DriveLock Defender Management

Documentation 2022.2

DriveLock SE 2022

Table of Contents

1 INTEGRATING MICROSOFT DEFENDER INTO DRIVELOCK 4

2 CONFIGURATION 5

2.1 Overview in the DriveLock Management Console 5

2.2 Easy configuration in the Taskpad view 6

2.3 Settings 7

2.3.1 General settings 7

2.3.1.1 Enable/disable Microsoft Defender control 7

2.3.1.2 Show advanced configuration options 8

2.3.1.3 Clear existing Microsoft Defender configuration 9

2.3.2 Settings for Defender scans with DriveLock Scheduler 9

2.3.2.1 Scheduled scan day 10

2.3.2.2 Scheduled scan time 10

2.3.2.3 Start scan only on specific events 10

2.3.2.4 Allow users to delay the scan 10

2.3.2.5 Maximum number of hours to delay the start of the scan 10

2.3.2.6 Time in minutes after which the notification is automatically closed 11

2.4 Windows Defender Antivirus and Windows Security 11

2.5 External drives 12

2.5.1 Scanning external drives 12

2.5.2 Configure removable drive locking 12

2.5.3 Configure drive whitelist rules 13

3 AGENT REMOTE CONTROL 15

3.1 Properties of the DriveLock Agent 15

3.1.1 Options in the Defender dialog 15

3.2 Disabling Defender in the Unlock Agent Wizard 17

3.2.1 Disable Microsoft Defender control 17

3.2.2 Disable Defender on the DriveLock Agent 18

4 EVENTS 19

4.1 Status report and events 19

4.2 Microsoft Defender events 19

5 MICROSOFT DEFENDER MANAGEMENT IN THE DOC 20

5.1 Dashboard 21

5.2 View 22

5.3 Quick scan for viruses 23

6 TROUBLESHOOTING 25

COPYRIGHT 26

1 Integrating Microsoft Defender into DriveLock

With DriveLock, you can configure Microsoft Defender via the Policy Editor and monitor the current status of DriveLock Agents in the DriveLock Operations Center (DOC).

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

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

Note: Note that due to a known issue with the GPO ADMX format, DriveLock only supports Windows 8.1 and newer operating systems.

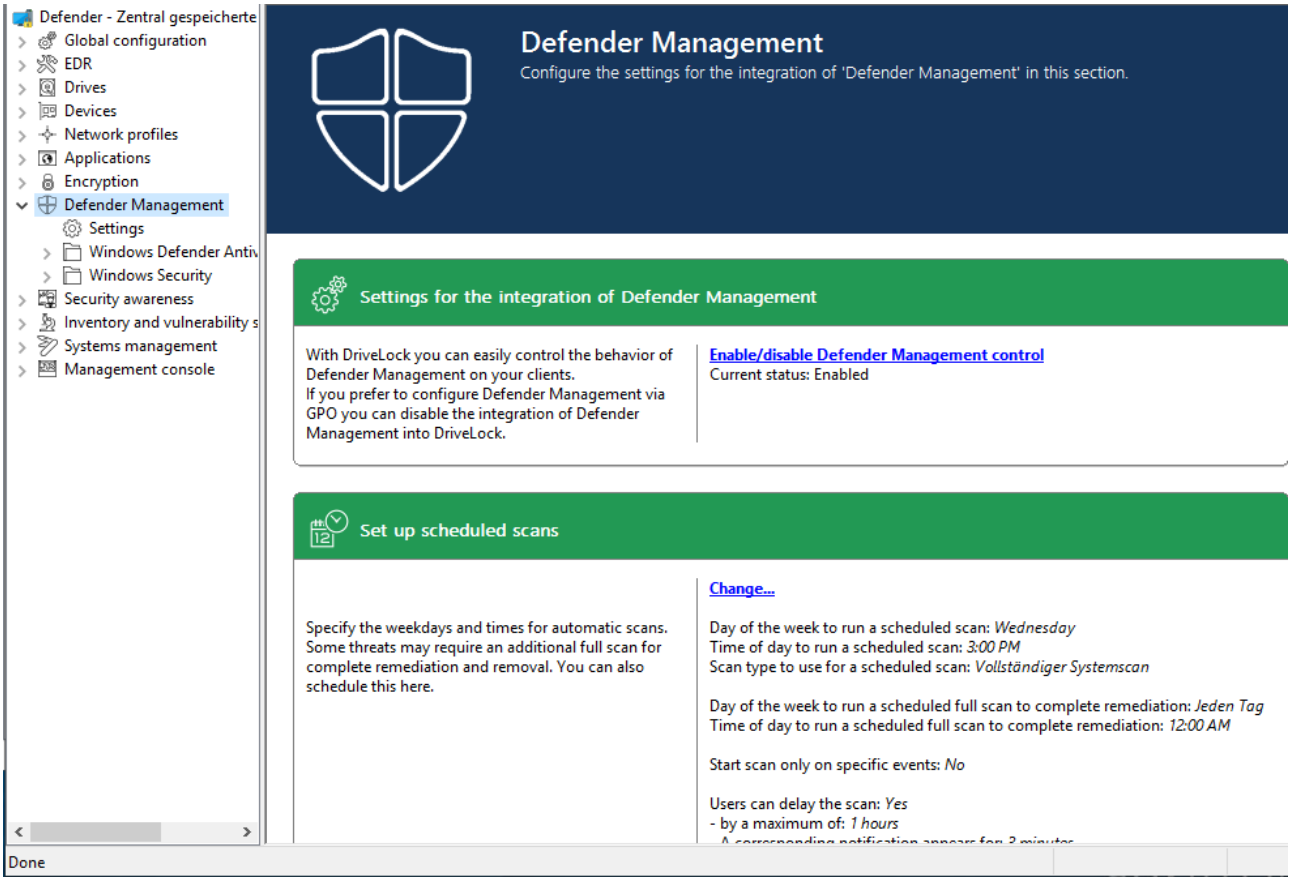
The DriveLock Operations Center (DOC) allows you to view status reports on current threats and the status of DriveLock Agents. Any threats found can be analyzed precisely and, if necessary, false or irrelevant notifications can be suppressed.

