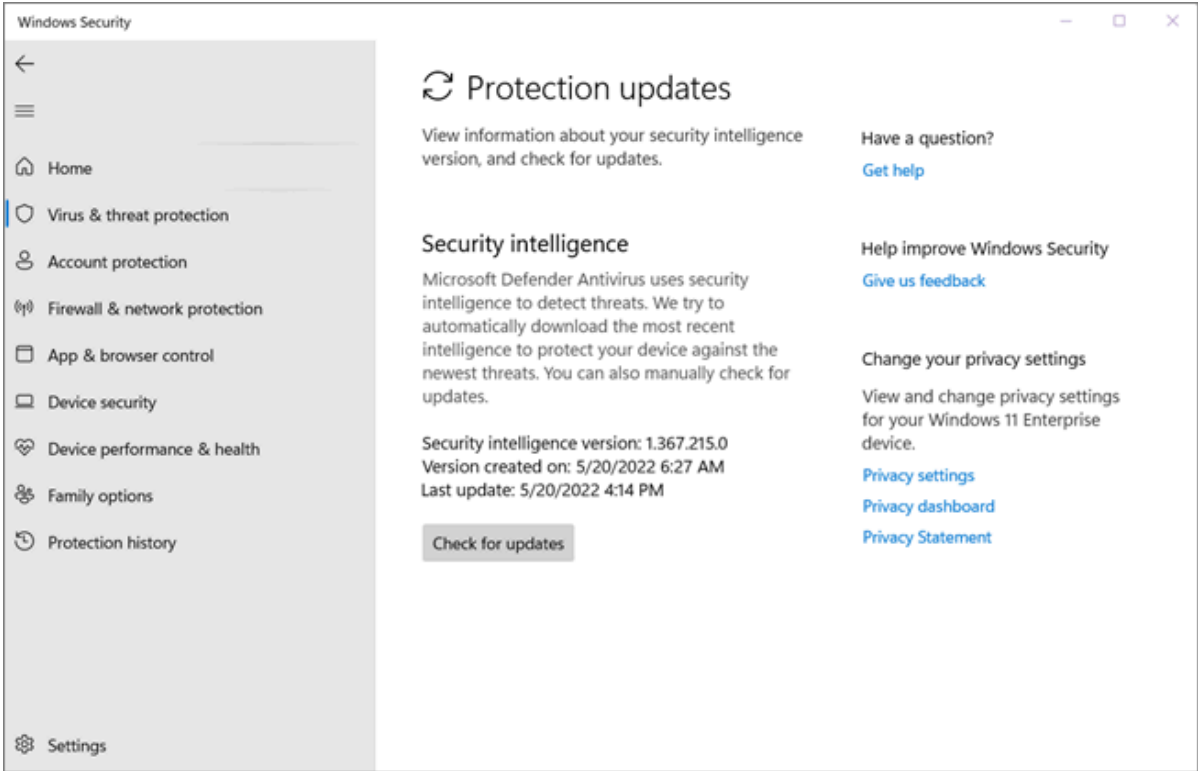
# Error code 0x8050800C

Message: ERR\_MP\_BAD\_INPUT\_DATA

Possible reason: This error indicates that there might be a problem with your security product.

Resolution:

- Update the definitions. Either:
  - Get your security intelligence updates in the Windows Security app.



,

- Download the latest definitions from the [Microsoft Security Intelligence site](#).

[!NOTE] The size of the definitions file downloaded from the site can exceed 60 MB and shouldn't be used as a long-term solution for updating definitions.

- Run a full scan.
- Restart the device and try again.

# Error code 0x80508020

Message: ERR\_MP\_BAD\_CONFIGURATION

Possible reason: This error indicates that there might be an engine configuration error.

Commonly, this error is related to input data that doesn't allow the engine to function properly.

# Error code 0x805080211

Message: ERR\_MP\_QUARANTINE\_FAILED

Possible reason: This error indicates that Microsoft Defender Antivirus failed to quarantine a threat.

# Error code 0x80508022

Message: ERR\_MP\_REBOOT\_REQUIRED

Possible reason: This error indicates that a reboot is required to complete threat removal.

# Error code 0x80508023

Message: ERR\_MP\_THREAT\_NOT\_FOUND

Possible reason: This error indicates that the threat might no longer be present on the media, or malware might be stopping you from scanning your device.

Resolution: Run the [Microsoft Safety Scanner](#) then update your security software and try again.

## Error code 0x80508024

Message: ERR\_MP\_FULL\_SCAN\_REQUIRED

Possible reason: This error indicates that a full system scan might be required.

Resolution: Run a full system scan.

## Error code 0x80508025

Message: ERR\_MP\_MANUAL\_STEPS\_REQUIRED

Possible reason: This error indicates that manual steps are required to complete threat removal.

Resolution: Follow the manual remediation steps outlined in the [Microsoft Malware Protection Encyclopedia](#) [↗](#). You can find a threat-specific link in the event history.

## Error code 0x80508026

Message: ERR\_MP\_REMOVE\_NOT\_SUPPORTED

Possible reason: This error indicates that removal inside the container type might not be not supported.

