

Management of Microsoft Defender Antivirus More than just a Microsoft antivirus scanner configuration



convenient - integrative - holistically secure

- Centralised configuration for all prevention tools via the DriveLock management console eliminates the need for additional management solutions such as Microsoft Intune or SCCM.
- Defender settings can be tailored to the security features of DriveLock application control.
- All Defender AV settings can be easily and quickly configured within a DriveLock policy, without having to distribute individual group policies.
- Via the DriveLock management console the use of external drives can be linked to the result of a Defender AV scan.
- Threats from AV scans can trigger alerts in the DriveLock Endpoint Detection & Response (EDR) solution, which will then trigger automated processes in response (launch of an information campaign, execution of scripts, etc.).
- The defender's view in the DriveLock Operations Centre meet legal obligation requirements and enables compliance reporting.

Management of Microsoft Defender Antivirus

Pre-installed in Windows 10, **Microsoft Defender Antivirus** is real-time antivirus protection developed by Microsoft to detect and remove malware and other potentially unwanted programs.

DriveLock **integrates** the Microsoft Defender Antivirus management into its Zero Trust platform and enables shared centralised management of DriveLock prevention tools - **application control, interface control, and EDR - with the Microsoft antivirus scanner.**

This allows DriveLock customers to further minimise the risk of losing data due to malware, spyware, or ransomware and manage everything from a centralised platform within DriveLock.

The DriveLock Management Console can be used to configure the following Windows Defender client settings using DriveLock policies:

- Scan settings for file accesses and response options if malware is found
- Enable rules for file checks or processes
- Regular scan checks with the date, time, frequency and type of response
- Use of the virus scanner when connecting external drives and automatic blocking of access if malware is detected
- Overview of the nature and content of end-user notifications

DriveLock EDR functions enable additional responsiveness through an integration with Microsoft Defender Antivirus. When malware is detected, **automatic processes can be enabled to** which effectively prevent further propagation, such as shutting down or isolating computers on the network.

The state-of-the-art **DriveLock Operations Centre** with its own anti-virus dashboard provides a quick overview of the current protection level allows administrators not only to perform a detailed analysis of individual systems but also to perform additional activities in the event of security incidents, such as starting a complete scan, a computer or manually updating threat definitions.

An overview of detected threats, Defender security audit results, and the health of DriveLock protected computers helps managers assess and demonstrate the effectiveness of their compliance and protection measures.

= 🗙 Drive	Lock								ያ Administrator@roc	ot 🤝 🌐 en
Dashboard	Standard Dashboard Application Control	Dashboard	Security Awareness	Device Control Dashboa	ird Vulnerab	ility scan Microsoft Defende	er Disk Encryption +			
Computers	Protected computers (Total)		Affected computers	(Total)		Computer reporting (Total)		Protecti	ion Status	
Groups		\bigcirc			\wedge			\square	\square	\square
Security Awareness	7	\bigcirc	7		ΔīΖ	15	\cup	Affected computer Not up to date 7 3	Protected 7	Inactive
Inventory								46.67% of 15 20.00% of 15	46.67% of 15	6.67% of 15
Events	Threat Category Password stealer		_			Threat Severity				
⊶¢ edr	Trojan downloader Worm	-			-					Low
Defender	Backdoor Trojan		-		-					Moderate
Vulnerability Scanner	Exploit Tool Trojan dropper									High 15.15% Severe
Tasks	Virus Behavlor	-								39.39%
2 Accounts	Ransomware 0 1	2	3 4	5	6					
	Affected computer count history			Threat history by severity						
	- Low - Moderate - Severe					- Low - Moderate - High - Severe				
	8					35	1			
	· · · · · · · · · · · · · · · · · · ·					30				
	6					25				
	4				_	20				
	3				L	15				
	2					10				
	1					5				
	0 5/8/2020	5/9/2020	5/10/2020	5/11/2020		0	8/2020 5/9/2020	5/10/2020	5/11/2020	

Advantages of the DriveLock Microsoft Defender Management at a glance

- > The configuration of DriveLock and Microsoft Defender Antivirus security settings through a single policy
- Management of the system environment using dashboards and modular overview graphics via the central and web-based DriveLock Operations Centre

Simple configuration options

CriveLock	–	<
📢 File Action View Window Help	- 5	×
◆ ⇒ 2 🖾 📓 🖬 👦		
Image: Microsoft Defender - Centrally stored > Image: Global configuration > Image: Store Stress > Image: Devices > Image: Devices <td>soft Defender' in this section.</td> <td>^</td>	soft Defender' in this section.	^
 > ☐ Windows Defender Antivirus > ☐ Windows Security > ☐ Windows Security > ☐ Security awarenes > ③ Inventory and vulnerability scan > Ø Systems management > ☐ Management console With DriveLock you can easily control the behavior of Microsoft Defender on your clients. If you prefer to configure Microsoft Defender via GPO you can disable the integration of Microsoft Defender into DriveLock.	Enable/disable Microsoft Defender control Current status: Enabled	
et of scans		
Specify the weekdays and times for automatic scans. Some threats may require an additional full scan for complete remediation and removal. You can also schedule this here.	Change Day of the week to run a scheduled scan: Not configured Time of day to run a scheduled scan: Not configured Scan type to use for a scheduled scan: Full system scan Day of the week to run a scheduled full scan to complete remediation: Every Day Time of day to run a scheduled full scan to complete remediation: 0:00	
		~

Automatic response to detected threats, such as blocking user access or applying tighter security settings

Holistic security from a single source:

DriveLock offers Defender Antivirus Management as a building block of its Zero Trust platform to implement a comprehensive security strategy.

