DriveLock Events

List of DriveLock Events 2023.1

DriveLock SE 2023

Table of Contents

1 DriveLock Version 2023.1

The events apply to DriveLock version 2023.1.

1.1 List of all DriveLock events

Event ID	Source	Audit event	Severity	Short text	Long text
100	DriveLock	no	Information	Service installed	The [ServiceName] service was installed.
101	DriveLock	no	Information	Service removed	The [ServiceName] service was removed.
102	DriveLock	no	Error	Cannot remove service	The [ServiceName] service could not be removed.
103	DriveLock	no	Error	Control handler error	The control handler could not be installed.
104	DriveLock	no	Error	Initialization failed	The initialization process failed.
105	DriveLock	no	Information	Service started	The [ServiceName] service was started. Version: [InstalledVersion]

Event ID	Source	Audit event	Severity	Short text	Long text
106	DriveLock	no	Error	Unsupported request	The [ServiceName] service received an unsupported request.
107	DriveLock	no	Information	Debug message	Debug: [DebugMsg]
108	DriveLock	no	Information	Service stopped	The service [ServiceName] was stopped.
109	DriveLock	no	Information	Trace message	Trace: [DebugMsg]
110	DriveLock	no	Audit	Drive connected and unlocked	The drive [DriveLetter] ([StorageType]) was added to the system. It is a [StorageBus] bus device. The drive is [UserLockState] for this event's user account. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [DriveLetter]0 Hardware Id: [DriveLetter]1

Event ID	Source	Audit event	Severity	Short text	Long text
111	DriveLock	no	Audit	Drive connected and controlled	The drive [DriveLetter] ([StorageType]) was added to the system. It is controlled by DriveLock because of company policy. As an ACL was applied to the drive, some users may no longer be able to access it. It is a [StorageBus] bus device. The drive is [UserLockState] for this event's user account. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [DriveLetter]0 Hardware Id: [DriveLetter]1
112	DriveLock	no	Audit	Drive connected, error locking drive	The drive [DriveLetter] ([StorageType]) was added to the system. It was not locked due to a system error. It is a [StorageBus] bus device. The drive should be [UserLockState] for this event's user account. Device Id:

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [DriveLetter]0 Hardware Id: [DriveLetter]1
113	DriveLock	no	Audit	Drive disconnected	The drive [DriveLetter] was disconnected from the system. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
114	DriveLock	no	Information	Drive unlocked	The drive [DriveLetter] was unlocked on the system. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]

Event ID	Source	Audit event	Severity	Short text	Long text
115	DriveLock	no	Audit	Drive state changed	The drive [DriveLetter] ([StorageType]) will be controlled by DriveLock. As an ACL was applied to the drive, some users may no longer be able to access it. It is a [StorageBus] bus device. The drive is [UserLockState] for this event's user account. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [DriveLetter]0 Hardware Id: [DriveLetter]1
116	DriveLock	no	Error	Drive locking error	Locking of drive [DriveLetter] ([StorageType]) was attempted but the system reported an error. It is a [StorageBus] bus device. The drive should be [UserLockState] for this event's user account. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [DriveLetter]0 Hardware Id: [DriveLetter]1
117	DriveLock	no	Information	Licensing message	Licensing: [LicenseInfo]
118	DriveLock	no	Error	Account error	Cannot add account [UserName] (domain [DomainName]) to the allow list.
119	DriveLock	no	Error	Configuration file error	Configuration file error: [FileName]
120	DriveLock	no	Audit	Serial port locked	The serial port [HardwareID] is controlled by DriveLock because of company policy. As an ACL was applied to the port, some users may no longer

Event ID	Source	Audit event	Severity	Short text	Long text
					be able to access it. Friendly name: [DisplayName] Hardware Id: [CompatibleID] Class Id: [ClassID]
121	DriveLock	no	Error	Error locking serial port	Locking of serial port [HardwareID] was attempted but the system reported an error. Friendly name: [DisplayName] Hardware Id: [CompatibleID] Class Id: [ClassID]
122	DriveLock	no	Error	Windows Firewall error	Error while configuring the Windows Firewall. DriveLock remote control may not work on this agent. Error code: [ErrorCode] Error: [ErrorMessage]
123	DriveLock	no	Warning	No GPO present	Warning: No Group Policy configuration present.
124	DriveLock	no	Information	Device restarted	The device [DisplayName] is managed

Event ID	Source	Audit event	Severity	Short text	Long text
					by DriveLock and was restarted due to a user change. Hardware ID: [HardwareID] Class ID: [ClassID]
125	DriveLock	no	Error	Device restart - Error	The device [DisplayName] is managed by DriveLock. The current user changed but there was an error restarting the device. Hardware ID: [HardwareID] Class ID: [ClassID]
126	DriveLock	no	Warning	Device restart - Needs reboot	DriveLock attempted to restart the managed device [DisplayName] due to a user change but the device does not support this. A reboot is required to re-enable the device. Hardware ID: [HardwareID] Class ID: [ClassID]
127	DriveLock	no	Audit	Parallel port locked	The parallel port [DisplayName] is controlled by DriveLock because of company policy. As an ACL was applied to the port, some users may no longer be able to access it. Friendly name:

Event ID	Source	Audit event	Severity	Short text	Long text
					[HardwareID] Hardware Id: [CompatibleID] Class Id: [ClassID]
128	DriveLock	no	Error	Error locking parallel port	Locking of parallel port [DisplayName] was attempted but the system reported an error. Friendly name: [HardwareID] Hardware Id: [CompatibleID] Class Id: [ClassID]
129	DriveLock	no	Audit	Device connected and locked	The device [DisplayName] was connected to the computer. It was locked due to company policy. Device type: [DeviceType] Hardware ID: [HardwareID] Class ID: [ClassID] Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
130	DriveLock	no	Audit	Device connected and	The device [DisplayName] was con-

Event ID	Source	Audit event	Severity	Short text	Long text
				not locked	nected to the computer. Device type: [DeviceType] Hardware ID: [HardwareID] Class ID: [ClassID] Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
131	DriveLock	no	Audit	Temporarily unlocked	DriveLock Agent was temporarily unlocked by an administrator. Administrator computer: [ComputerName] (unique ID [ComputerGuid]) Administrator account: [UserName2] (domain [DomainName2], SID [SID]) Unlock period: [UnlockTime] [UnlockUnit] Reason: [Reason]
132	DriveLock	no	Audit	Temporary unlocked cancelled	The temporary unlock mode of the DriveLock Agent was canceled by an administrator. Administrator computer: [ComputerName] (unique ID [ComputerGuid]) Administrator account: [UserName2] (domain

Event ID	Source	Audit event	Severity	Short text	Long text
					[DomainName2], SID [SID])
133	DriveLock	no	Audit	File accessed	File accessed. File path: [Path] File name: [Path]1 Drive: [Path]2 File size: [Size] File name hash: [MD5Hash] File content hash: [Path]0 Access direction: [AccessDirection] Process: [ProcessName] Device identification: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
134	DriveLock	no	Error	Agent not licensed	DriveLock is not licensed to run on this computer.
135	DriveLock	no	Error	Logon error	The user [UserName] cannot be impersonated on this computer. Please check the user name and password in the configuration. Error code:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorCode] Error: [ErrorMessage]
136	DriveLock	no	Error	Shadow copy upload error	Cannot upload shadow copy file [FileName] to the central storage location [UploadLocation]. Error code: [ErrorCode] Error: [ErrorMessage]
137	DriveLock	no	Warning	Conflicting policy detected	A Microsoft policy that can conflict with a DriveLock policy was detected on this computer. Refer to the DriveLock Manual for more information about this policy. It is recommended to disable the Microsoft policy.
138	DriveLock	no	Error	CD writer - Reboot required	A CD writer ([DriveLetter]) was restarted to change CD burning permissions. Windows reported that a reboot is needed to complete the change. The drive may be disabled

Event ID	Source	Audit event	Severity	Short text	Long text
					until the next reboot.
139	DriveLock	no	Warning	Temporary unlock ended	The temporary unlock mode of the DriveLock Agent ended because the unlock time elapsed.
140	DriveLock	no	Audit	Volume mounted	A DriveLock encrypted volume was mounted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Drive letter: [DriveLetter] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
141	DriveLock	no	Audit	Volume unmounted	A DriveLock encrypted volume was unmounted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Drive letter:

Event ID	Source	Audit event	Severity	Short text	Long text
					[DriveLetter] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
142	DriveLock	no	Audit	Volume created	A DriveLock encrypted volume was created/formatted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] File system: [FileSystemType] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
143	DriveLock	no	Audit	Password changed	The password for a DriveLock encrypted volume was changed. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber])

Event ID	Source	Audit event	Severity	Short text	Long text
					(Serial number [HWSerialNumber])
144	DriveLock	no	Information	Network changed	A network connection was changed. Network adapter: [NetAdapter] Network location name: [DisplayName] Network location GUID: [ObjectID]
145	DriveLock	no	Audit	File blocked by content scanner	File blocked by content scanner. Content does not match file extension. File path: [Path] File name: [Path]1 Drive: [Path]2 File size: [Size] File name hash: [MD5Hash] File content hash: [Path]0 Access direction: [AccessDirection] Process: [ProcessName] Device ID: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])

Event ID	Source	Audit event	Severity	Short text	Long text
146	DriveLock	no	Audit	Process blocked	The execution of a process was blocked by company policy. Process: [ProcessName] File Hash: [ProcessHash] Applied rule: [ObjectID] Rule type: [WlType]
147	DriveLock	no	Audit	Process started	A process was started. Process: [ProcessName] File Hash: [ProcessHash] Applied rule: [ObjectID] Rule type: [WlType]
148	DriveLock	no	Audit	File extension blocked	File blocked by file filter. Access denied due to file type. File path: [Path] File name: [Path]1 Drive: [Path]2 File size: [Size] File name hash: [MD5Hash] File content hash: [Path]0 Access direction: [AccessDirection] Process: [ProcessName] Device ID: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])

Event ID	Source	Audit event	Severity	Short text	Long text
149	DriveLock	no	Warning	Network profile shutdown	The computer is shut down because of a Network Profiles policy. Network location GUID: [ObjectID]
150	DriveLock	no	Warning	Network adapter disabled	Network adapters are disabled because of a Network Profiles policy. Network location GUID: [ObjectID]
151	DriveLock	no	Warning	Windows Terminal Services disabled	Windows Terminal Services are disabled on this computer. DriveLock depends on Terminal Services to detect user changes in real-time. Legacy functions are used to maintain DriveLock functionality, consider enabling Terminal Services.
152	DriveLock	no	Warning	Policy storage extraction failed	The policy storage container [PolicyStorageContainer] cannot be unpacked to the local computer. Some functions relying on files stored in this container may fail.

Event ID	Source	Audit event	Severity	Short text	Long text
153	DriveLock	no	Warning	Configuration file applied	The configuration file [FileName] was successfully applied.
154	DriveLock	no	Error	Configuration file download error	The configuration file [FileName] could not be downloaded. Error code: [ErrorCode] Error: [ErrorMessage]
155	DriveLock	no	Error	Configuration file error	The configuration file [FileName] could not be loaded into the local registry. Error code: [ErrorCode] Error: [ErrorMessage]
156	DriveLock	no	Error	Configuration file error	A temporary copy of the configuration file [FileName] could not be created. Error code: [ErrorCode] Error: [ErrorMessage]
157	DriveLock	no	Warning	Configuration file error	The configuration file [FileName] is invalid or corrupt. Error code: [ErrorCode] Error: [ErrorMessage]
158	DriveLock	no	Warning	Configuration file	The configuration file [FileName]

Event ID	Source	Audit event	Severity	Short text	Long text
				error	could not be read. Error code: [ErrorCode] Error: [ErrorMessage]
159	DriveLock	no	Warning	Account error	User account [UserName] could not be impersonated to access the configuration file [FileName]. Error code: [ErrorCode] Error: [ErrorMessage]
160	DriveLock	no	Warning	Disk Protection installation error	Not enough disk space available to install and configure Disk Protection. Required disk space: [RequiredSpace] bytes Available disk space: [AvailableSpace] bytes
161	DriveLock	no	Error	Account error	User account [UserName] could not be impersonated to access the Disk Protection package. Error code: [ErrorCode] Error: [ErrorMessage]
162	DriveLock	no	Warning	Disk Protection package download error	The Disk Protection package could not be downloaded from [URL] Error code: [ErrorCode] Error: [ErrorMes-

Event ID	Source	Audit event	Severity	Short text	Long text
					sage]
163	DriveLock	no	Warning	Disk Protection installation error	The Disk Protection package is not installed locally.
164	DriveLock	no	Warning	Disk Protection download successful	The Disk Protection package was successfully downloaded.
165	DriveLock	no	Warning	Disk Protection installation error	The Disk Protection package could not be extracted. The file [PackagePath] may be missing or corrupt.
166	DriveLock	no	Warning	Disk Protection installation error	The Disk Protection configuration script [ScriptFile] is missing in the DriveLock policy.
167	DriveLock	no	Warning	Disk Protection installation error	The command line [CmdLine] could not be executed. Error code: [ErrorCode] Error: [ErrorMessage]
168	DriveLock	no	Warning	Disk Protection install-	Disk Protection was successfully

Event ID	Source	Audit event	Severity	Short text	Long text
				ation successful	installed.
169	DriveLock	no	Warning	Disk Protection installation error	Disk Protection installation failed.
170	DriveLock	no	Warning	Disk Protection installation error	Disk Protection is configured on this computer but the installation failed.
171	DriveLock	no	Warning	Disk Protection installation error	The status information file [FileName] could not be created.
172	DriveLock	no	Warning	Disk Protection installation error	The Disk Protection configuration script [FileName] could not be copied to its target location. Error code: [ErrorCode] Error: [ErrorMessage]
173	DriveLock	no	Audit	File created	New file created. File path: [Path] File name: [Path]1 Drive: [Path]2 File size: [Size] File name hash: [MD5Hash] File content hash: [Path]0 Access direction: [AccessDirection] Process: [ProcessName] Device identification:

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
174	DriveLock	no	Warning	Disk Protection installation prevented	The Disk Protection should be installed but the installation is prevented by administrative intervention.
175	DriveLock	no	Warning	Disk Protection installation error	The Disk Protection setup could not clean up installation files. Error code: [ErrorCode] Error: [ErrorMessage]
176	DriveLock	no	Warning	Pre-boot authentication error	Pre-boot authentication is configured on this computer but the initialization failed.
179	DriveLock	no	Warning	Disk Protection	Disk Protection started encrypting

Event ID	Source	Audit event	Severity	Short text	Long text
				encryption started	local hard disks.
181	DriveLock	no	Warning	Disk Protection encryption successful	Disk Protection successfully encrypted local hard disks.
183	DriveLock	no	Warning	Disk Protection decryption started	Disk Protection started decrypting local hard disks.
184	DriveLock	no	Warning	Disk Protection decryption successful	Disk Protection successfully decrypted local hard disks.
185	DriveLock	no	Warning	Disk Protection upload error	The Disk Protection data [LogFile] could not be uploaded to the DriveLock Enterprise Service. Error [ErrorMessage]
186	DriveLock	no	Warning	Disk Protection system error	The log file [LogArchive] could not be added to the log archive [LogFile].
187	DriveLock	no	Warning	Disk Protection system error	Emergency Recovery Information could not be moved to [TargetFolder]. Error code: [ErrorCode] Error:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorMessage]
188	DriveLock	no	Warning	Disk Protection uninstallation successful	Disk Protection was successfully uninstalled.
189	DriveLock	no	Error	Disk Protection installation - wrong package version	Disk Protection installation or update was aborted because the wrong version of the installation package was detected. Installed version: [InstalledVersion] Expected version: [ExpectedVersion]
190	DriveLock	no	Warning	File already present	The file [PolicyStorageContainer] already existed in the temporary location when extracting Policy File storage from file [FileName].
191	DriveLock	no	Warning	DriveLock Enterprise Service selected	The DriveLock Enterprise Service [DesName] was selected by DriveLock. Connection ID: [ObjectID] Used for: [AgentServerType]

Event ID	Source	Audit event	Severity	Short text	Long text
192	DriveLock	no	Warning	DriveLock Enterprise Service not available	No DriveLock Enterprise Service is available because no valid server connection is configured.
193	DriveLock	no	Warning	Command line execution error	The file [CmdLine] does not exist while trying to execute an event command or script.
194	DriveLock	no	Warning	Command line execution error	A process could not be created while executing an event command or script. Command line: [CmdLine] Error code: [ErrorCode] Error: [ErrorMessage]
195	DriveLock	no	Warning	Agent communication failed	Internal agent communication failed while executing an event command or script with user permissions. Command line: [CmdLine] Error code: [ErrorCode] Error: [ErrorMessage]
196	DriveLock	no	Warning	Command line not executed	No user is logged on. Therefore an event command or script could not be

Event ID	Source	Audit event	Severity	Short text	Long text
					executed with user permissions. Command line: [CmdLine]
197	DriveLock	no	Warning	Command line executed (user)	An event command or script was executed with user permissions. Command line: [CmdLine]
198	DriveLock	no	Warning	Command line executed	An event command or script was executed with system permissions. Command line: [CmdLine]
199	DriveLock	no	Warning	Drive temporarily unlocked	Drive types temporarily unlocked by administrative intervention are [DriveType1] [DriveType2] [DriveType3] [DriveType4] [DriveType5] [DriveType6] [DriveType7] [DriveType8] [DriveType9] [DriveType1]0
200	DriveLock	no	Warning	Devices temporarily unlocked	Device classes temporarily unlocked by administrative intervention are: [DeviceTypes]

Event ID	Source	Audit event	Severity	Short text	Long text
202	DriveLock	no	Warning	File copy error	Copying existing files failed while encrypting volume [FileName]. Volume GUID: [VolumeID]
203	DriveLock	no	Warning	Files deleted	Existing files were deleted from volume [FileName]. Reason: [AcDeleteReason] Volume GUID: [VolumeID]
205	DriveLock	no	Warning	File delete error	Deleting existing files failed while encrypting volume [FileName]. Volume GUID: [VolumeID]
206	DriveLock	no	Warning	Disk Protection uninstallation failed	Disk Protection uninstallation failed.
207	DriveLock	no	Warning	Disk Protection cannot apply configuration	The Disk Protection configuration could not be applied.
208	DriveLock	no	Warning	Disk Protection key backup failed	The Disk Protection key backup failed.

