GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

LOG DESCRIPTION

Version 2.7.1

Document last updated: June 30 2025

Reference: ses-en-log_guide-v2.7.1

Getting started

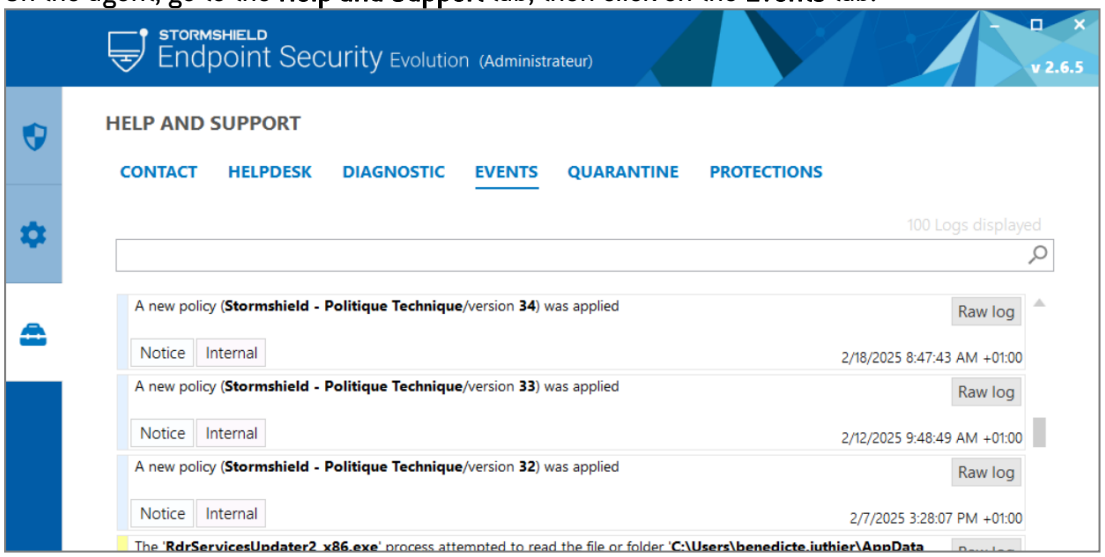
Stormshield Endpoint Security Evolution (SES Evolution) logs agent activity while they operate. To achieve this, the solution relies on a log mechanism whose format and meaning are described in this document.

The logs generated are stored in JSON format on the agent, server and log database, and can be viewed from the administration console and the agent interface. They can also be read on the Syslog server if you have configured one.

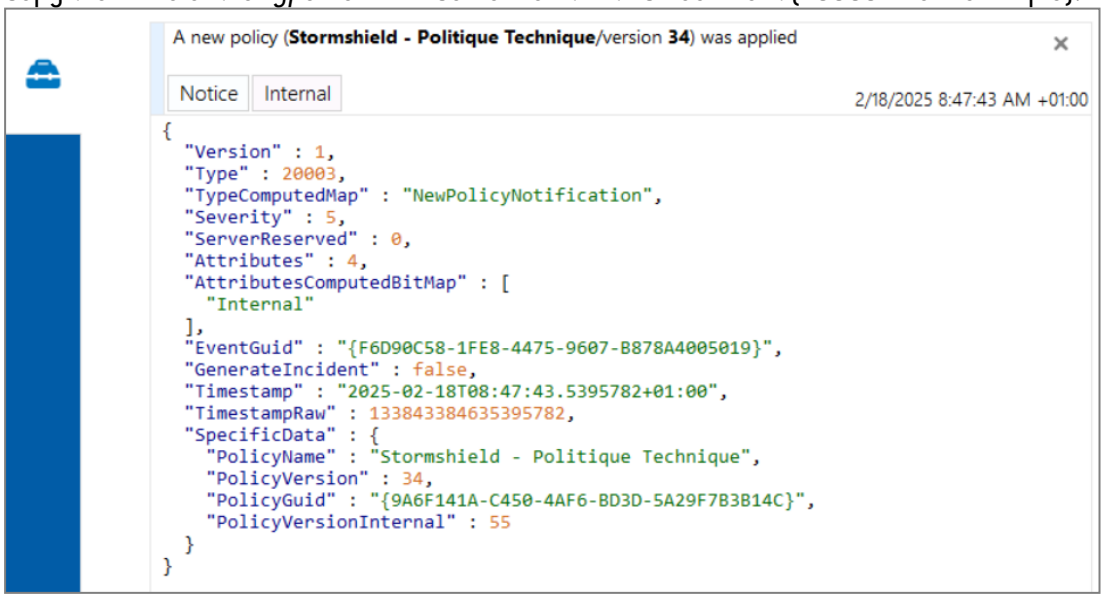
This document lists all log identifiers and describes the various fields. To find out the meaning of a log, we recommend that you search for the identifier in this document.

Finding out the log IDs on the agent

1. On the agent, go to the **Help and Support** tab, then click on the **Events** tab.



2. Click on the Log brut button of the desired log.
3. Copy the value of the *Type* field and search for it in this document (*20003* in our example).



Finding out the log IDs on the administration console

1. From the administration console, go to the **Agent logs** menu.
2. In the log panel, click on a log line and unfold it.
3. Click on the **Raw log** tab.
4. Copy the value of the *Type* field and search for it in this document.

For more information on logs, refer to the SES Evolution *Administration guide*.

Fields common to all events

Fields found in all the logs that the agent generates.

Field	Meaning
Type	Type of event. The descriptions given in the details of logs vary according to the type of event. This field can contain one of the values listed in page LogType.
_Category	Event category (file or registry protection, etc.). This field can contain one of the values listed in page LogCategory.
Severity	Level of severity of the log.
ServerReserved	Information generated by the console, which allows the server to process the event upon receipt (e.g. by storing it in a database or sending it to a Syslog server).
Attributes	Log attributes. This field can contain combined binary values listed in section LogAttributes.
EventGuid	Unique ID of the log generated by the agent.
GenerateIncident	Information indicating whether the generated log should trigger context generation.

Additional common fields for all events sent via Syslog.

The additional fields present in logs sent via Syslog are as follows:

Field	Meaning
AgentName	Name of the log issuing agent.
AgentGuid	Log issuing agent Guid.
CategoryName	Log category name.
IncidentGuid	Context Guid.
AgentGroupName	Name of the agent group to which the agent belongs when the log is issued.
AgentGroupGuid	Guid of the agent group to which the agent belongs when the log is issued.
SeverityName	Log severity name.
PolicyName	Name of the policy applied to the agent when the log is issued.
Message	Log message.
AgentAddresses	List of agent IP addresses.
AttackTriggerCondition	Attack intent of the rule that generated the log.
AttackCVEId	List of CVEs associated with the log.
AttackSESId	List of IDs associated with the log.
AttackMitreTacticId	List of Mitre Att&ck tactic IDs or tags.
AttackMitreTacticName	List of Mitre Att&ck tactics.
AttackMitreTechnicId	List of Miter Att&ck technique and sub-technique IDs or tags.
AttackMitreTechnicName	List of Miter Att&ck techniques and sub-techniques.
OperatingSystemType	Operating system type.

Event no. 7: Process access

AgentOperationProcessAccess: The agent detected that a process is requesting access to another process or to one of its threads, or is attempting to duplicate a handle that belongs to another process.

Field	Meaning
SourceProcess	Details about the process that is receiving a handle: whether it is the process that is performing the action during direct access to the object, or whether it is a third-party process in the case of a handle duplication. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
TargetProcess	Details about the process being illegally accessed. More details on this block in section ProcessStaticInfoTemplate.
Details	Details about the object being illegally accessed. More details on this block in section AgentOperationProcessAccessDetailsProcessTemplate, AgentOperationProcessAccessDetailsThreadTemplate.
ObjectType	Type of object that is being illegally accessed (process or thread). This field can contain one of the values listed in page ProcessAccessObjectType.
Operation	Type of operation performed (access to the object or duplication of its handle). This field can contain one of the values listed in page ProcessAccessOperation.
DuplicatingProcess	Details about the process that is duplicating the handle. More details on this block in section ProcessStaticInfoTemplate.

Event no. 11: Process execution

AgentOperationProcessExecution: The agent detected that a process was created.

Field	Meaning
SourceProcess	Details about the process that requested the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
CreatedProcess	Information about the created process. More details on this block in section ProcessStaticInfoTemplate.
ParentProcess	Information about the parent process of the created process. More details on this block in section ProcessStaticInfoTemplate.

Event no. 39: Raw volume access

AgentOperationRawVolumeAccess: The agent detected access to a storage volume without going through the file system.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the volume.
VolumeZone	Attributes of the volume. This field can contain combined binary values listed in section VolumeZone.
AccessType	Type of access (read or write). This field can contain one of the values listed in page VolumeAccessType.
DataOffset	Position of written or read data.
DataLength	Length of written or read data.

Event no. 40: Network access link

AgentOperationNetworkAccessBind: The agent detected that a process is attempting to open a network port to become a server.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Protocol	IP protocol used. This field can contain one of the values listed in page NetworkAccessProtocol.
AddressFamily	IP address family (IPv4 or IPv6). This field can contain one of the values listed in page NetworkAccessAddressFamily.
LocalAddress	IP address of the interface used to open the network port.
LocalPort	Listening port.

Event no. 41: Inbound network access

AgentOperationNetworkAccessAccept: The agent detected that a process is attempting to receive network connection.

Field	Meaning
SourceProcess	Details of the process performing the network operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Protocol	IP protocol used. This field can contain one of the values listed in page NetworkAccessProtocol.
AddressFamily	IP address family (IPv4 or IPv6). This field can contain one of the values listed in page NetworkAccessAddressFamily.
LocalAddress	IP address of the interface used by the machine protected by the agent.
RemoteAddress	IP address of the third-party host.
LocalPort	Communication port used by the machine protected by the agent.
RemotePort	Communication port used by the third-party host.

Event no. 42: Outbound network access

AgentOperationNetworkAccessConnect: The agent detected that a process is attempting to set up a network connection.

Field	Meaning
SourceProcess	Details of the process performing the network operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Protocol	IP protocol used. This field can contain one of the values listed in page NetworkAccessProtocol.
AddressFamily	IP address family (IPv4 or IPv6). This field can contain one of the values listed in page NetworkAccessAddressFamily.
LocalAddress	IP address of the interface used by the machine protected by the agent.
RemoteAddress	IP address of the third-party host.
LocalPort	Communication port used by the machine protected by the agent.
RemotePort	Communication port used by the third-party host.

Event no. 43: Process hollowing

AgentOperationProcessHollowing: The agent has detected process hollowing.

Field	Meaning
SourceProcess	Information about the process that performed the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
CreatedProcess	Information about the created process. More details on this block in section ProcessStaticInfoTemplate.
Operation	Method used for process hollowing. This field can contain one of the values listed in page ProcessHollowingOperation.

Event no. 44: Stack pivoting

AgentOperationStackPivot: The agent's memory protection was enabled.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.

Event no. 45: Load driver

AgentOperationDriverLoading: The agent detected that a process is attempting to load a driver.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the executable file corresponding to the loaded driver.
FileOwner	Owner of the executable file corresponding to the driver. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
HashMd5	MD5 hash of the executable file corresponding to the loaded driver.
HashSha1	SHA-1 hash of the executable file corresponding to the loaded driver.
HashSha256	SHA-256 hash of the executable file corresponding to the loaded driver.

Event no. 46: Protect driver

AgentOperationDriverGuard: The DRIVER_OBJECT structure of a driver on the agent is corrupted.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
CorruptedDriverName	Name of the driver with the altered DRIVER_OBJECT structure.
CorruptingDriverPath	Path to the driver that caused the corruption.
FileOwner	Owner of the driver that caused the corruption. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
HashMd5	MD5 hash of the driver that caused the corruption.
HashSha1	SHA-1 hash of the driver that caused the corruption.
HashSha256	SHA-256 hash of the driver that caused the corruption.

Event no. 47: Execution flow hijacking

AgentOperationHoneyPot: A process is trying to call kernel32.dll functions illegally (Execution flow hijacking).

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
FunctionName	Name of the called function.
CallerModuleFilename	Module that made the illegal call.
ExtraParametersInfo	Parameters sent to the called function.

Event no. 50: Access token manipulation

AgentOperationTokenGuard: The agent detected that a process is attempting to modify its security token.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Details	Additional information about the modification of the security token. More details on this block in section AgentOperationTokenGuardDetailsTokenDuplicateTemplate, AgentOperationTokenGuardDetailsTokenModifyTemplate.
DetailsType	Type of modification of the security token. This field can contain one of the values listed in page TokenGuardDetailsType.

Event no. 51: Keylogging

AgentOperationKeylogging: The agent detected that a process is attempting to log keystrokes intended for another process.

Field	Meaning
SourceProcess	Process at the source of the keylogging operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
TargetProcess	Process targeted by the keylogging attempt. More details on this block in section ProcessStaticInfoTemplate.
KeyloggingMethod	Method used during the keylogging attempt. This field can contain one of the values listed in page KeyloggingMethod.

Event no. 53: Heap spray

AgentOperationHeapSpray: The agent detected that protection against heap spray attacks was enabled.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
PreallocatedPageHit	Memory page used for heap spray.

Event no. 54: LRPC Access

AgentOperationLrpcAccess: The agent detected that a process is attempting to log in to a software component on the agent.

Field	Meaning
SourceProcess	Process at the source of the LRPC communication (LRPC client process). More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
CallerModuleName	Name of the module on the agent that was contacted by the unauthorized process.

Event no. 55: Protection against code injection

AgentOperationCreateRemoteThread: The agent detected that a process is attempting to inject code into another process.

Field	Meaning
SourceProcess	Process at the source of the code injection. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
TargetProcess	Process targeted by the code injection. More details on this block in section ProcessStaticInfoTemplate.

Event no. 56: Process shut down

AgentOperationProcessExit: The agent detected that a process ended.

Field	Meaning
SourceProcess	Information on the process that is ending. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
ExitStatusCode	Output code of the process.
CreatorProcessGuid	Unique ID generated by the agent for the process that created the process being shut down.

Event no. 57: Application hooking (all)

AgentOperationSetWindowsHookExAll: The agent detected that a process is attempting to inject code into all processes using the SetWindowsHookEx function.

Field	Meaning
SourceProcess	Process at the source of the action. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
HookId	Type of hook that the source process wanted to set. This field can contain one of the values listed in page SetWindowsHookExHookId.
ModuleName	Path to the injected executable.

Event no. 58: Application hooking

AgentOperationSetWindowsHookEx: The agent detected that a process is attempting to inject code into a process using the SetWindowsHookEx function.

Field	Meaning
SourceProcess	Process at the source of the action. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
TargetProcess	Details about the process targeted by the operation. More details on this block in section ProcessStaticInfoTemplate.
HookId	Type of hook that the source process wanted to set. This field can contain one of the values listed in page SetWindowsHookExHookId.
ModuleName	Path to the injected executable.

Event no. 59: Process access with privilege escalation

AgentOperationProcessAccessWithPrivilegeEscalation: The agent detected that a process is requesting access to another process or to one of its threads by using privilege escalation.

Field	Meaning
SourceProcess	Details about the process that is receiving a handle: whether it is the process that is performing the action during direct access to the object, or whether it is a third-party process in the case of a handle duplication. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
TargetProcess	Details about the process being illegally accessed. More details on this block in section ProcessStaticInfoTemplate.
Details	Details about the object being illegally accessed. More details on this block in section AgentOperationProcessAccessDetailsProcessTemplate, AgentOperationProcessAccessDetailsThreadTemplate.
ObjectType	Type of object that is being illegally accessed (process or thread). This field can contain one of the values listed in page ProcessAccessObjectType.

Event no. 60: EDR detection bypass

AgentOperationEDRBypass: The agent detected a malicious actor attempting to disable an EDR detection means on the workstation.

Field	Meaning
SourceProcess	Process detected as malicious. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Method	Bypass method detected. This field can contain one of the values listed in page EDRBypassMethod.
HardwareBreakpointInformation	Information associated with the hardware breakpoint. Empty block if the detected method is not compatible. More details on this block in section AgentOperationEDRBypassDetailsBreakpointInformationTemplate, AgentOperationEDRBypassDetailsNoInformationTemplate.
FunctionPatchInformation	Information associated with the detected code tampering. Empty block if the detected method is not compatible. More details on this block in section AgentOperationEDRBypassDetailsFunctionPatchInformationTemplate, AgentOperationEDRBypassDetailsNoInformationTemplate.
IdentifiedTarget	Technical value specified by Stormshield to characterize the type of attack.

Event no. 64: Fileless

AgentOperationFileless: The agent detected a malicious actor attempting to execute code in a suspicious manner.

Field	Meaning
SourceProcess	Process detected as malicious. More details on this block in section ProcessStaticInfoTemplate.
TargetProcess	Process targeted by the attack. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Method	Execution method detected. This field can contain one of the values listed in page FilelessAttackMethod.
TrampolineStartInformation	Information associated with the use of trampoline. Empty block if the detected method is not compatible. More details on this block in section AgentOperationFilelessDetailsTrampolineStartInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.
ModuleStompingInformation	Information associated with module overwrite. Empty block if the detected method is not compatible. More details on this block in section AgentOperationFilelessDetailsModuleStompingInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.
DynamicMemoryInformation	Information about dynamically allocated memory usage. Empty block if the detected method is not compatible. More details on this block in section AgentOperationFilelessDetailsDynamicMemoryInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.
ThreadStartAddressSpoofingInformation	Information about the exchange of a thread's start address. Empty block if the detected method is not compatible. More details on this block in section AgentOperationFilelessDetailsThreadStartAddressSpoofingInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.

