RELEASE NOTES

Security Manager | AV Defender

Security Manager | AV Defender is an integrated AV offering available for all N-able clients as a licensable option who are on N-central 9.3 or above. Management and deployment are done through your N-central server.

AV Defender Update Version 5.3.31.774

Issues Resolved in this build:

- An issue has been resolved for Windows 10 TH2 systems.
- In some situations, Windows 10 systems displayed Blue Screen when scanning EFS encrypted files through the System Redirector and has now been resolved.
- An issue where Advanced Threat Control caused delays on loading websites in IE when folder redirection was activated in Group Policy Object has been resolved.
- Vulnerabilities ZDI-CAN3749 and ZDI-CAN-3829 (Zero Day Initiative) have been resolved.
- In some cases, Endpoint Security could not be installed on machines running Wyse TCX and has been resolved.
- When installing Endpoint Security with AVC on Windows 10 x64 systems, some machines entered recovery mode and this issue has now been resolved.
- OpenSSL vulnerability CVE02016-2107 has been rectified.
- An issue which affected the scan process on Windows 10 devices in Offline Files mode has been resolved.
- An issue with boot time slowdown on Windows Server 2012 R2 devices has been rectified.
- An issue where, in some situations, when installing Firewall module, error code 234 was received and has now been resolved.
- In some situations, Endpoint Security prevented web pages from loading in Google Chrome version 38.0.2125.101 and has been resolved.
- An issue with On-demand scan returning error code 1460 has been resolved.

- An issue with AVC, where backups were failing when using VSS and Veeam 8 has been resolved.
- An issue where Data Protection module incorrectly blocked web pages based on partial matches has been resolved.
- An incompatibility between Endpoint Security and Sales Assistant for Windows * has been resolved.
- Update server error code 1460 has been resolved.

Enhancements in this Release:

- Added support for Windows10 Redstone.
- Added support for Scan SSL in the Firefox 64-bit browser.
- Integrated OpenSSL version 1.0.1 in the security components of the product.
- Added exclusions for System Center Configuration Manager 2012 following recommendations from the Vendor.
- Added support for uninstalling the incompatible F-Secure Client Security 12 product.

NOTE: After a system upgrade to Windows 10 Redstone, the Firewall and Content Control modules require a product update to work properly. In such cases it is recommended to first upgrade the OS and the security agent after that.

AV Defender Update Version 5.3.28.761

Issues Resolved in this build:

- An issue that prevented full scans from completing successfully, in some cases, has been resolved.
- In some situations, HP machines with specific hardware configuration, were starting Windows OS in recovery mode.
- Data Protection policy rules not applying on HTTPS pages when the browser toolbar was disabled.

- Endpoint Security Relay was unable to update the endpoints connected to it, in some cases.
- The Firewall module was malfunctioning on certain Windows 10 machines, when added to Endpoint Security instances, with Content Control enabled.
- In some cases, the Bitdefender Endpoint Agent service was unable to start after a product update.
- During scans, the Endpoint Security icon was not visible in the Notification Area of Windows 10 TH2.
- An issue with the Proxy mechanism when importing proxy settings from the browser.
- Juniper Host Checker integration not integrating correctly.
- In some cases, the Microsoft Access database files could not be opened after a full system scan.

Enhancements in this Release:

- Performance improvements of scheduled scans when the Run the task with low priority option is set.
- Product and Signature update verification methods.
- Integrated the OpenSSL version 1.0.1q in the product's security components. For more information, refer to OpenSSL Security Advisory (English only).
- Installation process improvements that address the replacement of previous Endpoint Security versions.
- Traffic scan module improvement to increase the detection of trusted websites.

AV Defender Update Version 5.3.26.749

NOTE: Due to a Microsoft issue in the Windows 10 threshold 2 upgrade the firewall NDIS driver is compromised and will not be operational. To resolve this issue, allow your endpoints to check for updates (through maintenance windows) and the issue will be resolved automatically by a patch placed on the AV Defender update infrastructure.

