



AlteonOS

RELEASE NOTES

(Alteon VA Cloud Deployments)

*Version 32.6.0.00 Rev. 1
April 01, 2020*



TABLE OF CONTENTS

| | |
|---|-------------------------------------|
| CONTENT | 4 |
| RELEASE SUMMARY | 4 |
| SUPPORTED PLATFORMS AND MODULES | 4 |
| UPGRADE PATH | 4 |
| Before Upgrade – Important! | 4 |
| General Considerations | Error! Bookmark not defined. |
| Downgrade | 5 |
| WHAT'S NEW IN 32.6.0.0 | 5 |
| Network HSM | Error! Bookmark not defined. |
| Virtualization on Alteon D-9800, D-5820, D-5424 | Error! Bookmark not defined. |
| WAF Security Events per Application | 6 |
| Outbound SSLi Wizard | 6 |
| AppShape++ Enhancements | 6 |
| Cloud Init | 7 |
| AppWall Enhancements | 7 |
| Anti-Scraping Thresholds per URI | 7 |
| Forensics Filters | 7 |
| High Availability Enhancements | 7 |
| Alteon VA White Label Support | 8 |
| WHAT'S CHANGED IN 32.6.0.0 | 8 |
| OpenSSL Version | 8 |
| Number of FQDN Servers | 8 |
| Health Check Source MAC | 9 |
| Server Session Shutdown | 9 |



| | |
|---|-----------|
| Banner Length | 9 |
| Alteon VA – Number of Supported NICs (Hyper-V, OpenXEN) | 9 |
| Integrated AppWall..... | 9 |
| Block Terminal Output per SSH Session | 10 |
| MAINTENANCE FIXES | 10 |
| Fixed in 32.6.0.0 | 10 |
| General Bug Fixes | 10 |
| AppWall Bug Fixes..... | 18 |
| KNOWN LIMITATIONS | 20 |
| RELATED DOCUMENTATION..... | 20 |

CONTENT

Radware announces the release of AlteonOS version 32.6.0.0. These release notes describe new and changed features introduced in this version on top of version 32.4.1.0.

RELEASE SUMMARY

Release Date: February 27, 2020

Objective: Major software release that introduces and/or enhances a number of capabilities and solves a number of issues.

SUPPORTED PLATFORMS AND MODULES

- Alteon VA running on VMware ESXi 6.0, 6.5, 6.7 (*new*), KVM, Hyper-V and OpenXen
- Alteon VA on AWS
- Alteon VA on Azure
- Alteon VA on Nutanix
- Alteon VA on Oracle Cloud

For more information on platform specifications, refer to the *Alteon Installation and Maintenance Guide*.

Alteon 32.6.0.0 is supported by APSolute Vision version 4.50 and later.

Integrated AppWall version: 7.6.7.0

OpenSSL version: 1.1.1d

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 29.5, 30.x, 31.x and 32.x.

General upgrade instructions are found in the *Alteon Installation and Maintenance Guide*.

Before Upgrade – Important!

1. Before performing an upgrade, back up your current configuration.
2. To ensure a successful upgrade, run the [Upgrade Advisor Tool](#) with your current configuration and the target version. Then, perform the required actions as instructed in the report output. The Upgrade Advisory Tool includes all the limitation and upgrade considerations specifically relevant to

the source configuration, version, device details and target version. Make sure to update the Upgrade Advisory Tool DB before performing the analysis. The Upgrade Advisor Tool is available on the Customer Portal.

