




# DriveLock Events

## List of DriveLock Events 2020.1

---

DriveLock SE 2020



---

## Table of Contents

<b>1 DRIVELOCK VERSION 2020.1</b> .....	<b>3</b>
1.1 Events .....	3
<b>COPYRIGHT</b> .....	<b>156</b>

# 1 DriveLock Version 2020.1

The events apply to DriveLock version 2020.1.

## 1.1 Events

Event ID	Source	Severity	Short text	Long text
100	DriveLock	Information	Service installed	The [ServiceName] service was installed.
101	DriveLock	Information	Service removed	The [ServiceName] service was removed.
102	DriveLock	Error	Cannot remove service	The [ServiceName] service could not be removed.
103	DriveLock	Error	Control handler error	The control handler could not be installed.
104	DriveLock	Error	Initialization failed	The initialization process failed.
105	DriveLock	Information	Service started	The [ServiceName] service was started.
106	DriveLock	Error	Unsupported request	The [ServiceName] service received an unsupported request.
107	DriveLock	Information	Debug message	Debug: [DebugMsg]

Event ID	Source	Severity	Short text	Long text
108	DriveLock	Information	Service stopped	The service [ServiceName] was stopped.
109	DriveLock	Information	Trace message	Trace: [DebugMsg]
110	DriveLock	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]): [SessionLockState]
111	DriveLock	Audit	Drive connected and locked	The drive [DriveLetter] ([StorageType]) was added to the system. It is controlled by {Product} 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] [HWPro-

Event ID	Source	Severity	Short text	Long text
				ductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
112	DriveLock	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: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
113	DriveLock	Audit	Drive disconnected	The drive [DriveLetter] was disconnected from the system. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])

Event ID	Source	Severity	Short text	Long text
114	DriveLock	Information	Drive unlocked	The drive [DriveLetter] was unlocked on the system. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
115	DriveLock	Audit	Drive locked	The drive [DriveLetter] ([StorageType]) will be controlled by {Product}. 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]): [SessionLockState]
116	DriveLock	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 [User-

Event ID	Source	Severity	Short text	Long text
				LockState] for this event's user account. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
117	DriveLock	Information	Licensing message	Licensing: [LicenseInfo]
118	DriveLock	Error	Account error	Cannot add account [UserName] (domain [DomainName]) to the allow list.
119	DriveLock	Error	Configuration file error	Configuration file error: [FileName]
120	DriveLock	Audit	Serial port locked	The serial port [HardwareID] is controlled by {Product} because of company policy. As an ACL was applied to the port, some users may no longer be able to access it. Friendly name: [DisplayName] Hardware Id: [CompatibleID] Class Id: [ClassID]
121	DriveLock	Error	Error locking serial port	Locking of serial port [HardwareID] was

Event ID	Source	Severity	Short text	Long text
				attempted but the system reported an error. Friendly name: [DisplayName] Hardware Id: [CompatibleID] Class Id: [ClassID]
122	DriveLock	Error	Windows Firewall error	Error while configuring the Windows Firewall. {Product} remote control may not work on this agent. Error code: [ErrorCode] Error: [ErrorMessage]
123	DriveLock	Warning	No GPO present	Warning: No Group Policy configuration present.
124	DriveLock	Information	Device restarted	The device [DisplayName] is managed by {Product} and was restarted due to a user change. Hardware ID: [HardwareID] Class ID: [ClassID]
125	DriveLock	Error	Device restart - Error	The device [DisplayName] is managed by {Product}. The current user changed but there was an error restarting the device. Hardware ID: [HardwareID] Class ID: [ClassID]



Event ID	Source	Severity	Short text	Long text
126	DriveLock	Warning	Device restart - Needs reboot	{Product} 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	Audit	Parallel port locked	The parallel port [DisplayName] is controlled by {Product} because of company policy. As an ACL was applied to the port, some users may no longer be able to access it. Friendly name: [HardwareID] Hardware Id: [CompatibleID] Class Id: [ClassID]
128	DriveLock	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	Audit	Device connected and locked	The device [DisplayName] was connected to the computer. It was locked due to com-

Event ID	Source	Severity	Short text	Long text
				pany policy. Device type: [DeviceType] Hardware ID: [HardwareID] Class ID: [ClassID] Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
130	DriveLock	Audit	Device connected and not locked	The device [DisplayName] was connected to the computer. Device type: [DeviceType] Hardware ID: [HardwareID] Class ID: [ClassID] Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
131	DriveLock	Audit	Temporarily unlocked	{Product} Agent was temporarily unlocked by an administrator. Administrator computer: [DisplayName] (unique ID [ComputerGuid]) Administrator account: [UserName] (domain [Domain], SID [SID]) Unlock period: [UnlockTime] [UnlockUnit] Reason: [Reason]
132	DriveLock	Audit	Temporary unlocked can-	The temporary unlock mode of the

Event ID	Source	Severity	Short text	Long text
			celled	{Product} Agent was canceled by an administrator. Administrator computer: [DisplayName] (unique ID [ComputerGuid]) Administrator account: [UserName] (domain [Domain], SID [SID])
133	DriveLock	Audit	File accessed	File accessed. File path: [Path] File name: [FileName] Drive: [DriveLetter] File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName] Device identification: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
134	DriveLock	Error	Agent not licensed	{Product} is not licensed to run on this computer.
135	DriveLock	Error	Logon error	The user [UserName] cannot be impersonated on this computer. Please check the user name and password in the con-

Event ID	Source	Severity	Short text	Long text
				figuration. Error code: [ErrorCode] Error: [ErrorMessage]
136	DriveLock	Error	Shadow copy upload error	Cannot upload shadow copy file [FileName] to the central storage location [UploadLocation]. Error code: [ErrorCode] Error: [ErrorMessage]
137	DriveLock	Warning	Conflicting policy detected	A Microsoft policy that can conflict with a {Product} policy was detected on this computer. Refer to the {Product} Manual for more information about this policy. It is recommended to disable the Microsoft policy.
138	DriveLock	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 until the next reboot.
139	DriveLock	Warning	Temporary unlock ended	The temporary unlock mode of the

Event ID	Source	Severity	Short text	Long text
				{Product} Agent ended because the unlock time elapsed.
140	DriveLock	Audit	Volume mounted	A {Product} 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	Audit	Volume unmounted	A {Product} encrypted volume was unmounted. Status: [CryptStatus] Volume container: [DriveLetter] Volume GUID: [VolumeID] Drive letter: [FileName] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
142	DriveLock	Audit	Volume created	A {Product} encrypted volume was created/formatted. Status: [CryptStatus] Volume container: [FileName] Volume

Event ID	Source	Severity	Short text	Long text
				GUID: [VolumeID] File system: [FileSystemType] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
143	DriveLock	Audit	Password changed	The password for a {Product} encrypted volume was changed. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
144	DriveLock	Information	Network changed	A network connection was changed. Network adapter: [NetAdapter] Network location name: [DisplayName] Network location GUID: [ObjectID]
145	DriveLock	Audit	File blocked by content scanner	File blocked by content scanner. Content does not match file extension. File path: [Path] File name: [FileName] Drive:

Event ID	Source	Severity	Short text	Long text
				[DriveLetter] File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName] Device ID: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
146	DriveLock	Audit	Process blocked	The execution of a process was blocked by company policy. Process: [ProcessName] File Hash: [ProcessHash] Applied whitelist rule: [ObjectID] Whitelist rule type: [WType]
147	DriveLock	Audit	Process started	A process was started. Process: [ProcessName] File Hash: [ProcessHash] Applied whitelist rule: [ObjectID] Whitelist rule type: [WType]
148	DriveLock	Audit	File extension blocked	File blocked by file filter. Access denied due to file type. File path: [Path] File name: [FileName] Drive: [DriveLetter] File size:

Event ID	Source	Severity	Short text	Long text
				[Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName] Device ID: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
149	DriveLock	Warning	Network profile shutdown	The computer is shut down because of a Network Profiles policy. Network location GUID: [ObjectID]
150	DriveLock	Warning	Network adapter disabled	Network adapters are disabled because of a Network Profiles policy. Network location GUID: [ObjectID]
151	DriveLock	Warning	Windows Terminal Services disabled	Windows Terminal Services are disabled on this computer. {Product} depends on Terminal Services to detect user changes in real-time. Legacy functions are used to maintain {Product} functionality, consider enabling Terminal Services.



Event ID	Source	Severity	Short text	Long text
152	DriveLock	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.
153	DriveLock	Warning	Configuration file applied	The configuration file [FileName] was successfully applied.
154	DriveLock	Error	Configuration file download error	The configuration file [FileName] could not be downloaded. Error code: [ErrorCode] Error: [ErrorMessage]
155	DriveLock	Error	Configuration file error	The configuration file [FileName] could not be loaded into the local registry. Error code: [ErrorCode] Error: [ErrorMessage]
156	DriveLock	Error	Configuration file error	A temporary copy of the configuration file [FileName] could not be created. Error code: [ErrorCode] Error: [ErrorMessage]
157	DriveLock	Warning	Configuration file error	The configuration file [FileName] is invalid

Event ID	Source	Severity	Short text	Long text
				or corrupt. Error code: [ErrorCode] Error: [ErrorMessage]
158	DriveLock	Warning	Configuration file error	The configuration file [FileName] could not be read. Error code: [ErrorCode] Error: [ErrorMessage]
159	DriveLock	Warning	Account error	User account [UserName] could not be impersonated to access the configuration file [FileName]. Error code: [ErrorCode] Error: [ErrorMessage]
160	DriveLock	Warning	{FDE} installation error	Not enough disk space available to install and configure {DiskProtection}. Required disk space: [RequiredSpace] bytes Available disk space: [AvailableSpace] bytes
161	DriveLock	Error	Account error	User account [UserName] could not be impersonated to access the {DiskProtection} package. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
162	DriveLock	Warning	{FDE} package download error	The {DiskProtection} package could not be downloaded from [URL] Error code: [ErrorCode] Error: [ErrorMessage]
163	DriveLock	Warning	{FDE} installation error	The {DiskProtection} package is not installed locally.
164	DriveLock	Warning	{FDE} download successful	The {DiskProtection} package was successfully downloaded.
165	DriveLock	Warning	{FDE} installation error	The {DiskProtection} package could not be extracted. The file [PackagePath] may be missing or corrupt.
166	DriveLock	Warning	{FDE} installation error	The {DiskProtection} configuration script [ScriptFile] is missing in the {Product} policy.
167	DriveLock	Warning	{FDE} installation error	The command line "[CmdLine]" could not be executed. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
168	DriveLock	Warning	{FDE} installation successful	{DiskProtection} was successfully installed.
169	DriveLock	Warning	{FDE} installation error	{DiskProtection} installation failed.
170	DriveLock	Warning	{FDE} installation error	{DiskProtection} is configured on this computer but the installation failed.
171	DriveLock	Warning	{FDE} installation error	The status information file [FileName] could not be created.
172	DriveLock	Warning	{FDE} installation error	The {DiskProtection} configuration script [FileName] could not be copied to its target location. Error code: [ErrorCode] Error: [ErrorMessage]
173	DriveLock	Audit	File created	New file created. File path: [Path] File name: [FileName] Drive: [DriveLetter] File size: [Size] File name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName] Device identification: [HWVendorID] [HWProductID] (Rev. [HWRe-

Event ID	Source	Severity	Short text	Long text
				visionNumber]) (Serial number [HWSerialNumber])
174	DriveLock	Warning	{FDE} installation prevented	The {DiskProtection} should be installed but the installation is prevented by administrative intervention.
175	DriveLock	Warning	{FDE} installation error	The {DiskProtection} setup could not clean up installation files. Error code: [ErrorCode] Error: [ErrorMessage]
176	DriveLock	Warning	Pre-boot authentication error	Pre-boot authentication is configured on this computer but the initialization failed.
179	DriveLock	Warning	{FDE} encryption started	{DiskProtection} started encrypting local hard disks.
181	DriveLock	Warning	{FDE} encryption successful	{DiskProtection} successfully encrypted local hard disks.
183	DriveLock	Warning	{FDE} decryption started	{DiskProtection} started decrypting local hard disks.

