AlteonOS

RELEASE NOTES

Version 32.6.10.0
September 30, 2022

TABLE OF CONTENTS

CONTENT

Radware announces the release of AlteonOS version 32.6.10.0. These release notes describe new and changed features introduced in this version on top of version 32.6.9.0.

RELEASE SUMMARY

Release Date: September 30, 2022

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:

- 4208, 4208S
- 5224, 5224XL
- 5208, 5208 XL/Extreme, 5208S
- 5424S, 5424SL, 5820S, 5820SL
- 6024, 6024 XL/Extreme, 6024S, 6024SL, 6024 FIPS II
- 6420, 6420 XL/Extreme, 6420S, 6420SL
- 6420p, 6420p XL/Extreme
- 7612S, 7612SL
- 7220S, 7220SL
- 8420, 8420 XL/Extreme, 8420S, 8420SL
- 8820, 8820 XL/Extreme, 8820S, 8820SL
- 9800, 9800S, 9800SL
- 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 32.6.10.0 is supported by APSolute Vision version 4.30 and later.

Integrated AppWall version: 7.6.17.0

OpenSSL version:

- FIPS II model: 1.0.2u
- S/SL models, standard models and VA: 1.1.1p

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 32.6.10.0:

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 32.6.10.0 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	

General Considerations

- Hypervisors (ADC-VX) running a certain version only support vADCs that run the same version or later.

Important!

- For Alteon 5424, 5820, 7612, 7220, and 9800, vADCs running this version require ADC-VX running at minimum version 32.6.0.0.
- For Alteon 5208, vADCs running this version require ADC-VX running at minimum version 32.6.3.0.
- For Alteon 6024, vADCs running this version require ADC-VX running at minimum version 32.6.2.0.

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 32.6.10.0

OCSP Health Check

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

The OCSP health check allows monitoring OCSP servers that are load-balanced by Alteon by requesting to validate a user-provided server certificate. The validation request must also include the issuer of the tested certificate (a TrustCA certificate).

The user can decide whether the health check is successful if the OCSP response status is successful irrespective of the certificate status or if the returned certificate status must be "Good".

The health check supports sending the OCSP request over HTTP or HTTPS, using the POST method.

WHAT'S NEW IN 32.6.9.0

Session Reuse for SSL Health Checks

When performing HTTPS health checks on a server, if the SSL session ID is enabled on the servers, Alteon activates SSL session reuse, lowers the MP CPU utilization, and allows for a larger number of health checks to be performed.

Integrated AppWall

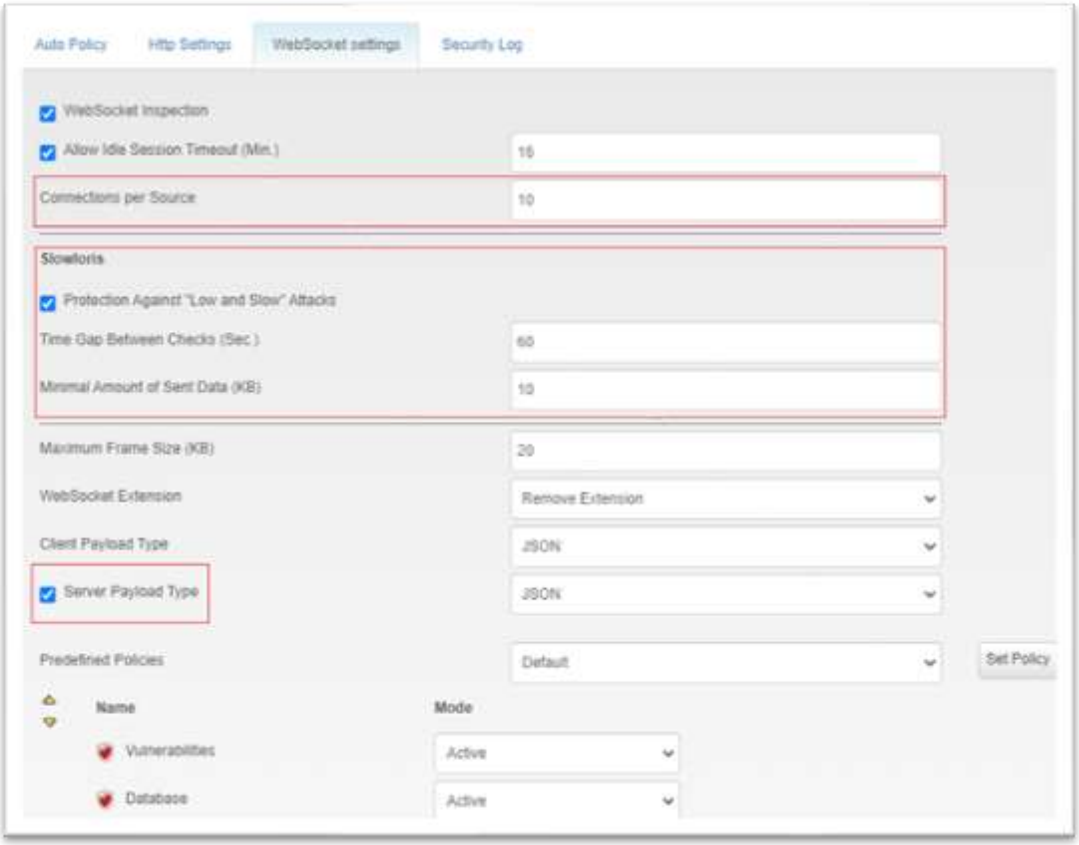
WebSocket

In the previous version support of the WebSocket protocol was introduced. In this version, the following WebSocket support was added:

- **Connection per source** - where the maximum number of connections that a source can open to a specific WebSocket application is defined.
- **Low & Slow attack mitigation** where we configure the following:
  - Time Gap Between Checks - The time span during which the AppWall is counting the traffic rate on the inspected connection.
  - Minimal traffic volume threshold to trigger protection.

Two minor changes were also introduced:

- The enforcement of the WebSocket server response payload type can be optional.
- When the WebSocket is in "block" mode in the Tunnel configuration, the client connection is closed with a Security Page and not with a TCP reset.



☑ WebSocket Inspection

☑ Allow Idle Session Timeout (Min.) 15

Connections per Source 10

Slowloris

☑ Protection Against "Low and Slow" Attacks

Time Gap Between Checks (Sec.) 60

Minimal Amount of Sent Data (KB) 10

Maximum Frame Size (KB) 20

WebSocket Extension: Remove Extension

Client Payload Type: JSON

☑ Server Payload Type: JSON

Predefined Policies: Default

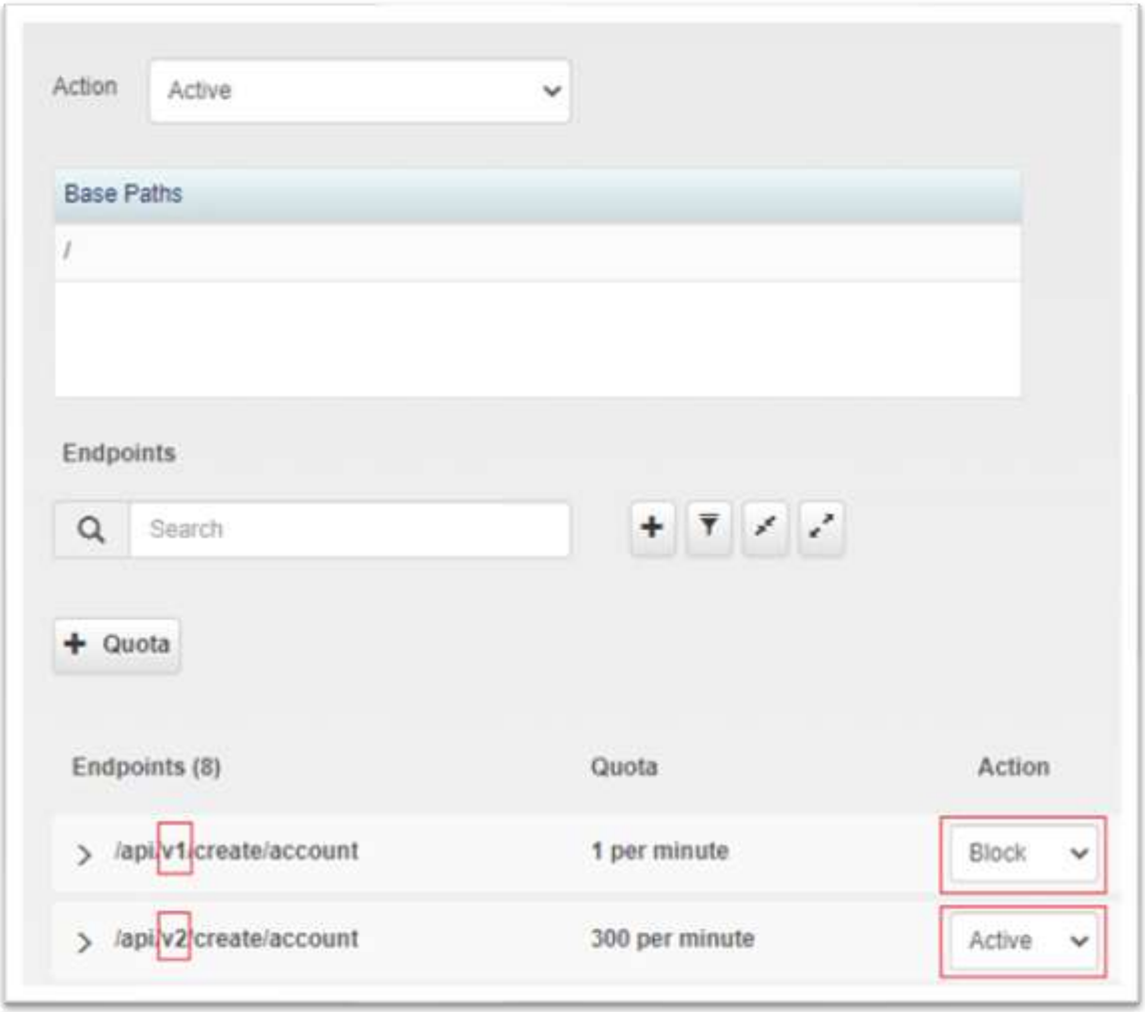
Name	Mode
Vulnerabilities	Active
Database	Active

API Security

In the API Security module, a new "Block" action for the endpoint’s schema enforcement is added.

Previously, “Active”, “Passive” and “Bypass” actions were supported. The new "Block" action will immediately block the client request. It manages use cases such as:

- When an endpoint is deprecated (for example, because of a bug) and the customer does not want any request to reach the API service, the deprecated endpoint can be in Block mode where the new endpoint can be in Active mode
- When an endpoint presents some security risks (for example, data leakage, 0-days attacks, injections) and the customer wants to immediately block any incoming request to this endpoint until it is fixed.



Action: Active

Base Paths
/

Endpoints

Endpoints (8)	Quota	Action
/api/v1/create/account	1 per minute	Block
/api/v2/create/account	300 per minute	Active

Advanced Base64 Attack in HTTP Headers

Following previous deliveries related to Base64 Heuristic Detection and Multiple Encoded attacks, in this version, we added support for multiple-encoded attacks in the HTTP header, such as harmful Injections, with the AppWall Database filter.

WHAT’S NEW IN 32.6.8.0

GEL Entitlement Migration Workflow

The GEL Migration workflow allows migration of GEL Alteon instances from one entitlement to another entitlement, which is placed on the same LLS or on a different LLS.
Multiple GEL instances can be selected for this migration, and a migration summary report will be displayed at the end of the process.

The workflow can be downloaded from GitHub at: https://github.com/Radware/Migrating-Alteon-GEL-Entitlements

Upload the workflow to APSolute Vision (**Automation > Workflow**) or to vDirect (**Inventory > Workflow** *template*).