Resolution: Microsoft Defender Antivirus isn't able to remediate threats detected inside the archive. Consider manually removing the detected resources.

## Error code 0x80508027

Message: ERR\_MP\_REMOVE\_LOW\_MEDIUM\_DISABLED

Possible reason: This error indicates that removal of low and medium threats might be disabled.

Resolution: Check the detected threats and resolve them as required.

## Error code 0x80508029

Message: ERROR\_MP\_RESCAN\_REQUIRED

Possible reason: This error indicates a rescan of the threat is required.

Resolution: Run a full system scan.

## Error code 0x80508030

Message: ERROR\_MP\_CALLISTO\_REQUIRED

Possible reason: This error indicates that an offline scan is required.

Resolution: Run offline Microsoft Defender Antivirus. For more information, see [Help protect my PC with Microsoft Defender Offline](#) [↗](#).

# Error code 0x80508031

Message: `ERROR_MP_PLATFORM_OUTDATED`

Possible reason: This error indicates that Microsoft Defender Antivirus doesn't support the current version of the platform and requires a new version of the platform.

Resolution: You can only use Microsoft Defender Antivirus in Windows 10 and Windows 11. For Windows 8, Windows 7 and Windows Vista, you can use System Center Endpoint Protection.

## Internal error codes

The following error codes are used during internal testing of Microsoft Defender Antivirus.

If you see these errors, you can try to update definitions and force a rescan directly on the endpoint.

# Error code 0x80501004

Message displayed: `ERROR_MP_NO_INTERNET_CONN`

Possible reason for error and resolution: Check your Internet connection, then run the scan again.

# Error code 0x80501000

Message displayed: `ERROR_MP_UI_CONSOLIDATION_BASE`

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

# Error code 0x80501001

Message displayed: `ERROR_MP_ACTIONS_FAILED`

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

# Error code 0x80501002

Message displayed: `ERROR_MP_NOENGINE`

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

# Error code 0x80501003

Message displayed: `ERROR_MP_ACTIVE_THREATS`

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

# Error code 0x805011011

Message displayed: `MP_ERROR_CODE_LUA_CANCELLED`

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

# Error code 0x80501101

Message displayed: `ERROR_LUA_CANCELLATION`

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501102

Message displayed: MP\_ERROR\_CODE\_ALREADY\_SHUTDOWN

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501103

Message displayed: MP\_ERROR\_CODE\_RDEVICE\_S\_ASYNC\_CALL\_PENDING

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501104

Message displayed: MP\_ERROR\_CODE\_CANCELLED

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501105

Message displayed: MP\_ERROR\_CODE\_NO\_TARGETOS

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501106

Message displayed: MP\_ERROR\_CODE\_BAD\_REGEX

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501107

Message displayed: MP\_ERROR\_TEST\_INDUCED\_ERROR

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80501108

Message displayed: MP\_ERROR\_SIG\_BACKUP\_DISABLED

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508001

Message displayed: ERR\_MP\_BAD\_INIT\_MODULES

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508002

Message displayed: ERR\_MP\_BAD\_DATABASE

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508004

Message displayed: ERR\_MP\_BAD\_UFS

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050800C

Message displayed: ERR\_MP\_BAD\_INPUT\_DATA

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050800D

Message displayed: ERR\_MP\_BAD\_GLOBAL\_STORAGE

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050800E

Message displayed: ERR\_MP\_OBSOLETE

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050800F

Message displayed: ERR\_MP\_NOT\_SUPPORTED

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050800F

Message displayed: ERR\_MP\_NO\_MORE\_ITEMS

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508010

Message displayed: ERR\_MP\_NO\_MORE\_ITEMS

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508011

Message displayed: ERR\_MP\_DUPLICATE\_SCANID

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508012

Message displayed: ERR\_MP\_BAD\_SCANID

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508013

Message displayed: ERR\_MP\_BAD\_USERDB\_VERSION

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508014

Message displayed: ERR\_MP\_RESTORE\_FAILED

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508016

Message displayed: ERR\_MP\_BAD\_ACTION

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80508019

Message displayed: ERR\_MP\_NOT\_FOUND

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80509001

Message displayed: ERR\_RELO\_BAD\_EHANDLE

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x80509003

Message displayed: ERR\_RELO\_KERNEL\_NOT\_LOADED

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050A001

Message displayed: ERR\_MP\_BADDB\_OPEN

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050A002

Message displayed: ERR\_MP\_BADDB\_HEADER

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050A003

Message displayed: ERR\_MP\_BADDB\_OLDENGINE

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050A004

Message displayed: ERR\_MP\_BADDB\_CONTENT

Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050A005

Message displayed: ERR\_MP\_BADDB\_NOTSIGNED



Possible reason for error and resolution: This error is internal. The cause isn't clearly defined.

## Error code 0x8050801

Message displayed: ERR\_MP\_REMOVE\_FAILED

Possible reason for error and resolution: This error is internal. It might be triggered when malware removal isn't successful.

## Error code 0x80508018

Message displayed: ERR\_MP\_SCAN\_ABORTED

Possible reason for error and resolution: This error is internal. It might have triggered when a scan fails to complete.

## Feedback

Was this page helpful? 

👍 Yes

👎 No

[Provide product feedback](#)