Event ID	Source	Audit event	Severity	Short text	Long text
209	DriveLock	no	Warning	Disk Protection no license	Disk Protection is configured to encrypt local hard disks but is not licensed on this computer.
210	DriveLock	no	Warning	Cannot enumerate PBA users	Disk Protection cannot enumerate configured pre-boot authentication users.
211	DriveLock	no	Warning	Cannot add user to PBA	Disk Protection cannot add user [UserName] (domain [DomainName]) to the pre-boot authentication user database.
212	DriveLock	no	Warning	Cannot remove user from PBA	Disk Protection cannot remove user [UserName] (domain [DomainName]) from the pre-boot authentication user database.
213	DriveLock	no	Warning	Cannot deactivate PBA	Pre-boot authentication cannot be deactivated while the hard disk is encrypted. The DriveLock configuration is inconsistent and should

Event ID	Source	Audit event	Severity	Short text	Long text
					be changed so that pre-boot authentication is active while hard disks are encrypted.
214	DriveLock	no	Warning	Could not read recovery information	Encrypted container recovery information could not be read from file [FileName] in order to upload this information to the server. Error code: [ErrorCode] Error: [ErrorMessage]
215	DriveLock	no	Warning	Server or network error while uploading recovery information	Uploading encrypted container recovery information from file [FileName] failed with a server or network error. Error: [ErrorMessage]
216	DriveLock	no	Warning	Server or network error while uploading status file	Uploading of status file [FileName] failed with a server or network error. Error: [ErrorMessage]
217	DriveLock	no	Warning	Incompatible server version (needs	The configured server is not compatible with this version of the agent.

Event ID	Source	Audit event	Severity	Short text	Long text
				update)	It must be upgraded in order to support all features of this version. Missing method: [MethodName]
218	DriveLock	no	Audit	File accessed	File accessed. File path: [Path] File name: [FileName] File name hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
219	DriveLock	no	Warning	File extension blocking	File blocked. Access to file extension is not allowed. File path: [Path] File name: [FileName] File name hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
220	DriveLock	no	Warning	Internal error with recovery information	An internal error occurred while creating recovery information for encrypted volume [FileName]. Volume GUID: [VolumeID]

Event ID	Source	Audit event	Severity	Short text	Long text
221	DriveLock	no	Warning	Application hash database missing	The application hash database [FileName] is missing from the policy file storage. Please check if the group policy or configuration file is correctly applied. Rule: [ObjectID]
222	DriveLock	no	Warning	Cannot open application hash database	The application hash database [FileName] cannot be opened. Please verify the file using Management Console. The underlying application rule will not function. Rule: [ObjectID]
223	DriveLock	no	Warning	Cannot apply application hash database	The application hash database [FileName] cannot be stored and applied to the Application Launch Filter driver. The underlying application rule will not function. Rule: [ObjectID]
224	DriveLock	no	Warning	Encrypted volume password recovered	A DriveLock Encrypted volume password was recovered. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID]

Event ID	Source	Audit event	Severity	Short text	Long text
					Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
225	DriveLock	no	Warning	Illegal offline unlock attempt	DriveLock detected an illegal attempt to unlock the agent using the offline unlock functionality.
226	DriveLock	no	Warning	Offline unlock requested	An offline unlock request was initiated by the user. Request code: [RequestCode]
227	DriveLock	no	Error	DriveLock program file tampered	A DriveLock program file was tampered or changed or the digital signature could not be verified. File: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
228	DriveLock	no	Warning	Event queue full	The event queue was full and wrapped. Some older events were

Event ID	Source	Audit event	Severity	Short text	Long text
					deleted and will not be forwarded to external targets.
229	DriveLock	no	Warning	Running in simulation mode	DriveLock is running in simulation mode. Nothing will be locked or filtered.
230	DriveLock	no	Warning	SSL: Cannot create DH parameters	The encrypted communications layer (SSL) could not create key exchange parameters (DH). Default values will be used resulting in weaker encryption.
231	DriveLock	no	Error	SSL: Cannot generate self-signed certificate	The encrypted communications layer (SSL) could not create the self-signed certificate used for encryption. SSL will be unavailable. Error code: [ErrorCode] Error: [ErrorMessage]
232	DriveLock	no	Error	SSL: Cannot open certificate file	The encrypted communications layer (SSL) cannot open the certificate file used for encryption. SSL will be

Event ID	Source	Audit event	Severity	Short text	Long text
					unavailable. Certificate file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
233	DriveLock	no	Error	SSL: Cannot convert certificate	The encrypted communications layer (SSL) could not convert the certificate used for encryption to its internal format. SSL will be unavailable. Error code: [ErrorCode] Error: [ErrorMessage]
234	DriveLock	no	Error	Cannot add port to Windows Firewall exceptions	Error while adding a port exception to the Windows Firewall. DriveLock remote control may not work on this agent. Port: [Port] Error code: [ErrorCode] Error: [ErrorMessage]
235	DriveLock	no	Error	SSL: Cannot set up	The encrypted communications layer (SSL) could not be set up. Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
236	DriveLock	no	Error	Remote control: Cannot set up server	The remote control server component coud not be set up. Agent remote control will be unavailable. Error: [ErrorMessage]
237	DriveLock	no	Error	Remote control: Internal error	Agent remote control: An internal SOAP communications error occurred. Error: [ErrorMessage]
238	DriveLock	no	SuccessAudit	Remote control: Function called	An Agent remote control function was called. Calling IP address: [IPAddress] Called function: [FunctionName]
239	DriveLock	no	SuccessAudit	Remote control: HTTP-GET request	A HTTP-GET request was sent to the Agent. Requesting IP address: [IPAddress] Requested URL: [URL]
240	DriveLock	no	Warning	GPO: Cannot cache locally	A DriveLock group policy configuration database could not be cached locally. GPO Object GUID: [ObjectID] GPO Name: [GpoName] Database file: [FileName] Error code:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorCode] Error: [ErrorMessage]
241	DriveLock	no	Error	GPO: Cannot open and extract	A DriveLock group policy configuration database could no opened and extracted. Settings from this GPO object will not be applied. GPO Object GUID: [ObjectID] GPO Name: [GpoName] Database file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
242	DriveLock	no	Error	GPO: Fall-back configuration applied	A group policy configuration was detected but no settings could be retrieved from the configuration databases. DriveLock will fall-back to a configuration where all removable drives are blocked.
243	DriveLock	no	Error	GPO: Cannot open	A group policy configuration data-

Event ID	Source	Audit event	Severity	Short text	Long text
				database	base could not be opened. Database file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
244	DriveLock	no	Error	GPO: Cannot access GPO	DriveLock Agent cannot access Windows group policy configuration. Error code: [ErrorCode] Error: [ErrorMessage]
245	DriveLock	no	Information	GPO: Configuration applied	A group policy configuration was applied. GPO Object GUID: [ObjectID] GPO Name: [GpoName] GPO Linked from: [GpoLinkedFrom]
246	DriveLock	no	Error	Cannot store configuration status	The Agent cannot store the configuration status used by other DriveLock components. Error code: [ErrorCode] Error: [ErrorMessage]
247	DriveLock	no	Error	Cannot initialize configuration store	DriveLock Agent cannot initialize the configuration database stores.

Event ID	Source	Audit event	Severity	Short text	Long text
248	DriveLock	no	Error	DES: Queued file was deleted	A file queued for uploading to the DriveLock Enterprise Service was deleted locally before it could be uploaded. File name: [FileName]
249	DriveLock	no	Error	Configuration file: Fall-back configuration applied	A configuration using configuration files was detected but no settings could be retrieved from a configuration database. DriveLock will fall-back to a configuration where all removable drives are blocked.
250	DriveLock	no	Warning	Configuration file: Using cached copy	The configuration file [FileName] could not be loaded from it's original location. A locally cached copy was used.
251	DriveLock	no	Error	Configuration file: Cannot extract	A DriveLock configuration file could no be extracted. Settings from this file will not be applied. Database file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
252	DriveLock	no	SuccessAudit	Usage policy accepted	Usage policy for drive [DriveLetter] was accepted by the user. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
253	DriveLock	no	FailureAudit	Usage policy declined	Usage policy for drive [DriveLetter] was declined by the user. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
254	DriveLock	no	Warning	Usage policy: No user logged in	Usage policy for drive [DriveLetter] was not presented as no user is currently logged on. Proceeding as if the policy was declined.
255	DriveLock	no	Information	Deferred hash completed	Deferred content hash generation completed. File path: [Path] File name: [FileName] Drive: [DriveLetter] File

Event ID	Source	Audit event	Severity	Short text	Long text
					name hash: [MD5Hash] File content hash: [MD5Hash] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
256	DriveLock	no	Information	File content changed	File content changed. File path: [Path] File name: [FileName] Drive: [Path]0 Old file name hash: [MD5Hash] Old file content hash: [MD5Hash] New file content hash: [MD5Hash] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
257	DriveLock	no	SuccessAudit	File deleted	File deleted. Process: [Path]0 File path: [Path] File name: [FileName] Drive: [DriveLetter] File name hash: [MD5Hash] File content hash: [MD5Hash] Device Id: [HWVendorID]

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
258	DriveLock	no	SuccessAudit	File renamed	File renamed. Process: [Path]2 Old file path: [Path] Old file name: [Path]0 New file name: [FileName] Old file name hash: [MD5Hash] File content hash: [MD5Hash] New file name hash: [MD5Hash] Drive: [Path]1 Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
259	DriveLock	no	Information	FIPS mode enabled	DriveLock uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1051) running on a Windows platform per FIPS 140-2

Event ID	Source	Audit event	Severity	Short text	Long text
					Implementation Guidance section G.5 guidelines. FIPS mode was successfully enabled.
260	DriveLock	no	Error	FIPS mode activation failed	DriveLock encryption: FIPS mode could not be activated due to error [ErrorMessage].
261	DriveLock	no	Error	Cannot start driver	Cannot start the device driver [DriverName]. DriveLock may not function correctly. Error code: [ErrorCode] Error: [ErrorMessage]
262	DriveLock	no	Error	ALF driver communication error	An error occurred while communicating with the Application Launch Filter device driver. Error code: [ErrorCode] Error: [ErrorMessage]
263	DriveLock	no	Error	Error determining process details	An error occurred while determining detailed information for a process. Process: [ProcessName] File Hash:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ProcessHash]
264	DriveLock	no	Error	Cannot merge GPO into RSoP	Cannot merge the GPO configuration database [FileName] into the resulting set of policy.
265	DriveLock	no	Error	Cannot merge Registry into RSoP	Cannot merge GPO registry information into the resulting set of policy.
266	DriveLock	no	Error	Cannot start encryption driver	Cannot open or start the encryption device driver. Error code: [ErrorCode] Error: [ErrorMessage]
267	DriveLock	no	Error	Cannot install encryption driver	Cannot install the encryption device driver. Function: [Function] Error code: [ErrorCode] Error: [ErrorMessage]
268	DriveLock	no	Error	Cannot upgrade Mobile Encryption Application	Mobile Encryption Application cannot be automatically updated. Target location: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
269	DriveLock	no	Error	Cannot attach CD/DVD filtering driver	The CD/DVD filtering driver cannot be attached to a drive. Drive letter: [DriveLetter] Error code: [ErrorCode] Error: [ErrorMessage]
270	DriveLock	no	Error	Cannot apply CD/DVD filtering configuration	The drive filtering configuration cannot be applied to the CD/DVD filtering driver. Incorrect access permissions / filtering may be set. Drive letter: [DriveLetter] Error code: [ErrorCode] Error: [ErrorMessage]
271	DriveLock	no	SuccessAudit	CD/DVD write operation started	A CD/DVD write operation was started on drive [DriveLetter]. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName] Hardware Id: [HardwareID]
272	DriveLock	no	FailureAudit	CD/DVD write operation blocked	A CD/DVD write operation was blocked on drive [DriveLetter]. Device Id: [HWVendorID] [HWProductID]

Event ID	Source	Audit event	Severity	Short text	Long text
					(Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName] Hardware Id: [HardwareID]
273	DriveLock	no	Information	CD/DVD write operation finished	A CD/DVD write operation was finished on drive [DriveLetter]. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName] Bytes written: [DataSize] Hardware Id: [HardwareID]
274	DriveLock	no	SuccessAudit	CD/DVD media erase operation executed	A CD/DVD media erase operation was executed on drive [DriveLetter]. The media was [BlankMethod] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName] Hardware Id: [HardwareID]

Event ID	Source	Audit event	Severity	Short text	Long text
275	DriveLock	no	SuccessAudit	CD/DVD media erase operation blocked	A CD/DVD media erase operation was blocked on drive [DriveLetter]. The media should be [BlankMethod] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName] Hardware Id: [HardwareID]
276	DriveLock	no	Information	System verification successfull	A system verification operation on drive [DriveLetter] was executed and succeeded. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Status: [ActionResult] Hardware Id: [HardwareID]
277	DriveLock	no	Error	System verification failed	A system verification operation on drive [DriveLetter] was executed and reported a problem. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWSerialNumber]) Status: [ActionResult] Hardware Id: [HardwareID]
278	DriveLock	no	Error	No or wrong enforced encryption settings	A drive is configured for enforced encryption but enforced encryption settings are either not present or you configured a FIPS-only mode for encryption and selected an incompatible algorithm for enforced encryption. The drive will be blocked and no encryption is executed.
279	DriveLock	no	Error	Cannot send SNMP trap	A SNMP trap could not be sent to the configured trap receiver. Function name: [ErrorMessage] Error code: [ErrorCode]
280	DriveLock	no	Error	Cannot load file filter DLL	Cannot load a configured file filtering dynamic link library (DLL). DLL file:

Event ID	Source	Audit event	Severity	Short text	Long text
					[FileName] Error code: [ErrorCode] Error: [ErrorMessage]
281	DriveLock	no	Error	Cannot find function in DLL	Cannot find the configured function [FunctionName] in a filtering dynamic link library (DLL). DLL file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
282	DriveLock	yes	Audit	Temporarily unlocked (offline)	DriveLock Agent was temporarily unlocked using offline unlocking. Unlock period: [UnlockTime] [Unlock-Unit]
283	DriveLock	no	Information	Drive connected to thin client	The drive [DriveLetter] (mounted as [FileName]) was added to thin client [ComputerName] (unique ID [ComputerGuid]). Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])

Event ID	Source	Audit event	Severity	Short text	Long text
284	DriveLock	no	Information	Drive disconnected from thin client	The drive [DriveLetter] (mounted as [FileName]) was disconnected from thin client [ComputerName] (unique ID [ComputerGuid]). Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
285	DriveLock	no	Error	Enforced encryption - Formatting error	An error occurred while creating an encrypted volume during enforced encryption. Container: [DebugMsg] Error text: [FunctionName] Error code: [ErrorCode] Error: [ErrorMessage]
286	DriveLock	no	Error	No server defined for recovery	No server is defined for uploading encryption recovery information.
287	DriveLock	no	Error	No server defined for inventory	No server is defined for uploading collected inventory data.
288	DriveLock	no	Information	Inventory collection successful	Hard- and software inventory data was successfully collected and

Event ID	Source	Audit event	Severity	Short text	Long text
					uploaded. DES server: [DesName] Connection ID: [ObjectID]
289	DriveLock	no	Information	Inventory collection failed	An error occurred while collecting hard- and software inventory data. DES server: [DesName] Connection ID: [ObjectID] Error: [ErrorMessage]
290	DriveLock	no	Warning	Uninstallation password configured	An uninstallation password is configured. Please refer to the DriveLock manual if you want to update this Agent.
291	DriveLock	no	Error	Cannot start mDNS/DNS-SD responder	The DriveLock mDNS/DNS-SD responder could not be started. Zero-configuration functions will not be available Error code: [ErrorCode] Error: [ErrorMessage]
292	DriveLock	no	Error	DNS-SD service registration failed	DNS-SD service registration of the DriveLock Agent failed.

Event ID	Source	Audit event	Severity	Short text	Long text
293	DriveLock	no	Information	Security awareness campaign element acknowledged	A security awareness campaign element was acknowledged by the user. Campaign element: [ObjectID] Element description: [DisplayName]
294	DriveLock	no	Error	Cannot download centrally stored policy	The centrally stored policy [ConfigId] could not be downloaded. Server: [ServerName] Error: [ErrorMessage]
295	DriveLock	no	Error	Centrally stored policy: Cannot extract	A centrally stored policy could no be extracted. Settings from this file will not be applied. Configuration ID: [ConfigId] Error code: [ErrorCode] Error: [ErrorMessage]
296	DriveLock	no	Warning	Centrally stored policy: Using cached copy	The centrally stored policy [ConfigId] could not be loaded from the server. A locally cached copy was used.
297	DriveLock	no	Error	Centrally stored policy: Fall-back configuration applied	A configuration using centrally stored policies was detected but no settings could be retrieved from a server.

Event ID	Source	Audit event	Severity	Short text	Long text
					DriveLock will fall-back to a configuration where all removable drives are blocked.
298	DriveLock	no	Information	Centrally stored policy applied	The centrally stored policy [ConfigId] was successfully applied.
299	DriveLock	no	Information	Centrally stored policy downloaded	The centrally stored policy [DisplayName] was successfully downloaded. Configuration ID: [ConfigId] Version: [InstalledVersion]
300	DriveLock	no	Information	iTunes-synchronized device connected	An iTunes-synchronized device has been connected. HardwareID: [HardwareID] Device: [DisplayName] Serial: [Serial] IMEI: [IMEI] Firmware: [FirmwareVersion]
301	DriveLock	no	Information	iTunes-synchronized device disconnected	An iTunes-synchronized device has been disconnected. HardwareID: [HardwareID] Device: [DisplayName]

Event ID	Source	Audit event	Severity	Short text	Long text
					Serial: [Serial] IMEI: [IMEI] Firmware: [FirmwareVersion]
302	DriveLock	no	Information	File synchronized (iTunes-synchronized device)	File synchronized with iTunes-synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]
303	DriveLock	no	Information	Contacts synchronized (iTunes-synchronized device)	Contacts synchronized with iTunes-synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]
304	DriveLock	no	Information	Calendar syn-	Calendar synchronized with iTunes-

Event ID	Source	Audit event	Severity	Short text	Long text
				chronization (iTunes-synchronized device)	synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]
305	DriveLock	no	Information	Bookmarks synchronization (iTunes-synchronized device)	Bookmarks synchronized with iTunes-synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]
306	DriveLock	no	Information	Notes synchronized (iTunes-synchronized device)	Notes synchronized with iTunes-synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]

Event ID	Source	Audit event	Severity	Short text	Long text
307	DriveLock	no	Information	Mail accounts synchronized (iTunes-synchronized device)	Mail accounts synchronized with iTunes-synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]
308	DriveLock	no	Error	Apple driver communication error	An error occurred while communicating with the Apple filter device driver. Error code: [ErrorCode] Error: [ErrorMessage]
309	DriveLock	no	Error	Cannot initialize apple filter device driver	Apple filter device driver could not be initialized. Error code: [ErrorCode] Error: [ErrorMessage]
310	DriveLock	no	Error	Antivirus installation failed	Installation of Antivirus failed. Error code: [ErrorCode] Error: [ErrorMessage]
311	DriveLock	no	Error	Initial Antivirus con-	Initial configuration of Antivirus failed.

