AlteonOS

RELEASE NOTES

(Alteon VA Cloud Deployments)

Version 33.0.2.0 Rev. 2
November 23, 2021

TABLE OF CONTENTS

CONTENT

Radware announces the release of AlteonOS version 33.0.2.0. These release notes describe new and changed features introduced in this version on top of version 33.0.1.50.

RELEASE SUMMARY

Release Date: September 30, 2021

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

SUPPORTED PLATFORMS AND MODULES

This version is supported by the following platforms:

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

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

Alteon 33.0.2. 0 is supported by APSolute Vision version 4.30 and later.

Integrated AppWall version: 7.6.13. 0

OpenSSL version: 1.1.1l

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 28.*x*, 29.*x,* 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 33.0.2.0:

Current Version	Upgrade Path	Notes
28.*x*	> 29.0.9.0 > 30.5.3.0 > this version	As an alternative, you can upgrade directly to 33.0.2.0 using the recovery process. **Note**: You must save the configuration before starting this process.
29.0.*x* (*x*=<8)	> 29.0.9.0 > 30.5.3.0 > this version	
29.0.*x* (*x* > 8)	> 30.5.3.0 > this version	
29.5.*x* (*x*=<7)	> 29.5.8.0 > 30.5.3.0 > this version	
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 33.0.2.0

This section describes the new features and components introduced in this version on top of Alteon version 33.0.1.50.

Enable VMA Source Port for FTP

The VMA source port can now be enabled when load balancing FTP traffic. For passive FTP, this requires an AppShape++ script (an AS++ script that handles FTP is available in the Knowledgebase).

NFR ID: 200925-000050

Route to Resolved FQDN IP Address

In some scenarios, the hostname for the servers to which traffic needs to be forwarded is dynamic. This requires resolving (DNS) a hostname in the HTTP request received from client and forward the request to the resolved IP address.

For this purpose, the following capabilities were added:

- **Mid-session DNS resolving** (first introduced in version 33.0.1.50): The Alteon sideband connection mechanism now supports DNS connection and a number of new AppShape++ commands were added (an AppShape++ script is required to handle extracting the relevant hostname from the HTTP request, handling the DNS resolution via the sideband connection and making the load-balancing decision based on the DNS record received).
- Allow the AppShape++ `host` command to function on a virtual service, and forward client traffic to the specified IP address, and not to any Alteon configured real server.

  Notes:

  - When used on a virtual service, the `host` command does not select a real server, while when used on a filter, it does and forwards the client traffic to the specified IP address via the selected server (next hop).
  - Even though no real servers are being used, because this is a virtual service, it is required to attach a group with a dummy real server and enable Service Always Up parameter (`/cfg/slb/virt <virt id>/service <port>/appshape/alwayson`) to ensure that virtual server is always up and receiving traffic.

NFR ID: 201204-000103

Close Connection on Fastage

In this version, it is now possible to send an RST to the client, server, or both, when the session fastage is out (using `/cfg/slb/virt/service/clfstage`).

Important Notes:

- When Close Connection on Fastage is enabled, Radware highly recommends setting the fastage to 0 (the default value) for the session RST to be sent within 2 seconds.

- Requests that arrive during fastage (after the connection is closed by FIN and until Alteon sends an RST and clears the session entries) causes the session to be refreshed, and as a result Alteon does not send the RST. To avoid the session being refreshed and ensure that the RST is sent within the defined fastage time, session drop (`/cfg/slb/adv/sessdrop`) must be set to enabled
- in force proxy mode, when FIN is received from either side (client or server) RST is immediately sent to both the client and server.

NFR ID: 210516-000032

Integrated AppWall

64 bit Support

The support of 64bits for AppWall integrated enables the AppWall module to take advantage of higher memory platforms in order to support more connection concurrency.

Prior to this version, a maximum of 4 GB could be allocated to the AppWall module. Now, depending on the platform memory and form-factor, more memory can be allocated for AppWall.

Enhanced Security Attacks Protection

As part of advanced security attacks, an attacker can now send a multiple encoded attack.

For example, the attacker can encode a parameter value with Base64 multiple times that contains an SQL Injection.

In the Tunnel Parsing Properties, setting how many times AppWall decodes a parameter value to assess the security of the request has been added. In this version, AppWall supports the Cookie header, whether or not a parameter is in JSON format. Security inspection is done with the Database Security filter and the Vulnerabilities Security filter.

Visibility

Traffic Event Support for H2 Gateway Traffic

The following traffic events are now supported with H2 Gateway traffic: Unified event, Security event, SSL connection/failure, L4 events (the H2 Gateway is available only in virtual services).

Note: In H2 full proxy mode, only L4 events are supported.

Alteon PPS Statistics per Device

Packets Per Second statistics are now available per device (`/stat/slb/dvcstats`).

Note: PPS per device statistics currently only include virtual service traffic.

NFR ID: 200706-000123

Interface MIB Enhancement

In this version, it is now possible to configure an alias and name for the management interface.

ifAlias parameter is now available as read-only as part of the standard MIB. It supports the alias information of both the management and data interfaces.

NFR ID: 190911-000253

Sideband Policy Statistics

Sideband policy statistics are now available, reflecting the traffic metrics (throughput, sessions, CPS, and so on) and the SSL information of the sideband traffic.

Ansible Module for "command" Execution

A new MIB parameter, **agAlteonCliCommand**, is now available to handle all the CLI commands that do not have MIB support (or Ansible support).
This MIB accepts CLI commands as text.

For more details on the MIB behavior and limitations, see Radware’s Knowledge Base.

NFR ID: 210505-000103

HTTP/3 Gateway – POC

HTTP/3 is the third major version of the Hypertext Transfer Protocol used to exchange information on the World Wide Web, alongside HTTP/1.1 and HTTP/2.

HTTP/3 uses similar HTTP semantics as HTTP/2. The main difference is in the underlying transport. Both HTTP/1.1 and HTTP/2 use TCP as their transport, while HTTP/3 uses QUIC, a transport layer network protocol which uses user space congestion control over the User Datagram Protocol (UDP).

The switch to QUIC aims to fix a major problem of HTTP/2 called "head-of-line blocking": because the parallel nature of HTTP/2's multiplexing is not visible to TCP's loss recovery mechanisms, a lost or reordered packet causes all active transactions to experience a stall regardless of whether that transaction was impacted by the lost packet. Because QUIC provides native multiplexing, lost packets only impact the streams where data has been lost.

As of August 2021, the HTTP/3 protocol is still officially an Internet Draft, but is already supported by 73% of running web browsers.

Alteon now has a POC-level implementation for HTTP/3 to HTTP/1.1 gateway, which can allow Web sites to enjoy the advantages of HTTP/3 transport over the Internet, without any modification to the website.

For a POC build, contact ADC PM.

WHAT'S NEW IN 33.0.1.50

This section describes the new features and components introduced in this version on top of Alteon version 33.0.1.0.

Mid-session DNS Resolving

In some cases the load balancing decision needs to be based on the DNS resolution of the hostname in an HTTP request.

For this purpose, the Alteon sideband connection mechanism now supports DNS connection and a number of new AppShape++ commands were added (an AppShape++ script is required to handle extracting the relevant hostname from the HTTP request, handling the DNS resolution via the sideband connection and making the load-balancing decision based on the DNS record received).

NFR ID: 200602-000040

DNS over HTTPS (DoH) Gateway to DNS over UDP

DoH is a protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol. The goal is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks.

Alteon now supports realizing the security goals for DNS traffic over the public network without the need to replace the existing DNS servers to DoH servers. This is achieved by providing a gateway between DoH and DNS over UDP.

Note: Gateway between DoH and DNS over TCP was previously supported.

The DNS UDP back-end connection is implemented using the sideband connection mechanism.

An AppShape++ script is required to handle extracting the DNS query from the HTTP request, forwarding it to the sideband DNS over UDP connection, handling sideband connection response and encapsulating DNS response within HTTP response to client. The script can also handle cases where a truncated DNS response is received from the UDP servers (retransmitting the DNS query to the backend servers over TCP).

NFR ID: 201204-000103

AppShape++ Commands

A number of commands and events were added to support the new DNS sideband connection developed and its integration with HTTP traffic:

New commands:

- DNS::construct_query – Generates a DNS query as a binary string.
- DNS::parse_message – Parses the input binary data as a DNS message (query or response) into an internal buffer.
- DNS::message – Returns the content of the current DNS message.

- DNS::release_message – Releases the memory allocated for the DNS message before the session ends to reduce the memory used.
- HTTP::content_length – Retrieves the value of the Content-length header (size of the message body in bytes).
- HTTP::headers – Removes or replaces the entire HTTP headers section in a message (not valid for HTTP messages generated by a device).
- Sideband::payload – Retrieves or manipulates payload collected up to this time.
- Sideband::send – Sends the specified data message through the sideband connection.
- UDP::age – Closes session after a specified period.