Warning: A license is required for Defender Management.

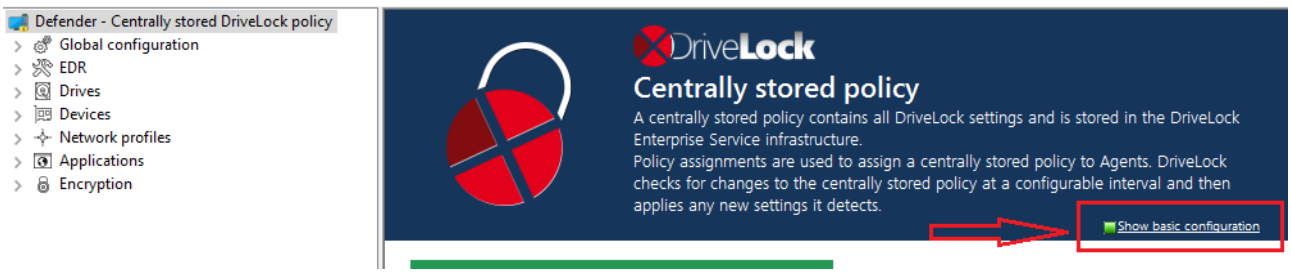
2 Configuration

2.1 Overview in the DriveLock Management Console

Once licensed, the policy includes the new node **Defender Management**. Here you can configure the settings for Defender. From this overview, you can enable (or disable) Defender functionality and thereby integrate its control into DriveLock.



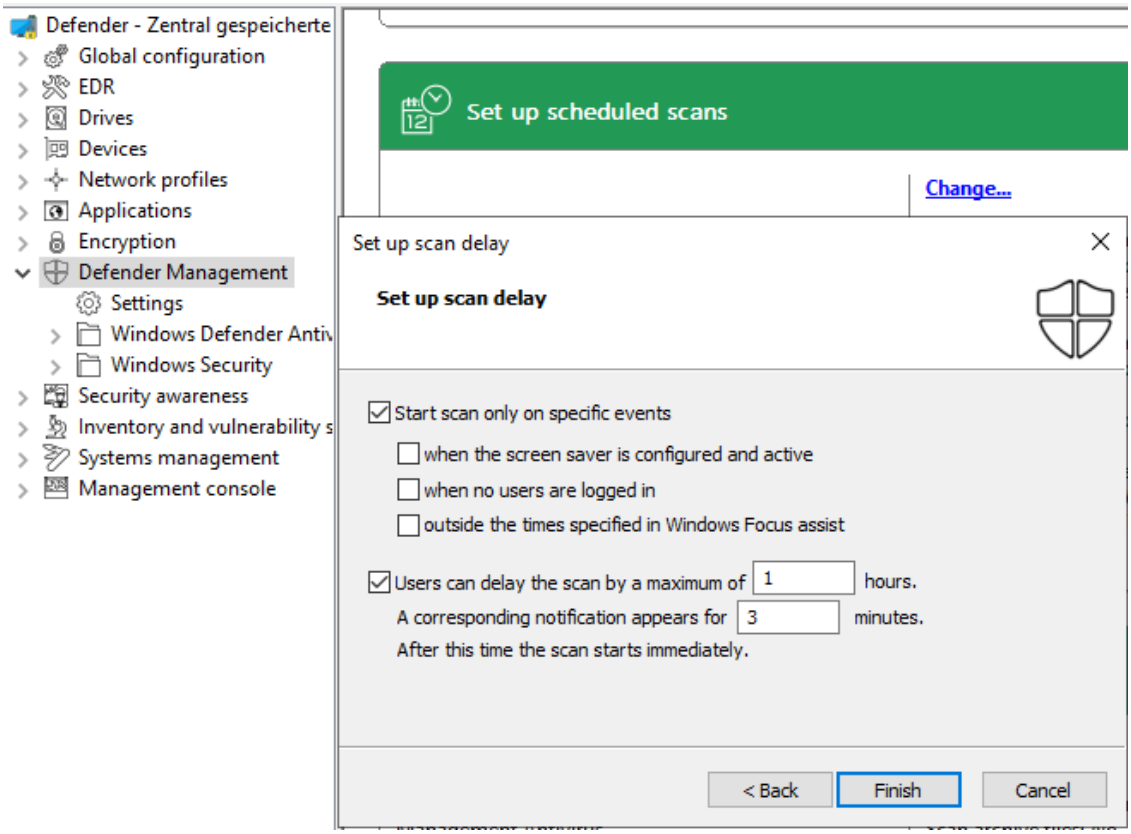
In case another view opens in your policy, you might have to change the **Show basic configuration** setting. To see the basic configuration options, make sure to enable this setting at the highest level of the policy, see figure:



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.

1. **Set up scheduled scans**
   Here you can configure the following:
   - Time and type of scan: 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. Microsoft Defender's own settings such as **Randomize scheduled task times** or **Start the scheduled scan only when computer is on but not in use** are not considered.
   - Time for complete remediation: This specification is necessary because some threats can be eliminated by Microsoft Defender only after another complete scan.
   - Scan delay and scan events: When you set up scheduled scans, you can define that scans may only start under certain conditions and that users may delay scans.