Event ID	Source	Severity	Short text	Long text
184	DriveLock	Warning	{FDE} decryption successful	{DiskProtection} successfully decrypted local hard disks.
185	DriveLock	Warning	{FDE} upload error	The {DiskProtection} data [LogFile] could not be uploaded to the {PrefixEnterpriseService}. Error [ErrorMessage]
186	DriveLock	Warning	{FDE} system error	The log file [LogArchive] could not be added to the log archive [LogFile]
187	DriveLock	Warning	{FDE} system error	Emergency Recovery Information could not be moved to [TargetFolder]. Error code: [ErrorCode] Error: [ErrorMessage]
188	DriveLock	Warning	{FDE} uninstallation successful	{DiskProtection} was successfully uninstalled.
189	DriveLock	Error	{FDE} installation - wrong package version	{DiskProtection} installation or update was aborted because the wrong version of the installation package was detected. Installed version: [InstalledVersion] Expected version: [ExpectedVersion]

Event ID	Source	Severity	Short text	Long text
190	DriveLock	Warning	File already present	The file [PolicyStorageContainer] already existed in the temporary location when extracting Policy File storage from file [FileName]
191	DriveLock	Warning	{PrefixEnterpriseService} selected	The {PrefixEnterpriseService} [DesName] was selected by {Product}. Connection ID: [ObjectID] Used for: [AgentServerType]
192	DriveLock	Warning	{PrefixEnterpriseService} not available	No {PrefixEnterpriseService} is available because no valid server connection is configured.
193	DriveLock	Warning	Command line execution error	The file [CmdLine] does not exist while trying to execute an event command or script.
194	DriveLock	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]

Event ID	Source	Severity	Short text	Long text
195	DriveLock	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	Warning	Command line not executed	No user is logged on. Therefore an event command or script could not be executed with user permissions. Command line: [CmdLine]
197	DriveLock	Warning	Command line executed (user)	An event command or script was executed with user permissions. Command line: [CmdLine]
198	DriveLock	Warning	Command line executed	An event command or script was executed with system permissions. Command line: [CmdLine]
199	DriveLock	Warning	Drive temporarily unlocked	Drive types temporarily unlocked by administrative intervention are [DriveType1] [DriveType2] [DriveType3]



Event ID	Source	Severity	Short text	Long text
				[DriveType4] [DriveType5] [DriveType6] [DriveType7] [DriveType8] [DriveType9] [DriveType10]
200	DriveLock	Warning	Devices temporarily unlocked	Device classes temporarily unlocked by administrative intervention are [DeviceTypes]
202	DriveLock	Warning	File copy error	Copying existing files failed while encrypting volume [FileName]. Volume GUID: [VolumeID]
203	DriveLock	Warning	Files deleted	Existing files were deleted from volume [FileName]. Reason: [AcDeleteReason] Volume GUID: [VolumeID]
205	DriveLock	Warning	File delete error	Deleting existing files failed while encrypting volume [FileName]. Volume GUID: [VolumeID]
206	DriveLock	Warning	{FDE} uninstallation failed	{DiskProtection} uninstallation failed.

Event ID	Source	Severity	Short text	Long text
207	DriveLock	Warning	{FDE} cannot apply configuration	The {DiskProtection} configuration could not be applied.
208	DriveLock	Warning	{FDE} key backup failed	The {DiskProtection} key backup failed.
209	DriveLock	Warning	{FDE} no license	{DiskProtection} is configured to encrypt local hard disks but is not licensed on this computer.
210	DriveLock	Warning	Cannot enumerate PBA users	{DiskProtection} cannot enumerate configured pre-boot authentication users.
211	DriveLock	Warning	Cannot add user to PBA	{DiskProtection} cannot add user [UserName] (domain [DomainName]) to the pre-boot authentication user database.
212	DriveLock	Warning	Cannot remove user from PBA	{DiskProtection} cannot remove user [UserName] (domain [DomainName]) from the pre-boot authentication user database.
213	DriveLock	Warning	Cannot deactivate PBA	Pre-boot authentication cannot be deactivated while the hard disk is encrypted.

Event ID	Source	Severity	Short text	Long text
				The {Product} configuration is inconsistent and should be changed so that pre-boot authentication is active while hard disks are encrypted.
214	DriveLock	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	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	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	Warning	Incompatible server version (needs update)	The configured server is not compatible with this version of the agent. It must be

Event ID	Source	Severity	Short text	Long text
				upgraded in order to support all features of this version. Missing method: [MethodName]
218	DriveLock	Audit	File accessed	File accessed. File path: [Path] File name: [FileName] File name hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
219	DriveLock	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	Warning	Internal error with recovery information	An internal error occurred while creating recovery information for encrypted volume [FileName]. Volume GUID: [VolumeID]
221	DriveLock	Warning	Application hash database missing	The application hash database [FileName] is missing from the policy file storage.

Event ID	Source	Severity	Short text	Long text
				Please check if the group policy or configuration file is correctly applied. Whitelist rule: [ObjectID]
222	DriveLock	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. Whitelist rule: [ObjectID]
223	DriveLock	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. Whitelist rule: [ObjectID]
224	DriveLock	Warning	Encrypted volume password recovered	A {Product} Encrypted volume password was recovered. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number

Event ID	Source	Severity	Short text	Long text
				[HWSerialNumber]
225	DriveLock	Warning	Illegal offline unlock attempt	{Product} detected an illegal attempt to unlock the agent using the offline unlock functionality.
226	DriveLock	Warning	Offline unlock requested	An offline unlock request was initiated by the user. Request code: [RequestCode]
227	DriveLock	Error	{Product} program file tampered	A {Product} program file was tampered or changed or the digital signature could not be verified. File: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
228	DriveLock	Warning	Event queue full	The event queue was full and wrapped. Some older events were deleted and will not be forwarded to external targets.
229	DriveLock	Warning	Running in simulation mode	{Product} is running in simulation mode. Nothing will be locked or filtered.
230	DriveLock	Warning	SSL: Cannot create DH para-	The encrypted communications layer (SSL)

Event ID	Source	Severity	Short text	Long text
			meters	could not create key exchange parameters (DH). Default values will be used resulting in weaker encryption.
231	DriveLock	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	Error	SSL: Cannot open certificate file	The encrypted communications layer (SSL) cannot open the certificate file used for encryption. SSL will be unavailable. Certificate file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
233	DriveLock	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]

Event ID	Source	Severity	Short text	Long text
234	DriveLock	Error	Cannot add port to Windows Firewall exceptions	Error while adding a port exception to the Windows Firewall. {Product} remote control may not work on this agent. Port: [Port] Error code: [ErrorCode] Error: [ErrorMessage]
235	DriveLock	Error	SSL: Cannot set up	The encrypted communications layer (SSL) could not be set up. Error: [ErrorMessage]
236	DriveLock	Error	Remote control: Cannot set up server	The remote control server component could not be set up. Agent remote control will be unavailable. Error: [ErrorMessage]
237	DriveLock	Error	Remote control: Internal error	Agent remote control: An internal SOAP communications error occurred. Error: [ErrorMessage]
238	DriveLock	SuccessAudit	Remote control: Function called	An Agent remote control function was called. Calling IP address: [IPAddress] Called function: [FunctionName]
239	DriveLock	SuccessAudit	Remote control: HTTP-GET	A HTTP-GET request was sent to the Agent.



Event ID	Source	Severity	Short text	Long text
			request	Requesting IP address: [IPAddress] Requested URL: [URL]
240	DriveLock	Warning	GPO: Cannot cache locally	A {Product} group policy configuration database could no be cached locally. GPO Object GUID: [ObjectID] GPO Name: [GpoName] Database file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
241	DriveLock	Error	GPO: Cannot open and extract	A {Product} 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	Error	GPO: Fall-back configuration applied	A group policy configuration was detected but no settings could be retrieved from the configuration databases. {Product} will fall-back to a configuration where all removable drives are blocked.

Event ID	Source	Severity	Short text	Long text
243	DriveLock	Error	GPO: Cannot open database	A group policy configuration database could not be opened. Database file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
244	DriveLock	Error	GPO: Cannot access GPO	{Product} Agent cannot access Windows group policy configuration. Error code: [ErrorCode] Error: [ErrorMessage]
245	DriveLock	Information	GPO: Configuration applied	A group policy configuration was applied. GPO Object GUID: [ObjectID] GPO Name: [GpoName] GPO Linked from: [GpoLinkedFrom]
246	DriveLock	Error	Cannot store configuration status	The Agent cannot store the configuration status used by other {Product} components. Error code: [ErrorCode] Error: [ErrorMessage]
247	DriveLock	Error	Cannot initialize configuration store	{Product} Agent cannot initialize the configuration database stores.

Event ID	Source	Severity	Short text	Long text
248	DriveLock	Error	{PrefixES}: Queued file was deleted	A file queued for uploading to the {PrefixEnterpriseService} was deleted locally before it could be uploaded. File name: [FileName]
249	DriveLock	Error	Configuration file: Fall-back configuration applied	A configuration using configuration files was detected but no settings could be retrieved from a configuration database. {Product} will fall-back to a configuration where all removable drives are blocked.
250	DriveLock	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	Error	Configuration file: Cannot extract	A {Product} configuration file could no be extracted. Settings from this file will not be applied. Database file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
252	DriveLock	SuccessAudit	Usage policy accepted	Usage policy for drive [DriveLetter] was accepted by the user. Device Id: [HWVen-

Event ID	Source	Severity	Short text	Long text
				dorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
253	DriveLock	FailureAudit	Usage policy declined	Usage policy for drive [DriveLetter] was declined by the user. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
254	DriveLock	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	Information	Deferred hash completed	Deferred content hash generation completed. File path: [Path] File name: [FileName] Drive: [DriveLetter] File name hash: [MD5Hash] File content hash: [MD5Hash] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])

Event ID	Source	Severity	Short text	Long text
				alNumber])
256	DriveLock	Information	File content changed	File content changed. File path: [Path] File name: [FileName] Drive: [DriveLetter] 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	SuccessAudit	File deleted	File deleted. Process: [ProcessName] File path: [Path] File name: [FileName] Drive: [DriveLetter] File name hash: [MD5Hash] File content hash: [MD5Hash] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
258	DriveLock	SuccessAudit	File renamed	File renamed. Process: [ProcessName] Old file path: [Path] Old file name: [FileName] New file name: [FileName] Old file name

Event ID	Source	Severity	Short text	Long text
				hash: [MD5Hash] File content hash: [MD5Hash] New file name hash: [MD5Hash] Drive: [DriveLetter] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
259	DriveLock	Information	FIPS mode enabled	{Product} uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1051) running on a Windows platform per FIPS 140-2 Implementation Guidance section G.5 guidelines. FIPS mode was successfully enabled.
260	DriveLock	Error	FIPS mode activation failed	{Product} encryption: FIPS mode could not be activated due to error [ErrorMessage]
261	DriveLock	Error	Cannot start driver	Cannot start the device driver [Driver-Name]. {Product} may not function correctly. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
262	DriveLock	Error	ALF driver communication error	An error occurred while communicating with the Application Launch Filter device driver. Error code: [ErrorCode] Error: [ErrorMessage]
263	DriveLock	Error	Error determining process details	An error occurred while determining detailed information for a process. Process: [ProcessName] File Hash: [ProcessHash]
264	DriveLock	Error	Cannot merge GPO into RSoP	Cannot merge the GPO configuration database [FileName] into the resulting set of policy.
265	DriveLock	Error	Cannot merge Registry into RSoP	Cannot merge GPO registry information into the resulting set of policy.
266	DriveLock	Error	Cannot start encryption driver	Cannot open or start the encryption device driver. Error code: [ErrorCode] Error: [ErrorMessage]
267	DriveLock	Error	Cannot install encryption	Cannot install the encryption device driver.