Event no. 103: Creating a registry key

AgentOperationRegistryKeyCreate: The agent detected that a registry key was created or renamed.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Details	Details about the operation. More details on this block in section AgentOperationRegistryKeyCreateDetailsCreateTemplate, AgentOperationRegistryKeyCreateDetailsRenameTemplate, AgentOperationRegistryKeyCreateDetailsCreateLinkTemplate.
DetailsType	Type of operation (creation or renaming). This field can contain one of the values listed in page RegistryKeyCreateDetailsType.
Path	Path to the registry key after creation or renaming.

Event no. 104: Reading a registry key

AgentOperationRegistryKeyRead: The agent detected that a registry key was read.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the registry key that was read.
InformationClass	Type of information requested about the registry key. This field can contain one of the values listed in page RegistryQueryInformationClass.

Event no. 109: Writing a registry key

AgentOperationRegistryKeyWrite: The agent detected that a registry key was modified.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Details	Details about the operation. More details on this block in section AgentOperationRegistryKeyWriteDetailsSubkeyCreateTemplate, AgentOperationRegistryKeyWriteDetailsSubkeyRenameTemplate, AgentOperationRegistryKeyWriteDetailsSetInformationTemplate, AgentOperationRegistryKeyWriteDetailsSetSecurityTemplate.
DetailsType	Type of operation (writing information about key or security descriptor). This field can contain one of the values listed in page RegistryKeyWriteDetailsType.
Path	Path to the modified registry key.

Event no. 112: Deleting a registry key

AgentOperationRegistryKeyDelete: The agent detected that a registry key was deleted or renamed.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Details	Details about the operation. More details on this block in section AgentOperationRegistryKeyDeleteDetailsDeleteTemplate, AgentOperationRegistryKeyDeleteDetailsRenameTemplate.
DetailsType	Type of operation (deleting or renaming). This field can contain one of the values listed in page RegistryKeyDeleteDetailsType.
Path	Path to the deleted registry key.

Event no. 113: Creating a registry value

AgentOperationRegistryValueCreate: The agent detected that a registry value was created.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the registry key containing the value.
ValueName	Name of the registry value.
ValueDataType	Type of registry value. This field can contain one of the values listed in page RegistryValueType.
ValueData	Data written in the registry value.

Event no. 114: Reading a registry value

AgentOperationRegistryValueRead: The agent detected that a registry value was read.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the registry key containing the value.
ValueName	Name of the registry value.

Event no. 115: Writing a registry value

AgentOperationRegistryValueWrite: The agent detected that a registry value was modified.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the registry key containing the value.
ValueName	Name of the registry value.
ValueDataType	Type of registry value. This field can contain one of the values listed in page RegistryValueType.
ValueData	Data written in the registry value.

Event no. 116: Deleting a registry value

AgentOperationRegistryValueDelete: The agent detected that a registry value was deleted.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Path	Path to the registry key containing the value.
ValueName	Name of the registry value.

Event no. 173: Create file

AgentOperationFileCreate: The agent detected that a process is attempting to create an item on a file system.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Description if the item was created from the network; otherwise, it will be empty. More details on this block in section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Details about the creation operation. More details on this block in section AgentOperationFileDetailsCreateTemplate, AgentOperationFileDetailsCreateHardLinkDestinationTemplate, AgentOperationFileDetailsRenameDestinationTemplate, AgentOperationFileDetailsMoveFileExDestinationTemplate, AgentOperationFileDetailsSetOwnerDestinationTemplate.
DetailsType	Type detail block. This field can contain one of the values listed in page FileCreateDetailsType.
Path	Path to the created item.
MatchingPath	Part of the path affected by a rule on the agent. If this field is empty, this means that the entire path is affected by the rule.
VolumeZone	Type of volume on which the item is located. This field can contain combined binary values listed in section VolumeZone.
FileObjectType	Type of item created (file or folder). This field can contain one of the values listed in page FileObjectType.
FileOwner	Security ID of the owner of the created item. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 174: Execute file

AgentOperationFileExecute: The agent detected that a process is attempting to execute a file.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
Path	Path to the item.
MatchingPath	Part of the path affected by a rule on the agent. If this field is empty, this means that the entire path is affected by the rule.
VolumeZone	Type of volume on which the item is located. This field can contain combined binary values listed in section VolumeZone.
FileObjectType	Type of item on the file system (file or folder). This field can contain one of the values listed in page FileObjectType.
FileOwner	Owner of the item. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
PageProtection	Permissions requested when loading the item in memory. This field can contain combined binary values listed in section MemoryProtection.

Event no. 175: Read file

AgentOperationFileRead: The agent detected that a process is attempting to read the contents of an item on a file system.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Detail block if the item was created from the network; otherwise, it will be empty. More details on this block in section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Details about the creation operation. More details on this block in section AgentOperationFileDetailsSectionMappingTemplate, AgentOperationFileDetailsReadDataTemplate.
DetailsType	Type of detail block. This field can contain one of the values listed in page FileReadDetailsType.
Path	Path to the targeted item.
MatchingPath	Portion of the path affected by a rule on the agent. If this field is empty, this means that the entire path triggered the application of the rule.
VolumeZone	Details of the volume on which the item is located. This field can contain combined binary values listed in section VolumeZone.
FileObjectType	Type of item targeted (file or folder). This field can contain one of the values listed in page FileObjectType.
FileOwner	Security ID of the owner of the targeted item. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 176: Write file

AgentOperationFileWrite: The agent detected that a process is attempting to write the contents of an item on a file system.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Detail block if the item was created from the network; otherwise, it will be empty. More details on this block in section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Details about the creation operation. More details on this block in section AgentOperationFileDetailsCreateTemplate, AgentOperationFileDetailsCreateChildTemplate, AgentOperationFileDetailsCreateHardLinkSourceTemplate, AgentOperationFileDetailsCreateChildHardLinkDestinationTemplate, AgentOperationFileDetailsRenameChildSourceTemplate, AgentOperationFileDetailsRenameChildDestinationTemplate, AgentOperationFileDetailsMoveFileExChildSourceTemplate, AgentOperationFileDetailsMoveFileExChildDestinationTemplate, AgentOperationFileDetailsSectionMappingTemplate, AgentOperationFileDetailsWriteDataTemplate, AgentOperationFileDetailsSetInformationTemplate, AgentOperationFileDetailsSetSecurityTemplate, AgentOperationFileDetailsDeleteChildTemplate.
DetailsType	Type of detail block. This field can contain one of the values listed in page FileWriteDetailsType.
Path	Path to the targeted item.
MatchingPath	Portion of the path affected by a rule on the agent. If this field is empty, this means that the entire path triggered the application of the rule.
VolumeZone	Details of the volume on which the item is located. This field can contain combined binary values listed in section VolumeZone.
FileObjectType	Type of item targeted (file or folder). This field can contain one of the values listed in page FileObjectType.
FileOwner	Security ID of the owner of the targeted item. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 177: Delete file

AgentOperationFileDelete: The agent detected that a process is attempting to delete an item on a file system.

Field	Meaning
SourceProcess	Details about the process that is performing the operation. More details on this block in section ProcessStaticInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Description if the item was deleted from the network; otherwise, it will be empty. More details on this block in section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Details about the delete operation. More details on this block in section AgentOperationFileDetailsCreateTemplate, AgentOperationFileDetailsCreateHardLinkDestinationTemplate, AgentOperationFileDetailsRenameSourceTemplate, AgentOperationFileDetailsRenameDestinationTemplate, AgentOperationFileDetailsMoveFileExSourceTemplate, AgentOperationFileDetailsMoveFileExDestinationTemplate, AgentOperationFileDetailsSetOwnerSourceTemplate, AgentOperationFileDetailsDeleteTemplate.
DetailsType	Type of operation. This field can contain one of the values listed in page FileDeleteDetailsType.
Path	Path to the deleted item.
MatchingPath	Part of the path affected by a rule on the agent. If this field is empty, this means that the entire path is affected by the rule.
VolumeZone	Type of volume on which the item is located. This field can contain combined binary values listed in section VolumeZone.
FileObjectType	Type of item deleted (file or folder). This field can contain one of the values listed in page FileObjectType.
FileOwner	Security ID of the owner of the deleted item. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 301: Floppy disk

AgentOperationFloppy: The agent detected an attempt to use a plug and play disk reader.

Field	Meaning
PnPDeviceInfo	Information about the floppy disk drive. More details on this block in section PnPDeviceInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.

Event no. 302: CD/DVD

AgentOperationCDRom: The agent detected an attempt to use an optical disk reader (in particular CD, DVD and Blu-Ray.

Field	Meaning
Operation	Operation performed on the optical disk reader. This field can contain one of the values listed in page CDRomOperation.
PnPDeviceInfo	Information about the optical disk reader. More details on this block in section PnPDeviceInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.

Event no. 303: COM Port

AgentOperationComPort: The agent detected an attempt to use a COM port.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.

Event no. 305: USB device

AgentOperationUsbDevice: The agent detected the use of a USB device.

Field	Meaning
UsbDeviceInfo	Information about the USB device. More details on this block in section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
PhysicalConsoleSession	Information relating to the physical user session (console). More details on this block in section PhysicalConsoleSessionTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
DeviceEventType	Event for the USB device. This field can contain one of the values listed in page UsbDeviceEventType.

Event no. 321: USB volume tracking data

AgentOperationUsbVolumeTrackingDataUpdate: Block indicating a change in the tracking data of a volume.

Field	Meaning
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate.
OldTrackingData	Tracking data of the volume before changes. More details on this block in section UsbVolumeTrackingDataTemplate.
NewTrackingData	Tracking data of the volume after changes. More details on this block in section UsbVolumeTrackingDataTemplate.
PhysicalConsoleSession	Information relating to the physical user session (console). More details on this block in section PhysicalConsoleSessionTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
FilesystemType	Type of file system on the volume. This field can contain one of the values listed in page FilesystemType.
VolumePath	Path to the volume.
TotalAllocationUnits	Total number of allocation units for the volume.
SectorsPerAllocationUnit	Number of allocation units per sector for the volume.
BytesPerSector	Number of bytes per sector for the volume.
VolumeLabel	Name of the volume

Event no. 322: Mounting / unmounting a USB volume.

AgentOperationUsbVolumeMount: Block indicating a change in the tracking data of a volume.

Field	Meaning
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate.
TrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate.
PhysicalConsoleSession	Information relating to the physical user session (console). More details on this block in section PhysicalConsoleSessionTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
FilesystemType	Type of file system on the volume. This field can contain one of the values listed in page FilesystemType.
VolumePath	Path to the volume.
TotalAllocationUnits	Total number of allocation units for the volume.
SectorsPerAllocationUnit	Number of allocation units per sector for the volume.
BytesPerSector	Number of bytes per sector for the volume.
VolumeLabel	Name of the volume
VolumeMountEvent	Event relating to the volume (mounting or unmounting). This field can contain one of the values listed in page UsbVolumeMountEventType.

Event no. 325: End of USB volume scan

AgentInternalUsbVolumeScanSuccess: The agent successfully analyzed a USB volume with the purpose of restoring the trust level.

Field	Meaning
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate.
TrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate.
ScannedFileCount	Number of files analyzed on the USB volume.
QuarantinedFileCount	Number of files detected as quarantined during the analysis of the USB volume.
VolumePath	Path to volume

Event no. 326: USB volume scan error

AgentInternalUsbVolumeScanError: The agent encountered an error during the analysis of a USB volume; the trust level will not be restored.

Field	Meaning
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate.
TrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate.
ErrorCode	Error code of the error encountered during the analysis of the USB volume.
VolumePath	Path to volume
Filepath	Path of the file causing the USB scan error.

Event no. 327: USB volume hash calculation error

AgentInternalUsbVolumeFootprintComputationError: An error occurred while calculating the hash of a USB volume.

Field	Meaning
UsbDeviceInfo	Information about the USB device on which the volume is located. More details on this block in section UsbDeviceInfoTemplate.
TrackingData	Volume tracking data. More details on this block in section UsbVolumeTrackingDataTemplate.
ErrorCode	Error code of the error encountered during the calculation of the USB volume's hash.
VolumePath	Path to volume

Event no. 361: Bluetooth

AgentOperationBluetoothAccess: A Bluetooth radio (Bluetooth device that listens on connections) on the agent received a connection request from a third-party Bluetooth device.

Field	Meaning
ConnectedDeviceInfo	Information on the device that is logging in. More details on this block in section BluetoothDeviceInfoTemplate.
LocalRadioDeviceInfo	Information on the local radio to which the device is logging in. More details on this block in section BluetoothDeviceInfoTemplate.
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.

Event no. 400: Wi-Fi network

AgentOperationWifiAccessConnectedNetwork: The agent detected access to a WiFi network.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
ConnectionMode	WiFi connection mode This field can contain combined binary values listed in section WifiConnectionMode.
AuthAlgo	Type of WiFi authentication. This field can contain combined binary values listed in section WifiAuthAlgo.
Ssid	Name of the WiFi network.
RemoteMacAddress	Remote MAC address (address of the access point in Infrastructure mode, or address generated by the host in ad hoc connection mode).

Event no. 401: Wi-Fi feature

AgentOperationWifiAccessFunctionnality: The agent detected access to the WiFi feature.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.

Event no. 1000: System logs lost

AgentInternalLostBuffers: The agent lost logs.

Field	Meaning
LostBuffersCount	Number of logs lost.

Event no. 1006: Temporary web access started

AgentInternalTemporaryWebAccessStart: Temporary web access started.

Field	Meaning
User	ID of the user who requested the start of the temporary web access. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
Duration	Duration of the temporary web access.

Event no. 1007: Temporary web access failed to start

AgentInternalTemporaryWebAccessStartFailed: temporary web access failed to start.

Field	Meaning
User	ID of the user who requested the start of the temporary web access. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
ErrorCode	Error code corresponding to the error encountered when starting the temporary web access.

Event no. 1008: Temporary web access stopped

AgentInternalTemporaryWebAccessStop: temporary web access ended.

Field	Meaning
User	ID of the user who requested the shutdown of the temporary web access. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 1009: Failed to stop temporary web access

AgentInternalTemporaryWebAccessStopFailed: Temporary web access failed to stop.

Field	Meaning
User	ID of the user who requested the shutdown of the temporary web access. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
ErrorCode	Error code corresponding to the error encountered when shutting down the temporary web access.

Event no. 1010: Failed to generate system log

AgentInternalLogExceedMaxSize: Description generated when a log could not be issued due to its large size.

Field	Meaning
FaultyLogType	Type of the log that could not be issued This field can contain one of the values listed in page LogType.

Event no. 1011: Maximum number of temporary web accesses reached

AgentInternalTemporaryWebAccessMaxCountReached: The maximum number of temporary web access logins has been reached.

Field	Meaning
User	ID of the user who requested the start of the temporary web access. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 1013: Start of log flooding

AgentFloodStart: Log flooding start log.

Field	Meaning
FloodID	Log flooding ID.
FloodStartTime	Information about the start of log flooding.
FloodInformation	Information about the log causing log flooding. More details on this block in section AgentFloodInformationTemplate.

Event no. 1014: End of log flooding

AgentFloodStop: Log flooding end log.

Field	Meaning
FloodID	Log flooding ID.
FloodStartTime	Information about the start of log flooding.
FloodStopTime	Log flooding end date.
FloodTotalGeneratedLogs	Number of logs generated by this log flooding.
FloodInformation	Information about the log causing log flooding. More details on this block in section AgentFloodInformationTemplate.

Event no. 20003: New policy

AgentInternalNewPolicyNotification: The agent applied a new policy.

Field	Meaning
PolicyName	Name of policy applied.
PolicyVersion	Version of policy applied.
PolicyGuid	ID of the policy applied, in the form of a GUID.
PolicyVersionInternal	Internal version for diagnosis purposes.

Event no. 20004: The service did not stop correctly

AgentInternalServiceDidNotEndCorrectly: A service on the agent detected that the agent's previous session ended unexpectedly.

Field	Meaning
ServiceName	Name of the service that shut down unexpectedly.

Event no. 20006: Agent update

AgentInternalEndUpgradeAgentSucceeded: Agent software upgrade operation successful.

Field	Meaning
VersionFrom	Version of the agent before upgrade.
VersionTo	Version of the agent present on the machine after upgrade

Event no. 20007: Agent update failed

AgentInternalEndUpgradeAgentFailed: Agent software upgrade operation failed.

Field	Meaning
VersionFrom	Version of the agent before upgrade.
VersionTo	Version of the agent present on the machine after upgrade
ErrorCode	Error code associated with the failed agent software upgrade.

Event no. 20008: Error while applying the policy

AgentInternalNewPolicyErrorNotification: The agent could not apply a new policy.

Field	Meaning
PolicyName	Name of the policy that could not be applied.

Event no. 20009: Hive package

AgentInternalInvalidHivePackage: The agent received invalid policy data.

Field	Meaning
HivePackageFullPath	Full path to the file containing policy data in registry hive format.
LoadingOperationStatus	Error code associated with an attempt to load policy data.

Event no. 20010: Starting agent uninstallation

AgentInternalStartUninstallAgent: The agent starts uninstalling.

Event no. 20011: Agent uninstall

AgentInternalEndUninstallAgentSucceeded: Agent uninstall operation successful.

Event no. 20012: Agent uninstall failed

AgentInternalEndUninstallAgentFailed: Agent uninstall operation failed.