Event ID	Source	Audit event	Severity	Short text	Long text
				figuration failed	Service: [ServiceName] ([FunctionName]) Error code: [ErrorCode] Error: [ErrorMessage]
312	DriveLock	no	Error	Antivirus uninstallation failed	Uninstallation of Antivirus failed. Error code: [ErrorCode] Error: [ErrorMessage]
313	DriveLock	no	Error	Antivirus initialization failed	Initialization of Antivirus failed. Error code: [ErrorCode] Error: [ErrorMessage]
314	DriveLock	no	Error	Antivirus configuration failed	Configuration of Antivirus failed. Setting: [FunctionName] Error code: [ErrorCode] Error: [ErrorMessage]
315	DriveLock	no	Error	Antivirus quarantine initialization failed	Initialization of Antivirus quarantine failed. Error code: [ErrorCode] Error: [ErrorMessage]
316	DriveLock	no	FailureAudit	Malware detected	Virus or malware detected. Detected malware: [DetectionName] ([Detec-

Event ID	Source	Audit event	Severity	Short text	Long text
					tionType]) Scan result: [DetectionType]3 Detection accuracy: [DetectionAccuracy] Infected file: [Path] [ArchivePath] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Drive letter: [DetectionType]0 File name: [DetectionType]1 File name hash: [DetectionType]2
317	DriveLock	no	Error	AV Definition: Copying failed	Copying antivirus definitions from an UNC path failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
318	DriveLock	no	Error	AV Definition: Verification failed	Verification of antivirus definitions failed. Definition file: [FileName]
319	DriveLock	no	Error	AV Definition: Reading/extracting failed	Reading and extracting antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorMessage]
320	DriveLock	no	Error	AV Definition: Activating failed	Activating antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
321	DriveLock	no	Error	AV Definition: Caching failed	Caching antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
322	DriveLock	no	Error	AV Definition: Applying to scan engine failed	Applying antivirus definitions to the scan engine failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
323	DriveLock	no	Information	Antivirus definitions updated	Antivirus definitions updated. Definition file: [FileName]
324	DriveLock	no	Error	Quarantine: Deleting file failed	Deleting a file from antivirus quarantine failed. Quarantined file: [FileName] Error code: [ErrorCode]

Event ID	Source	Audit event	Severity	Short text	Long text
					Error: [ErrorMessage]
325	DriveLock	no	Information	Quarantined file deleted	A file was deleted from antivirus quarantine. Quarantined file: [FileName]
326	DriveLock	no	Error	Quarantine: Restoring file failed	Restoring a file from antivirus quarantine failed. Quarantined file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
327	DriveLock	no	Information	Quarantined file restored	A file was restored from antivirus quarantine. Quarantined file: [FileName]
328	DriveLock	no	Warning	Old antivirus definitions detected	Antivirus definitions are [AvDefAgeDays] days old. For continued protection please update antivirus definitions.
329	DriveLock	no	Warning	Hard disk self-monitoring status could not be read	Hard disk self-monitoring (S.M.A.R.T.) status could not be read. Device Id: [HWVendorID] [HWProductID] (Rev.

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWRevisionNumber]) (Serial number [HWSerialNumber]) Drive letter: [DriveLetter] Hardware Id: [HardwareID]
330	DriveLock	no	Warning	Hard disk failed (Hard disk self-monitoring)	Hard disk self-monitoring (S.M.A.R.T.) reported the drive failed. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Drive letter: [DriveLetter] Hardware Id: [HardwareID]
331	DriveLock	no	Audit	Volume created (enforced encryption)	A DriveLock encrypted volume was created/formatted by enforced encryption. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] File system: [FileSystemType] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWSerialNumber])
332	DriveLock	no	Warning	Volume mount error	Mounting of the encrypted volume [FileName] failed. Existing data will not be preserved. Volume GUID: [VolumeID]
333	DriveLock	no	Error	AV Definition: Manual update to older definition prevented	The user tried to update to an antivirus definition older than the current definition. This is not supported. Definition file: [FileName]
334	DriveLock	no	Error	Server communication failed	Communication with the DriveLock Enterprise Service failed. Server: [ServerName] Error: [ErrorMessage]
335	DriveLock	no	Error	AV Definition: Down-	Downloading antivirus definitions

Event ID	Source	Audit event	Severity	Short text	Long text
				load failed	failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage] Additional information: [ErrorMessage2]
336	DriveLock	no	Error	AV Definition: Merging incremental definitions failed	Merging incremental antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
337	DriveLock	no	Information	AV Definition: Incremental definitions successfully merged	Incremental antivirus definitions successfully merged. Definition file: [FileName]
338	DriveLock	no	Warning	License expired. Grace period active	Your subscription license is expired. You will receive free updates and definitions until [LicenseInfo].
339	DriveLock	no	Error	License expired	Your subscription license expired on [LicenseInfo].
340	DriveLock	no	Error	Scheduled job: Load	Loading scheduled antivirus scan job

Event ID	Source	Audit event	Severity	Short text	Long text
				failed	failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
341	DriveLock	no	Error	Scheduled job: Execution failed	Executing a scheduled antivirus scan job failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
342	DriveLock	no	Information	Scheduled job: Successfully executed	Scheduled antivirus scan job successfully executed. Job ID: [ConfigId] Job description: [DisplayName] Number of scanned files: [NumFiles] Number of detections: [NumDetections]
343	DriveLock	no	Warning	Scheduled job: Running with standard scanning profile	Application of the configured scanning profile failed. Scheduled antivirus scan job will run with default profile. Job ID: [ConfigId] Job description: [DisplayName]

Event ID	Source	Audit event	Severity	Short text	Long text
344	DriveLock	no	Error	Scheduled job: Scanning failed	Scanning a file in a scheduled antivirus scan job failed. Job ID: [ConfigId] Job description: [DisplayName] Failed file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
345	DriveLock	no	Warning	Scheduled job: Not executed due to manual reconfiguration	A scheduled antivirus scan was not executed due to manual reconfiguration. Job ID: [ConfigId] Job description: [DisplayName]
346	DriveLock	no	Warning	AV Definition: No updates due to manual reconfiguration	Antivirus definitions will not be updated due to manual reconfiguration.
347	DriveLock	no	Warning	Uninstall due to manual reconfiguration	Antivirus will be uninstalled due to manual reconfiguration.
348	DriveLock	no	Information	Install due to manual reconfiguration	Antivirus will be installed due to manual reconfiguration.

Event ID	Source	Audit event	Severity	Short text	Long text
349	DriveLock	no	Error	Existing product uninstallation failed	An existing antivirus product was detected but the configured automatic uninstallation failed. Detected product: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
350	DriveLock	no	Error	Cannot load existing product update engine	The engine for updating existing antivirus products could not be loaded. Error code: [DisplayName] Error: [ErrorCode]
351	DriveLock	no	Information	Existing product uninstalled	An existing antivirus product was detected and uninstalled. Detected product: [DisplayName]
352	DriveLock	no	Information	Existing product detected	An existing antivirus product was detected. Detected product: [DisplayName]
353	DriveLock	no	Information	Antivirus scan successfull	An antivirus scan on drive [DriveLetter] was executed and succeeded. Device Id: [HWVendorID] [HWPro-

Event ID	Source	Audit event	Severity	Short text	Long text
					ductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Status: [ActionResult] Hardware Id: [HardwareID]
354	DriveLock	no	Error	Antivirus scan failed	An antivirus scan on drive [DriveLetter] was executed and reported a problem. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Status: [ActionResult] Hardware Id: [HardwareID]
355	DriveLock	no	Warning	Realtime virus scanning temporarily disabled	Realtime virus scanning was temporarily disabled by administrative intervention.
356	DriveLock	no	Error	Disk Protection installation error	Installation of the Disk Protection package failed. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
357	DriveLock	no	Error	Disk Protection uninstallation error	Uninstallation of the Disk Protection package failed. Error code: [UserName] Error: [ErrorCode]
358	DriveLock	no	Information	Disk Protection configuration change delayed	A change in the Disk Protection configuration was detected, but the change is not applied due to the 'delay decryption' setting in the policy.
359	DriveLock	no	Warning	FDE: Manual reconfiguration	Disk Protection is manually reconfigured.
360	DriveLock	no	Warning	Disk Protection integration module error	The Disk Protection integration module could not be loaded. Error code: [ErrorCode] Error: [ErrorMessage]
361	DriveLock	no	Error	Automatic updates: Load failed	Loading the automatic updates job schedule failed. Error code: [ErrorCode] Error: [ErrorMessage]
362	DriveLock	no	Error	Automatic updates:	Retrieving automatic update inform-

Event ID	Source	Audit event	Severity	Short text	Long text
				Retrieving data failed	ation from server [ServerName] failed. Package type: [ServiceName] Error: [ErrorMessage]
363	DriveLock	no	Error	Automatic updates: Download failed	Downloading automatic updates failed. Package file: [URL] Error code: [ErrorCode] Error: [ErrorMessage]
364	DriveLock	no	Error	Automatic updates: Execution failed	Executing an automatic update failed. Package type: [ServiceName] Version: [InstalledVersion] Action: [ActionName] Error code: [ErrorCode] Error: [ErrorMessage]
365	DriveLock	no	Information	Automatic updates: Execution started	Execution of an automatic update started. Package type: [ServiceName] Version: [InstalledVersion]
366	DriveLock	no	Error	Disk Protection Remote wipe request failed	A Disk Protection remote wipe request was received but could not be executed Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
367	DriveLock	no	Information	Disk Protection Remote wipe request executed	A Disk Protection remote wipe request was executed. The system will now reboot. User message: [ActionName]
368	DriveLock	no	Audit	Network resource locked	The network resource [NetDrivePath] ([NetDriveType]) will be controlled by DriveLock. As an ACL was applied to the drive, some users may no longer be able to access it. The drive is [User-LockState] for this event's user account. Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
369	DriveLock	no	Audit	Network resource not locked	The network resource [NetDrivePath] ([NetDriveType]) will be controlled by DriveLock. As an ACL was applied to the drive, some users may no longer be able to access it. The drive is [User-LockState] for this event's user account. Applied whitelist rule:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
370	DriveLock	no	Audit	Network resource not locked, error	The network resource [NetDrivePath] ([NetDriveType]) will be controlled by DriveLock. As an ACL was applied to the drive, some users may no longer be able to access it. The drive is [User-LockState] for this event's user account. Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
371	DriveLock	no	Audit	File accessed	File accessed. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access

Event ID	Source	Audit event	Severity	Short text	Long text
					direction: [AccessDirection] Process: [ProcessName]
372	DriveLock	no	Audit	File blocked by content scanner	File blocked by content scanner. Content does not match file extension. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
373	DriveLock	no	Audit	File extension blocked	File blocked by file filter. Access denied due to file type. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File size: [Size] File

Event ID	Source	Audit event	Severity	Short text	Long text
					name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
374	DriveLock	no	Audit	File created	New file created. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
375	DriveLock	no	Audit	File deleted	File deleted. Process: [FileName] File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File name hash: [MD5Hash] File content hash: [MD5Hash]

Event ID	Source	Audit event	Severity	Short text	Long text
376	DriveLock	no	Audit	File renamed	File renamed. Process: [ProcessName] Old file path: [Path] Old file name: [FileName] New file name: [FileName] Old file name hash: [MD5Hash] File content hash: [MD5Hash] New file name hash: [MD5Hash] Network resource: [NetDrivePath] ([NetDriveType])
377	DriveLock	no	SuccessAudit	Usage policy accepted	Usage policy for network resource [NetDrivePath] ([NetDriveType]) was accepted by the user.
378	DriveLock	no	FailureAudit	Usage policy declined	Usage policy for network resource [NetDrivePath] ([NetDriveType]) was declined by the user.
379	DriveLock	no	Information	System verification successfull	A system verification operation on network resource [NetDrivePath] ([NetDriveType]) was executed and succeeded. Status: [ActionResult]

Event ID	Source	Audit event	Severity	Short text	Long text
380	DriveLock	no	Error	System verification failed	A system verification operation on network resource [NetDrivePath] ([NetDriveType]) was executed and reported a problem. Status: [ActionResult]
381	DriveLock	no	Information	Antivirus scan successfull	An antivirus scan on drive [NetDrivePath] ([NetDriveType]) was executed and succeeded. Status: [ActionResult]
382	DriveLock	no	Error	Antivirus scan failed	An antivirus scan on drive [NetDrivePath] ([NetDriveType]) was executed and reported a problem. Device Id: [NetDriveType] [ActionResult] (Rev. %4) (Serial number %5) Status: %6
383	DriveLock	no	FailureAudit	Malware detected	Virus or malware detected. Detected malware: [DetectionName] ([DetectionType]) Detection accuracy: [DetectionAccuracy] Infected file: [Path]

Event ID	Source	Audit event	Severity	Short text	Long text
					[ArchivePath] Network resource: ([NetDriveType]) [NetDrivePath] File name: [FileName] File name hash: [MD5Hash]
384	DriveLock	no	Information	Deferred hash completed	Deferred content hash generation completed. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File name hash: [MD5Hash] File content hash: [MD5Hash]
385	DriveLock	no	Information	File content changed	File content changed. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File name hash: [MD5Hash] Old file content hash: [MD5Hash] New file content hash: [MD5Hash]

Event ID	Source	Audit event	Severity	Short text	Long text
386	DriveLock	no	Audit	Volume mounted	A DriveLock encrypted volume was mounted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Drive letter: [DriveLetter] Network resource: [NetDrivePath] ([NetDriveType])
387	DriveLock	no	Audit	Volume unmounted	A DriveLock encrypted volume was unmounted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Drive letter: [DriveLetter] Network resource: [NetDrivePath] ([NetDriveType])
388	DriveLock	no	Audit	Volume created	A DriveLock encrypted volume was created/formatted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] File system: [FileSystemType] Network resource: [NetDrivePath] ([NetDriveType])

Event ID	Source	Audit event	Severity	Short text	Long text
389	DriveLock	no	Audit	Password changed	The password for a DriveLock encrypted volume was changed. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Network resource: [NetDrivePath] ([NetDriveType])
390	DriveLock	no	Warning	Encrypted volume password recovered	A DriveLock Encrypted volume password was recovered. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Network resource: [NetDrivePath] ([NetDriveType])
391	DriveLock	no	Warning	Cannot send event by e-mail	DriveLock cannot send an event to a defined e-mail target. Error: [ErrorMessage]
392	DriveLock	no	Warning	Internal event queue full	The internal event queue was full. [EventCount] events were dropped during the last [IntValue] msec.

Event ID	Source	Audit event	Severity	Short text	Long text
393	DriveLock	no	Warning	External event queue full	The external event queue was full. [EventCount] events were dropped since [UnlockTime].
394	DriveLock	no	Audit	File securely deleted	A file was securely deleted. File: [FileName] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Method: [SecureEraseAlgorithm]
395	DriveLock	no	Warning	File securely deleted	A file was securely deleted. File: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) Algorithm: [SecureEraseAlgorithm]
396	DriveLock	no	Error	Event data encryption failed	Error while reading the certificate file [FileName] for event data encryption. Event data will be anonymized. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
397	DriveLock	no	Error	Event data encryption failed	Error while encrypting event data. Event data will be anonymized. Error code: [ErrorCode] Error: [ErrorMessage]
398	DriveLock	no	Error	Secure deletion failed	Secure deletion of a file failed. File: [FileName] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Error code: [ErrorCode] Error: [ErrorMessage]
399	DriveLock	no	Warning	Secure deletion failed	Secure deletion of a file failed. File: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) Error code: [ErrorCode] Error: [ErrorMessage]
400	DriveLock	no	Information	Required encryption cancelled	Required encryption of a drive was cancelled by the user.
401	DriveLock	no	Information	Required encryption	A rule for enforced / required encryp-

Event ID	Source	Audit event	Severity	Short text	Long text
				rule selected	tion was selected by the user. Rule ID: [ConfigId] Rule name: [DisplayName]
402	DriveLock	no	Audit	User password removed	The user password for a DriveLock encrypted volume was removed. The administrative password is needed to access the volume. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
403	DriveLock	no	Audit	User password removed	The user password for a DriveLock encrypted volume was removed. The administrative password is needed to access the volume. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Network resource: [NetDrivePath] ([NetDriveType])

Event ID	Source	Audit event	Severity	Short text	Long text
404	DriveLock	no	Audit	User password removed	The administrative password for a DriveLock encrypted volume was removed. Only the user password can be used to access the volume. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
405	DriveLock	no	Audit	User password removed	The administrative password for a DriveLock encrypted volume was removed. Only the user password can be used to access the volume. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Network resource: [NetDrivePath] ([NetDriveType])
406	DriveLock	no	Information	Encrypted folder created	An encrypted folder was successfully created. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVen-

Event ID	Source	Audit event	Severity	Short text	Long text
					dorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Initial user ID: [UserID]
407	DriveLock	no	Information	Encrypted folder recovered	An encrypted folder was successfully recovered. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Recovered user ID: [UserID]
408	DriveLock	no	Information	Encrypted folder mounted	An encrypted folder was successfully mounted. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID]

Event ID	Source	Audit event	Severity	Short text	Long text
409	DriveLock	no	Information	Encrypted folder unmounted	An encrypted folder was successfully unmounted. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID]
410	DriveLock	no	Error	Creation of an encrypted folder failed	Creation of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Initial user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
411	DriveLock	no	Error	Recovery of an encrypted folder failed	Recovery of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWSerialNumber]) Recovered user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
412	DriveLock	no	Error	Mount of an encrypted folder failed	Mount of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
413	DriveLock	no	Error	Creation of recovery data failed	The creation of folder recovery information failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Error code:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorCode] Error: [ErrorMessage]
414	DriveLock	no	Information	User successfully authenticated	An user was successfully authenticated against an encrypted folder. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Permissions: [DfpUserPerms] [DfpReadonlyPerms]
415	DriveLock	no	Information	User successfully added	An user was successfully added to the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber])

Event ID	Source	Audit event	Severity	Short text	Long text
					(Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Added user ID: [UserID] Permissions: [DfpUserPerms] [UncPath]0
416	DriveLock	no	Information	User successfully deleted	An user was successfully deleted from the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Deleted user ID: [UserID]
417	DriveLock	no	Error	Authentication against encrypted folder failed	Authentication against an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev.