New subcommands for DNS::edns0

- del_option – Deletes one of the ends0 options.
- add_option – Adds an option to edns0 pseudo-RR.
- get_option – Retrieves the value of the specified edns0 option.
- has_option – Checks the presence of the specified edns0 option.
- delrr – Removes the entire edns0 pseudo-RR.
- newrr – Creates an edns0 pseudo-RR.

New events

- SIDEBAND_RESPONSE – Triggered when a response message arrives on the sideband channel.
- SIDEBAND_FAILURE – Triggered when a sideband encounters a problem that prevents it from returning a valid response.

WHAT'S NEW IN 33.0.1.0

This section describes the new features and components introduced in this version on top of Alteon version 33.0.0.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 33.0.1.0.

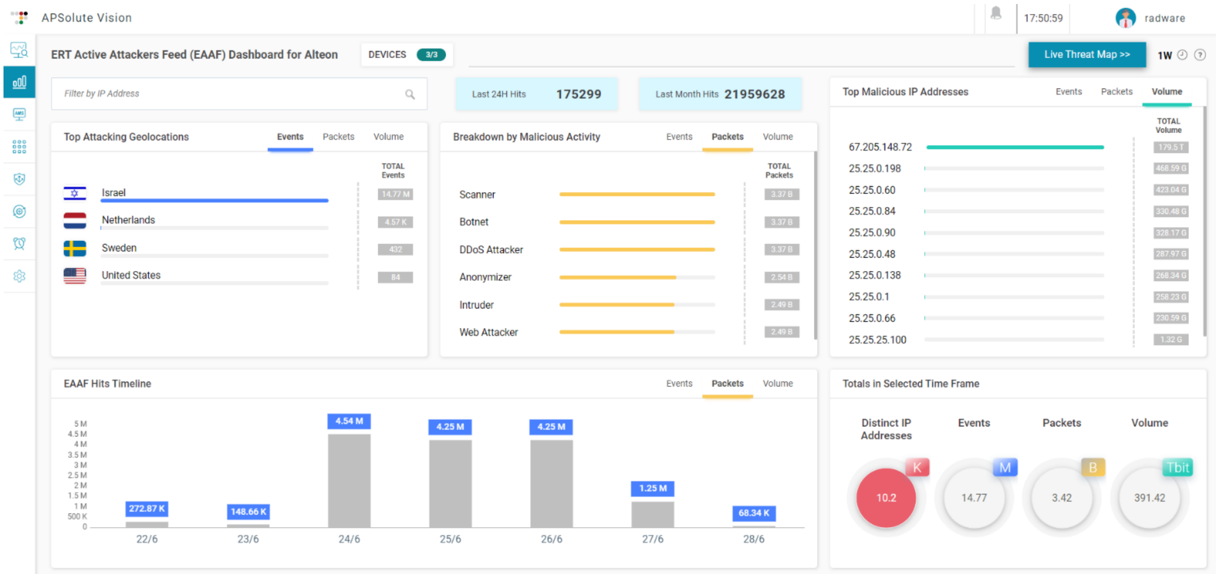
ERT Active Attackers Feed (EAAF)

The Radware ERT Active Attackers Feed (EAAF) is a subscription service that enhances Radware's Alteon Security capabilities by identifying and blocking IP addresses involved in major attacks in real-time, providing preemptive protection from known and currently active source IP addresses.

Starting with this version, Alteon fully supports the ERT Active Attackers Feed, meaning Alteon can mitigate traffic based on the updated feed, send EAAF events to APSolute Vision for display on a dedicated dashboard.

In addition, Alteon can mitigate IP addresses behind a CDN (IP header support). The user can select the relevant IP header from a list, or enter the header manually.

Note: The ERT Active Attackers Feed requires the Secure package and Secure subscription to download the updated feeds.



Top Attacking Geolocations

	TOTAL Events
Israel	14.77 M
Netherlands	4.57 K
Sweden	432
United States	84

Breakdown by Malicious Activity

	TOTAL Packets
Scanner	3.37 B
Botnet	3.37 B
DDoS Attacker	3.37 B
Anonymizer	2.54 B
Intruder	2.49 B
Web Attacker	2.49 B

Top Malicious IP Addresses

	TOTAL Volume
67.205.148.72	179.5 T
25.25.0.198	468.59 G
25.25.0.60	423.04 G
25.25.0.84	330.48 G
25.25.0.90	328.17 G
25.25.0.48	287.97 G
25.25.0.138	268.34 G
25.25.0.1	258.23 G
25.25.0.66	230.59 G
25.25.25.100	1.32 G

EAAF Hits Timeline

Totals in Selected Time Frame

Distinct IP Addresses	Events	Packets	Volume
10.2 K	14.77 M	3.42 B	391.42 Tbit

LinkProof Dashboard in APSolute Vision

The LinkProof analytics dashboard is now available as part of the ADC Analytics *System and Network* dashboard. It provides visibility into the status of each of the WAN Link as well as their current and historical performance up to 3 months.

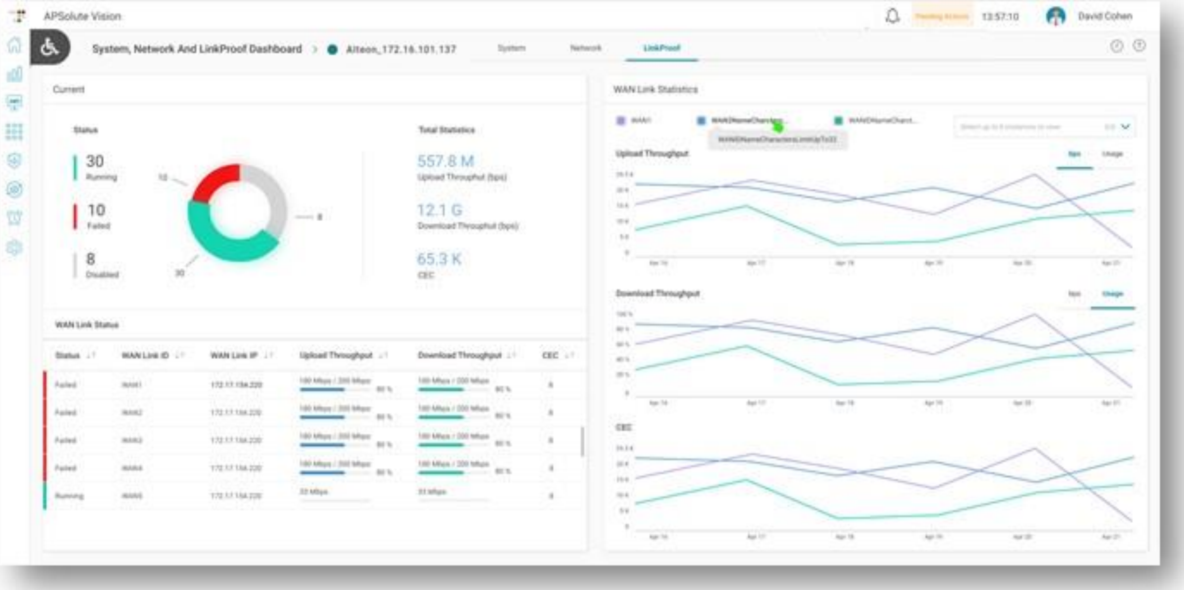
The LinkProof analytics in APSolute Vision includes the following:

- LinkProof dashboard
  - Current real-time status and performance
  - Performance over time, in a range from 15 minutes to 3 months
- LinkProof reporting template and widgets

This capability is available for WAN links defined in Alteon with the Perform license or above. It also requires the APSolute Vision ADC Analytics license.

These metrics are available over JSON using https://<device ip_address>/reporter/wanlink.

NFR: 200424-000128



WAN Link Status

Status	WAN Link ID	WAN Link IP	Upload Throughput	Download Throughput	CEC
Failed	WAN1	172.17.154.220	100 Mbps / 200 Mbps 80 %	100 Mbps / 200 Mbps 80 %	4
Failed	WAN2	172.17.154.220	100 Mbps / 200 Mbps 80 %	100 Mbps / 200 Mbps 80 %	4
Failed	WAN3	172.17.154.220	100 Mbps / 200 Mbps 80 %	100 Mbps / 200 Mbps 80 %	4
Failed	WAN4	172.17.154.220	100 Mbps / 200 Mbps 80 %	100 Mbps / 200 Mbps 80 %	4
Running	WAN5	172.17.154.220	33 Mbps	33 Mbps	4

Ansible Modules

Enable/disable/shutdown for a Specific Real Server Member of a Group

This feature enables configuring the real server state in a group via Ansible. For example, the same real server state can be enabled in group1 but disabled in group 2.