3. Read the [Upgrade Limitations](#) in these Release Notes for new upgrade limitations related to this version.

The following table describes the specific upgrade path from each version to 32.6.0.0:

| Current Version | Upgrade Path | Notes |
|------------------|--------------------------------------|---|
| 29.5.x (x<7) | > 29.5.8.0 > 30.5.3.0 > this version | As an alternative, you can upgrade directly to 32.6.0.0 using the recovery process. Note: You must save the configuration before starting this process. |
| 29.5.x (x>7) | > 30.5.3.0 > this version | |
| 30.x =< 30.5.2.0 | > 30.5.3.0 > this version | |
| 30.x > 30.5.2.0 | Direct upgrade to this version | |
| 31.x | Direct upgrade to this version | |
| 32.x | Direct upgrade to this version | |

Downgrade

Configuration rollback (downgrade) is not supported. The configuration should be saved before upgrading to a newer version. If you perform version rollback, Radware recommends the following procedure:

1. Set the configuration block for the next boot to **factory** (the management port setting can be kept).
2. Change the image for the next boot to the image to which you want to roll back.
3. Perform reboot.
4. After reboot, Alteon will run with the previous version with the factory default configuration.
5. Upload the configuration that was saved before the version upgrade

WHAT'S NEW IN 32.6.0.0

This section describes the new features and components introduced in this version on top of Alteon version 32.4.1.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.6.0.0.

WAF Security Events per Application

Security events are the events reported by WAF when an attack is detected. This allows user visibility to the protected traffic, refinement of false positives, and detailed explanations of security attacks.

Security events generated by the integrated AppWall module can currently be shown in AppWall Forensics, and can be sent to Vision Reporter, where they are presented in the WAF dashboard, Forensics and Alerts. Starting from this version, Alteon can also send the WAF security events, in CEF format, via its event logging module (over TCP/TLS), in the context of the application. This lets you correlate between the security event and its relevant traffic event using the WAF transaction ID, to obtain more information on the transaction.

The security events per application can be viewed on the Alteon Cloud Control Application Dashboard, version 1.3.0 and alter, but are currently not available on the APSolute Vision Application Dashboard. However, they can be sent to a third-party SIEM.

Outbound SSLi Wizard

An updated wizard for quick and easy configuration of an outbound SSL Inspection solution is now available using a vDirect workflow available on APSolute Vision 4.50.

The updated wizard adds 2-box Layer 3 deployment to the previously supported single-box Layer 3.


Wizard Support Notes:

- Layer 3 network deployment refers to both transparent and explicit proxy:
 - Layer 3 network deployment refers to both transparent and explicit proxy and is now supported in both single box and 2-box deployments.
 - Fully transparent network deployments (Alteon as bump-in-the-wire), support single box only.
- To access the wizard, access vDirect from APSolute Vision 4.50, navigate to the catalog, and filter by SSL inspection.

AppShape++ Enhancements

The following AppShape++ capabilities were added:

- The **httponly** flag is added to the **persist cookie insert** and **persist cookie rewrite** commands. This flag informs the browser not to display the cookie through client-side scripts (document.cookie and others).
NFR ID: 190911-000550 (prod00271354)
- The 308 response code option is added to **http::redirect** command. 308 is the Permanent Redirect response code and it indicates that the resource requested has been definitively moved to the URL given by the Location headers.



NFR ID: 190925-000125 (prod00253762)

Cloud Init

Using Cloud-Init, customers can now spin up a preconfigured Alteon VA in an OpenStack environment. Cloud Init enables the following pre-configuration:

- **Management info** – Management IP address management mask and gateway (both IPV4 and IPV6)
- **User credentials**
- **VA resources** – Such as number of vCPUs and RAM size per Alteon and AppWall.
- **Jumbo frame configuration (MTU size)**
- **Option to enter any of the Alteon configuration parameters**

All of these configurations are done at the initial Alteon boot with no need for an additional boot, as required when configuring some of these parameters (such as the VA resources, and jumbo frames).

AppWall Enhancements

Anti-Scraping Thresholds per URI

Anti-Scraping now supports defining thresholds per URI. In Anti-Scraping mode, the Activity Tracking module counts the HTTP transaction rate to the defined application scope (domain/page) per user per second. You can define different thresholds and different blocking time settings for each (up to 30) protected URI.

