

Dell Data Security Technical Newsletter

Volume 82, January 2022



Important Update: Dell Endpoint Security North America Phone Number Has Changed

Dell Endpoint Security has a new number for support tickets. Customers in North America should now call +1 877.459.7304, ext. 6236710.

Netskope Version 91

Netskope Release 91 is available, including new Advanced Analytics for Cloud Firewall and several product fixes.

Version 91 Release Notes can be found [here](#).

Apache Log4J Vulnerability CVE-2021-44228

In December of 2021 vulnerability CVE-2021-44228 was disclosed, which affects the common logging library Log4j2. Dell Security Management Server and Dell Security Management Server Virtual version 11.2 and earlier are unaffected by CVE-2021-44228.

More information can be found in the [Additional Information for Dell Endpoint Security with regard to Apache Log4j Remote Code Execution Vulnerability \(CVE-2021-44228\)](#) article.

VMWare Carbon Black Cloud Windows Sensor 3.8 now available

Version 3.8 of the VMWare Carbon Black Cloud Windows Sensor is now available for download from the VMWare Carbon Black Cloud Console.

More information about the release can be found on the [Release Notes](#) page.

Dell Trusted Device 4.0

Dell Trusted Device 4.0 is now available, with new features and functionality.

The following platforms are now supported by BIOS Verification:

- Latitude 5421
- Latitude 5521
- Precision 3560
- Precision 3561
- Precision 5560
- Precision 5760
- Precision 7560
- XPS 9310
- XPS 9310 2-In-1

These platforms are now supported by Intel ME Verification:

- Latitude 5320

- Latitude 5420
- Latitude 5421
- Latitude 5520
- Latitude 5521
- Latitude 7320
- Latitude 7320 2-In-1
- Latitude 7420 16 Technical Advisories
- Latitude 7520
- Latitude 9520
- Precision 3560
- Precision 3561
- Precision 5560
- Precision 5760
- Precision 7560
- Precision 7760
- XPS 9310
- XPS 9310 2-In-1

Resolved Issues in DTD 4.0

- A rare issue resulting in a computer crash after applying Windows updates to a computer protected by Trusted Device. [DPS-4142]
- An issue resulting in mishandled validation of SAN leaf certificates when Trusted Device is installed on a non-English operating system. [DPS-4197]
- An issue resulting in BIOS Events & Indicator of Attack incorrectly writing duplicate Information events to Event Viewer. [DPS-4232]

[What is Dell Trusted Device? | Dell US](#)

KB Article Updates for Dell Encryption Activation Issues

Dell Support has updated various KB articles to assist with troubleshooting activation issues with Dell Encryption. [KB article](#) has been updated with several tips and information to help with troubleshooting.

Dell Data Security Chat

For U.S. customers only, [Chat](#) support is now available Monday through Friday, 7 a.m. to 7 p.m. CST.

Dell Data Security ProSupport for Software

- 24x7 support and issue resolution from a team of technicians.
- Within the U.S., the **dedicated number is 877.459.7304, ext. 6236710.**
- For a list of in-country phone numbers, click [here](#).

NEW: Dell Data Security Advanced Support for Software

- Direct and easy access to your own dedicated security expert.
- Support for all of your Dell endpoint security software.
- Personalized support including customized communication plans, health checks and more!

For more information, click [here](#) or contact your account executive.