PMTU Discovery Support

When operating in Proxy mode (Delayed Bind Force Proxy), Alteon separately manages connections to the clients and connections to the servers, and as a result can support PMTU discovery:

- On the client side, if Alteon receives from the client a packet longer than the MTU, Alteon sends an ICMP error back to the client.
- On the server side, if Alteon receives an ICMP error, it adjusts the MTU accordingly to be correct, and resends the data with the new MTU.

When operating in Layer 4 mode (Delayed Bind Disabled), Alteon does not perform connection termination, so the PMTU is negotiated between the origin client and server. If the server responds with an ICMP error, Alteon forwards it to client like any other response from the server.

NFR ID: 210814-000040

Integrated AppWall

WebSocket

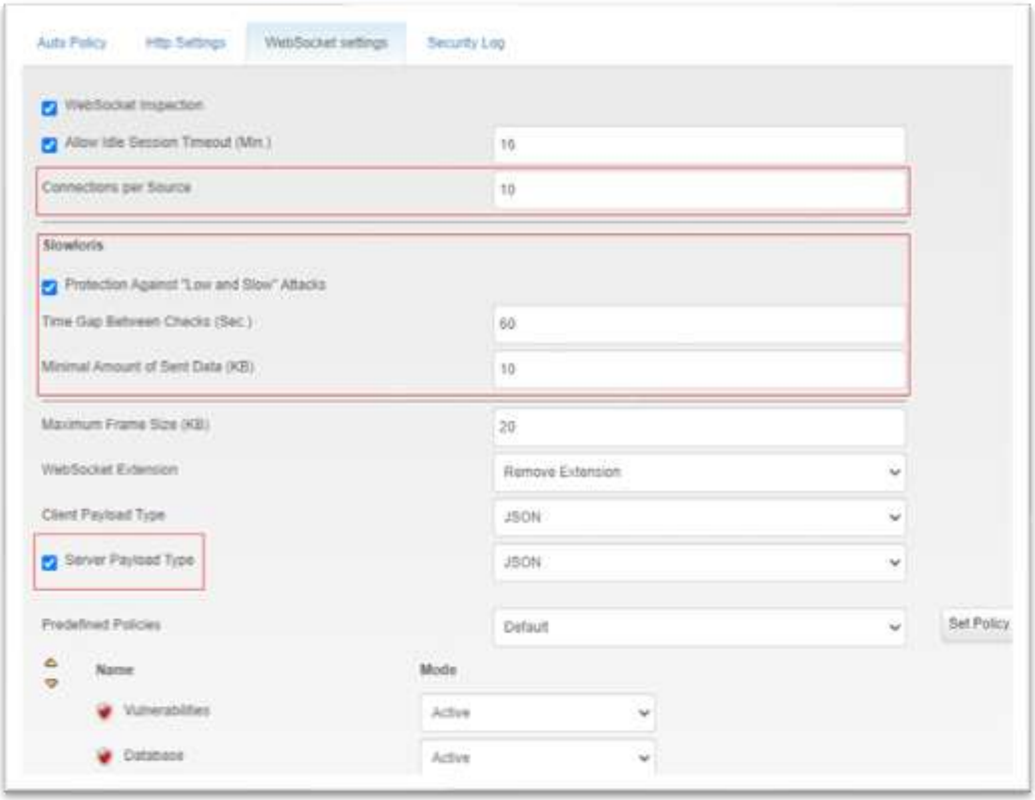
In the previous version support of the WebSocket protocol was introduced. In this version, the following WebSocket support was added:

- **Connection per source** - where the maximum number of connections that a source can open to a specific WebSocket application is defined.
- **Low & Slow attack mitigation** where we configure the following:
  - Time Gap Between Checks - The time span during which the AppWall is counting the traffic rate on the inspected connection.
  - Minimal traffic volume threshold to trigger protection.

Two minor changes were also introduced:

- The enforcement of the WebSocket server response payload type can be optional.

- When the WebSocket is in “block” mode in the Tunnel configuration, the client connection is closed with a Security Page and not with a TCP reset.



☑ WebSocket Inspection

☑ Allow Idle Session Timeout (Min.): 16

Connections per Source: 10

Slowloris

☑ Protection Against "Low and Slow" Attacks

Time Gap Between Checks (Sec.): 60

Minimal Amount of Sent Data (KB): 10

Maximum Frame Size (KB): 20

WebSocket Extension: Remove Extension

Client Payload Type: JSON

☑ Server Payload Type: JSON

Predefined Policies: Default

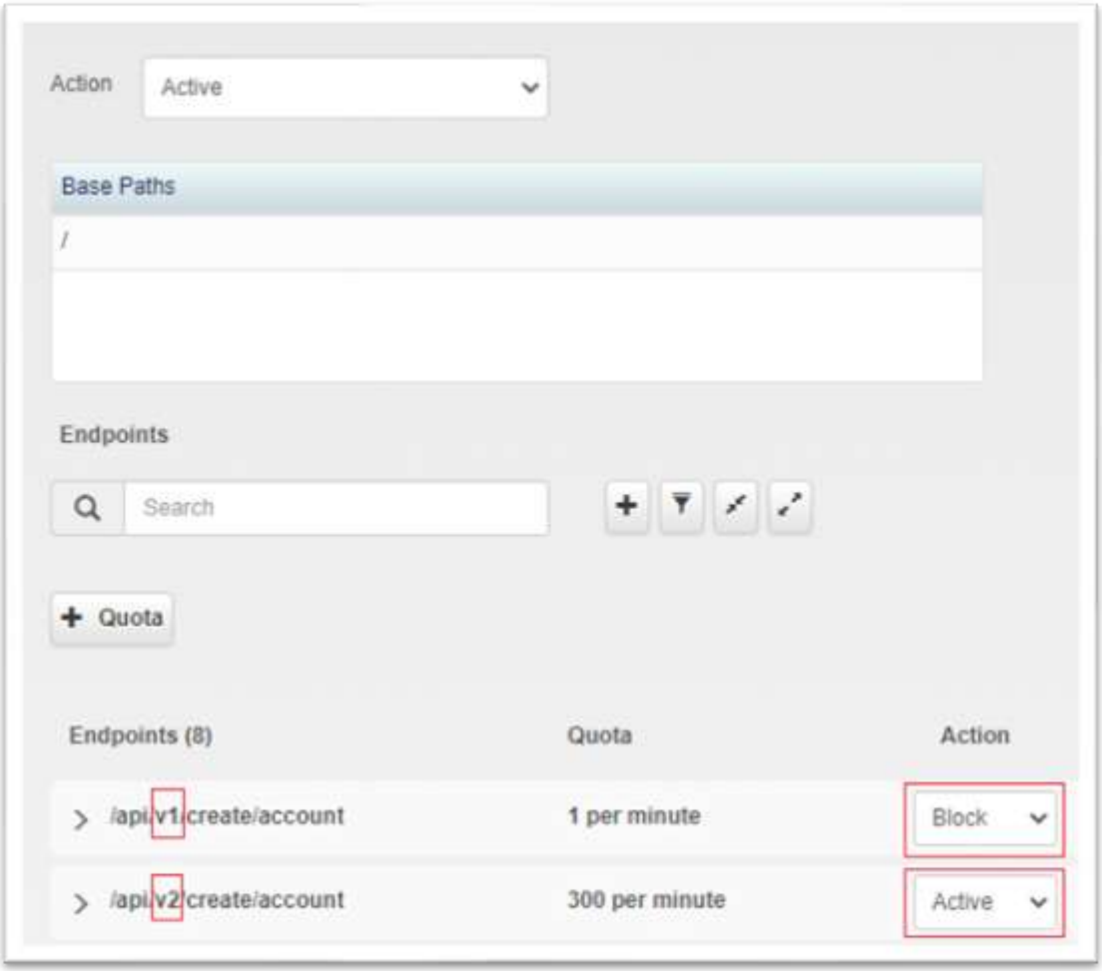
Name	Mode
Vulnerabilities	Active
Database	Active

API Security

In the API Security module, a new "Block" action for the endpoint’s schema enforcement is added.

Previously, “Active”, “Passive” and “Bypass” actions were supported. The new "Block" action will immediately block the client request. It manages use cases such as:

- When an endpoint is deprecated (for example, because of a bug) and the customer does not want any request to reach the API service, the deprecated endpoint can be in Block mode where the new endpoint can be in Active mode
- When an endpoint presents some security risks (for example, data leakage, 0-days attacks, injections) and the customer wants to immediately block any incoming request to this endpoint until it is fixed.



Action: Active

Base Paths
/

Endpoints

Endpoints (8)	Quota	Action
/api/v1/create/account	1 per minute	Block
/api/v2/create/account	300 per minute	Active

Advanced Base64 Attack in HTTP Headers

Following previous deliveries related to Base64 Heuristic Detection and Multiple Encoded attacks, in this version, we added support for multiple-encoded attacks in the HTTP header, such as harmful Injections, with the AppWall Database filter.

WHAT'S NEW IN 32.6.7.0

DNSSEC Support for SOA Record (GSLB)

Alteon can now provide SOA records secured with DNSSEC, if the DNS query requires it (in previous versions the DO flag was ignored for SOA queries).

NFR ID: 210805-000092

SameSite Cookie Attribute

The SameSite attribute of the Set-Cookie HTTP response header lets you declare if your cookie should be restricted to a first-party or same-site context.

The default cookie-sending behavior if the SameSite attribute is not specified in the cookie was recently changed to be as for SameSite Lax. In previous versions, the default was that cookies were sent for all requests (None). Most new browser versions support this new behavior while some browsers still behave according to the old default.

For that reason it is important to allow specifically setting the SameSite attribute with the requested value.

Alteon now allows the following:

- To specify the SameSite attribute value for the cookie inserted by Alteon for persistency purposes both via CLI and WBM and via AppShape++ (using the `persist cookie` command).
- To retrieve the SameSite attribute from a cookie or change its value via the following AppShape++command: `HTTP::cookie samesite`
- To specify the SameSite attribute when inserting a cookie via the following command: `HTTP::cookie insert`
- To change the SameSite attribute value for a cookie via the following command: `HTTP::cookie set`

FIPS Card Support for 7612

- The Nitrox III FIPS SSL card is now supported for the Alteon 7612 platform.
- To order Alteon 7612 FIPS, order the D-7216S platform required and the separate FIPS II card part number (factory installed).

PPS Statistics per Service and per SP

PPS statistics is now available for the following:

- Per virtual server with virtual service, group, real server, and content rule granularity
- Per filter, with group and real server granularity.
- Per device, displaying accumulative PPS of virtual servers and filters traffic.

These statistics are available via the CLI, WBM, and SNMP.

The PPS statistics per device and per service are also available as part of the system and virtual service Basic Analytics JSON

NFR ID: 200706-000123

Integrated AppWall

WebSocket

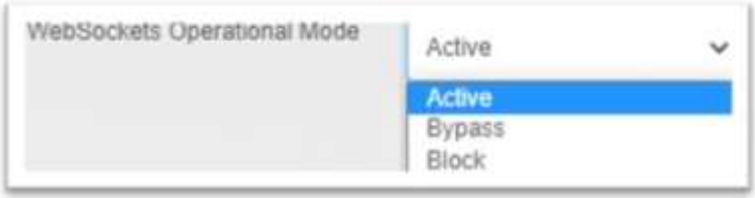
In this version, WebSocket protocol support is added.

WebSocket is a communications protocol, providing bi-directional communication channels and enables streams of messages over a TCP connection. WebSockets are becoming increasingly popular, because they greatly simplify the communication between a client and a server.

The WebSocket protocol enables interaction between a client application and a web server with lower overhead, facilitating real-time data transfer from and to the server. This is made possible by providing a standardized way for the server to send content to the client without being first requested by the client and allowing messages to be passed back and forth while keeping the connection open. In this way, a two-way ongoing conversation can take place between the client and the server. To achieve compatibility, the WebSocket handshake uses the HTTP Upgrade Header to change from the HTTP protocol to the WebSocket protocol.