Event ID	Source	Severity	Short text	Long text
			driver	Function: [Function] Error code: [ErrorCode] Error: [ErrorMessage]
268	DriveLock	Error	Cannot upgrade Mobile Encryption Application	Mobile Encryption Application cannot be automatically updated. Target location: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
269	DriveLock	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	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	SuccessAudit	CD/DVD write operation started	A CD/DVD write operation was started on drive [DriveLetter]. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRe-



Event ID	Source	Severity	Short text	Long text
				visionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName]
272	DriveLock	FailureAudit	CD/DVD write operation blocked	A CD/DVD write operation was blocked on drive [DriveLetter]. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Process: [ProcessName]
273	DriveLock	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]
274	DriveLock	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

Event ID	Source	Severity	Short text	Long text
				[HWSerialNumber]) Process: [ProcessName]
275	DriveLock	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]
276	DriveLock	Information	System verification successful	A system verification operation on drive [DriveLetter] was executed and succeeded. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Status: [ActionResult]
277	DriveLock	Error	System verification failed	A system verification operation on drive [DriveLetter] was executed and reported a problem. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRe-

Event ID	Source	Severity	Short text	Long text
				visionNumber]) (Serial number [HWSerialNumber]) Status: [ActionResult]
278	DriveLock	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	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	Error	Cannot load file filter DLL	Cannot load a configured file filtering dynamic link library (DLL). DLL file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
281	DriveLock	Error	Cannot find function in DLL	Cannot find the configured function [FunctionName] in a filtering dynamic link lib-

Event ID	Source	Severity	Short text	Long text
				rary (DLL). DLL file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
282	DriveLock	Audit	Temporarily unlocked (off-line)	{Product} Agent was temporarily unlocked using offline unlocking. Unlock period: [UnlockTime] [UnlockUnit]
283	DriveLock	Information	Drive connected to thin client	The drive [DriveLetter] (mounted as [FileName]) was added to thin client [DisplayName] (unique ID [ComputerGuid]). Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
284	DriveLock	Information	Drive disconnected from thin client	The drive [DriveLetter] (mounted as [FileName]) was disconnected from thin client [DisplayName] (unique ID [ComputerGuid]). Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])

Event ID	Source	Severity	Short text	Long text
285	DriveLock	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	Error	No server defined for recovery	No server is defined for uploading encryption recovery information.
287	DriveLock	Error	No server defined for inventory	No server is defined for uploading collected inventory data.
288	DriveLock	Information	Inventory collection successful	Hard- and software inventory data was successfully collected and uploaded. DES server: [DesName] Connection ID: [ObjectID]
289	DriveLock	Information	Inventory collection failed	An error occurred while collecting hard- and software inventory data. DES server: [DesName] Connection ID: [ObjectID] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
290	DriveLock	Warning	Uninstallation password configured	An uninstallation password is configured. Please refer to the {Product} manual if you want to update this Agent.
291	DriveLock	Error	Cannot start mDNS/DNS-SD responder	The {Product} mDNS/DNS-SD responder could not be started. Zero-configuration functions will not be available Error code: [ErrorCode] Error: [ErrorMessage]
292	DriveLock	Error	DNS-SD service registration failed	DNS-SD service registration of the {Product} Agent failed.
293	DriveLock	Information	Security awareness campaign element acknowledged	A security awareness campaign element was acknowledged by the user. Campaign element: [ObjectID] Element description: [DisplayName]
294	DriveLock	Error	Cannot download centrally stored policy	The centrally stored policy [ConfigId] could not be downloaded. Server: [ServerName] Error: [ErrorMessage]
295	DriveLock	Error	Centrally stored policy: Can-	A centrally stored policy could no be extrac-

Event ID	Source	Severity	Short text	Long text
			not extract	ted. Settings from this file will not be applied. Configuration ID: [ConfigId] Error code: [ErrorCode] Error: [ErrorMessage]
296	DriveLock	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	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. {Product} will fall-back to a configuration where all removable drives are blocked.
298	DriveLock	Information	Centrally stored policy applied	The centrally stored policy [ConfigId] was successfully applied.
299	DriveLock	Information	Centrally stored policy downloaded	The centrally stored policy [DisplayName] was successfully downloaded. Configuration ID: [ConfigId] Version: [InstalledVersion]

Event ID	Source	Severity	Short text	Long text
300	DriveLock	Information	iTunes-synchronized device connected	An iTunes-synchronized device has been connected. HardwareID: [HardwareID] Device: [DisplayName] Serial: [Serial] IMEI: [IMEI] Firmware: [FirmwareVersion]
301	DriveLock	Information	iTunes-synchronized device disconnected	An iTunes-synchronized device has been disconnected. HardwareID: [HardwareID] Device: [DisplayName] Serial: [Serial] IMEI: [IMEI] Firmware: [FirmwareVersion]
302	DriveLock	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	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] Syn-



Event ID	Source	Severity	Short text	Long text
				cType: [SyncType]
304	DriveLock	Information	Calendar synchronization (iTunes-synchronized device)	Calendar synchronized with iTunes-synchronized device. Process: [ProcessName] Device: [DisplayName] Rule: [ObjectID] Blocked: [UserLockState] Filename: iDevice://[FileName] Hash: [MD5Hash] SyncType: [SyncType]
305	DriveLock	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	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	Severity	Short text	Long text
307	DriveLock	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	Error	Apple driver communication error	An error occurred while communicating with the Apple filter device driver. Error code: [ErrorCode] Error: [ErrorMessage]
309	DriveLock	Error	Cannot initialize apple filter device driver	Apple filter device driver could not be initialized. Error code: [ErrorCode] Error: [ErrorMessage]
310	DriveLock	Error	Antivirus installation failed	Installation of Antivirus failed. Error code: [ErrorCode] Error: [ErrorMessage]
311	DriveLock	Error	Initial Antivirus configuration failed	Initial configuration of Antivirus failed. Service: [ServiceName] ([FunctionName]) Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
312	DriveLock	Error	Antivirus uninstallation failed	Uninstallation of Antivirus failed. Error code: [ErrorCode] Error: [ErrorMessage]
313	DriveLock	Error	Antivirus initialization failed	Initialization of Antivirus failed. Error code: [ErrorCode] Error: [ErrorMessage]
314	DriveLock	Error	Antivirus configuration failed	Configuration of Antivirus failed. Setting: [FunctionName] Error code: [ErrorCode] Error: [ErrorMessage]
315	DriveLock	Error	Antivirus quarantine initialization failed	Initialization of Antivirus quarantine failed. Error code: [ErrorCode] Error: [ErrorMessage]
316	DriveLock	FailureAudit	Malware detected	Virus or malware detected. Detected malware: [DetectionName] ([DetectionType]) Scan result: [ScanResult] Detection accuracy: [DetectionAccuracy] Infected file: [Path][ArchivePath] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Drive letter: [DriveLet-

Event ID	Source	Severity	Short text	Long text
				ter] File name: [FileName] File name hash: [MD5Hash]
317	DriveLock	Error	AV Definition: Copying failed	Copying antivirus definitions from an UNC path failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
318	DriveLock	Error	AV Definition: Verification failed	Verification of antivirus definitions failed. Definition file: [FileName]
319	DriveLock	Error	AV Definition: Reading/extracting failed	Reading and extracting antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
320	DriveLock	Error	AV Definition: Activating failed	Activating antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
321	DriveLock	Error	AV Definition: Caching failed	Caching antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
322	DriveLock	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	Information	Antivirus definitions updated	Antivirus definitions updated. Definition file: [FileName]
324	DriveLock	Error	Quarantine: Deleting file failed	Deleting a file from antivirus quarantine failed. Quarantined file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
325	DriveLock	Information	Quarantined file deleted	A file was deleted from antivirus quarantine. Quarantined file: [FileName]
326	DriveLock	Error	Quarantine: Restoring file failed	Restoring a file from antivirus quarantine failed. Quarantined file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
327	DriveLock	Information	Quarantined file restored	A file was restored from antivirus quarantine. Quarantined file: [FileName]

Event ID	Source	Severity	Short text	Long text
328	DriveLock	Warning	Old antivirus definitions detected	Antivirus definitions are [AvDefAgeDays] days old. For continued protection please update antivirus definitions.
329	DriveLock	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. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Drive letter: [DriveLetter]
330	DriveLock	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]
331	DriveLock	Audit	Volume created (enforced encryption)	A {Product} encrypted volume was created/formatted by enforced encryption. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] File

Event ID	Source	Severity	Short text	Long text
				system: [FileSystemType] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
332	DriveLock	Warning	Volume mount error	Mounting of the encrypted volume [FileName] failed. Existing data will not be preserved. Volume GUID: [VolumeID]
333	DriveLock	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	Error	Server communication failed	Communication with the {PrefixEnterpriseService} failed. Server: [Server-Name] Error: [ErrorMessage]
335	DriveLock	Error	AV Definition: Download failed	Downloading antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage] Additional information: [ErrorMessage2]

Event ID	Source	Severity	Short text	Long text
336	DriveLock	Error	AV Definition: Merging incremental definitions failed	Merging incremental antivirus definitions failed. Definition file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage]
337	DriveLock	Information	AV Definition: Incremental definitions successfully merged	Incremental antivirus definitions successfully merged. Definition file: [FileName]
338	DriveLock	Warning	License expired. Grace period active	Your subscription license is expired. You will receive free updates and definitions until [LicenseInfo]
339	DriveLock	Error	License expired	Your subscription license expired on [LicenseInfo]
340	DriveLock	Error	Scheduled job: Load failed	Loading scheduled antivirus scan job failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
341	DriveLock	Error	Scheduled job: Execution failed	Executing a scheduled antivirus scan job failed. Job ID: [ConfigId] Job description:



Event ID	Source	Severity	Short text	Long text
				[DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
342	DriveLock	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	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]
344	DriveLock	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	Warning	Scheduled job: Not executed due to manual recon-	A scheduled antivirus scan was not executed due to manual reconfiguration.

Event ID	Source	Severity	Short text	Long text
			figuration	Job ID: [ConfigId] Job description: [DisplayName]
346	DriveLock	Warning	AV Definition: No updates due to manual reconfiguration	Antivirus definitions will not be updated due to manual reconfiguration.
347	DriveLock	Warning	Uninstall due to manual reconfiguration	Antivirus will be uninstalled due to manual reconfiguration.
348	DriveLock	Information	Install due to manual reconfiguration	Antivirus will be installed due to manual reconfiguration.
349	DriveLock	Error	Existing product un-installation failed	An existing antivirus product was detected but the configured automatic un-installation failed. Detected product: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
350	DriveLock	Error	Cannot load existing product update engine	The engine for updating existing antivirus products could not be loaded. Error code: [DisplayName] Error: [ErrorCode]

Event ID	Source	Severity	Short text	Long text
351	DriveLock	Information	Existing product uninstalled	An existing antivirus product was detected and uninstalled. Detected product: [DisplayName]
352	DriveLock	Information	Existing product detected	An existing antivirus product was detected. Detected product: [DisplayName]
353	DriveLock	Information	Antivirus scan successfull	An antivirus scan on drive [DriveLetter] was executed and succeeded. Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Status: [ActionResult]
354	DriveLock	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]
355	DriveLock	Warning	Realtime virus scanning temporarily disabled	Realtime virus scanning was temporarily disabled by administrative intervention.