Note: If you want to use Microsoft Defender's own scheduler, configure the appropriate settings in the **Windows Defender Antivirus** subnode in the **Scan** setting.

2. **Scanning options**:
   Configure the antivirus scanning options here.
3. **Exclusions**:
   Configure the exclusions here to exclude certain files from Microsoft Defender anti-virus scans. For more information, see Microsoft.
4. **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
5. **Attack surface reduction**:
   Create rules for Attack Surface Reduction (ASR) here.

2.3 Settings

2.3.1 General settings

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

2.3.1.1 Enable/disable Microsoft Defender control

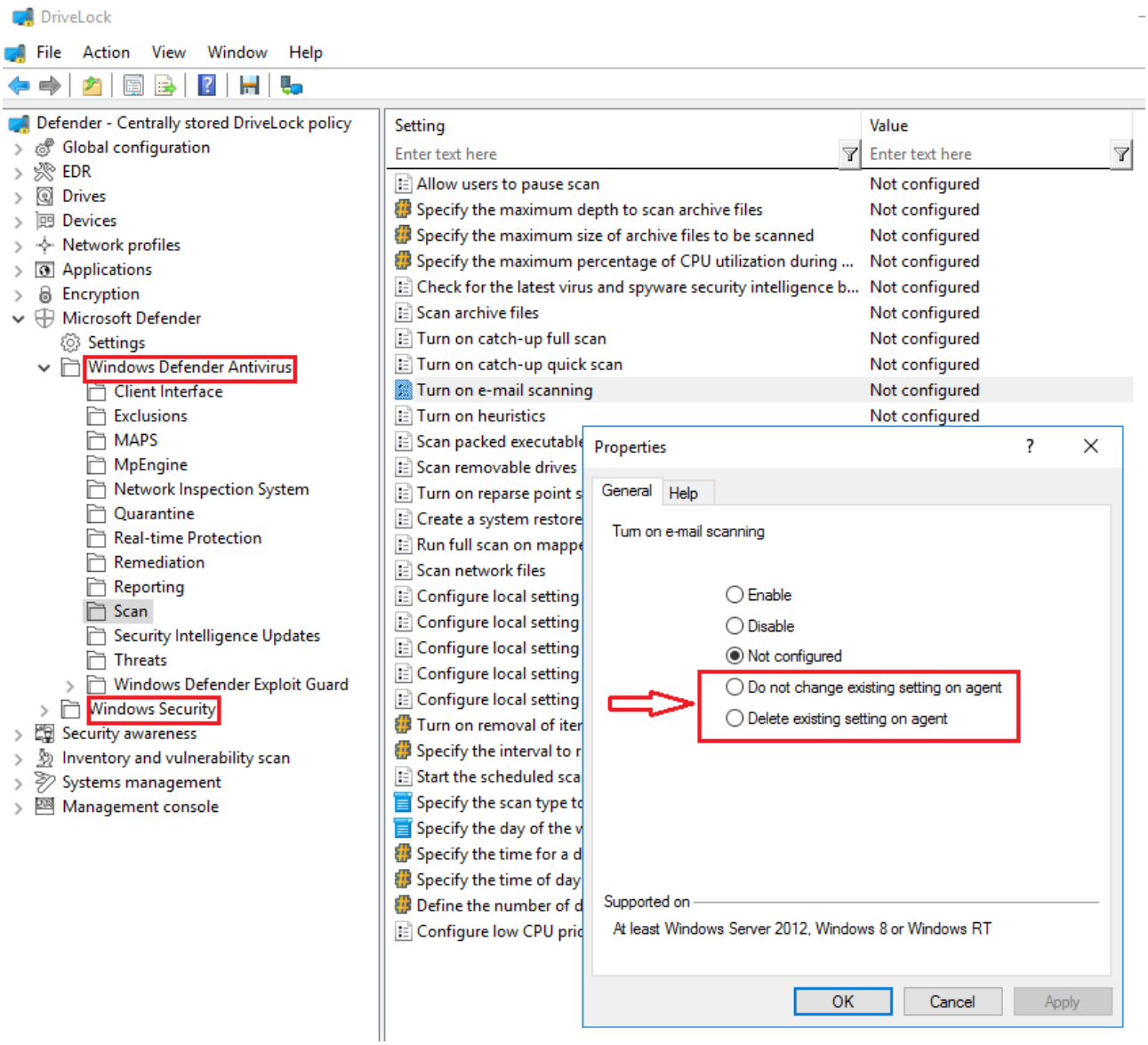
To permit DriveLock to control Microsoft Defender on DriveLock Agents, you must activate the **Enable/disable Microsoft Defender control** setting in the policy. This is the default setting.

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

2.3.1.2 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.

2.3.1.3 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.

2.3.2 Settings for Defender scans with DriveLock Scheduler

The following settings apply to executing scheduled scans with DriveLock Scheduler:

- Scheduled scan day
- Scheduled scan time

- Start scan only on specific events
- Allow users to delay the scan
- Maximum number of hours to delay the start of the scan
- Time in minutes after which the notification is automatically closed

2.3.2.1 Scheduled scan day

This setting lets you specify a day when scanning will be performed.

You can change or delete the day of the week for the Defender scan by setting it to **Not Configured**.

2.3.2.2 Scheduled scan time

This setting lets you specify a time when scanning will be performed.

You can change or delete the time for the Defender scan by setting it to **Not Configured**.

2.3.2.3 Start scan only on specific events

With this setting, you can specify that the Defender scan may start only when certain events occur. This will keep users from being disturbed during their work by scanning processes.

> Note: The screen saver must be active and configured when you select the corresponding option. Otherwise the option will be ignored.