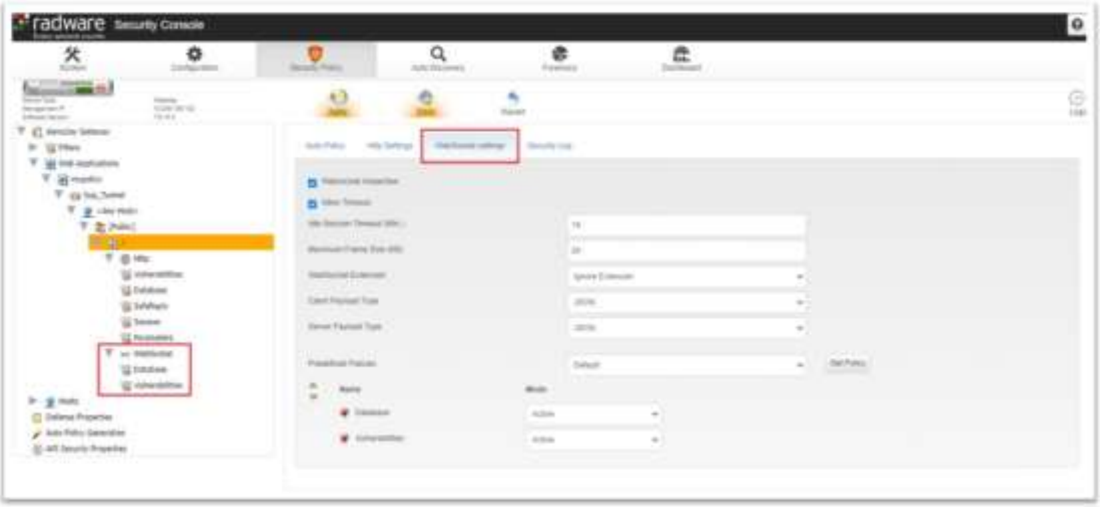
AppWall WebSocket support:

- At the tunnel level, you can define the WebSocket operation mode: Bypass, Block or Active (inspect the WebSocket traffic).



WebSockets Operational Mode: Active

- Define a security policy per WebSocket application
- Define a specific WebSocket idle session timeout
- Set a maximum WebSocket frame size
- Define how AppWall behaves related to the WebSocket extensions:
  - Remove the extensions
  - Block traffic containing extensions
  - Ignore the extensions
- Define the Client-to-Server payload type (Binary, JSON, XML or Unstructured)
- Define the Server-to-Client payload type (Binary, JSON, XML or Unstructured)
- Support of Database Security and Vulnerabilities filters



Base64 Heuristic Detection

The way to detect a Base64 payload is not so obvious. If Base64 detection is not process correctly, it may be a source of false negatives or false positives (for example, payload with and without padding.).

Therefore, in this version we introduce a heuristic detection of Base64 payloads that increases accuracy in the attack detection.

In order to optimize performance, the configuration is opened to inspect the pre-decode values in addition to the post-decode values.

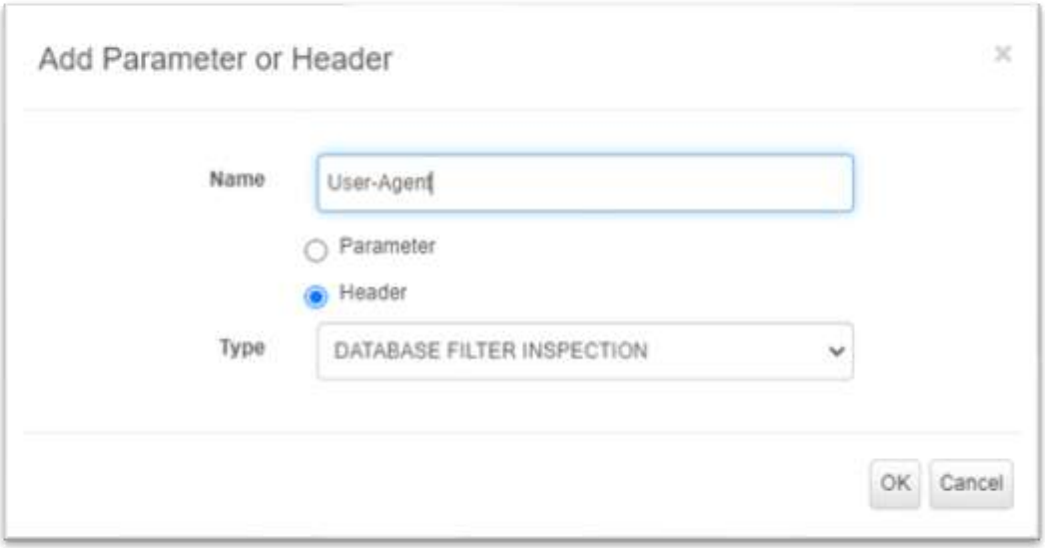
Multiple Encoded Attacks

In the previous release, we introduced support for multiple-encoded attacks for any parameter. In this version, we added the support for multiple-encoded attacks in the HTTP headers with the Vulnerabilities filter.

HTTP Header Inspection with the Database Filter

AppWall provides support for attacks in the HTTP headers, such as Injection and Cross-Site Scripting. You can configure AppWall to inspect HTTP headers with the Database filter.

You can also configure the way HTTP headers are to be inspected. The refinements can be done per-Virtual Directory from the Database filter configuration screen or the Quick-Click refinements from the Forensics view.



Add Parameter or Header

Name: User-Agent

○ Parameter

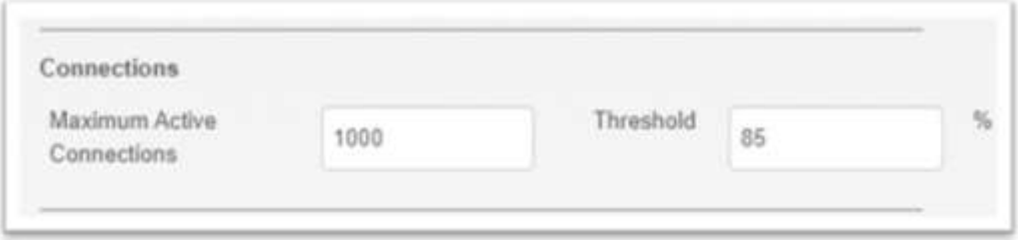
● Header

Type: DATABASE FILTER INSPECTION

Maximum Active Connection Alert

AppWall can limit the number of connections for every AppWall tunnel (referred to as SECWA in the Alteon WAF). When AppWall receives the maximum limit of active connection in a tunnel, no new connections are opened.

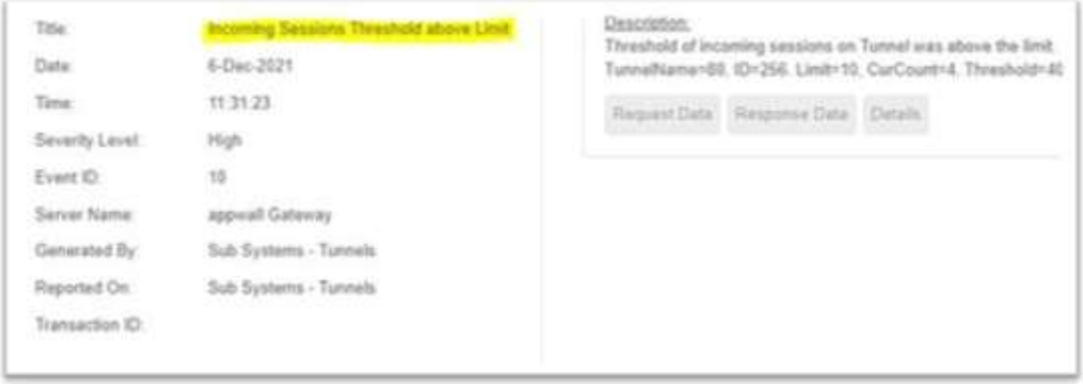
In this version, we added the option to configure a threshold (in percentage) of active connections. When the threshold is reached, an alert is sent in the Forensics Security events before the maximum number of allowed active connections is reached and the connections queue gets completely full.



Connections

Maximum Active Connections: 1000

Threshold: 85 %

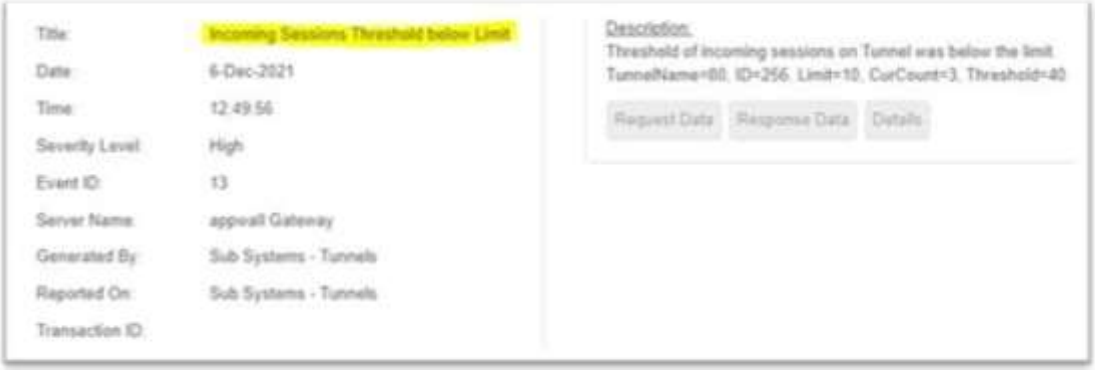


Title:	Incoming Sessions Threshold above Limit
Date:	6-Dec-2021
Time:	11:31:23
Severity Level:	High
Event ID:	10
Server Name:	appwall Gateway
Generated By:	Sub Systems - Tunnels
Reported On:	Sub Systems - Tunnels
Transaction ID:	

Description:
Threshold of incoming sessions on Tunnel was above the limit.
TunnelName=80, ID=256, Limit=10, CurCount=4, Threshold=40

The events are reported in 1-minute intervals. If current active connections exceed the threshold, AppWall will report this event every minute.

When the number of active connections in the tunnel decreases below the threshold a system log event is reported:



Title:	Incoming Sessions Threshold below Limit
Date:	6-Dec-2021
Time:	12:49:56
Severity Level:	High
Event ID:	13
Server Name:	appwall Gateway
Generated By:	Sub Systems - Tunnels
Reported On:	Sub Systems - Tunnels
Transaction ID:	

Description:
Threshold of incoming sessions on Tunnel was below the limit
TunnelName=80, ID=256, Limit=10, CurCount=3, Threshold=40

Note: To configure an alert for this event with external logging, refer to the Knowledge base article ; BP3182.

WHAT'S NEW IN 32.6.6.0

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

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

Visibility

Alteon PPS Statistics per Device

PPS statistics are now available per device (`/stat/slb/dvcstats`).

Note: PPS per device statistics currently only includes virtual service traffic. (In future versions, this counter is scheduled to also include the filter 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 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

Integrated AppWall

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.

WHAT’S NEW IN 32.6.5.0

LinkProof Dashboard in APSolute Vision ADC Analytics

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.

The metrics are available over JSON using **Error! Hyperlink reference not valid.**.

NFR: 200424-000128

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.

