DriveLock Defender Integation

Manual 2020.1

DriveLock SE 2020

Table of Contents

1 Integrating Microsoft Defender into DriveLock

DriveLock allows you to configure Microsoft Defender using policies in the DriveLock Management Console (DMC) and to monitor the current status of DriveLock Agents in the DriveLock Operations Center (DOC).

All available Microsoft Defender Antivirus Group Policy (GPO) settings can be configured in the DMC.

For quick configuration, selected settings are available from within the Taskpad view:

- Settings for scanning file accesses and response to detected malware
- Exceptions for file checks or processes
- Regular scans with date and time, frequency and type of response
- Type and content of end user notifications

In addition, you can configure settings for using Defender to scan external drives:

- Use virus scanner when connecting external drives and, if necessary, automatically block access if malware is detected

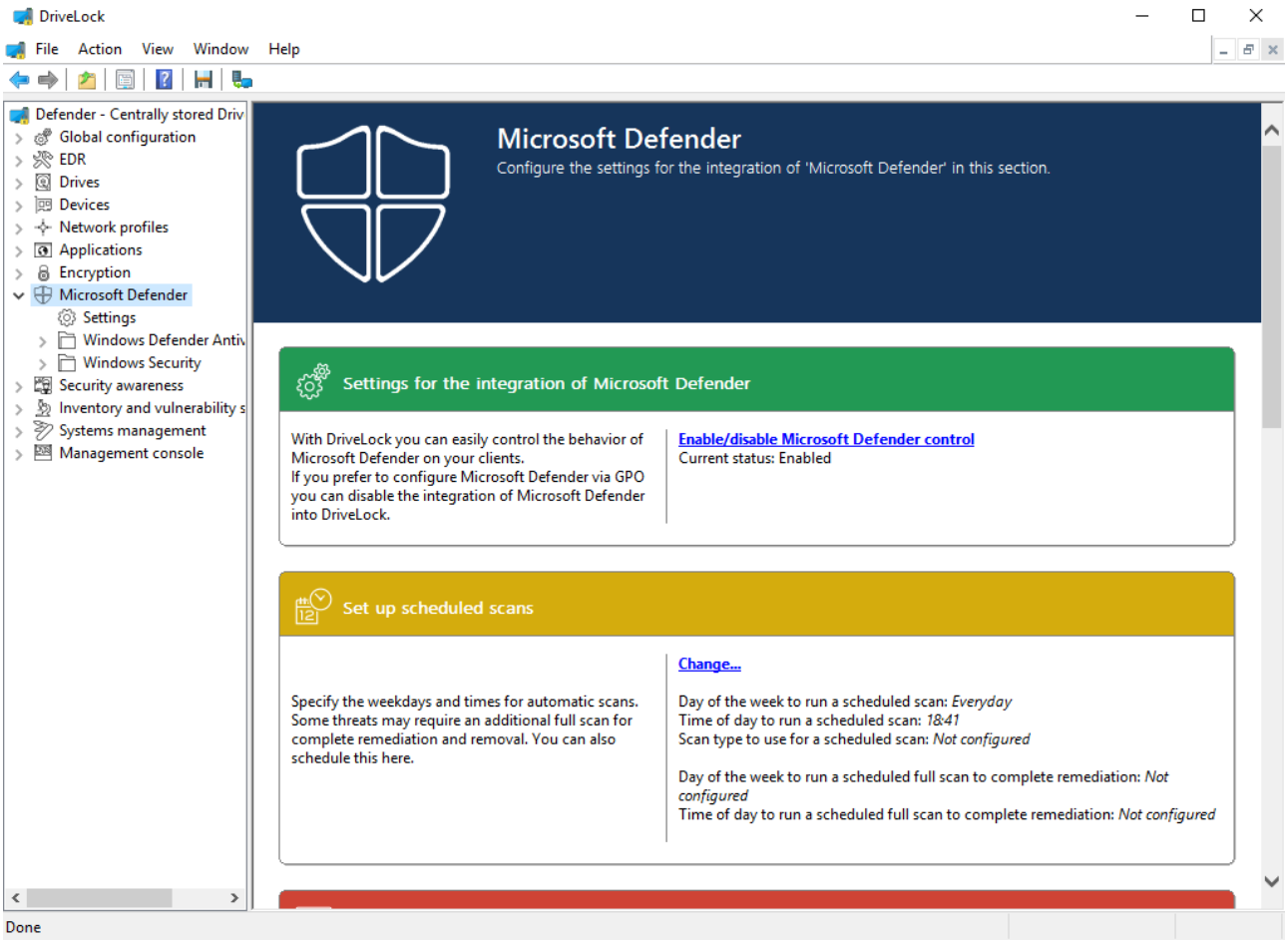
The DriveLock Operations Center (DOC) allows you to view status reports on current threats and the status of DriveLock Agents. Any threats found can be analyzed precisely and, if necessary, false or irrelevant notifications can be suppressed.