You can specify a detailed setting of notification times in the Windows Focus Assist, which DriveLock will query. Use this option to run the scan (or display notifications) only outside of these configured times.

2.3.2.4 Allow users to delay the scan

To keep the CPU load on the respective client computers as low as possible, you can specify here that users are allowed to delay a Defender scan. Select **Enable** to do so.

You can configure how long the delay will last and whether a corresponding notification will be displayed to the user.

2.3.2.5 Maximum number of hours to delay the start of the scan

At times, users may want to postpone the start of a Defender scan, for example, to continue to work without interruption or when performing automated tasks. For this reason, a delay of up to 16 hours can be configured.

Enter an appropriate value in the dialog.

Once the delay expires, the notification dialog is closed on the client computer and the scan is then started immediately.

2.3.2.6 Time in minutes after which the notification is automatically closed

Use this setting to configure how long the notification dialog stays open for the user.

As soon as the notification dialog closes automatically without the user entering a delay, the scan is started. In this case, the shorter configured time (delay or display time) always applies.

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

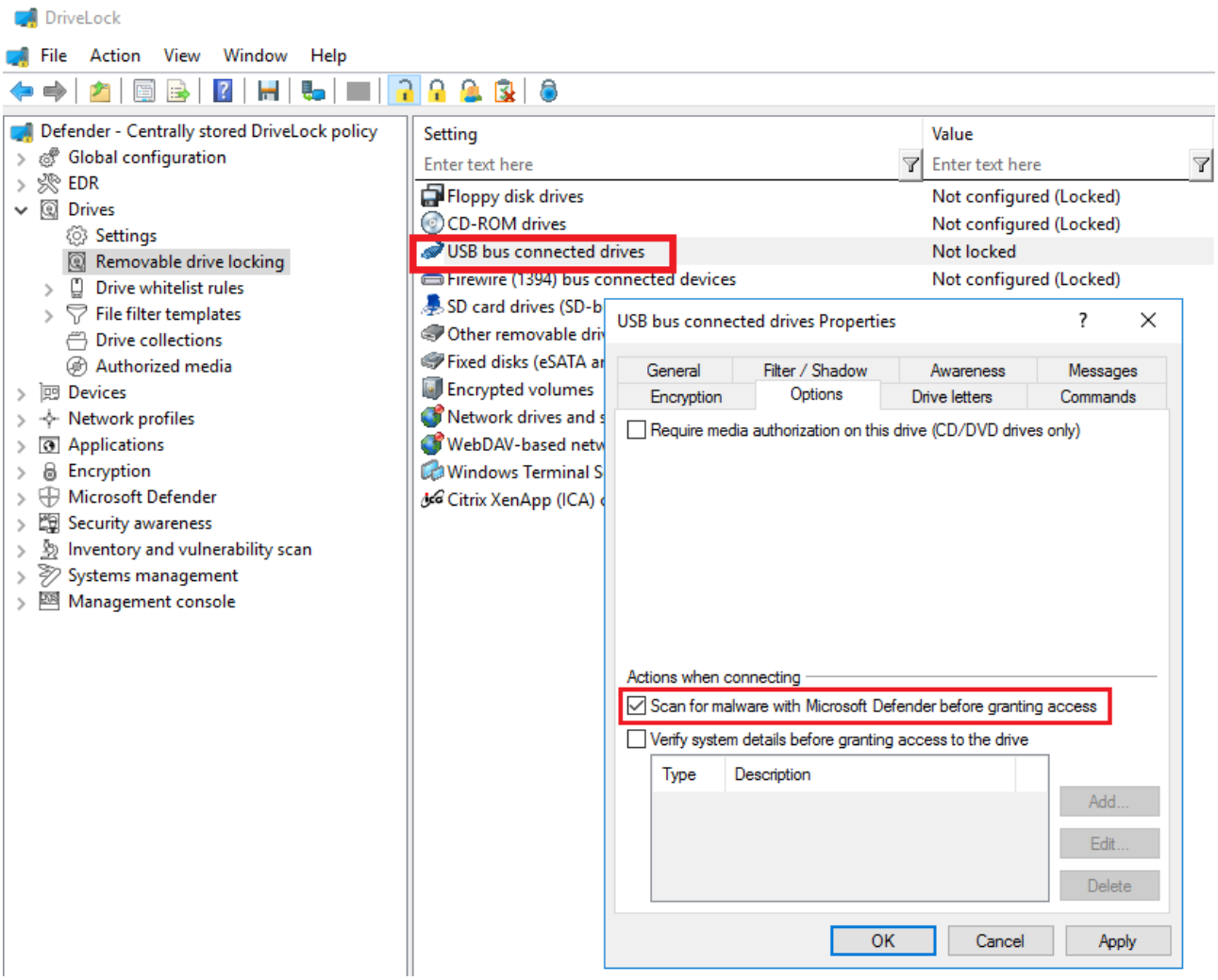
2.5.1 Scanning external drives

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:

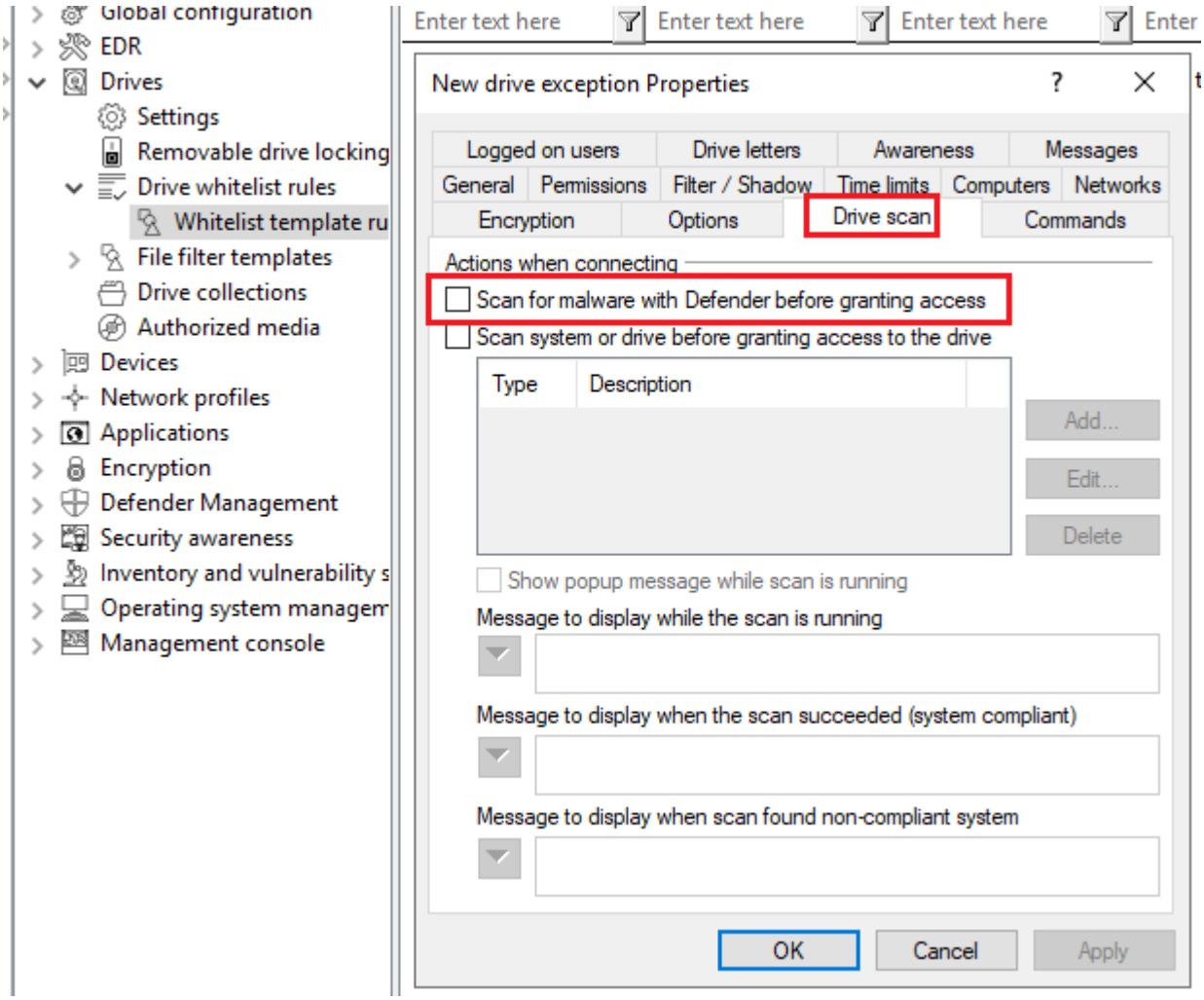
1. Open the **Drives** node in the policy, select the **Removable drive locking** subnode and select the relevant drive to edit it.
2. Switch to the **Options** tab in the dialog.
3. Check the option **Scan for malware with Microsoft Defender before granting access**.



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. In the dialog, switch to the **Drive scan** tab.
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. You can configure the messages to suit your requirements.

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

3 Agent remote control

3.1 Properties of the DriveLock Agent

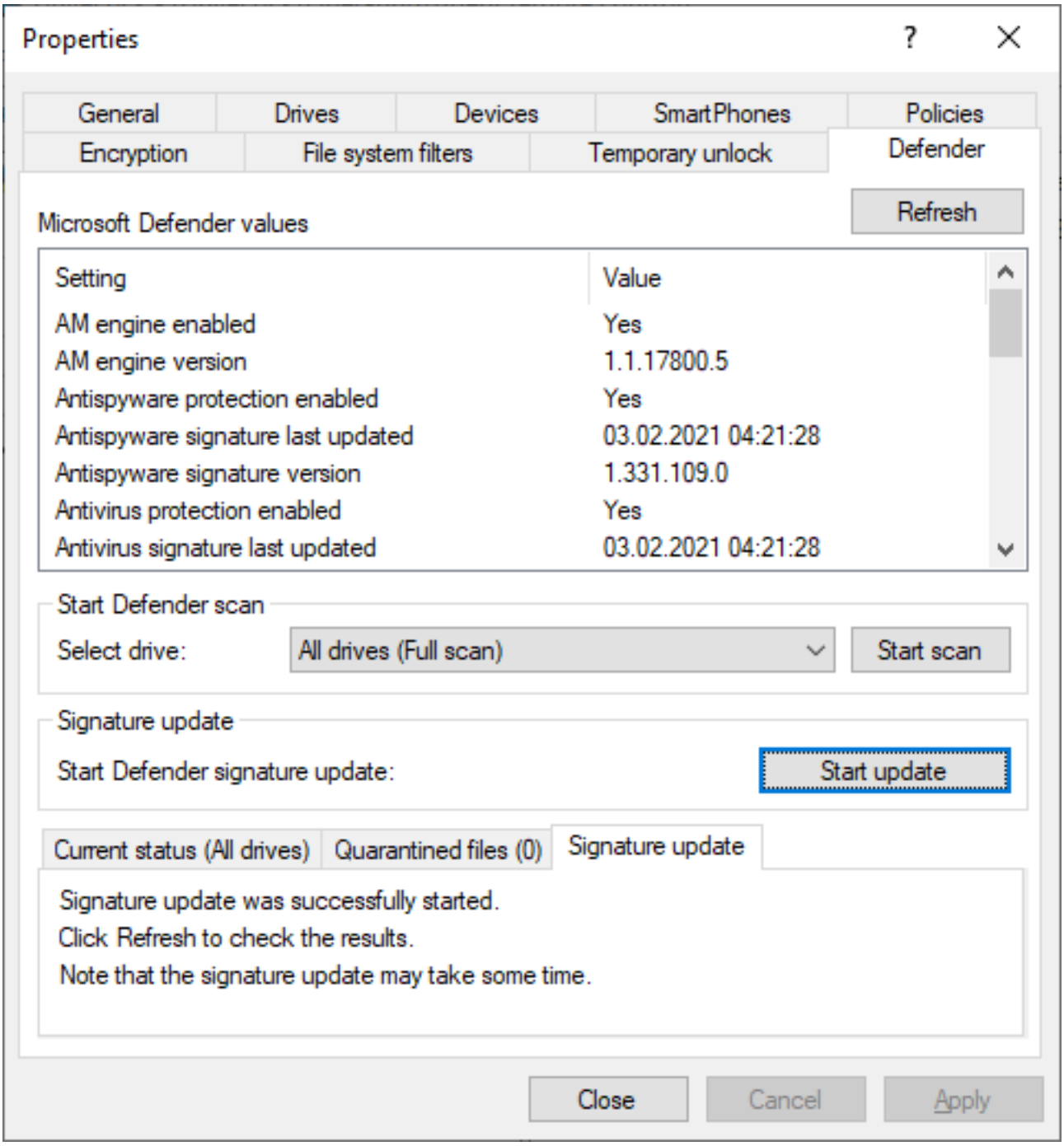
Connect to a DriveLock Agent via **Agent remote control** and open its properties dialog by double-clicking on it.