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage] Authentication type: [UncPath]0
418	DriveLock	no	Information	Offline encryption started	An offline encryption operation was started for an encrypted folder. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Job type: [DfpJobType] - [UncPath]0
419	DriveLock	no	Information	Offline encryption completed	An offline encryption operation was successfully completed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWPro-

Event ID	Source	Audit event	Severity	Short text	Long text
					ductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Number of processed files: [IntValue]
420	DriveLock	no	Warning	Offline encryption cancelled	An offline encryption operation was cancelled. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Number of files: [IntValue] Number of incomplete files: [UncPath]0
421	DriveLock	no	Error	Offline encryption: File error	A file in an offline encryption operation could not be processed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVen-

Event ID	Source	Audit event	Severity	Short text	Long text
					dorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Job ID: [DfpJobID] Processed file: [FileName] Error code: [ErrorCode] Error: [UncPath]0 User action: [UncPath]1
422	DriveLock	no	Information	User certificate requested	An user certificate was requested. Requesting user: [UserID] Certificate serial number: [CertSerNo]
423	DriveLock	no	Information	User certificate issued	An user certificate was issued. Requesting user: [UserID] Certificate serial number: [CertSerNo]
424	DriveLock	no	Error	User certificate request failed	An error occurred while requesting an user certificate. Requesting user: [UserID] Certificate serial number: [CertSerNo] Server error: [ErrorMessage] Error code: [ErrorCode] Error:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorMessage2]
425	DriveLock	no	Error	User certificate issued	An error occurred while calling a File Protection web service. Server URL: [URL] Server error: [ErrorMessage] Error code: [ErrorCode] Error: [ErrorMessage2]
426	DriveLock	no	Information	Encrypted folder created	An encrypted folder was successfully created. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Initial user ID: [UserID]
427	DriveLock	no	Information	Encrypted folder recovered	An encrypted folder was successfully recovered. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Recovered user ID:

Event ID	Source	Audit event	Severity	Short text	Long text
					[UserID]
428	DriveLock	no	Information	Encrypted folder mounted	An encrypted folder was successfully mounted. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID]
429	DriveLock	no	Information	Encrypted folder unmounted	An encrypted folder was successfully unmounted. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID]
430	DriveLock	no	Error	Creation of an encrypted folder failed	Creation of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource:

Event ID	Source	Audit event	Severity	Short text	Long text
					[NetDrivePath] ([NetDriveType]) Initial user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
431	DriveLock	no	Error	Recovery of an encrypted folder failed	Recovery of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Recovered user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
432	DriveLock	no	Error	Mount of an encrypted folder failed	Mount of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
433	DriveLock	no	Error	Creation of recovery data failed	The creation of folder recovery information failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Error code: [ErrorCode] Error: [ErrorMessage]
434	DriveLock	no	Information	User successfully authenticated	An user was successfully authenticated against an encrypted folder. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Permissions: [DfpUserPerms] [DfpReadonlyPerms]
435	DriveLock	no	Information	User successfully added	An user was successfully added to the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Added user ID: [UserID]

Event ID	Source	Audit event	Severity	Short text	Long text
					Permissions: [DfpUserPerms] [DfpReadonlyPerms]
436	DriveLock	no	Information	User successfully deleted	An user was successfully deleted from the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Deleted user ID: [UserID]
437	DriveLock	no	Error	Authentication against encrypted folder failed	Authentication against an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage] Authentication

Event ID	Source	Audit event	Severity	Short text	Long text
					type: [DfpAuthTypes]
438	DriveLock	no	Information	Offline encryption started	An offline encryption operation was started for an encrypted folder. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Job type: [DfpJobType] - [DfpJobDirection]
439	DriveLock	no	Information	Offline encryption completed	An offline encryption operation was successfully completed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Num-

Event ID	Source	Audit event	Severity	Short text	Long text
					ber of processed files: [IntValue]
440	DriveLock	no	Warning	Offline encryption cancelled	An offline encryption operation was cancelled. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Number of files: [IntValue] Number of incomplete files: [IntValue2]
441	DriveLock	no	Error	Offline encryption: File error	A file in an offline encryption operation could not be processed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Job ID: [DfpJobID] Processed file:

Event ID	Source	Audit event	Severity	Short text	Long text
					[FileName] Error code: [ErrorCode] Error: [ErrorMessage] User action: [DfpUserAction]
442	DriveLock	no	Error	Initialization error	File Protection could not be initialized on this computer. Error code: [URL] Error: [ErrorCode]
443	DriveLock	no	Error	Component start error	A DriveLock system component could not be started on this computer. Error code: [ErrorMessage] Error: [ErrorMessage] Component ID: [IntValue] Name: [ErrorCode]
444	DriveLock	no	Warning	Ignoring Group Policy settings	Group Policy settings are ignored as a centrally stored policy or configuration file is applied which is configured to ignore GPO.

Event ID	Source	Audit event	Severity	Short text	Long text
445	DriveLock	no	Information	User successfully changed	An user was successfully changed in the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Changed user ID: [UserID] Permissions: [DfpUserPerms] [UncPath]0
446	DriveLock	no	Information	User successfully changed	An user was successfully changed in the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Changed user ID: [UserID] Permissions: [DfpUserPerms] [DfpReadonlyPerms]
447	DriveLock	no	Information	Encrypted folder pass-	An encrypted folder users password

Event ID	Source	Audit event	Severity	Short text	Long text
				word changed	was successfully changed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Changed user ID: [UserID] Changed by user ID: [UserID]
448	DriveLock	no	Information	Encrypted folder password changed	An encrypted folder users password was successfully changed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Changed user ID: [UserID] Changed by user ID: [UserID]
449	DriveLock	no	Error	Password change in an encrypted folder failed	Changing a password in an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Changed user ID:

Event ID	Source	Audit event	Severity	Short text	Long text
					[UserID] Error code: [ErrorCode] Error: [ErrorMessage]
450	DriveLock	no	Error	Password change in an encrypted folder failed	Changing a password in an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Changed user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
451	DriveLock	no	Error	No or wrong enforced encryption settings	A drive is configured for enforced encryption using File Protection but enforced encryption settings are not present. The drive will be blocked and no encryption is executed.
452	DriveLock	no	Warning	Wrong application	The application hash database

Event ID	Source	Audit event	Severity	Short text	Long text
				hash database hash algorithm	[FileName] uses an other hash algorithm than configured globally for application filtering. Applications in this database will not be detected. Rule: [ObjectID]
453	DriveLock	no	Information	Installation successful, uninstalling update service	The Agent Update service will be uninstalled as it detected a successfull installation.
454	DriveLock	no	Information	Update service started	The Agent Update service was started.
455	DriveLock	no	Information	Update service stopped	The Agent Update service was stopped.
456	DriveLock	no	Error	No server connection detected	The Agent Update service was unable to find a DriveLock Enterprise Service. Installation and updates will not take place as expected.
457	DriveLock	no	Information	Missing service was registered	The Agent Update service successfully registered a missing Agent service.

Event ID	Source	Audit event	Severity	Short text	Long text
458	DriveLock	no	Error	Error registering missing service	The Agent Update service was not able to register a missing Agent service.
459	DriveLock	no	Warning	Removed corrupted Agent installation	The Agent Update service has removed a corrupted Agent installation.
460	DriveLock	no	Warning	Agent installation started	The Agent Update service started installing the Agent.
461	DriveLock	no	Warning	Agent installation successful	The Agent Update service successfully installed the Agent.
462	DriveLock	no	Error	Error starting process	Error while starting Agent registration process. Error code: [ErrorCode] Error: [ErrorMessage]
463	DriveLock	no	Error	Error starting update service	Error while starting Agent update service. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
464	DriveLock	no	Error	Error installing agent	Error while installing the Agent. Package file: [FileName] Installation log: [LogFile] Error code: [ErrorCode] Error: [ErrorMessage]
465	DriveLock	no	Information	Windows Firewall status change	Client compliance status changed for Windows Firewall. Firewall enabled: [ComponentEnabled]
466	DriveLock	no	Information	Script status change	Client compliance status changed for script [ComplianceName]. Status: [ComplianceValue]
467	DriveLock	no	Information	Windows Update status change	Client compliance status changed for Windows Update. Updates enabled: [ComponentEnabled] Available updates: [AvblUpdates] Last successful update: [LastSuccessUpdate]
468	DriveLock	no	Information	WSC Firewall status change	Client compliance status changed for Windows Security Center - Firewall. Is installed: [ComponentInstalled] Is

Event ID	Source	Audit event	Severity	Short text	Long text
					enabled: [ComponentEnabled] Is up-to-date: [ComponentUptodate]
469	DriveLock	no	Information	WSC Antivirus status change	Client compliance status changed for Windows Security Center - Antivirus. Is installed: [ComponentInstalled] Is enabled: [ComponentEnabled] Is up-to-date: [ComponentUptodate]
470	DriveLock	no	Information	WSC Anti-Spyware status change	Client compliance status changed for Windows Security Center - Anti-Spyware. Is installed: [ComponentInstalled] Is enabled: [ComponentEnabled] Is up-to-date: [ComponentUptodate]
471	DriveLock	no	Warning	Remote control declined	The user declined remote control access.
472	DriveLock	no	Information	Remote control accepted	The user accepted remote control access.

Event ID	Source	Audit event	Severity	Short text	Long text
473	DriveLock	no	Audit	Process blocked	The execution of a process was blocked by company policy. Process: [ProcessName] File Hash: [FileHash] Applied rule: [ObjectID] Rule type: [WlType] File owner (user name): [OwnerName] File owner (user sid): [OwnerSID] File version: [VersionInfo] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [ProcessName]0 Certificate thumb print: [ProcessName]1 Description: [ProcessName]2 Product: [ProcessName]3 Command line: [ProcessName]7 Parent Process: [ProcessName]5 ([ProcessName]6) Software: [FileHash]0 [ProcessName]9 ([ProcessName]8)
474	DriveLock	no	Audit	Process started	A process was started. Process: [ProcessName] File Hash: [FileHash] Applied rule: [ObjectID] Rule type:

Event ID	Source	Audit event	Severity	Short text	Long text
					[WlType] File owner (user name): [OwnerName] File owner (user sid): [OwnerSID] File version: [VersionInfo] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [ProcessName]0 Certificate thumb print: [ProcessName]1 Description: [ProcessName]2 Product: [ProcessName]3 Unique Process ID: [ProcessName]4 Command line: [ProcessName]7 Parent Process: [ProcessName]5 ([ProcessName]6) Software: [FileHash]0 [ProcessName]9 ([ProcessName]8)
475	DriveLock	no	Information	PBA activated	Pre-boot authentication was successfully activated.
476	DriveLock	no	Information	PBA deactivated	Pre-boot authentication was successfully deactivated.
477	DriveLock	no	Information	EFS created	Embedded file system (EFS) was suc-

Event ID	Source	Audit event	Severity	Short text	Long text
					cessfully created in the SECURDSK folder.
478	DriveLock	no	Error	PBA activation failed	Pre-boot authentication could not be activated. EFS file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
479	DriveLock	no	Error	PBA deactivation failed	Pre-boot authentication could not be deactivated. EFS file: [FileName] Error: [ErrorMessage]
480	DriveLock	no	Error	EFS creation failed	Embedded file system (EFS) could not be created. EFS file: [FileName] Error: [ErrorMessage]
481	DriveLock	no	Error	Exception occurred	An exception occurred in a Disk Protection component. Error: [ErrorMessage]
482	DriveLock	no	Information	Encryption configuration changed	Encryption configuration has changed. Drive: [DriveLetter]

Event ID	Source	Audit event	Severity	Short text	Long text
					Algorithm: [EncryptionAlgorithm]
483	DriveLock	no	Error	Invalid XML configuration	An invalid XML configuration was detected. XML path: [FileName]
484	DriveLock	no	Information	XML configuration imported	A XML configuration was successfully imported. XML path: [FileName] Imported data: [ActionName]
485	DriveLock	no	Error	BitLocker-encrypted drive detected	The drive [DriveLetter] is encrypted with BitLocker drive encryption. It cannot be encrypted with Disk Protection.
486	DriveLock	no	Error	Failed to create disk key	The random encryption key for the local system could not be generated. Error code: [ErrorCode] Error: [ErrorMessage]
487	DriveLock	no	Error	Disk Protection Encryptor service	A general error occurred in the Disk Protection Encryptor service. Error

Event ID	Source	Audit event	Severity	Short text	Long text
				error	code: [ErrorCode] Error: [ErrorMessage]
488	DriveLock	no	Error	Disk Protection Management service error	A general error occurred in the Disk Protection Management service. Error code: [ErrorCode] Error: [ErrorMessage]
489	DriveLock	no	Audit	Cannot decrypt removable drive	The removable drive [DriveLetter] could not be unlocked / decrypted. Error code: [ErrorCode] Error: [ErrorMessage]
490	DriveLock	no	Error	Encryption interoperation failed	A storage encryption interoperation failed. Operation: [Function] Error code: [ErrorCode] Error: [ErrorMessage]
491	DriveLock	no	Error	User store operation failed	A user store operation failed. Store type: [StoreType] Operation: [Function] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
492	DriveLock	no	Error	Data store operation failed	A data store operation failed. Store type: [StoreType] Operation: [Function] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
493	DriveLock	no	Error	CD/DVD encryption failed	An error occurred while encrypting a CD/DVD-ROM using Disk Protection. Error code: [ErrorCode] Error: [ErrorMessage]
494	DriveLock	no	Error	Password complexity not met	The password for user [UserName]" does not meet the password complexity requirements."
495	DriveLock	no	Information	Disk Protection information	Disk Protection information: [DebugMsg]
496	DriveLock	no	Audit	Removable drive decrypted	The removable drive [DriveLetter] was successfully unlocked / decrypted.
497	DriveLock	no	Information	Encryption completed	Encryption of drive [DriveLetter] was successfully completed.

Event ID	Source	Audit event	Severity	Short text	Long text
498	DriveLock	no	Information	Decryption completed	Decryption of drive [DriveLetter] was successfully completed.
499	DriveLock	no	Information	Encryption started	Encryption of drive [DriveLetter] was started with algorithm [EncryptionAlgorithm]. [EncPercent] of the drive are already encrypted.
500	DriveLock	no	Information	Decryption started	Decryption of drive [DriveLetter] was started. [EncPercent] of the drive are already encrypted.
501	DriveLock	no	Information	Error en-/decrypting disk sector	A disk error occurred while en-/decrypting sector [SectorNo] on drive [DriveLetter]. The disk may be defective.
502	DriveLock	no	Audit	Successful pre-boot authentication	Successful pre-boot authentication. Logon type: [LogonType] User: [UserName] Logon time: [LogonTime]
503	DriveLock	no	Audit	Successful emergency	Successful emergency pre-boot

Event ID	Source	Audit event	Severity	Short text	Long text
				pre-boot authentication	authentication. Logon type: [LogonType] User: [UserName] Logon time: [LogonTime]
504	DriveLock	no	Audit	Failed pre-boot authentication	Failed pre-boot authentication. Logon type: [LogonType] User: [UserName] Logon time: [LogonTime]
505	DriveLock	no	Error	Empty pre-boot user store	The pre-boot user store could not be saved as it would not contain any user after saving.
506	DriveLock	no	Information	Disk Protection encryptor service started	The Disk Protection encryptor service was started.
507	DriveLock	no	Information	Disk Protection encryptor service stopped	The Disk Protection encryptor service was stopped.
508	DriveLock	no	Information	Disk Protection management service star-	The Disk Protection management service was started.

Event ID	Source	Audit event	Severity	Short text	Long text
				ted	
509	DriveLock	no	Information	Disk Protection management service stopped	The Disk Protection management service was stopped.
510	DriveLock	no	Error	Disk Protection installation failed	An error occurred while installing Disk Protection. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
511	DriveLock	no	Error	Disk Protection uninstallation failed	An error occurred while uninstalling Disk Protection. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
512	DriveLock	no	Error	Disk Protection upgrade failed	An error occurred while upgrading Disk Protection. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
513	DriveLock	no	Error	Disk Protection policy	An error occurred while applying Disk

Event ID	Source	Audit event	Severity	Short text	Long text
				failed	Protection policy. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
514	DriveLock	no	Information	Disk check succeeded	Disk check (ChkDsk) on drive [DriveLetter] ([ObjectID]) succeeded.
515	DriveLock	no	Error	Disk check failed	Disk check (ChkDsk) on drive [DriveLetter] ([ObjectID]) failed. Error code: [ErrorCode] Error: [ErrorMessage]
516	DriveLock	no	Warning	Disk Protection self wipe	This computer is offline for a long period. Disk Encryption self-wipe will be initiated in [UnlockTime] days when this computer stays offline.
517	DriveLock	no	Warning	No license - decryption scheduled	Company policy or licensing on this computer is configured to start decryption of all hard disks. Decryption is scheduled to start on [StatisticTimeStamp].