Warning: Microsoft Defender Management requires a valid license.

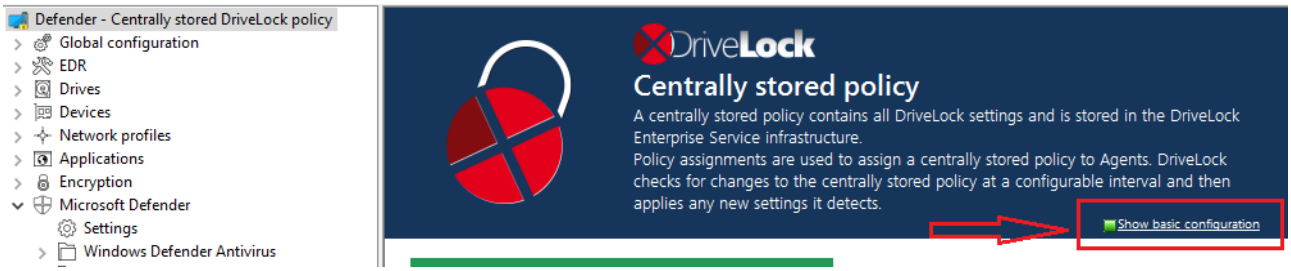
2 Configuration

2.1 Overview in the DriveLock Management Console

There is a new **Microsoft Defender** node in the policy where you can specify the settings. From this overview, you can enable (or disable) Defender functionality and thereby integrate its control into DriveLock.



In case another view opens in your policy, you might have to change the **Show basic configuration** setting. To see the basic configuration options, make sure to enable this setting at the highest level of the policy, see figure:



2.2 Easy configuration in the Taskpad view

In addition to enabling Microsoft Defender control, you can configure other basic settings in the Taskpad view of the **Microsoft Defender** node.

- **Set up scheduled scans**
  You can specify the times for automatic scans here.
  First, you can specify the time for a scheduled scan and the scan type to be used.
  Second, you can specify the time to complete the remediation. This information is needed because some threats can only be removed by Microsoft Defender after another full scan.

  > Note: If you specify the time for the scheduled scan at this point, DriveLock uses its own scheduler to start the scan at the defined time. Settings such as **Randomize scheduled task times** or **Start the scheduled scan only when computer is on but not in use** are not considered. The scan always starts at the specified time.

  If you want to use Defender's default scheduler, please make the appropriate settings in the **Scan** option of the **Windows Defender Antivirus** subnode.
- **Scanning options**:
  Configure the antivirus scanning options here.
- **Exclusions**:
  Configure the exclusions here to exclude certain files from Microsoft Defender antivirus scans. For more information, see Microsoft.
- **Automatic remediation action**:
  Configure the automatic remediation action for each threat alert level.
  The classification of individual threats according to threat alert level (low, medium, high, severe) is stored in the Defender signature definitions. For example, you can display this information using Powershell with the Get-MpThreatCatalog command. The SeverityID corresponds to the threat alert level:
  1 = Low
  2 = Medium
  4 = High
  5 = Severe
- **Attack surface reduction**:
  Create rules for Attack Surface Reduction (ASR) here.

2.3 Settings for Microsoft Defender

You can configure the following general settings to integrate Microsoft Defender into DriveLock:

- Enable/disable Microsoft Defender control
- Clear existing Microsoft Defender configuration
- Show advanced configuration options

2.3.1 Enable/disable Microsoft Defender control

To permit DriveLock to control Microsoft Defender on DriveLock Agents, you must activate the **Enable/disable Microsoft Defender control** setting in the policy. This is the default setting.

Note: This setting only affects the control by DriveLock and not the actual functionality of Microsoft Defender.