This feature is supported in Alteon version 32.4.*x* and later.

Ansible module name: alteon_config_group_real_server

NFR ID: 210204-000099

Configuration BGP peers Radware Internal -- GitHub (Enhancement)

This Ansible module enables configuring some of the BGP elements via Ansible.

This feature is supported in Alteon version 32.4.*x* and later.

Refer to the following table for details and limitations of this feature

BGP Element	Ansible Module Name	Limitations
BGP global parameters	alteon_config_bgp_global	Currently does not support configuring global parameters related to FRR mode.

BGP Element	Ansible Module Name	Limitations
BGP peer table	alteon_config_bgp_peer	Parameters related to FRR mode can be configured. However, if the mode is **legacy**, the fields are not set with the new value (but no error message is sent).
BGP aggregation table	alteon_config_bgp_aggregations	

NFR ID: 210119-000134

Public Cloud HA Enhancements

AWS Route Table Update on Failover

Alteon VA for AWS already supports transferring the elastic IP addresses of VIPs from the Alteon VA master to the backup in a manner that ensures the application will continue operating seamlessly in case of Alteon failover. Prior to this version, this support did not cover a scenario where the Alteon pair is used as the next hop in AWS routing.

Starting with this version, Alteon supports dynamically updating the AWS routing table when failover occurs. The Target of specified routes is updated with the ENI (Elastic Network Interface) of the Alteon that is now active.

To configure AWS route table update on Alteon failover:

1. Create the routes in the AWS routing table using the ENI of the primary Alteon as the Target.
2. On both Alteon devices, configure the routes that must be updated. Per route specify the route ID in theAWS routing table, the ENI of the Alteon which you are configuring, and the ENI of the peer Alteon.

   Note: Currently this configuration is available only via the CLI (`cfg/sys/aws/routes`).

Session Mirroring for SingleIP Alteon Devices in Azure

Prior to this version, session mirroring could not be supported on Azure in SingleIP mode because different VIPs are used for the same application in the two Alteon devices, and as a result the destination IP address of the sessions created on one Alteon device does not match the VIP on the peer Alteon.

To solve this issue, the ability to configure additional virtual IP addresses on Alteon VA in SingleIP mode was added in this version. This allows using the HA and session mirroring capabilities in the same manner as in multiple IP mode (the virtual IP addreseses are active on the active Alteon and are transferred to the peer Alteon when failover occurs – both the private and public ID):

- The session mirroring will work only for services deployed using the secondary VIP.
- The secondary VIP must be explicitly defined as Client NAT (PIP) for all its services.
- In the High Availability for Azure section, the local Alteon NIC ID and the peer Alteon NIC ID must be configured for the secondary VIP.

Important! The transfer of public IP addreseses on Azure takes time, sometimes up to 10 minutes, in which case the mirrored sessions will be irrelevant. Therefore, Radware recommends configuring session mirroring only when the clients access the services handled by Alteon devices using the private IP addresses.

Mellanox ConnectX-4 Support

Starting with Alteon version 33.0.0.0, Radware has added support for a new NIC (Network Interface Card) called ConnectX-4 (specific model: HPE Ethernet 10/25Gb 2-port 640FLR-SFP28 Adapter 817749-B21). Refer to the following link for a full specification of the NIC:

https://h20195.www2.hpe.com/v2/GetDocument.aspx?docname=a00047733enw&doctype=quickspecs&doclang=EN_US&searchquery=&cc=za&lc=en#

The support is added only for the Alteon VA platform using the Ubuntu-18 operating system.

Customers are expected to first install the NIC in their designated compute engine (VMware or other) in order to start utilizing it with Alteon VA.

NFR ID: 200722-000045

Cipher Configuration on Management

The cipher for management connection is now available for configuration (in OpenSSL format). In addition, the default “main” cipher-suite is now available by default to improve the security of the management connection.

Important: The default management cipher is now set to “main” and supports the following suites:

```
kEECDH+ECDSA:kEECDH:kEDH:RSA:kECDH:+AESCCM:+ARIA:+CAMELLIA:+SHA:+SEED:
!NULL:!aNULL:!RC4:!3DES:!DSS:!SRP:!PSK
```

NFR ID: 200724-000003

Bot Manager Additions

- Bot Manager now supports HTTP/2 traffic.
- **Sideband processing time –**The length of time in which Alteon sends requests to the sideband endpoint until it receives a response from it is now measured and displayed in the virtual service statistics (CLI and WBM), virtual service JSON, and unified event. The End-to-End time is also updated with the sideband processing time when the sideband takes place in the transaction, as follows:
  - **rdwrAltSidebandProcessTime** – The sideband processing time (in microseconds) per transaction. It displays in the unified event when the value is other than 0.

- **sidebandProcessingUsecs** – The sideband processing time (in microseconds) per virtual service. It displays in the virtual service Basic Analytics (https://device-ip/reporter/virtualServer).

Client IP Support in Traffic Event

In a proxy/CDN deployment, the original Client IP address is placed in a specific IP header, while the source IP address of the connection is the IP address of the proxy or CDN.

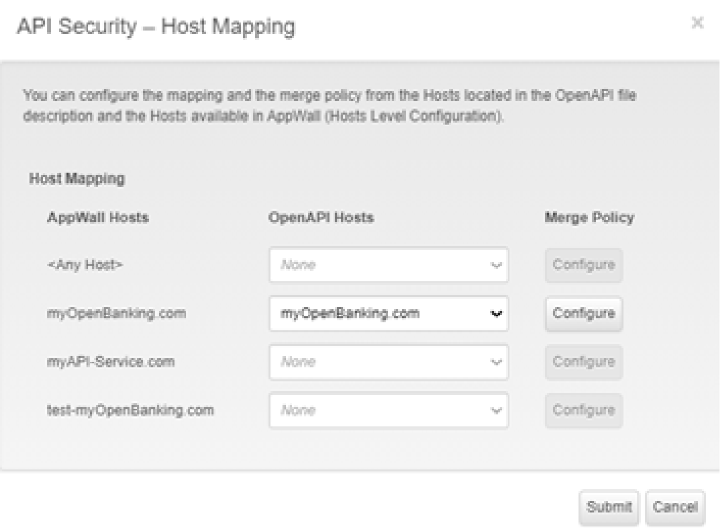
Starting with this version, a new field has been added to the virtual service which the user can define the IP header used by its CDN/proxy (default X-Forwarded-For). The IP address found in that header will be available at the unified event in a new parameter called **rdwrAltClientIp**.

Note: If the specified header is not available at the request, this field will contain the source IP address of the connection.

In addition, a new parameter called **rdwrAltIpHeader** is also available to contain the full content of the defined IP Header. This is required when the IP header contains a list of poxy IP addresses.

AppWall Features

1. API Security hosts protection has been updated with two new functionalities:
   a. **Host Mapping**: During the process of uploading a new OpenAPI file, it is now possible to choose to which AppWall Hosts to attach the OpenAPI file definition. An explicit use case is when DevOps usually assesses the configuration in a staging (pre-production) environment. With Host Mapping, DevOps can upload the future production OpenAPI file definition into a staging host and evaluate the schema enforcement, the Quota management, and the security inspection.



API Security – Host Mapping

You can configure the mapping and the merge policy from the Hosts located in the OpenAPI file description and the Hosts available in AppWall (Hosts Level Configuration).

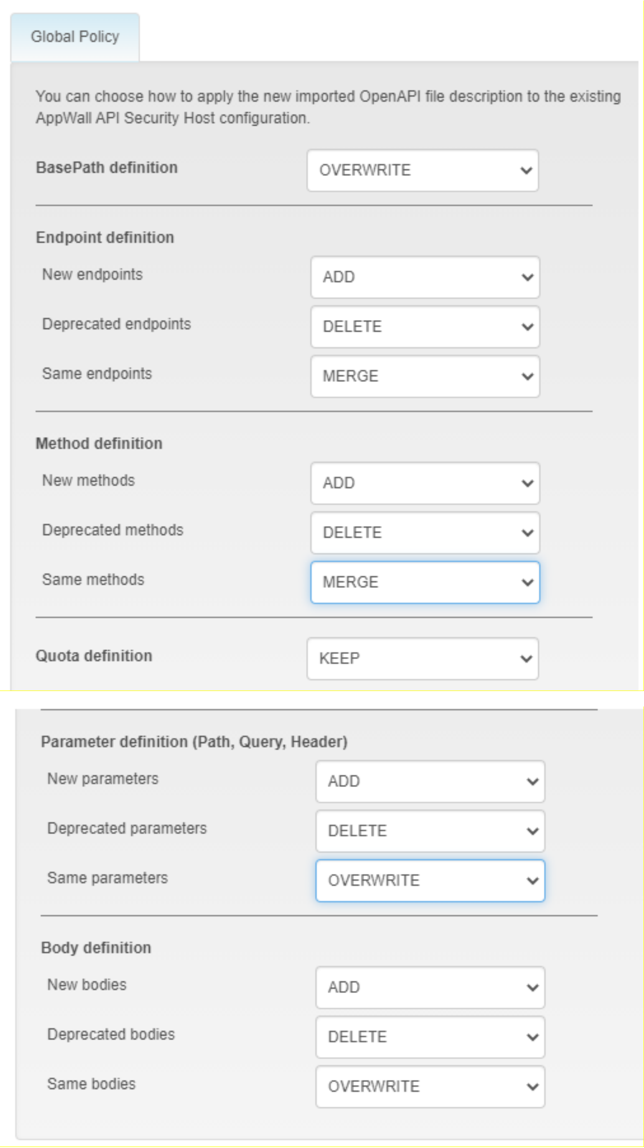
Host Mapping

AppWall Hosts	OpenAPI Hosts	Merge Policy
<Any Host>	None	Configure
myOpenBanking.com	myOpenBanking.com	Configure
myAPI-Service.com	None	Configure
test-myOpenBanking.com	None	Configure