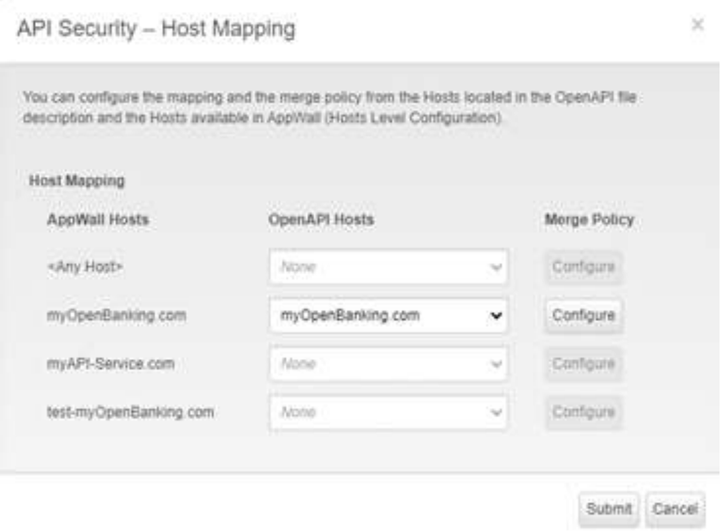
Important: The default management cipher is now set to “main” and supports the following suites:

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

NFR ID: 200724-000003

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)

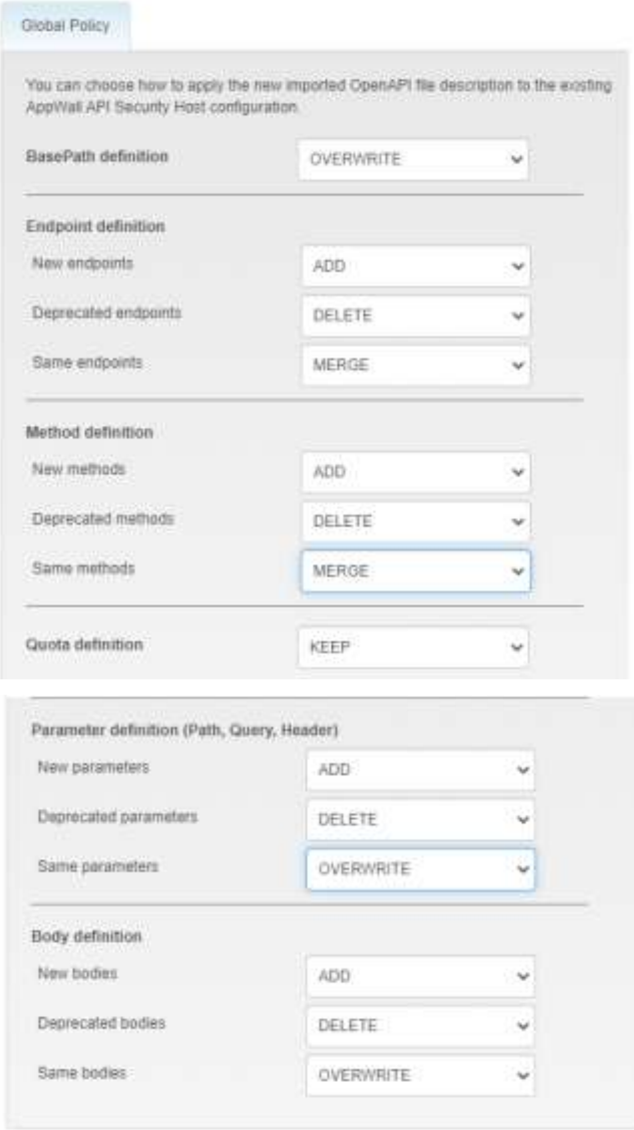
Host Mapping

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.



Global Policy

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 32.6.4.0

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

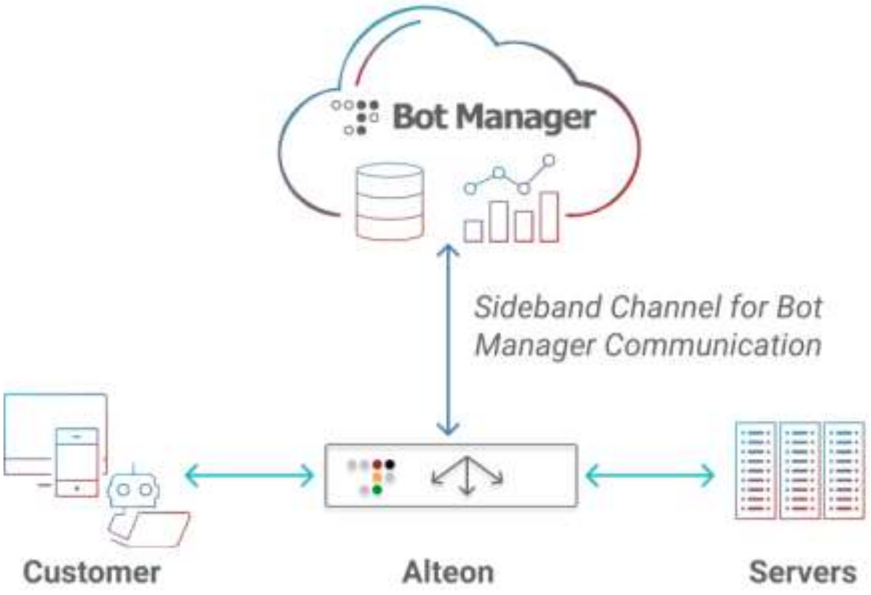
WHAT’S NEW IN 32.6.3.0

This section describes the new features and components introduced in this version on top of Alteon version 32.6.2.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.6.3.0.

BOT Manager Integration

Starting with this version, Radware’s Bot Manager protection can be set per virtual service. Bot Manager protection provides comprehensive protection of Web applications and mobile apps from automated threats such as bots. Bot Manager provides precise bot management across all channels by combining behavioral modeling for granular intent analysis, collective bot intelligence and fingerprinting of browsers, devices and machines. It protects against all forms of account takeover (such as credential stuffing and brute force), denial of inventory, DDoS, and payment fraud, and Web scraping to help organizations safeguard and grow their online operations.



When a client request reaches an application in Alteon which is protected by Bot Manager, Alteon extracts information from the request headers and sends this information via a *sideband* connection to the Bot Manager endpoint. Alteon then acts according to the Bot Manager response, either Allowing the request, Blocking it, or challenging the user with a captcha test.

Alteon Bot Manager protection is available in either Active or Report-only mode. Detailed Bot Manager analytics is available at the Bot Manager portal (a direct link is available from the Alteon WBM).

For the integrated Bot Manager to function, you must have at minimum the Perform package, and you must have a Standalone Bot Manager license.

Integrated AppWall

Monitor Mode for SSL Traffic

Starting with this version, Monitor mode in Integrated AppWall supports SSL traffic (RSA keys only).

WAF SUS Update over HTTPS

Starting with this version, Integrated AppWall allows updating WAF SUS over HTTPS.

DPDK Support for 5208

Starting with this version, the Alteon 5208 platform uses the DPDK infrastructure. This allows for integration of more advanced capabilities. For example, it allows using Alteon 5208 with an external HSM.

Important! Upgrade to this version of a 5208 platform working in ADC-VX mode requires that both the ADC-VX and all its vADCs are upgraded to this same version, as DPDK and non-DPDK-based versions cannot be mixed on the same device.

New Platform Flavor – Alteon D 5208 Bypass

Alteon D 5208 has a new hardware bypass for the copper ports.

The platform can be configured to bypass traffic upon power failure, ensuring outbound traffic continues to flow.

The switch inside the platform includes a mechanical bypass and is different than the switch on a regular 5208 platform. As a result, the regular Alteon D 5208 cannot be upgraded to an Alteon D 5208 bypass.

New PNs for the Alteon D 5208 bypass have already been added to the latest price list.

Note: The color of the new platform flavor is black.

DNS Nameserver (NS) Records Support

For security reasons, some DNS cache servers require authoritative nameservers to answer NS queries for the domains for which it is authoritative.

Alteon now answers such queries for the domains for which it is authoritative if the nameservers were configured for that domain. In addition, if the nameserver hostname is in the same domain as the hostname for which the NS query arrived, and the user specified an IPv4 and/or IPv6 address for the nameservers, the answer will also include A and/or AAAA records for each nameserver in the ADDITIONAL section (glue records).

The following configuration is required for the GSLB/LinkProof participating Alteons:

- **Define Nameserver Group/s** – A list of hostnames that serve as nameservers for the same hostnames. For each nameserver, you can also define IPv4 and IPv6 addresses.
- When configuring a hostname, either via a virtual service or a DNS Rule, attach the relevant nameserver group.

NFR ID: 200327-000083

LinkProof Basic Analytics Metrics

Alteon LinkProof counter-based (metrics) reporting allows for the collection of WAN Link statistics in JSON format. The JSON is retrieved from Alteon using HTTPS requests. The information includes:

- WAN Link ID status
- Current upload: throughput, throughput Utilization, throughput limit
- Current download: throughput, throughput Utilization, throughput limit
- Total upload and download throughput
- Current connections per sec
- Current concurrent connection

This data can also be used for integration with third-party SIEMs such as Splunk or ELK.

Notes: LinkProof counter-based (metrics) reporting is supported by the Perform package and above.

NFR ID: 200605-000087

BGP Enhancements

The following new capabilities are provided using a new BGP routing module - FRR. This module is currently supported only in Standalone and Alteon VA form factors and should currently only be used when one of the following enhancements is required (full FRR support scheduled for next major release).

To activate FRR module set BGP mode to FRR (default is Legacy).

BGP Graceful Restart (RFC 4724)

BGP Graceful Restart enables retention of the routing table when routers are restarting.

This capability is available in FRR mode and is currently available in Standalone and Alteon VA form factors.

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

NFR ID: 190911-000276

BGP Community Support

BGP communities provide policy-driven decision-making for incoming and outcoming routes.

NFR ID: 190911-000426

Secure Password Policy

Starting with this version, the administrator can enforce password strengths criteria for the passwords of local users (both predefined and user-defined).

When password strength is configured, it is applied to passwords of newly created users as well as password changes for existing users.

The password strength criteria are not applied to the default predefined Admin user.

NFR ID: 200227-000015

WHAT'S NEW IN 32.6.2.0

This section describes the new features and components introduced in this version on top of Alteon version 32.6.1.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.6.2.0.

Integrated AppWall – Monitor Mode

In *Monitor* mode, AppWall receives a copy of traffic (mirroring) and performs detection and reporting only, without adding any latency or failure point to the inline traffic, but also with no attack mitigation.

Alteon with integrated AppWall in Monitor mode must be installed out-of-path. Alteon itself acts as a transparent conduit to the WAF module.

To support this mode, the new Monitor option was added to the filter **Action** parameter.

Currently, Monitor mode does not handle encrypted traffic. Traffic should be received in clear text (decrypted). Encrypted traffic support (RSA keys) is planned as a second phase.

Integrated AppWall – API Security

The usage of APIs in Web applications and services is on the rise, and security concerns and needs are not entirely covered by traditional protections in WAF. AppWall's API security module provides protections that cover security concerns and the need for working with APIs.

API Security can be automatically configured by importing an OpenAPI document to AppWall. AppWall automatically updates the API security module for hosts configured under the Host Level Configuration that match the ones defined in the OpenAPI document. All API endpoints will be added to the endpoint list of the host, allowing API requests to these endpoints automatically. API requests to the allowed endpoints are still scanned by AppWall's security protections for embedded attacks.

GEL Certificate Loading

Starting with this version, users can load the certificates to be used for communication between Alteon and the license server (LLS or CLS).

Using this certificate, and with the appropriate configuration, LLS communication between Alteon and the LLS cannot also be available over HTTPS.

GEL WBM

The GEL configuration and license activation was added to the WBM (to the *License* pane).

An indication that Alteon is running within the grace period was added to the Alteon landing page, alerting you that the license will permanently expire in *nn* days (Alteon enters a 30-day grace period as the result of license expiration or communication problems with the license server).