2.3.2 Clear existing Microsoft Defender configuration

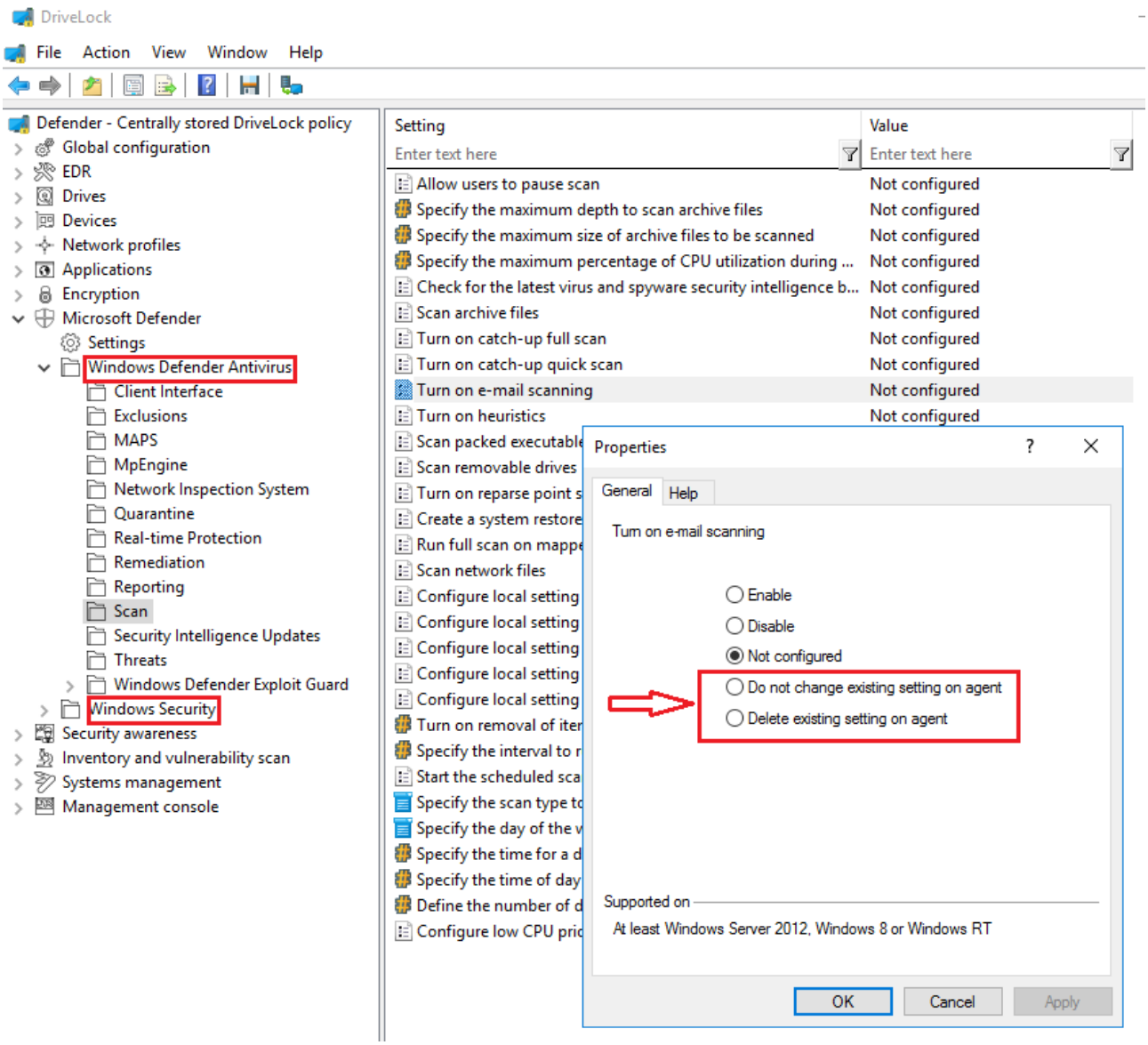
The **Clear existing Microsoft Defender configuration** setting determines whether DriveLock maintains existing Defender settings on the agent or deletes them before applying the policy.

By default, the DriveLock Agent maintains the existing Defender configuration and only applies those settings that are included in the DriveLock policy.

2.3.3 Show advanced configuration options

If you select **Show advanced configuration options**, two additional configuration options appear in the configuration dialogs of the **Windows Defender Antivirus and Windows Security** nodes, which are invisible otherwise.

The example shows the dialog for the e-mail scan settings:



These configuration options provide the following benefits:

- **Do not change existing setting on agent**
  If a setting is already applied to the agent, DriveLock will not change it.

  > Note: In contrast to **Not configured**, DriveLock does not change such a setting, regardless of whether it is set in another assigned DriveLock policy or not. This applies to policies that come **before** this policy in the order of assignment.

  Example:
  You want to apply specific Defender settings to all DriveLock Agents. Create a DriveLock policy with the appropriate settings and assign them to your agents. You want to allow one department to configure some of these settings independently (e.g.,

via Group Policy, manually or with another external tool). To avoid having to copy the entire policy and only change these few settings, you can create a new policy and set the relevant settings in this policy to **Do not change existing setting on agent**. Assign this new policy to the agents so that it appears after the existing Defender policy.