On the **Defender** tab you can find current information about the Defender status on the respective agent.

Note: Please refer to the DriveLock Administration documentation at DriveLock Online Help for general information on agent remote control.

3.1.1 Options in the Defender dialog

On this tab you can see the time of the last scan on the agent, check whether any errors occurred and, for example, whether antivirus protection is enabled or what version the signature has.



The following options are available:

- Click **Refresh** to reload the values.
- Click **Start Scan** to start a Defender scan immediately. Then if you click **Refresh**, the current status will appear on the corresponding tab.
- Click **Start update** below Signature update to prompt Defender to renew the signature.

- The **Current status** tab provides an overview of the history and result of the last scan performed.
- The **Quarantined files** tab lists all the files in quarantine (not just those from the last scan).
- On the **Signature update** tab you can see the process of the signature update.

3.2 Disabling Defender in the Unlock Agent Wizard

DriveLock Defender Management can be temporarily disabled for individual agents in the unlock wizard. This is convenient if you want to change some Defender settings manually, for example, in order to analyze an agent's behavior, install specific software or remove viruses manually.

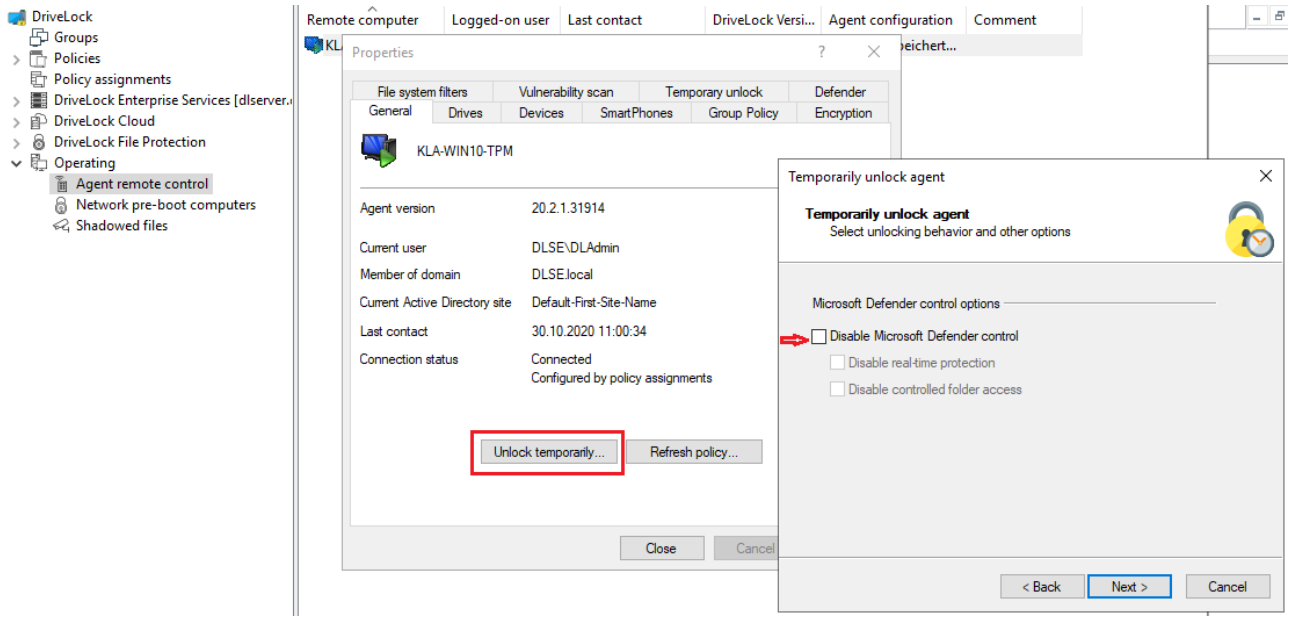
Note: Please refer to the DriveLock Administration documentation at DriveLock Online Help for general information on unlocking the agent temporarily.