Alteon VA Enhancements

Single IP Mode with Management/Data Port Separation

The ability to support one data port with a single IP address for all data communication (interface IP address, VIPs, and PIPs) and a separate management port has now been extended to all hypervisors (KVM, VMware, Hyper-V, and OpenXEN) in both DPDK as well as TUN/TAP ***mode***. **It is** also **supported** in **private** Cloud **environments as well** as **in Public cloud** environments **(AWS and Azure).**

Cloud Init Support in Common Cloud Deployments

Starting with this version, a preconfigured Alteon VA using Cloud-Init can be deployed in the following common Cloud environments (beyond the existing support of Cloud-Init in OpenStack):

- VMware using VMware vApp (similar to Cloud-Init)
- AWS
- Azure

For further details, refer to the Cloud-Init Appendix of the *Alteon VA Installation and Maintenance Guide*.

Alteon VA Time-based Throughput License

A time limit option was added to the Alteon VA throughput license, letting you use Alteon VA in PoCs for more than the default 30 days demo license. When the throughput license expires, the throughput license is reduced to 1 Mbps.

Alteon VA – VMware ESXi 7.0 Support

Starting with this version, Alteon VA supports the recently released VMware ESXI version 7.0 on top of the earlier version.

Cloud-Init Residuals

The Cloud-Init capabilities were expanded to now include the following:

- **GEL Support** – Supporting both GEL configuration and GEL license activation. With this capability you can now automate the entire Alteon deployment cycle and can have a running licensed and configured Alteon as part of the Alteon deployment using vDirect. For further details, refer to the Cloud-Init appendix in the *Alteon VA Installation and Maintenance Guide*.
- **Miscellaneous** – Through Cloud-Init you can configure the following:
  - Also disable DPDK (and run in TUN/TAP) when Alteon VA has more than 3 GB RAM
  - Configure the resources for FastView

DPDK Support for 6024

Starting with this version, the Alteon 6024 platform uses the DPDK infrastructure. This allows for integration of more advanced capabilities. For example, it allows using Alteon 6024 with an external HSM.

Important! Upgrade to this version of a 6024 platform working in ADC-VX mode requires that both the ADC-VX and all its vADCs are upgraded to this version, as DPDK and non-DPDK-based versions cannot be mixed on the same device.

New Ansible Modules

Since the last release, the following modules were added to the Ansible playbook:

- **Alteon_config_ha_service** – Configures the high availability service mode parameters
- **Alteon_config_slb_pip6** – Configures the PIP IPV6 parameters

Traffic Events via Management Port

Starting with this version, you can select whether the traffic event logs are sent via the data path or the management path. This configuration is done at the Remote Logging object.

Note: Sending traffic event via the management port is only available over the TCP/TLS protocol.

With this new capability, you can manage Alteon via the management network as required in most large enterprises where the management network is separated from the data network for security reasons.

Traffic Events in JSON Format

Alteon now supports traffic event logs in JSON format (in addition to the current CEF format).

This allows for easier integration with an external SIEM that does not support the CEF format. The JSON format for traffic events is supported only for *unified events* and *security events*, and only over the TCP/TLS syslog protocol.

Note: All the keys and values remain the same in both CEF and JSON formats.

Integrated AppWall Enhancements

Suppressing Repeated Events

AppWall suppresses repeated events during a defined period. At the end of this period, there will be one new event representing all the suppressed events.

Event suppression can be configured separately for each event in the *Event Map* tab for the specific log type.

New Parsing Property - Allow Parameter Name Before the JSON Block

AppWall's RFC validation engine can now ignore non-JSON characters in the body before a valid JSON object, if enabled. By default, this property is disabled.

ISP-based Geolocation

Alteon now supports determining to which ISP the source or destination IP address belongs. This enables performing action, group, or data center selection based on ISP.

Important! The following requirements must be fulfilled before starting to work with ISP-based decisions:

- Alteon must have at minimum a Perform package plus Perform subscription to allow geolocation-based decisions.
- The MaxMind GeoIP2 ISP database must be uploaded on Alteon. The ISP database is only available for purchase directly from MaxMind by the customer and is not available from Radware for either manual or automatic upgrade. Once the database is purchased, the two files obtained from MaxMind must be aggregated in a zip file and uploaded to Alteon using the manual Geo DB Update pane/CLI command.

Once the prerequisites are fulfilled, in order to make ISP-based decisions, do the following:

1. Set the **Network Class** as type **Region**, and select **Network Type ISP** (in CLI, run the command `cfg/slb/nwclss <X>/network <y>/type`).
2. Enter the ISP name. Using and asterisk (*), you can set the name to match all ISPs beginning with a certain string **‘string***). All ISPs that contain a certain string (***string***), all ISPs that end with a certain string (***string**) or an ISP matching exactly a string (**string**).

3. Use this Network Class in virtual servers, filters, or GSLB Client Network rules to make decisions based on ISP.

NFR ID: 191111-000119

GSLB Client Networks Enhancements

Multiple Network Classes per Client Network

A Client Network rule lets you specify the GSLB decision to be made for a specific client subnet or network class. Now you can attach to each Client Network rule multiple network classes for increased flexibility.

Note: New CLI commands were added for supporting multiple network classes per client network rule (`addnwcls`, `rmnwcls`). If the client network is defined using both `adnwcls` and the legacy `sip` command, the `sip` command is ignored.

NFR ID: 190911-000568

Description Field for Client Network

A description field was added to Client Network rules, for ease of management (the rule ID is numeric).

NFR ID: 190911-000342

SHA2 and AES-256 Support for SNMPv3

Starting with this version, the following SNMPv3 support was added for stronger security

- **authentication type** – Support for SHA256
- **privacy type –** Support for AES256

NFR ID: prod00268561

TCP SACK Control on Management Port

Enabling the TCP SACK improves the performance on management ports. However, this can expose the device to the following vulnerabilities:

- CVE-2019-11477
- CVE-2019-11478

For additional information about these vulnerabilities. please access the Radware Knowledge Base.

TCP SACK can be enabled/disabled via CLI using the following command (enabled by default):

```
/maint/debug/tcpsack <ena/dis>
```

This requires a reboot

This feature is relevant on following Alteon platforms: 5208, 5224, 6420, 8420.

This feature is also available for versions 31.0.14.0, 32.2.6.0, 32.4.4.0.

High Speed Packet Capture

A new capability was added to the packet capture to allow minimal impact on management performance.

To use this high speed packet capture capability, use ‘-sp- flag in the `/maint/pktcap/data/capture` command and select the SP number on which to perform the capture (or leave it empty for all SPs).

Note: The following flags are not supported when using the -sp flag: -l, -e, -n, -x, and -A.

WHAT’S NEW IN 32.6.1.0

This section describes the new features and components introduced in this version on top of Alteon version 32.6.0.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.6.1.0.

Out-of-path WAF Security Events

Starting with this version, WAF Security events per application are also supported in Out-of-Path (OOP) mode. Prior to this version, WAF Security events per application were only supported in inline mode.

These events are sent in CEF format via its event logging module (over TCP/TLS), in the context of the application.

Note: In OOP mode, it is not possible to correlate between the security event and its relevant traffic event. This means that the traffic event in OOP mode will not have security severity due to a WAF attack detected and will not include the WAF transaction ID.

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

25Gbps Support for Alteon 5424/5820 and 9800

Starting with this version, Alteon 5424, 5820 and 9800 support 25GE technology.

Alteon 5424 and 5820 have four (4) ports that support 25GE (ports 1-4).

Note: It is not possible to mix between speeds. The first four ports work with 25GE only or 10GE only. You need to configure each one of the four ports to the required speed.

Alteon 9800 has eight (8) ports that support the following speeds: 100, 40, 25, 10 Gbps.

1Gbps Support for Alteon 7612

Starting with this version, Alteon 7612 supports 1Gbps on the SFP+ ports (ports 7-18).

DHCPv6 Support

Starting with this version, the Alteon DHCP capabilities on the management port were extended and now also support DHCPv6 on top of the existing support of DHCPv4. Alteon receives its management IPv6 address from the DHCP server, while the gateway address is received from the router advertisements (RA). SLAAC addresses are also received through the router advertisements.

The Alteon outgoing packets set the IP address received from the DHCP server as the source address. Radware recommends that when communicating with Alteon, use this address as the destination address and not any of the SLAAC addresses.

GEL DNS Server

Starting with this version, in the GEL configuration there is a separate configuration for a DNS server for GEL purposes. This enables a platform with a GEL license to co-exist with a SecureURL configuration, where each of them requires a different DNS server on different ports (management port versus data ports).

Alteon VA - SingleIP Mode with Management/data Port Separation

Prior to this version, when configured with a single port, Alteon VA had a single IP address for all its entities – interfaces, VIPs, and PIPs. Starting with this version, this capability was also enhanced for an Alteon VA running with two ports.

In this mode, one port is assigned for management and the other port for data. All the entities on the data ports, interfaces, VIPs, and PIPs are set automatically to a single IP address, obtained through a DHCP server.

Currently this option is available on an Alteon VA running in DPDK mode under VMware.

Alteon VA - Azure Government support – HA support

Starting with this version, Alteon VA running on Azure Government supports HA.

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.

Network HSM

Starting with this version, Alteon can provide FIPS-compliant solutions in conjunction with the SafeNet Luna Network HSM 7 appliance from Gemalto/Thales.

Because it is network-based, you can use the SafeNet Luna solution with multiple Alteon form-factors:

- Alteon VA, with at least 3 GB RAM
- Alteon Application Switch platforms 4208, 5424, 5820, 7612, 7220, 9800, in standalone mode.

When operating with network HSM, Alteon offloads the public key cryptography (SSL handshake) to the SafeNet Luna appliance, while the symmetric key cryptography (SSL data encryption/decryption) is performed by Alteon.

Alteon supports working with a pair of redundant SafeNet Luna devices.

Note: Currently, Alteon can only communicate with SafeNet Luna devices over IPv4.

When operation with network HSM is enabled on Alteon (requires reboot), you can still generate keys and certificates on Alteon, import non-HSM keys and certificates, and associate them to virtual services and filters:

- If an HSM-originated certificate is associated to a virtual service or filter, the SSL handshake is performed by the network HSM.
- If a non-HSM certificate is associated to a virtual service or filter, the SSL offload will be performed entirely by Alteon software.

For more details, see the *Alteon Application Guide*.

For pricing information, contact your local Radware Sales representative.

Virtualization on Alteon D-9800, D-5820, D-5424

Starting with this version, Alteon D-9800, D-5820, and D-5424 support ADC-VX mode and its related features.

Alteon D-9800 supports up to 72 instances with the default memory of 192 GB (available elastic core allocation modes: system default and Maximum vADC density).

Alteon D-5820/D-5424 supports up to 10 instances with the default memory of 32 GB (with 32 GB RAM no other elastic core allocation modes are available except of the default mode - 10 vADCs).

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-labelling.

WHAT'S CHANGED IN 32.6.10.0

SSH Library Upgrade to Support SHA2 MAC Algorithm

The Mocana SSH library was upgraded to support the SHA2 MAC algorithm.

It is now possible to disable the hmac-sha1 MAC algorithm using the following command:

```
/cfg/sys/access/sshd/weakmac command
```

NFR ID: 210718-000079

OpenSSL Upgrade

The OpenSSL version was updated, for both the data and management path, to version 1.1.1p.

Integrated AppWall

- Signature Operation Mode:

  A new Operation mode, **Forced Active,** is now available. If the Database Security filter or the Vulnerabilities Security filter are in Passive mode, the RuleID or PatternID configured as **Forced Active** will block the traffic.

  From the AppWall Management Console, in the Database Security filter, the configuration has been consolidated. Two tabs exist today:

  - **Rule Operations** allows the configuration of the Auto Passive Mode, the definition of the Operation Mode for any RuleID, and an aggregated view of the Database Security filter of each Application Path where the Database filter is defined.
  - **Parameter Refinements** allows to exclude RuleIDs per parameters/headers.
- FileUpload Security filter:
  - Support of files with no extension.

- Advanced support of files upload with content the Content-Type multipart/form-data.