Forensics Filters

Forensics events can now be filtered by: URI, Parameter Name, and Refinements. Filtering by refinements display either refined events or events not refined.

Note: When upgrading from previous versions, filtering by 'Refined' includes only new events generated after the upgrade. Filtering 'Not Refined' events includes all events from before the upgrade, refined and not. Radware advises to use this filter together with a time range filter.

High Availability Enhancements

New tracking options (VIP and server group) were added to Alteon High Availability capability. These options are not available in the legacy VRRP mode.

In this version, these new options are configurable via CLI only:

- **VIP Tracking**

A user can mark the VIPs to track, and when any of these VIPs is unavailable (at least one of its services is unavailable) a failover will occur.

The user has the option to determine the criteria for the VIP to fail over according to its services, meaning to limit the failover only if specific services of that virtual services are not available.

NFR ID: 191006-000023

- **Group Tracking**

A user can select a real servers group to track, and when that group is not available a failover will occur.

A group is considered as not available according to the number of available real servers as configured for the Group status threshold parameters.

Radware recommends using the group tacking option mainly when working with filters, where a virtual service is not relevant, and as result the VIP tracking option cannot be used.

NFR ID: 190911-000428 (prod00269501)

Alteon VA White Label Support

Starting with this version, Alteon VA can be white-labeled for OEMs, with the same functionality as the platform white-labeling.

WHAT'S CHANGED IN 32.6.0.0

OpenSSL Version

The OpenSSL version is updated in this release as follows:

- Alteon VA now use OpenSSL 1.1.1d

Number of FQDN Servers

The number of supported FQDN servers on Alteon VA was increased and depends on the Alteon VA footprint and, when running in public Clouds, on whether a server's autoscaling feature is enabled.

Alteon VA

| Memory size | Max number of FQDN entries | Maximum number of IP address per FQDN entry |
|--------------------------|----------------------------|---|
| Memory size - up to 6 GB | 57 | 30 |
| 6GB < memory size ≤ 16GB | 115 | 30 |
| 16GB < memory size | 230 | 30 |

Alteon VA on Azure/AWS when Real Server Autoscaling is Enabled

| Memory size | Max number of FQDN entries | Maximum number of IP address per FQDN entry |
|--------------------------|----------------------------|---|
| Memory size - up to 6 GB | 20 | 100 |
| 6GB < memory size<=16GB | 40 | 100 |
| 16GB < memory size | 230 | 100 |

Health Check Source MAC

When working in legacy VRRP high availability mode, you can now set health check traffic to servers to use the VR MAC for the server's VR owner instead of the interface MAC.

NFR ID: 190911-0 (prod00270223)

Server Session Shutdown

Real servers can be shut down gracefully by continuing to send to the server traffic belonging to active connections (Connection Shutdown), and in addition can continue allocating to the server new connections if they belong to persistent session entries (Session Shutdown). Previously, Session Shutdown was only available when persistency mode was cookie or SSL ID. Now this is also available for client IP persistency.

NFR ID: 190911-0000346 (prod00 273440)

Banner Length

The CLI banner length has been increased from 80 characters to the standard banner length of 319 characters (`/cfg/sys/bannr`).

Note: The data type of `agCurCfgLoginBanner` and `agNewCfgLoginBanner` was changed from `DisplayString (SIZE(0..79))` to `OCTECT STRING (SIZE(0..318))`.

NFR ID: 190912-000126

Alteon VA – Number of Supported NICs (Hyper-V, OpenXEN)

The number of vNICs Alteon VA runs on Hyper-V or OpenXEN was increased from three (3) to eight (8) vNICs (one [1] for management and seven [7] for data).

Integrated AppWall

The following are changes and modifications made to the AppWall module:

- For Alteon VA in SingleIP mode, the configuration and monitoring of the integrated AppWall module is now provided via the Alteon WBM instead of the legacy Java-based UI.