Event ID	Source	Audit event	Severity	Short text	Long text
518	DriveLock	no	Error	EFS file update failed	EFS file [FileName] could not be updated as part of company policy. Error: [ErrorMessage]
519	DriveLock	no	Error	Invalid disk configuration	Disk Protection installation is not possible on this computer. The disk / partition configuration does not allow installation ([DebugMsg]).
520	DriveLock	no	Error	No policy - All DESs are offline	Cannot load company policy. All configured DriveLock Enterprise Services are not reachable.
521	DriveLock	no	Error	Cannot determine computer token	Cannot determine the computer token. Error code: [ErrorCode] Error: [ErrorMessage]
522	DriveLock	no	Error	Error loading policy assignments	An error occurred while loading policy assignments from server [ServerName]. Error: [ErrorMessage]
523	DriveLock	no	Error	Policy integrity check	The integrity of an assigned policy

Event ID	Source	Audit event	Severity	Short text	Long text
				failed	could not be verified. Policy ID: [ServerName] Policy name: [ErrorMessage] Actual hash: %3 Expected hash: %4
524	DriveLock	no	Audit	File auditing	File accessed. DeviceName: [DisplayName] HardwareId: [HardwareID] ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] Access direction: [AccessDirection] File name hash: [MD5Hash] File content hash: [MD5Hash] File name: [DisplayName]0
525	DriveLock	no	Audit	File blocked by content scanner	File blocked by content scanner. Content does not match file extension. DeviceName: [DisplayName] HardwareId: [HardwareID] ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] Access direction: [AccessDirection] File name hash: [MD5Hash] File content hash:

Event ID	Source	Audit event	Severity	Short text	Long text
					[MD5Hash] File name: [DisplayName]0
526	DriveLock	no	Audit	File extension blocked	File blocked by file filter. Access denied due to file type. DeviceName: [DisplayName] HardwareId: [HardwareID] ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] Access direction: [AccessDirection] File name hash: [MD5Hash] File content hash: [MD5Hash] File name: [DisplayName]0
527	DriveLock	no	Audit	File deleted	File deleted. DeviceName: [DisplayName] HardwareId: [HardwareID]

Event ID	Source	Audit event	Severity	Short text	Long text
					ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] File name hash: [MD5Hash] File content hash: [MD5Hash] File name: [FileName]
528	DriveLock	no	Audit	File created	New file created. DeviceName: [DisplayName] HardwareId: [HardwareID] ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] File name hash: [MD5Hash] File content hash: [MD5Hash] File name: [FileName]
529	DriveLock	no	Audit	File renamed	File renamed. DeviceName: [DisplayName] HardwareId: [HardwareID] ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] Old file name hash: [MD5Hash] New file name: [FileName] New file name hash: [MD5Hash] File content

Event ID	Source	Audit event	Severity	Short text	Long text
					hash: [DisplayName]0 Old file name: [DisplayName]1
530	DriveLock	no	Error	Actual licensing	Licensing is configured using ActiveDirectory objects. The actual licensing status is: Device Control: [LicDLock] Disk Protection: [LicFde] Encryption 2-Go: [LicDlv] File Protection: [LicFfe] BitLocker Management: [LicBitLock] Application Control: [LicALF] Application Behavior Control: [LicDLock]9 Security Awareness Content: [LicDLock]0 Legacy OS Support: [LicDLock]1 DriveLock PBA: [LicDLock]3 Vulnerability Scanner: [LicDLock]4 Defender Management:

Event ID	Source	Audit event	Severity	Short text	Long text
					[LicDLock]5 BitLocker 2 Go: [LicDLock]6 EDR: [LicDLock]7 Native Security: [LicDLock]8 Detected without errors: [LicSure]
531	DriveLock	no	Information	Scheduled job: Started	Scheduled antivirus scan job was started. Job ID: [ConfigId] Job description: [DisplayName]
532	DriveLock	no	Information	Scheduled job: Initiated shutdown	Scheduled antivirus scan job initiated system shutdown after execution. Job ID: [ConfigId] Job description: [DisplayName]

Event ID	Source	Audit event	Severity	Short text	Long text
533	DriveLock	no	Warning	No policy - wiped	No valid policy available - the company policy was wiped because the computer was offline for a long period of time.
534	DriveLock	no	Warning	Policy wipe - Warning	The computer is offline for [DisplayName] days. The company policy will be wiped soon.
535	DriveLock	no	Error	Company policy wiped	The company policy was wiped because the computer was offline for a long period of time.
536	DriveLock	no	Information	Company policy in use again	The company policy is in used again after it was wiped because the computer was offline for a long period of time.
537	DriveLock	no	Error	URL categorizer failed	The URL categorizer returned an error while categorizing an URL. Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
538	DriveLock	no	Error	Network filter driver error	An error occurred while communicating with the network filtering driver. Error code: [ErrorCode] Error: [ErrorMessage]
539	DriveLock	no	Error	Network filter driver error	An error occurred while setting up network filtering. Error code: [ErrorCode] Error: [ErrorMessage]
546	DriveLock	no	Warning	Application Control temporarily disabled	Application Control was temporarily disabled by administrative intervention. Learn written files: [LearnWrittenFiles] Learn executed files: [LearnExecutedFiles] User has to approve files before learning: [UserApprovalMode]
547	DriveLock	no	Warning	Web Security temporarily disabled	Web Security was temporarily disabled by administrative intervention.
550	DriveLock	no	Information	PBA password change	User [UserName] (domain [DomainName]) changed the pass-

Event ID	Source	Audit event	Severity	Short text	Long text
					word in pre-boot authentication.
551	DriveLock	no	SuccessAudit	Usage policy accepted by authorized user	Usage policy for drive [DriveLetter] was accepted by authorized user [UserName]@[DomainName]. Logged on user was [UserName2]@[DomainName2]
553	DriveLock	no	Information	MTP/WPD/Android not supported on this platform	Control of portable mobile and Android devices is not available on this platform. Please refer to the DriveLock website for detailed information.
554	DriveLock	no	Information	Picture taken	A picture was taken with camera [CameraName] for event ID [EventID] ([EventNumber]).
555	DriveLock	no	Information	Scheduled action: Started	Scheduled power action was started. Job ID: [ConfigId] Job description: [DisplayName]

Event ID	Source	Audit event	Severity	Short text	Long text
556	DriveLock	no	Error	Scheduled action: Execution failed	Executing a scheduled power action failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
557	DriveLock	no	Information	Scheduled action: Successfully executed	Scheduled power action successfully executed. Job ID: [ConfigId] Job description: [DisplayName]
558	DriveLock	no	Error	Scheduled action: Load failed	Loading scheduled power action failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
559	DriveLock	no	Information	Power scheme changed	Computer power scheme successfully changed. Rule ID: [ConfigId] Rule name: [DisplayName] Power scheme: [FunctionName]
560	DriveLock	no	Error	Power scheme change failed	Changing computer power scheme failed. Rule ID: [ConfigId] Rule name: [DisplayName] Power scheme: [Func-

Event ID	Source	Audit event	Severity	Short text	Long text
					tionName] Error code: [ErrorCode] Error: [ErrorMessage]
561	DriveLock	no	Error	Cannot encrypt drives larger 2 TB	The drive [DriveLetter] is larger than 2 TB. It cannot be encrypted with Disk Protection.
562	DriveLock	no	Warning	Antivirus error	An antivirus error occurred while scanning object [FileName]. Error: [ErrorMessage]
563	DriveLock	no	Information	Definition update started	Antivirus definition update was started from source [MethodName].
564	DriveLock	no	Error	Error starting definition update	Antivirus definition update could not be started from source [MethodName]. Error code: [ErrorCode] Error: [ErrorMessage]
565	DriveLock	no	Warning	Package download	The [PackageType] package could not

Event ID	Source	Audit event	Severity	Short text	Long text
				error	be downloaded from [URL] Error code: [ErrorCode] Error: [ErrorMessage]
566	DriveLock	no	Information	Package download successful	The [PackageType] package was successfully downloaded.
567	DriveLock	no	Warning	Package extraction error	The [PackageType] package could not be extracted. The file [PackagePath] may be missing or corrupt. Error code: [ErrorCode] Error: [ErrorMessage]
568	DriveLock	no	Warning	Package installation prevented	The [PackageType] package should be installed but the installation is prevented by administrative intervention.
569	DriveLock	no	Information	Package installation successful	[PackageType] was successfully installed.
570	DriveLock	no	Error	Package installation error	[PackageType] installation failed. Command line: [CmdLine] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
571	DriveLock	no	Information	Package uninstallation successful	[PackageType] was successfully uninstalled.
572	DriveLock	no	Error	Package uninstallation error	[PackageType] uninstallation failed. Command line: [CmdLine] Error code: [ErrorCode] Error: [ErrorMessage]
573	DriveLock	no	Error	Incremental definition update failed	Incremental definition update failed to apply the patch package. Old definition file: [OldValue] New definition file: [NewValue] Error: [ErrorMessage]
574	DriveLock	no	Error	Definition update error	An error occurred while updating antivirus definitions. Error: [ErrorMessage]
575	DriveLock	no	Warning	Real-time scanning stopped	Real-time antivirus scanning was stopped.
576	DriveLock	no	Warning	Definition update requires reboot	A previous Antivirus definition update required a system reboot. No further updates will be possible until the system is rebooted.

Event ID	Source	Audit event	Severity	Short text	Long text
577	DriveLock	no	Information	Encrypted folder properties changed	The Properties of an encrypted folder have changed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] [ExtendedAuditing] Folder name: [FolderName]
578	DriveLock	no	Information	Encrypted folder properties changed	The Properties of an encrypted folder have changed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [ExtendedAuditing] Folder name: %8 Remote Audit activated: %9
579	DriveLock	no	SuccessAudit	Network pre-boot authentication succeeded	The network pre-boot authentication succeeded.
580	DriveLock	no	Error	Error during network	An error occurred during network

Event ID	Source	Audit event	Severity	Short text	Long text
				pre-boot authentication	pre-boot authentication. Error: [ErrorMessage]
581	DriveLock	no	Error	Error during network pre-boot authentication (1)	An error occurred during network pre-boot authentication. Error: [ErrorMessage] Parameter: [ErrorMessage2]
582	DriveLock	no	Error	Error retrieving custom computer name	An error occurred while retrieving the custom computer name. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
583	DriveLock	no	Error	Error with Active Directory inventory	An error occurred while generating Active Directory inventory. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
584	DriveLock	no	Information	Active Directory inventory started	Active Directory inventory generation was triggered by DES.
585	DriveLock	no	Information	Network pre-boot	Network pre-boot authentication was

Event ID	Source	Audit event	Severity	Short text	Long text
				authentication disabled	disabled.
586	DriveLock	no	Information	Network pre-boot authentication enabled	Network pre-boot authentication was enabled.
587	DriveLock	no	Error	Error reading Windows network configuration	An error occurred while reading the Windows network configuration (for network pre-boot configuration). Error code: [ErrorCode] Error: [ErrorMessage]
588	DriveLock	no	Error	Cannot load configuration from EFS	Cannot load network pre-boot configuration from embedded file system (EFS).
589	DriveLock	no	Error	Cannot write configuration to EFS	Cannot write network pre-boot configuration to embedded file system (EFS).
590	DriveLock	no	Error	Error installing net-	An error occurred while installing the

Event ID	Source	Audit event	Severity	Short text	Long text
				work pre-boot authentication	network pre-boot authentication. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
591	DriveLock	no	Error	Error registering network pre-boot authentication	An error occurred while registering the network pre-boot authentication with the server. Step: [StepName] Error: [ErrorMessage]
592	DriveLock	no	Error	Error uninstalling network pre-boot authentication	An error occurred while uninstalling the network pre-boot authentication. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
593	DriveLock	no	Information	Machine learning completed	Machine learning for local application whitelist was completed.
594	DriveLock	no	Error	Error during machine learning	An error occurred during machine learning of the local application whitelist. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
595	DriveLock	no	Error	Error during machine learning	An error occurred during machine learning of executable file [FileName]".
Error code: [ErrorCode]					
Error: [ErrorMessage]"					
596	DriveLock	no	Information	Machine learning completed	Machine learning of executable file [FileName]" completed.
Reason: [AlfLearnReason]"					
597	DriveLock	no	Error	Application Control license required	The company policy contains settings for application control features requiring a special license which is not present on the system. Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
598	DriveLock	no	Information	Security awareness campaign presented	A security awareness campaign was presented to the user. Campaign: [ObjectID] Description: [DisplayName]
599	DriveLock	no	Information	Security awareness campaign completed	A security awareness campaign was completed by the user. Module: [ObjectID] Description: [DisplayName]
600	DriveLock	no	Information	Program start approved	Start of executable file [FileName] was approved by the user.
601	DriveLock	no	Error	Invalid policy signing certificate	The configured policy signing certificate cannot be read. Error code: [ErrorCode] Error: [ErrorMessage]
602	DriveLock	no	Information	Program start declined by user	Start of executable file [FileName] was declined by the user.
603	DriveLock	no	Information	Security awareness skill test closed	The user did not pass a security awareness test. Module: [ObjectID] Description: [DisplayName] Result: [ErrorCode]

Event ID	Source	Audit event	Severity	Short text	Long text
604	DriveLock	no	Information	Security awareness test successful	A security awareness test was successfully completed by the user. Module: [ObjectID] Description: [DisplayName] Result: [ErrorCode]
605	DriveLock	no	Warning	Security awareness campaign cancelled	A security awareness campaign was cancelled by the user. Module: [ObjectID] Description: [DisplayName] Progress: [ErrorCode]
606	DriveLock	no	Error	Policy integrity check failed	The digital signature of an assigned policy could not be verified using the configured policy signing certificate. Policy ID: [ServerName] Policy name: [ErrorMessage]
607	DriveLock	no	Error	Security awareness campaign: Retrieving data failed	Retrieving security awareness campaign content from server [ServerName] failed. Package type: [SecAwPackageType] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
608	DriveLock	no	Error	Security awareness campaign: Download failed	Downloading security awareness campaign content failed. Package file download URL: [URL] Error code: [ErrorCode] Error: [ErrorMessage]
609	DriveLock	no	Error	BitLocker key backup failed	The BitLocker recovery key backup failed. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
610	DriveLock	no	Warning	BitLocker cannot apply configuration	The BitLocker configuration could not be applied.
611	DriveLock	no	Warning	BitLocker not licensed	BitLocker is configured to encrypt local hard disks but is not licensed on this computer.
612	DriveLock	no	Information	BitLocker will not be installed or uninstalled	A change in the BitLocker configuration was detected, but the change is not applied due to the 'delay decryption' setting in the policy.

Event ID	Source	Audit event	Severity	Short text	Long text
613	DriveLock	no	Warning	BitLocker manually reconfigured	BitLocker is manually reconfigured.
614	DriveLock	no	Warning	Decryption scheduled	Company policy or licensing on this computer is configured to start decryption of all hard disks. Decryption is scheduled to start on [StatisticTimeStamp].
615	DriveLock	no	Information	BitLocker encryption successful	BitLocker successfully encrypted hard disk: [DriveLetter].
616	DriveLock	no	Information	BitLocker decryption successful	BitLocker successfully decrypted local hard disk: [DriveLetter].
617	DriveLock	no	Error	BitLocker key backup creation failed	The BitLocker key backup creation failed.
618	DriveLock	no	Information	BitLocker encryption started	BitLocker started encrypting local hard disk: [DriveLetter].
619	DriveLock	no	Information	BitLocker decryption	BitLocker started decrypting local

Event ID	Source	Audit event	Severity	Short text	Long text
				started	hard disk: [DriveLetter].
620	DriveLock	no	Error	BitLocker system error	BitLocker Emergency Recovery Information could not be moved to [TargetFolder]. Error code: [ErrorCode] Error: [ErrorMessage]
621	DriveLock	no	Information	BitLocker login succeeded	BitLocker login succeeded.
622	DriveLock	no	Warning	BitLocker login failed	BitLocker login failed.
623	DriveLock	no	Warning	BitLocker password reset dialog cancelled	The BitLocker password reset dialog was cancelled.
624	DriveLock	no	Information	BitLocker password dialog finished	The BitLocker password dialog was finished.
625	DriveLock	no	Error	BitLocker encryption failed	The BitLocker encryption failed. Error: [ErrorMessage].
626	DriveLock	no	Information	BitLocker protectors	The BitLocker protectors [Protectors]

Event ID	Source	Audit event	Severity	Short text	Long text
				applied	were applied for drive [DriveLetter].
627	DriveLock	no	Information	BitLocker encryption algorithm applied	The encryption algorithm [EncryptionAlgorithm] is used to encrypt drive [DriveLetter].
628	DriveLock	no	Information	BitLocker recovery data upload	BitLocker recovery data was uploaded to the server.
629	DriveLock	no	Error	BitLocker recovery data upload failed	BitLocker recovery data upload failed. Error: [ErrorMessage]
630	DriveLock	no	Warning	BitLocker not controlled by DriveLock detected	Drive [DriveLetter] is already encrypted with BitLocker but not controlled by DriveLock.
631	DriveLock	no	Warning	Locked drive detected	BitLocker: locked drive [DriveLetter] detected.
632	DriveLock	no	Information	BitLocker configuration succeeded	BitLocker configuration succeeded.