Event ID	Source	Severity	Short text	Long text
356	DriveLock	Error	{FDE} installation error	Installation of the {DiskProtection} package failed. Error code: [ErrorCode] Error: [ErrorMessage]
357	DriveLock	Error	{FDE} uninstallation error	Uninstallation of the {DiskProtection} package failed. Error code: [UserName] Error: [ErrorCode]
358	DriveLock	Information	{FDE} configuration change delayed	A change in the {DiskProtection} configuration was detected, but the change is not applied due to the 'delay decryption' setting in the policy.
359	DriveLock	Warning	FDE: Manual reconfiguration	{DiskProtection} is manually reconfigured.
360	DriveLock	Warning	{FDE} integration module error	The {DiskProtection} integration module could not be loaded. Error code: [ErrorCode] Error: [ErrorMessage]
361	DriveLock	Error	Automatic updates: Load failed	Loading the automatic updates job schedule failed. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
362	DriveLock	Error	Automatic updates: Retrieving data failed	Retrieving automatic update information from server [ServerName] failed. Package type: [ServiceName] Error: [ErrorMessage]
363	DriveLock	Error	Automatic updates: Download failed	Downloading automatic updates failed. Package file: [URL] Error code: [ErrorCode] Error: [ErrorMessage]
364	DriveLock	Error	Automatic updates: Execution failed	Executing an automatic update failed. Package type: [ServiceName] Version: [InstalledVersion] Action: [ActionName] Error code: [ErrorCode] Error: [ErrorMessage]
365	DriveLock	Information	Automatic updates: Execution started	Execution of an automatic update started. Package type: [ServiceName] Version: [InstalledVersion]
366	DriveLock	Error	{FDE} Remote wipe request failed	A {DiskProtection} remote wipe request was received but could not be executed Error code: [ErrorCode] Error: [ErrorMessage]

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

Event ID	Source	Severity	Short text	Long text
370	DriveLock	Audit	Network resource not locked, error	The network resource [NetDrivePath] ([NetDriveType]) will be controlled by {Product}. As an ACL was applied to the drive, some users may no longer be able to access it. The drive is [UserLockState] for this event's user account. Applied whitelist rule: [ObjectID] Screen state (keyboard [Win]-[L]): [SessionLockState]
371	DriveLock	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 direction: [AccessDirection] Process: [ProcessName]
372	DriveLock	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 dir-

Event ID	Source	Severity	Short text	Long text
				action: [AccessDirection] Process: [ProcessName]
373	DriveLock	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 name hash: [MD5Hash] File content hash: [MD5Hash] Access direction: [AccessDirection] Process: [ProcessName]
374	DriveLock	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	Audit	File deleted	File deleted. Process: [ProcessName] File path: [Path] File name: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) File name hash: [MD5Hash] File content



Event ID	Source	Severity	Short text	Long text
				hash: [MD5Hash]
376	DriveLock	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	SuccessAudit	Usage policy accepted	Usage policy for network resource [NetDrivePath] ([NetDriveType]) was accepted by the user.
378	DriveLock	FailureAudit	Usage policy declined	Usage policy for network resource [NetDrivePath] ([NetDriveType]) was declined by the user.
379	DriveLock	Information	System verification successful	A system verification operation on network resource [NetDrivePath] ([NetDriveType]) was executed and succeeded. Status: [ActionResult]

Event ID	Source	Severity	Short text	Long text
380	DriveLock	Error	System verification failed	A system verification operation on network resource [NetDrivePath] ([NetDriveType]) was executed and reported a problem. Status: [ActionResult]
381	DriveLock	Information	Antivirus scan successful	An antivirus scan on drive [NetDrivePath] ([NetDriveType]) was executed and succeeded. Status: [ActionResult]
382	DriveLock	Error	Antivirus scan failed	An antivirus scan on drive [NetDrivePath] ([NetDriveType]) was executed and reported a problem. Device Id: [NetDriveType] [ActionResult] (Rev. []) (Serial number []) Status: []
383	DriveLock	FailureAudit	Malware detected	Virus or malware detected. Detected malware: [DetectionName] ([DetectionType]) Detection accuracy: [DetectionAccuracy] Infected file: [Path][ArchivePath] Network resource: ([NetDriveType]) [NetDrivePath] File name: [FileName] File name hash: [MD5Hash]

Event ID	Source	Severity	Short text	Long text
384	DriveLock	Information	Deferred hash completed	Deferred content hash generation completed. File path: [Path] File name: [FileName][FileName]etwork resource: [NetDrivePath] ([NetDriveType]) File name hash: [MD5Hash] File content hash: [MD5Hash]
385	DriveLock	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]
386	DriveLock	Audit	Volume mounted	A {Product} encrypted volume was mounted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Drive letter: [DriveLetter] Network resource: [NetDrivePath] ([NetDriveType])
387	DriveLock	Audit	Volume unmounted	A {Product} encrypted volume was

Event ID	Source	Severity	Short text	Long text
				unmounted. Status: [CryptStatus] Volume container: [DriveLetter] Volume GUID: [VolumeID] Drive letter: [FileName] Network resource: [NetDrivePath] ([NetDriveType])
388	DriveLock	Audit	Volume created	A {Product} encrypted volume was created/formatted. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] File system: [FileSystemType] Network resource: [NetDrivePath] ([NetDriveType])
389	DriveLock	Audit	Password changed	The password for a {Product} encrypted volume was changed. Status: [CryptStatus] Volume container: [FileName] Volume GUID: [VolumeID] Network resource: [NetDrivePath] ([NetDriveType])
390	DriveLock	Warning	Encrypted volume password recovered	A {Product} Encrypted volume password was recovered. Status: [CryptStatus] Volume container: [FileName] Volume

Event ID	Source	Severity	Short text	Long text
				GUID: [VolumeID] Network resource: [NetDrivePath] ([NetDriveType])
391	DriveLock	Warning	Cannot send event by e-mail	{Product} cannot send an event to a defined e-mail target. Error: [ErrorMessage]
392	DriveLock	Warning	Internal event queue full	The internal event queue was full. [EventCount] events were dropped during the last [IntValue] msec.
393	DriveLock	Warning	External event queue full	The external event queue was full. [EventCount] events were dropped since [UnlockTime]
394	DriveLock	Audit	File securely deleted	A file was securely deleted. File: [FileName] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])
395	DriveLock	Warning	File securely deleted	A file was securely deleted. File: [FileName] Network resource: [NetDrivePath]

Event ID	Source	Severity	Short text	Long text
				([NetDriveType]
396	DriveLock	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]
397	DriveLock	Error	Event data encryption failed	Error while encrypting event data. Event data will be anonymized. Error code: [ErrorCode] Error: [ErrorMessage]
398	DriveLock	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	Warning	Secure deletion failed	Secure deletion of a file failed. File: [FileName] Network resource: [NetDrivePath] ([NetDriveType]) Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
400	DriveLock	Information	Required encryption cancelled	Required encryption of a drive was cancelled by the user.
401	DriveLock	Information	Required encryption rule selected	A rule for enforced / required encryption was selected by the user. Rule ID: [ConfigId] Rule name: [DisplayName]
402	DriveLock	Audit	User password removed	The user password for a {Product} 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	Audit	User password removed	The user password for a {Product} encrypted volume was removed. The administrative password is needed to access the volume. Status: [CryptStatus] Volume container: [FileName] Volume GUID:

Event ID	Source	Severity	Short text	Long text
				[VolumeID] Network resource: [NetDrivePath] ([NetDriveType])
404	DriveLock	Audit	User password removed	The administrative password for a {Product} 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	Audit	User password removed	The administrative password for a {Product} 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	Information	Encrypted folder created	An encrypted folder was successfully cre-



Event ID	Source	Severity	Short text	Long text
				ated. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Initial user ID: [UserID]
407	DriveLock	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	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	Severity	Short text	Long text
409	DriveLock	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	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	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 [HWSerialNumber]) Recovered user ID: [UserID]

Event ID	Source	Severity	Short text	Long text
				Error code: [ErrorCode] Error: [ErrorMessage]
412	DriveLock	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	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: [ErrorCode] Error: [ErrorMessage]
414	DriveLock	Information	User successfully authenticated	An user was successfully authenticated against an encrypted folder. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device

Event ID	Source	Severity	Short text	Long text
				Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Permissions: [DfpUserPerms] [DfpReadOnlyPerms]
415	DriveLock	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]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Added user ID: [UserID] Permissions: [DfpUserPerms] [DfpReadOnlyPerms]
416	DriveLock	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:

Event ID	Source	Severity	Short text	Long text
				[UserID] Deleted user ID: [UserID]
417	DriveLock	Error	Authentication against encrypted folder failed	Authentication against 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] Authentication type: [DfpAuthTypes]
418	DriveLock	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] - [DfpJobDirection]
419	DriveLock	Information	Offline encryption com-	An offline encryption operation was suc-

Event ID	Source	Severity	Short text	Long text
			pleted	cessfully completed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Number of processed files: [IntValue]
420	DriveLock	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: [IntValue2]
421	DriveLock	Error	Offline encryption: File error	A file in an offline encryption operation could not be processed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device Id: [HWVendorID] [HWProductID] (Rev.

Event ID	Source	Severity	Short text	Long text
				[HWRevisionNumber]) (Serial number [HWSerialNumber]) Job ID: [DfpJobID] Processed file: [FileName] Error code: [ErrorCode] Error: [ErrorMessage] User action: [DfpUserAction]
422	DriveLock	Information	User certificate requested	An user certificate was requested. Requesting user: [UserID] Certificate serial number: [CertSerNo]
423	DriveLock	Information	User certificate issued	An user certificate was issued. Requesting user: [UserID] Certificate serial number: [CertSerNo]
424	DriveLock	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: [ErrorMessage2]
425	DriveLock	Error	User certificate issued	An error occurred while calling a {FileProtection} web service. Server URL: [URL]

Event ID	Source	Severity	Short text	Long text
				Server error: [ErrorMessage] Error code: [ErrorCode] Error: [ErrorMessage2]
426	DriveLock	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	Information	Encrypted folder recovered	An encrypted folder was successfully recovered. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Recovered user ID: [UserID]
428	DriveLock	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	Information	Encrypted folder unmoun-	An encrypted folder was successfully



Event ID	Source	Severity	Short text	Long text
			ted	unmounted. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID]
430	DriveLock	Error	Creation of an encrypted folder failed	Creation of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Initial user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
431	DriveLock	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	Error	Mount of an encrypted folder failed	Mount of an encrypted folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath]

Event ID	Source	Severity	Short text	Long text
				([NetDriveType]) Authenticated user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
433	DriveLock	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	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	Information	User successfully added	An user was successfully added to the encrypted folder users. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath]

Event ID	Source	Severity	Short text	Long text
				([NetDriveType]) Authenticated user ID: [UserID] Added user ID: [UserID] Permissions: [DfpUserPerms] [DfpReadOnlyPerms]
436	DriveLock	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	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 type: [DfpAuthTypes]
438	DriveLock	Information	Offline encryption started	An offline encryption operation was started for an encrypted folder. Folder path:

Event ID	Source	Severity	Short text	Long text
				[UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Authenticated user ID: [UserID] Job ID: [DfpJobID] Job type: [DfpJobType] - [DfpJobDirection]
439	DriveLock	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] Number of processed files: [IntValue]
440	DriveLock	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]

Event ID	Source	Severity	Short text	Long text
441	DriveLock	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: [FileName] Error code: [ErrorCode] Error: [ErrorMessage] User action: [DfpUserAction]
442	DriveLock	Error	Initialization error	{FileProtection} could not be initialized on this computer. Error code: [URL] Error: [ErrorCode]
443	DriveLock	Error	Component start error	A {Product} system component could not be started on this computer. Error code: [ErrorCode] Error: [ErrorMessage] Component ID: [IntValue]
444	DriveLock	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	Severity	Short text	Long text
445	DriveLock	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] [DfpReadOnlyPerms]
446	DriveLock	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	Information	Encrypted folder password changed	An encrypted folder users password was successfully changed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Device

Event ID	Source	Severity	Short text	Long text
				Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Changed user ID: [UserID] Changed by user ID: [UserID]
448	DriveLock	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	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: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
450	DriveLock	Error	Password change in an	Changing a password in an encrypted

Event ID	Source	Severity	Short text	Long text
			encrypted folder failed	folder failed. Folder path: [UncPath] Folder ID: [DfpVolumeID] Network resource: [NetDrivePath] ([NetDriveType]) Changed user ID: [UserID] Error code: [ErrorCode] Error: [ErrorMessage]
451	DriveLock	Error	No or wrong enforced encryption settings	A drive is configured for enforced encryption using {FileProtection} but enforced encryption settings are not present. The drive will be blocked and no encryption is executed.
452	DriveLock	Warning	Wrong application hash database hash algorithm	The application hash database [FileName] uses an other hash algorithm than configured globally for application filtering. Applications in this database will not be detected. Whitelist rule: [ObjectID]
453	DriveLock	Information	Installation successful, uninstalling update service	The Agent Update service will be uninstalled as it detected a successful installation.