WHAT’S CHANGED IN 32.6.9.0

GEL Allocation Granularity

The following Alteon throughput allocation options are now available: 1.5 Gbps, 2.5 Gbps, 4 Gbps, 6 Gbps and 7 Gbps.

Note: This eequires APSolute Vision 5.3 *x*.

NFR ID: 220109-000019

Syslog Server for Integrated WAF

It is now possible to set up to five (5) syslog servers (IP address and Port) for integrated WAF.

- WBM: **Security > Web Security > Reporter > Syslog Servers tab.**
- CLI: `cfg/sec/websec/syslog`

Notes:

- After upgrade from an earlier Alteon version, the syslog servers that were previously configured via the SNMPv3 target address table will be converted to the new integrated WAF syslog server setting.
- Use the Management Traffic Routing feature to determine if the syslog events should be set via the data port or management port.

HTTP/HTTPS Health Check

- Starting with this version, an IPv4 HTTP/HTTPS health check can be set to terminate the connection using FIN in case of timeout (the default remains RST).
- Configuration of this feature is available only via CLI using the `conntout <fin | rst>` command.
- **Note:** Radware recommends closing the connection with RST in case of timeout, for faster response release. Closing with FIN may cause high MP CPU utilization if many real servers are unreachable.
- **NFR ID:** 211020-000175

Number of Alteon DNS Responders

The number of supported DNS Responders has been increased from 5 to 18, starting with this version (18 VIPs for TCP, and 18 VIPs for UDP).

NFR ID: 211102-000089

Ping6 Response

Response to the **ping6** command now includes the same information as the IPv4 **ping** command (TTL, latency, and so on).

For multiple ping6 attempts, the following command can be used:

```
times <#num_of_times> <#delay_between_times> “ping6 <ipv6_address>”
```

For example, to run the ping6 command four (4) times without delay, run the following command:

```
times 4 0 “ping6 4001::3”
```

NFR ID: 211102-000064

QAT Driver/Engine Upgrade

The Intel QAT driver used in Alteon S and SL models has been updated to QAT.L.4.17.0-00002.

OpenSSL Upgrade

The OpenSSL version was updated, for both the data and management path, to version 1.1.1n.

Integrated AppWall

1. **Database Filter:** In the inspection settings, we can configure the filter to do a partial inspection of the parameters (for example, inspect only the first 150 characters).
2. Content**-type HTTP Header** multipart/form-data can be refined if it does not follow RFC (specific implementation with a different delimiter than in the RFC).
3. URL**-encoded encoding**: More support and refinement options were added in the Parsing properties. Per URI, it can be specified which reserved characters are **un**encoded.
4. Cookie **Reply flag:** We can now enforce the cookie flag SameSite (Strict, LAX or None) on behalf of the origin server.

WHAT’S CHANGED IN 32.6.8.0

Empty Group Association to FQDN Server and Virtual Service

A group without servers can now be associated to an FQDN server. With this association, the group name (description) is automatically set on apply (so that the group’s configuration will be different than the factory default).

In addition, you can now assign a group without real servers to other components (virtual service, filter, sideband, and so on) as long as the group description is not empty.

NFR ID: 220111-000026, 210302-000006

HTTP Header Length

The maximum HTTP header length that Alteon can process in proxy mode has now been increased to 128000 bytes.

NFR ID: 211209-000097

Treck Version

The Treck version has been updated to 6.0.1.76.

Remove Vulnerable Expat Library

To eliminate vulnerabilities, the old and unused Expat library was removed. The XML configuration was also removed from the CLI and WBM as it uses the Expat library.

Include "remote address" at the TACACS request

The "remote address" attribute is now available as part of the TACACS request.

NFR ID: 210319-000010

Ignore Non-existing Fields in JSON

REST requests will now ignore non-existing fields and will not fail the transaction. This is required to allow using the same REST API calls for different versions (backward-compatibility support).

Event Counter Default Change

The event counter `(/stat/counter/`) is used for debugging purposes. As this counter has an impact on performance. it is now set to disabled by default.

When requested by TAC, enable event counter using the command `/stat/counter/event ena` before issuing TechData. Radware recommends disabling again when it is completed. Disabling/enabling the event counter is available in vADC, VA, and Standalone.

AppWall Integrated

- **SafeReply Filter:** The settings of the SafeReply filter have been moved. Previously, the settings were global when the SafeReply filter was activated. In this version, the settings can be specifically set per Application Path.
- **API Security:** When merging a new OpenAPI schema in an existing configuration, the merge policy can be defined. In this version, during the merge process, the value for the Quota is set, by default, to “Keep”.

- **Tunnel Parsing Properties:** In the “Request Boundaries" section, AppWall can accept HTTP GET requests with a Body to mitigate attacks, such as HTTP Request Smuggling attacks. In this version, the “Support Framing for Request Message” option has been removed (doing a TCP reset) rather than presenting a Security Page by the “Allow a GET request with body” option.
- **Auto-Discovery and Auto-Policy:** These two features, Auto-Discovery and Auto-Policy, have been coupled. When activating Auto-Policy in an Application Path, Auto-Discovery is automatically activated. When Auto-Policy in the last Application Path is deactivated, Auto-Discovery will also be automatically deactivated. It is still possible, though, to Activate Auto-Discovery alone. This will require manual deactivation.
- **Forensics Security Events:**
    - It is now possible to filter security events per key words found in the security event Description field.
    - It is now possible to filter WebSocket Security Events.

WHAT’S CHANGED IN 32.6.7.0

None

WHAT’S CHANGED IN 32.6.6.0

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

5. 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
6. 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.

APM Occurrences Removal

Due to Flash deprecation, APM is no longer supported. Therefore, APM occurrences 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.

SSL Private Key Storage Encryption using AES

Newly created private keys are now stored and exported with AES256 encryption.

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

NFR ID: 200921-000220

WHAT'S CHANGED IN 32.6.5.0

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.

NFR ID: 200724-000003

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

Bot Manager – User ID

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).

AppWall Features

7. 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.
8. 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.
9. 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.
10. 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 32.6.4.0

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.

WHAT'S CHANGED IN 32.6.3.0

High Availability Enhancements

HAID Mechanism for Alteon VA

Alteon VA can either use the VM MAC or a floating MAC as its MAC address in HA communication. The floating MAC has the advantage that it ensures a faster network update when failover occurs, but has the disadvantage that it does not allow more than one pair/group of Alteon VAs on the same Layer 3 network.

To overcome this problem, the HAID mechanism used for Alteon hardware platforms is now also extended to Alteon VA. The HAID lets you generate a different floating MAC for each Alteon VA redundant pair.

NFR ID: 200506-000156

Extend HAID Range

The HAID maximum value is now extended to 256, allowing for up to 256 pairs/groups of Alteon devices on the same Layer 2 network

NFR ID: 200506-000156, 200620-000015

Extend Floating MAC Mechanism in Alteon VA

Prior to this version, the floating MAC mechanism was used in Alteon VA only for interface floating IP addresses. This is now also extended for PIPs and VIPs.

To support this, the new value **extended** was added to the floating MAC parameter (`/cfg/l3/ha/fmac ext`). The value **enable** only enables use of floating MACs for floating IP addresses, while **extended** enables use of floating MAC for floating IP addresses, VIPs, and PIPs.

LDAP Health Check Enhancement

Prior to this version, the LDAP health check allowed configuring only the domain component of a base DN in FQDN format. Starting with this version, it is now possible to define the base DN in LDAP format.

A new parameter, **Base DN Format** (`dnformat`) has been added which lets you specify whether the base DN parameter includes only the domain component of the DN in FQDN format, or a DN in LDAP format.

NFR ID: 200723-000119

Increase Number of Certificates per Group

Alteon supports up to 256 certificates per group, while the number of groups depends on the form factor with the maximum being 1024 groups. In some cases, there is a need for just a few certificate groups but with more certificates per group.

Starting with this version, it is possible to increase the number of certificates per group. However, to preserve the same memory consumption, the number of configurable groups must be lowered. For example, if the number of certificates per group is increased to 512, the number of groups must be decreased by half. The maximum number of certificates is the maximum number of server certificates supported in the form factor.

The default number of certificate groups and certificates per group remains as it was in previous versions. To change it:

- **CLI**: `cfg/slb/adv/memmng/maxcert and cfg/slb/adv/memmng/maxgroup`

- **Web UI**: **System > Memory Management**

Important! For these changes to take effect, Apply and Save must be performed and then the device must be rebooted.

NFR ID: 200602-000034

Increased Tunnels and Static Tunnel Routes Configuration Capacity

Starting with this version, you can support 8k Layer 3 tunnels and static tunnel routes if memory allows. To increase the number of tunnels and static tunnel routes to 8k, use the CLI command `/c/slb/adv/memmng/tnltbl`. This change requires **Apply**, **Save**, and **Reboot** to become active.

NFR ID: 200322-000001

User Role can be Restricted from Viewing the Syslog Logs

By default, a user with the **User** role can view the syslog logs via the CLI or WBM.

Starting with this version, the Administrator can specify the **User** role to view or not view the syslog logs.

CLI: `/cfg/sys/access/user/usrlog`

WBM: **System > Users > Local Users**

Note: This support is applicable to local users only (both predefined and user-defined). It is not applicable to remote users.

NFR ID: 200814-000008

Enlarge Login Banner Size

The CLI banner length has been increased from 319 characters to 1300 characters (which can be set using the `/cfg/sys/bannr` command).

NFR ID: 200921-000035

OpenSSL Version

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

User Lockout Notification During SSH Connection

Starting with this version, when a user is in lockout state due to multiple failed login attempts, no notification displays during SSH connection. With this change, Alteon does not open an SSH connection for users in lockout state, and as a result protects Alteon from redundant opened SSH connections.

Note: The Telnet behavior was not changed and a notification still displays during lockout.

WHAT'S CHANGED IN 32.6.2.0

Alteon VA Infrastructure Upgrades

VMware Tools Upgrade

The VMware tools version deployed with Alteon VA was upgraded to version 10.2.1.

Alteon VA DPDK Upgrade

The DPDK version of Alteon VA was upgraded from version 18.02 to version 19.11.

OpenSSL Upgrade

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

Alteon VA minimum requirements

The minimum disk size requirement for the Alteon VA is now 14 GB (this also includes Alteon VA with AppWall).

Delayed Bind Enable Mode Retired

The delayed bind enable mode is an old legacy mode that allowed some Layer 7 functionality before the introduction of proxy mode. This mode has many limitations and as such it was decided to retire it and remove it from CLI and WBM.

For existing devices that have this mode in their configurations, the capability will be preserved after upgrade.

Real Server Tracking Logic Changes in WBM

An option to automatically add all the real servers (including those that will be added in the future) was added to the WBM.

NFR ID: 190911-000343

Syslog Support Enhancements

RFC 5424 Format for Additional Message Types

Alteon syslog messages can be sent in IETF-Syslog (RFC5424) format in addition to the common BSD-Syslog (RFC3164) format.

This can be done using the `/c/sys/syslog/format` command (in WBM**, System > Logging and Alerts > Syslog Format**).

The syslog format setting is now available for:

- Alteon system events

- Alteon traffic log
- Session log
- Syslog messages sent from AppShape++
- URLF logs

Limitations

The following syslog message types do not support the new syslog format and will continue to be sent in BSD-syslog format:

- WAF log messages
- Defense messaging

AppWall Syslog Limitation Removal

The limitation that AppWall syslogs are not sent when the Alteon syslog protocol is set to TCP/TLS was removed. Starting with this version, even though AppWall syslogs do not support the TCP protocol, they will continue to be sent over UDP events if Alteon syslogs are set to TCP/TLS.