- **Delete existing setting on agent**
  If you specify this value for a Defender setting from the **Windows Defender Antivirus** node, the Defender setting is deleted from the DriveLock Agent. The Defender will then use its default setting.
  This option can be compared to the Clear existing Microsoft Defender configuration setting, except that it is used for a single setting, while **Clear existing Microsoft Defender configuration** will clear all settings.

2.4 Windows Defender Antivirus and Windows Security

The **Windows Defender Antivirus** and **Windows Security** subnodes contain all settings for Microsoft Defender that can be distributed using Group Policy as of June 2019.

The DriveLock Agent stores the settings from the DriveLock policy in the same location in the registry where Group Policy settings are stored. The Defender settings can then be found at

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender` and/or
- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center`

If the Clear existing Microsoft Defender configuration setting is disabled, you can use Group Policy or another external tool to distribute some of the Defender settings in addition to the DriveLock policy.

2.5 External Drives

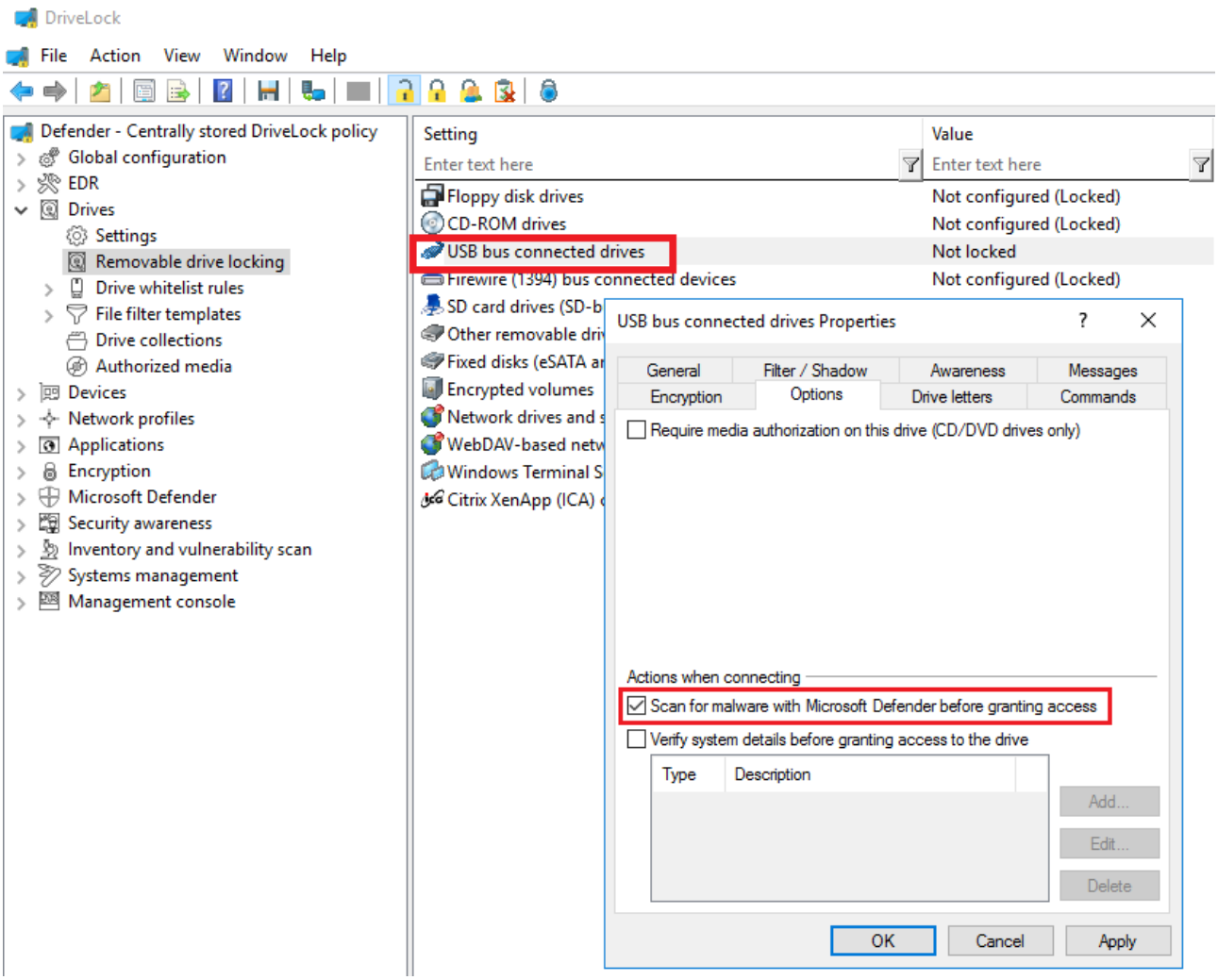
2.5.1 Scanning external drives

You can configure an external drive in policies to automatically start a virus scan when it is connected to the computer. This way, users can only access the drive when the scan is complete and no malware has been found.