- Integrated AppWall module can now report events to APSolute Vision using IPv6 addresses.
- The Forensic events filter by time range now supports hour and minute ranges.
- Integrated AppWall can now synchronize Signature Updates and Geolocation data that was manually installed to a backup HA device. To initiate the synchronization, click **Apply** after installing the new updates on the primary device.
- Disabling the publishing of an event also disables sending the event to APSolute Vision.
- AppWall notifies you of configuration file issues and recommends a solution.
- Fixes and improvements to AppWall's configuration **Apply** mechanism.
- Fixes and improvements to the config sync mechanism.

Block Terminal Output per SSH Session

When Display Log (displog) is enabled, all syslog messages are sent to the Telnet/SSH screen. These output printouts cause vDirect scripts to fail.

Starting with this version, you can disable the Display Log per local user if the Display Log is globally enabled. This way, a customer who wants to work with displog enabled can create a local Admin user for vDirect purposes and disable Display Log for that specific user only.

Important: Radware recommends disabling `/oper/displog` in production, as it may affect performance.

MAINTENANCE FIXES

Fixed in 32.6.0.0

General Bug Fixes

| Item | Description | Bug ID |
|------|--|--------------|
| 1. | After HA failover, Alteon lost router connectivity in order to reach real servers. | prod00277714 |
| 2. | The remote system refused the connection, impacting Azure NA self-service. | prod00277310 |
| 3. | When using HTTP/2 after login, traffic stops working. | prod00278069 |
| 4. | Configuration sync failed with a timeout. | prod00273097 |
| 5. | Could not configure service 111 for TCP or UDP. | prod00272645 |

| Item | Description | Bug ID |
|------|--|--------------|
| 6. | An unexpected LACP changed state resulted in the device switching to BACKUP state. | prod00278166 |
| 7. | Could not sync or apply changes. | prod00276398 |
| 8. | When an HTTP modification string was configured with multiple escape sequences, Alteon did not insert an escape sequence. | prod00276937 |
| 9. | On DPDK platforms, Interface errors for port statistics were issued. | prod00278282 |
| 10. | Using WBM, when "Return to Last Hop" was set for a virtual server, an additional field type was also set internally. | prod00276932 |
| 11. | Using WBM, could not the configure sync passphrase. | prod00274326 |
| 12. | Alteon was rebooted unexpectedly by watchdog. | prod00273480 |
| 13. | Using LinkProof NG, when uploading or downloading WAN link limits are configured above 455 Mbps, WAN link bandwidth utilization displayed incorrect statistics. | prod00273018 |
| 14. | Alteon rebooted with a power cycle. | prod00272623 |
| 15. | Using WBM, a notify view iso could not be configured without creating a custom notify tag. | prod00273727 |
| 16. | Using WBM, a user could change the admin password while being authenticated via TACACS or RADIUS. Usually a user is not allowed to change the admin password when logged in with "admin Privileged" using TACACS or RADIUS. | prod00277355 |
| 17. | During SNMP polling, a panic occurred. | prod00277994 |
| 18. | IEEE 802.3 standard protocol packets (such as STP packets that run over LLC) were sometimes incorrectly classified as packets with a length error by the Fortville MAC. The CRC was not stripped from such packets, and the RLEC counter was incremented. These packets later caused problems when transmitted with the unstripped CRC to other entities in the network. | prod00273095 |
| 19. | The Intermediate CA certificate could not be imported due to unexpected max limit. | prod00278076 |
| 20. | After upgrading to version 32.2.1.0, MP CPU utilization spiked. | prod00273887 |