Event no. 20013: Invalid policy package CAB file

AgentInternalInvalidPolicyPackageCab: The agent could not validate a CAB file containing policies.

Field	Meaning
PolicyPackageCabFullPath	Full path to the CAB file containing policies.
LoadingOperationStatus	Error code associated with an attempt to load the CAB file containing policies.

Event no. 20015: Kernel corruption detected

AgentInternalKernelCorruptionBugcheck: The agent restarted after a blue screen due to corrupted kernel structures.

Field	Meaning
Bugcheck	Detailed information on the blue screen event.

Event no. 20016: Invalid policy package signature

AgentInternalInvalidPolicyPackageSignature: The agent could not validate the signature of a CAB file containing policies.

Field	Meaning
StatusCode	Status of the signature verification.
PolicyPackageFile	Path to the CAB file containing policies.

Event no. 20017: Starting agent update

AgentInternalStartAgentUpgrade: The agent starts applying an upgrade.

Field	Meaning
AgentUpgradeType	Origin of the upgrade (standalone or from server) This field can contain one of the values listed in page AgentUpgradeType.
UpgradeForced	The upgrade has been forced

Event no. 20018: The signature of the policy package has expired

AgentInternalPolicyPackageSignerExpired: Some items have expired in the signature certificate validation chain for the CAB file that contains policies.

Field	Meaning
PolicyPackageFile	Path to the CAB file containing policies.

Event no. 20019: The LRPC self-protection failed

AgentInternalSelfProtectionLrpcFailure: The self-protection module that validates the agent's inter-module communications encountered a failure.

Field	Meaning
ServerServiceName	Name of the module that detected the failure. This module acts as a communication server and could not verify the identity of another module that attempted to contact it.
SelfProtectionModuleName	Name of the faulty self-protection module.
StatusCode	Error code returned by the module that detected the failure.

Event no. 20020: Policy application error after update

AgentInternalNewPolicyFromUpdateErrorNotification: The agent could not apply a new policy received together with a software upgrade.

Field	Meaning
PolicyName	Name of policy applied.

Event no. 20021: New policy applied after update

AgentInternalNewPolicyFromUpdateNotification: The agent applied a new policy received together with a software update.

Field	Meaning
PolicyName	Name of policy applied.
PolicyVersion	Version of policy applied.
PolicyGuid	GUID of policy applied.
PolicyVersionInternal	Internal version for diagnosis purposes.

Event no. 20022: Configuration application

AgentInternalNewConfigurationNotification: The agent applied a new configuration.

Event no. 20023: Configuration application error

AgentInternalNewConfigurationErrorNotification: The agent could not apply a new configuration.

Field	Meaning
StatusCode	Error code.

Event no. 20024: Error applying configuration for new version

AgentInternalNewConfigurationFromUpdateErrorNotification: The agent could not apply a new configuration received together with a software upgrade.

Event no. 20025: New configuration applied for new version

AgentInternalNewConfigurationFromUpdateNotification: The agent scheduled the application of a new configuration together with a software upgrade.

Event no. 20026: Invalid configuration package CAB file

AgentInternalInvalidConfigurationPackageCab: Application of new agent configuration failed.

Field	Meaning
PackageCabFullPath	Path to the CAB file containing the configuration that could not be loaded.
LoadingOperationStatus	Result of loading operation.

Event no. 20027: Downgrading to an older agent version is not allowed

AgentInternalDowngradeIsNotAuthorized: The agent received a software upgrade from a lower version to its current version, but did not apply it as the configuration prohibited it.

Event no. 20028: Safe mode login

AgentInternalSafeModeSessionNotification: A session was opened in safe mode.

Field	Meaning
Timestamp	Date and time the session was opened.
LoginName	Domain name and user of the opened session.

Event no. 20030: Maintenance mode is enabled

AgentInternalMaintenanceModeStart: Maintenance mode is enabled.

Field	Meaning
User	ID of the user who requested Maintenance mode. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20031: Maintenance mode is disabled

AgentInternalMaintenanceModeStop: Maintenance mode is disabled.

Event no. 20032: Agent update not applied

AgentInternalMaintenanceModeAgentUpgradePostponed: The agent detected that a software update is available on the server, but was not applied immediately as the agent is in Maintenance mode

Event no. 20033: Shutting down the Base Filtering Engine service (BFE)

AgentInternalBfeIsStoppedNotification: The agent detected that the Base Filtering Engine (BFE) was shut down.

Event no. 20034: Repair failed

AgentInternalRepairFailureNotification: Description of the failed repair.

Field	Meaning
User	ID of the user who requested the repair. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
Result	Result of a failed repair.

Event no. 20035: End of repair

AgentInternalRepairSuccessNotification: Description of the successful repair.

Field	Meaning
User	ID of the user who requested the repair. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20036: Unable to modify active features

AgentInternalEndAgentModularityFailed: Information relating to the failure when enabling or disabling one or several modules on the agent.

Field	Meaning
ErrorCode	Error code relating to the failure when enabling or disabling one or several modules on the agent.

Event no. 20037: Modifying the active features

AgentInternalEndAgentModularitySucceeded: Log indicating that one or several modules on the agent has/have been enabled or disabled.

Event no. 20038: Unable to communicate with the server

AgentInternalCommFinishFailedState: Agent-server communication has encountered an irrecoverable error

Field	Meaning
ErrorCode	Error code returned by the last status function executed.
StateName	Name of the last valid status of the status host
State	Index of the last valid status of the status host

Event no. 20039: Applying a forced update

AgentInternalForcedPatchApplication: A forced update was installed on the agent.

Event no. 20040: Starting the challenge

AgentInternalChallengeStart: A challenge has started on the agent.

Field	Meaning
Duration	Duration of the challenge which is starting now. This field can contain one of the values listed in page ChallengeDuration.
Options	Challenge options, such as tracing. The value of this field depends on the type of challenge.
ChallengeAction	Action corresponding to the started challenge. This field can contain one of the values listed in page ChallengeActionMap.

Event no. 20041: End of challenge

AgentInternalChallengeStop: A challenge has been stopped on the agent.

Field	Meaning
ChallengeAction	Action corresponding to the stopped challenge. This field can contain one of the values listed in page ChallengeActionMap.
Manual	Indicates if the challenge was stopped manually or automatically.
User	SID of the user who requested to stop the challenge. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20042: Ending the challenge failed

AgentInternalChallengeStopFailure: A challenge failed to stop.

Field	Meaning
ErrorCode	A challenge failed to stop.

Event no. 20043: Wrong version of the installation packet

AgentInternalWrongCabinetVersion: The version of the .cab file is different from the agent's current version.

Event no. 20044: Several interfaces match a network test

AgentInternalMultipleNetworkInterfacesMatchingTest: Several network interfaces may match a conditional policy test.

Field	Meaning
InterfaceName	Na of the interface as specified in the network test.
InterfaceDescription	Description of the interface as specified in the network test.

Event no. 20045: Starting the challenge failed

AgentInternalChallengeStartFailure: A challenge failed to start.

Field	Meaning
ErrorCode	Error code returned when a challenge failed to start.

Event no. 20048: External event

AgentOperationExternal: Description of the external event received by the agent.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Description	Message of the external event received by the agent.
OriginType	Where the external event received by the agent comes from.
ExtraData	Data extracted from the external event received by the agent.
Fields	Description of the rule fields getting the log. More details on this block in section AgentFieldsTemplate.

Event no. 20049: Maximum number of challenge attempts reached

AgentInternalChallengeTooManyFailedAttempts: A challenge was canceled after too many codes were tried.

Field	Meaning
User	SID of the user who last entered an incorrect challenge response. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20050: Modification of active functions postponed

AgentInternalMaintenanceModeAgentModularityPostponed: The agent detected new active features on the server, but they were not applied immediately as the agent is in Maintenance mode.

Event no. 20051: Agent update not necessary

AgentInternalEndUpgradeAgentNothingToDo: The software update has been stopped. The agent is already up to date.

Event no. 20052: Agent Guid update

AgentInternalEndUpgradeAgentGuidUpdated: The agent GUID has been updated.

Event no. 20053: Maintenance mode exit error

AgentInternalMaintenanceModeStopFailed: Return to normal protection mode failed.

Field	Meaning
ErrorCode	Error code that prevented Maintenance mode from shutting down.

Event no. 20054: Kerberos ticket

AgentOperationKerberosPassTheTicket: Detail block generated when the agent detects Mimikatz stealing a Kerberos ticket.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
SourceProcess	Details about the process that is performing the operation.
KirbiFileFullPath	Full path to the Kirbi file generated by Mimikatz.

Event no. 20055: ARP spoofing

AgentOperationArpSpoofing: Description generated when the agent detects an ARP spoofing attack.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
IPInterface	Interface containing the spoofed IP address.
SpoofedIP	Spoofed IP address.
OldMacAddress	MAC address before the IP address was spoofed.
SpoofedMacAddress	MAC address with which the IP address was spoofed.

Event no. 20056: Malicious use of the certutil decoding parameter

AgentOperationCertutilDecodeMaliciousUsage: Description generated when the agent detects malicious use of Microsoft program certutil to decode a file.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
SourceProcess	Information on certutil.
ParentProcess	Source process of the action that used certutil.
SourceFilePath	Path to the file to decode.
DestinationFilePath	Path to decoded file.
FileContentType	File type detected. This field can contain one of the values listed in page CertutilDecodedFileType.
FileContent	File contents (limited to the first 80 bytes maximum).

Event no. 20057: Malicious use of certutil download

AgentOperationCertutilDownloadMaliciousUsage: Description generated when the agent detects malicious use of Microsoft program certutil to download a file.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
SourceProcess	Information on certutil.
ParentProcess	Source process of the action that used certutil.
DownloadUrl	URL used to download the target file.
DestinationFilePath	Path to downloaded file.

Event no. 20059: Error while running script

AgentInternalScriptRuntimeError: Description generated when an execution error occurs in a script.

Field	Meaning
ExecutionStatus	Error code relating to script execution.
ScriptGuid	GUID of failed script.

Event no. 20060: WMI Persistence

AgentOperationWmiPersistence: Description generated when the agent detects a WMI persistence attack.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
ConsumerType	Type of consumer related to a WMI event. This field can contain one of the values listed in page WmiPersistenceConsumerTypeMap.
ExecutedAction	Command line or content of the script used by WMI.
ActionName	Name of the consumer or action used by WMI.
Trigger	WMI trigger conditions.
Namespace	WMI-related space name.
ESS	WMI-related ESS.
Consumer	Consumer for the WMI recording.
PossibleCause	Possible cause for the WMI event triggering.
TimeCreated	Date and time when the event log related to WMI triggering was created.

Event no. 20061: Discovery

AgentOperationDiscovery: Environment discovery log

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
SourceProcess	Discovery source process
DiscoveryProcess	Discovery process
BeginningTime	Start date
TriggerTime	Triggering date and time

Event no. 20062: Uninstalling the agent is not allowed.

AgentInternalUninstallForbidden: Description generated when the agent uninstallation was blocked by the policy.

Field	Meaning
User	SID of the user who tried to uninstall Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
UninstallAttemptDateTime	Date and time of uninstallation attempt

Event no. 20064: Apply features on the agent

AgentInternalStartModularityAgent: The agent is applying the features

Event no. 20065: Starting agent repair

AgentInternalStartRepairAgent: The agent starts repairing

Field	Meaning
User	User who started agent repair Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20066: Missing shadow copy storage space

AgentInternalVolumeWithoutShadowStorage: Shadow copies cannot be created on the volume because there is no storage space for them.

Field	Meaning
VolumePath	Path to volume
DriveLetter	Drive letter for the volume if there is one
VolumeLabel	Volume description

Event no. 20067: Snapshot creation failed

AgentInternalShadowCopyCreationFailure: Unable to create the shadow copy

Field	Meaning
VolumePath	Path to volume
DriveLetter	Drive letter for the volume if there is one
VolumeLabel	Volume description
ErrorCode	Code or the error

Event no. 20068: Ransomware

AgentOperationRansomware: Ransomware behavior has been detected.

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
SourceProcess	Ransomware source process
AlteredFileListFilePath	Path to the file containing the list of files encrypted by the ransomware
OverallAlteredFilesCount	Number of files encrypted by the ransomware
AlteredFiles	Paths to the first 10 files encrypted by the ransomware More details on this block in section RenamedFilesRendering.

Event no. 20069: Error while downloading a resource

AgentInternalResourcePackageDownloadFailed: Detail block generated when an attempt to download a resource file from the agent handler failed.

Field	Meaning
StatusCode	Error code encountered while downloading the file
ResourceGuid	Unique ID of the resource that failed to download

Event no. 20070: Resource signature verification error

AgentInternalInvalidResourcePackageSignature: Detail block generated when the agent was unable to validate the digital signature of a cabinet file containing a policy resource

Field	Meaning
StatusCode	Error code encountered while verifying the signature
ResourceGuid	Unique ID of the resource for which the signature verification failed
ResourcePackageFile	Full path of the resource file for which the signature verification failed

Event no. 20071: SecOps signature verification failed

AgentInternalSecOpsInvalidPackageSignature: Detail block generated when the agent was unable to validate the digital signature of a cabinet file containing a scan task

Field	Meaning
StatusCode	Error code returned while verifying the signature
SecOpsGuid	Unique ID of the task for which the signature verification failed
SecOpsPackageFile	Full path of the task file for which the signature verification failed

Event no. 20072: SecOps request validation failed

AgentInternalSecOpsInvalidJsonSize: Detail block generated when the size of the JSON file describing a scan task is invalid

Field	Meaning
StatusCode	Error code returned while verifying the JSON file of the scan task
SecOpsGuid	Unique ID of the task for which the JSON file is invalid
SecOpsPackageFile	Full path of the scan task file for which the size of the JSON file is invalid
JsonSize	Size of the scan task JSON file with an invalid size

Event no. 20073: Downgrading to an older intermediate version is required

AgentInternalDowngradeWithPivotVersion223IsRequired: The agent received a software update from a version lower than 2.2.3. The agent must be updated to version 2.2.3 before it can be updated to a lower version.

Event no. 20079: Yara process scan

AgentOperationYaraProcessAnalysisMatch: Detail block generated for each Yara pattern (process) detection rule

Field	Meaning
SourceProcess	Process involved in the detection operation
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
SourceProcessImageFileDetails	Details on the image file of the process that was scanned More details on this block in section AgentOperationYaraAnalysisFilesDetailsTemplate.
MatchedYaraRules	Detail block regarding Yara rules that allowed detection More details on this block in section AgentOperationYaraRuleInformationTemplate.

Event no. 20080: Yara file scan

AgentOperationYaraFileAnalysisMatch: Detail block generated for each Yara pattern detection rule on a file

Field	Meaning
SourceProcess	Process involved in the detection operation
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
FileDetails	Details on the file involved during detection More details on this block in section AgentOperationYaraAnalysisFilesDetailsTemplate.
SourceProcessImageFileDetails	Details on the image file of the process that interacted with the file More details on this block in section AgentOperationYaraAnalysisFilesDetailsTemplate.
MatchedYaraRules	Detail block regarding Yara rules that allowed detection More details on this block in section AgentOperationYaraRuleInformationTemplate.

Event no. 20081: Yara file scan (no source processes)

AgentOperationYaraFileAnalysisMatchNoSourceProcess: Detail block generated for each Yara pattern detection rule on a file

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
FileDetails	Details on the file involved during detection More details on this block in section AgentOperationYaraAnalysisFilesDetailsTemplate.
MatchedYaraRules	Detail block regarding Yara rules that allowed detection More details on this block in section AgentOperationYaraRuleInformationTemplate.

Event no. 20082: Parent PID spoofing

AgentOperationPpidSpoofing: PPID spoofing protection

Field	Meaning
Action	Action performed by the agent. More details on this block in section AgentActionTemplate.
Correlation	Data related to the advanced protection More details on this block in section AgentCorrelationTemplate.
SourceProcess	Process from which the Parent PID Spoofing attack originated
ParentProcess	Process behind which the source process attempted to hide during the Parent PID Spoofing attack
CreatedProcess	Process created by the source process during the Parent PID Spoofing attack
Description	Description of the Parent PID Spoofing attack

Event no. 20083: Starting agent integrity check

AgentInternalIntegrityStart: Detail block for launching a solution component check.

Field	Meaning
User	Identification of the user who initiated the integrity check. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20084: End of agent integrity check

AgentInternalIntegritySuccessNotification: Detail block regarding the success of solution component integrity checks.