2.5.2 Configure removable drive locking

Please do the following:

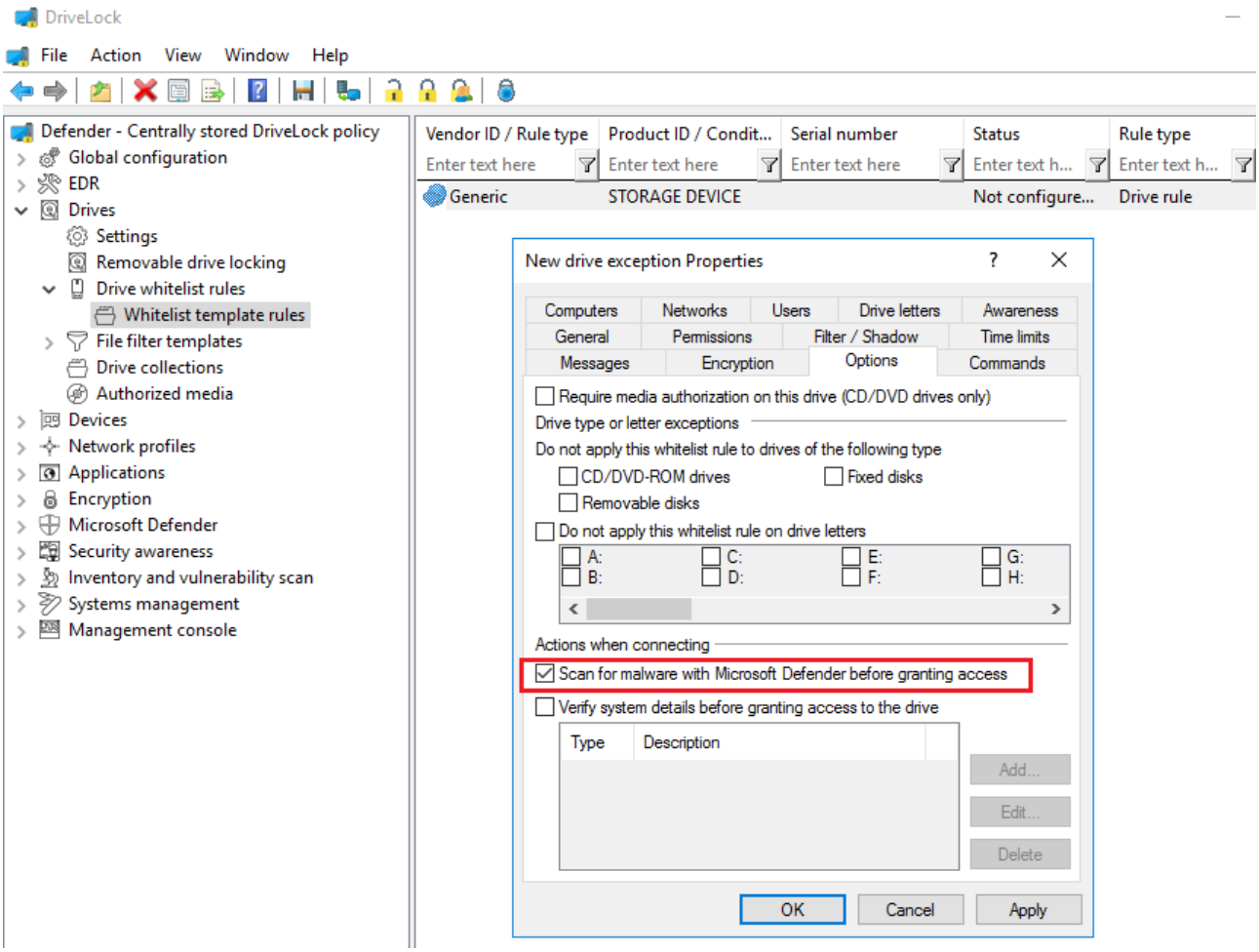
1. Open the **Drives** node in the policy, select the **Removable drive locking** subnode and select the relevant drive to edit it.
2. Switch to the **Options** tab in the dialog.
3. Check the option **Scan for malware with Microsoft Defender before granting access**.