Issues Resolved in this build:

- In some situations, the on-access scanning module was not functional after an OS upgrade to Windows 10 TH2 and has now been resolved.
- In some cases, Endpoint Security could not communicate with Control Center after updating from a previous version and is now resolved.
- In some situations, silent uninstallation was unable to complete and the issue is resolved.
- An installation issue on ATM machines running Windows 7 Professional 32-bit has been resolved
- After installing Endpoint Security on some Windows servers with virtual adapters, the machines registered a slowdown.
- In some situations, when the user logged into Windows, the Bitdefender icon did not show in

Windows Notifications Area and all protection modules were disabled. The issue has been resolved.

- An issue where Endpoint Security was blocking an ActiveX control that connects to CCTV cameras, thus preventing images from being displayed and has now been resolved.
- In some situations, Endpoint Security deployment was unsuccessful when installing the Firewall module.
- Endpoints were rebooting after each Sophos protection module removal.
- The firewall module of Endpoint Security could not be installed after OS upgrade to Windows 10. The issue is now resolved.
- Some webpages could not be accessed when Scan SSL was enabled.
- In some situations, Endpoint Security appeared outdated in Control Center even though the latest version was installed.
- Content Control was blocking airControl 2 application and is now resolved.

- In some situations, the following message was displayed: “There is no connection with the security host service. Please restart your system.” and all modules of the security agent were turned off, while in Control Center, only the antimalware module was reported as disabled. This issue has been resolved.

Enhancements in this Release:

- Added support for Windows 10 TH2.
- Added support for the removal of the following incompatible security products:
  - ESET NOD32 Antivirus 4.2.76.0
  - McAfee Endpoint Security Platform
  - McAfee Endpoint Security Threat Prevention
  - McAfee Endpoint Security Web Control
  - McAfee SaaS
  - Security Center Communication version 6.0.3 Patch 3
  - McAfee TPSConnector
  - Bitdefender BOX
  - Panda Free Antivirus (not silent)
- The communication between Endpoint Security and Cloud Services is also available over the HTTPS protocol. Port 7076 will be opened on Endpoint Security.
- General improvements to product's stability and performance.
- Added new file scan drivers and photon drivers to improve scanning performance.
- Endpoint Security Relay is now able to forward encrypted management messages and Cloud Services queries. Port 7076 will be opened on Endpoint Security Relays.

AV Defender Update Version 5.3.23.715

Issues Resolved in this build:

- A BSOD issue on Windows XP and Windows 2003 machines from Active Directory domains that were running some scripts at startup from Distributed File System locations has been resolved.
- Certificate warning messages were displayed on endpoints having SSL scan activated, when accessing secure websites using Google Chrome and has been resolved.
- Endpoints having the Scan SSL option enabled via policy received a website identity error after accessing https websites in Chrome, due to an outdated encryption algorithm in the Bitdefender CA. This issue is now fixed.
- Users with endpoints having the Scan SSL option enabled via policy could not login to the Microsoft Office Online website and is now resolved.
- In certain situations, Microsoft Office Excel 2007 was crashing on endpoints protected by Endpoint Security.
- Instability issues experienced in certain situations by the traffic scan module.
- Endpoint Security was blocking the SCCM PXE Image Builder application.
- In certain situations, the operating system reported that Bitdefender Endpoint Host Service terminated unexpectedly and this issue is now resolved.
- Endpoint Security console from an endpoint with terminal server role could not

be opened by users accessing the endpoint remotely.
- Environment variables defined via policy in the firewall rules, containing %AppData%, did not work as they were not properly expanded.
- A localization issue with the Bitdefender alert page displayed in the browser when a webpage was blocked has been resolved.

Important: This Endpoint Security version requires a system reboot.

Enhancements in this Release:

- Integrated the OpenSSL version 1.0.1p in the product's security components. For more information, refer to OpenSSL Security Advisory [9 Jul 2015] (English only).
- Added support for Windows 10.
- Improved performance for the Active Virus Control module.
- Added support for removing Sophos 10.0.12.510, including silent uninstalls.
- Added new file scan drivers that improve on-access scanning performance.

AV Defender Update Version 5.3.20.643

NOTE: Devices with AVD version 5.3.15 or lower installed will require a reboot. Devices with AVD version 5.3.20.642 will not require a reboot.

If you have a maintenance window configured to allow Security Manager Updates and reboots, your devices will automatically reboot according the schedule. The default maintenance window is not set to reboot.

Issues resolved in this build:

* An issue that caused endpoints updated to 5.3.20.642 to reboot outside of the defined window has been resolved.