Event ID	Source	Severity	Short text	Long text
454	DriveLock	Information	Update service started	The Agent Update service was started.
455	DriveLock	Information	Update service stopped	The Agent Update service was stopped.
456	DriveLock	Error	No server connection detected	The Agent Update service was unable to find a {PrefixEnterpriseService}. Installation and updates will not take place as expected.
457	DriveLock	Information	Missing service was registered	The Agent Update service successfully registered a missing Agent service.
458	DriveLock	Error	Error registering missing service	The Agent Update service was not able to register a missing Agent service.
459	DriveLock	Warning	Removed corrupted Agent installation	The Agent Update service has removed a corrupted Agent installation.
460	DriveLock	Warning	Agent installation started	The Agent Update service started installing the Agent.
461	DriveLock	Warning	Agent installation successful	The Agent Update service successfully

Event ID	Source	Severity	Short text	Long text
				installed the Agent.
462	DriveLock	Error	Error starting process	Error while starting Agent registration process. Error code: [ErrorCode] Error: [ErrorMessage]
463	DriveLock	Error	Error starting update service	Error while starting Agent update service. Error code: [ErrorCode] Error: [ErrorMessage]
464	DriveLock	Error	Error installing agent	Error while installing the Agent. Package file: [FileName] Installation log: [LogFile] Error code: [ErrorCode] Error: [ErrorMessage]
465	DriveLock	Information	Windows Firewall status change	Client compliance status changed for Windows Firewall. Firewall enabled: [ComponentEnabled]
466	DriveLock	Information	Script status change	Client compliance status changed for script [ComplianceName]. Status: [ComplianceValue]

Event ID	Source	Severity	Short text	Long text
467	DriveLock	Information	Windows Update status change	Client compliance status changed for Windows Update. Updates enabled: [ComponentEnabled] Available updates: [AvblUpdates] Last successful update: [LastSuccessUpdate]
468	DriveLock	Information	WSC Firewall status change	Client compliance status changed for Windows Security Center - Firewall. Is installed: [ComponentInstalled] Is enabled: [ComponentEnabled] Is up-to-date: [ComponentUptodate]
469	DriveLock	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	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: [Com-

Event ID	Source	Severity	Short text	Long text
				ponentUptodate]
471	DriveLock	Warning	Remote control declined	The user declined remote control access.
472	DriveLock	Information	Remote control accepted	The user accepted remote control access.
473	DriveLock	Audit	Process blocked	The execution of a process was blocked by company policy. Process: [ProcessName] File Hash: [ProcessHash] Applied whitelist rule: [ObjectID] Whitelist rule type: [WIType] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [VerProduct] Parent Process: [ProcessName] ([ProcessGuid])
474	DriveLock	Audit	Process started	A process was started. Process: [ProcessName] File Hash: [ProcessHash]

Event ID	Source	Severity	Short text	Long text
				Applied whitelist rule: [ObjectID] Whitelist rule type: [WType] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [VerProduct] Unique Process ID: [ProcessGuid] Parent Process: [ProcessName] ([ProcessGuid])
475	DriveLock	Information	PBA activated	Pre-boot authentication was successfully activated.
476	DriveLock	Information	PBA deactivated	Pre-boot authentication was successfully deactivated.
477	DriveLock	Information	EFS created	Embedded file system (EFS) was successfully created in the SECURDSK folder.
478	DriveLock	Error	PBA activation failed	Pre-boot authentication could not be activ-

Event ID	Source	Severity	Short text	Long text
				ated. EFS file: [FileName] Error: [ErrorMessage]
479	DriveLock	Error	PBA deactivation failed	Pre-boot authentication could not be deactivated. EFS file: [FileName] Error: [ErrorMessage]
480	DriveLock	Error	EFS creation failed	Embedded file system (EFS) could not be created. EFS file: [FileName] Error: [ErrorMessage]
481	DriveLock	Error	Exception occurred	An exception occurred in a {DiskProtection} component. Error: [ErrorMessage]
482	DriveLock	Information	Encryption configuration changed	Encryption configuration has changed. Drive: [DriveLetter] Algorithm: [EncryptionAlgorithm]
483	DriveLock	Error	Invalid XML configuration	An invalid XML configuration was detected. XML path: [FileName]
484	DriveLock	Information	XML configuration imported	A XML configuration was successfully

Event ID	Source	Severity	Short text	Long text
				imported. XML path: [FileName] Imported data: [ActionName]
485	DriveLock	Error	BitLocker-encrypted drive detected	The drive [DriveLetter] is encrypted with BitLocker drive encryption. It cannot be encrypted with {DiskProtection}.
486	DriveLock	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	Error	General error	A general error occurred in the {DiskProtection} Encryptor service. Error code: [ErrorCode] Error: [ErrorMessage]
488	DriveLock	Error	General error	A general error occurred in the {DiskProtection} Management service. Error code: [ErrorCode] Error: [ErrorMessage]
489	DriveLock	Audit	Cannot decrypt removable drive	The removable drive [DriveLetter] could not be unlocked / decrypted. Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
490	DriveLock	Error	Encryption interoperation failed	A storage encryption interoperation failed. Operation: [Function] Error code: [ErrorCode] Error: [ErrorMessage]
491	DriveLock	Error	User store operation failed	A user store operation failed. Store type: [StoreType] Operation: [Function] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
492	DriveLock	Error	Data store operation failed	A data store operation failed. Store type: [StoreType] Operation: [Function] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
493	DriveLock	Error	CD/DVD encryption failed	An error occurred while encrypting a CD/DVD-ROM using {DiskProtection}. Error code: [ErrorCode] Error: [ErrorMessage]
494	DriveLock	Error	Password complexity not met	The password for user "[UserName]" does not meet the password complexity requirements.



Event ID	Source	Severity	Short text	Long text
495	DriveLock	Information	{DiskProtection} information	{DiskProtection} information: [DebugMsg]
496	DriveLock	Audit	Removable drive decrypted	The removable drive [DriveLetter] was successfully unlocked / decrypted.
497	DriveLock	Information	Encryption completed	Encryption of drive [DriveLetter] was successfully completed.
498	DriveLock	Information	Decryption completed	Decryption of drive [DriveLetter] was successfully completed.
499	DriveLock	Information	Encryption started	Encryption of drive [DriveLetter] was started with algorithm [EncryptionAlgorithm]. [EncPercent] of the drive are already encrypted.
500	DriveLock	Information	Decryption started	Decryption of drive [DriveLetter] was started. [EncPercent] of the drive are already encrypted.
501	DriveLock	Information	Disk error during encryption	A disk error occurred while en-/decrypting sector [SectorNo] on drive [DriveLetter].

Event ID	Source	Severity	Short text	Long text
				The disk may be defective.
502	DriveLock	Audit	Successful pre-boot authentication	Successful pre-boot authentication. Logon type: [LogonType] User: [UserName] Logon time: [LogonTime]
503	DriveLock	Audit	Successful emergency pre-boot authentication	Successful emergency pre-boot authentication. Logon type: [LogonType] User: [UserName] Logon time: [LogonTime]
504	DriveLock	Audit	Failed pre-boot authentication	Failed pre-boot authentication. Logon type: [LogonType] User: [UserName] Logon time: [LogonTime]
505	DriveLock	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	Information	{FDE} encryptor service started	The {DiskProtection} encryptor service was started.
507	DriveLock	Information	{FDE} encryptor service	The {DiskProtection} encryptor service was

Event ID	Source	Severity	Short text	Long text
			stopped	stopped.
508	DriveLock	Information	{FDE} management service started	The {DiskProtection} management service was started.
509	DriveLock	Information	{FDE} management service stopped	The {DiskProtection} management service was stopped.
510	DriveLock	Error	{DiskProtection} installation failed	An error occurred while installing {DiskProtection}. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
511	DriveLock	Error	{DiskProtection} un-installation failed	An error occurred while uninstalling {DiskProtection}. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
512	DriveLock	Error	{DiskProtection} upgrade failed	An error occurred while upgrading {DiskProtection}. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
513	DriveLock	Error	{DiskProtection} policy failed	An error occurred while applying {DiskProtection} policy. Step: [StepName] Error

Event ID	Source	Severity	Short text	Long text
				code: [ErrorCode] Error: [ErrorMessage]
514	DriveLock	Information	Disk check succeeded	Disk check (Chkdsk) on drive [DriveLetter] ([ObjectID]) succeeded.
515	DriveLock	Error	Disk check failed	Disk check (Chkdsk) on drive [DriveLetter] ([ObjectID]) failed. Error code: [ErrorCode] Error: [ErrorMessage]
516	DriveLock	Warning	{DiskProtection} 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	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]
518	DriveLock	Error	EFS file update failed	EFS file [FileName] could not be updated as part of company policy. Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
519	DriveLock	Error	Invalid disk configuration	{DiskProtection} installation is not possible on this computer. The disk / partition configuration does not allow installation ([DebugMsg]).
520	DriveLock	Error	All {PrefixES} not reachable	Cannot load company policy. All configured {PrefixEnterpriseService}s are not reachable.
521	DriveLock	Error	Cannot determine computer token	Cannot determine the computer token. Error code: [ErrorCode] Error: [ErrorMessage]
522	DriveLock	Error	Error loading policy assignments	An error occurred while loading policy assignments from server [ServerName]. Error: [ErrorMessage]
523	DriveLock	Error	Policy integrity check failed	The integrity of an assigned policy could not be verified. Policy ID: [ServerName] Policy name: [ErrorMessage] Actual hash: [] Expected hash: []

Event ID	Source	Severity	Short text	Long text
524	DriveLock	Audit	File accessed	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: [FileName]
525	DriveLock	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: [MD5Hash] File name: [FileName]
526	DriveLock	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]

Event ID	Source	Severity	Short text	Long text
				Access direction: [AccessDirection] File name hash: [MD5Hash] File content hash: [MD5Hash] File name: [FileName]
527	DriveLock	Audit	File extension blocked	File deleted. 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]
528	DriveLock	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	Audit	File renamed	File renamed. DeviceName: [DisplayName] HardwareId: [HardwareID] ClassGuid: [ClassID] Process: [ProcessName] File size: [Size] File path: [Path] Old file name hash:

Event ID	Source	Severity	Short text	Long text
				[MD5Hash] New file name: [FileName] New file name hash: [MD5Hash] File content hash: [MD5Hash] Old file name: [FileName]
530	DriveLock	Error	Actual licensing	Licensing is configured using ActiveDirectory objects. The actual licensing status is: Drive and device locking: [LicDLock] {DiskProtection}: [LicFde] {ContainerEncryption}: [LicDiv] {FileProtection}: [LicFfe] BitLocker Management: [LicBitLock] Application Control: [LicALF] Security Awareness Content: [LicAware] Legacy OS Support: [LicLegacy] DriveLock PBA: [LicPBA] Vulnerability Scanning: [LicVulScan] Microsoft Defender Integration: [LicDefender] Error-free detected: [LicSure]
531	DriveLock	Information	Scheduled job: Started	Scheduled antivirus scan job was started. Job ID: [ConfigId] Job description: [DisplayName]



Event ID	Source	Severity	Short text	Long text
532	DriveLock	Information	Scheduled job: Initiated shutdown	Scheduled antivirus scan job initiated system shutdown after execution. Job ID: [ConfigId] Job description: [DisplayName]
533	DriveLock	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	Warning	Policy wipe - Warning	The computer is offline for [DisplayName] days. The company policy will be wiped soon.
535	DriveLock	Error	Company policy wiped	The company policy was wiped because the computer was offline for a long period of time.
536	DriveLock	Information	Company policy in use again	The company policy is in use again after it was wiped because the computer was offline for a long period of time.
537	DriveLock	Error	URL categorizer failed	The URL categorizer returned an error while categorizing an URL. Error:

Event ID	Source	Severity	Short text	Long text
				[ErrorMessage]
538	DriveLock	Error	Network filter driver error	An error occurred while communicating with the network filtering driver. Error code: [ErrorCode] Error: [ErrorMessage]
539	DriveLock	Error	Network filter driver error	An error occurred while setting up network filtering. Error code: [ErrorCode] Error: [ErrorMessage]
540	DriveLock	SuccessAudit	Web ressource access granted (based on URL)	A web ressource was accessed. Access was granted based on the URL defined in company policy. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Rule description: [DisplayName] Rule unique ID: [ObjectID]
541	DriveLock	FailureAudit	Web ressource access blocked (based on URL)	A web ressource was accessed and blocked based on the URL defined in company policy. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Rule description: [DisplayName] Rule unique ID: [ObjectID]

Event ID	Source	Severity	Short text	Long text
542	DriveLock	SuccessAudit	Web ressource access granted (based on category)	A web ressource was accessed. Access was granted based on the URL category defined in company policy. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Categories: [UrlCategory1] [UrlCategory2] [UrlCategory3] [UrlCategory4] [UrlCategory5] Category group: [UrlCategoryGroup] Rule description: [DisplayName] Rule unique ID: [ObjectID]
543	DriveLock	FailureAudit	Web ressource access blocked (based on category)	A web ressource was accessed and blocked based on the URL category defined in company policy. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Categories: [UrlCategory1] [UrlCategory2] [UrlCategory3] [UrlCategory4] [UrlCategory5] Category group: [UrlCategoryGroup] Rule description: [DisplayName] Rule unique ID: [ObjectID]
544	DriveLock	SuccessAudit	Web ressource access granted (no explicit rule)	A web ressource was accessed. Access was granted based on company policy (no

Event ID	Source	Severity	Short text	Long text
				explicit rule exists). URL: [Address] ([UrlType]) Protocol: [UrlProtocol]
545	DriveLock	FailureAudit	Web ressource access blocked (no explicit rule)	A web ressource was accessed and blocked based on company policy (no explicit rule exists). URL: [Address] ([UrlType]) Protocol: [UrlProtocol]
546	DriveLock	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	Warning	Web Security temporarily disabled	Web Security was temporarily disabled by administrative intervention.
548	DriveLock	SuccessAudit	Web ressource access granted (URL categorization failed)	A web ressource was accessed. URL categorization failed but access was granted based on company policy. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Rule

Event ID	Source	Severity	Short text	Long text
				description: [DisplayName] Rule unique ID: [ObjectID]
549	DriveLock	FailureAudit	Web ressource access blocked (URL categorization failed)	A web ressource was accessed, URL categorization failed and then it was blocked based on company policy. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Rule description: [DisplayName] Rule unique ID: [ObjectID]
550	DriveLock	Information	PBA password change	User [UserName] (domain [DomainName]) changed the password in pre-boot authentication.
551	DriveLock	SuccessAudit	Usage policy accepted by authorized user	Usage policy for drive [DriveLetter] was accepted by authorized user [UserName]@[Domain]. Logged on user was [UserName]@[DomainName]
552	DriveLock	Information	Web ressource categorized	A web ressource was categorized. URL: [Address] ([UrlType]) Protocol: [UrlProtocol] Categories: [UrlCategory1] [UrlCat-

Event ID	Source	Severity	Short text	Long text
				egory2] [UrlCategory3] [UrlCategory4] [UrlCategory5] Category group: [UrlCategoryGroup]
553	DriveLock	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	Information	Picture taken	A picture was taken with camera [CameraName] for event ID [EventID] ([EventNumber]).
555	DriveLock	Information	Scheduled action: Started	Scheduled power action was started. Job ID: [ConfigId] Job description: [DisplayName]
556	DriveLock	Error	Scheduled action: Execution failed	Executing a scheduled power action failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
557	DriveLock	Information	Scheduled action: Successfully executed	Scheduled power action successfully executed. Job ID: [ConfigId] Job description: [DisplayName]
558	DriveLock	Error	Scheduled action: Load failed	Loading scheduled power action failed. Job ID: [ConfigId] Job description: [DisplayName] Error code: [ErrorCode] Error: [ErrorMessage]
559	DriveLock	Information	Power scheme changed	Computer power scheme successfully changed. Rule ID: [ConfigId] Rule name: [DisplayName] Power scheme: [FunctionName]
560	DriveLock	Error	Power scheme change failed	Changing computer power scheme failed. Rule ID: [ConfigId] Rule name: [DisplayName] Power scheme: [FunctionName] Error code: [ErrorCode] Error: [ErrorMessage]
561	DriveLock	Error	Drive larger 2 TB detected	The drive [DriveLetter] is larger than 2 TB. It cannot be encrypted with {DiskPro-

Event ID	Source	Severity	Short text	Long text
				tection}.
562	DriveLock	Warning	Antivirus error	An antivirus error occurred while scanning object [FileName]. Error: [ErrorMessage]
563	DriveLock	Information	Definition update started	Antivirus definition update was started from source [MethodName]
564	DriveLock	Error	Error starting definition update	Antivirus definition update could not be started from source [MethodName]. Error code: [ErrorCode] Error: [ErrorMessage]
565	DriveLock	Warning	Package download error	The [PackageType] package could not be downloaded from [URL] Error code: [ErrorCode] Error: [ErrorMessage]
566	DriveLock	Information	Package download successful	The [PackageType] package was successfully downloaded.
567	DriveLock	Warning	Package extraction error	The [PackageType] package could not be extracted. The file [PackagePath] may be missing or corrupt. Error code: [ErrorCode]



Event ID	Source	Severity	Short text	Long text
				Error: [ErrorMessage]
568	DriveLock	Warning	Package installation prevented	The [PackageType] package should be installed but the installation is prevented by administrative intervention.
569	DriveLock	Information	Package installation successful	[PackageType] was successfully installed.
570	DriveLock	Error	Package installation error	[PackageType] installation failed. Command line: [CmdLine] Error code: [ErrorCode] Error: [ErrorMessage]
571	DriveLock	Information	Package uninstallation successful	[PackageType] was successfully uninstalled.
572	DriveLock	Error	Package uninstallation error	[PackageType] uninstallation failed. Command line: [CmdLine] Error code: [ErrorCode] Error: [ErrorMessage]
573	DriveLock	Error	Incremental definition update failed	Incremental definition update failed to apply the patch package. Old definition

Event ID	Source	Severity	Short text	Long text
				file: [OldValue] New definition file: [NewValue] Error: [ErrorMessage]
574	DriveLock	Error	Definition update error	An error occurred while updating antivirus definitions. Error: [ErrorMessage]
575	DriveLock	Warning	Real-time scanning stopped	Real-time antivirus scanning was stopped.
576	DriveLock	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.
577	DriveLock	Information	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]

Event ID	Source	Severity	Short text	Long text
578	DriveLock	Information	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: [] Remote Audit activated: []
579	DriveLock	SuccessAudit	Network pre-boot authentication succeeded	The network pre-boot authentication succeeded.
580	DriveLock	Error	Network pre-boot authentication error	An error occurred during network pre-boot authentication. Error: [ErrorMessage]
581	DriveLock	Error	Network pre-boot authentication error	An error occurred during network pre-boot authentication. Error: [ErrorMessage] Parameter: [ErrorMessage2]
582	DriveLock	Error	Error retrieving custom computer name	An error occurred while retrieving the custom computer name. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
583	DriveLock	Error	Error with Active Directory inventory	An error occurred while generating Active Directory inventory. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
584	DriveLock	Information	Active Directory inventory started	Active Directory inventory generation was triggered by DES.
585	DriveLock	Information	Network pre-boot authentication disabled	Network pre-boot authentication was disabled.
586	DriveLock	Information	Network pre-boot authentication enabled	Network pre-boot authentication was enabled.
587	DriveLock	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	Error	Cannot load network pre-boot configuration	Cannot load network pre-boot configuration from embedded file system (EFS).

Event ID	Source	Severity	Short text	Long text
589	DriveLock	Error	Cannot write network pre-boot configuration	Cannot write network pre-boot configuration to embedded file system (EFS).
590	DriveLock	Error	Error installing network pre-boot authentication	An error occurred while installing the network pre-boot authentication. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
591	DriveLock	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	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	Information	Machine learning completed	Machine learning for local application whitelist was completed.
594	DriveLock	Error	Error during machine learn-	An error occurred during machine learn-

Event ID	Source	Severity	Short text	Long text
			ing	ing of the local application whitelist. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
595	DriveLock	Error	Error during machine learning	An error occurred during machine learning of executable file "[FileName]". Error code: [ErrorCode] Error: [ErrorMessage]
596	DriveLock	Information	Machine learning completed	Machine learning of executable file "[FileName]" completed. Reason: [AlfLearnReason]
597	DriveLock	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]
598	DriveLock	Information	Security awareness campaign presented	A security awareness campaign was presented to the user. Campaign: [ObjectID] Description: [DisplayName]
599	DriveLock	Information	Security awareness cam-	A security awareness campaign was com-

Event ID	Source	Severity	Short text	Long text
			paign completed	pleted by the user. Module: [ObjectID] Description: [DisplayName]
600	DriveLock	Information	Program start approved	Start of executable file [FileName] was approved by the user.
601	DriveLock	Error	Invalid policy signing certificate	The configured policy signing certificate cannot be read. Error code: [ErrorCode] Error: [ErrorMessage]
602	DriveLock	Information	Program start declined	Start of executable file [FileName] was declined by the user.
603	DriveLock	Information	Security awareness test failed	The user did not pass a security awareness test. Module: [ObjectID] Description: [DisplayName] Result: [ErrorCode]
604	DriveLock	Information	Security awareness test successful	A security awareness test was successfully completed by the user. Module: [ObjectID] Description: [DisplayName] Result: [ErrorCode]

Event ID	Source	Severity	Short text	Long text
605	DriveLock	Warning	Security awareness campaign cancelled	A security awareness campaign was cancelled by the user. Module: [ObjectID] Description: [DisplayName] Progress: [ErrorCode]
606	DriveLock	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	Error	Security awareness campaign: Retrieving data failed	Retrieving security awareness campaign content from server [ServerName] failed. Package type: [SecAwPackageType] Error: [ErrorMessage]
608	DriveLock	Error	Security awareness campaign: Download failed	Downloading security awareness campaign content failed. Package file download URL: [URL] Error code: [ErrorCode] Error: [ErrorMessage]
609	DriveLock	Error	BitLocker key backup failed	The BitLocker recovery key backup failed. Step: [StepName] Error code: [ErrorCode]



Event ID	Source	Severity	Short text	Long text
				Error: [ErrorMessage]
610	DriveLock	Warning	BitLocker cannot apply configuration	The BitLocker configuration could not be applied.
611	DriveLock	Warning	BitLocker not licensed	BitLocker is configured to encrypt local hard disks but is not licensed on this computer.
612	DriveLock	Information	BitLocker configuration change delayed	A change in the BitLocker configuration was detected, but the change is not applied due to the 'delay decryption' setting in the policy.
613	DriveLock	Warning	BitLocker manually reconfigured	BitLocker is manually reconfigured.
614	DriveLock	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]

Event ID	Source	Severity	Short text	Long text
615	DriveLock	Information	BitLocker encryption successful	BitLocker successfully encrypted hard disk: [DriveLetter]
616	DriveLock	Information	BitLocker decryption successful	BitLocker successfully decrypted local hard disk: [DriveLetter]
617	DriveLock	Error	BitLocker key backup creation failed	The BitLocker key backup creation failed.
618	DriveLock	Information	BitLocker encryption started	BitLocker started encrypting local hard disk: [DriveLetter]
619	DriveLock	Information	BitLocker decryption started	BitLocker started decrypting local hard disk: [DriveLetter]
620	DriveLock	Error	BitLocker system error	BitLocker Emergency Recovery Information could not be moved to [TargetFolder]. Error code: [ErrorCode] Error: [ErrorMessage]
621	DriveLock	Information	BitLocker login succeeded	BitLocker login succeeded.