3.2.1 Disable Microsoft Defender control

Please do the following:

1. Select the DriveLock Agent you want to disable Defender control on.
2. Open the wizard for unlocking the agent by clicking the **Unlock temporarily** button.
3. Click **Next** until you get to the Defender options.
4. Disable the control for Microsoft Defender as shown below. You can also disable the real-time protection or the controlled folder access here.
5. On the last dialog page, specify how long you want your agent to be unlocked, and then click **Finish**.

Note: Once the temporary unlock is over, DriveLock will reapply the policy assigned to the agent. Depending on the configuration, however, this may imply that manual changes are undone.



3.2.2 Disable Defender on the DriveLock Agent

If you have configured the agent user interface in your policy to allow users to use temporary self-service unlock, they can also temporarily disable Microsoft Defender control.

Note: You can find more information about configuring the agent user interface or self-service unlock in the DriveLock Administration document as well.

4 Events

4.1 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.

4.2 Microsoft Defender events

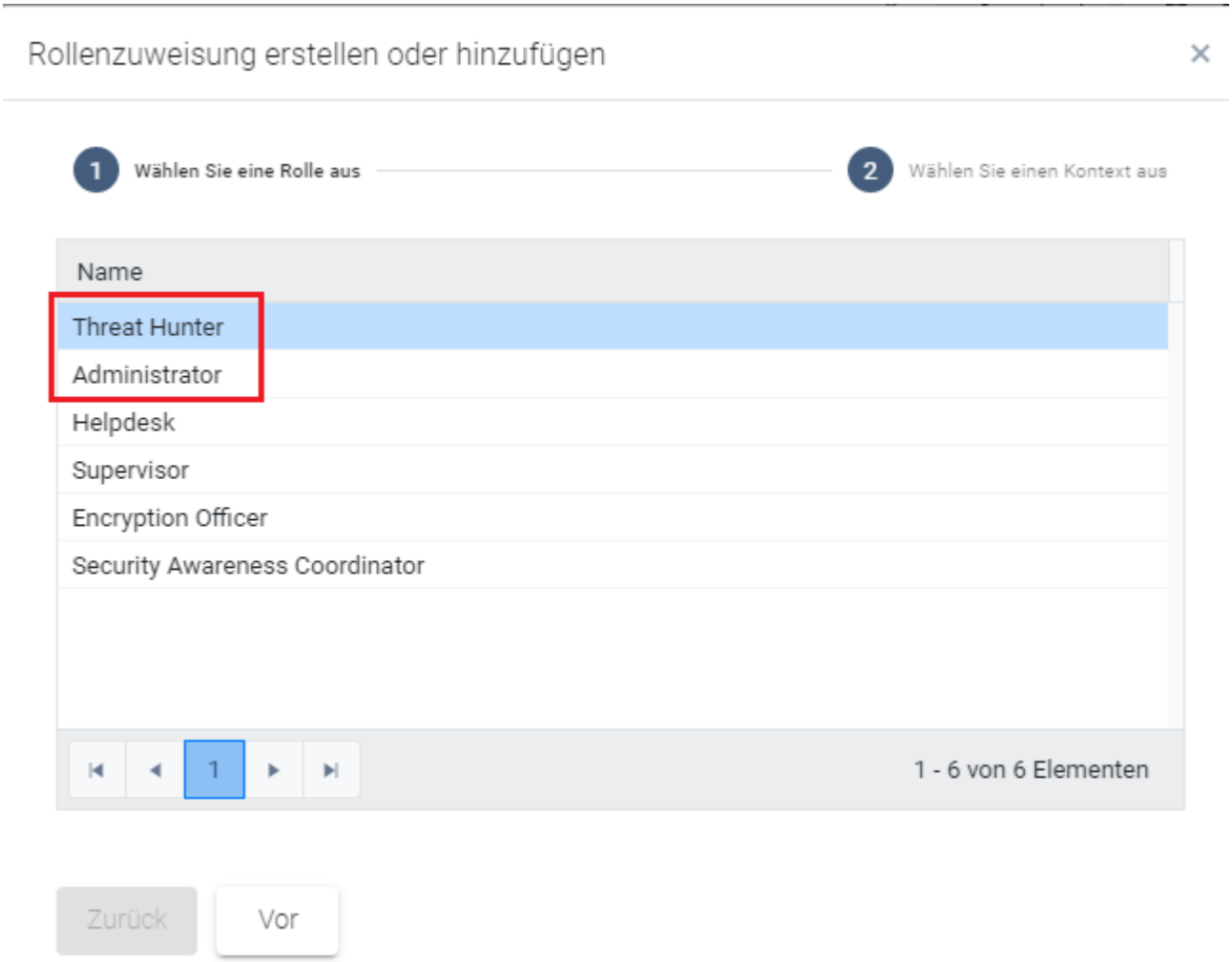
DriveLock Enterprise Service (DES) generates specific events for Defender. You can determine whether these events are sent to the DES and displayed in the DriveLock Operations Center (DOC) in the policy in the **EDR** node, **Events** subnode, **Microsoft Defender**, in the **DriveLock Enterprise Service** column.

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

5 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.

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.

5.1 Dashboard

Description of the widgets on the standard Microsoft Defender dashboard:

- **Protection** status shows the current status of the computers
  - Open threats
    Number of computers with open threats that could not be removed by Microsoft Defender.
  - Signatures or status not up to date
    Number of computers without open threats, whose Microsoft Defender signature definitions have been updated, and whose last status report was no longer than 1 week ago.
  - Protected
    Number of computers whose Microsoft Defender signature definitions are older than 1 week or whose last status message was more than 1 week ago.
  - Inactive
    Number of computers 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.
- **Feature overview**
  Indicates the number of computers having individual Microsoft Defender features enabled.
- **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.
- **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.
- **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.