   b. **OpenAPI file descriptor upgrade** is used after Host Mapping. It defines a Global Merge policy to combine the OpenAPI files into an existing AppWall host API security protection. Usually, for each subsequent release the development team provides an updated OpenAPI file that describes the new API service that must be merged into the AppWall API security module.

The API security lifecycle starts with the upload of the first OpenAPI file (version 1). After a period of time when refinements can occur, the API service is updated with a new release (version 2). AppWall performs the merge process of the new OpenAPI file.

The Global Merge policy offers multiple options to decide if the AppWall configuration should remain (with refinements), if the new OpenAPI file definition should replace the previous configuration, or to merge the definitions. The level of configuration is per base path, endpoints, methods, headers, parameters, and bodies.



You can choose how to apply the new imported OpenAPI file description to the existing AppWall API Security Host configuration.

BasePath definition: OVERWRITE

Endpoint definition

- New endpoints: ADD
- Deprecated endpoints: DELETE
- Same endpoints: MERGE

Method definition

- New methods: ADD
- Deprecated methods: DELETE
- Same methods: MERGE

Quota definition: KEEP

Parameter definition (Path, Query, Header)

- New parameters: ADD
- Deprecated parameters: DELETE
- Same parameters: OVERWRITE

Body definition

- New bodies: ADD
- Deprecated bodies: DELETE
- Same bodies: OVERWRITE

2. API Quota Management offers a rate limit functionality for API Security. When AppWall is installed in a cluster environment, each AppWall node inspects the traffic, and the cluster manager consolidates the number of API transactions processed from each AppWall node included in the cluster configuration. The cluster manager verifies if the quota is reached. Each AppWall node is updated and can block incoming traffic from a specific source IP address that may abuse the usage of the API service.
3. In this version, additional support has been added to decode Base64 data in headers. Support was added for more use cases in the Referer header and in the Cookie header.
4. The Destination IP, Destination Port, and Destination Host fields have been added to syslog messages generated by AppWall to external SIEM solutions.

WHAT'S NEW IN 33.0.0.0

This section describes the new features and components introduced in this version on top of Alteon version 32.6.3.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 33.0.0.0.

BOT Manager

Bot Manager per Content Rule Level

By default, the traffic that matches a content rule inherits the Bot Manager policy capabilities defined on the service.

Starting with this version, you can also **disable** Bot Manager processing in the content rule or set a **specific** Bot Manager policy per on the content rule (the default Bot Manager processing per content rule remains “**inherit”**).

This capability enriches the traffic matching possibilities to allow more accurate Bot Manager processing.

For example:

- A single virtual service that manages two (2) subdomains using two (2) content rules:
  - Content Rule 1 – Matches "**mobile.abc.com**" - Bot Manager policy with the mobile Application Type
  - Content Rule 2 – Matches "**web.abc.com**" - Bot Manager policy with the Web Application Type
- A single virtual service that manages three (3) unrelated applications:
  - Content Rule 1 - matches "**abc.com**" – Bot Manager policy with abc.com SID
  - Content Rule 2 - matches "**xyz.com**" – Bot Manager policy with xyz.com SID
  - Content Rule 2 - matches "**123.com**" – No Bot Manager processing

- Bypass Bot Manager protection for specific cases (such as a specific URL, User-Agent, and so on)

Bot Manager Policy Capabilities

- **Custom Response** – With this capability, you can define the required response in Active mode when receiving a CAPTCHA and/or block response. The response includes the response code, and optionally the response body and two (2) headers.
- **Web and Mobile on the Same Application** – For precise identification of a bot, it is important to distinguish between Web and mobile transactions. If the same virtual service (or content rule) manages both Web and the mobile traffic, you can now identify the Web/mobile transaction of the Bot Manager policy by classifying the traffic by user-agents, URLs, headers, or cookies. This allows the same Bot Manager policy to manage both Web and mobile traffic.
- **Include or Exclude Specific Headers** – For advanced Bot Manager detection, Alteon collects all the headers from a request and sends it to the Bot Manager endpoint for processing. Starting with this version, when "All Headers" is enabled, you can now specify a list of headers to either be included or excluded from the "All headers" collection.
- **Add SameSite Attribute to Set-cookie** – When Bot Manager is enabled, Alteon inserts a "set-cookie" header in the response back to the client so that the client can send it back on future requests. Starting with this version, the SameSite attribute has been added to the set-cookie operation. The SameSite cookie attribute lets you declare if your cookie should be restricted to a same-site or first-party situation. The default is Lax (enables only same-site cookies to be sent or accessed).
- **User ID encryption** – The User ID is an optional parameter in a Bot Manager policy. Starting with this version, the User ID value is encrypted using SHA1 when configured (instead of sending it in clear text).

Bot Manager in Unified Events

When Bot Manager is enabled in **active mode** and bot traffic is detected in a transaction, the unified event now includes the following new fields:

- The action code and action name received from Bot Manager for the transaction
- The identified bot code and bot type

Block Bot Manager Policy Configuration for a Redirect/Discard Service

Bot Manager processing is not relevant when the action is set to redirect and discard. Starting with this version, such a configuration is no longer allowed.

Integrated AppWall

Monitor Mode for SSL Traffic Enhancements

In this version, Radware has added the following new enhancements for Monitor mode for integrated AppWall:

- SSL Hardware offload support – SSL decryption by the SSL hardware cards is now available, which improves SSL performance for the Monitor model (the appliance must include a QAT card to use this ability).
- SSL Ticket reuse support

Google Cloud (GCP) Support

Alteon VA can now run on Google Cloud, in standalone mode (no HA).

BGP Enhancements

A new BGP library is now integrated into Alteon, which supports advanced capabilities such as IPv6 support. The first phase of the integration was part of version 32.6.3.0 and was limited to a small number of new capabilities, and only for non-ADC-VX form factors. The ADC-VX form-factor limitation is now removed, and additional capabilities have been introduced.

To ensure backward compatibility, the old BGP library is still available in the product and the user must select which BGP mode he wants to use:

- CLI: `/cfg/l3/bgp/mode`
- WBM: **Configuration > Network > Layer 3 > Dynamic Routing > BGP**

Note: Changing the BGP mode requires rebooting the device.

When upgrading from an older version to this version, if BGP is configured, the BGP mode is automatically set to the legacy library, while for fresh Alteon installations the BGP mode is set to FRR (the new library).

All of the new capabilities described here require the new FRR library.

IPv6

The new BGP library (FRR) provides BGP support over both IPv4 and IPv6 networks.

The user can now do the following:

- Define BGPv6 peers and verify their connection state
- Define IPv6 network filters and associate them to the Route Map access list
- Associate IPv6 network classes to the Route Map access list

- Dump the IPv6 prefixes it has learned via BGP
- View BGPv6 routes in the Alteon routing table

NFR ID: 191223-000038, 191223-000051

BGP Authentication

Alteon now supports the configuration of MD5 based authentication for BGP peers, meaning that each segment sent on the TCP connection between the peers is verified (each transmitted message has an MD5 digest that ca be checked by receiving peer).
MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made.
To enable MD5 authentication, configure the appropriate password for each peer (`cfg/l3/bgp/peer <peer id>/password`).

NFR ID: 200505-000068

BGP Graceful Restart (RFC 4724) – ADC-VX

Usually when BGP on a router restarts, all the BGP peers detect that the session went down and then came up.

This “down/up” transition results in a “routing flap” and causes BGP route re-computation, generation of BGP routing updates, and unnecessary churn to the forwarding tables.

BGP Graceful Restart enables retention of the routing table when routers restart. It enables a BGP speaker to indicate its ability to preserve its forwarding state during BGP restart, and forwards data packets along known routes while the routing protocol information is restored.