Event ID	Source	Audit event	Severity	Short text	Long text
633	DriveLock	no	Information	BitLocker configuration failed	BitLocker configuration failed. Error: [ErrorMessage].
634	DriveLock	no	Information	BitLocker password set	BitLocker password was set by the user for drive: [DriveLetter].
635	DriveLock	no	Information	BitLocker password set failed	Setting BitLocker password failed for drive: [DriveLetter]. Error message: [ErrorMessage].
636	DriveLock	no	Warning	BitLocker drive not compliant	DriveLock detected changes on drive [DriveLetter] that do not match the configuration. Actions will be taken to modify the configuration.
637	DriveLock	no	Information	BitLocker recovery key replaced	The recovery key of drive [DriveLetter] was recreated after recovery process.
638	DriveLock	no	Information	BitLocker internal message	BitLocker Management internal message: [DebugMsg]
639	DriveLock	no	Error	Server certificate error	Server certificate error detected. Cer-

Event ID	Source	Audit event	Severity	Short text	Long text
					tificate: [CertSubject]. Error message: [ErrorMessage]
640	DriveLock	no	Information	Security awareness campaign presented	The security awareness campaign '[SecAwPackageDisplayName]' was presented to the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Applied rule: [ObjectID]
641	DriveLock	no	Information	Security awareness campaign element acknowledged	The security awareness campaign element '[SecAwPackageDisplayName]' was acknowledged by the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Applied rule: [ObjectID]
642	DriveLock	no	Information	Security awareness campaign completed	The security awareness campaign '[SecAwPackageDisplayName]' was

Event ID	Source	Audit event	Severity	Short text	Long text
					completed by the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Applied rule: [ObjectID]
643	DriveLock	no	Warning	Security awareness campaign cancelled	The security awareness campaign ' [SecAwPackageDisplayName]' was cancelled by the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Progress: [SecAwResultScorePassed] passed / [SecAwResultScoreFailed] failed Applied rule: [ObjectID]
644	DriveLock	no	Information	Security awareness test failed	The user did not pass the security awareness test '[SecAwPackageDisplayName]'. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Result:

Event ID	Source	Audit event	Severity	Short text	Long text
					[SecAwResultScorePassed] passed / [SecAwResultScoreFailed] failed Applied rule: [ObjectID]
645	DriveLock	no	Information	Security awareness test successful	The security awareness test '[SecAwPackageDisplayName]' was successfully completed by the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Result: [SecAwResultScorePassed] passed / [SecAwResultScoreFailed] failed Applied rule: [ObjectID]
646	DriveLock	no	Information	Security awareness campaign in progress	The security awareness campaign '[SecAwPackageDisplayName]' is in progress. Content type: [SecAwPackageContentType] Language:

Event ID	Source	Audit event	Severity	Short text	Long text
					[SecAwPackageLanguage] Version: [SecAwPackageVersion] Currently: [SecAwSessionProgress] %% completed Applied rule: [ObjectID]
647	DriveLock	no	Information	Security awareness test in progress	The security awareness test ' [SecAwPackageDisplayName]' is in progress. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Current result: [SecAwResultScorePassed] passed / [SecAwResultScoreFailed] failed Applied rule: [ObjectID]
648	DriveLock	no	Audit	DLL blocked	The loading of a DLL was blocked by company policy. Process: [ProcessName] ([AcProcessID]) Applied rule: [ObjectID] Rule type: [WlType] DLL File Name: [FilePath] DLL File

Event ID	Source	Audit event	Severity	Short text	Long text
					Hash: [FileHash] File owner (user name): [OwnerName] File owner (user sid): [OwnerSID] File version: [VersionInfo] Certificate issuer: [ProcessName]0 Certificate subject: [ProcessName]1 Certificate serial: [ProcessName]2 Certificate thumb print: [ProcessName]3 Description: [ProcessName]4 Product: [ProcessName]5 Software: [ProcessName]8 [ProcessName]7 ([ProcessName]6)
649	DriveLock	no	Audit	DLL loaded	A DLL was loaded. Process: [ProcessName] ([AcProcessID]) Applied rule: [ObjectID] Rule type: [WlType] DLL File Name: [FilePath] DLL File Hash: [FileHash] File owner (user name): [OwnerName] File owner (user sid): [OwnerSID] File version: [VersionInfo] Certificate issuer: [Pro-

Event ID	Source	Audit event	Severity	Short text	Long text
					cessName]0 Certificate subject: [ProcessName]1 Certificate serial: [ProcessName]2 Certificate thumb print: [ProcessName]3 Description: [ProcessName]4 Product: [ProcessName]5 Software: [ProcessName]8 [ProcessName]7 ([ProcessName]6)
650	DriveLock	no	Audit	File Access blocked	The Access to a File was blocked by company policy. Process: [ProcessName] ([ProcessGuid]) Applied rule: [ObjectID] Rule type: [WIType] File Name: [FileName] AccessDirection: [AccessDirection]
651	DriveLock	no	Audit	File Access	A File was accessed. Process: [ProcessName] ([ProcessGuid]) Applied

Event ID	Source	Audit event	Severity	Short text	Long text
					rule: [ObjectID] Rule type: [WlType] File Name: [FileName] AccessDirection: [AccessDirection]
652	DriveLock	no	Audit	Registry Access blocked	The Access to the Registry was blocked by company policy. Process: [ProcessName] ([ProcessGuid]) Applied rule: [ObjectID] Rule type: [WlType] Path: [FileName] AccessDirection: [AccessDirection]
653	DriveLock	no	Audit	Registry Access	The Registry was accessed. Process: [ProcessName] ([ProcessGuid]) Applied rule: [ObjectID] Rule type: [WlType] Path: [RegistryPath] AccessDirection: [AccessDirection]
654	DriveLock	no	Audit	File Access approved	The Access to a File was approved by the user. Process: [ProcessName] ([ProcessGuid]) File Name: [FileName]

Event ID	Source	Audit event	Severity	Short text	Long text
655	DriveLock	no	Audit	File Access denied	The Access to a File was denied by the user. Process: [ProcessName] ([ProcessGuid]) File Name: [FileName]
656	DriveLock	no	Audit	Registry Access approved	The Access to the Registry was approved by the user. Process: [ProcessName] ([ProcessGuid]) Path: [FileName]
657	DriveLock	no	Audit	Registry Access denied	The Access to the Registry was denied by the user. Process: [ProcessName] ([ProcessGuid]) Path: [RegistryPath]
660	DriveLock	no	Error	BitLocker is missing	BitLocker is missing
661	DriveLock	no	Error	BitLocker Management detected BIOS	BitLocker Management detected BIOS. DriveLock PBA is only supported on UEFI.
662	DriveLock	no	Error	BitLocker system drive not prepared	BitLocker Management: BitLocker doesn't seem to be prepared for the system drive: [DriveLetter]. The drive

Event ID	Source	Audit event	Severity	Short text	Long text
					can be prepared using 'bdehdcfg.exe -target default -restart'
663	DriveLock	no	Information	Disk Protection recovery data upload	Disk Protection recovery data was uploaded to the server.
664	DriveLock	no	Error	Disk Protection recovery data upload failed	Disk Protection recovery data upload failed. Error: [ErrorMessage]
665	DriveLock	no	SuccessAudit	The DES transmitted authorization data to the PBA	The DES transmitted authorization data to the PBA.
666	DriveLock	no	Error	Invalid network PBA key registration	Recorded attempt to register the PBA network key a second time.
667	DriveLock	no	Error	Invalid network PBA authorization data registration	Recorded attempt to register the PBA authorization data a second time.
668	DriveLock	no	Error	Cannot decrypt mes-	Cannot decrypt message from net-

Event ID	Source	Audit event	Severity	Short text	Long text
				sage from network PBA	work PBA. Error: [ErrorMessage].
669	DriveLock	no	Error	Invalid network PBA message	An invalid message from the network PBA has been received. Error: [ErrorMessage].
670	DriveLock	no	FailureAudit	Computer not registered for network PBA	The server received an network PBA connect request for a not registered computer.
671	DriveLock	no	FailureAudit	No authorization data for network PBA	Unable to authorize network PBA because the computer has not registerd authorization data.
672	DriveLock	no	Error	PBA network issues	The PBA has problems to connect to the network. Error: [ErrorMessage].
673	DriveLock	no	Error	Network PBA cannot connect to the server	An error occurred while the network PBA tried to connect to the server. Info: [IPAddress]. Error: [ErrorMessage].

Event ID	Source	Audit event	Severity	Short text	Long text
674	DriveLock	no	Error	Invalid network PBA server response	The network PBA received an invalid server response. Error: [ErrorMessage].
675	DriveLock	no	Error	Network PBA authorization data decryption failed	The network PBA is unable to decrypt the authorization data. Error: [ErrorMessage].
676	DriveLock	no	Error	Network PBA cannot unlock disk	The network PBA is unable unlock the disk using the authorization data. Error: [ErrorMessage]. Details: [ErrorMessage2].
677	DriveLock	no	FailureAudit	Network PBA logon failed	Network PBA logon failed. User: [UserName].
678	DriveLock	no	FailureAudit	Automatic logon via network PBA failed.	Automatic logon via network PBA failed.
679	DriveLock	no	Information	Machine learning started	Machine learning for local application whitelist was started.

Event ID	Source	Audit event	Severity	Short text	Long text
680	DriveLock	no	Information	Application behavior recording started	Recording of application behavior was started.
681	DriveLock	no	Error	Configuration of Microsoft Defender failed	Error configuring Microsoft Defender. Error code: [ErrorCode]. Error: [ErrorMessage].
682	DriveLock	no	Information	Microsoft Defender configuration changes reverted	Detected Microsoft Defender configuration changes by a third party. The changes have been reverted. Details: [Details].
683	DriveLock	no	Error	Failed to revert Microsoft Defender configuration changes	Detected Microsoft Defender configuration changes by a third party. The changes cannot be reverted. Details: [Details]. Error code: [ErrorCode]. Error: [ErrorMessage].
684	DriveLock	no	Warning	Microsoft Defender detected a threat	Microsoft Defender detected the threat [DetectionName] ([DetectionType]). Infected file: [Path] Drive letter: [DriveLetter] File name:

Event ID	Source	Audit event	Severity	Short text	Long text
					[FileName] File name hash: [MD5Hash]
685	DriveLock	no	Warning	Microsoft Defender threat allowed	A user has allowed a threat detected by Microsoft Defender. Threat: [DetectionName] Category: [DetectionType]
686	DriveLock	no	Warning	Microsoft Defender threat restored from quarantine	A user has restored a quarantined threat detected by Microsoft Defender. Threat: [DetectionName] Category: [DetectionType]
687	DriveLock	no	Error	Microsoft Defender signature update failed	Unable to update Microsoft Defender signature definition. Details: [Details].
688	DriveLock	no	Audit	Encrypted volume connected	Encrypted volume [DriveLetter] was added to the system. It is encrypted with [EncryptionType]. Mobile Encryption Application: [FileVersion] Has

Event ID	Source	Audit event	Severity	Short text	Long text
					unencrypted part: [UnencryptedPartPresent], size: [DataSize], permission: [UserLockState]
689	DriveLock	no	Audit	Application behavior control changed	Application behavior control for [ProcessName] changed: Execute: [LocalBehaviorExecute] DLL load: [LocalBehaviorDllLoad] Write Files: [LocalBehaviorFileWrite]
690	DriveLock	no	Information	Vulnerability scan successful	Vulnerability scan was successfully executed and results were uploaded. DES server: [DesName] Connection ID: [ObjectID]
691	DriveLock	no	Error	Vulnerability catalog not downloaded	Vulnerability scan could not be executed because the vulnerabilities catalog was not yet downloaded from the server.

Event ID	Source	Audit event	Severity	Short text	Long text
692	DriveLock	no	Error	Vulnerability scan failed	The vulnerability scanner failed scanning. Error: [ErrorMessage]
693	DriveLock	no	Error	Error starting vulnerability scan	Error while starting a vulnerability scan. Error code: [ErrorCode] Error: [ErrorMessage]
694	DriveLock	no	Error	Error downloading vulnerability catalog	Error while downloading the vulnerability catalog. Server: [ServerName] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
695	DriveLock	no	Error	Error creating vulnerability scan result	Error while creating the vulnerability scan result. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
696	DriveLock	no	Warning	Microsoft Defender detected a threat on a network resource	Microsoft Defender detected the threat [DetectionName] ([DetectionType]). Infected network file: [Path] Network resource: [NetDrivePath] ([NetDriveType]) File

Event ID	Source	Audit event	Severity	Short text	Long text
					name: [FileName] File name hash: [MD5Hash]
697	DriveLock	no	Warning	Microsoft Defender detected a threat	Microsoft Defender detected the threat [DetectionName] ([DetectionType]). Infected file: [Path] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [DetectionName]0) Drive letter: [DriveLetter] File name: [FileName] File name hash: [MD5Hash]
698	DriveLock	no	Error	Microsoft Defender is disabled	Microsoft Defender is disabled and cannot be enabled by DriveLock.
699	DriveLock	no	Information	Applied Microsoft Defender configuration	Microsoft Defender configuration was successfully applied.

Event ID	Source	Audit event	Severity	Short text	Long text
700	DriveLock	no	Warning	Microsoft Defender blocked an operation	Microsoft Defender blocked an operation of type: [ASRRuleType] Detection time: [TimeStamp] Path: [FileName] Process: [ProcessName] Signature version: [SignatureVersion] Engine version[EngineVersion] Product version: [ProductVersion] User: [UserName]
701	DriveLock	no	Audit	Microsoft Defender audited an operation	Microsoft Defender audited an operation of type: [ASRRuleType] Detection time: [TimeStamp] Path: [FileName] Process: [ProcessName] Signature version: [SignatureVersion] Engine version[EngineVersion] Product version: [ProductVersion] User: [UserName]
702	DriveLock	no	Error	Error uploading data to DES	An error occurred while uploading data to DriveLock Enterprise Service. Upload URL: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
703	DriveLock	no	Information	Vulnerability scan started	Vulnerability scan was triggered by DES.
704	DriveLock	no	Error	Error reading volume identification file	An error occurred while reading the volume identification file from drive [DriveLetter]. Bus type: [StorageBus] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Error code: [ErrorCode] Error: [ErrorMessage] Hardware Id: [HardwareID]
705	DriveLock	no	Error	Error reading volume identification hash list file	An error occurred while reading the volume identification hash list file from drive [DriveLetter]. Bus type: [StorageBus] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Error code: [ErrorCode] Error: [ErrorMessage] Hardware Id: [HardwareID]

Event ID	Source	Audit event	Severity	Short text	Long text
706	DriveLock	no	Error	Volume identification file is expired	An error occurred while reading the volume identification file from drive [DriveLetter]: the file is expired. Bus type: [StorageBus] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
707	DriveLock	no	Warning	Unsecure transport protocol	Agent is using the unsecure HTTP protocol.
708	DriveLock	no	Error	Error enumerating local user accounts	An error occurred while enumerating local user accounts. Error code: [ErrorCode] Error: [ErrorMessage]
709	DriveLock	no	Error	Error enumerating local groups	An error occurred while enumerating local groups. Error code: [ErrorCode] Error: [ErrorMessage]
710	DriveLock	no	Error	Error changing local group information	An error occurred while changing local group information. Group:

Event ID	Source	Audit event	Severity	Short text	Long text
					[GroupName] Error code: [ErrorCode] Error: [ErrorMessage]
711	DriveLock	no	Error	Error reading local group members	An error occurred while reading local group members. Group: [GroupName] Error code: [ErrorCode] Error: [ErrorMessage]
712	DriveLock	no	Error	Error removing local group member	An error occurred while removing a local group member. Group: [GroupName] User: [UserName] Error code: [ErrorCode] Error: [ErrorMessage]
713	DriveLock	no	Error	Error adding local group member	An error occurred while adding a local group member. Group: [GroupName] User: [UserName] Error code: [ErrorCode] Error: [ErrorMessage]
714	DriveLock	no	Information	Local group member removed	A local group member was successfully removed. Group: [GroupName] User: [UserName]

Event ID	Source	Audit event	Severity	Short text	Long text
715	DriveLock	no	Information	Local group member added	A local group member was successfully added. Group: [GroupName] User: [UserName]
716	DriveLock	no	Error	Error adding local group	An error occurred while adding a local group. Group: [GroupName] Error code: [ErrorCode] Error: [ErrorMessage]
717	DriveLock	no	Information	Local group added	A local group was successfully added. Group: [GroupName]
718	DriveLock	no	Error	Error removing local group	An error occurred while removing a local group. Group: [GroupName] Error code: [ErrorCode] Error: [ErrorMessage]
719	DriveLock	no	Information	Local group removed	A local group was successfully removed. Group: [GroupName]
720	DriveLock	no	Error	Error adding local user	An error occurred while adding a local user. User: [UserName] Error code:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorCode] Error: [ErrorMessage]
721	DriveLock	no	Information	Local user added	A local user was successfully added. User: [UserName]
722	DriveLock	no	Error	Error removing local user	An error occurred while removing a local user. User: [UserName] Error code: [ErrorCode] Error: [ErrorMessage]
723	DriveLock	no	Information	Local user removed	A local user was successfully removed. User: [UserName]
724	DriveLock	no	Error	Error changing local user information	An error occurred while changing local user information. User: [UserName] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
725	DriveLock	no	Error	Error saving password protected user information	An error occurred while saving password protected local user information. User: [UserName] Error code:

Event ID	Source	Audit event	Severity	Short text	Long text
					[ErrorCode] Error: [ErrorMessage]
726	DriveLock	no	Error	Error saving certificate protected user information	An error occurred while saving certificate protected local user information. User: [UserName] Error code: [ErrorCode] Error: [ErrorMessage]
727	DriveLock	no	Information	Local user name changed	A local user name was changed. Old user name: [UserName] New user name: [NewValue]
728	DriveLock	no	Information	Local password changed	A local password name was changed. User name: [UserName] New password: [NewValue]
729	DriveLock	no	Information	Windows Firewall enabled	Windows Firewall was enabled for firewall profile [FirewallProfile].
730	DriveLock	no	Information	Windows Firewall disabled	Windows Firewall was disabled for firewall profile [FirewallProfile].

Event ID	Source	Audit event	Severity	Short text	Long text
731	DriveLock	no	Information	Firewall rule deleted	A Windows Firewall rule was deleted. Rule name: [RuleName] Rule ID: [RuleGuid] Direction: [FirewallRuleDirection]
732	DriveLock	no	Information	Firewall rule (unmanaged) deleted	An unmanaged Windows Firewall rule was deleted. Rule name: [RuleName] Rule group: [RuleGroup] Direction: [FirewallRuleDirection]
733	DriveLock	no	Error	Firewall rule could not be deleted	A Windows Firewall rule could not be deleted. Rule name: [RuleName] Rule ID: [RuleGuid] Direction: [FirewallRuleDirection] Error code: [ErrorCode] Error: [ErrorMessage]
734	DriveLock	no	Error	Firewall rule (unmanaged) could not be deleted	An unmanaged Windows Firewall rule could not be deleted. Rule name: [RuleName] Rule group: [RuleGroup] Direction: [FirewallRuleDirection] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
735	DriveLock	no	Information	Firewall rule (managed) created	A Windows Firewall rule managed by DriveLock was created. Rule name: [RuleName] Rule ID: [RuleGuid] Direction: [FirewallRuleDirection]
736	DriveLock	no	Error	Firewall rule (managed) could not be created	A Windows Firewall rule managed by DriveLock could not be created. Rule name: [RuleName] Rule ID: [RuleGuid] Direction: [FirewallRuleDirection] Error code: [ErrorCode] Error: [ErrorMessage]
737	DriveLock	no	Error	Firewall rule could not be configured	A Windows Firewall rule could not be configured. Rule name: [RuleName] Rule ID: [RuleGuid] Property: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
738	DriveLock	no	Warning	Firewall group policy override active	Changing or adding a firewall rule (or group) to the current profiles will not take effect because group policy overrides it on [Details] current profiles.