Field	Meaning
User	Identification of the user who initiated the integrity check. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Event no. 20085: End of repair requiring restart

AgentInternalRepairSuccessWithRebootNotification: Detail block about a successful repair that requires the workstation to be restarted

Field	Meaning
User	ID of the user who requested the repair. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
FileErrors	Number of differences in files, detected during the integrity check
DirectoryErrors	Number of differences in folders, detected during the integrity check
RegistryValueErrors	Number of differences in registry values, detected during the integrity check
RegistryKeyErrors	Number of differences in registry keys, detected during the integrity check
ServiceErrors	Number of differences in services, detected during the integrity check
DriverErrors	Number of differences in drivers, detected during the integrity check
EventLogErrors	Number of differences in event logs, detected during the integrity check
PerfCounterErrors	Number of differences in performance counters, detected during the integrity check
WfpCalloutErrors	Number of differences in WFP callouts, detected during the integrity check
WfpFilterErrors	Number of differences in WFP filters, detected during the integrity check
WfpProviderErrors	Number of differences in WFP providers, detected during the integrity check
WfpSublayerErrors	Number of differences in WFP sublayers, detected during the integrity check
DefenderExceptionErrors	Number of differences in registry values detected during the integrity check
WmiNamespaceErrors	Number of errors on WMI namespace elements
WmiProviderErrors	Number of errors on WMI provider elements
WmiClassErrors	Number of errors on WMI class elements

Event no. 20086: Repair successful, restart not required

AgentInternalRepairSuccessWithoutRebootNotification: Detail block about a successful repair that requires the workstation to be restarted

Field	Meaning
User	ID of the user who requested the repair. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
FileErrors	Number of differences in files, detected during the integrity check
DirectoryErrors	Number of differences in folders, detected during the integrity check
RegistryValueErrors	Number of differences in WFP sublayers, detected during the integrity check
RegistryKeyErrors	Number of differences in registry keys, detected during the integrity check
ServiceErrors	Number of differences in services, detected during the integrity check
DriverErrors	Number of differences in drivers, detected during the integrity check
EventLogErrors	Number of differences in event logs, detected during the integrity check
PerfCounterErrors	Number of differences in performance counters, detected during the integrity check
WfpCalloutErrors	Number of differences in WFP callouts, detected during the integrity check
WfpFilterErrors	Number of differences in WFP filters, detected during the integrity check
WfpProviderErrors	Number of differences in WFP providers, detected during the integrity check
WfpSublayerErrors	Number of differences in WFP sublayers, detected during the integrity check
DefenderExceptionErrors	Number of differences in Windows Defender exclusions detected during the integrity check.
WmiNamespaceErrors	Number of errors on WMI namespace elements
WmiProviderErrors	Number of errors on WMI provider elements
WmiClassErrors	Number of errors on WMI class elements

Event no. 20087: Agent integrity check failed

AgentInternalIntegrityErrorNotification: Detail block regarding the failed solution component integrity check.

Field	Meaning
User	Identification of the user who initiated the integrity check. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
Result	Result of a failed integrity check.

Event no. 20089: File deletion by remediation

AgentRemediationRemoveFile: Result of the remediation operation Delete file

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	File to delete

Event no. 20090: Process stop

AgentRemediationKillProcess: Result of the remediation operation Shut down process.

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Image of processes to be shut down
ProcessPID	PID of process to be shut down
KillChildren	Operation parameter

Event no. 20091: Delete registry key by remediation

AgentRemediationRemoveRegistryKey: Result of the remediation operation Delete registry key

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Registry key to be deleted

Event no. 20092: Delete registry value by remediation

AgentRemediationRemoveRegistryValue: Result of the remediation operation Delete registry value

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Path of the registry value to be deleted
TargetResourceName	Name of the registry value to be deleted

Event no. 20093: Registry value writing through remediation

AgentRemediationSetRegistryValue: Result of the remediation operation Set registry value

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Registry value to be modified
TargetResourceName	Name of the value to set

Event no. 20094: Run script

AgentRemediationExecutePowershellScript: Result of the remediation operation Run Powershell script

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
ScriptName	Script name
ScriptGuid	Script GUID
ScriptExitCode	Script return code
ScriptOutputFilePath	Name of script log file
ScriptOutput	Script log extract

Event no. 20095: Retrieve files from a shadow copy

AgentRemediationExtractFilesFromShadowCopy: Result of the remediation operation Extract backup files from a shadow copy

Field	Meaning
RemediationSpecificData	Information relating to the remediation operation More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Path of the restoration log
RestoredFilesCount	Number of files restored
OverallAlteredFilesCount	Total number of files altered during ransomware attack
RestoredFiles	First 10 files restored

Event no. 20097: IoC on a named object

AgentOperationIocAnalysisNamedObjectMatch: Detail block generated for each IoC detection rule in the namespace of the system's named objects

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
ObjectType	Type of object that triggered detection This field can contain one of the values listed in page IocNamedObjectType.
ObjectFullPath	Full path to object
MatchedStrings	Indicators that allowed object match More details on this block in section AgentOperationIocMatchedStringTemplate.

Event no. 20098: Event log match

AgentOperationIocAnalysisEventLogMatch: Detail block generated for each IoC detection rule in event logs

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
Channel	Channel of logs associated with detection
ProviderName	Provider that generated log
EventTypeId	Unique ID of event logs
EventTimestamp	Date and time event logs were generated
EventXml	Raw data in XML format representing the event
EventDetails	Details associated with the event
MatchedStrings	Indicators that allowed event match More details on this block in section AgentOperationIocMatchedStringTemplate.

Event no. 20099: IoC on a file name

AgentOperationIocAnalysisFilenameMatch: Detail block generated for each IoC detection rule in the namespace of the system's file names

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
SourceProcess	Process involved in the detection operation
FullPath	Full path to file
MatchedStrings	Indicators that allowed file name match More details on this block in section AgentOperationIocMatchedStringTemplate.

Event no. 20100: IoC on a file name (no source process)

AgentOperationIocAnalysisFilenameMatchNoSourceProcess: Detail block generated for each IoC detection rule in the namespace of the system's file names

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
FullPath	Full path to file
MatchedStrings	Indicators that allowed file name match More details on this block in section AgentOperationIocMatchedStringTemplate.

Event no. 20101: IoC on a DNS request

AgentOperationIocAnalysisDnsRequestMatch: Detail block generated for each IoC detection rule in DNS request log

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
DnsRequestTimestamp	Date and time entry was generated in the DNS request log
DnsRequest	Full DNS request
MatchedStrings	Indicators that allowed DNS request match More details on this block in section AgentOperationIocMatchedStringTemplate.

Event no. 20105: IoC on a file hash

AgentOperationIocFileSearchByHashFile: Detail block generated every time a file matching a hash IoC is detected

Field	Meaning
Action	Information on the action taken by the agent following detection. More details on this block in section AgentActionTemplate.
AnalysisProperties	Information on scan properties. More details on this block in section AgentAnalysisPropertiesTemplate.
FileDetails	Details on the file matching the hash More details on this block in section AgentOperationIocFileSearchDetailsTemplate.
SearchMatchInformation	Information on a match More details on this block in section AgentOperationIocFileSearchMatchInformationTemplate.

Event no. 20106: IoC on the hash of a process image file

AgentOperationIocFileSearchByHashProcess: Detail block generated every time the image file of a process matching a hash IoC is detected

Field	Meaning
Action	Information on the action taken by the agent following detection. More details on this block in section AgentActionTemplate.
AnalysisProperties	Information on scan properties. More details on this block in section AgentAnalysisPropertiesTemplate.
SourceProcessImageFileDetails	Details of the image file matching the hash More details on this block in section AgentOperationIocFileSearchDetailsTemplate.
SearchMatchInformation	Information on a match More details on this block in section AgentOperationIocFileSearchMatchInformationTemplate.
SourceProcess	Information on the source process.

Event no. 20107: IoC in the memory of a process

AgentOperationIocAnalysisTextualSearchProcessMatch: Detail block generated for each text IoC detection rule the type in a process memory

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
SourceProcess	Process involved in the detection operation
SourceProcessImageFileDetails	Details on the image file of the process that was scanned
MatchedStrings	Indicator that allowed memory match

Event no. 20108: IoC in the file of a process

AgentOperationIocAnalysisTextualSearchFileMatch: Detail block generated for each text IoC detection rule in a given file

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
SourceProcess	Process involved in the detection operation
SourceProcessImageFileDetails	Details on the image file of the process that was scanned
FileDetails	Details on the file that was scanned
MatchedStrings	Indicators that allowed the match in the file

Event no. 20109: IoC in the file of a process (no source process)

AgentOperationIocAnalysisTextualSearchFileMatchNoSourceProcess: Detail block generated for each text IoC detection rule in a given file

Field	Meaning
Action	Information about action taken by the agent after detection More details on this block in section AgentActionTemplate.
AnalysisProperties	Information about scan properties More details on this block in section AgentAnalysisPropertiesTemplate.
FileDetails	Details on the file that was scanned
MatchedStrings	Indicators that allowed the match in the file

Event no. 20111: Unable to open file to be monitored

AgentInternalFileMonitorOpenCursorFailure: Information concerning the failure to open a file that is supposed to be monitored.

Field	Meaning
DirectoryPath	Path to the directory containing the file.
FileName	File name.

Event no. 20112: Update download error

AgentInternalUpdateDownloadFailed: The agent was unable to download the update.

Field	Meaning
ErrorCode	Error code associated with failure to download agent software update.

Event no. 20113: Isolate computers

AgentRemediationIsolateComputer: An isolation request was received.

Field	Meaning
RemediationSpecificData	Information relating to the remediation action. More details on this block in section AgentRemediationSpecificDataTemplate.
ActionDateTime	Timestamp of the isolation action.

Event no. 20114: Undo computer isolation

AgentRemediationComputerIsolationLeave: An isolation stop request was received.

Field	Meaning
RemediationSpecificData	Information relating to the remediation action. More details on this block in section AgentRemediationSpecificDataTemplate.
ActionDateTime	Isolation stop timestamp.

Event no. 20116: File quarantined by the security policy

AgentFileQuarantinedFromProtectionRule: An attempt was made to automatically quarantine a file.

Field	Meaning
Result	Result of the quarantine attempt (success or failure).
ProtectionRuleDetails	Details of the scheduled scan that caused the quarantine. More details on this block in section AgentFileQuarantineRuleDetailsTemplate.
FilePath	Path of the quarantined file.
FileCreationTime	Creation date of the quarantined file.
FileModificationTime	Last modification date of the quarantined file.
FileSize	Size of the quarantined file.
FileOwner	ID of the owner of the quarantined file. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
QuarantineObjectId	ID of the file once quarantined.

Event no. 20117: File restored from quarantine

AgentFileRestoredFromQuarantine: An attempt has been made to restore a file from quarantine.

Field	Meaning
RemediationSpecificData	Details of the task causing the quarantine to stop. More details on this block in section AgentRemediationSpecificDataTemplate.
QuarantineObjectId	ID of the quarantined file.
FilePath	Path of the restored file.

Event no. 20118: Delete quarantined file

AgentFileRemovedFromQuarantine: An attempt was made to permanently delete a quarantined file.

Field	Meaning
Result	Result of the deletion attempt (success or failure).
QuarantineObjectId	ID of the quarantined file.
FilePath	Path of the original file when it was quarantined.

Event no. 20119: File quarantined upon request

AgentFileQuarantinedFromSecOpsTask: A file quarantine attempt was made at the request of the security administrator.

Field	Meaning
RemediationSpecificData	Details of the remediation task that caused the quarantine. More details on this block in section AgentRemediationSpecificDataTemplate.
FilePath	Path of the quarantined file.
FileCreationTime	Creation date of the quarantined file.
FileModificationTime	Last modification date of the quarantined file.
FileSize	Size of the quarantined file.
FileOwner	ID of the owner of the quarantined file. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
QuarantineObjectId	ID of the file once quarantined.

Event no. 20120: File restored from quarantine through updated exclusion

AgentFileRestoredFromQuarantineByExclusionUpdate: Details of the quarantine stop triggered by updated exclusion rules.

Field	Meaning
Result	Return code of the attempt to restore the quarantined file.
QuarantineObjectId	ID of the file restored from quarantine.
FilePath	Initial path of the file restored from quarantine.

Event no. 20121: Agent installation reference file missing

AgentInternalAgentPatchMissing: The agent's installation credentials or proof of authenticity are not present on the disk. The agent will attempt to restore them by requesting an update package from the agent handler if necessary.

Field	Meaning
SoftwareVersion	Software version.
CabMissing	Indicates whether the installation repository is missing.
Pkcs7Missing	Indicates whether the proof of authenticity of the installation repository is missing.

Event no. 20122: The agent installation reference file has been restored

AgentInternalAgentPatchRecovered: The agent installation repository has been restored and validated.

Field	Meaning
SoftwareVersion	Software version.

Event no. 20123: Agent installation reference file restore failed

AgentInternalAgentPatchNotRecovered: The agent installation repository could not be restored. To restore the agent's health status, it may be necessary to place it in an agent group corresponding to its current software version.

Field	Meaning
SoftwareVersion	Software version.

Event no. 20125: File quarantined by scheduled scan

AgentFileQuarantinedFromScheduledTask: A scheduled scan triggered an attempt to quarantine a file.

Field	Meaning
RemediationSpecificData	Details of the scheduled scan that caused the quarantine. More details on this block in section AgentRemediationSpecificDataTemplate.
FilePath	Path of the quarantined file.
FileCreationTime	Creation date of the quarantined file.
FileModificationTime	Last modification date of the quarantined file.
FileSize	Size of the quarantined file.
FileOwner	ID of the owner of the quarantined file. Note: This field is an SID. The **FileOwnerNameLookup** and **FileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
QuarantineObjectId	ID of the file once quarantined.

Event no. 20126: Deleting directory

AgentRemediationRemoveDirectory: Result of the "Remove file" remediation action.

Field	Meaning
RemediationSpecificData	Information relating to the remediation action. More details on this block in section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Deletion target folder.

List: AgentUpgradeType

List of possible sources of an agent upgrade.

Digital value	Associated symbol
0	Autonomous
1	ServerDistribution

List: BluetoothMajorDeviceClass

List of major device classes for Bluetooth devices.

Digital value	Associated symbol
0	MADC_MISCELLANEOUS
1	MADC_COMPUTER
2	MADC_PHONE
3	MADC_LAN_ACCESS_POINT
4	MADC_AUDIO_VIDEO
5	MADC_PERIPHERAL
6	MADC_IMAGING
7	MADC_WEARABLE
8	MADC_TOY
9	MADC_HEALTH
31	MADC_UNCATEGORIZED

Binary field: BluetoothMajorServiceClass

List of major service classes for Bluetooth devices.

Binary value	Associated symbol
0x00000001	MSC_LIMITED_DISCOVERABLE_MODE
0x00000008	MSC_POSITIONING
0x00000010	MSC_NETWORKING
0x00000020	MSC_RENDERING
0x00000040	MSC_CAPTURING
0x00000080	MSC_OBJECT_TRANSFERT
0x00000100	MSC_AUDIO
0x00000200	MSC_TELEPHONY
0x00000400	MSC_INFORMATION

List: BluetoothMinorDeviceClassAudioVideo

List of minor device classes for Bluetooth devices in the 'audio/video' major device class.

Digital value	Associated symbol
0	MIDC_UNCATEGORIZED
1	MIDC_WEARABLE_HEADSET
2	MIDC_HANDS_FREE_DEVICE
4	MIDC_MICROPHONE
5	MIDC_LOUDSPEAKER
6	MIDC_HEADPHONES
7	MIDC_PORTABLE_AUDIO
8	MIDC_CAR_AUDIO
9	MIDC_SET_TOP_BOX
10	MIDC_HIFI_AUDIO_DEVICE
11	MIDC_VCR
12	MIDC_VIDEO_CAMERA
13	MIDC_CAMCORDER
14	MIDC_VIDEO_MONITOR
15	MIDC_VIDEO_DISPLAY_LOUDSPEAKER
16	MIDC_VIDEO_CONFERENCING
18	MIDC_GAMING_TOY

List: BluetoothMinorDeviceClassComputer

List of minor device classes for Bluetooth devices in the 'computer' major device class.

Digital value	Associated symbol
0	MIDC_UNCATEGORIZED
1	MIDC_DESKTOP_WORKSTATION
2	MIDC_SERVER_CLASS_COMPUTER
3	MIDC_LAPTOP
4	MIDC_HANDLED_PC_PDA
5	MIDC_PALM_SIZED_PC_PDA
6	MIDC_WEARABLE_COMPUTER

Binary field: BluetoothMinorDeviceClassImaging

List of minor device classes for Bluetooth devices in the 'imaging' major device class.

Binary value	Associated symbol
0x00000001	MIDC_DISPLAY
0x00000002	MIDC_CAMERA
0x00000004	MIDC_SCANNER
0x00000008	MIDC_PRINTER

List: BluetoothMinorDeviceClassNetworkApLoadFactor

List of minor device classes for Bluetooth devices in the 'LAN /Network Access point' major device class.

Digital value	Associated symbol
0	MIDC_FULLY_AVAILABLE
1	MIDC_RANGE_1
2	MIDC_RANGE_2
3	MIDC_RANGE_3
4	MIDC_RANGE_4
5	MIDC_RANGE_5
6	MIDC_RANGE_6
7	MIDC_NO_SERVICE_AVAILABLE

List: BluetoothMinorDeviceClassPeripheralMajor

List of minor device classes for Bluetooth devices in the 'peripheral' major device class.

Digital value	Associated symbol
0	MIDC_NOT_KEYBOARD_POINTING_DEVICE
1	MIDC_KEYBOARD
2	MIDC_POINTING_DEVICE
3	MIDC_COMBO_KEYBOARD_POINTING_DEVICE

List: BluetoothMinorDeviceClassPeripheralMinor

List of minor device classes for Bluetooth devices in the 'peripheral' major device class.

Digital value	Associated symbol
0	MIDC_UNCATEGORIZED
1	MIDC_JOYSTICK
2	MIDC_GAMEPAD
3	MIDC_REMOTE_CONTROL
4	MIDC_SENSING_DEVICE
5	MIDC_DIGITIZER_TABLET
6	MIDC_CARD_READER

List: BluetoothMinorDeviceClassPhone

List of minor device classes for Bluetooth devices in the 'phone' major device class.

Digital value	Associated symbol
0	MIDC_UNCATEGORIZED
1	MIDC_CELLULAR
2	MIDC_CORDLESS
3	MIDC_SMARTPHONE
4	MIDC_WIRED_MODEM_VOICE_GATEWAY
5	MIDC_COMMON_ISDN_ACCESS

List: BluetoothMinorDeviceHealth

List of minor device classes for Bluetooth devices in the 'health' major device class.

