



DriveLock Vulnerability Scanner

Documentation 2022.1

DriveLock SE 2022



Table of Contents

1 DRIVELOCK VULNERABILITY SCAN	
1.1 Requirements	
1.2 Configuration in the DriveLock Management Console	
1.2.1 Vulnerability catalogs	
1.2.1.1 Updating the vulnerability catalogs	4
1.2.2 Configure vulnerability scan	4
1.3 Actions on the DriveLock Agent	5
1.3.1 Vulnerability scan on the DriveLock Agent	5
1.3.1.1 Start vulnerability scan via agent remote control	6
1.3.1.2 Start vulnerability scan via the command line	6
1.4 DriveLock Operations Center (DOC)	7
1.4.1 Vulnerability scan in the DOC	7
1.4.1.1 Vulnerability Scan view	7
2 INVENTORY	
2.1 Hardware and software inventory	9
2.2 Client compliance	
2.2.1 Client compliance settings	
COPYRIGHT	

1 DriveLock vulnerability scan

DriveLock Vulnerability Scanner allows you to automate regular scanning for known Windows and third-party vulnerabilities.

To do so, DriveLock accesses a database that is updated several times a day. The DriveLock Operations Center (DOC) then displays the findings in a separate new view with a risk and impact assessment, including missing patches, outdated software or libraries of known vulnerabilities.

1.1 Requirements

Licensing options:

- Vulnerability Scanner Basic: Scan for operating system vulnerabilities (OS Vulnerabilities)
- Vulnerability Scanner Extended: Scanning for operating system vulnerabilities and third-party vulnerabilities

System requirements:

- DriveLock: starting with version 2020.1 HF1
- Agent operating systems: Windows 8.1, Windows 10; Server 2012R2, 2016, 2019

1.2 Configuration in the DriveLock Management Console

1.2.1 Vulnerability catalogs

The vulnerability scan is based on catalogs that are first uploaded from the cloud to the central DriveLock Enterprise Service (DES) and then distributed to DriveLock Agents.

There are separate catalogs for operating system and third-party vulnerabilities.

In order to load the catalogs, the DES accesses

- a web service at https://service.drivelock.cloud and
- a configuration at https://download.drivelock.com/vulnerability-defintions/catalogs.json.

When setting up the vulnerability scan for the first time, it may take a while until the catalog is completely loaded on the DES. Any later updates only transfer the modifications and are thus considerably faster.



Mote: After entering the license, either restart DES or update the catalogs in the Management Console.

1.2.1.1 Updating the vulnerability catalogs

Please do the following:

In the context menu of the respective DES, click **All Tasks** and then **Update vulnerability**

catalog now (see figure).



1.2.2 Configure vulnerability scan

Vulnerability scanning is disabled by default; you must first enable and configure it in the policy where you licensed Vulnerability Scanner.

Please do the following:

- 1. Go to the Inventory and vulnerability scan node and open the Settings.
- 2. Open vulnerability scan.

 VulnerabiltyScan - Centrally stored DriveLock ◇ Global configuration > EDR > Drives > Devices > Network profiles Applications Encryption Microsoft Defender Security awareness > Inventory and vulnerability scan Systems management > Management console 	Setting Enter text here Hardware and software inventory Client compliance reporting settings Vulnerability scan Properties General Enable scanning for vulnerabilities Schedule When the agent service starts (not recommended) Every 30 Every 30 On demand (triggered by command line or remote control) Scan priority Normal priority Background processing priority Idle priority	Value Enter text here Not configured Configured X
	 Normal priority Background processing priority Idle priority 	
	OK Cancel	\pply

- 3. Check Enable scanning for vulnerabilities.
- 4. If you select the **On demand (...)** option, the vulnerability scan must be started via the agent remote control or alternatively via the agent command line.
- 5. Using the options to **Scanner priority** you can set the process priority of the scanner on the agent. If you want to reduce CPU usage and accept a longer runtime, you can select **Background processing priority** or even **Idle priority** here.