In summary, the following syslog message types do not support TCP/TLS, and will continue to be sent over UDP:

- Session log
- Syslog messages sent from AppShape++
- Defense Messaging
- URLF logs
- AppWall syslog

Treck Version Upgrade to 6.0.1.66

In this version, Treck was upgraded from version 6.0.1.44 to 6.0.1.66, which resolves the following CVEs (including Ripple20, and others):

- CVE-2020-11896
- CVE-2020-11897
- CVE-2020-11898
- CVE-2020-11899
- CVE-2020-11900
- CVE-2020-11901
- CVE-2020-11902
- CVE-2020-11903
- CVE-2020-11904
- CVE-2020-11905

- CVE-2020-11906
- CVE-2020-11907
- CVE-2020-11908
- CVE-2020-11909
- CVE-2020-11910
- CVE-2020-11911
- CVE-2020-11912
- CVE-2020-11913
- CVE-2020-11914

WHAT'S CHANGED IN 32.6.1.0

Syslog Enhancements

Syslog Support in RFC 5424

Starting with this version, Alteon syslog messages can be sent in IETF-Syslog (RFC5424) format in addition to the common BSD-Syslog (RFC3164) format.

This can be done using the `/c/sys/syslog/format` command (In **WBM, System > Logging and Alerts > Syslog Format**)

The syslog format setting is relevant for

- Alteon system events
- Alteon traffic log

Limitations

The following syslog message types do not support the new syslog format and will continue to be sent with BSD-syslog format:

- Session log
- WAF log messages
- Syslog messages sent from AppShape++
- Defense messaging
- URLF logs

NFR ID: 191120-000043

Syslog Over TCP

Starting with this version, Alteon system events can be sent to syslog servers over TCP. This can be done using the `/c/sys/syslog/proto` command (in WBM, **System > Logging and Alerts > Syslog Protocol**)

Limitations:

- The following syslog message types do not support TCP and will continue to be sent over UDP:
    - Session log
    - Syslog messages sent from AppShape++
    - Defense messaging
    - URLF logs
- WAF logs will not be sent when the Alteon syslog protocol is set to TCP/TLS.

Increase of the Number of Syslog Servers to Six

Prior to this version, five syslog servers were supported. Starting with this version, six syslog servers are supported.

NFR ID: 190911-000460

OpenSSL Version

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

TLS Allowed Versions Default

Prior to this version, by default TLS versions 1.1, 1.2, and (where relevant) 1.3 were enabled in newly configured SSL policies. TLS 1.1. is now considered insufficiently secure and allowing it caps the SSL grade provided by Qualys to B. Starting with this version, newly configured SSL policies will have TLS 1.1 disabled by default. Existing SSL policies will preserve the configuration before upgrade. Radware recommends to manually disable TLS 1.1 to achieve a higher SSL grade.

Support Radware-specific RADIUS VSA

Prior to this version, Alteon took the **Service-Type** value from the last attribute received from the RADIUS server. This could be a general attribute or vendor-specific, whichever was last on the list.

Starting with this version, Alteon can take the **Service-Type** value from the vendor-specific attribute irrespective of the order it is received from the RADIUS server. This can be done using the command `/cfg/sys/radius/prefer`

NFR ID: 200306-000092

Security Hardening

- Upon authentication failure, the error message does not reflect the reason for the failure.
- All password inputs are masked.

- The log command is available to all user roles using the CLI (to align with the behavior using WBM).
- For upgrades from versions 32.6.1.50 and later, 32.4.3.50 and later, 32.2.5.50 and later, and 31.0.13.50 and later, to any later version, Alteon uses the SHA2 algorithm for the digital signature (in all platforms).

NFR ID: 191126-000098

AppWall KPI Reflection in the Alteon System JSON

Starting with this version, the following AppWall KPIs are available in the Alteon system JSON when integrated AppWall is enabled: AppWall CPU, memory, swap, CPS, concurrent connection, transaction rate, and throughput bps

In addition, the AppWall CPU and memory are taken into consideration in the system health score calculation.

NFR ID: 191212-000019

Client NAT Port Assignment Logic

Starting with this version, it is possible to select the client NAT port assignment algorithm on Alteon running on the vADC form factor. The options are:

- Sequential (default) – Minimizes the probability of fast port reuse, but it can be a security vulnerability
- Random – Provides increased security, but the probability of fast port reuse is higher

This can be done using the command `/cfg/slb/adv/pport` (in WBM, **Application Delivery > Virtual Service > Settings > Session Management** tab).

Notes:

- The change in the client NAT port assignment algorithm will only take place after statistics are cleared `(/oper/slb/clear`).
- On Alteon VA and Alteon platforms in standalone mode, the client NAT port assignment uses an enhanced random mode that also minimizes fast port reuse probability.

NFR ID: 200407-000053

Alteon VA Auto-healing – Mismatch of Number Queues

Prior to this version, when there was a mismatch between the number of queues configured on the host and the Alteon VA VM configuration, Alteon VA would not boot up. This could occur, for example, when the number of SPs configured on the Alteon VA was greater than the number of queues the host supports.

Starting with this version, Alteon VA identifies this mismatch and reduces the number of SPs to match the number of supported queues.

Alteon VA Preserves Ports Order after Reboot

The issue when the ports order of an Alteon VA was changed after a reboot (mainly on Alteon VA platforms with more than four ports configured on them) was resolved for VMware and OpenStack/KVM deployments (in this version this capability is disabled by default).

Troubleshooting (More Information in Tech Data)

The following information was added to tech data to facilitate troubleshooting:

- Top 100 large files
- TCP sockets in use by MP (netstat)

WHAT'S CHANGED IN 32.6.0.0

OpenSSL Version

The OpenSSL version is updated in this release as follows:

- S/SL platform models, regular platform models, and Alteon VA now use OpenSSL 1.1.1d
- XL/Extreme platform models, as well as 6024 FIPS II, use OpenSSL 1.0.2u

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

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

Fixed in 32.6.10.0

General Bug Fixes

Item	Description	Bug ID
1.	Using SSH, there was no matching key exchange method found when connecting from Ubuntu 20.	DE70423
2.	On an Ubuntu 18 VA device, when selecting a time zone GMT offset greater than 4 hours, the GEL license activation failed.	DE73645
3.	Application delivery features were not available via API for the slbviewer user role.	DE74198
4.	When an IPv6 virtual server used IPv4 servers for load balancing and if any SLB config apply was performed, the existing sessions were closed.	DE74226
5.	An Alteon 5224 platform rebooted because of a power cycle.	DE74352
6.	PCI compliance with Alteon SSH failed.	DE74372 DE74374
7.	The device restarted by a software panic.	DE74396
8.	After config sync, the Traffic Event Log policy sent a log via the data interface.	DE74450
9.	There was a Switch HA failover issue.	DE74514
10.	vADC buffer memory related to SSL caused a reboot.	DE74589
11.	An SSH management connectivity issue occasionally caused a reboot.	DE74606
12.	The wrong time zone offset was sent to the NTP server.	DE74636

Item	Description	Bug ID
13.	On a vADC, the GET /config/SlbCurCfgEnhVirtServicesTable message was received during config sync and all hash tables were initialized (zeroed), causing a reboot.	DE74688
14.	A malformed server caused a miscalculation of the RTO, which led to the retransmission taking a minute, in which time the server closed the connection.	DE74760
15.	A vADC stopped processing production traffic.	DE74786
16.	The MP CPU utilization was high with DNS packets (dport 53).	DE74809
17.	When configuring network settings, an internal error was issued.	DE74816 DE74818
18.	On a 9800 platform with new hardware, the management port connectivity was down.	DE74827
19.	On an ADC-VX, an LACP issue was caused by high MP CPU utilization.	DE74842
20.	When the device started after a reboot, it stopped performing ARP base health checks.	DE74866
21.	Alteon VA devices deployed in Hyper-V experienced high CPU usage compared to other hypervisors.	DE74933
22.	Using SNMPv3, the "Unknown user name" is now issued for invalid usernames and invalid passwords.	DE74948
23.	The Ext.HC script did not generate traffic.	DE75007
24.	From WBM, when the SSH key was set to be deleted, after clicking **Submit** it was immediately deleted before the device was rebooted.	DE75020
25.	The device rebooted because of a software panic.	DE75038
26.	After inserting a 1 G GBIC, message logs did not display.	DE75056 DE75058
27.	Changing vADC CUs caused syslogs to be removed.	DE75086 DE75088
28.	AppWall LDAP connection failures were caused due to the multiple creation of MP processes.	DE75153
29.	After rebooting, configuration sync failed and the configuration was stuck in diff with the same error.	DE75227
30.	Alteon did not display the Korean language correctly when using local language-Korean.	DE75254

Item	Description	Bug ID
31.	When trying to use Single IP in Azure, a message was issued that the user should use Multiple IP address mode.	DE75284
32.	After an Apply failure due to an empty passphrase for certificates, after reboot the entire configuration went into diff.	DE75335
33.	There was duplicate entry validation error for two domains where one had a hostname and the other did not have a hostname.	DE75353 DE75355
34.	When using the Russia time zone, the incorrect time displayed for the /info/sys/time command and in AppWall Forensics.	DE75402
35.	On an Alteon VA, packets larger than the negotiated MTU size were forwarded.	DE75427
36.	On a vADC, when executing SSL stats commands, the vADC rebooted.	DE75446
37.	After the primary real server was activated in a group, the session handled by the backup real server was fastaged.	DE75536
38.	An SSH management connectivity issue occasionally caused a reboot.	DE75550
39.	When gathering the device output, memory stats information did not appear in the techdata.	DE75687
40.	The client certificate went through OCSP verification even though it is in OCSP stapling mode.	DE75806
41.	SNMP polling resulted in an incorrect response.	DE75838
42.	The DNS Cache per IP version feature was not working	DE75978

AppWall Bug Fixes

Item	**Description**	**Bug ID**
1.	Request of /v2/config/aw/SecurityEvents/ returned a false response.	DE75916
2.	The forensics search engine was not accurate.	DE74469
3.	Wildcard hostname (*nma.lt) worked incorrectly and caused false positive.	DE74667
4.	Session filter removed the cookie in passive mode.	DE74748
5.	There was no detailed information about a pattern.	DE74850
6.	Protected applications behind AppWall went down suddenly.	DE75232
7.	Under certain conditions, no explanation is provided in the	DE75513

Item	Description	Bug ID
	Forensics API Security event.	
8.	Geo filter (ZZ) to display the Forensics logs for Private networks did not work.	DE75593
9.	In Forensics, the filter according to the Geo-Location did not work.	DE74346

Fixed in 32.6.9.0

General Bug Fixes

Item	Description	Bug ID
1.	The IPv6 static route failed if the respected interface was configured with the same Apply.	DE67582
2.	Mirrored session statistics were not updated for Smart NAT Inbound traffic.	DE71994
3.	When the real and virtual server statistics were incremented or decremented the logs were not updated.	DE72086
4.	Using WBM, expired certificates could not be exported because there was a validation check on the “validation period” (1 to 3650).	DE72167
5.	A user was allowed to configure a duplicate Static ARP entry using WBM, but not the CLI.	DE72182 DE72184
6.	Attempting to delete a server or CA certificate group explicitly or implicitly resulted in an AX internal OOS failure.	DE72200
7.	Upgrade failed because of incorrect resource allocation (SP and AW cores).	DE72280 DE72282
8.	When trying to change the Traffic/AppWall capacity units (CUs) for a single vADC, an error occurred.	DE72342
9.	In an IPV6 environment, when Static NAT was configured, ICMP traffic failed.	DE72401
10.	IPsec sessions abruptly aged out due to an incorrect interpretation of TCP flags.	DE72425
11.	An Open SSL vulnerability (CVE 2022-0778) was fixed.	DE72461
12.	An HA failover caused SIP packets to be lost.	DE72528
13.	When there was an overflow of the Current Sessions value, unexpected statistics of Available Sessions and DNS answer resulted.	DE72558