Digital value	Associated symbol
0	MIDC_UNDEFINED
1	MIDC_BLOOD_PRESSURE
2	MIDC_THERMOMETER
3	MIDC_WEIGHING
4	MIDC_GLUCOSE_METER
5	MIDC_PULSE_OXYMETER
6	MIDC_HEART_PULSE_RATE_MONITOR
7	MIDC_HEALTH_DATA_DISPLAY

List: BluetoothMinorDeviceToy

List of minor device classes for Bluetooth devices in the 'toy' major device class.

Digital value	Associated symbol
1	MIDC_ROBOT
2	MIDC_VEHICLE
3	MIDC_DOLL_ACTION_FIGURE
4	MIDC_CONTROLLER
5	MIDC_GAME

List: BluetoothMinorDeviceWearable

List of minor device classes for Bluetooth devices in the 'wearable' major device class.

Digital value	Associated symbol
1	MIDC_WRIST_WATCH
2	MIDC_PAGER
3	MIDC_JACKET
4	MIDC_HELMET
5	MIDC_GLASSES

List: CDRomOperation

List of operations on an optical disk (in particular CD, DVD and Blu-Ray).

Digital value	Associated symbol
0	READ
1	WRITE

List: CertificateSignatureState

List of possible statuses when the agent verifies an Authenticode signature.

Digital value	Associated symbol
0	Unavailable
1	Trusted
2	NoSignature
3	Expired
4	Revoked
5	Untrusted
6	SecuritySettings
7	BadContent
8	BadSignature

List: CertutilDecodedFileType

Types of files detected for the use of the decode command in certutil.

Digital value	Associated symbol
0	Unknown
1	Certificate
2	PortableExecutable
3	ZipArchive

List: ChallengeActionMap

List of the types of actions for a challenge.

Digital value	Associated symbol
0	MaintenanceMode
1	StopAgent
2	UninstallAgent
3	DiagnosticSession
4	MaxValue

List: ChallengeDuration

List of the types of durations for a challenge.

Digital value	Associated symbol
0	NoDuration
1	FiveMinutes
2	ThirtyMinutes
3	TwoHours
4	OneDay
5	ThreeDays
6	OneWeek
7	TwoWeeks
8	UntilReboot
9	MaxValue

List: EDRBypassMethod

List of workaround methods supported by the agent.

Digital value	Associated symbol
0	NotSpecified
1	HardwareBreakpoint
2	FunctionPatch

Binary field: FileAttributes

List of file attributes.

Binary value	Associated symbol
0x00000001	FILE_ATTRIBUTE_READONLY
0x00000002	FILE_ATTRIBUTE_HIDDEN
0x00000004	FILE_ATTRIBUTE_SYSTEM
0x00000010	FILE_ATTRIBUTE_DIRECTORY
0x00000020	FILE_ATTRIBUTE_ARCHIVE
0x00000040	FILE_ATTRIBUTE_DEVICE
0x00000080	FILE_ATTRIBUTE_NORMAL
0x00000100	FILE_ATTRIBUTE_TEMPORARY
0x00000200	FILE_ATTRIBUTE_SPARSE_FILE
0x00000400	FILE_ATTRIBUTE_REPARSE_POINT
0x00000800	FILE_ATTRIBUTE_COMPRESSED
0x00001000	FILE_ATTRIBUTE_OFFLINE
0x00002000	FILE_ATTRIBUTE_NOT_CONTENT_INDEXED
0x00004000	FILE_ATTRIBUTE_ENCRYPTED
0x00008000	FILE_ATTRIBUTE_INTEGRITY_STREAM
0x00010000	FILE_ATTRIBUTE_VIRTUAL
0x00020000	FILE_ATTRIBUTE_NO_SCRUB_DATA
0x00040000	FILE_ATTRIBUTE_RECALL_ON_OPEN
0x00400000	FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS

List: FileCreateDetailsType

Types of detail blocks regarding file creation operations.

Digital value	Associated symbol
0	FILE_CREATE
1	FILE_CREATE_HARDLINK_DESTINATION
2	FILE_RENAME_DESTINATION
3	FILE_MOVEFILEEX_DESTINATION
4	FILE_SET_OWNER_DESTINATION

List: FileCreateDisposition

List of file creation methods.

Digital value	Associated symbol
0	FILE_SUPERSEDE
1	FILE_OPEN
2	FILE_CREATE
3	FILE_OPEN_IF
4	FILE_OVERWRITE
5	FILE_OVERWRITE_IF

Binary field: FileCreateOptions

Various options relating to file opening and creation.

Binary value	Associated symbol
0x00000001	FILE_DIRECTORY_FILE
0x00000002	FILE_WRITE_THROUGH
0x00000004	FILE_SEQUENTIAL_ONLY
0x00000008	FILE_NO_INTERMEDIATE_BUFFERING
0x00000010	FILE_SYNCHRONOUS_IO_ALERT
0x00000020	FILE_SYNCHRONOUS_IO_NONALERT
0x00000040	FILE_NON_DIRECTORY_FILE
0x00000080	FILE_CREATE_TREE_CONNECTION
0x00000100	FILE_COMPLETE_IF_OPLOCKED
0x00000200	FILE_NO_EA_KNOWLEDGE
0x00000400	FILE_OPEN_REMOTE_INSTANCE
0x00000800	FILE_RANDOM_ACCESS
0x00001000	FILE_DELETE_ON_CLOSE
0x00002000	FILE_OPEN_BY_FILE_ID
0x00004000	FILE_OPEN_FOR_BACKUP_INTENT
0x00008000	FILE_NO_COMPRESSION
0x00010000	FILE_OPEN_REQUIRING_OPLOCK
0x00020000	FILE_DISALLOW_EXCLUSIVE
0x00100000	FILE_RESERVE_OPFILTER
0x00200000	FILE_OPEN_REPARSE_POINT
0x00400000	FILE_OPEN_NO_RECALL
0x00800000	FILE_OPEN_FOR_FREE_SPACE_QUERY

List: FileDeleteDetailsType

Types of detail blocks regarding file removal operations.

Digital value	Associated symbol
0	FILE_CREATE
1	FILE_CREATE_HARDLINK_DESTINATION
2	FILE_RENAME_SOURCE
3	FILE_RENAME_DESTINATION
4	FILE_MOVEFILEEX_SOURCE
5	FILE_MOVEFILEEX_DESTINATION
6	FILE_SET_OWNER_SOURCE
7	FILE_DELETE

Binary field: FileDeleteFlags

List of file removal options.

Binary value	Associated symbol
0x00000001	FILE_DISPOSITION_DELETE
0x00000002	FILE_DISPOSITION_POSIX_SEMANTICS
0x00000004	FILE_DISPOSITION_FORCE_IMAGE_SECTION_CHECK
0x00000008	FILE_DISPOSITION_ON_CLOSE
0x00000010	FILE_DISPOSITION_IGNORE_READONLY_ATTRIBUTE

Binary field: FileDesiredAccess

Binary field corresponding to permissions to access an item in a file system.

Binary value	Associated symbol
0x00000001	FILE_READ_DATA
0x00000002	FILE_WRITE_DATA
0x00000004	FILE_APPEND_DATA
0x00000008	FILE_READ_EA
0x00000010	FILE_WRITE_EA
0x00000020	FILE_EXECUTE
0x00000040	FILE_DELETE_CHILD
0x00000080	FILE_READ_ATTRIBUTES
0x00000100	FILE_WRITE_ATTRIBUTES
0x00010000	DELETE
0x00020000	READ_CONTROL
0x00040000	WRITE_DAC
0x00080000	WRITE_OWNER
0x00100000	SYNCHRONIZE
0x01000000	ACCESS_SYSTEM_SECURITY
0x02000000	MAXIMUM_ALLOWED
0x10000000	GENERIC_ALL
0x20000000	GENERIC_EXECUTE
0x40000000	GENERIC_WRITE
0x80000000	GENERIC_READ

List: FileInformationClass

Types of information that can be read or written to a file.

Digital value	Associated symbol
4	FileBasicInformation
15	FileFullEaInformation
19	FileAllocationInformation
20	FileEndOfFileInformation
31	FileMoveClusterInformation
36	FileTrackingInformation
39	FileValidDataLengthInformation
44	FileSfioReserveInformation
71	FileCaseSensitiveInformation
74	FileStorageReserveIdInformation
75	FileCaseSensitiveInformationForceAccessCheck

List: FilelessAttackMethod

Fileless code execution method.

Digital value	Associated symbol
0	ThreadStartAddressSpoofing
1	DynamicMemory
2	ModuleStomping
3	Trampoline

List: FileMoveFileExOperation

List of file system operations that can be scheduled at restart.

Digital value	Associated symbol
1	FILE_MOVEFILEEX_DELETE
2	FILE_MOVEFILEEX_RENAME
3	FILE_MOVEFILEEX_REPLACE

List: FileObjectType

Various types of items on a file system.

Digital value	Associated symbol
0	FILE_OBJECT_TYPE_FILE
1	FILE_OBJECT_TYPE_DIRECTORY
2	FILE_OBJECT_TYPE_UNKNOWN

List: FileReadDetailsType

Types of detail blocks regarding file reading operations.

Digital value	Associated symbol
0	FILE_SECTION_MAPPING
1	FILE_READ_DATA

Binary field: FileRenameFlags

List of file renaming options.

Binary value	Associated symbol
0x00000001	FILE_RENAME_REPLACE_IF_EXISTS
0x00000002	FILE_RENAME_POSIX_SEMANTICS
0x00000004	FILE_RENAME_SUPPRESS_PIN_STATE_INHERITANCE
0x00000008	FILE_RENAME_SUPPRESS_STORAGE_RESERVE_INHERITANCE
0x00000010	FILE_RENAME_NO_INCREASE_AVAILABLE_SPACE
0x00000020	FILE_RENAME_NO_DECREASE_AVAILABLE_SPACE
0x00000040	FILE_RENAME_IGNORE_READONLY_ATTRIBUTE
0x00000080	FILE_RENAME_FORCE_RESIZE_TARGET_SR
0x00000100	FILE_RENAME_FORCE_RESIZE_SOURCE_SR

List: FilesystemType

List of the types of file systems for a volume.

Digital value	Associated symbol
0	UNKNOWN
1	RAW
2	NTFS
3	FAT
4	CDFS
5	UDFS
6	LANMAN
7	WEBDAV
8	RDPDR
9	NFS
10	MS_NETWARE
11	NETWARE
12	BSUDF
13	MUP
14	RSFX
15	ROXIO_UDF1
16	ROXIO_UDF2
17	ROXIO_UDF3
18	TACIT
19	FS_REC
20	INCD
21	INCD_FAT
22	EXFAT
23	PSFS
24	GPFS
25	NPFS
26	MSFS
27	CSVFS
28	REFS

Digital value	Associated symbol
29	OPENAFS

List: FileWriteDetailsType

Types of detail blocks regarding file writing operations.

Digital value	Associated symbol
0	FILE_CREATE
1	FILE_CREATE_CHILD
2	FILE_CREATE_CHILD_HARDLINK_DESTINATION
3	FILE_RENAME_CHILD_SOURCE
4	FILE_RENAME_CHILD_DESTINATION
5	FILE_MOVEFILEEX_CHILD_SOURCE
6	FILE_MOVEFILEEX_CHILD_DESTINATION
7	FILE_SECTION_MAPPING
8	FILE_WRITE_DATA
9	FILE_SET_INFORMATION
10	FILE_SET_SECURITY
11	FILE_DELETE_CHILD
12	FILE_CREATE_HARDLINK_SOURCE

List: IOCAlgorithmDigest

Binary field corresponding to the various hash algorithms that an IoC search may use.

Digital value	Associated symbol
0	MD5
1	SHA1
2	SHA256
3	Fuzzy

List: IocNamedObjectType

Types of system objects supported

Digital value	Associated symbol
0	Undefined
1	AlpcPort
2	Callback
3	Device
4	Directory
5	Driver
6	Event
7	FilterConnectionPort
8	Job
9	Key
10	KeyedEvent
11	Mailslot
12	Mutant
13	Pipe
14	Partition
15	Section
16	Semaphore
17	Session
18	SymbolicLink
19	Timer
20	Type
21	WindowStation

List: KeyloggingMethod

Binary field corresponding to keylogging methods.

Digital value	Associated symbol
1	GetAsyncKeyState
2	GetKeyState
4	GetKeyboardState
8	GetRawInputBuffer
16	GetRawInputData
32	SetWindowsHookEx

Binary field: LogAttributes

Binary field corresponding to the agent events category.

Binary value	Associated symbol
0x00000000	None
0x00000001	SelfProtection
0x00000002	Protection
0x00000004	Internal
0x00000008	Audit
0x00000010	Context
0x00000020	External
0x00000100	Flood

List: LogCategory

List of possible event categories.

Digital value	Associated symbol
0	ProcessAccess
1	Registry
2	File
3	Keylogging
4	Other

List: LogType

List of possible events.

Digital value	Associated symbol
7	AgentOperationProcessAccess
8	AgentOperationProcessAccessDetailsProcess
9	AgentOperationProcessAccessDetailsThread
10	AgentOperationProcessAccessEmptyBlock
11	AgentOperationProcessExecution
39	AgentOperationRawVolumeAccess
40	AgentOperationNetworkAccessBind
41	AgentOperationNetworkAccessAccept
42	AgentOperationNetworkAccessConnect
43	AgentOperationProcessHollowing
44	AgentOperationStackPivot
45	AgentOperationDriverLoading
46	AgentOperationDriverGuard
47	AgentOperationHoneyPot
48	AgentOperationTokenGuardDetailsTokenDuplicate
49	AgentOperationTokenGuardDetailsTokenModify
50	AgentOperationTokenGuard
51	AgentOperationKeylogging
53	AgentOperationHeapSpray
54	AgentOperationLrpcAccess
55	AgentOperationCreateRemoteThread
56	AgentOperationProcessExit
57	AgentOperationSetWindowsHookExAll
58	AgentOperationSetWindowsHookEx
59	AgentOperationProcessAccessWithPrivilegeEscalation
60	AgentOperationEDRBypass
61	AgentOperationEDRBypassDetailsNoInformation
62	AgentOperationEDRBypassDetailsBreakpointInformation
63	AgentOperationEDRBypassDetailsFunctionPatchInformation

Digital value	Associated symbol
64	AgentOperationFileless
65	AgentOperationFilelessDetailsDynamicMemoryInformation
66	AgentOperationFilelessDetailsModuleStompingInformation
67	AgentOperationFilelessDetailsTrampolineStartInformation
68	AgentOperationFilelessDetailsThreadStartAddressSpoofingInformation
69	AgentOperationFilelessDetailsNoInformation
100	AgentOperationRegistryKeyCreateDetailsCreate
101	AgentOperationRegistryKeyCreateDetailsRename
102	AgentOperationRegistryKeyCreateDetailsCreateLink
103	AgentOperationRegistryKeyCreate
104	AgentOperationRegistryKeyRead
105	AgentOperationRegistryKeyWriteDetailsSubkeyCreate
106	AgentOperationRegistryKeyWriteDetailsSubkeyRename
107	AgentOperationRegistryKeyWriteDetailsSetInformation
108	AgentOperationRegistryKeyWriteDetailsSetSecurity
109	AgentOperationRegistryKeyWrite
110	AgentOperationRegistryKeyDeleteDetailsDelete
111	AgentOperationRegistryKeyDeleteDetailsRename
112	AgentOperationRegistryKeyDelete
113	AgentOperationRegistryValueCreate
114	AgentOperationRegistryValueRead
115	AgentOperationRegistryValueWrite
116	AgentOperationRegistryValueDelete
150	AgentOperationFileDetailsAccessFromNetwork
151	AgentOperationFileDetailsAccessNotFromNetwork
152	AgentOperationFileDetailsCreate
153	AgentOperationFileDetailsCreateChild
154	AgentOperationFileDetailsCreateHardLinkDestination
155	AgentOperationFileDetailsCreateChildHardLinkDestination
156	AgentOperationFileDetailsRenameSource
157	AgentOperationFileDetailsRenameChildSource

Digital value	Associated symbol
158	AgentOperationFileDetailsRenameDestination
159	AgentOperationFileDetailsRenameChildDestination
160	AgentOperationFileDetailsMoveFileExSource
161	AgentOperationFileDetailsMoveFileExChildSource
162	AgentOperationFileDetailsMoveFileExDestination
163	AgentOperationFileDetailsMoveFileExChildDestination
164	AgentOperationFileDetailsSetOwnerSource
165	AgentOperationFileDetailsSetOwnerDestination
166	AgentOperationFileDetailsSectionMapping
167	AgentOperationFileDetailsReadData
168	AgentOperationFileDetailsWriteData
169	AgentOperationFileDetailsSetInformation
170	AgentOperationFileDetailsSetSecurity
171	AgentOperationFileDetailsDelete
172	AgentOperationFileDetailsDeleteChild
173	AgentOperationFileCreate
174	AgentOperationFileExecute
175	AgentOperationFileRead
176	AgentOperationFileWrite
177	AgentOperationFileDelete
178	AgentOperationFileDetailsCreateHardLinkSource
300	PnPDeviceInfo
301	AgentOperationFloppy
302	AgentOperationCDRom
303	AgentOperationComPort
304	UsbDeviceInfo
305	AgentOperationUsbDevice
306	NotUsbDeviceInfo
320	UsbVolumeTrackingData
321	AgentOperationUsbVolumeTrackingDataUpdate
322	AgentOperationUsbVolumeMount