1.3 Actions on the DriveLock Agent

1.3.1 Vulnerability scan on the DriveLock Agent

The vulnerability catalogs are downloaded from the DriveLock Enterprise Service (DES) to the DriveLock Agent and are updated on a regular basis.

You can find the catalogs on the agent under:

- C:\ProgramData\CenterTools DriveLock\VulScan\3P and
- C:\ProgramData\CenterTools DriveLock\VulScan\OS.

The actual vulnerability scan is performed by **DLVulScan.exe**. The **DLOvalHelper.exe** is also involved in transferring the catalogs to the agent. Both are located in the DriveLock directory on the agent.

1.3.1.1 Start vulnerability scan via agent remote control

Please do the following:

- Connect to the respective agent via the **agent remote control**.
 For more information on remote agent control, see the Administration Guide at DriveLock Online Help.
- 2. Click the **Start scanning** button.

DriveLock	Remo	te computer	Logged-on	user Last c	ontact	DriveL	ock Versi	Agent cor	figuration
 Device Scanner Groups Policies Centrally stored policies Computer-specific policy customiz Active Directory / Local computer p Configuration files Policy assignments Policy assignments PriveLock Enterprise Services [dlserver.u) DriveLock Cloud OpriveLock File Protection Operating Agent remote control 	KLING KL	Properties General Encryption Vulnerability So Last scan Detected vulner Vulnerability I Q < none >	Drives File syst canner erabilities from la D Der	Device em filters Licensed Never Re-upload st scan	es Sr Vulnerabil d results	martPhones lity scan	Group Temporary Start sca	p Policy y unlock	peichert
୍ଷିତି Network pre-boot computers ≪୍ୱି Shadowed files		< Comment			Close	Ca	ncel	> ^ Apply	

- 3. Click the **Re-upload results** button reload the scan results.
- 4. Or click **Reload Catalog** to reload the scan catalog.

Mote: These two options are intended mainly for troubleshooting.

5. If vulnerabilities were detected during the last scan, they will be displayed with ID and description in the dialog.

1.3.1.2 Start vulnerability scan via the command line

Actions can be triggered on the agent via command line.



For more information on **obtaining the agent status via the command line**, refer to the Administration Guide under DriveLock Online Help.

Trigger actions via the following command lines:

drivelock -vulscan: Start scanning for vulnerabilities

drivelock -vsupload: Reload results

drivelock -vsresetcatalog: Reload or reset catalogs

The options are also available via "drivelock /?":

-resetdeviceusagepolicy ... Reset usage policy shown list for dev Vulnerability scan: -vulscan ... execute vulnerablity scan -vsupload ... re-upload last vulnerablity scan result -vsresetcatalog ... reload vulnerability catalog

1.4 DriveLock Operations Center (DOC)

1.4.1 Vulnerability scan in the DOC

You can see the status of the vulnerability scan on the agents in the DriveLock Operations Center (DOC) in the **Vulnerability Scan** view.

To indicate the criticality of a vulnerability, the Common Vulnerability Scoring System is used as a rating system. The base score reflects how critical a vulnerability is. It ranges from S1 (uncritical) to S10 (highest criticality).

For more information about the DOC, see the **DriveLock Control Center** documentation on DriveLock OnlineHelp.

1.4.1.1 Vulnerability Scan view

The default preconfigured view is **High risk computers**. This includes all computers that have open vulnerabilities with a base score > = S7.

