Adaptive Defense and Endpoint Protection

External Release Notes

Correction Changelog

Table of Contents

1. Scope of the document

What kind of information is contained within the Release Notes?

The Adaptive Defense and Endpoint Protection Release Notes lists a changelog of fixed issues and corrections of the Adaptive Defense products (Adaptive Defense and Adaptive Defense 360) and Endpoint Protection products (Endpoint Protection and Endpoint Protection Plus) version to version.

As a lot of the modules are common across products, we have gathered the bugfixing list in a single document. Nonetheless, should a particular issue apply only to a particular product, it will be specified as such.

The list of solved issues is split according to the module they apply to, whereas it is the Adaptive Defense console, protection or agent. Moreover, there could be other general improvements that have been added as a separate item.

2. May 2017 - Changes included in version AD 2.4 // EPP 7.70.00

2.1. Protection 7.70.00

2.1.1. New features:

- New anti-exploit technology.
- Compatibility with Server Core https://msdn.microsoft.com/en-us/library/dd184075.aspx

For more information on what's new in version 2.4 of Adaptive Defense products and 7.70.00 of Endpoint Protection products, click here.

2.1.2. Changes and improvements:

- **Improved logs**
- **Improvements to Block mode with an advanced user:**
  - Permission inheritance.
    - Whenever an unknown process tries to load, we'll make a query and apply the reply to all other operations performed by the process (loading of unknown DLLs).
    - Whenever a known process tries to load unknown DLLs, we'll make a query concerning the first of them, and will apply the reply to all other unknown DLLs that the process tries to load.
  - If the pop-up message that requires user interaction times out, a reminder will be displayed locally.
- **Exclusion management**: Unification of exclusions between the advanced protection and the antivirus protection.
- **Infection source identification**.
- **Improved sending of files:**
  - The size of the file being sent is now included.
  - Management of unsent files.
- **Consistency between the status of the AV and/or advanced protections** displayed in the tooltip and in the local console.
- **Modifications to the installer:**
  - Changes to the text strings displayed during the uninstall process.
  - Avdetect.ini: Updated the protection data.
  - PSSDET: Improved detection of competitive antivirus solutions.
  - Improved Generic uninstaller
- **Modifications to the firewall:**
  - Improved domain filtering using blacklists for YouTube and Facebook.
  - Improved fragmentation management in Network Provider (NNSPRV.sys).
  - Improved management of multiplexers, affecting connectivity performance in virtual environments.
  - Support for IPv6 traffic from Microsoft Teredo hosts.
  - Corrections to certificate parsing in NNSHTTPS.sys.
  - New public/private IP feature. Ability to send information upon opening a connection whose actual source is an internal network. Handling of Remote Desktop (RDP) connections.

2.2. Agent 7.71.00

- Solved issues related to how the upgrade is scheduled at the shutdown. Under some circumstances, existing group policies were removed or not considered.
- Solved knowledge update error (internal configuration file was corrupted).
- Solved one specific scenario where changes in the console were not propagated to the endpoint.

3. November 15th, 2016 - Changes included in version AD 2.4 // EPP 7.70.00

3.1   Protection 7.65.00

- Fixed connectivity problems when end users were moving from one network with a configured proxy to another one with different network configuration.
- Full support Windows 10 Anniversary Edition (already available in protection version 7.62.00).
- Solved problem when sending unknown samples to Panda servers. This incident could lead to performance problems (high CPU usage of **psanhost**) and bandwidth consumption problems in some situations.
- Fixed spam detection ratio problem and performance in some Exchange servers.
- Fixed BSOD problem associated to the firewall/network infrastructure. This fix affects as well as some network interception issues detected in the previous firewall drivers.
- Fixed some scenarios that lead to errors 2081 and 2123, when installing the protection.
- Fixed bug that was preventing psinfile driver from unloading when coexisting with Novell client.
- Fixed punctual integration error when installing the Android protection.
- Fixed performance problem of a Panda related MSI installer.
- Fixed some discrepancies in WSC in the detected protections.

Changes in local desktop alerts (popups):

- Adaptive Defense malware blocking.
- Removed **Block** button for users without privileges.
- Hardening mode: better management of local alerts – only in Adaptive Defense 360

3.2   Console 2.3.5 // 7.65.00

- Removed the checkbox of rebooting the endpoint when launching an on-demand analysis.
- Configurable FROM field in SMTP alerts.

3.3   Agent 7.65.00

- Solved problem occurring when launching the upgrade in 64 bits. The protection was not upgraded. The box was shown in the console as "**pending for reboot**" or "**upgrade failed**".

3.4   Other improvements

- Generic uninstaller included in the protection installer.
- Statistics are zip-compressed before being uploaded to the SRF Panda servers.
- Changes in the SRF retries management (associated to the unknown samples delivery).
- Other minor improvements in detection, firewall and IoCs.

4. September 28th 2016 - Changes included in version AD 2.3.1 // EPP 7.61.00

Find the Release Notes for Protection version 7.62.00, Protection version 7.60.00.0010 and Agent 7.62.00.

4.1   Protection 7.60.00.0010

- Solved problem when sending unknown samples to Panda servers. This incident could lead to performance problems (high CPU usage of **psanhost**) and bandwidth consumption problems in some situations.

- Detection improvements.

4.2   Protection 7.62.00

- Fixes associated to version 7.60.00.0010.
- Fixed problem with new installations in W10 Anniversary Update, that was generating BSOD – unsigned drivers - in some scenarios (UEFI, Secure Boot, 64 bits, etc.)
- Fixed spam detection ratio problem and performance in some Exchange servers (see IMPORTANT NOTE below).
- Fixed bug that was preventing **psinfile** driver from unloading when coexisting with Novell client.
- Removed the checkbox of rebooting the end-point when launching an on-demand analysis.

4.3   Agent 7.62.00

- Solved problem with Home/Starter versions of the Windows Operative Systems, when the upgrade cannot take place at the shutdown.

- Solved problem when programming the upgrade in some 64 bits Operative Systems. The upgrade was not programmed and thus was not taking place. Box was shown as Pending for reboot in the console.

IMPORTANT NOTE: This version is only available for Windows 10 and Windows 2016 servers.