

Antimalware Agent Updates

March 2023

After being installed on a Windows managed device, the Antimalware Agent auto-updates when a new agent version is released to the cloud service (i.e., the same repository from which signature updates are pulled). This document lists the released Antimalware Agent versions and fixes.

- ♦ [“How to Know What Version is Installed” on page 1](#)
- ♦ [“Version 7.8.2.254” on page 2](#)
- ♦ [“Version 7.6.3.212” on page 2](#)
- ♦ [“Version 7.5.3.195” on page 2](#)
- ♦ [“Version 7.4.3.146” on page 2](#)
- ♦ [“Version 7.2.2.92” on page 3](#)

How to Know What Version is Installed

In ZENworks Control Center, you can use the Device Malware Signature Version dashlet located on the Security Dashboard to view the Antimalware Agent version installed on each managed device.

By default, managed devices check for Antimalware Agent updates every 4 hours. If an update is available, it is installed immediately. You can customize how often the check occurs by using the [Antimalware Agent Schedules](#) configuration settings at the zone, device folder, or device level. ZENworks Control Center navigation for these schedules is shown below:

- ♦ **Zone:** Configuration > Management Zone Settings > Security
- ♦ **Device folder:** Folder object (*Details* link) > Settings > Security
- ♦ **Device:** Device object > Settings > Security

Updates do not typically require a reboot, but the schedule lets you postpone potential reboots if desired. For more information about configuring the schedules, see [“Antimalware Agent Schedules”](#) in the *ZENworks Endpoint Security Antimalware Reference*.

To force managed devices to check for and install updates, use the “Update Antimalware Agent” action in the Device Malware Signature Version dashlet.

Version 7.8.2.254

Released: March 21, 2023

Change log from version 7.6.3.212 to 7.8.2.254

New Features and Improvements:

- ♦ The security agent now automatically scans USB devices before users log into the Windows system.
- ♦ Added support for Windows 11 Enterprise Multi-Session (22H2).
- ♦ Added support for Windows ARM64 CPUs.

Resolved Issues:

- ♦ Fixed an issue that caused the security agent to create database registry files on partitions smaller than 1 GB.
- ♦ In certain scenarios, endpoints encountered critical errors (BSOD) when the Antimalware module was active.
- ♦ Fixed an issue that caused the Antimalware module to prompt users to take actions on clean files.
- ♦ Fixed an issue where the security agent caused high CPU usage on Microsoft Windows Server 2019.
- ♦ Fixed an issue that was causing high disk usage when scanning certain SSD drives.

Version 7.6.3.212

Released: September 21, 2022

New Features and Improvements:

Added support for Windows 11 22H2

Resolved Issues:

- ♦ Fixed an issue that affected a few product files after an unexpected shut down.
- ♦ Resolved an edge-case scenario where the Antimalware module displayed On-Access as disabled in the local interface even though it was enabled in the policy.
- ♦ Security fixes

Version 7.5.3.195

Released: July 7, 2022

Resolved an issue with the update module of the Endpoint Security Endpoint SDK. The issue manifests in the form of an update error (error code -1016) visible in the Update.

Version 7.4.3.146

Released: February 4, 2022

Resolved issues:

- ♦ Fixed the following security vulnerability:
 - ♦ CVE-2021-4199

- ♦ CVSS Score: 7.8
- ♦ Risk Level: High
- ♦ Vulnerability details: Allows a remote attacker to escalate local privileges to the SYSTEM.
- ♦ **NOTE:** CVE-2021-4198, regarding a crash in the `messaging_ipc.dll`, has been recently published. This vulnerability was previously fixed and shipped in September 2021.

No reboot is required.

- ♦ Fixed an issue where the integrated Support Tool, when run manually to collect log files for troubleshooting purposes, would sometimes remove directories in the same destination path as the saved logs.

Version 7.2.2.92

Released: October 28, 2021

Resolved issues:

- ♦ Resolved an issue where the Endpoint Security Service generated high RAM usage when the endpoint received new policy settings.
- ♦ Resolved an issue where the Endpoint Security Console service randomly created a certain file on endpoints.
- ♦ Addressed a specific scenario where the product caused critical errors (BSOD). The issue is now fixed.
- ♦ Resolved an issue where the Endpoint Security Console service crashed after installing the security agent on a different partition in Windows Server 2012.
- ♦ In some cases, the agent installation failed on endpoints with Windows Defender enabled. The issue is now fixed.
- ♦ Fixed two security vulnerabilities in the update module:
 - ♦ [CVE-2021-3459, CVSS Score 7.8, High](#)
 - ♦ [CVE-2021-3823, CVSS Score 7.1, High](#)

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/en-us/legal>.

© Copyright 2023 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (Micro Focus) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