This capability is now available in Alteon, but only in FRR mode. It is possible to globally enable Graceful Restart (disabled by default) and to tweak the restart and stale time.

When Graceful Restart is globally enabled, it can also be enabled/disabled per BGP peer.

This capability was initially introduced in the previous version but not for ADC-VX platforms. Now it is available for all form factors.

NFR ID: 190911-000276

BGP Community Support – ADC-VX

BGP communities provide policy-driven decision-making for incoming and outcoming routes. The main objective of the community attribute is to minimize the management overhead of routing policy implementation. The community attribute tags a group of IP prefixes using a particular value and the route-map rules can be based on these community attribute values instead of individual IP prefixes/AS values.

Alteon provides support for the following three major types of community attributes:

- Standard Community Attribute [RFC 1997 - BGP Communities Attribute]
- Extended Community Attribute [RFC 4360 - BGP Extended Communities Attribute]
- Large Community Attribute [RFC 8092 - BGP Large Community Attributes

This capability is available only in FRR mode and was initially introduced in the previous version but not for ADC-VX platforms. Now it is available for all form factors.

NFR ID: 190911-000426

Multiple RW and RO SNMP Communities

Multiple community strings are supported on the same Alteon device for SNMP1 and SNMP2.

NFR ID: 200511-000135

Static Routes on the Management Interface

Starting with this version, you can define static routes on the Management interface. This is available for all form factors (standalone, ADC-VX, and vADC).

NFR ID: 200511-000006

Traffic Distribution for Alteon VA

When more than two SPs are allocated for Alteon VA, the TD process is required to distribute the traffic between the SPs.

Prior to this version, by default, the traffic was distributed based on RSS. In this version, it is now possible to select a different algorithm using the new command `cfg/slb/adv/tdhash`. The options are:

- RSS (default)
- L3 – Hash of the source and destination IP address
- L4 – Hash of the source IP address, and port and destination IP address, and port for TCP and UDP packets. For non-TCP/UDP packets, L3 hash is performed

In addition, a new command `cfg/slb/adv/tdtnhash` was added to allow distributing the traffic that arrives via an L3 tunnel in an optimal way. The options are:

- L3 – Hash of source and destination IP address in the tunnel's inner header (default value).
- L4 – Hash of source IP address, and port and destination IP address, and port for TCP and UDP packets. For non-TCP/UDP packets, L3 hash is performed.
- None – The distribution is based on the tdhash configuration described above, which takes into account only the packet IP header.

Disable ARP for VIPs

Starting with this version, it is possible to disable answering ARP requests for VIP addresses. By default, ARP is enabled. This can be useful in certain two-tier cluster scenarios where the same VIP is configured on both T1 and T2 devices (the two tiers are connected via a Layer 3 tunnel) and the client and both Alteon tiers are in the same Layer 2 network.

Any MSS Values

The MSS parameter in a TCP policy can now accept any value that is less than MTU-40.

Note: In WBM, in order to enter a value other than the available predefined options, click the empty line at the end of the drop-down list.

WHAT'S CHANGED IN 33.0.2.0

Additional Disk for Alteon VA on VMware

On Alteon VA devices, the requirement for additional disk space increases as applications use the disk space for database storage.

In previous versions, Alteon supported adding a secondary disk, where all the application-related data was moved, and the primary disk was left with the OS-related items needed to boot up the VA device, which cannot be removed. Most of the primary disk space was left unused.

Starting with this version, Alteon supports VA disk expansion for Ubuntu 12-based running on VMware ESX server. This new feature provides an efficient way to increase the primary disk size of VA while avoiding disk space wastage.

Notes:

- You cannot perform both VA disk expansion and addition of a secondary disk.
- VA disk expansion is allowed only once, so Radware recommends increasing the disk size fully as needed during the VA disk expansion procedure.
- VA disk expansion is supported only on VAs deployed using OVAs of version 31.0.0.0 and later.
- VA disk expansion is supported starting with Alteon versions 32.4.8.0, 32.6.6.0, and 33.0.2.0 and later.
- Once VA disk expansion is performed, you cannot upgrade/downgrade to a version where this feature is not supported.

OpenSSL Version

The OpenSSL version has been updated to OpenSSL 1.1.1l.

AppWall Enhancements

1. AppWall management API Security hosts protection has been updated. You can now:

   a. Edit the Path parameter name
   b. Add/delete a new Endpoint definition
   c. Add/delete a new Method
   d. Other UI improvements

2. Database Security Filter performance has been improved in term of time to inspect the request data

A new section was added to the Tunnel Parsing Properties to refine the HTTP boundaries per URI. You can now configure AppWall to accept HTTP requests with a Body or refine such HTTP requests (HTTP Request Smuggling attacks) from the security events. If so, AppWall will accept the request and transfer the body payload to the server.

SSL Private Key Store Encryption using AES

In this version, newly created private keys are now stored and exported with AES256 encryption.

Important: Existing private keys will still be encrypted using 3DES.

NFR ID: 200921-000220

Application Service Engine Logs Enhancements

The `logonses`, `svrtylvl`, and `printon` commands control the trace log session feature.

When `logonses` is enabled, the Application Service Engine (AX) stores the logs in memory (according to the value of `setlevel`) and prints to hard disk only the session logs defined with a severity level (`svrtylvl`). You can set the logs to print immediately or on session end (the setting is controlled `printon`).

This feature improves the readability of the logs as only the relevant logs are printed and in chronological order.

APM Removal from WBM

Due to the deprecation of the Flash player, APM can no longer be supported. Therefore, APM related parameters and mentions were removed from WBM, documentation, and partially from CLI.

Note: Radware recommends that you delete the APM Server configured on your devices as well as disable APM on all the applications. This is required to eliminate performance impact.

WHAT’S CHANGED IN 33.0.1.0

Cluster Persistency Data Sync

The cluster persistency data sync interval (`/c/slb/sync/cluster/interval`) determines timing for synchronization of new persistency entries and updates of the persistency entries ages.

In this version, a new value was added for the interval parameter – 0. When the interval is set to 0, new persistency entries are immediately synced to the other cluster members. When the interval is greater than 0, the previous behavior is maintained; new entries are synchronized once 32 new entries need sync or the interval is reached, whichever occurs first.

SSLi Dynamic Certificate Cache Key

The dynamic certificates generated for outbound SSL inspection are stored in a cache. Prior to this version, the cache key was based on SNI + destination IP + destination port. In cases where the same certificate (SNI) is received from different IP addresses/ports, Alteon generated and stored duplications of the certificate.

To overcome this situation, this vesion introduces the option to generate and store the dynamic certificate based on SNI only (the default remains SNI + destination IP + destination port).

Notes:

- Changing the cache key (/`c/slb/ssl/inspect/cachekey`) requires first disabling the SSL inspection filters.
- In a 2 box solution, the cache key configuration must be done on the client-side box.

NFR ID: 201210-000099

OpenSSL Version

The OpenSSL version for S/SL platform models, regular platform models, and Alteon VA has been updated to OpenSSL 1.1.1k.

Server Failure Reason on Block State

A server failure reason is now also available when the server is in the **Block** state due to

- An advanced health check failure
- A server is down in another service that uses the same server group
- A server that has multiple rports while one port is down

Trace Log Update

From WBM it is now possible to set the application level trace log of each module. The default level remains “Error” as in previous versions.

Bot Manager Updates

- The User ID is an optional parameter in a Bot Manager policy. Starting with this version, the User ID value is encrypted using SHA1 when configured (instead of sending it in clear text).
- It is now possible to clear Bot Manger statistics separately from the SLB statistics. This can be done using the CLI command `/stats/security/botmng/clear`, or from the WBM
- The cookies that are added to the client communications as part of Bot management processing, have now been removed from the client request before sending to the server.

Security Notice when Telnet is Enabled

Telnet is a non-secure plain-text protocol. Radware recommends using SSH instead. A warning message displays when enabling Telnet.

NFR ID: 201231-000094

Warning Messages and Notifications

- A message is sent to the syslog every 15 minutes when a packet capture is running. This periodic syslog can be disabled using the following command: `/maint/pktcap/pcaplog`
- When switch HA is enabled, Radware highly recommends to sync the PIP configuration. On Apply, a warning message displays when switch HA is enabled if PIP synchronization is disabled.
- The legacy Device Performance Monitoring capability (DPM) is not related to ADC Basic Analytics and it is being retired. As DPM has a performance impact, it should not be enabled if not specifically required.

  To eliminate misconfiguration, the following message displays when enabling DPM: “*DPM shouldn’t be enabled for ADC Basic analytics support*”

Traffic Events Update

In the unified event, the **in** and **out** parameters that represent the number of bytes in the request and response now appear in the event even if their values are 0 (for example, in a GET request the in value that is generally 0 now displays in the event).