OriveLock

	Computers: I High risk computers Select preconfigured view here
<u>Ģ</u> p	
G	Computers
B	
	Computers with appressed vulnerabilities Computers with appressed vulnerabilities Computers with appressed vulnerabilities Computers with a least one suppressed vulnerability
ъ¢	CVE list
Ð	All items Displays all entries without filtering and grouping Displays all entries without filtering and grouping Shows vulnerabilities that have been suppressed for all computers
\diamondsuit	Detected vulnerabilities
Ø	All items Displays all entries without filtering and grouping
â	
	Apply Open in new tab

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

- 1. Computers (computer overview)
 - Displays the open or suppressed vulnerabilities for a computer
 - Allows suppressing the vulnerability for one or for all computers
- 2. CVE List (Common Vulnerabilities and Exposures (CVE®))
 - Shows the existing CVEs
 - -> Allows suppressing for all computers
 - Displays the computers at risk in the detailed view of a CVE
 -> Allows to navigate to the vulnerable computers (opens the Detected Vulnerabilities list).
- 3. Detected vulnerabilities (vulnerability overview)
 - Shows when a specific vulnerability was detected for a computer
 - Allows suppressing the vulnerability for one or for all computers

2 Inventory

The DriveLock Agent retrieves information about the current hardware or software of the client computer regularly or at specified times; this information is then transmitted to the DriveLock Enterprise Service. The collected data can be analyzed centrally via the DriveLock Control Center (DCC) or the DriveLock Operations Center (DOC). That way, you get a quick overview of the programs or software patches that are installed on your computers.

2.1 Hardware and software inventory

Here you can specify when the DriveLock Agent collects certain information, and whether this feature stays disabled or not.

Please do the following:

1. Go to the **Inventory and vulnerability scan** node, open the **Settings** sub-node, and then click **Hardware and software inventory**.

> Image: Global configuration Enter text here Image: Enter text here > Image: State S	Inter text here
> ※ EDR Image: Hardware and software inventory No > Image: Devices Image: Client compliance reporting settings No	Not configured
Drives	lak an dimond
N DP Devices	vot configured
A Network profiles Galaxies Co	Configured
 Network profiles Applications Encryption Defender Management Security awareness Inventory and vulnerability scan Settings Systems management Systems management Management console Properties Inventory collection Collect device information Collect dive information Collect patch and hotfix information Schedule When the agent service starts (not recommended) Every 30 days Every 30 days Condemand (triggered by command line or remote control) 	X

2. To allow the agent to collect information about the computer, select **Enable collecting inventory data**.

- 3. Choose which data you want the agent to collect and send to the DriveLock Enterprise Service.
- 4. Next, define the time when the agent starts gathering information and when the data is sent to the DriveLock Enterprise Service.
- Note: Please note that it takes some time for the agent to collect the data and the workload on the system is slightly higher than it would be otherwise. Therefore, the scan will also be delayed for a few minutes after the agent is started (if you have selected this option).

2.2 Client compliance

This option allows you to specify the parameters that will be checked on the computer for the client compliance status.

2.2.1 Client compliance settings

Please do the following:

1. Go to the **Inventory and vulnerability scan** node, open the **Settings** sub-node, and then click **Client compliance reporting settings**.

🦪 VulnerabiltyScan - Centrally stored DriveLoc	Setting	Value
> 💣 Global configuration	Enter text here	Enter text here
> 🔆 EDR	Hardware and software inventory	Configured
> 🕘 Drives	Client compliance reporting settings	Not configured
> Per Devices	SVulnerability scan	Configured
 Devices Network profiles Applications Encryption Defender Management Security awareness Inventory and vulnerability scan Settings Systems management Management console 	Vulnerability scan Properties Quinerability scan Properties Quinerability scan Quinterability windows Update status Quinterability no more than 30 available updates Windows firewall Quinterability Windows firewall enabled and running Windows Security Center At least one product of the following product types must be Installed Running Quinterability windows Quinterability Anti-Spyware Quinterability	p to date
	OK Cancel	Apply

- 2. Select the required settings.
- 3. On the **Commands** tab you can configure executable programs or scripts of your choice.

Add them to the policy file store first and select them from there. The DriveLock Agent calls the programs or scripts on the clients; they must return 1 for compliant and 0 for non-compliant.

The DriveLock Control Center (DCC / Helpdesk) displays the compliance status of the agents in detail.





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.