Digital value	Associated symbol
323	NotUsbVolumeTrackingData
324	PhysicalConsoleSession
325	AgentInternalUsbVolumeScanSuccess
326	AgentInternalUsbVolumeScanError
327	AgentInternalUsbVolumeFootprintComputationError
350	BluetoothDeviceInfoDefault
351	BluetoothDeviceInfoComputer
352	BluetoothDeviceInfoPhone
353	BluetoothDeviceInfoNetworkApLoadFactor
354	BluetoothDeviceInfoAudioVideo
355	BluetoothDeviceInfoPeripheral
356	BluetoothDeviceInfoImaging
357	BluetoothDeviceInfoWearable
358	BluetoothDeviceInfoToy
359	BluetoothDeviceInfoHealth
360	BluetoothDeviceInfo
361	AgentOperationBluetoothAccess
400	AgentOperationWifiAccessConnectedNetwork
401	AgentOperationWifiAccessFunctionnality
1000	AgentInternalLostBuffers
1006	AgentInternalTemporaryWebAccessStart
1007	AgentInternalTemporaryWebAccessStartFailed
1008	AgentInternalTemporaryWebAccessStop
1009	AgentInternalTemporaryWebAccessStopFailed
1010	AgentInternalLogExceedMaxSize
1011	AgentInternalTemporaryWebAccessMaxCountReached
1012	AgentFloodInformation
1013	AgentFloodStart
1014	AgentFloodStop
20002	AgentInternalLostBuffers
20003	AgentInternalNewPolicyNotification

Digital value	Associated symbol
20004	AgentInternalServiceDidNotEndCorrectly
20006	AgentInternalEndUpgradeAgentSucceeded
20007	AgentInternalEndUpgradeAgentFailed
20008	AgentInternalNewPolicyErrorNotification
20009	AgentInternalInvalidHivePackage
20010	AgentInternalStartUninstallAgent
20011	AgentInternalEndUninstallAgentSucceeded
20012	AgentInternalEndUninstallAgentFailed
20013	AgentInternalInvalidPolicyPackageCab
20015	AgentInternalKernelCorruptionBugcheck
20016	AgentInternalInvalidPolicyPackageSignature
20017	AgentInternalStartAgentUpgrade
20018	AgentInternalPolicyPackageSignerExpired
20019	AgentInternalSelfProtectionLrpcFailure
20020	AgentInternalNewPolicyFromUpdateErrorNotification
20021	AgentInternalNewPolicyFromUpdateNotification
20022	AgentInternalNewConfigurationNotification
20023	AgentInternalNewConfigurationErrorNotification
20024	AgentInternalNewConfigurationFromUpdateErrorNotification
20025	AgentInternalNewConfigurationFromUpdateNotification
20026	AgentInternalInvalidConfigurationPackageCab
20027	AgentInternalDowngradeIsNotAuthorized
20028	AgentInternalSafeModeSessionNotification
20030	AgentInternalMaintenanceModeStart
20031	AgentInternalMaintenanceModeStop
20032	AgentInternalMaintenanceModeAgentUpgradePostponed
20033	AgentInternalBfeIsStoppedNotification
20034	AgentInternalRepairFailureNotification
20035	AgentInternalRepairSuccessNotification
20036	AgentInternalEndAgentModularityFailed
20037	AgentInternalEndAgentModularitySucceeded

Digital value	Associated symbol
20038	AgentInternalCommFinishFailedState
20039	AgentInternalForcedPatchApplication
20040	AgentInternalChallengeStart
20041	AgentInternalChallengeStop
20042	AgentInternalChallengeStopFailure
20043	AgentInternalWrongCabinetVersion
20044	AgentInternalMultipleNetworkInterfacesMatchingTest
20045	AgentInternalChallengeStartFailure
20046	AgentAction
20047	AgentFields
20048	AgentOperationExternal
20049	AgentInternalChallengeTooManyFailedAttempts
20050	AgentInternalMaintenanceModeAgentModularityPostponed
20051	AgentInternalEndUpgradeAgentNothingToDo
20052	AgentInternalEndUpgradeAgentGuidUpdated
20053	AgentInternalMaintenanceModeStopFailed
20054	AgentOperationKerberosPassTheTicket
20055	AgentOperationArpSpoofing
20056	AgentOperationCertutilDecodeMaliciousUsage
20057	AgentOperationCertutilDownloadMaliciousUsage
20058	AgentCorrelation
20059	AgentInternalScriptRuntimeError
20060	AgentOperationWmiPersistence
20061	AgentOperationDiscovery
20062	AgentInternalUninstallForbidden
20063	AgentInternalLogExceedMaxSize
20064	AgentInternalStartModularityAgent
20065	AgentInternalStartRepairAgent
20066	AgentInternalVolumeWithoutShadowStorage
20067	AgentInternalShadowCopyCreationFailure
20068	AgentOperationRansomware

Digital value	Associated symbol
20069	AgentInternalResourcePackageDownloadFailed
20070	AgentInternalInvalidResourcePackageSignature
20071	AgentInternalSecOpsInvalidPackageSignature
20072	AgentInternalSecOpsInvalidJsonSize
20073	AgentInternalDowngradeWithPivotVersion223IsRequired
20074	AgentAnalysisProperties
20075	AgentOperationYaraRuleInformationTag
20076	AgentOperationYaraRuleInformationMetadata
20077	AgentOperationYaraRuleInformation
20078	AgentOperationYaraAnalysisFilesDetails
20079	AgentOperationYaraProcessAnalysisMatch
20080	AgentOperationYaraFileAnalysisMatch
20081	AgentOperationYaraFileAnalysisMatchNoSourceProcess
20082	AgentOperationPpidSpoofing
20083	AgentInternalIntegrityStart
20084	AgentInternalIntegritySuccessNotification
20085	AgentInternalRepairSuccessWithRebootNotification
20086	AgentInternalRepairSuccessWithoutRebootNotification
20087	AgentInternalIntegrityErrorNotification
20088	AgentOperationYaraRuleInformationMatchedString
20089	AgentRemediationRemoveFile
20090	AgentRemediationKillProcess
20091	AgentRemediationRemoveRegistryKey
20092	AgentRemediationRemoveRegistryValue
20093	AgentRemediationSetRegistryValue
20094	AgentRemediationExecutePowershellScript
20095	AgentRemediationExtractFilesFromShadowCopy
20096	AgentRemediationSpecificData
20097	AgentOperationIocAnalysisNamedObjectMatch
20098	AgentOperationIocAnalysisEventLogMatch
20099	AgentOperationIocAnalysisFilenameMatch

Digital value	Associated symbol
20100	AgentOperationIocAnalysisFilenameMatchNoSourceProcess
20101	AgentOperationIocAnalysisDnsRequestMatch
20102	AgentRemediationRestoredFileFromShadowCopy
20103	AgentOperationIocFileSearchDetails
20104	AgentOperationIocFileSearchMatchInformation
20105	AgentOperationIocFileSearchByHashFile
20106	AgentOperationIocFileSearchByHashProcess
20107	AgentOperationIocAnalysisTextualSearchProcessMatch
20108	AgentOperationIocAnalysisTextualSearchFileMatch
20109	AgentOperationIocAnalysisTextualSearchFileMatchNoSourceProcess
20110	AgentOperationIocMatchedString
20111	AgentInternalFileMonitorOpenCursorFailure
20112	AgentInternalUpdateDownloadFailed
20113	AgentRemediationIsolateComputer
20114	AgentRemediationComputerIsolationLeave
20115	AgentFileQuarantineRuleDetails
20116	AgentFileQuarantinedFromProtectionRule
20117	AgentFileRestoredFromQuarantine
20118	AgentFileRemovedFromQuarantine
20119	AgentFileQuarantinedFromSecOpsTask
20120	AgentFileRestoredFromQuarantineByExclusionUpdate
20121	AgentInternalAgentPatchMissing
20122	AgentInternalAgentPatchRecovered
20123	AgentInternalAgentPatchNotRecovered
20124	AgentActionTag
20125	AgentFileQuarantinedFromScheduledTask
20126	AgentRemediationRemoveDirectory
20127	AgentInternalPolymorphicLog
11	AgentOperationProcessExecution
1012	AgentFloodInformation
1013	AgentFloodStart
1014	AgentFloodStop

List: MemoryMappingType

Memory mapping type.

Digital value	Associated symbol
0x00020000	MEM_PRIVATE
0x00040000	MEM_MAPPED
0x01000000	MEM_IMAGE

Binary field: MemoryProtection

List of memory protections

Binary value	Associated symbol
0x00000001	PAGE_NOACCESS
0x00000002	PAGE_READONLY
0x00000004	PAGE_READWRITE
0x00000008	PAGE_WRITECOPY
0x00000010	PAGE_EXECUTE
0x00000020	PAGE_EXECUTE_READ
0x00000040	PAGE_EXECUTE_READWRITE
0x00000080	PAGE_EXECUTE_WRITECOPY
0x00000100	PAGE_GUARD
0x00000200	PAGE_NOCACHE
0x00000400	PAGE_WRITECOMBINE
0x00000800	PAGE_GRAPHICS_NOACCESS
0x00001000	PAGE_GRAPHICS_READONLY
0x00002000	PAGE_GRAPHICS_READWRITE
0x00004000	PAGE_GRAPHICS_EXECUTE
0x00008000	PAGE_GRAPHICS_EXECUTE_READ
0x00010000	PAGE_GRAPHICS_EXECUTE_READWRITE
0x00020000	PAGE_GRAPHICS_COHERENT

List: NetworkAccessAddressFamily

List of IP address modes.

Digital value	Associated symbol
2	IPV4
23	IPV6

List: NetworkAccessOperation

List of the types of network communication operations.

Digital value	Associated symbol
0	Connect
1	Bind
2	Accept

List: NetworkAccessProtocol

List of the types of network communication IP protocols.

Digital value	Associated symbol
6	TCP
17	UDP

Binary field: PrivilegeHigh

Binary field corresponding to the second part of the permissions that the security token of a process may include.

Binary value	Associated symbol
0x00000001	SE_RELABEL_PRIVILEGE
0x00000002	SE_INC_WORKING_SET_PRIVILEGE
0x00000004	SE_TIME_ZONE_PRIVILEGE
0x00000008	SE_CREATE_SYMBOLIC_LINK_PRIVILEGE
0x00000010	SE_DELEGATE_SESSION_USER_IMPERSONATE_PRIVILEGE

Binary field: PrivilegeLow

Binary field corresponding to the first part of the permissions that the security token of a process may include.

Binary value	Associated symbol
0x00000004	SE_CREATE_TOKEN_PRIVILEGE
0x00000008	SE_ASSIGNPRIMARYTOKEN_PRIVILEGE
0x00000010	SE_LOCK_MEMORY_PRIVILEGE
0x00000020	SE_INCREASE_QUOTA_PRIVILEGE
0x00000040	SE_MACHINE_ACCOUNT_PRIVILEGE
0x00000080	SE_TCB_PRIVILEGE
0x00000100	SE_SECURITY_PRIVILEGE
0x00000200	SE_TAKE_OWNERSHIP_PRIVILEGE
0x00000400	SE_LOAD_DRIVER_PRIVILEGE
0x00000800	SE_SYSTEM_PROFILE_PRIVILEGE
0x00001000	SE_SYSTEMTIME_PRIVILEGE
0x00002000	SE_PROF_SINGLE_PROCESS_PRIVILEGE
0x00004000	SE_INC_BASE_PRIORITY_PRIVILEGE
0x00008000	SE_CREATE_PAGEFILE_PRIVILEGE
0x00010000	SE_CREATE_PERMANENT_PRIVILEGE
0x00020000	SE_BACKUP_PRIVILEGE
0x00040000	SE_RESTORE_PRIVILEGE
0x00080000	SE_SHUTDOWN_PRIVILEGE
0x00100000	SE_DEBUG_PRIVILEGE
0x00200000	SE_AUDIT_PRIVILEGE
0x00400000	SE_SYSTEM_ENVIRONMENT_PRIVILEGE
0x00800000	SE_CHANGE_NOTIFY_PRIVILEGE
0x01000000	SE_REMOTE_SHUTDOWN_PRIVILEGE
0x02000000	SE_UNDOCK_PRIVILEGE
0x04000000	SE_SYNC_AGENT_PRIVILEGE
0x08000000	SE_ENABLE_DELEGATION_PRIVILEGE
0x10000000	SE_MANAGE_VOLUME_PRIVILEGE
0x20000000	SE_IMPERSONATE_PRIVILEGE

Binary value	Associated symbol
0x40000000	SE_CREATE_GLOBAL_PRIVILEGE
0x80000000	SE_TRUSTED_CREDMAN_ACCESS_PRIVILEGE

Binary field: ProcessAccessMask

Binary field corresponding to permissions to access a process.

Binary value	Associated symbol
0x0001	PROCESS_TERMINATE
0x0002	PROCESS_CREATE_THREAD
0x0004	PROCESS_SET_SESSIONID
0x0008	PROCESS_VM_OPERATION
0x0010	PROCESS_VM_READ
0x0020	PROCESS_VM_WRITE
0x0040	PROCESS_DUP_HANDLE
0x0080	PROCESS_CREATE_PROCESS
0x0100	PROCESS_SET_QUOTA
0x0200	PROCESS_SET_INFORMATION
0x0400	PROCESS_QUERY_INFORMATION
0x0800	PROCESS_SUSPEND_RESUME
0x1000	PROCESS_QUERY_LIMITED_INFORMATION
0x2000	PROCESS_SET_LIMITED_INFORMATION
0x10000	DELETE
0x20000	READ_CONTROL
0x40000	WRITE_DAC
0x80000	WRITE_OWNER
0x100000	SYNCHRONIZE

List: ProcessAccessObjectType

List of object types affected by process access protection.

Digital value	Associated symbol
1	Process
2	Thread

List: ProcessAccessOperation

List of operations that can trigger process access protection.

Digital value	Associated symbol
1	Open
2	Duplicate

List: ProcessHollowingOperation

List of methods used for process hollowing.

Digital value	Associated symbol
1	EntryPointDataModification
2	EntryPointRelocation
3	PebImageBaseAddressModification
4	ProcessDoppelganging
5	ProcessHerpaderping
6	ProcessGhosting

Binary field: RegistryAccessMask

Binary field corresponding to permissions to access a registry key.

Binary value	Associated symbol
0x0001	KEY_QUERY_VALUE
0x0002	KEY_SET_VALUE
0x0004	KEY_CREATE_SUB_KEY
0x0008	KEY_ENUMERATE_SUB_KEYS
0x0010	KEY_NOTIFY
0x0020	KEY_CREATE_LINK
0x0200	KEY_WOW64_32KEY
0x0100	KEY_WOW64_64KEY
0x00010000	DELETE
0x00020000	READ_CONTROL
0x00040000	WRITE_DAC
0x00080000	WRITE_OWNER
0x02000000	MAXIMUM_ALLOWED

Binary field: RegistryCreateOptions

Binary field corresponding to the various options when a registry key is created.

Binary value	Associated symbol
0x0001	REG_OPTION_VOLATILE
0x0002	REG_OPTION_CREATE_LINK
0x0004	REG_OPTION_BACKUP_RESTORE
0x0008	REG_OPTION_OPEN_LINK
0x0010	REG_OPTION_DONT_VIRTUALIZE

List: RegistryKeyCreateDetailsType

Types of descriptions of registry key creation operations.

Digital value	Associated symbol
0	REGISTRY_KEY_CREATE
1	REGISTRY_KEY_RENAME
2	REGISTRY_KEY_CREATE_LINK

List: RegistryKeyDeleteDetailsType

Types of descriptions of registry key deletion operations.

Digital value	Associated symbol
0	REGISTRY_KEY_DELETE
1	REGISTRY_KEY_RENAME

List: RegistryKeyWriteDetailsType

Types of descriptions of registry key writing operations.

Digital value	Associated symbol
0	REGISTRY_KEY_CREATE_SUBKEY
1	REGISTRY_KEY_RENAME_SUBKEY
2	REGISTRY_KEY_SET_INFORMATION
3	REGISTRY_KEY_SET_SECURITY

List: RegistryQueryInformationClass

Types of information that can be read on a registry key.

Digital value	Associated symbol
0	KeyBasicInformation
1	KeyNodeInformation
2	KeyFullInformation
3	KeyNameInformation
4	KeyCachedInformation
5	KeyFlagsInformation
6	KeyVirtualizationInformation
7	KeyHandleTagsInformation
8	KeyTrustInformation
9	KeyLayerInformation

List: RegistrySetInformationClass

Types of information that can be written on a registry key.

Digital value	Associated symbol
0	KeyWriteTimeInformation
1	KeyWow64FlagsInformation
2	KeyControlFlagsInformation
3	KeySetVirtualizationInformation
4	KeySetDebugInformation
5	KeySetHandleTagsInformation
6	KeySetLayerInformation

List: RegistryValueType

List of the types of possible registry values.

Digital value	Associated symbol
0	REG_NONE
1	REG_SZ
2	REG_EXPAND_SZ
3	REG_BINARY
4	REG_DWORD
5	REG_DWORD_BIG_ENDIAN
6	REG_LINK
7	REG_MULTI_SZ
8	REG_RESOURCE_LIST
9	REG_FULL_RESOURCE_DESCRIPTOR
10	REG_RESOURCE_REQUIREMENTS_LIST
11	REG_QWORD

List: RemediationActionResultMap

Remediation operation result

Digital value	Associated symbol
0	Success
1	Ignore
2	Error
3	Partial

Binary field: ScriptTriggers

Binary field corresponding to the various triggers that the script service can use to run script.