AppWall Features

1. In the Tunnel configuration, AppWall now defines multiple properties related to the HTTP parser per URI. The following changes have been added in this version:
   a. By default, when adding a new URI, the following parameters are validated:
      i. Allow Parameter without an equal sign
      ii. Fast Upload for large HTTP requests
      iii. Fast Upload for large HTTP requests with files

   b. The option “Use IIS Extended Unicode Measures (Block Unicode Payloads)” has been removed from the AppWall management console but is still available from the configuration file.

2. The BruteForce Security Filter prevents remote users from attempting to guess the username and password of an authorized user. The option “Shared IP auto-Detection” check box has been removed from the AppWall management console to limit false positives.
3. Remote File Inclusion (RFI) and Local File Inclusion (LFI) are file inclusion vulnerabilities that allow an attacker to include a file or expose sensitive internal content, usually exploiting a “dynamic file inclusion” mechanism implemented in the application. In the Hosts protection section, by default, Redirect Validation is in passive mode with the option “Protect against external URL” activated.
4. The Tunnel IP (VIP), the Port and the Host have been added to the system log event titled "Large number of parameters in request".

WHAT’S CHANGED IN 33.0.0.0

DNS Resolver Enhancements

DNS Cache per IP version

In previous versions, the cache used to provide persistency for DNS responses provided by Alteon kept a single record per domain name + client subnet combination. In a scenario where both IPv4 and IPv6 VIPs are available for the same domain, this was problematic – when the same client/client subnet sent both A record and AAAA record queries for the same domain, the IPv4 and IPv6 responses would overwrite each other, and persistency was not maintained.

Staring with this version, separate records are maintained per IP version, ensuring persistency can be maintained in such scenarios.

NFR ID: 201123-000091

Response for Unsupported Record Types (first introduced in version 32.6.3.50)

Previously, Alteon used to answer queries for unsupported record type of domains supported by the Alteon DNS resolver (for GSLB and LinkProof) with "Domain does not exist" (NXDOMAIN). This was now changed to the standard behavior required for such a scenario – answering with a No Error response code and 0 records.

NFR ID: 200723-000119

OpenSSL Version

The OpenSSL version for S/SL platform models, regular platform models, and Alteon VA has been updated to OpenSSL 1.1.1i.

Note: The CVE-2021-3449 vulnerability that was discovered for OpenSSL 1.1.1 is fixed in this version for the data path. For the management path, Radware currently recommends disabling TLS 1.2.

Treck Version

The Treck version has been updated to 6.0.1.69.

MAINTENANCE FIXES

The following sections list the fixed bugs included in this release.

Fixed in 33.0.2.0

General Bug Fixes

Item	Description	Bug ID
1.	The L4oper user could not view the Virtual Servers pane.	DE65790
2.	Self-generated sessions (such as sideband connections and rlogging traffic) now apply the PIP configuration regardless of the PIP port processing settings	DE66411
3.	Too many core files took up too much disk space, resulting in techdata failing.	DE66124
4.	The CRL could mistakenly be considered expired before the true expiration time because of the time zone.	DE66218
5.	The device became full with too many open files, causing it to run slowly.	DE66427
6.	Alteon sent malformed SNMPv3 traps when aes128 or aes256 were configured as the privacy protocol.	DE66749
7.	STP packets dropped by the ND caused a loop.	DE66782
8.	When passing the client certificate via the HTTP header in a multiline in compatible mode, the last hyphen (-) was removed.	DE67198
9.	The router ID was not visible for between routers for traceroute.	DE67261
10.	There was a WBM error for the SLBVIEW user.	DE67376
11.	Using WBM, the DNS responder VIP displayed as up even if it was disabled by configuration.	DE67545
12.	With VMAsport enabled, SSL-ID based persistency was not maintained correctly.	DE67634
13.	When traffic matches a filter that is configured with layer7 loopup, Alteon panicked.	DE67656

Item	Description	Bug ID
14.	Incorrect units displayed for uploading/downloading bandwidth for WANlink real servers.	DE67714
15.	The network driver process was stuck and caused Linux core 0 to be stuck. This caused the MP to be stuck.	DE67718
16.	When deleting a group and the FQDN associated with that group, the group was deleted twice from the AX database.	DE67724
17.	There was a non-existing Rlogging policy on a disabled traffic event policy.	DE67727 DE67730
18.	In WBM, the real server table displayed as empty.	DE67822
19.	Using AppShape++, when attaching/detaching a content class SSL from a filter, the AppShape++ command was removed and recreated, but the order was incorrect.	DE67834
20.	AppWall init completion took a very long time.	DE67867
21.	When the /stats/slb/virt all CLI command was executed, the virtual server internal index passed incorrectly. Due to this, the CLI did not display statistics. The same behavior also occurred for the /info/slb/virt all command.	DE67901
22.	There was a crash in the external "nano messages" package.	DE67940
23.	The AppWall process took more time to start than expected.	DE68031 DE68035
24.	In a virtual environment, configuration sync from the ADC-VX failed.	DE68062
25.	An empty AVP prevented AppShape++ from parsing a RADIUS transaction.	DE68082
26.	Some Fastview configuration files were not updated as part of the new feature using FastView JS injection capabilities.	DE68089
27.	When the hold timer expired, Alteon sent a notification with a cease.	DE68095

AppWall Bug Fixes

Item	Description	Bug ID
1.	HRS attack: HTTP GET request with BODY was not being blocked while there was a security event.	DE65623
2.	Under some conditions, the AppWall management console WAF stopped working and was not accessible.	DE67515

Item	Description	Bug ID
3.	The AppWall Activity Tracker recognized a legitimate Google search engine as a bad bot.	DE67646
4.	Wrong hosts reported with AppWall Hosts protection.	DE64012
5.	AppWall blocked the server response when a tunnel was in passive mode.	DE65600

Fixed in 33.0.1.50

General Bug Fixes

Item	Description	Bug ID
1.	In an RSTP environment, the port state transition from DISACRD to FORWARD was delayed.	DE66169 DE66170
2.	The SSL Hello health check caused a memory leak which led to a panic.	DE66191
3.	Alteon VA in DPDK mode crashed when BWM processing with BW shaping was enabled.	DE66399 DE66402
4.	After configuring a deny route for a DSR VIP with tunnels set to real servers, the MP panicked.	DE66473 DE66476
5.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66480 DE66483
6.	Using WBM, when users of type 'user' was disabled, they could still successfully log in.	DE66531 DE66534
7.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66573 DE66576
8.	Could not create a new BWM policy on a 4208 device.	DE66623 DE66626
9.	Panic analysis.	DE66641 DE66644
10.	A panic anaylsis resulted in the following fix: The Watcher can now run over multiple CPU cores, ensuring that it retrieves the expected CPU time even if an unexpected event occurs on CPU #0.	DE66705 DE66708
11.	After a Trust CA group was configured, no other certificates could	DE66722

Item	Description	Bug ID
	be deleted even if they were not part of the Trust CA group.	DE66725
12.	Using WBM, after receiving the "Apply Operation succeeded" message, no configuration change actually occurred. This was because a previous Apply has failed due to a certificate error.	DE66731 DE66734
13.	When AES128 or AES256 were configured as the privacy protocol, Alteon sent malformed SNMPv3 traps	DE66752
14.	In an SLB environment, changing a virtual server IP address from a non-VSR to a VSR VIP address resulted in the old VIP entry not being removed from the ARP table.	DE66805 DE66808
15.	BGP neighboship did not get established because of issues with the AS number functionality.	DE66813 DE66816
16.	Using WBM, when refreshing the Virtual Services tab, the VS status displayed as Warning instead of UP.	DE66883 DE66886
17.	The user was unable to access Alteon WBM.	DE66892 DE66895
18.	Panic analysis.	DE66956 DE66959
19.	Starting with this version, the SNMPv3 target address table is available in the Ansible module.	DE67004 DE67007
20.	When the SP CPU was activated, a false `Throughput threshold exceed` message displayed.	DE67121 DE67124 DE67127
21.	There was an overflow of RAM disk memory allocated for logs.	DE67133 DE67136
22.	Using WBM, real servers and groups are not displayed for HA tracking.	DE67277 DE67280
23.	When a PUSH/ACK was received from a client after the session closed or timed out, the RST always went to the AW monitor and dropped.	DE67292 DE67295
24.	There were WBM errors for the SLBVIEW user. Added support for missing tables in the users file to remove the errors.	DE67379
25.	In WBM, HAID did not display properly.	DE67455 DE67458