| Item | Description | Bug ID |
|------|--|--------------|
| 21. | In a LinkProof for Alteon environment, there were Intermittent ICMP packet drops. When pinging from the same sequence number, the ping reply packets dropped intermittently. | prod00276794 |
| 22. | In a GSLB environment, Alteon became stuck with high MP CPU utilization. | prod00276521 |
| 23. | A confusing configuration resulted while implementing LDAP(S) health check. | prod00275746 |
| 24. | After deploying a TCP optimization policy, the software panicked. | prod00277925 |
| 25. | Using WBM, the maximum session number did not change after adding a CU. It only changed using the CLI. | prod00274759 |
| 26. | The GSLB DNS client network rules real server selection pane was too small. | prod00272845 |
| 27. | Alteon HA did not behave as expected. | prod00274959 |
| 28. | When enabling the HTTP/2 policy, a panic occurred. | prod00273689 |
| 29. | When running the /stat/slb/clear command, only some of the filter statistics were cleared and the other statistics remained. | prod00272890 |
| 30. | Added GSLB site IP address validation. | prod00277096 |
| 31. | Connections to a VIP closed abruptly. | prod00276585 |
| 32. | In an SLB environment, after a config sync was performed with PIP sync disabled. Alteon did not replace the client IP address with a PIP. | prod00277546 |
| 33. | SIP INVITE and fragmented packets are not forwarded to real servers. | prod00273233 |
| 34. | After a panic, the Admin context went into a reboot loop. | prod00276328 |
| 35. | After upgrading to version 32.2.1.0, session logs were not generated. | prod00272747 |
| 36. | A health check failure occurred because of a corruption in the small/medium/jumbo packet free pool list due to a synchronization problem in the ARP module. | prod00274564 |
| 37. | Enabling and disabling HTTP/2 caused service impact. | prod00275412 |

| Item | Description | Bug ID |
|------|---|--------------|
| 38. | An explicit proxy caused unexpected behavior for HTTP/HTTPS traffic. | prod00278448 |
| 39. | When idbynum was enabled, there were issues with Revert Apply. | prod00273942 |
| 40. | When importing a configuration with BGP, Alteon issued Notice messages with non-ASCII characters. | prod00275648 |
| 41. | When VLAN 1 was disabled and an Apply was done for any configuration change, the ping response to the interface was delayed, causing a timeout. | prod00273594 |
| 42. | When the DNS virtual service protocol was UDP stateless, the HTTP and FTP services failed for IPv6 traffic. | prod00273830 |
| 43. | There were many FLOOD entries being created in the FDB table for the PIP MAC. This caused some of the traffic to fail. | prod00277247 |
| 44. | Using WBM, when starting a packet capture, unexpected data displayed for /c/sys/alerts when the packet capture filter string was set to more than 128 characters. | prod00275475 |
| 45. | Using WBM, you could not edit the IP address for a new Outbound LLB Rule. | prod00277384 |
| 46. | When the Alteon HA state changed from Master to Backup, the gateway and real server's health checks failed. | prod00278209 |
| 47. | In a GSLB with VRRP/HA environment, after applying a configuration, the DSSP health checks failed. | prod00273187 |
| 48. | In an SLB environment with a pbind client IP address, persistence was not maintained. | prod00276271 |
| 49. | With a lower BFD rx-int configured, when the session table type was changed from ABT to PBT, the BFD session went down, causing the BGP session to be deleted. This issue is addressed by yielding control to the SP for sending BFD packets. | prod00272649 |
| 50. | After resetting the admin password from the console, the new password was seen in clear text in diff flash. | prod00274143 |
| 51. | In an Azure environment, Alteon VA crashed. | prod00276480 |
| 52. | Using WBM, could not configure BGP 4-byte-ASN. | prod00276809 |