Binary value	Associated symbol
0x00000000	None
0x00000001	PolicyPackageChange
0x00000002	Periodic
0x00000004	NetworkEvent
0x00000008	RuleEvent
0x00000010	StopAgent
0x00000020	PolicyApplied
0x00000040	Scheduled
0x00000080	SecOps

Binary field: SecurityClass

Types of information that can be read or written on a security descriptor of a registry key.

Binary value	Associated symbol
0x00000001	OWNER_SECURITY_INFORMATION
0x00000002	GROUP_SECURITY_INFORMATION
0x00000004	DACL_SECURITY_INFORMATION
0x00000008	SACL_SECURITY_INFORMATION
0x00000010	LABEL_SECURITY_INFORMATION
0x00000020	ATTRIBUTE_SECURITY_INFORMATION
0x00000040	SCOPE_SECURITY_INFORMATION
0x00000080	PROCESS_TRUST_LABEL_SECURITY_INFORMATION
0x00000100	ACCESS_FILTER_SECURITY_INFORMATION
0x00010000	BACKUP_SECURITY_INFORMATION
0x10000000	UNPROTECTED_SACL_SECURITY_INFORMATION
0x20000000	UNPROTECTED_DACL_SECURITY_INFORMATION
0x40000000	PROTECTED_SACL_SECURITY_INFORMATION
0x80000000	PROTECTED_DACL_SECURITY_INFORMATION

List: SetWindowsHookExHookId

Field corresponding to the possible types of hooks with SetWindowsHookEx.

Digital value	Associated symbol
0xffffffff	WH_MSGFILTER
0	WH_JOURNALRECORD
1	WH_JOURNALPLAYBACK
2	WH_KEYBOARD
3	WH_GETMESSAGE
4	WH_CALLWNDPROC
5	WH_CBT
6	WH_SYSMSGFILTER
7	WH_MOUSE
8	WH_HARDWARE
9	WH_DEBUG
10	WH_SHELL
11	WH_FOREGROUNDIDLE
12	WH_CALLWNDPROCRET
13	WH_KEYBOARD_LL
14	WH_MOUSE_LL

List: Severity

List of the levels of severity of events recorded in logs.

Digital value	Associated symbol
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

Binary field: ThreadAccessMask

Binary field corresponding to permissions to access a process thread.

Binary value	Associated symbol
0x0001	THREAD_TERMINATE
0x0002	THREAD_SUSPEND_RESUME
0x0004	THREAD_ALERT
0x0008	THREAD_GET_CONTEXT
0x0010	THREAD_SET_CONTEXT
0x0020	THREAD_SET_INFORMATION
0x0040	THREAD_QUERY_INFORMATION
0x0080	THREAD_SET_THREAD_TOKEN
0x0100	THREAD_IMPERSONATE
0x0200	THREAD_DIRECT_IMPERSONATION
0x0400	THREAD_SET_LIMITED_INFORMATION
0x0800	THREAD_QUERY_LIMITED_INFORMATION
0x1000	THREAD_RESUME
0x10000	DELETE
0x20000	READ_CONTROL
0x40000	WRITE_DAC
0x80000	WRITE_OWNER
0x100000	SYNCHRONIZE

List: TokenGuardDetailsType

List of the types of security token changes.

Digital value	Associated symbol
0	TokenDuplicate
1	TokenReplace
2	TokenModify

List: TrampolineType

Trampoline type detected.

Digital value	Associated symbol
0	None
1	X64Pattern
2	X86Pattern

List: UsbDeviceClass

List of USB device classes.

Digital value	Associated symbol
0x00	IN_INTERFACE_DESCRIPTORS
0x01	AUDIO
0x02	COMMUNICATIONS_CDC_CONTROL
0x03	HID
0x05	PHYSICAL
0x06	IMAGE
0x07	PRINTER
0x08	MASS_STORAGE
0x09	HUB
0x0A	CDC_DATA
0x0B	SMART_CARD
0x0D	CONTENT_SECURITY
0x0E	VIDEO
0x0F	PERSONAL_HEALTHCARE
0x10	AUDIO_VIDEO_DEVICES
0x11	BILLBOARD_DEVICE_CLASS
0x12	USB_TYPE_C_BRIDGE_CLASS
0xDC	DIAGNOSTIC_DEVICE
0xE0	WIRELESS_CONTROLLER
0xEF	MISCELLANEOUS
0xFE	APPLICATION_SPECIFIC
0xFF	VENDOR_SPECIFIC

List: UsbDeviceEventType

List of events relating to USB devices.

Digital value	Associated symbol
0x00	CONNECT
0x01	DISCONNECT

List: UsbVolumeEnrollFileState

List of the statuses of the enrollment file for a USB device.

Digital value	Associated symbol
0x00	NOT_FOUND
0x01	MALFORMED
0x02	BAD_VERSION
0x03	BAD_ENCRYPTION
0x04	CONTENT_MISMATCH
0x05	VALID

List: UsbVolumeMountEventType

List of events when a volume is mounted or unmounted.

Digital value	Associated symbol
0x00	MOUNT
0x01	UNMOUNT

List: UsbVolumeTrustFootprintFileState

List of the statuses of the hash file for a USB device.

Digital value	Associated symbol
0x00	NOT_FOUND
0x01	MALFORMED
0x02	BAD_VERSION
0x03	BAD_ENCRYPTION
0x04	CONTENT_MISMATCH
0x05	VALID

List: VolumeAccessType

List of modes to access a volume without going through the file system.

Digital value	Associated symbol
1	Read
2	Write

Binary field: VolumeZone

Binary field corresponding to the characteristics of a storage volume.

Binary value	Associated symbol
0x00000001	OPERATING_SYSTEM
0x00000002	COMPUTER_BOOT
0x00000004	SYSTEM_SNAPSHOT
0x00000008	CD_ROM
0x00000010	ISO
0x00000020	VIRTUAL_DISK
0x00000040	FLOPPY
0x00000080	REMOTE_LANMAN
0x00000100	REMOTE_CSC
0x00000200	REMOTE_RDP_DR
0x00000400	REMOTE_WEBDAV
0x00000800	REMOTE_MAILSLOT
0x00001000	REMOTE_VMWARE
0x00002000	REMOTE_VBOX
0x00004000	REMOTE_UNKNOWN
0x00008000	REMOVABLE_UNKNOWN
0x00010000	NOT_REMOVABLE_UNKNOWN

Binary field: WifiAuthAlgo

List of the types of authentication on WiFi networks.

Binary value	Associated symbol
0x00000001	Wpa2Enterprise
0x00000002	Wpa2Personal
0x00000004	WpaEnterprise
0x00000008	WpaPersonal
0x00000010	Open
0x00000020	Shared

Binary field: WifiConnectionMode

List of WiFi connection modes.

Binary value	Associated symbol
0x00000001	Infrastructure
0x00000002	AdHoc

List: WmiPersistenceConsumerTypeMap

List of the consumers detected during a persistence linked to WMI.

Digital value	Associated symbol
0	CommandLineEventConsumer
1	ActiveScriptEventConsumer

Block: AgentActionTagTemplate

Details of a MITRE tag associated with a rule.

Field	Meaning
RuleTag	Name of the tag associated with the rule that triggered the log generation.

Block: AgentActionTemplate

Description of an action performed by the agent.

Field	Meaning
PolicyGuid	ID of the policy associated with the rule that caused the event.
PolicyVersion	Version of the policy associated with the rule that caused the event.
RuleGuid	ID of a specific sub-rule inside a rule (internal parameter of the product).
BaseRuleGuid	ID of the rule associated with the log.
IdentifierGuid	Unique ID of the application ID that caused the event.
Blocked	Indicates that the agent blocked the action.
RequestMoveToQuarantine	Request to quarantine the source process. This is a request that has not yet been sent.
UserDecision	Indicates the user's decision.
SourceProcessKilled	Indicates that SES stopped the process performing the operation.
RuleTags	Tags associated with the rule that triggered the log generation. More details on this block in section AgentActionTagTemplate.

Block: AgentAnalysisPropertiesTemplate

Detail block generated for all logs relating to scans (e.g., YARA scans)

Field	Meaning
AnalysisUnitGuid	Unique ID of the analysis unit
Triggers	Triggers associated with the scan This field can contain combined binary values listed in section ScriptTriggers.
AssociatedEventGuid	ID of the log that triggered the scan
AssociatedScheduledTaskGuid	ID of the scheduled task associated with the scan
AssociatedSecOpsGuid	ID of the scan task associated with the scan
AssociatedSecOpsRequestGuid	ID of the task request associated with the scan
AssociatedBaseRuleGuid	ID of the basic rule that allowed the scan to be launched
AssociatedRuleGuid	ID of the rule that allowed the scan to be launched

Block: AgentCorrelationTemplate

Information about an advanced protection

Field	Meaning
PackageGuid	Protection's unique identifier
PackageVersion	Protection by correlation version.
AttackIntent	Attack intent identified by correlation protection.

Block: AgentFieldsTemplate

Description of the rule fields associated to event transfer.

Field	Meaning
_RuleGuid	ID of a specific sub-rule inside the rule (internal parameter of the product).
_BaseRuleGuid	ID of the rule associated with the event.

Block: AgentFileQuarantineRuleDetailsTemplate

Information about the quarantine rule.

Field	Meaning
RuleGuid	ID of a specific rule within the rule group (meaning is internal to the product).
BaseRuleGuid	ID of the rule that created the quarantine
PolicyGuid	ID of the policy to which the rule relates.
PolicyVersion	Version number of the policy to which the rule relates.

Block: AgentFloodInformationTemplate

Information about the source of the log flooding.

Field	Meaning
TriggeringEventGUID	GUID of the event causing log flooding.
TriggeringEventBaseRuleGUID	GUID of the rule causing log flooding.
TriggeringEventPolicyGUID	GUID of the policy causing log flooding.
TriggeringEventPolicyVersion	Version of the policy causing log flooding.
TriggeringEventTimestamp	Time of the log that triggered log flooding.

Block: AgentInternalPolymorphicLogTemplate

Polymorphic log

Block: AgentOperationEDRBypassDetailsBreakpointInformationTemplate

Additional information related to bypassing the means of detection of an EDR. This block contains the information specific to the hardware breakpoints.

Field	Meaning
ModuleName	Name of the impacted module as defined in the PE module export table.
NearestSymbol	Name of the routine in which the breakpoint was detected.

Block: AgentOperationEDRBypassDetailsFunctionPatchInformationTemplate

Additional information related to bypassing the means of detection of an EDR. This block contains information specific to function content corruption.

Field	Meaning
ModuleName	Name of the impacted module as defined in the PE module export table.
NearestSymbol	Name of the routine that has been corrupted.
ExpectedOpCodes	Code of the routine used as the basis for comparison.
ReadOpCodes	Code of the routine that was actually executed.

Block: AgentOperationEDRBypassDetailsNoInformationTemplate

Additional information related to bypassing the means of detection of an EDR. This block is empty.

Block: AgentOperationFileDetailsAccessFromNetworkTemplate

Description of a client's access to a file system from the network.

Field	Meaning
ShareName	Path to the shared network that the network client is accessing.
AddressFamily	IP address family (IPv4 or IPv6). This field can contain one of the values listed in page NetworkAccessAddressFamily.
Address	IPv4 or IPv6 address of the network client.
Port	Communication port to which the network client logged in.

Block: AgentOperationFileDetailsAccessNotFromNetworkTemplate

Empty block that appears when a file is accessed locally.

Block: AgentOperationFileDetailsCreateChildHardLinkDestinationTemplate

Detail block regarding the creation of a new hard link with a parent directory on the file system, when the destination path matches a rule on the agent.

Field	Meaning
FileName	Name of the created item.
SourcePath	Indicates the source path of the hard link.
Flags	Hard link creation options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsCreateChildTemplate

Detail block regarding the creation of a new sub-item of a folder on a file system.

Field	Meaning
FileName	Name of the created item.
Disposition	Creation parameters. This field can contain one of the values listed in page FileCreateDisposition. For further information on this field, refer to page CreateFileW, section dwCreationDisposition of the Microsoft documentation.
Options	Various creation options. This field can contain combined binary values listed in section FileCreateOptions. For further information on this field, refer to page FLT_PARAMETERS, section Options of the Microsoft documentation.
Attributes	Attributes indicated. This field can contain combined binary values listed in section FileAttributes. For further information on this field, refer to page CreateFileW, section dwFlagsAndAttributes of the Microsoft documentation.
DesiredAccess	Access permissions requested. This field can contain combined binary values listed in section FileDesiredAccess. For further information on this field, refer to page CreateFileW, section dwDesiredAccess of the Microsoft documentation.

Block: AgentOperationFileDetailsCreateHardLinkDestinationTemplate

Detail block regarding the creation of a new hard link on a file system, when the destination path matches a rule on the agent.

Field	Meaning
SourcePath	Indicates the source path of the hard link.
Flags	Hard link creation options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsCreateHardLinkSourceTemplate

Detail block regarding the creation of a new hard link on a file system, when the source path matches a rule on the agent.

Field	Meaning
DestinationPath	Indicates the destination path of the hard link.
Flags	Hard link creation options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsCreateTemplate

Description of how a new item on a file system was created.

Field	Meaning
Disposition	Creation parameters. This field can contain one of the values listed in page FileCreateDisposition. For further information on this field, refer to page CreateFileW, section dwCreationDisposition of the Microsoft documentation.
Options	Various creation options. This field can contain combined binary values listed in section FileCreateOptions. For further information on this field, refer to page FLT_PARAMETERS, section Options of the Microsoft documentation.
Attributes	Attributes indicated. This field can contain combined binary values listed in section FileAttributes. For further information on this field, refer to page CreateFileW, section dwFlagsAndAttributes of the Microsoft documentation.
DesiredAccess	Access permissions requested. This field can contain combined binary values listed in section FileDesiredAccess. For further information on this field, refer to page CreateFileW, section dwDesiredAccess of the Microsoft documentation.

Block: AgentOperationFileDetailsDeleteChildTemplate

Detail block regarding the removal of a sub-item of a folder on a file system.

Field	Meaning
FileName	Name of the removed item.
Flags	Removal options. This field can contain combined binary values listed in section FileDeleteFlags.

Block: AgentOperationFileDetailsDeleteTemplate

Detail block regarding an item being deleted on a file system.

Field	Meaning
Flags	Removal options. This field can contain combined binary values listed in section FileDeleteFlags.

Block: AgentOperationFileDetailsMoveFileExChildDestinationTemplate

Detail block regarding how a sub-item in a folder on a file system was deleted or moved, as scheduled at startup, when the destination path matches a rule on the agent.

Field	Meaning
FileName	Name of the moved or deleted item.
SourcePath	Path to the source item.
Operation	Nature of the operation (move, delete, replace). This field can contain one of the values listed in page FileMoveFileExOperation.
IsNewOperation	Indicates whether it is a new operation scheduled at startup or whether, for example, it is a manual modification of the registry that may have changed the sequence of scheduled operations.

Block: AgentOperationFileDetailsMoveFileExChildSourceTemplate

Detail block regarding how a sub-item in a folder on a file system was deleted or moved, as scheduled at startup, when the source path matches a rule on the agent.

Field	Meaning
FileName	Name of the moved or deleted item.
DestinationPath	Path to the destination item.
Operation	Nature of the MoveFileEx operation (move, delete, replace). This field can contain one of the values listed in page FileMoveFileExOperation.
IsNewOperation	Indicates whether it is a new operation scheduled at startup or whether, for example, it is a manual modification of the registry that may have changed the sequence of scheduled operations.

Block: AgentOperationFileDetailsMoveFileExDestinationTemplate

Description of how an item on a file system scheduled at startup was deleted or moved, when the destination path is affected by a rule on the agent.

Field	Meaning
SourcePath	Path to the source item.
Operation	Nature of the operation (move, delete, replace). This field can contain one of the values listed in page FileMoveFileExOperation.
IsNewOperation	Indicates whether it is a new operation scheduled at startup or a manual modification of the registry that changed the sequence of scheduled operations.

Block: AgentOperationFileDetailsMoveFileExSourceTemplate

Description of how an item on a file system scheduled at startup was deleted or moved, when the source path is affected by a rule on the agent.

Field	Meaning
DestinationPath	Path to the destination item.
Operation	Nature of the MoveFileEx operation (move, delete, replace). This field can contain one of the values listed in page FileMoveFileExOperation.
IsNewOperation	Indicates whether it is a new operation scheduled at startup or whether, for example, it is a manual modification of the registry that may have changed the sequence of scheduled operations.

Block: AgentOperationFileDetailsReadDataTemplate

Detail block regarding the data of an item being read on a file system.

Block: AgentOperationFileDetailsRenameChildDestinationTemplate

Detail block regarding how a sub-item in a folder on a file system was renamed, when the destination path matches a rule on the agent.

Field	Meaning
FileName	Name of the renamed item.
SourcePath	Path to the item before it was renamed.
Flags	Renaming options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsRenameChildSourceTemplate

Detail block regarding how a sub-item in a folder on a file system was renamed, when the source path matches a rule on the agent.

Field	Meaning
FileName	Name of the renamed item.
DestinationPath	Path to the item after it was renamed.
Flags	Renaming options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsRenameDestinationTemplate

Description of how an item on a file system was renamed, when the destination path is affected by a rule on the agent.

Field	Meaning
SourcePath	Path to the item before it was renamed.
Flags	Renaming options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsRenameSourceTemplate

Description of how an item on a file system was renamed, when the source path is affected by a rule on the agent.