Fixed in 33.0.1.0

General Bug Fixes

Item	Description	Bug ID
1.	The random salt was a predictable random number generation function generating a similar sequence.	DE63668
2.	Could not enable the extended_log via Ansible.	DE63841
3.	For some edge cases, AppWall did not come up because of an invalid variable that was not initialized. The fix was to initialize the variable.	DE63985
4.	When Alteon initiated the connection to a peer that was not directly connected, the outgoing interface was not selected correctly, resulting in the BGP connection not being initiated. For the fix, the interface used to reach BGP peer is now selected.	DE63992
5.	The real health check displayed a different times in CLI and WBM.	DE64033
6.	On a 4208 platform, the option to convert to virtual (ADC-VX/ADC) mode displayed the following error message: The operation cannot be performed	DE64092
7.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64155
8.	The MGMT port status was DOWN but the Link and operational status was UP.	DE64235
9.	In an SLB environment with cookie insert enabled, the server responses to the client undergoing cookie processing had a mismatch of the SRC MAC with an incoming client request.	DE64248
10.	An internal link on Alteon VA caused connections to drop.	DE64257
11.	In an HA environment, when the RADIUS service was enabled with mirroring and associated with an AppShape++ script , RADIUS authentication timed out.	DE64321
12.	Applying part of the nginx when disabling the Web proxy took too much time.	DE64336
13.	When pbind clientip and vmasport were enabled, the persistent session was not permanently deleted.	DE64356

Item	Description	Bug ID
14.	Servers were vulnerable to CVE-2021-3449 if they had TLSv1.2 and renegotiation enabled (default). **Fix**: The MP OpenSSL version has been upgraded to 1.1.1k to fix this.	DE64380
15.	Added a REGEX to accept the dot (.), slash (/), and backslash (\) characters.	DE64459 DE64466
16.	Config sync transmit was aborted between two devices when the sync request was received from a third device.	DE64488
17.	Predefined HTTP headers were used when POST HTTP health checks were sent without taking into the account the actual body length.	DE64524
18.	After receiving the same routes in BGP updates when Alteon failed to set a protocol owner, Alteon deleted the RIB.	DE64534
19.	Using WBM, ephemeral servers did not display in the Configuration menu.	DE64586
20.	After performing /boot/shutdown, TLS version 1.1 was incorrectly being set to enabled.	DE64597
21.	In a BGP environment, when BGP peers were directly connected, the BGP state stayed as Connect even though the local interface was disabled.	DE64648
22.	Using a logical expression health check resulted in an unexpected real server state.	DE64691
23.	Upgrading an ADC-VX generated the following error message on the console: write error: Broken pipe	DE64704
24.	The management Web server did not work due to a bug with the access SSL key on FIPS.	DE64727 DE64732
25.	When the primary group was in an overloaded state, real servers in the backup group displayed as being in the BLOCKED state in the virtual server information.	DE64759
26.	An ICMP unreachable packet coming from the server side gateway was forwarded to the MP instead of the VMASP, which led to a panic while updating the filter information to the frame's metadata.	DE64787
27.	The Layer 2 system configuration had an incorrect BoardType for 7216NCX.	DE64884 DE64889

Item	Description	Bug ID
28.	When real servers were down, Alteon sent traps with the wrong OID.	DE64900
29.	In an SLB environment, when the primary server failed, the secondary backup displayed as "UP" instead of "BLOCKED".	DE64925
30.	On a 7220 platform, when Alteon received a packet with a size greater than 1500, it panicked.	DE64947
31.	In DPS Perform mode, AppWall was not pushed to vADCs.	DE64997
32.	The weighted least connection was not correct.	DE65009
33.	When there was a state transition from backup to master, GARP was not sent.	DE65041
34.	An SP memory leak was caused due to a combination of Bot Manager and the Mux.	DE65056
35.	There was an incorrect rule ID for retrieving statistics from the SP.	DE65178
36.	Added the FastView smfhub self-healing mechanism.	DE65204
37.	Defect that tracked DE65346 -- Device auto rebooted with reason of hardware watchdog.	DE65235
38.	Accessing a device using APSolute Vision or WBM caused a memory leak and eventually led to a panic.	DE65241
39.	In an SLB environment, when a connection closed from the server side with an RST, traffic failed on the new connection that matched the session that was in fastage.	DE65285
40.	Even though there are no open connections, new SSH connections were ignored with a "max connection reached" error.	DE65302
41.	The comparison function used to compare the SSL policy name was incorrect.	DE65318
42.	Added more information to the debug log when an ASSERT occurs on an ndebug image.	DE65338
43.	After performing config apply, GSLB DNS responses returned a remote IP address instead of a local VIP.	DE65365
44.	The MP CPU utilization was high when querying virtual stats.	DE65380
45.	A conncection drop occurred because a virtual service was reset due to a virtual index mismatch after applying new configuration changes.	DE65406
46.	SIP UDP service run by AppShape++ failed (it was used for persistency and/or Layer 7 manipulation).	DE65436

Item	Description	Bug ID
47.	After attaching a second hard disk to Alteon VA, the DPDK network driver did not load.	DE65452 DE65459
48.	The Alteon Data interface with port range 40k-45k mistakenly was accessible from outside world.	DE65486
49.	Even though the SP/MP profiling logic was disabled by default, Alteon panics with SP profiling logic being triggered.	DE65492
50.	Whenever multiple requests were sent with a cookie in a single session for multiple services, Alteon did not decrement the current session properly.	DE65505
51.	Alteon displayed the diff and diff flash without any configuration changes.	DE65536
52.	Using RCA, there was an incorrect virt-sever ID display.	DE65567
53.	AppWall crashed when not receiving the i/o time.	DE65571
54.	The SP performed unequal traffic distribution.	DE65606
55.	When burst traffic was sent to Alteon, some p-sessions remained in the zombie/stale state.	DE65664
56.	Added support for the IF IP to connect to the service dashboard.	DE65681
57.	Added a maint debug CLI command to export the virtual stat service table to understand the cause of the virtual stats not working.	DE65706
58.	A new Regex command forbade a hyphen (-) by mistake.	DE65721
59.	When an ARP entry is deleted, sending queued packets to the ARP entry after ARP resolution some times leads to an MP freeze and eventually leads to an MP panic.	DE65743
60.	In an RTSP environment, the RTSP service stopped working and all the SYN packets were dropped.	DE65747
61.	When all 24 GBICs were inserted, the Watcher timed out when ports were initiated.	DE65785
62.	When a vADC Layer 2 configuration was applied/pushed to an ADC-VX (with /c/vadc/add or rem), if at the same time a vADC Apply (or config sync) occurred indicated by a flag, a race condition while logging this configuration caused the vADC to freeze while waiting for the flag, and was eventually restarted by the Watcher.	DE65832
63.	Performing gtcfg via SCP resulted in a panic.	DE65858
64.	Multi-line notices via ansible did not work.	DE65859

Item	Description	Bug ID
65.	Added the HW platform type MIBs for 6024, 5208, and 8420 to the MIB tree.	DE65866
66.	When vmasport was enabled, the service ceased working.	DE65897
67.	The AppWall service did not restart after being ended by the MP.	DE65918
68.	The /c/port xxx/gig/cur command displayed breakout details, even though breakout was not applicable.	DE65938
69.	When the rlogging TCP health check is running via the MGMT port, Alteon sometimes panics.	DE65955
70.	When BFD and tunneling were enabled, a panic occurred.	DE66002
71.	Using SNMP, OIDs errorCountersSpTable and eventCountersSpTable could cause Alteon to not be accessible via SSH or WBM.	DE66031
72.	With the command logging feature enabled, Apply/Save resulted in a panic.	DE66103
73.	While initiating the SSL client connection for the SSL health check, the vADC MP crashed.	DE66140
74.	Adding and deleting real servers or groups resulted inan AX Out-Of-Sync error.	DE66180

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall Publisher does not send syslog security events .	DE64858
2.	Under rare conditions, after an upgrade, the AppWall configuration file was empty.	DE65443
3.	In APSolute Vision, Brute Force security events do not display the “request data” payload.	DE65248
4.	Could not submit a change to the AppWall configuration from the user interface.	DE65271 DE58941
5.	An AppWall configuration file became corrupted after a system upgrade.	DE64176
6.	A RuleID was triggered with a request that does not contain a character.	DE64175
7.	A RuleID was triggered with a request that contains a specific Chinese character.	DE64517