Event ID	Source	Severity	Short text	Long text
622	DriveLock	Warning	BitLocker login failed	BitLocker login failed.
623	DriveLock	Warning	BitLocker password reset dialog cancelled	The BitLocker password reset dialog was cancelled.
624	DriveLock	Information	BitLocker password dialog finished	The BitLocker password dialog was finished.
625	DriveLock	Error	BitLocker encryption failed	The BitLocker encryption failed. Error: [ErrorMessage]
626	DriveLock	Information	BitLocker protectors applied	The BitLocker protectors [Protectors] were applied for drive: [DriveLetter]
627	DriveLock	Information	BitLocker encryption algorithm applied	The encryption algorithm [EncryptionAlgorithm] is used to encrypt drive: [DriveLetter]
628	DriveLock	Information	BitLocker recovery data upload	BitLocker recovery data was uploaded to the server.
629	DriveLock	Error	BitLocker recovery data	BitLocker recovery data upload failed.

Event ID	Source	Severity	Short text	Long text
			upload failed	Error: [ErrorMessage]
630	DriveLock	Warning	BitLocker not controlled by DriveLock detected	Drive [DriveLetter] is already encrypted with BitLocker but not controlled by DriveLock.
631	DriveLock	Warning	Locked drive detected	BitLocker: locked drive [DriveLetter] detected.
632	DriveLock	Information	BitLocker configuration succeeded	BitLocker configuration succeeded.
633	DriveLock	Information	BitLocker configuration failed	BitLocker configuration failed. Error: [ErrorMessage]
634	DriveLock	Information	BitLocker password set	BitLocker password was set by the user for drive: [DriveLetter]
635	DriveLock	Information	BitLocker password set failed	Setting BitLocker password failed for drive: [DriveLetter]. Error message: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
636	DriveLock	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	Information	BitLocker recovery key replaced	The recovery key of drive [DriveLetter] was recreated after recovery process.
638	DriveLock	Information	BitLocker internal message	BitLocker Management internal message: [DebugMsg]
639	DriveLock	Error	Server certificate error	Server certificate error detected. Certificate: [CertSubject]. Error message: [ErrorMessage]
640	DriveLock	Information	Security awareness campaign presented	The security awareness campaign ' [SecAwPackageDisplayName]' was presented to the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion]

Event ID	Source	Severity	Short text	Long text
641	DriveLock	Information	Security awareness campaign element acknowledged	The security awareness campaign element '[SecAwPackageDisplayName]' was acknowledged by the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion]
642	DriveLock	Information	Security awareness campaign completed	The security awareness campaign '[SecAwPackageDisplayName]' was completed by the user. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion]
643	DriveLock	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

Event ID	Source	Severity	Short text	Long text
644	DriveLock	Information	Security awareness test failed	The user did not pass the security awareness test '[SecAwPackageDisplayName]'. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version: [SecAwPackageVersion] Result: [SecAwResultScorePassed] passed / [SecAwResultScoreFailed] failed
645	DriveLock	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
646	DriveLock	Information	Security awareness campaign in progress	The security awareness campaign '[SecAwPackageDisplayName]' is in progress. Content type: [SecAwPackageContentType] Language: [SecAwPackageLanguage] Version:

Event ID	Source	Severity	Short text	Long text
				[SecAwPackageVersion] Current progress: [SecAwSessionProgress][SecAwSessionProgress]
647	DriveLock	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
648	DriveLock	Audit	DLL blocked	The loading of a DLL was blocked by company policy. Process: [ProcessName] ([ProcessGuid]) Applied whitelist rule: [ObjectID] Whitelist rule type: [WIType] DLL File Name: [ProcessName] DLL File Hash: [ProcessHash] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Cer-



Event ID	Source	Severity	Short text	Long text
				tificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [Ver-Product]
649	DriveLock	Audit	DLL loaded	A DLL was loaded. Process: [ProcessName] ([ProcessGuid]) Applied whitelist rule: [ObjectID] Whitelist rule type: [WType] DLL File Name: [ProcessName] DLL File Hash: [ProcessHash] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [Ver-Product]
650	DriveLock	Audit	File Access blocked	The Access to a File was blocked by company policy. Process: [ProcessName] ([ProcessGuid]) Applied whitelist rule: [ObjectID] Whitelist rule type: [WType] File Name: [FileName] AccessDirection:

Event ID	Source	Severity	Short text	Long text
				[AccessDirection]
651	DriveLock	Audit	File Access	A File was accessed. Process: [ProcessName] ([ProcessGuid]) Applied whitelist rule: [ObjectID] Whitelist rule type: [WType] File Name: [FileName] AccessDirection: [AccessDirection]
652	DriveLock	Audit	Registry Access blocked	The Access to the Registry was blocked by company policy. Process: [ProcessName] ([ProcessGuid]) Applied whitelist rule: [ObjectID] Whitelist rule type: [WType] Path: [FileName] AccessDirection: [AccessDirection]
653	DriveLock	Audit	Registry Access	The Registry was accessed. Process: [ProcessName] ([ProcessGuid]) Applied whitelist rule: [ObjectID] Whitelist rule type: [WType] Path: [RegistryPath] AccessDirection: [AccessDirection]
654	DriveLock	Audit	File Access approved	The Access to a File was approved by the

Event ID	Source	Severity	Short text	Long text
				user. Process: [ProcessName] ([ProcessGuid]) File Name: [FileName]
655	DriveLock	Audit	File Access denied	The Access to a File was denied by the user. Process: [ProcessName] ([ProcessGuid]) File Name: [FileName]
656	DriveLock	Audit	Registry Access approved	The Access to the Registry was approved by the user. Process: [ProcessName] ([ProcessGuid]) Path: [FileName]
657	DriveLock	Audit	Registry Access denied	The Access to the Registry was denied by the user. Process: [ProcessName] ([ProcessGuid]) Path: [RegistryPath]
660	DriveLock	Error	BitLocker is missing	BitLocker is missing
661	DriveLock	Error	BitLocker Management detected BIOS	BitLocker Management detected BIOS. DriveLock PBA is only supported on UEFI.
662	DriveLock	Error	BitLocker system drive not prepared	BitLocker Management: BitLocker doesn't seem to be prepared for the system drive:

Event ID	Source	Severity	Short text	Long text
				[DriveLetter]. The drive can be prepared using 'bdehdcfg.exe -target default -restart'
663	DriveLock	Information	{DiskProtection} recovery data upload	{DiskProtection} recovery data was uploaded to the server.
664	DriveLock	Error	{DiskProtection} recovery data upload failed	{DiskProtection} recovery data upload failed. Error: [ErrorMessage]
665	DriveLock	SuccessAudit	The DES transmitted authorization data to the PBA	The DES transmitted authorization data to the PBA.
666	DriveLock	Error	Invalid network PBA key registration	Recorded attempt to register the PBA network key a second time.
667	DriveLock	Error	Invalid network PBA authorization data registration	Recorded attempt to register the PBA authorization data a second time.
668	DriveLock	Error	Cannot decrypt message from network PBA	Cannot decrypt message from network PBA. Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
669	DriveLock	Error	Invalid network PBA message	An invalid message from the network PBA has been received. Error: [ErrorMessage]
670	DriveLock	FailureAudit	Computer not registered for network PBA	The server received an network PBA connect request for a not registered computer.
671	DriveLock	FailureAudit	No authorization data for network PBA	Unable to authorize network PBA because the computer has not registered authorization data.
672	DriveLock	Error	PBA network issues	The PBA has problems to connect to the network. Error: [ErrorMessage]
673	DriveLock	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]
674	DriveLock	Error	Invalid network PBA server response	The network PBA received an invalid server response. Error: [ErrorMessage]
675	DriveLock	Error	Network PBA authorization data decryption failed	The network PBA is unable to decrypt the authorization data. Error: [ErrorMessage]

Event ID	Source	Severity	Short text	Long text
676	DriveLock	Error	Network PBA cannot unlock disk	The network PBA is unable unlock the disk using the authorization data. Error: [ErrorMessage]. Details: [ErrorMessage2]
677	DriveLock	FailureAudit	Network PBA logon failed	Network PBA logon failed. User: [User-Name]
678	DriveLock	FailureAudit	Automatic logon via network PBA failed.	Automatic logon via network PBA failed.
679	DriveLock	Information	Machine learning started	Machine learning for local application whitelist was started.
680	DriveLock	Information	Application behavior recording started	Recording of application behavior was started.
681	DriveLock	Error	Configuration of Microsoft Defender failed	Error configuring Microsoft Defender. Error code: [ErrorCode]. Error: [ErrorMessage]
682	DriveLock	Information	Microsoft Defender configuration changes reverted	Detected Microsoft Defender configuration changes by a third party. The changes

Event ID	Source	Severity	Short text	Long text
				have been reverted. Details: [Details]
683	DriveLock	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	Warning	Microsoft Defender detected a threat	Microsoft Defender detected the threat [DetectionName] ([DetectionType]). Infected file: [Path] Drive letter: [DriveLetter] File name: [FileName] File name hash: [MD5Hash]
685	DriveLock	Warning	Microsoft Defender threat allowed	A user has allowed a threat detected by Microsoft Defender. Threat: [DetectionName] Category: [DetectionType]
686	DriveLock	Warning	Microsoft Defender threat restored from quarantine	A user has restored a quarantined threat detected by Microsoft Defender. Threat: [DetectionName] Category: [DetectionType]

Event ID	Source	Severity	Short text	Long text
687	DriveLock	Error	Microsoft Defender signature update failed	Unable to update Microsoft Defender signature definition. Details: [Details]
688	DriveLock	Audit	Encrypted volume connected	Encrypted volume [DriveLetter] was added to the system. It is encrypted with [EncryptionType]. Mobile Encryption Application: [FileVersion] Has unencrypted part: [UnencryptedPartPresent], size: [DataSize], permission: [UserLockState]
689	DriveLock	Audit	Application behavior control changed	Application behavior control for [ProcessName] changed: Execute: [LocalBehaviorExecute] DLL load: [LocalBehaviorDllLoad] Write Files: [LocalBehaviorFileWrite]
690	DriveLock	Information	Vulnerability scan successful	Vulnerability scan was successfully executed and results were uploaded. DES server: [DesName] Connection ID: [ObjectID]
691	DriveLock	Error	Vulnerability catalog not	Vulnerability scan could not be executed



Event ID	Source	Severity	Short text	Long text
			downloaded	because the vulnerabilities catalog was not yet downloaded from the server.
692	DriveLock	Error	Vulnerability scan failed	The vulnerability scanner failed scanning. Error: [ErrorMessage]
693	DriveLock	Error	Error starting vulnerability scan	Error while starting a vulnerability scan. Error code: [ErrorCode] Error: [ErrorMessage]
694	DriveLock	Error	Error downloading vulnerability catalog	Error while downloading the vulnerability catalog. Server: [ServerName] Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
695	DriveLock	Error	Error creating vulnerability scan result	Error while creating the vulnerability scan result. Step: [StepName] Error code: [ErrorCode] Error: [ErrorMessage]
696	DriveLock	Warning	Microsoft Defender detected a threat on a network resource	Microsoft Defender detected the threat [DetectionName] ([DetectionType]). Infected network file: [Path] Network resource:

Event ID	Source	Severity	Short text	Long text
				[NetDrivePath] ([NetDriveType]) File name: [FileName] File name hash: [MD5Hash]
697	DriveLock	Warning	Microsoft Defender detected a threat	Microsoft Defender detected the threat [DetectionName] ([DetectionType]). Infected file: [Path] Device Id: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber]) Drive letter: [DriveLetter] File name: [FileName] File name hash: [MD5Hash]
698	DriveLock	Error	Microsoft Defender is disabled	Microsoft Defender is disabled and cannot be enabled by DriveLock.
699	DriveLock	Information	Applied Microsoft Defender configuration	Microsoft Defender configuration was successfully applied.
700	DriveLock	Warning	Microsoft Defender blocked an operation	Microsoft Defender blocked an operation of type: [ASRRuleType] Detection time: [TimeStamp] Path: [FileName] Process: [ProcessName] Signature version: [Sig-