2.5.3 Configure drive whitelist rules

Please do the following:

1. Open the **Drives** node in the policy and select the **Drive whitelist rules** subnode. Create a new whitelist rule or open an existing one for editing.
2. Switch to the **Options** tab in the dialog.
3. Check the option **Scan for malware with Microsoft Defender before granting access**.



Note: If the drive is encrypted, DriveLock starts the scan as soon as the drive is connected and decrypted.

On the DriveLock Agent, a message appears in the system tray icon.

If Microsoft Defender finds a threat on the drive, it will noticeably increase the scanning time. Microsoft Defender then attempts to eliminate the threats. If that fails, the drive must be disconnected and reconnected so that Microsoft Defender can finish removing the threat.

A message will inform the user whether the removal was successful and whether the drive can be accessed.

Note: If Microsoft Defender cannot eliminate the threat, the only remaining option is to access the drive by temporarily unlocking it.

3 Events

3.1 Status report and events

The DriveLock Agent regularly sends the current Defender status to the DriveLock Enterprise Service (DES). The status includes information such as definition version numbers, last scan times and threats found.

The status is sent after the start of the service and then every 24 hours. In addition, this also happens after configuration changes, after updating Microsoft Defender and when threats occur.

> Note: The status is always sent, regardless of whether the **Enable/disable Microsoft Defender control** option is set or not.

3.2 Microsoft Defender events

The following table contains the events generated by the DriveLock Enterprise Service (DES). You can determine whether these events are sent to the DES and displayed in the DriveLock Operations Center (DOC) in the policy in the **EDR** node, **Events** subnode, **Microsoft Defender**, in the **DriveLock Enterprise Service** column.

For a complete list of all DriveLock events, refer to the corresponding documentation on DriveLock OnlineHelp.

ID	Type	Short text	Long text	Explanation
681	Error	Configuration of Microsoft Defender failed	Error in the Microsoft Defender con-figuration. Error code: [ErrorCode] Error: [ErrorMessage]	This event is generated if the Microsoft Defender settings from the DriveLock policy could not be applied. The error code is the Windows error code.
682	Information	Microsoft Defender con-figuration changes reverted	Configuration changes to Microsoft Defender detected by third parties. The changes have been undone. Details: [Details]	This event is generated when DriveLock has detected third-party configuration changes to Microsoft Defender

ID	Type	Short text	Long text	Explanation
				and was able to undo the changes according to DriveLock policy. Only those configuration changes that are included in the DriveLock policy are reverted. If the **Clear existing Microsoft Defender configuration** option is set, all settings that are not included in the policy are also removed.
683	Error	Failed to revert Microsoft Defender configuration changes	Configuration changes to Microsoft Defender detected by third parties. The changes could not be undone. Details: [Details] Error code: [ErrorCode]. Error: [ErrorMessage]	This event is generated when DriveLock detects configuration changes made to Microsoft Defender by a third party and is unable to undo the changes according to DriveLock policy. Details: Contains the list of configuration changes found
684	Warning	Microsoft Defender detected a threat	Microsoft Defender has detected the [DetectionName] ([DetectionType])	This event is generated when Microsoft Defender

ID	Type	Short text	Long text	Explanation
			threat. Infected file: [Path] Drive: [DriveLetter] Filename: [FileName] Filename hash: [MD5Hash]	has detected a threat. Unlike event 697, this event does not contain any information about the affected drive because this information could not be found. • DetectionName: Name of the threat • DetectionType: Category of threat, e.g. Trojan, SpyWare, etc. • Path: Full file path • FileName: File name • MD5Hash: MD5 from the file name
685	Warning	Microsoft Defender threat allowed	A user allowed a threat that Microsoft Defender detected. Threat: [DetectionName] Category: [DetectionType]	This event is generated when the user allowed a threat detected by Microsoft Defender.
686	Warning	Microsoft Defender threat	A user restored a threat from quarantine that was detected by	This event is generated when Microsoft Defender restored a

ID	Type	Short text	Long text	Explanation
		restored from quarantine	Microsoft Defender. Threat: [DetectionName] Category: [DetectionType]	threat from quarantine.
687	Error	Microsoft Defender signature update failed	Microsoft Defender signature definition could not be updated. Details: [Details]	This event is generated if the Microsoft Defender signature definitions could not be updated.
696	Warning	Microsoft Defender detected a threat	Microsoft Defender detected the [DetectionName] ([DetectionType]) threat. Infected network file: [Path] Network drive: [NetDrivePath] ([NetDriveType]) File name: [FileName] File name hash: [MD5Hash].	This event is generated when Microsoft Defender detected a threat on a network drive.
697	Warning	Microsoft Defender detected a threat	Microsoft Defender detected the [DetectionName] ([DetectionType]) threat. Infected file: [Path] Device identification: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Serial number [HWSerialNumber])	This event is generated when Microsoft Defender detected a threat. Unlike event 684, this event contains hardware information about the affected drive.