| Item | Description | Bug ID |
|------|---|--------------|
| 53. | When the primary WAN link went down and the backup WAN link took over, an incorrect syslog message displayed. | prod00276690 |
| 54. | When logged in as a TACACS or RADIUS user, could not modify or create SNMPv3 authentication or privacy passwords. | prod00277002 |
| 55. | In a GEL environment, the Alteon VA prompt license server was constantly reestablished. | prod00274364 |
| 56. | Alteon was affected by CVE 2019-11477, CVE 2019-11478, and CVE 2019-11479. This is now fixed. | prod00273355 |
| 57. | Alteon Indirectly caused a vulnerability to a DNS cache poisoning attack. | prod00274788 |
| 58. | When sending syslog messages, a panic occurred. | prod00272886 |
| 59. | After the device reset, it failed to connect the Alteon VA management IPv6 address . | prod00275197 |
| 60. | Using WBM, during configuration sync, continuous fetching of the virtual server table caused a panic. | prod00277466 |
| 61. | The backup group status in a content rule displayed an incorrect status when the backup group was not directly associated to any service. | prod00276757 |
| 62. | Config sync or disabling virt synchronization removed virtual servers from the backup device. | prod00273198 |
| 63. | When AES was used for privacy and/or encryption, the initialization vector was not set properly, causing AES encryption failure. | prod00276314 |
| 64. | A configuration change to the shutdown definition was not displayed correctly using the /cfg/slb/group x/cur command. | prod00272735 |
| 65. | NTP requests were not sent in an OSPF network. | prod00274317 |
| 66. | On the APSolute Vision Analytics Dashboard, there was an Alteon SP CPU display issue. | prod00274472 |
| 67. | When changing to the default configuration, the runtime session capacity was not reflected. | prod00276873 |

| Item | Description | Bug ID |
|------|---|--------------|
| 68. | During an upgrade to version 32.2.30 or later, the configuration became stuck in diff. | prod00276741 |
| 69. | Using WBM, there was an HTTP modification rule configuration issue. | prod00273399 |
| 70. | When processing the second fragment destined for the Alteon interface when the redirect filter was configured, Alteon panicked. | prod00277545 |
| 71. | There was a disparity of the MAC address between the primary and backup devices. | prod00275355 |
| 72. | On an Alteon VA, Alteon reset the connection when traffic failed over. | prod00277406 |
| 73. | VRs and Switch HA and Service HA configurations sometimes would flap or go into the INIT state after synching the configuration from the secondary device to the primary device if there was a difference in the configuration between the two devices. | prod00276502 |
| 74. | SSL traffic caused a panic. | prod00278066 |
| 75. | When changing the "DNS Responder VIP" to "dis to ena" or vice versa, Alteon did not update the flags that are used to identify the configuration change. As a result, Alteon found no config change during an Apply and an issue occurred. | prod00273284 |
| 76. | Throughput Threshold alerts displayed despite the threshold level being set 0 (disabled). | prod00276301 |
| 77. | Using Passive FTP, an RTS session was created instead of a filter session for FTP data traffic. | prod00272720 |
| 78. | During bootup time while loading the configurations from flash, the Apply failed. | prod00274184 |
| 79. | ICAP responses were not forwarded to the client. | prod00276505 |

| Item | Description | Bug ID |
|------|---|--------------|
| 80. | <p>The priorities for remote real servers among different GSLB network did not behave as expected.</p> <p>In this version, priority is given to nwclasses matching in added networks. As a result, if there is a SIP match for one of the networks, a network with SIP=any will not be considered. If there is no SIP match for networks with SIP configured, then a network with SIP=any will be considered. Priority is considered among the real servers of the matched network.</p> | prod00276835 |
| 81. | BGP 4 Byte ASN was not compatible with Cisco Nexus 9K and Huawei routers. | prod00276710 |
| 82. | In an IPv6 SLB environment with an IPv6 HTTP health check and IPv6 HA configured, the memory allocated for HTTP HC was not freed, which led to a memory leak. | prod00276967 |
| 83. | SNMP data in the polling interface details incorrectly represented the interface type. | prod00273384 |
| 84. | Trend Micro's IWSVA (AV) in ICAP mode (with Alteon acting as ICAP client) was only partially working. | prod00277016 |
| 85. | An ICMP error message (destination unreachable) was not supported for the response (ICMP Error) to Outbound SmartNAT traffic with ESP/AH/GRE payloads. This is now supported. | prod00275320 |
| 86. | In an SLB environment with preemption disabled for the primary real server, when it was in the failed state and the backup real server became the primary, the original primary real server became the backup server when its health check came UP, even though preemption was disabled. | prod00277335 |
| 87. | An HTTP header modification value set to None was considered as valid input. | prod00277184 |
| 88. | Using the preempt disabled feature, a primary real server that was moved to the OPER DIS state by the HC module when the backup was UP for the service, continued to be in the OPER DIS state even when the "backup" and "preempt dis" settings were removed from it. | prod00276617 |