Event ID	Source	Severity	Short text	Long text
				natureVersion] Engine version[EngineVersion] Product version: [ProductVersion] User: [UserName]
701	DriveLock	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]
800	DCC	Information	Control Center started	The {PrefixControlCenter} has been started. Connected to: [DesName]
801	DCC	Information	Control Center terminated	The {PrefixControlCenter} has been terminated.
802	DCC	Information	{PrefixEnterpriseService} changed	The {PrefixEnterpriseService} has been changed. The {PrefixControlCenter} is now connected to: [DesName]

Event ID	Source	Severity	Short text	Long text
803	DCC	Information	Added user account	For the user ([AccountName]) an user account has been added.
804	DCC	Information	Removed user account	The account for the user ([AccountName]) has been removed.
805	DCC	Information	Changed permission	The permissions from the user account ([AccountName]) has been changed. Tenants: [Tenants] Home:[Tenants][Tenants] [PermissionHome][PermissionHome] Helpdesk:[PermissionHome][PermissionHome] [PermissionHelpdesk] Forensics:[PermissionHelpdesk][PermissionForensics] [PermissionForensics] Report:[PermissionForensics][PermissionForensics] [PermissionReport] Inventory:[PermissionReport][PermissionInventory][PermissionInventory] Configuration: [PermissionInventory] [PermissionConfiguration] A = allow, N = not set, D = deny

Event ID	Source	Severity	Short text	Long text
806	DCC	Information	Start decrypting personal data	Start decrypting personal data
807	DCC	Information	Stop decrypting personal data	Stop decrypting personal data
808	DCC	Information	Open connection to remote desktop	Open connection to remote desktop: [DisplayName]
809	DCC	Information	Close connection to remote desktop	Close connection to remote desktop: [DisplayName]
810	DCC	Information	New initial BitLocker password from {PrefixControlCenter}	Set new initial BitLocker password for client [DisplayName] from {PrefixControlCenter}
811	DCC	Information	Sent agent action to change BitLocker password from {PrefixControlCenter}	Sent agent action to change BitLocker password to client(s) [DisplayName] from {PrefixControlCenter}
900	DriveLock	SuccessAudit	{Product} configuration element changed	A {Product} configuration element was changed. Object type: [ObjectType] Object

Event ID	Source	Severity	Short text	Long text
				path: [Path] Object unique ID: [ObjectID] Configuration element: [ConfigElement] Data type: [DataType] New value: [NewValue] Old value: [OldValue]
901	DriveLock	SuccessAudit	{Product} configuration element added	A {Product} 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	SuccessAudit	{Product} configuration element deleted	A {Product} configuration element was deleted. Object type: [ObjectType] Object path: [Path] Object unique ID: [ObjectID] Configuration element: [ConfigElement] Data type: [DataType]
910	DriveLock	Information	{PrefixManagementConsole} started	{PrefixManagementConsole} was started. Object type: [ObjectType] Object path: [Path] Object unique ID: [ObjectID]

Event ID	Source	Severity	Short text	Long text
911	DriveLock	Information	{PrefixManagementConsole} stopped	{PrefixManagementConsole} was stopped.
912	DriveLock	Information	Device scanner executed	Device scanner was executed. Scanned computers: [Computers]
920	DriveLock	Information	Remote agent connection established	Remote agent connection established. Agent computer: [DisplayName] (unique ID [ComputerGuid])
921	DriveLock	Information	Remote agent connection disconnected	Remote agent connection disconnected. Agent computer: [DisplayName] (unique ID [ComputerGuid])
922	DriveLock	Information	Remote agent action executed	Remote agent action was executed. Agent computer: [DisplayName] (unique ID [ComputerGuid]) Action: [ActionName] Result: [ActionResult]
923	DriveLock	Information	Shadow files viewer connected remotely	Shadowed files viewer was connected to network location. Location: [Computers]

Event ID	Source	Severity	Short text	Long text
924	DriveLock	Information	Offline unlock wizard failed	The offline unlock wizard was executed and failed. Request code: [RequestCode] Request computer name: [AgentComputerName]
925	DriveLock	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]
926	DriveLock	Information	{FDE} Emergency logon succeeded	A Full Disc Encryption emergency logon was executed and succeeded. Recovery code: [RequestCode] Recovery user name: [UserName] Recovery computer name: [DisplayName] Response code: [UnlockCode]
927	DriveLock	Information	{FDE} Emergency logon succeeded	A Full Disc Encryption emergency logon was executed and succeeded. Recovery



Event ID	Source	Severity	Short text	Long text
				code: [RequestCode] Recovery user name: [UserName] Recovery data file: [FileName] Response code: [UnlockCode]
928	DriveLock	Information	{FDE} Recovery Disk Key created	A Full Disc Encryption recovery disk key was created. Recovery computer name: [DisplayName] (unique ID [ComputerGuid]) Disk key file: [UnlockCode]
929	DriveLock	Information	{FDE} Recovery Disk Key created	A Full Disc Encryption recovery disk key was created. Recovery data file: [FileName] Disk key file: [UnlockCode]
930	DriveLock	Information	{PrefixEnterpriseService} selected	The {PrefixEnterpriseService} [DesName] was selected by {PrefixMMC}. Connection ID: [ObjectID]
931	DriveLock	Warning	{PrefixEnterpriseService} not available	No {PrefixEnterpriseService} is available because no valid server connection is configured.
932	DriveLock	Error	{FDE} Recovery failed	A Full Disc Encryption recovery process

Event ID	Source	Severity	Short text	Long text
				failed. Recovery computer name: [DisplayName] (unique ID [ComputerGuid]) Error: [ErrorMessage]
933	DriveLock	Error	{FDE} Recovery failed	A Full Disc Encryption recovery process failed. Recovery data file: [FileName] Error: [ErrorMessage]
934	DriveLock	Information	{FDE} installation package uploaded	A Full Disc Encryption installation package was uploaded to the server. Package version: [FileName] Server: [ServerName]
935	DriveLock	Information	{FDE} installation package upload failed	A Full Disc Encryption installation package upload failed. Package version: [FileName] Server: [ServerName] Error: [ErrorMessage]
936	DriveLock	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: [DisplayName] Response code:

Event ID	Source	Severity	Short text	Long text
				[UnlockCode]
937	DriveLock	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]
2000	DES	Error	Push installation failed	The push installation of the agent failed on computer [DisplayName]. Error message: ([PiErrorCode]) [PiErrorMessage] Installation step: [PiErrorStep] Attempt number: #[PiAttempts]
2001	DES	Information	Push installation successful	The push installation of the agent on computer [DisplayName] was successful.
2002	DES	Error	AV pattern download failed	The download of AV pattern file [FileName] from the {Product} cloud has failed. Error message: [ErrorMessage]
2003	DES	Information	AV pattern download suc-	The download of AV pattern file

Event ID	Source	Severity	Short text	Long text
			successful	[FileName] from the {Product} cloud was successful.
2004	DES	Error	File download failed	The download of file [FileName] from the {Product} cloud has failed. Error message: [ErrorMessage]
2005	DES	Information	File download successful	The download of file [FileName] from the {Product} cloud was successful.
2006	DES	Information	{FDE} recovery data saved	The {FDE} Recovery Data ( [FdeRecoveryDataType] ) from Computer [DisplayName] has been saved.
2007	DES	Information	{ContainerEncryption} recovery data saved	The recovery data for encrypted volume ( path: '[FilePath][FileName]' , VolumeID: [VolumeID]) has been saved.
2008	DES	Information	DFP recovery data saved	The recovery data for encrypted folder ( path: '[UncPath]' , VolumeID: [DfpVolumeID]) has been saved.

Event ID	Source	Severity	Short text	Long text
2009	DES	Information	DB maintenance successful	The database maintenance for '[DisplayName]' finished successfully.
2010	DES	Error	DB maintenance aborted	The database maintenance for '[DisplayName]' aborted with an error: '[ErrorMessage]'.
2011	DES	Information	DB eventgrooming successful	The database event grooming for '[DisplayName]' finished successfully.
2012	DES	Error	DB event grooming aborted	The database event grooming for '[DisplayName]' aborted with an error: '[ErrorMessage]'.
2013	DES	Information	DB backup successful	The database backup for '[DisplayName]' finished successfully.
2014	DES	Error	DB backup aborted	The database backup for '[DisplayName]' aborted with an error: '[ErrorMessage]'.
2015	DES	Information	DB shrunked successful	The database '[DisplayName]' was shrunked successfully.

Event ID	Source	Severity	Short text	Long text
2016	DES	Error	Error shrinking database	Error on shrinking database '[DisplayName]': '[ErrorMessage]'.
2017	DES	Error	AV pattern sync failed	The download of AV pattern file [FileName] from the central {PrefixES} has failed. Error message: [ErrorMessage]
2018	DES	Information	AV pattern sync successful	The download of AV pattern file [FileName] from the central {PrefixES} was successful.
2019	DES	Error	File download failed	The download of file [FileName] from the central {PrefixES} has failed. Error message: [ErrorMessage]
2020	DES	Information	File download successful	The download of file [FileName] from the central {PrefixES} was successful.
2021	DES	Information	The {PrefixES} was started	The {PrefixES} was started.
2022	DES	Information	CSP active	The centrally stored policy [CspName], version [CspVersion], ID: [CspID] is now avail-

Event ID	Source	Severity	Short text	Long text
				able on the {PrefixES}.
2023	DES	Information	CSP inactive	The centrally stored policy [CspName], version [CspVersion], ID: [CspID] is not available on the {PrefixES}.
2024	DES	Information	CSP deleted	The centrally stored policy [CspName], ID: [CspID] was deleted.
2025	DES	Information	CSP assignment active	The centrally stored policy assignment is now active on the {PrefixES}. Name: [CspAssignmentName], order: [CspAssignmentOrder], CSP ID: [CspID]
2026	DES	Information	CSP assignment deleted	The centrally stored policy assignment [CspAssignmentName] was deleted.
2027	DES	SuccessAudit	Group created	The [GroupMemberType] group [GroupName] (identifier: [GroupIdentifier]) was created.
2028	DES	SuccessAudit	Group deleted	The [GroupMemberType] group

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



Event ID	Source	Severity	Short text	Long text
2032	DES	SuccessAudit	Group updated	The group with identifier [GroupIdentifier] was updated. Name: [GroupName], Description: [GroupDescription]
2033	DES	SuccessAudit	Dynamic group created	The dynamic group [GroupName] (identifier: [GroupIdentifier]), type: [GroupMemberType] was created.
2034	DES	SuccessAudit	Dynamic group deleted	The dynamic group [GroupName] (identifier: [GroupIdentifier]), type: [GroupMemberType] was deleted.
2035	DES	SuccessAudit	Dynamic group updated	The dynamic group with identifier [GroupIdentifier] was updated. Name: [GroupName], Description: [GroupDescription]
2036	DES	SuccessAudit	Dynamic group changed	The dynamic group [GroupName] (identifier: [GroupIdentifier]) was changed. group definition (old): [GroupDynDefinitionOld] group definition (new): [GroupDynDefinitionNew]

Event ID	Source	Severity	Short text	Long text
2100	DOC	SuccessAudit	Account created	The account [AccountDisplayName] (identifier: [AccountIdentifier]) was created
2101	DOC	SuccessAudit	Account deleted	The account [AccountDisplayName] (identifier: [AccountIdentifier]) was deleted
2102	DOC	SuccessAudit	Role assignment created	The role [RoleDisplayName] (id: [RoleID]) was assigned to the account [AccountDisplayName] (identifier: [AccountIdentifier]). OU Restrictions: ([OuRestriction])
2103	DOC	SuccessAudit	Role assignment deleted	The role assignment [RoleDisplayName] (id: [RoleID]) was removed from the account [AccountDisplayName] (identifier: [AccountIdentifier])
3001	DES	SuccessAudit	Suspicious user file activity	Suspicious user file activity detected in past [Duration] days (rolling). User: [UserName] ([Domain]) Count of files: [FileCount] Number of bytes: [ByteCount] Number of sessions: [SessionCount] Total

---

Event ID	Source	Severity	Short text	Long text
				session time (min): [SessionDuration]

## 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.

© 2020 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.