ID	Type	Short text	Long text	Explanation
			Drive: [DriveLetter] File name: [FileName] File name hash: [MD5Hash].	
698	Error	Microsoft Defender is disabled	Microsoft Defender is disabled and cannot be activated by DriveLock.	This event is generated when the Windows Defender Antivirus Service is not running on the agent.
699	Information	Applied Microsoft Defender configuration	Microsoft Defender configuration was successfully applied.	This event is generated when the DriveLock policy was successfully applied.
700	Warning	Microsoft Defender blocked an operation	Microsoft Defender prevented an action: [ASRRuleType] Recognition time: [TimeStamp] Path: [FileName] Process: [ProcessName] Signature version: [SignatureVersion] Engine version [EngineVersion] Product version: [ProductVersion] User:	This event is generated when one of the attack surface reduction rules has blocked an action. • ASRRuleType: Name of the rule • TimeStamp: Time • FileName: Complete file name of the affected file • ProcessName:

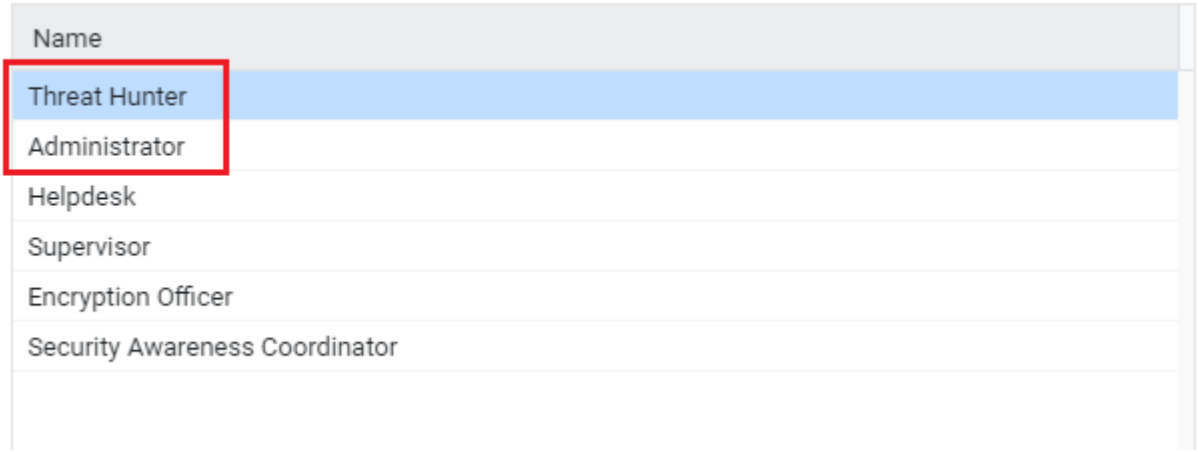
ID	Type	Short text	Long text	Explanation
			[UserName]	Affected process name • SignatureVersion: Version number of the antivirus signature • EngineVersion: Version number of the NIS Engine (Network Real-time Inspection service) • ProductVersion: Version number of the Defender • UserName: User-name
701	Audit	Microsoft Defender audited an operation	Microsoft Defender has logged an action: [ASRRuleType] Recognition time: [TimeStamp] Path: [FileName] Process: [ProcessName] Sig-nature version: [Sig-natureVersion] Engine version [EngineVersion] Product version: [Pro-ductVersion] User: [UserName]	This event is gen-erated when one of the attack surface reduction rules is applied in Audit Mode.

ID	Type	Short text	Long text	Explanation
702	Error	Error uploading data to DES		This is another DES event that is generated when sending the status to the DES fails. You can find this event in the EDR node, Events, then General agent events, in the Server communications sub-node.

4 Microsoft Defender Management in the DOC

You can see the status of Microsoft Defender on the agents in the DriveLock Operations Center (DOC) in the **Microsoft Defender** view. For more information about the DOC, see the **DriveLock Control Center** documentation on DriveLock OnlineHelp.

The Administrator or Threat Hunter role is required to be able to see the Micorsoft Defender view (see figure).



The DOC Dashboard also displays the Microsoft Defender status with various widgets. If the Microsoft Defender dashboard does not appear automatically, you can add it using the appropriate template.