NOTE: This build also contains all the fixes in 5.3.20.642, noted below.

AV Defender Update Version 5.3.20.642

NOTE: This update requires a reboot.

Issues resolved in this build:

- An issue where an AVC driver appeared in Device Manager with an exclamation mark has now been resolved.
- An issue where Content Control was unable to block access to specific websites if accessed from Google has been resolved.

- An issue where the AVC module was triggering a Java applet crash has been resolved.
- An issue where in some situations, virtual machines from VMware Workstation and Oracle VirtualBox were prevented from starting has been resolved.
- An isolated issue where the Active Virus Control module was introducing a reboot loop on x64 desktop computers with special hardware configuration has now been resolved.
- A change in the installer, causing Endpoint Security to fail to update on certain computers by returning error code 1003 has been resolved.
- An issue where a BSOD error occurred on Windows Server 2012 systems when on-demand scan tasks were running has been resolved.
- An issue where exclusions for on-access scanning were not applying on BitLocker encrypted devices has been resolved.
- An issue caused by a conflict between the Bitdefender firewall and Check Point VPN has been resolved.
- An issue where some websites would not load or apply exclusions when the Scan SSL option was enabled has now been resolved.
- On Windows 7 systems, the exclusions for network drives did not function properly. The issue is now fixed.
- An issue where a critical message containing a false alarm was displayed in the AV Defender client user interface has now been resolved.
- In some situations, the installing or uninstall modules was generating some product instabilities and this issue has been resolved.
- A problem where, in some situations, after an update, the services were unable to start has been resolved.
- Enhancements in this Release
- Optimization of the antivirus detection mechanism at product installation
- Improvements were made to the AVC module.
- A limit on data transfers to the Bitdefender Labs has been instituted to limit big data transfers over the internet
- Improvements on the Endpoint Security self-removal process after failed installations.
- New file scan drivers that improve on-access and on-demand scanning performance have been added.
- Files or folders created after the policy has been applied can now be excluded from scanning. Added exclusions for Windows Server 2008 R2 domain controller.
- Endpoint Security is now available to run on computers with older processors that do not have SSE2 support.

Enhancements in this Release

- Optimization of the antivirus detection mechanism at product installation.
- Improvements were made to the AVC module.

- A limit on data transfers to the Bitdefender Labs has been instituted to limit big data transfers over the internet
- Improvements on the Endpoint Security self-removal process after failed installations.
- New file scan drivers that improve on-access and on-demand scanning performance have been added.
- Files or folders created after the policy has been applied can now be excluded from scanning. Added exclusions for Windows Server 2008 R2 domain controller.
- Endpoint Security is now available to run on computers with older processors that do not have SSE2 support.

New products have been added to the anti-virus software detection mechanism:

- Agnitum Outpost Antivirus*
- Agnitum Outpost Security Suite Free*
- Agnitum Outpost Security Firewall Pro*
- Agnitum Outpost Security Suite Pro*
- AVG AntiVirus 2015*
- AVG AntiVirus FREE 2015*
- Comodo Antivirus
- Comodo Firewall
- Comodo Internet Security
- Comodo Internet Security Pro
- F-secure Anti-Virus for Windows Servers – Virus & Spy Protection
- FortiClient*
- G DATA TOTAL PROTECTION
- G DATA INTERNET SECURITY
- G DATA ANITVIRUS
- Malwarebytes (MEE) 1.75.0.1300*
- Norman Endpoint Protection 9.0
- Norton Security with Backup
- Norton Security
- Panda Antivirus Pro 2015
- Panda GOLD Protection 2015
- Panda Internet Security 2015
- Panda Global Protection 2015
- Panda Devices Agent*
- Avira Professional Security 12*
- Trusteer Rapport
- Eset File Server 4.5.12005
- Vipre Business Agent 7.0.5725*
- Symantec.cloud - Endpoint Protection NIS-21.5.0.19

*Support provided for silent uninstall as well

AV Defender Version 5.3.15.539

NOTE: This upgrade requires a reboot.

If you have a maintenance window configured to allow Security Manager Upgrades and reboots, your devices will reboot automatically according the schedule. The default maintenance window is not set to reboot.