| Item | Description | Bug ID |
|------|--|--------------|
| 89. | When changing from ena to dis and vice versa, could not apply the /cfg/l3/ha/switch/filtbpbk command. | prod00277754 |
| 90. | After reverting an unsaved configuration, the HA state remained INIT and was not updated automatically. | prod00272982 |
| 91. | In an SLB environment, when the session move operation was executed, in some cases this operation was not reset on one of the SPs, which resulted in all subsequent session move operations to fail on that particular SP. | prod00276338 |
| 92. | During stress traffic, a panic occurred. | prod00278082 |
| 93. | When viph1th was enabled, there was no response to ICMP health checks to VIP IP addresses. | prod00274665 |
| 94. | When a device came up after reboot, the HA status displayed as NONE because the HA state was recorded based on the current HA service group state for which the apply was in process. | prod00275641 |
| 95. | When a device came up after reboot, the HA status displayed as NONE because the HA state was recorded based on the current HA service group state for which the apply was in process. | prod00278452 |
| 96. | After upgrading to version 31.0.11.0 SSL offload did not work properly. | prod00276275 |
| 97. | After upgrading to version 31.0.11.0, SSL offload did not work properly. | prod00275661 |
| 98. | In a GSLB environment, Alteon did not resolve a DNS query even though the remote real servers were UP. | prod00272895 |
| 99. | After applying configuration changes, a VIP stopped responding. | prod00272783 |
| 100. | After running a scan over SSH, the device panicked. | prod00274827 |
| 101. | A packet capture's TCP stream displayed corrupted data. | prod00273699 |
| 102. | IPv6 SNMP queries over the data port were not working because checking for management access with the ingress data port failed. | prod00277308 |
| 103. | In a DSR environment, there was a discrepancy between /info/swkey and virtual server statistics. | prod00277933 |

| Item | Description | Bug ID |
|------|---|--------------|
| 104. | When a DUT was connected on one port and a server connected on a different port, there was a MAC flap on Layer 2. | prod00273064 |
| 105. | Traffic was forwarded to a failed WAN real server. | prod00276353 |
| 106. | When the management port was disabled, syslog messages were not sent on the data port. | prod00278038 |
| 107. | Using APSolute Vision, importing a certificate Alteon did not work with the ADC + Certificate Administrator role. | prod00274710 |
| 108. | Could not log in to AppWall. | prod00275566 |
| 109. | After upgrading to version 32.2.3.0, the device constantly rebooted due to a panic. | prod00278288 |
| 110. | An invalid hypervisor type was set for virtual platforms. | prod00276259 |
| 111. | HTTP health check edit page via BBI does not show configured settings and values | prod00275723 |
| 112. | Using WBM, generating a certificate resulted in an invalid EC key size (6). error. | prod00272976 |
| 113. | Using QAS, after a Submit the rport of the service was overwritten. | prod00272878 |
| 114. | Using switch HA, an unexpected failback sometimes occurred. | prod00274832 |
| 115. | Using WBM, when VIPs were added or removed from the HA service list, the device panicked. | prod00273659 |