4.1 Dashboard

Understanding the widgets:

- **Threats**
  Indicates the number of threats that are currently suppressed for all computers. A threat that is suppressed for only one computer will not appear here.
- **Computer**
  Indicates the number of computers having suppressed threats.
- **Latest Microsoft Defender events**
  Shows Microsoft Defender events from the last week. Note that you need to enable the sending of events to the DES for this option.
- **Microsoft Defender state** provides an overview of the status of Microsoft Defender on the computers:

- Not set: The status has not yet been reported
- Active
- Partly active: One or more Microsoft Defender components are not running, e.g. real-time protection
- Inactive: The Microsoft Defender Service is not running

- **Threats by category**
  Displays all threats that have occurred and groups them by category. We do not distinguish between threats that have already been resolved and those that are still open.
- **Threats by severity**
  Displays all threats that have occurred and groups them by severity. We do not distinguish between threats that have already been resolved and those that are still open.
- **Threat history by category**
  Shows threat history by category
- **Threat history by severity**
  Shows threat history by severity
- **Affected computer count history**
  Shows the history of affected computers by number
- **Services or features to be enabled**, **Protection status**, **Service overview**, **Suppressed threats**: refer to this section please.
- **Feature overview**
  Indicates the number of computers having individual Microsoft Defender features enabled.

4.2 View

The Microsoft Defender view has a bar with widgets at the top of the screen that provide an overview of the agents' status. If you click on one of the widgets, the corresponding list of computers or threats is displayed in the area below. Select a computer or threat to get a detailed view on the right side.

Understanding the widgets:

- **Protection** status shows the current status of the computers
  - Affected computers
    Number of computers with open threats that Microsoft Defender was unable to remove

- Not up to date
  Number of computers without open threats, with updated Microsoft Defender signature definitions, and with a last status message not more than 1 week ago
- Protected
  Number of computers with Microsoft Defender signature definitions older than 1 week or with a status message more than 1 week ago
- Inactive
  Number of computers that are not running Microsoft Defender Service

- **Service overview** shows the number of computers running the Windows Defender Antimalware Service or Windows Defender Antivirus Network Inspection Service.
- **Services or features to be enabled** shows the number of computers running Microsoft Defender Services or features that are available but not active. They may still be enabled to provide full protection.
  - Services that can be enabled are the Windows Defender Antimalware Service and Windows Defender Antivirus Network Inspection Service.
  - Features that can be enabled include access protection, real-time protection, and behavior and tamper protection. Here the system checks whether the feature is actually available. For example, tamper protection is only available from Windows 10 1903 onwards.

Note: This widget does not reflect the settings in the DriveLock policy. Even if a feature on the computer has been disabled as a result of a policy, it will still appear in this list.

- **Suppressed threats** With DriveLock, you can choose to suppress certain threats you want to ignore. These threats and affected computers are displayed here.
  - Computer
    Indicates the number of computers having suppressed threats.
  - Threats
    Number of threats suppressed.

Tabs:

1. **Computers with threats**
   Depending on the selected context, all affected computers are displayed here.
   The detail view on the right consists of different blocks:

- **Overall computer status** provides an overview of the status of Microsoft Defender, such as version numbers, available features and services, and the last update date. The lines that suggest an issue are highlighted in red in this view.
- Open/ resolved/ suppressed threats
  Based on the status of existing threats, they are displayed under open, resolved or suppressed threats. Open threats can be suppressed for the selected computer or for all computers.
- The **Open encyclopedia** link will take you to a Microsoft information page where you can get more information about the threat.
- The **Show threat detection details** link opens the details view of the threat on the computer, where you can see which files are affected or when the threat was found.
- **Properties**
  The properties include general operating system information and the detailed status of Micrsosoft Defender, as displayed on a computer via the Powershell command `Get-MpComputerStatus`, for example.
- The **Last update** line shows when the DES was last updated by the agent.

2. **Detected threats**
   The list contains all threats found in the company.
   The detailed view on the right then contains a list of computers on which the threats are open, resolved or suppressed.
3. **Threat detection details**
   Each threat can occur several times on the same computer, e.g. in different directories, on different USB sticks or several times in a row. The items shown in the list correspond to the occurrence of a threat on a computer. So several lines may contain the same computer with the same threat.
   The detail view shows affected files and the properties of the threat. In the properties you can see the status of the threat and when the last Defender action took place.

5 Troubleshooting

When tracing is enabled, the following log files are created on the agent:

- DlSvcDefender.log
- DES.log

You can also save the latest status sent by the agent to the DES to a file. To do so, you need to enable tracing and set the following registry key on the agent:

- Registry key: `HKLM\Software\CenterTools\TraceLog`
- DWORD value: DlSvcDefender_LogStatus
- The file DefenderStatus.json is then saved in the trace directory.

Copyright