Fixed in 33.0.0.0

General Bug Fixes

Item	Description	Bug ID
1.	Upon Submit, there was a Quick Service setup wizard internal error.	DE57042
2.	On PSU failure, Alteon displayed a generic message instead of a more specific one.	DE59051
3.	In WBM, the equivalent to the filterpbkp CLI command was missing.	DE59723
4.	When the SSH connection with the correct password was attempted for a locked user, the user lockout status was checked too late.	DE60697
5.	Using WBM, a 50X error occurred due to buffer leak in an HTTPS request.	DE60769
6.	When resolving a DNS PTR record, IP matching was skipped (for both hostlk enabled or disabled) if the service hostname was not configured. Now, the service hostname check is skipped only if the hostlk is disabled.	DE60814
7.	When sending an OCSP request over the management port, there were two leaks.	DE60854
8.	When a syslog file had long log messages, the /info/sys/log command did not display any log messages.	DE60890
9.	When the management WBM listener connection control block was closed during its validation, a 50X WBM error displayed.	DE60918
10.	During configuration export, creating the AppWall configuration failed, and as a result the entire operation failed.	DE60945 DE60954
11.	Alteon sometimes would crash when it received the same applyfilter deletion and network class deletion that was assigned to the PIP that was defined for the real server.	DE61034
12.	Following a set of SNMP operations, on some occasions Alteon panicked from a memory corruption with a boot reason power cycle.	DE61048
13.	In an Alteon HA environment with an SNAT configuration in AppShape++, changing, applying, and synching non-SLB configurations resulted in the following syslog warning: Configuration is not synchronized	DE61099

Item	Description	Bug ID
14.	If Alteon received a request when all real servers were down, the group with all the real servers' indexes less than 33 and the RR, BW, or response metric failed to select a real server, even if they came up.	DE61149
15.	When Alteon had high MP memory utilization, restarting caused configuration loss. Alteon came up with the default configuration.	DE61210
16.	There was no support for query type return errors even if the domain was found.	DE61257
17.	On a 6024 standalone platform, starting with version 32.6.2.0 the maximum real servers' value was incorrectly reduced from 8K to 1K as a result of a defect (DE61270) when moving the 6024 platform to the DPDK infrastructure.	DE61279
18.	Accidently blocked disabled content rules with an HTTP content class to be configured on an HTTPS service without an SSL policy. It was blocked only if the content rule was enabled.	DE61347
19.	AppWall was stuck and did not process traffic but was not restarted by the MP.	DE61469
20.	Using WBM, when configuring the Nameserver group under DNS Authority, the table name in the mapping file was incorrect.	DE61488
21.	Alteon did not forward traffic when LACP was disabled and worked as expected when LACP was enabled.	DE61527
22.	Using WBM, there was a display issue when modifying a virtual service with actionredirect.	DE61604
23.	There was no support for query type return errors even if the domain was found.	DE61646
24.	The serial number was missing in the output for the /info/sys/general command.	DE61670 DE61679
25.	vADCs did not process SSL traffic.	DE61699
26.	On a 4208 platform, the link was down for the 1 GB SFP port.	DE61715 DE61724
27.	There were no Mibs for the health check count to display them for the command /info/sys/capcityswitchCapHealthCheck MaxEntswitchCapHealthCheckCurEnt.	DE61745
28.	Alteon closed the front-end and back-end SSL connection abruptly. Fixed the classification of second request if there is content class SSL.	DE61786

Item	Description	Bug ID
29.	When a DNS responder service was created, the user was allowed to configure parameters, which caused errors. Now the user can no longer configure parameters in this case.	DE61884
30.	In an HA environment, synching the configuration to the peer device with sync tunnel config flag disabled results in the peer panicking.	DE61964 DE62017
31.	When the ND packet aggregation mechanism was active, a ping response was not sent immediately, resulting in a delay in the ICMP response.	DE62067
32.	When while handling malicious DNS packet with compression pointer loops, Alteon panicked.	DE62134
33.	Snmpbulkwalk on the capacityUsageStats node returned invalid OID output.	DE62236
34.	Failed to access the Alteon WBM and the SSH connectivity was lost.	DE62312
35.	After upgrading to version 31.0.13.0, uneven load balancing started.	DE62338
36.	In a DSR and multi-rport configuration environment, the /stat/slb/virt X command returned statistics as 0.	DE62346
37.	Actions changing the configuration (such as Apply, Save, and Diff) were incorrectly allowed for users with viewer/operator classes of service when REST requests were sent.	DE62396
38.	Even after changing the log level from debug to error, warning messages continued to be issued.	DE62439
39.	A ticket from a failed connection required passing over the authentication policy on the next connection.	DE62489
40.	In rare circumstances during tsdmp or techdata export, a panic would occur.	DE62555
41.	With specific browsers, HTTP2 traffic with an uncommon form in the header was not answered.	DE62611
42.	Exporting a configuration from ADC-VX did not work.	DE62636
43.	Incorrect MTU syslog messages were issued for vADCs.	DE62658 DE62663
44.	The packet capture timestamp was incorrect.	DE62734
45.	On an ADC-VX, the HW Watchdog rarely rebooted due to an unknown trigger.	DE62751

Item	Description	Bug ID
46.	While exporting techdata, IPv6 connectivity went down for a short while and then came back up.	DE62824
47.	When uploading a Layer 2 packet capture from an ADC-VX to the FTP server, Alteon panicked.	DE62855
48.	Using Ansible, could not configure the TLS 1_3 parameter.	DE62866
49.	The WANlink current sessions count for IPv6 SmartNAT were not decremented properly due to using the wrong index. As a result, the /stat/slb/real and /stat/slb/lp/wanlink command displayed accumulated values. It has been fixed by using an appropriate index for updating the statistics.	DE62886
50.	There was vADC auto-reboot issue because of a software panic.	DE62947
51.	A config sync from a non-HA device to an HA-configured device caused the loss of the HA configurations.	DE62954
52.	Health check tables were not supported for the l4 admin and slb admin users.	DE62978
53.	Using WBM, from the Virtual Service Monitoring perspective, the health check failure reason differed from the correct one displayed by the CLI when some of the related virtual services for the given virtual server were blocked.	DE63055
54.	A non-supported configuration caused a crash.	DE63074
55.	There was an Inconsistency in the current throughput per second statistics units of virtual servers.	DE63120
56.	In an HA environment, a config sync operation with a tunnel configuration led to disruption in traffic on the peer device due to a shift in the internal tunnel indices.	DE63195
57.	The /maint/geo/info command displayed an error message when the ISP GeoDB was not yet loaded onto Alteon.	DE63206
58.	In Ansible, it was not possible to remove one VLAN from all interfaces because the value "0" was not accepted.	DE63213
59.	When multiple VIPs are configured with srcnet, the ptmout value was not being considered.	DE63484
60.	When VIRT6 went down, when deleting the IPv6 SLB virt, Alteon panicked.	DE63545
61.	When the user changed the dbind settings to disabled along with the SSL configuration, the dbind configuration was set to forceproxy even though it was set to disabled.	DE63561

Item	Description	Bug ID
62.	SSL statistics in the CLI and WBM did not match on Alteon running version 32.4.5.0.	DE63573
63.	Fetching the routing table via REST API when the routing table was full caused a panic.	DE63590
64.	When a real server had an rport set to 0 and an rport ser to x, the service became unavailable.	DE63624
65.	After SSL Offloading was enabled, Alteon stopped accepting connections.	DE63632
66.	LACP failed due to TX latency on the network driver.	DE63648
67.	When a vADC management gateway was configured with an IP address other than the ADC-VX management gateway, Alteon caused an ADC-VX management connectivity issue.	DE63694
68.	After changing the admin password and Applying, there were configuration sync issues with the peer.	DE63761
69.	Using CLI, after running the /stats/slb/virt command, backup real servers did not display.	DE63805
70.	After changing a group on an FQDN server, the servers were bound to the older group as well as the new group.	DE63835
71.	After a signal panic, Alteon stopped booting.	DE63893
72.	When HA mode was set to VRRP, VRs with some specific VRIDs were active on the backup vADC because some of the VRID bits were incorrectly used in the HAID calculation, causing the advertisements to be dropped due to a bad HAID.	DE63910 DE64075
73.	On a 9800 platform with QAT, SPTHREADS caused a panic.	DE63923
74.	In some edge cases, AppWall did not come up because of an invalid variable that was not initialized. The fix was to initialize the variable.	DE63980
75.	On the 4208 platform, the option to convert to virtual mode (ADC-VX) was mistakenly available.	DE64100
76.	After Alteon received a packet and tried to open a session entry, an incorrect initialization of a pointer resulted in a NULL access and Alteon panicked.	DE64190
77.	Alteon VA did not initiate a BGP connection to a peer.	DE64238

AppWall Bug Fixes

Item	Description	Bug ID
1.	High volume of Forensics security events can cause CPU spikes on backup devices	DE63625
2.	Wrong management IP used to send security events to APSolute Vision	DE62702
3.	When AppWall (7.6.9.50) is configured in Transparent Proxy mode, the IP configured in the tunnel parameter as “forwarding IP” replaced the real client IP	DE62493
4.	Failure in AppWall under rare condition, when decoding Base64 traffic	DE62625
5.	Failures occurred to update AppWall Security updates	DE61559
6.	Under certain conditions, the AppWall management console can disclose local file	DE61634
7.	Under rare and extreme conditions, AppWall ignore the server response	DE61267

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/1027843

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*

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