AppWall Bug Fixes

| Item | Description | Bug ID |
|------|---|---------|
| 1. | Scenarios where the 'Replace HTTP Reply Messages with Custom Messages' feature did not function. | DE53496 |
| 2. | After performing a 'Revert' for AppWall in Alteon, you must refresh the page. | DE50247 |
| 3. | For AppWall in Alteon, in some scenarios, the AppWall page is grayed-out for a brief period while applying a new configuration. | DE51355 |

| Item | Description | Bug ID |
|------|---|---------|
| 4. | For AppWall in Alteon, in rare cases, when applying configuration changes, AppWall's "Login" page is shown and the login will not succeed. In such cases, a restart to AppWall's service is needed. | DE51346 |
| 5. | Source Blocking module might not be enforced on IPv6 sources identified using an HTTP Header, as in the case of CDNs. | DE51975 |
| 6. | Auto Discovery should be set manually to "Resume Auto Discovery" when enabling "Auto Policy Generation" on an already-configured application path in the security policy. | DE52165 |
| 7. | When using Source Blocking with IPv6 addresses, at least one IPv4 address must exist in the list for the feature to be enabled. | DE49832 |
| 8. | Rare case leading AppWall to restart. | DE53577 |
| 9. | Scenarios where the 100-Continue header was not sent correctly by AppWall in Alteon, causing the transaction to fail. | DE53201 |
| 10. | Rare case when refining parsing properties failed with a server error. | DE53336 |
| 11. | Event log filters by date may include additional events in some scenarios. | DE54073 |
| 12. | Rare case that led to the error "Server Error: "Get of FilterAdv/Database failed!" in the WebUI for AppWall in Alteon. | DE51538 |
| 13. | Scenario where sync fails for AppWall in Alteon. | DE53151 |
| 14. | AppWall in Alteon does not parse parameters which value contains Emoji Unicode characters. | DE51007 |
| 15. | LDAP group-based authentication may fail in some scenarios. | DE53520 |
| 16. | Some scenarios where Redirect Validation was not enforced on specific URL prefixes. | DE53373 |
| 17. | A Vulnerability security event is wrongly classified as "HTTP Method Violation". | DE53368 |
| 18. | Wrong title in "Threat" field for FastUpload events. | DE53379 |
| 19. | LDAP group authentication may fail login in some scenarios. | DE53261 |

| Item | Description | Bug ID |
|------|---|---------|
| 20. | Rare case where transactions were blocked while the tunnel Operational Mode is in Bypass. | DE52453 |
| 21. | Wrong tunnel name reported on Source Blocking events in some scenarios. | DE52002 |
| 22. | Scenario where Source Blocking stopped blocking blocked sources after a configuration change. | DE52167 |
| 23. | LDAP attribute cannot be modified when using LDAP group-based authentication. | DE53760 |
| 24. | A specific type of injection was not detected. | DE53785 |
| 25. | Scenario where LDAP configuration was not kept after reboot. | DE54019 |
| 26. | Rare case where an error was shown in WebUI after adding publishing rules. | DE53413 |
| 27. | Filtering Event Log based on predefined forensics view may not work in some cases. | DE54045 |

KNOWN LIMITATIONS


The list of known limitations, available to customers only, is available at the following link:

https://support.radware.com/app/answers/answer_view/a_id/1022905

RELATED DOCUMENTATION

The following documentation is related to this version:

- *Alteon Installation and Maintenance Guide*
- *Alteon VA Installation and Maintenance Guide*
- *Alteon Getting Started Guide*
- *Alteon Web Based Management Application Guide*
- *Alteon Command Line Interface Application Guide*
- *Alteon Command Reference*
- *Alteon REST API User Guide*

- 
- *Alteon AppShape++ SDK Guide*
 - *AppWall for Alteon NG User Guide*
 - *FastView for Alteon NG User Guide*
 - *LinkProof for Alteon NG User Guide*
 - *LinkProof NG User Guide*
 - *Alteon Troubleshooting Guide*



North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 69710, Israel

Tel: 972 3 766 8666

© 2020 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners. Printed in the U.S.A