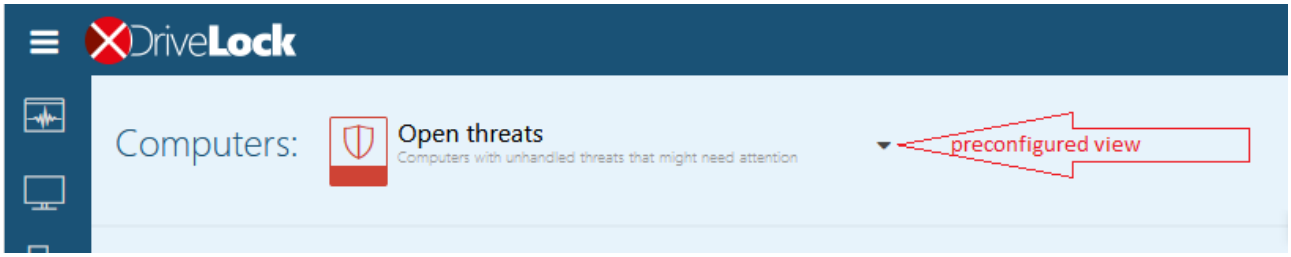
real-time protection

- Inactive: The Microsoft Defender Service is not running

- **Affected computer count history**
  Shows the history of affected computers by number
- **Threat history by severity**
  Shows threat history by severity
- **Threat history by category**
  Shows threat history by category

5.2 View

The **Open threats** view is opened by default as a preconfigured view for the **Computer** list.



By clicking on the down arrow you can select more views from three different areas:

1. **Computer**
   The Computers section will show the affected computers based on the view you choose.
   For example, the preconfigured view **Features to enable** displays the number of computers where Microsoft Defender features are available but not active. 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.
   By clicking on you can display the detailed view for each computer, which is composed 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**

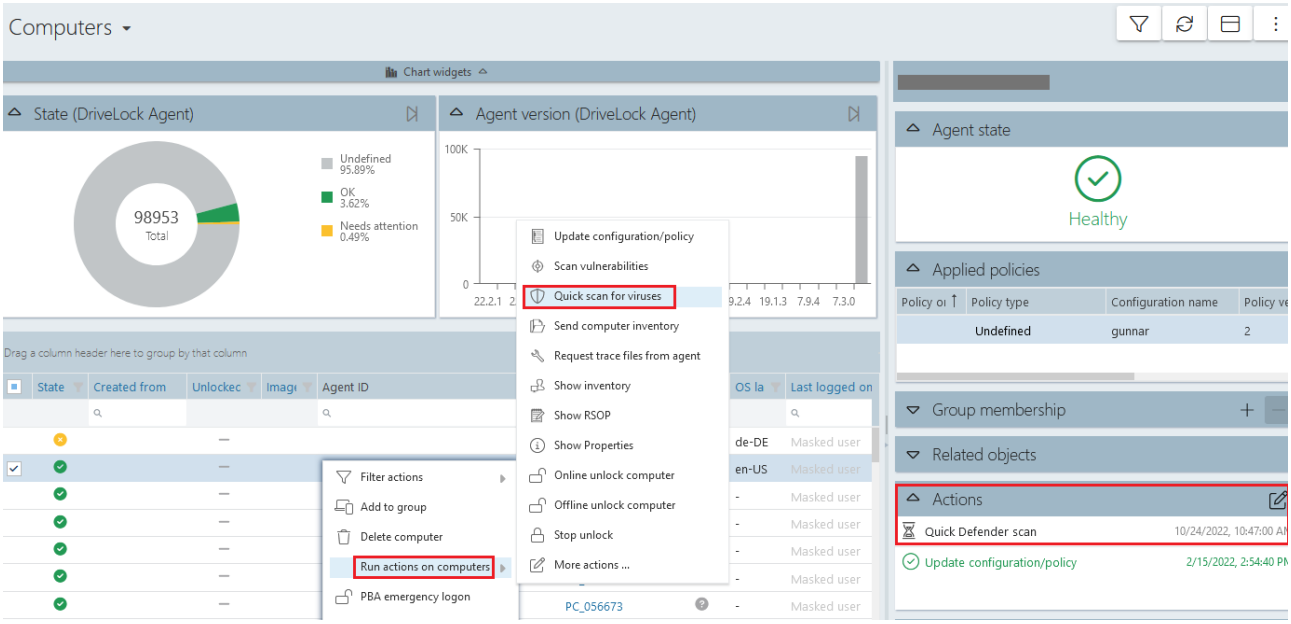
Based on the status of existing threats, they are displayed under open, resolved or suppressed threats. Open threats can be suppressed for the selected computer or for all computers.
The **Open encyclopedia** link will take you to a Microsoft information page where you can get more information about 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**
   Here you can select how the detected threats are grouped (by category or by severity) or whether all suppressed threats are displayed as a preconfigured view.
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.

5.3 Quick scan for viruses

To quickly scan an individual computer for viruses, open the computer's context menu in the **Computer** view, then click **Run actions on computer** and select the **Quick scan for viruses** menu command. The start of this quick scan is displayed in the computer details under **Actions** . If a virus is found, it will be displayed under **Detected threats**.



Warning: The quick scan can only work if a user is logged in to the system locally. Logging in via a remote desktop connection (RDP session) is not adequate because Defender management tasks cannot be performed from the DOC in RDP sessions or Terminal Server / Citrix sessions.

6 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-Wert: DlSvcDefender_LogStatus
- The file **DefenderStatus.json** is then saved in the trace directory.

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.

© 2022 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.