Issues resolved in this build:

- An issue where AVC was causing a BSOD on some specific HP hardware has been resolved.
- An issue where quarantined files detected on network shares had incorrect links in the Quarantine window. The files could not be restored to the original location in this case. This issue is now resolved.
- An issue where in some situations, devices updating from upgrade.bitdefender.com despite the update server being specified as a local relay is resolved.
- An issue where removing F-Secure 10.x and 11.x was not consistently successful has been resolved.
- An issue with the installation crashing on any supported 64-bit system, while the Microsoft Visual C++ 2010 Redistributable for 64 bits was previously installed in the system with wrong msvcr100.dll or msvcp100.dll files has been resolved.
- An issue with BitDefender Personal CA.Net-Defender certificate installation for Firefox browsers on Windows 8 systems has been resolved.
- An issue causing certain HTTPS web addresses to be blocked by even though exceptions for these links existed Has been resolved
- An issue where exclusions defined using the %appdata% variable were not properly applied has been resolved.
- On-demand exclusions now apply to Quick Scan tasks
- In certain situations, while the firewall module was enabled the user login to the domain account was performed slowly. This issue is resolved.
- An issue where the 7-day notification was displayed although the last on-demand scan was run within that period has been resolved.
- An issue where Java was crashing while Active Virus Control was enabled on 32-bit operating systems has been resolved.
- An issue was resolved causing failover to a second ‘Update Server’ within a customer not to function properly.
- A vulnerability related to the update service, caused by the name not being encased in quotes, has been resolved.

Enhancements in this Release

- The AV Defender file and rootkit drivers have been significantly improved.
- Performance optimization has been done in this release.
- Improvements were made to the Traffic Scan module.
- Several optimizations have been added for the following Microsoft applications:
  - Team Foundation Server (all versions)
  - System Center Operations Manager 2012, 2012R2
  - System Center data Protection Manager 2010
  - Microsoft Data Protection Manager (DPM)

AV Defender Version 5.3.13.492

Issues resolved in this build:

- In some instances, the Traffic Scan, Anti-phishing and Web Categories services have stopped functioning due to recent errors with a core component. This issue is now fixed.
- An issue in a network with multiple DNS servers, when the first DNS server from the list was not resolving the addresses, the update failed with error code 1022...
- An issue that caused removed rules from Data Protections Policies not to take effect until the next agent restart or profile reapplication (every 12 hours).
- The Content Control module was unable to block specific embedded videos in webpages.
- The Browser Search Advisor was not functioning with Bing search engines.
- An issue that occurred when the target file inside a previously excluded folder was scanned after the folder exclusion was replaced with the file exclusion.
- The firewall description in the Endpoint Security GUI has been adjusted.
- In certain situations, The Traffic Scan, Anti-phishing and Web Categories services would no longer function due to some errors recently occurred at a core component of the Bitdefender engine.
- An issue where signature updates would fail returning the 2004 error code.

Enhancements in this Release

- Major improvements at the Endpoint Security file and rootkit drivers.
- Improved the Endpoint Security stability and performance.

Support has been added for removal of the following competitive products:

- Malwarebytes Anti-Malware version 1.75.0.1300
- iSheriff Endpoint Security
- Symantec Endpoint Protection Small Business Edition 12

AV Defender Version 5.3.11.463

Issues resolved in this build:

- In some instances, the Traffic Scan, Anti-phishing and Web Categories services have stopped functioning due to recent errors with a core component. This issue is now fixed.

AV Defender Version 5.3.11.462

Issues resolved in this build:

- The file, folder and process exclusions did not take effect while the user was logged off. The exclusions would take effect when a user next logged on. This issue is now fixed.
- In some situations, Windows machines created with Sysprep were unable to properly load the antimalware module. This is discussed in detail at http://www.bitdefender.com/support/how-to-troubleshoot-cloning-a-windows-system-with-sysprep-tool-when-endpoint-security-is-installed-1243.html
- In some instances, a product update may fail when the update server's address was a FQDN. This issue is now fixed.
- When multiple update locations were defined and one contained older files than those currently installed, product downgrade was possible. This issue is now fixed, only updating to higher versions being allowed.
- In some instances, the Firewall module caused slow login to Active Directory computers. This issue is now fixed.
- In some instances, the antimalware engines would fail to load, causing the On-access Scanning module to fail as well. This issue is now fixed.
- In certain situations, the update server was downloading new signatures without cleaning the old ones, increasing the amount of used disk space sometimes filling the drive. This issue is now fixed.
- In certain situations, the update information in the about window would appear as though it had never updated. This issue is now fixed.
- In rare situations, due to process race condition, some instances of the scheduled on-demand scan tasks did not run. This issue is now fixed.
- In some instances, Downloading PDF files with Internet Explorer 8 was would not work when Content Control is present. This issue is now fixed.