Event ID	Source	Audit event	Severity	Short text	Long text
739	DriveLock	no	Error	Error managing firewall settings	An error occurred while managing Windows Firewall settings. Action: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
740	DriveLock	no	Warning	Error reading firewall rules	An error occurred while reading Windows Firewall rules. Action: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
741	DriveLock	no	Error	Error configuring global firewall settings	An error occurred while configuring global Windows Firewall settings. Property: [StepName] Profile: [FirewallProfile] Error code: [ErrorCode] Error: [ErrorMessage]
742	DriveLock	no	Error	Error configuring firewall logging	An error occurred while configuring Windows Firewall logging. NetSh command: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
743	DriveLock	no	Error	Error reading firewall	An error occurred while reading Win-

Event ID	Source	Audit event	Severity	Short text	Long text
				logs	dows Firewall log data. Error code: [ErrorCode] Error: [ErrorMessage]
744	DriveLock	no	Error	Failed to register as Windows Firewall application	Failed to register DriveLock as a Windows Firewall application. Error code: [ErrorCode] Error: [ErrorMessage]
745	DriveLock	no	FailureAudit	Incoming connection dropped	An incoming connection was dropped. Source IP: [SrcIp] Source Port: [SrcPort] Destination IP: [DstIp] Destination Port: [DstPort] Communication partner: [PartnerName] Protocol: [Protocol]
746	DriveLock	no	SuccessAudit	Incoming connection allowed	An incoming connection was allowed. Source IP: [SrcIp] Source Port: [SrcPort] Destination IP: [DstIp] Destination Port: [DstPort] Communication partner: [PartnerName] Protocol: [Protocol]
747	DriveLock	no	FailureAudit	Outgoing connection	An outgoing connection was

Event ID	Source	Audit event	Severity	Short text	Long text
				dropped	dropped. Source IP: [SrcIp] Source Port: [SrcPort] Destination IP: [DstIp] Destination Port: [DstPort] Communication partner: [PartnerName] Protocol: [Protocol]
748	DriveLock	no	SuccessAudit	Outgoing connection allowed	An outgoing connection was allowed. Source IP: [SrcIp] Source Port: [SrcPort] Destination IP: [DstIp] Destination Port: [DstPort] Communication partner: [PartnerName] Protocol: [Protocol]
749	DriveLock	no	SuccessAudit	Retrieved user password	Password (and user name) for account [UserName] were successfully retrieved.
750	DriveLock	no	FailureAudit	Failed to retrieve user password	Password (and user name) for account [UserName] could not be retrieved. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Audit event	Severity	Short text	Long text
751	DriveLock	no	Audit	Deeply nested archive blocked	File blocked by content scanner. Deeply nested archives are not allowed. File path: [Path] File name: [Path]1 Drive: [Path]2 File size: [Size] File name hash: [MD5Hash] File content hash: [Path]0 Access direction: [AccessDirection] Process: [ProcessName] Device ID: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
752	DriveLock	no	Audit	Deeply nested archive blocked	File blocked by content scanner. Deeply nested archives are not allowed. File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]

Event ID	Source	Audit event	Severity	Short text	Long text
753	DriveLock	no	Audit	Process stopped	The process [ProcessName] was stopped. Process ID: [AcProcessID]
754	DriveLock	no	Information	User requests unlock of drive	User requests unlock of drive [DriveLetter]. The stated reason is: [Reason] Hardware ID: [HardwareID] Device ID: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) Serial number: [HWSerialNumber] Bus: [StorageBus] Type: [StorageType] Applied whitelist rule: [DriveLetter]0
755	DriveLock	no	Audit	Bluetooth device connected and locked	The device [DisplayName] was connected to the computer. It was locked due to company policy. Device type: [DeviceType] Hardware ID: [HardwareID] Class ID: [ClassID] Vendor ID: [BthVendorID] Product ID: [BthProductID] Major class: [BthMajorClass] Minor class: [DisplayName]0 Address: [DisplayName]1 Applied whitelist rule: [ObjectID] Screen state (keyboard

Event ID	Source	Audit event	Severity	Short text	Long text
					[Win]-[L]): [SessionLockState]
756	DriveLock	no	Audit	Bluetooth device connected and not locked	The device [DisplayName] was connected to the computer. Device type: [DeviceType] Hardware ID: [HardwareID] Class ID: [ClassID] Vendor ID: [BthVendorID] Product ID: [BthProductID] Major class: [BthMajorClass] Minor class: [DisplayName]0 Address: [DisplayName]1 Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
757	DriveLock	no	Error	PBA activation failed due to Secure Boot	SecureBoot is active but the Microsoft Corporation UEFI CA 2011 Certificate

Event ID	Source	Audit event	Severity	Short text	Long text
				issues	is missing.
758	DriveLock	no	Information	xxx Removable media encrypted	xxx Removable drive [DriveLetter] encrypted with BitLocker To Go. Encryption algorithm: [EncryptionAlgorithm] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
759	DriveLock	no	Information	Password changed	xxx The password for a BitLockert To Go encrypted media was changed. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
760	DriveLock	no	Warning	xxx Encrypted drive	xxx The password for a BitLockert To

Event ID	Source	Audit event	Severity	Short text	Long text
				password recovered	Go encrypted media recovered. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
761	DriveLock	no	Information	xxx BitLocker To Go Drive unlocked	xxx BitLockert To Go encrypted drive unlocked. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
762	DriveLock	no	Information	xxx Drive locked	xxx BitLockert To Go encrypted drive locked. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]

Event ID	Source	Audit event	Severity	Short text	Long text
763	DriveLock	no	Information	xxx BitLocker To Go recovery data uploaded	xxx BitLockert To Go recovery data was uploaded to the server. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
764	DriveLock	no	Error	xxx Encryption failed	xxx Encryption of the removable drive [DriveLetter] with BitLocker To Go failed. Encryption algorithm: [EncryptionAlgorithm] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
765	DriveLock	no	Error	xxx Password change for a BitLockert To Go encrypted media failed	xxx The password change for a BitLockert To Go encrypted media failed. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID]

Event ID	Source	Audit event	Severity	Short text	Long text
					[HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
766	DriveLock	no	Error	xxx Recovery of a BitLocker To Go media failed	xxx Recovery of a BitLockert To Go encrypted media failed. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
767	DriveLock	no	Error	xxx Unlocking of a BitLocker To Go volume failed	xxx Unlock of a BitLocker To Go volume failed. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]

Event ID	Source	Audit event	Severity	Short text	Long text
768	DriveLock	no	Error	xxx Locking of a BitLocker To Go volume failed	xxx Locking of a BitLocker To Go volume failed. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
769	DriveLock	no	Error	xxx Upload of BitLockert To Go recovery data failed	xxx Upload of BitLockert To Go recovery data failed. Drive: [DriveLetter] Volume ID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Hardware Id: [HardwareID]
800	DCC	no	Information	Control Center started	The DriveLock Control Center has been started. Connected to: [DesName].
801	DCC	no	Information	Control Center terminated	The DriveLock Control Center has been terminated.

Event ID	Source	Audit event	Severity	Short text	Long text
802	DCC	no	Information	DriveLock Enterprise Service changed	The DriveLock Enterprise Service has been changed. The DriveLock Control Center is now connected to: [DesName].
803	DCC	no	Information	Added user account	For the user ([AccountName]) an user account has been added.
804	DCC	no	Information	Removed user account	The account for the user ([AccountName]) has been removed.
805	DCC	no	Information	Changed permission	The permissions from the user account ([AccountName]) has been changed. Tenants: [Tenants] Home:%t%t[PermissionHome] Helpdesk:%t%t[PermissionHelpdesk] Forensics:%t[PermissionForensics] Report:%t%t[PermissionReport] Inventory:%t[PermissionInventory] Configuration:%t[PermissionConfiguration] A = allow, N = not set, D = deny

Event ID	Source	Audit event	Severity	Short text	Long text
806	DCC	no	Information	Start decrypting personal data	Start decrypting personal data
807	DCC	no	Information	Stop decrypting personal data	Stop decrypting personal data
808	DCC	no	Information	Open connection to remote desktop	Open connection to remote desktop: [DisplayName]
809	DCC	no	Information	Close connection to remote desktop	Close connection to remote desktop: [DisplayName]
810	DCC	no	Information	New initial BitLocker password	Set new initial BitLocker password for client [DisplayName]
811	DCC	no	Information	Sent agent action to change BitLocker password	Sent agent action to change BitLocker password to client(s) [DisplayName]
900	DriveLock	yes	SuccessAudit	DriveLock configuration element changed	A DriveLock configuration element was changed. Object type: [ObjectType] Object path: [Path]

Event ID	Source	Audit event	Severity	Short text	Long text
					Object unique ID: [ObjectID] Configuration element: [ConfigElement] Data type: [DataType] New value: [NewValue] Old value: [OldValue]
901	DriveLock	yes	SuccessAudit	DriveLock configuration element added	A DriveLock configuration element was added. Object type: [ObjectType] Object path: [Path] Object unique ID: [ObjectID] Configuration element: [ConfigElement] Data type: [DataType] New value: [NewValue]
902	DriveLock	yes	SuccessAudit	DriveLock configuration element deleted	A DriveLock configuration element was deleted. Object type: [ObjectType] Object path: [Path] Object unique ID: [ObjectID] Configuration element: [ConfigElement] Data type: [DataType]

Event ID	Source	Audit event	Severity	Short text	Long text
910	DriveLock	yes	Information	DriveLock Management Console started	DriveLock Management Console was started. Object type: [ObjectType] Object path: [Path] Object unique ID: [ObjectID]
911	DriveLock	yes	Information	DriveLock Management Console stopped	DriveLock Management Console was stopped.
912	DriveLock	yes	Information	Device scanner executed	Device scanner was executed. Scanned computers: [Computers]
920	DriveLock	yes	Information	Remote agent connection established	Remote agent connection established. Agent computer: [ComputerName] (unique ID [ComputerGuid])
921	DriveLock	yes	Information	Remote agent connection disconnected	Remote agent connection disconnected. Agent computer: [ComputerName] (unique ID [ComputerGuid])

Event ID	Source	Audit event	Severity	Short text	Long text
922	DriveLock	yes	Information	Remote agent action executed	Remote agent action was executed. Agent computer: [ComputerName] (unique ID [ComputerGuid]) Action: [ActionName] Result: [ActionResult]
923	DriveLock	yes	Information	Shadow files viewer connected remotely	Shadowed files viewer was connected to network location. Location: [Computers]
924	DriveLock	yes	Information	Offline unlock wizard failed	The offline unlock wizard was executed and failed. Request code: [RequestCode] Request computer name: [AgentComputerName]
925	DriveLock	yes	Information	Offline unlock succeeded	The offline unlock wizard was executed and succeeded. Request code: [RequestCode] Request computer name: [AgentComputerName] Unlocked drives: [UnlockDrives] Unlocked devices: [UnlockDevices] Unlock time: [UnlockTime] Unlock code: [UnlockCode] Reason: [Reason]

Event ID	Source	Audit event	Severity	Short text	Long text
926	DriveLock	yes	Information	Disk Protection Emergency logon succeeded	A Full Disc Encryption emergency logon was executed and succeeded. Recovery code: [RequestCode] Recovery user name: [UserName] Recovery computer name: [ComputerName] Response code: [UnlockCode]
927	DriveLock	yes	Information	Disk Protection Emergency logon succeeded	A Full Disc Encryption emergency logon was executed and succeeded. Recovery code: [RequestCode] Recovery user name: [UserName] Recovery data file: [FileName] Response code: [UnlockCode]
928	DriveLock	yes	Information	Disk Protection Recovery Disk Key created	A Full Disc Encryption recovery disk key was created. Recovery computer name: [ComputerName] (unique ID [ComputerGuid]) Disk key file: [UnlockCode]
929	DriveLock	yes	Information	Disk Protection Recovery Disk Key created	A Full Disc Encryption recovery disk key was created. Recovery data file:

Event ID	Source	Audit event	Severity	Short text	Long text
					[FileName] Disk key file: [UnlockCode]
930	DriveLock	yes	Information	DriveLock Enterprise Service selected	The DriveLock Enterprise Service [DesName] was selected by DriveLock MMC. Connection ID: [ObjectID]
931	DriveLock	yes	Warning	DriveLock Enterprise Service not available	No DriveLock Enterprise Service is available because no valid server connection is configured.
932	DriveLock	yes	Error	Disk Protection Recovery failed	A Full Disc Encryption recovery process failed. Recovery computer name: [ComputerName] (unique ID [ComputerGuid]) Error: [ErrorMessage]
933	DriveLock	yes	Error	Disk Protection Recovery failed	A Full Disc Encryption recovery process failed. Recovery data file: [FileName] Error: [ErrorMessage]
934	DriveLock	yes	Information	Disk Protection installation package	A Full Disc Encryption installation package was uploaded to the server.

Event ID	Source	Audit event	Severity	Short text	Long text
				uploaded	Package version: [FileName] Server: [ServerName]
935	DriveLock	yes	Information	Disk Protection installation package upload failed	A Full Disc Encryption installation package upload failed. Package version: [FileName] Server: [ServerName] Error: [ErrorMessage]
936	DriveLock	yes	Information	BitLocker Management Emergency logon succeeded	A BitLocker Management emergency logon was executed and succeeded. Recovery code: [RequestCode] Recovery user name: [UserName] Recovery computer name: [ComputerName] Response code: [UnlockCode]
937	DriveLock	yes	Information	BitLocker Management Emergency logon succeeded	A BitLocker Management emergency logon was executed and succeeded. Recovery code: [RequestCode] Recovery user name: [UserName] Recovery data file: [FileName] Response code: [UnlockCode]

Event ID	Source	Audit event	Severity	Short text	Long text
2000	DES	yes	Error	Push installation failed	The push installation of the agent failed on computer [ComputerName]. Error message: ([PiErrorCode]) [PiErrorMessage] Installation step: [PiErrorStep] Attempt number: # [PiAttempts]
2001	DES	yes	Information	Push installation successful	The push installation of the agent on computer [ComputerName] was successful.
2002	DES	no	Error	AV pattern download failed	The download of AV pattern file [FileName] from the DriveLock cloud has failed. Error message: [ErrorMessage].
2003	DES	no	Information	AV pattern download successful	The download of AV pattern file [FileName] from the DriveLock cloud was successful.
2004	DES	no	Error	File download failed	The download of file [FileName] from the DriveLock cloud has failed. Error

Event ID	Source	Audit event	Severity	Short text	Long text
					message: [ErrorMessage].
2005	DES	no	Information	File download successful	The download of file [FileName] from the DriveLock cloud was successful.
2006	DES	no	Information	Disk Protection recovery data saved	The Disk Protection Recovery Data ([FdeRecoveryDataType]) from Computer [ComputerName] has been saved.
2007	DES	no	Information	Encryption 2-Go recovery data saved	The recovery data for encrypted volume (path: '[FilePath][FileName]' , VolumeID: [VolumeID]) has been saved.
2008	DES	no	Information	DFP recovery data saved	The recovery data for encrypted folder (path: '[UncPath]' , VolumeID: [DfpVolumeID]) has been saved.
2009	DES	no	Information	DB maintenance successful	The database maintenance for '[DisplayName]' finished successfully.

Event ID	Source	Audit event	Severity	Short text	Long text
2010	DES	no	Error	DB maintenance aborted	The database maintenance for '[DisplayName]' aborted with an error: '[ErrorMessage]'.
2011	DES	no	Information	DB eventgrooming successful	The database event grooming for '[DisplayName]' finished successfully. Deleted event count: [EventCount]
2012	DES	no	Error	DB event grooming aborted	The database event grooming for '[DisplayName]' aborted with an error: '[ErrorMessage]'.
2013	DES	no	Information	DB backup successful	The database backup for '[DisplayName]' finished successfully.
2014	DES	no	Error	DB backup aborted	The database backup for '[DisplayName]' aborted with an error: '[ErrorMessage]'.
2015	DES	no	Information	DB shrinked successful	The database '[DisplayName]' was shrinked successfully.

Event ID	Source	Audit event	Severity	Short text	Long text
2016	DES	no	Error	Error shrinking database	Error on shrinking database '[DisplayName]': '[ErrorMessage]'.
2017	DES	no	Error	AV pattern sync failed	The download of AV pattern file [FileName] from the central DES has failed. Error message: [ErrorMessage].
2018	DES	no	Information	AV pattern sync successful	The download of AV pattern file [FileName] from the central DES was successful.
2019	DES	no	Error	File download failed	The download of file [FileName] from the central DES has failed. Error message: [ErrorMessage].
2020	DES	no	Information	File download successful	The download of file [FileName] from the central DES was successful.
2021	DES	no	Information	The DES was started	The DES was started.
2022	DES	no	Information	CSP active	The centrally stored policy [CspName], version [CspVersion], ID:

Event ID	Source	Audit event	Severity	Short text	Long text
					[CspID] is now available on the DES.
2023	DES	no	Information	CSP inactive	The centrally stored policy [CspName], version [CspVersion], ID: [CspID] is not available on the DES.
2024	DES	yes	Information	CSP deleted	The centrally stored policy [CspName], ID: [CspID] was deleted.
2025	DES	yes	Information	Policy assignment activated	The policy assignment (centrally stored policy) was activated. Target: [CspAssignmentName], order: [CspAssignmentOrder], policy: [CspName] (ID: [CspID]).
2026	DES	yes	Information	Policy assignment deleted	The assignment of policy [CspAssignmentName] was deleted.
2027	DES	yes	SuccessAudit	Group created	The [GroupMemberType] group [GroupName] (identifier: [GroupIdentifier]) was created.