Field	Meaning
DestinationPath	Path to the item after it was renamed.
Flags	Renaming options. This field can contain combined binary values listed in section FileRenameFlags.

Block: AgentOperationFileDetailsSectionMappingTemplate

Detail block regarding an item on a file system being loaded in memory.

Field	Meaning
PageProtection	Permissions requested when loading the item in memory. This field can contain combined binary values listed in section MemoryProtection.

Block: AgentOperationFileDetailsSetInformationTemplate

Detail block regarding the information of an item being written on a file system.

Field	Meaning
InformationClass	Type of information written. This field can contain one of the values listed in page FileInformationClass.

Block: AgentOperationFileDetailsSetOwnerDestinationTemplate

Description of how the owner of an item on a file system was changed, when the item is affected by a rule on the agent.

Field	Meaning
OldFileOwner	Initial owner of the item. Note: This field is an SID. The **OldFileOwnerNameLookup** and **OldFileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Block: AgentOperationFileDetailsSetOwnerSourceTemplate

Description of how the owner of an item on a file system was changed, when the item is affected by a rule on the agent.

Field	Meaning
NewFileOwner	New owner requested for the item. Note: This field is an SID. The **NewFileOwnerNameLookup** and **NewFileOwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Block: AgentOperationFileDetailsSetSecurityTemplate

Detail block regarding the security descriptor of an item being written on a file system.

Field	Meaning
SecurityInformation	Type of information written about the security descriptor. This field can contain combined binary values listed in section SecurityClass.

Block: AgentOperationFileDetailsWriteDataTemplate

Detail block regarding the data of an item being written on a file system.

Block: AgentOperationFilelessDetailsDynamicMemoryInformationTemplate

Additional information related to dynamically allocated memory usage.

Field	Meaning
ModuleName	Name of module used.
MemoryMapping	Type of memory mapping used. This field can contain one of the values listed in page MemoryMappingType.
InitialPageProtection	Initial page rights. This field can contain combined binary values listed in section MemoryProtection.
FinalPageProtection	Final page rights. This field can contain combined binary values listed in section MemoryProtection.

Block: AgentOperationFilelessDetailsModuleStompingInformationTemplate

Additional information related to module overwriting.

Field	Meaning
ModuleName	Name of stomped module.
FinalPageProtection	Final page rights. This field can contain combined binary values listed in section MemoryProtection.

Block: AgentOperationFilelessDetailsNoInformationTemplate

Empty block.

Block: AgentOperationFilelessDetailsThreadStartAddressSpoofingInformationTemplate

Additional information related to exchanging thread start addresses.

Field	Meaning
ModuleName	Name of the module to be executed. Empty if not available.

Block: AgentOperationFilelessDetailsTrampolineStartInformationTemplate

Additional information related to the use of trampoline.

Field	Meaning
ModuleName	Name of the module to be executed. Empty if not available.
TrampolinePattern	Trampoline pattern detected. This field can contain one of the values listed in page TrampolineType.

Block: AgentOperationIocFileSearchDetailsTemplate

Details of the file matching the hash

Field	Meaning
FileFullPath	Path to the file
FileCreateTime	Created on
LastModified	Last modified on
Owner	Owner Note: This field is an SID. The **OwnerNameLookup** and **OwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
HashMd5	MD5 hash
HashSha1	SHA1 hash
HashSha256	SH256 hash
HashSSDeep	SSDEEP hash

Block: AgentOperationIocFileSearchMatchInformationTemplate

Match information.

Field	Meaning
HashAlgorithm	Hash algorithm used This field can contain one of the values listed in page IOCAlgorithmDigest.
SimilarityRate	Similarity rate
MatchedHash	Hash matching trigger

Block: AgentOperationIocMatchedStringTemplate

Technical template used to arrange chain tables in a series

Field	Meaning
MatchedString	Indicators that allowed the match in the file

Block: AgentOperationProcessAccessDetailsProcessTemplate

Description of access to a process.

Field	Meaning
DesiredAccess	Access permissions requested for access to the process. This field can contain combined binary values listed in section ProcessAccessMask.
MatchingAccess	Access permissions granted by the agent for access to the process. This field can contain combined binary values listed in section ProcessAccessMask.

Block: AgentOperationProcessAccessDetailsThreadTemplate

Description of access to a thread in a process.

Field	Meaning
DesiredAccess	Access permissions requested for access to the thread. This field can contain combined binary values listed in section ThreadAccessMask.
MatchingAccess	Access permissions granted by the agent for access to the thread. This field can contain combined binary values listed in section ThreadAccessMask.

Block: AgentOperationProcessAccessEmptyBlockTemplate

Empty block that appears when a process or thread is accessed through the acquisition of a handle on the object, instead of the duplication of a handle belonging to the target process.

Block: AgentOperationRegistryKeyCreateDetailsCreateLinkTemplate

Description of the creation of a registry key obtained as a symbolic link.

Field	Meaning
TargetPath	Path to the registry key to which the created symbolic link points.

Block: AgentOperationRegistryKeyCreateDetailsCreateTemplate

Description of how a registry key was created.

Field	Meaning
Options	Various options in the creation of a registry key. This field can contain combined binary values listed in section RegistryCreateOptions.
DesiredAccess	Permissions requested on the registry key. This field can contain combined binary values listed in section RegistryAccessMask.

Block: AgentOperationRegistryKeyCreateDetailsRenameTemplate

Description of the creation of a registry key obtained by renaming an existing key.

Field	Meaning
SourcePath	Path to the registry key before it was renamed.

Block: AgentOperationRegistryKeyDeleteDetailsDeleteTemplate

Description of how a registry key was deleted.

Block: AgentOperationRegistryKeyDeleteDetailsRenameTemplate

Description of the removal of a registry key obtained by renaming an existing key.

Field	Meaning
DestinationPath	New path requested for the registry key.

Block: AgentOperationRegistryKeyWriteDetailsSetInformationTemplate

Description of how the registry key information was written.

Field	Meaning
InformationClass	Type of information written about the registry key. This field can contain one of the values listed in page RegistrySetInformationClass.

Block: AgentOperationRegistryKeyWriteDetailsSetSecurityTemplate

Description of how the registry key security descriptor was written.

Field	Meaning
SecurityInformation	Type of information written about the security descriptor. This field can contain combined binary values listed in section SecurityClass.

Block: AgentOperationRegistryKeyWriteDetailsSubkeyCreateTemplate

Description of how a subkey was created in a registry key.

Field	Meaning
Options	Various options in the creation of a registry key. This field can contain combined binary values listed in section RegistryCreateOptions.
DesiredAccess	Permissions requested on the registry key. This field can contain combined binary values listed in section RegistryAccessMask.
SubkeyName	Name of the subkey that was created.

Block: AgentOperationRegistryKeyWriteDetailsSubkeyRenameTemplate

Description of how a subkey was renamed in a registry key.

Field	Meaning
SourcePath	Path to the registry key before it was renamed.
DestinationPath	New path requested for the registry key.

Block: AgentOperationTokenGuardDetailsTokenDuplicateTemplate

Description of how a security token was modified through the duplication of a third-party token.

Field	Meaning
User	Security ID of the user whose token was duplicated. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.

Block: AgentOperationTokenGuardDetailsTokenModifyTemplate

Description of the direct modification of a security token.

Field	Meaning
PrivilegesLow	Second part of the requested permissions. This field can contain combined binary values listed in section PrivilegeLow.
PrivilegesHigh	First part of the requested permissions. This field can contain combined binary values listed in section PrivilegeHigh.

Block: AgentOperationYaraAnalysisFilesDetailsTemplate

Detail block generated to list the details of a YARA scan file

Field	Meaning
FileFullPath	Absolute path to the file
FileCreateTime	File created on
LastModified	File last modified on
Owner	Information about the identity of the file owner Note: This field is an SID. The **OwnerNameLookup** and **OwnerDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
HashMd5	MD5 hash of the file
HashSha1	SHA1 hash of the file
HashSha256	SHA256 hash of the file
HashSSDeep	SSDeep hash of the file

Block: AgentOperationYaraRuleInformationMatchedStringTemplate

Detail block generated to list Yara rule matches

Field	Meaning
MatchedStringValue	Text match value

Block: AgentOperationYaraRuleInformationMetadataTemplate

Detail block generated to list the details of metadata associated with a Yara rule

Field	Meaning
MetadataKey	Key associated with the metadata
MetadataValue	Value associated with the metadata

Block: AgentOperationYaraRuleInformationTagTemplate

Detail block generated to list the details of a tag associated with a Yara rule

Field	Meaning
TagName	Tag name

Block: AgentOperationYaraRuleInformationTemplate

Detail block generated to list the details of a Yara rule

Field	Meaning
MatchedRule	Name of the Yara rule that found a match
Tags	List of tags associated with the Yara rule More details on this block in section AgentOperationYaraRuleInformationTagTemplate.
Metadatas	List of metadata associated with the Yara rule More details on this block in section AgentOperationYaraRuleInformationMetadataTemplate.
MatchedStrings	Text match for the Yara rule More details on this block in section AgentOperationYaraRuleInformationMatchedStringTemplate.

Block: AgentPEInfoTemplate

Information contained in the PE file resources.

Field	Meaning
OriginalFilename	Name given to the file when it was created.
Description	File role description
ProductName	Name of the product that embeds the file
CompanyName	Name of the company that generated the file
FileVersion	File version

Block: AgentRemediationRestoredFileFromShadowCopyTemplate

Information relating to file restoration

Field	Meaning
Filename	Path of a file restored from a shadow copy

Block: AgentRemediationSpecificDataTemplate

Specific items found in all remediation logs

Field	Meaning
Result	Result code of the remediation operation This field can contain one of the values listed in page RemediationActionResultMap.
StatusCode	Status code of the remediation operation
SecOpsTaskGuid	SecOps task ID
SecOpsTaskRequestGuid	SecOps request ID
ScheduledTaskRequestGuid	GUID of the scheduled task.

Block: BluetoothDeviceInfoAudioVideoTemplate

Description of a Bluetooth audio or video device.

Field	Meaning
Info	Additional information relating to a Bluetooth audio or video device. This field can contain one of the values listed in page BluetoothMinorDeviceClassAudioVideo.

Block: BluetoothDeviceInfoComputerTemplate

Description of a Bluetooth audio or video device.

Field	Meaning
Info	Additional information relating to a Bluetooth computer device. This field can contain one of the values listed in page BluetoothMinorDeviceClassComputer.

Block: BluetoothDeviceInfoDefaultTemplate

Description of a Bluetooth device.

Field	Meaning
Info	Additional information relating to the nature of a Bluetooth device.

Block: BluetoothDeviceInfoHealthTemplate

Description of a Bluetooth health device.

Field	Meaning
Info	Additional information relating to a Bluetooth health device. This field can contain one of the values listed in page BluetoothMinorDeviceHealth.

Block: BluetoothDeviceInfoImagingTemplate

Description of a Bluetooth imaging device.

Field	Meaning
Info	Additional information relating to a Bluetooth imaging device. This field can contain combined binary values listed in section BluetoothMinorDeviceClassImaging.

Block: BluetoothDeviceInfoNetworkApLoadFactorTemplate

Description of a Bluetooth network or access point device.

Field	Meaning
Info	Additional information relating to a Bluetooth network or access point device. This field can contain one of the values listed in page BluetoothMinorDeviceClassNetworkApLoadFactor.

Block: BluetoothDeviceInfoPeripheralTemplate

Description of a Bluetooth keyboard or pointer device.

Field	Meaning
Major	Additional information relating to a Bluetooth device that makes it possible to determine if the device is a keyboard or pointer. This field can contain one of the values listed in page BluetoothMinorDeviceClassPeripheralMajor.
Minor	Additional information relating to the nature of a Bluetooth device. This field can contain one of the values listed in page BluetoothMinorDeviceClassPeripheralMinor.

Block: BluetoothDeviceInfoPhoneTemplate

Description of a Bluetooth phone device.

Field	Meaning
Info	Additional information relating to a Bluetooth phone device. This field can contain one of the values listed in page BluetoothMinorDeviceClassPhone.

Block: BluetoothDeviceInfoTemplate

Description of a Bluetooth device.

Field	Meaning
ClassOfDevice	Device class value.
DeviceName	Name of the device.
MajorServiceClass	Value of the major service class. This field can contain combined binary values listed in section BluetoothMajorServiceClass.
MajorDeviceClass	Value of the major device class. This field can contain one of the values listed in page BluetoothMajorDeviceClass.
MinorDeviceClass	Value of the minor device class. More details on this block in section BluetoothDeviceInfoComputerTemplate, BluetoothDeviceInfoPhoneTemplate, BluetoothDeviceInfoNetworkApLoadFactorTemplate, BluetoothDeviceInfoAudioVideoTemplate, BluetoothDeviceInfoPeripheralTemplate, BluetoothDeviceInfoWearableTemplate, BluetoothDeviceInfoToyTemplate, BluetoothDeviceInfoHealthTemplate, BluetoothDeviceInfoDefaultTemplate.

Block: BluetoothDeviceInfoToyTemplate

Description of a Bluetooth toy device.

Field	Meaning
Info	Additional information relating to a Bluetooth toy device. This field can contain one of the values listed in page BluetoothMinorDeviceToy.

Block: BluetoothDeviceInfoWearableTemplate

Description of a Bluetooth wearable device.

Field	Meaning
Info	Additional information relating to a Bluetooth wearable device. This field can contain one of the values listed in page BluetoothMinorDeviceWearable.

Block: CertificateInformationRendering

Information about a certificate

Field	Meaning
Algorithm	Signature algorithm for the certificate.
IssuerCN	Issuer Common Name.
SubjectCN	Subject Common Name.
SigningTime	Date and time of the signature.
ValidityStart	Validity start date.
ValidityEnd	Validity end date.

Block: NotUsbDeviceInfoTemplate

Empty block that appears when a file was not accessed on a USB mass storage device.

Block: NotUsbVolumeTrackingDataTemplate

Empty block that appears when a file was not accessed on a USB mass storage device.

Block: PhysicalConsoleSessionTemplate

Block indicating data from the console session.

Field	Meaning
PhysicalConsoleSessionId	ID of the console session.
LoginUserName	Name of the user logged in to the console session ("domain name/user name" format).

Block: PnPDeviceInfoTemplate

Description of a plug and play device.

Field	Meaning
ClassGuid	GUID of the plug and play device class.
ClassName	Name of the plug and play device class.
DeviceDescription	Description of the plug and play device.
FriendlyName	Common name of the plug and play device.
Manufacturer	Vendor of the plug and play device.

Block: ProcessStaticInfoTemplate

Description of a process.

Field	Meaning
PID	ID of the process.
ProcessGuid	Unique ID generated by the agent for this process.
ProcessImageName	Path to the executable file of the process.
VolumeZone	Type of volume on which the item is located This field can contain combined binary values listed in section VolumeZone.
ProcessCommandLine	Command line of the process.
User	Security ID of the user whose token was used as the main token of the process. Note: This field is an SID. The **UserNameLookup** and **UserDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
IntegrityLevel	Security ID of the process integrity level. Note: This field is an SID. The **IntegrityLevelNameLookup** and **IntegrityLevelDomainLookup** automatic fields resolve this SID into a user name and a domain respectively.
SessionID	ID of the session during which the process is running.
HashMd5	MD5 hash of the main executable in the process.
HashSha1	SHA-1 hash of the main executable in the process.
HashSha256	SHA-256 hash of the main executable in the process.
IsProtectedOrCritical	Indicates whether the process is protected or critical.
CertificateSignatureState	Value indicating the digital signature status of a process. This field can contain one of the values listed in page CertificateSignatureState.
Certificates	Certificates that signed the process. More details on this block in section CertificateInformationRendering.
ProcessStartTime	Date and time the process session was started.
ProcessStartTimeRaw	Date and time the process session was started, represented as a whole number.
PEInformation	Information from the PE file

Block: RenamedFilesRendering

Partial list of the files renamed during a suspected ransomware attack.

Field	Meaning
SourceFilename	Name of the original file.
DestinationFilename	Name of the encrypted file.

Block: UsbDeviceInfoTemplate

Description of a USB device.

Field	Meaning
VendorId	ID of the USB device vendor.
ProductId	ID of the USB device model.
Class	USB device class. This field can contain one of the values listed in page UsbDeviceClass.
SubClass	USB device sub-class.
Protocol	Protocol of the USB device.
SerialNumber	Serial number of the USB device.
VendorName	Name of the USB device vendor.
ProductName	Name of the USB device model.
Interfaces	Interfaces of the USB device. More details on this block in section UsbDeviceInterfacesRendering.

Block: UsbDeviceInterfacesRendering

Information about the USB device.

Field	Meaning
Class	Device class. This field can contain one of the values listed in page UsbDeviceClass.
Subclass	Device sub-class.
Protocol	Protocol

Block: UsbVolumeTrackingDataTemplate

Tracking data of a USB volume.

Field	Meaning
EnrollFileState	Status of the enrollment file (absent, present but invalid, present but contains inconsistent data, present and valid). This field can contain one of the values listed in page UsbVolumeEnrollFileState.
FootprintFileState	Status of the hash file (absent, present but invalid, present but contains inconsistent data, present and valid). This field can contain one of the values listed in page UsbVolumeTrustFootprintFileState.
VendorId	ID of the USB device vendor as indicated in the enrollment file.
ProductId	ID of the USB device model as indicated in the enrollment file.
SerialNumberHashSha256	256 hash of the USB device serial number as indicated in the enrollment file.
EnrollGuid	Unique ID of the enrolled volume.

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.