- In a network environment using OpenDNS, updates would continuously fail due to malformed DNS requests. This issue is now fixed.
- Creating a Machine Catalog with MCS in XenDesktop 7.5 failed if AV defender was installed. The issue is now fixed.
- In some situations, Windows Action Center reported that AV defender was not installed. This issue is now fixed.
- In some situations, When the On-access Scanning module was set to Permissive and was scanning only applications extensions, an infected file could be executed. The issue is now fixed.
- In some situations, the Web Category filter did not apply after multiple refresh of the webpage. The issue is now fixed.
- The default rule for printing in another network was not working in all situations. The issue is now fixed.
- Copyright information was updated.
- Fixed the abnormal situation when our Photon technology was activated only after the first update. The feature is functioning now from the moment the endpoint is installed.

Enhancements in this build:

- Major improvement of the update mechanism in Endpoint Security for better performance.
- New SQL Server exclusions have been added to the hardcoded exclusion list to cover more instances running on the same machine.
- The device will reboot only once when multiple competitors are removed during the installation process.
- The number of queries performed in-the-cloud from our Antimalware, Anti,phishing and Web Categories modules has been optimized.
- Network path exclusion for AVC/IDS now support mapped network drives as well.
- On access scanning performance has been improved with the addition of new file scan drivers.

Known issues in this build:

When a content control keyword is removed from a previously configured profile the profile changes will not take effect on first application. These will be resolved in the regular profile validation that occurs every 12 hours. If you need to work around this issue before that time a restart of the agent will resolve the issue.

AV Defender Version 5.3.6.387

Issues resolved in this build:

- Resolved an Endpoint Security Relay security vulnerability
- Solved an issue with the Downloader for Windows failing to download installation files in certain situations during the installation of AV Defender software.
- An issue where the downloader application stopped responding when the application window was moved.
- An issue where Windows 8.1 (64-bit) Action Center did not display the installed Endpoint Security components.
- An issue where computers configured for the Endpoint Security Update Server role failed to obtain the virus signatures updates.
- An issue that caused the application to crash unexpectedly in certain circumstances
- An issue that caused a performance impact on slow machines during Endpoint Security Updates.
- An issue causing computers hosting the Update Server component to experience a performance impact during updates. This issue was mitigated by optimizing the update mirroring process on the Update Server.

Enhancements in this build:

- AV Defender is now compatible with Bitdefender Security for Exchange
  - Note: For the two applications to work together on the same system, it is required that Bitdefender Security for Exchange be installed first.
- Several optimization improvements have been added to the AV Defender client to improve stability
- AV Defender's client user interface now has the ability to scan and report detected malware for the Metro user interface available in Windows 8 and Windows 8.1 store apps.
- The Custom scan option has been enhanced to allow scanning in archives.
- The AV Defender client has been updated with the latest technology drivers available in Bitdefender.

Third Party removal tool enhancements:

The following new products were added in the competitor detection and removal mechanism:

- o AVG Internet Security 2014
- ○ AVG Antivirus 2014
- ○ AVG Antivirus Free 2014

Upgrading/Updating to this Release

Please observe the following important upgrade notes, especially as this relates to rebooting devices following an upgrade.

- Updating will happen automatically according to your configured maintenance windows. A reboot may be required to complete the update. If you select to perform an upgrade on demand your system will perform a full installer based upgrade of the AV Defender engine. This will require a reboot. It is recommended to choose the update path to complete the update through a configured maintenance window.
- When AV Defender is pending a reboot due an upgrade, it temporarily uses the default profile until the upgrade device is rebooted. This default profile is configured to automatically upgrade to the latest version if these is an upgrade available, but will not automatically reboot the device.
  Therefore, if a partner upgrades a device, they should reboot the device for the upgrade to take effect; otherwise, they will see the device upgrade outside of the maintenance window, but the device will not reboot.