Event ID	Source	Audit event	Severity	Short text	Long text
2028	DES	yes	SuccessAudit	Group deleted	The [GroupMemberType] group [GroupName] (identifier: [GroupIdentifier]) was deleted.
2029	DES	yes	SuccessAudit	Group member added	The group member [GroupMemberName] (identifier: [GroupMemberIdentifier]) was added to the [GroupMemberType] group: [GroupName] (identifier: [GroupIdentifier]). Type: [GroupChildType]
2030	DES	yes	SuccessAudit	Group member removed	The group member [GroupMemberName] (identifier: [GroupMemberIdentifier]) was removed from the [GroupMemberType] group: [GroupName] (identifier: [GroupIdentifier]). Type: [GroupChildType]
2031	DES	yes	SuccessAudit	Group member updated	The group member [GroupMemberName] (identifier: [GroupMemberIdentifier]) was updated in the [GroupMemberType] group:

Event ID	Source	Audit event	Severity	Short text	Long text
					[GroupName] (identifier: [GroupIdentifier]). Exclude status is: [GroupMemberExclude].
2032	DES	yes	SuccessAudit	Group updated	The group with identifier [GroupIdentifier] was updated. Name: [GroupName], Description: [GroupDescription]
2033	DES	yes	SuccessAudit	Dynamic group created	The dynamic group [GroupName] (identifier: [GroupIdentifier]), type: [GroupMemberType] was created.
2034	DES	yes	SuccessAudit	Dynamic group deleted	The dynamic group [GroupName] (identifier: [GroupIdentifier]), type: [GroupMemberType] was deleted.
2035	DES	yes	SuccessAudit	Dynamic group updated	The dynamic group with identifier [GroupIdentifier] was updated. Name: [GroupName], Description: [GroupDescription]

Event ID	Source	Audit event	Severity	Short text	Long text
2036	DES	yes	SuccessAudit	Dynamic group changed	The dynamic group [GroupName] (identifier: [GroupIdentifier]) was changed. group definition (old): [GroupDynDefinitionOld] group definition (new): [GroupDynDefinitionNew]
2037	DES	yes	Information	Policy assignment deactivated	The policy assignment (centrally stored policy) was deactivated. Target: [CspAssignmentName], order: [CspAssignmentOrder], Policy: [CspName] (ID: [CspID]).
2038	DES	no	Information	Audit event cleanup successful	Audit event cleanup for database '[DisplayName]' finished successfully. Deleted audit event count: [EventCount]
2039	DES	no	Error	Audit event cleanup aborted	Audit event cleanup for database '[DisplayName]' aborted with an error: ' [ErrorMessage]'.
2040	DES	yes	Information	Policy assignment cre-	The policy assignment (centrally

Event ID	Source	Audit event	Severity	Short text	Long text
				ated	stored policy) was created. Target: [CspAssignmentName], order: [CspAssignmentOrder], Policy: [CspName] (ID: [CspID]).
2041	DES	yes	Information	Policy assignment changed	The policy assignment (centrally stored policy) was changed. Target: [CspAssignmentName], order: [CspAssignmentOrder], Policy: [CspName] (ID: [CspID]).
2100	DOC	yes	SuccessAudit	Account created	The account [AccountDisplayName] (identifier: [AccountIdentifier]) was created
2101	DOC	yes	SuccessAudit	Account deleted	The account [AccountDisplayName] (identifier: [AccountIdentifier]) was deleted
2102	DOC	yes	SuccessAudit	Role assignment created	The role [RoleDisplayName] (id: [RoleID]) was assigned to the account [AccountDisplayName] (identifier:

Event ID	Source	Audit event	Severity	Short text	Long text
					[AccountIdentifier]). OU Restrictions: ([OuRestriction]), Group [GroupName] (identifier: [GroupIdentifier])
2103	DOC	yes	SuccessAudit	Role assignment deleted	The role assignment [RoleDisplayName] (id: [RoleID]) was removed from the account [AccountDisplayName] (identifier: [AccountIdentifier])
2104	DOC	yes	SuccessAudit	Account email changed	The email of account '[AccountDisplayName]' was changed from [AccountIdentifier] to [AccountIdentifier2]'
2105	DES	no	SuccessAudit	Agent successfully registered	An agent successfully registered
2106	DES	no	FailureAudit	Attempt to register with invalid join token	The agent tried to register with the invalid join token '[JoinToken]'

Event ID	Source	Audit event	Severity	Short text	Long text
2107	DES	no	FailureAudit	Rejected attempt to change agent ID	The agent tried to update its agent ID to the new value '[IdToken]'. This is not permitted. Please reset the agent registration via DOC if this change is intended
2108	DES	no	FailureAudit	Rejected agent access because of not existing agent ID	Rejected access to DES for agent. The agent sent the not existing agent ID '[IdToken]'
2109	DES	no	FailureAudit	Rejected agent access because of improper agent ID	Rejected access to DES for agent. The agent sent the agent ID '[IdToken]' which does not belong to it. The conflicting data (name/ID) is: [AgentRejectedReason]
2110	DES	yes	Information	Uploaded trace files to DriveLock support	Uploaded trace files from agent to DriveLock support for further analysis
2111	DES	yes	Information	Default data masking enabled	Default data masking is enabled. All relevant user data is masked according to the settings.

Event ID	Source	Audit event	Severity	Short text	Long text
2112	DES	yes	Information	Default data masking disabled	Default data masking is disabled. The relevant user data is shown in the original text.
2113	DES	yes	Information	Data masking configuration changed	Data masking configuration has been changed
2114	DES	yes	Information	Request for unmasking data generated	Request for unmasking data of '[PiiObjectType]' for [Duration] minutes has been generated. Reason for unmasking: [Reason]
2115	DES	yes	SuccessAudit	Request for unmasking data accepted	Request from '[UserName]' for unmasking data of '[PiiObjectType]' for [Duration] minutes has been accepted. Reason for unmasking: [Reason]
2116	DES	yes	FailureAudit	Request for unmasking data denied	Request from '[UserName]' for unmasking data of '[PiiObjectType]' for [Duration] minutes has been denied. Reason for unmasking: [Reason]

Event ID	Source	Audit event	Severity	Short text	Long text
2117	DES	yes	SuccessAudit	Started showing unmasked data	Unmasking data has started.
2118	DES	yes	SuccessAudit	Stopped showing unmasked data	Showing unmasked data has ended
2119	DES	yes	SuccessAudit	Custom data masking settings changed	Custom data masking settings have been changed
2120	DES	yes	SuccessAudit	Custom data masking settings reset	Custom data masking settings have been reset
2121	DES	yes	SuccessAudit	Started showing masked data	Masking data has started
2122	DES	yes	SuccessAudit	Stopped showing masked data	Showing masked data has ended
2123	DES	yes	FailureAudit	Request for unmasking with wrong or invalid code	Request for unmasking data of '[PiiObjectType]' for [Duration] minutes with wrong or invalid code. Reason for unmasking: [Reason]

Event ID	Source	Audit event	Severity	Short text	Long text
2150	DES	yes	Information	Tenant created	A tenant was created
2151	DES	yes	Information	Tenant attached	A tenant was attached
2152	DES	yes	Information	Tenant detached	A tenant was detached
2153	DES	yes	Information	Global tenant configuration modified	The global configuration of the tenant has been modified
2160	DES	yes	Information	Certificate was created	Certificate '[FileName]' was created
2161	DES	yes	Information	Certificate was deleted	Certificate '[FileName]' was deleted
2162	DES	yes	Information	Certificate was changed	Certificate '[FileName]' was changed
2170	DES	yes	Information	API key added	Added an API key '[DisplayName]' holding the permissions '[Details]' which is valid until [TimeStamp]

Event ID	Source	Audit event	Severity	Short text	Long text
2171	DES	yes	Information	API key added (no expiration)	Added an API key '[DisplayName]' holding the permissions '[Details]'. The key does not expire.
2172	DES	yes	Information	Deleted API key	Deleted the API key '[DisplayName]'.
2173	DES	yes	Information	Modified API key	Modified API key '[DisplayName]'. New permissions are: [Details]
2180	DES	yes	Information	Azure AD Sync Configuration was added	Azure AD Sync Configuration for Azure AD tenant '[DisplayName]' was added
2181	DES	yes	Information	Azure AD Sync Configuration was deleted	Azure AD Sync Configuration for Azure AD tenant '[DisplayName]' was deleted
2182	DES	yes	Information	Azure AD Sync was triggered	Azure AD Sync for Azure AD tenant ' [DisplayName]' was triggered
2183	DES	yes	Information	Azure AD Sync Config updated	Azure AD Sync config for Azure AD tenant '[DisplayName]' was updated

Event ID	Source	Audit event	Severity	Short text	Long text
2200	DES	yes	Information	Windows authentication enabled	Logon via Windows authentication enabled.
2201	DES	yes	Information	Windows authentication disabled	Logon via Windows authentication disabled
2210	DES	yes	Information	SAML authentication configuration created	SAML authentication configuration '[DisplayName]' created.
2211	DES	yes	Information	SAML authentication configuration deleted	SAML authentication configuration '[DisplayName]' deleted
2212	DES	yes	Information	SAML authentication configuration modified	SAML authentication configuration '[DisplayName]' modified. Changes: [Details].
2213	DES	yes	Information	SAML authentication configuration enabled	SAML authentication configuration '[DisplayName]' enabled.
2214	DES	yes	Information	SAML authentication configuration disabled	SAML authentication configuration '[DisplayName]' disabled.

Event ID	Source	Audit event	Severity	Short text	Long text
2215	DES	yes	Information	Mandatory SSO login enabled	Mandatory login via single sign on (SSO) enabled. The following users may bypass this setting: [Details]
2216	DES	yes	Information	Mandatory SSO login disabled	Mandatory login via single sign on (SSO) disabled.
2217	DES	yes	Information	SSO user exclude list changed	The list of users which may login bypassing single sign on (SSO) has changed: [Details].
2220	DES	yes	Information	Role created	Role created: [RoleDisplayName]
2221	DES	yes	Information	Role deleted	Role deleted: [RoleDisplayName]
2222	DES	yes	Information	Role modified	Role modified: [RoleDisplayName]
2223	DES	yes	Information	Role permission modified	Role permission modified: [RoleDisplayName]
2230	DES	yes	Information	Dashboard widget template added	A dashboard widget template was added

Event ID	Source	Audit event	Severity	Short text	Long text
2231	DES	yes	Information	Dashboard widget template deleted	A dashboard widget template was deleted
2232	DES	yes	Information	Dashboard widget template modified	A dashboard widget template was modified
2240	DES	yes	Information	Computer deleted	Computer [Computers] deleted with options: DeleteComputerEvents: [DeleteComputerEvents], DeleteComputerGroupDefinitions: [DeleteComputerGroupDefinitions], DeleteComputerRecoveryData: [DeleteComputerRecoveryData]
2241	DES	yes	Information	Agent action added	Added agent action [Type] for computer [ComputerName]
2242	DES	yes	Information	Agent action updated	Updated agent action [Type] for computer [ComputerName]
2243	DES	yes	Information	Agent action deleted	Deleted agent action [Type] for computer [ComputerName]

Event ID	Source	Audit event	Severity	Short text	Long text
2290	DES	yes	Information	Alert state changed	Alert '[DisplayName]' (identifier: [ObjectID]) state was changed from [IntValue] to [IntValue2]
2330	DES	yes	Information	Threat was suppressed in general	Threat '[DisplayName]' was suppressed for all computers
2331	DES	yes	Information	Threat is no longer suppressed in general	Threat '[DisplayName]' is no longer suppressed for all computers
2332	DES	yes	Information	Threat was suppressed for a computer	Threat '[DisplayName]' was suppressed for a computer
2333	DES	yes	Information	Threat is no longer suppressed for a computer	Threat '[DisplayName]' is no longer suppressed for a computer.
2320	DES	yes	Information	Vulnerability was suppressed in general	Vulnerability '[DisplayName]' was suppressed for all computers
2321	DES	yes	Information	Vulnerability is no	Vulnerability '[DisplayName]' is no

Event ID	Source	Audit event	Severity	Short text	Long text
				longer suppressed in general	longer suppressed for all computers.
2322	DES	yes	Information	Vulnerability was suppressed for a computer	Vulnerability '[DisplayName]' was suppressed for a computer
2323	DES	yes	Information	Vulnerability is no longer suppressed for a computer	Vulnerability '[DisplayName]' is no longer suppressed for a computer
2340	DES	yes	Information	File Protecion recovery executed	File Protecion recovery was executed
2341	DES	yes	Information	Encryption 2-Go recovery executed	Encryption 2-Go recovery was executed
2342	DES	yes	Information	BitLocker To Go recovery executed	BitLocker To Go recovery was executed
2343	DES	yes	Information	BitLocker recovery executed	BitLocker recovery was executed

Event ID	Source	Audit event	Severity	Short text	Long text
2344	DES	yes	Information	Local user account recovery executed	Local user account recovery was executed
2380	DES	yes	Information	Report created	Report created: [DisplayName]
2381	DES	yes	Information	Report deleted	Report deleted: [DisplayName]
2382	DES	yes	Information	Report modified	Report modified: [DisplayName]
2400	DES	yes	Information	Drive rule created	Drive rule [RuleName] was created in policy [CspName], version [CspVersion]
2401	DES	yes	Information	Drive rule deleted	Drive rule [RuleName] was deleted in policy [CspName], version [CspVersion]
2402	DES	yes	Information	Drive rule changed	Drive rule [RuleName] was changed in policy [CspName], version [CspVersion]
2403	DES	yes	Information	Application rule cre-	Application rule [RuleName] was cre-

Event ID	Source	Audit event	Severity	Short text	Long text
				ated	ated in policy [CspName], version [CspVersion]
2404	DES	yes	Information	Application rule deleted	Application rule [RuleName] was deleted in policy [CspName], version [CspVersion]
2405	DES	yes	Information	Application rule changed	Application rule [RuleName] was changed in policy [CspName], version [CspVersion]
2406	DES	yes	Information	Security awareness rule created	Security awareness rule [RuleName] was created in policy [CspName], version [CspVersion]
2407	DES	yes	Information	Security awareness rule deleted	Security awareness rule [RuleName] was deleted in policy [CspName], version [CspVersion]
2408	DES	yes	Information	Security awareness rule changed	Security awareness rule [RuleName] was changed in policy [CspName], version [CspVersion]

Event ID	Source	Audit event	Severity	Short text	Long text
2500	DES	yes	Information	Policy created	Policy created: [CspName], ID: [ConfigId]
2501	DES	yes	Information	Policy saved	Policy saved: [CspName] (ID: [ConfigId])
2502	DES	yes	Information	Policy published	Policy published: [CspName], version: [CspVersion] (ID: [ConfigId]), publish comment: [CspPublishComment]
2503	DES	yes	Information	Policy unpublished	Policy unpublished: [CspName], version: [CspVersion] (ID: [ConfigId])
2504	DES	yes	Information	Policy history deleted	Policy history deleted: [CspName], version: [CspVersion] (ID: [ConfigId]), deleted previous versions: [BoolValue]
2513	DES	yes	Information	Policy assignment rearranged	Policy assignment rearranged: [CspAssignmentName]
2540	DES	yes	Information	Policy collection created	The [GroupMemberType] policy collection [GroupName] (identifier:

Event ID	Source	Audit event	Severity	Short text	Long text
					[GroupIdentifier]) was created.
2541	DES	yes	Information	Policy collection deleted	The [GroupMemberType] policy collection [GroupName] (identifier: [GroupIdentifier]) was deleted.
2542	DES	yes	Information	Policy collection updated	The policy collection with identifier [GroupIdentifier] was updated. Name: [GroupName], Description: [GroupDescription]
2543	DES	yes	Information	Added policy to policy collection	The policy [GroupMemberName] (identifier: [GroupMemberIdentifier]) was added to the [GroupMemberType] policy collection: [GroupName] (identifier: [GroupIdentifier]). Type: [GroupChildType]
2544	DES	yes	Information	Removed policy from policy collection	The policy [GroupMemberName] (identifier: [GroupMemberIdentifier]) was removed from the [GroupMemberType] policy collection:

Event ID	Source	Audit event	Severity	Short text	Long text
					[GroupName] (identifier: [GroupIdentifier]). Type: [GroupChildType]
2545	DES	yes	Information	Policy collection member updated	The policy collection member [GroupMemberName] (identifier: [GroupMemberIdentifier]) was updated in the [GroupMemberType] policy collection: [GroupName] (identifier: [GroupIdentifier]). Exclude status is: [GroupMemberExclude].
2550	DES	yes	Information	Enabled network PBA interface	Enabled the network PBA interface on DES '[DesName]'.
2551	DES	yes	Information	Disabled network PBA interface	Disabled the network PBA interface on DES '[DesName]'.
2660	DES	yes	Information	DiskEncrypt company certificate created	A new DiskEncrypt company certificate with the name '[DisplayName]' has been created. The thumbprint is '

Event ID	Source	Audit event	Severity	Short text	Long text
					[CertThumbprint]'.
2661	DES	yes	Information	DiskEncrypt company certificate updated	The DiskEncrypt company certificate has been updated. The new certificate has the name '[DisplayName]' and has the thumbprint '[CertThumbprint]'.
2662	DES	yes	Information	DiskEncrypt company selected	A DiskEncrypt company certificate has been selected. The certificate has the name '[DisplayName] and the thumbprint '[CertThumbprint]'.
2663	DES	yes	Information	DiskEncrypt company downloaded	A copy of the DiskEncrypt company certificate has been downloaded. The certificate has the name '[DisplayName] and the thumbprint '[CertThumbprint]'.
2664	DES	yes	Information	DiskEncrypt policy downloaded as MSI	The DiskEncrypt policy '[CspName]' (version: [CspVersion]) has been downloaded as a MSI package.

Event ID	Source	Audit event	Severity	Short text	Long text
2665	DES	yes	Information	DiskEncrypt policy downloaded as CCP	The DiskEncrypt policy '[CspName]' (version: [CspVersion]) has been downloaded as a CCP package.
2666	DES	yes	Information	DiskEncrypt recovery environment created	A new DiskEncrypt recovery environment with the name '[DisplayName]' was created.
2667	DES	yes	Information	DiskEncrypt recovery environment modified	The DiskEncrypt recovery environment with the name '[DisplayName]' was modified. New data: [Details]
2668	DES	yes	Information	DiskEncrypt recovery environment deleted	The DiskEncrypt recovery environment with the name '[DisplayName]' was deleted.
2669	DES	yes	Information	Disk recovery using DiskEncrypt challenge/response executed	A disk recovery with challenge/response was executed using the DiskEncrypt recovery environment '[DisplayName]'.

Event ID	Source	Audit event	Severity	Short text	Long text
2670	DES	yes	Information	DiskEncrypt recovery environment exported	The DiskEncrypt recovery environment '[DisplayName]' was exported'.
2680	DES	yes	Information	Successful login at DriveLock Operations Center	A user successfully logged in to the DriveLock Operations Center using the authentication method ' [LogonMethod]'.
2681	DES	yes	Error	Failed login at DOC	A user failed to login to the DriveLock Operations Center using the authentication method '[LogonMethod]'. Reason: [LogonError].
2702	DES	yes	Information	Account modified	The account [AccountDisplayName] (identifier: [AccountIdentifier]) has been modified
2710	DES	no	Information	Computer selected for AD inventory	The computer was selected by the server to collect AD inventory data.
2720	DES	yes	Information	xxxMFA method	xxxThe MFA method '[DisplayName]'

Event ID	Source	Audit event	Severity	Short text	Long text
				added	has been added
2721	DES	yes	Information	xxxMFA method deleted	xxxThe MFA method '[DisplayName]' has been deleted
2722	DES	yes	Information	xxxMFA method disabled	xxxThe MFA method '[DisplayName]' has been disabled
2723	DES	yes	Information	xxxMFA logon requirements changed	xxxThe logon methods which require MFA have been changed to: '[Details]'
2724	DES	yes	Information	xxxMFA disabled by admin	xxxMFA has been disabled for user '[UserName]'
2725	DES	yes	Warning	xxxMFA code rejected	xxxThe MFA code has not been accepted

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.