Item	Description	Bug ID
14.	Bandwidth utilization was displayed incorrectly as Mbps, when it should have been MBps.	DE72624
15.	After upgrade, the configuration was not preserved.	DE72653
16.	In and ADC-VX environment, when executing putconfig and tech data collection at the same time on a vADC, the vADC rebooted.	DE72662
17.	When there was a TCB block leak, DSSP health checks failed.	DE72725
18.	During a vADC shut down, the ADC-VX process requests the TD to recycle network driver buffers. This process took more time than was allocated for the TD process to run.	DE72742 DE72744
19.	On a 6024 platform, increasing the session table by size 200% required a minimum 64 RAM.	DE72807
20.	The Ansible module description of vip_health_check_mode was incorrect.	DE72819
21.	Using APSolute Vision the Alteon EAAF data base of was not updated.	DE72826
22.	VRRP did not sending advertisements because the VR state was incorrected checked.	DE72836
23.	Using Alteon VA, in some cases when running Ubuntu18 OS and DPDK, allocation of SPs was not based on the vCPU configuration.	DE72845
24.	The AppWall nodejs mdoule flapped on virtual plaforms in the following cases: 1. When there are more than 10 vADCs 2. When vADCs are configured with the basic flavor.	DE72859
25.	An Alteon cluster running on Azure had high availability issues.	DE72943
26.	The Persistency gmetric was not working correctly.	DE72964
27.	In version 32.6.6.50, there was a sudden reboot.	DE72970
28.	An Alteon NG 5424-S rebooted because of a BSP problem with the monotonic timer.	DE72988
29.	Alteon VA version 33.0.4.0 using Ubuntu12 rebooted on the execution of the Display Certificates Group configuration.	DE73037
30.	There was an error with traps for IPv6-related events.	DE73067
31.	Cookie-based real server selection caused a reboot. Defensive code was aded to address the issue.	DE73089
32.	A request to make to increase the height of the "Configuration Sync - Peers" in WBM.	DE73190

Item	Description	Bug ID
33.	A DNS responder with delegation for TCP session did not close.	DE73212
34.	In a WANlink environment, traffic was processed by ISP, which was down.	DE73234
35.	Disk space exceeded the high threshold with 80 % usage because of the AppWall cores.	DE73250
36.	On a version 30.5.22.0 vADC, FQDN resolution update failed.	DE73306
37.	On an Alteon VA, intermediate certificates were not fetched.	DE73342
38.	A health check timeout failure caused a reboot due to a race condition when freeing the object.	DE73536
39.	Fixed Ansible documentation in alteon-device-facts.	DE73622
40.	Continuous operations on real server groups (additions, deletions, amendments) could lead to an internal OOS state.	DE73664
41.	In an Alteon VA environment, occasionally empty syslog messages were generated when the size exceeded 1300 bytes.	DE73748
42.	On a vADC, inbound host-based LLB rules were not created using the LinkProof menu due to RBAC issues.	DE73774
43.	SSLi did not forward traffic when creating the FW HA, due to 10G not working correctly on VHT.	DE73814 DE73816
44.	Trying to add vADC licenses to the ADC-VX when vadcadv had a custom flavor caused an error.	DE74076

AppWall Bug Fixes

Item	Description	Bug ID
1.	Under certain conditions, Source Blocking reports an “Always Blocked” IP source.	DE72050
2.	The Forensics session and the Dashboard’s Current Activity is not displayed on the AppWall Management Console.	DE73465
3.	For database refinements which involve XML, a false positive is shown, and the request is still blocked.	DE74094

Fixed in 32.6.8.0

General Bug Fixes

Item	Description	Bug ID

Item	Description	Bug ID
1.	The special Regex character '\' '\\' should be added.	DE69957
2.	During vADC creation, the rm system call failed because of a typo in the path. The path to the file to be deleted was fixed.	DE69963 DE69965
3.	With IDS chain configured, ICMP responses from the server were not forwarded to the client.	DE70045
4.	FQDN real server IP addresses incorrectly ended with a period (".").	DE70253
5.	Rebooting an ADC-VX caused vADCs to be stuck in the initialization stage.	DE70263
6.	The ICMPv4 real server health check failed while a CLI ping worked correctly. A v4 debug command was added.	DE70302
7.	A user was locked out after making a password change.	DE70324
8.	A mechanism was added that prevents false PS (power supply) status indications when there is a dual PS configuration.	DE70368
9.	The TLS 1.3 protocol did not display in the Backend SSL policy.	DE70445
10.	The XFF code in the HTTP/2 proxy used the VIP instead of the Client IP address.	DE70460
11.	The AppWall check did not recognize that AppWall was frozen and did not restart AppWall.	DE70469
12.	Configuration sync failed due to a long certificate group ID.	DE70485 DE70487
13.	When LACP was disabled on ports, the port mask was not updated correctly on both the MP and SP. This wrong port mask in the SP impacted packet forwarding.	DE70514
14.	A panic occurred during a packet capture.	DE70543
15.	The HTTP/2 health check did not contain the ALPN protocol in the SSL handshake.	DE70592
16.	After an unexpected reboot of Alteon VA on ESXi 7.0, could not save changes after Apply, and received error messages.	DE70599
17.	The MP CPU utilization was high when applying the configuration, causing a network interrupt.	DE70613
18.	After upgrade, empty groups with no real server added to them	DE70632

Item	Description	Bug ID
	could shift the group index map.	
19.	The ARP table information was not the same between the CLI and WBM.	DE70689
20.	A mixed type SNS request failed (dnsrespoder VIP IPv4 and query type IPv6, and vice versa).	DE70703
21.	An unexpected VRRP failback when preemption is disabled.	DE70747
22.	A panic occurred due to memory corruption.	DE70771 DE70773
23.	Alteon displayed inaccurate SFP Tx and Rx power values.	DE70786
24.	Could not manual delete a session table entry for VPN traffic.	DE70803
25.	Uppercase characters were, incorrectly, added to HTTP headers for HTTP/2 proxy, which generated the following error: Upper case characters in header name	DE70812
26.	The max_cipher_list_length was increased from 16000 to 20000.	DE70967
27.	In 32.6.7.0 as SC11788 (DE69479)	DE70999
28.	If multiple VIPs had the same IP address as the VSR, traffic failed to all virtual servers when one of these virtual servers was deleted.	DE71071
29.	When running dbind disable service, a panic occured when Alteon received the RST packet from the server.	DE71114
30.	Following the successful deletion of an HTTPS virtual service (and all its SSL elements), trying to reconfigure the same service resulted in an "internal out-of-sync configuration" state. A console message and recommendation to reset the device followed.	DE71134
31.	Enabling IPv6 on a virtual server caused a panic.	DE71147
32.	Real server health checks were not started when there was a run-time instance with an improper index in the dispatch queue of slice 4.	DE71267
33.	After resetting a non-debug Alteon VA platform, GEL licenses some times were lost when they passed non-GEL applicable validations.	DE71294
34.	Fixed the License Manager connection failure algorithm.	DE71351
35.	The LINK LED remained ON even when the optical cable was pulled off or the ACT LED was not working.	DE71471

Item	Description	Bug ID
36.	The file descriptor was allocated and not released during execution of SP/MP profiling./maint/debug/cpuProfiling/	DE71500 DE71502
37.	A MAC flap occurred because of VRRP advertisements sent by the backup Alteon device.	DE71522
38.	When an AppShape++ script was applied with cmd logging enabled, Alteon rebooted.	DE71528
39.	The GEL license logs were generated every 5 minutes, causing memory leaks.	DE71582
40.	Support of stapling and client certificate verification added.	DE71594
41.	Alteon could be down when a specific traffic pattern request interacted with the redirect service using dynamic tokens.	DE71619
42.	On a vADC device, the MP CPU reached 100%.	DE71656
43.	When a DPDK image reset, an unexpected DNS server IP address was added by BSP.	DE71756
44.	After the AppWal health check failed, the MP restarted AppWall every 15 seconds .	DE71820
45.	The Application Services engine was not synchronized with the current configuration.	DE71840
46.	The remote real server DSSP health check was reported as UP even though the related virtual server had the status of "NO SERVICES UP", due to a WANlink real server health check failure.	DE71899
47.	Could not allocate memory to run the diff command.	DE71907
48.	After switching the BGP mode to FRR, the BGP ASMODE default value changed to 2 bytes when it should have been 4 bytes.	DE72020
49.	Port errors increased in version 32.6.6.50 as compared to version 32.4.6.0 with the same physical cables and toplogy.	DE72573

AppWall Bug Fixes

Item	Description	Bug ID
1.	When adding a host under an existing Webapp using API, an Error 400 was shown.	DE70145
2.	A Corrupted Configuration File Detected error was shown.	DE70260
3.	HTTP DELETE requests were being blocked by AppWall’s	DE70675

Item	Description	Bug ID
	FileUpload filter and reported as PUT.	
4.	The Brute Force filter was not working on API-based server responses.	DE70797
5.	A Threshold of incoming sessions event was shown when the total active connections were much lower than the maximum.	DE71105
6.	Under some conditions, long header Hostnames led to a syslog failure.	DE70821
7.	The APSolute Vision AppWall dashboard displayed wrong data	DE70207

Fixed in 32.6.7.0

General Bug Fixes

Item	Description	Bug ID
1.	Wrong management of TSO buffers and logs flood from the AE module caused a panic.	DE66433
2.	An upgrade from version 32.4.4.50 to 32.6.3.50 caused CPU pressure.	DE68305
3.	Azure Government Alteon VA boot looped on deployment.	DE68563
4.	On an Alteon-VA platform with BWM configured, when switching from DPDK to TUNTAP, in some instances a software panic occurred.	DE68861
5.	Alteon 6420 running on version 32.4.6.50 rebooted due to a software panic	DE68956
6.	Under a heavy load due to BGP traffic, BGP peer sessions were flapping with holdtimer expiry notifications. This has been addressed with a config option and recommended values of keepalive/holdtime.	DE69009
7.	A MAC flap occurred because of HA advertisements sent by the backup Alteon device.	DE69139 DE69141
8.	Upgraded to the latest NGINX version because of a vulnerability.	DE69162
9.	In some instances, an Alteon reset occurred when an obsolete TACACS state structure was accessed when the V4 data port TCP connection to the TACACS server was waiting for graceful termination.	DE69252
10.	On an Alteon 6024 platform, the primary and secondary	DE69295

Item	Description	Bug ID
	devices rebooted automatically due to a stack overflow.	
11.	On an Alteon 6420 platform, there was a data transmission problem with packet fragmentation with a one minute delay.	DE69331 DE69333
12.	When attaching or detaching an SSL policy, the wrong port changed.	DE69392
13.	When attaching or detaching an SSL policy, the wrong port changed.	DE69394
14.	On an Alteon 6420 platform, there was a data transmission problem with packet fragmentation with a one minute delay.	DE69403
15.	On a 7612 platform, after a vADC was enabled there was a large VS address delay.	DE69411 DE69413
16.	After upgrading from 32.6.3.50 to 32.6.6.0, there was latency/delays.	DE69415 DE69417
17.	When a DNS Response was received with new IP addresses and new real servers created, the Save flag was set to ON.	DE69421
18.	In a BGP, BFD environment, BFD connections went down when BWM processing was enabled, leading to BGP adjacency going down.	DE69439
19.	Config apply took more than 10 minutes.	DE69479
20.	Because the hostname was limited to 30 characters, it displayed in two lines when the hostname had more than 30 characters. The limit has now been increased to 64 characters.	DE69497
21.	When configuring cntclss values, a max length validation failure did not display the correct error.	DE69509
22.	In an ADC-VX environment, trying to create vADC 10 caused a panic.	DE69549
23.	Could not view the connection statistics in both WBM and CLI.	DE69594
24.	Could not configure the user role WSAdmin in SA mode.	DE69640
25.	In an SLB environment with VLAN level proxy configured, in some instances the MAC flapped after an SLB config apply.	DE69667
26.	After upgrading Alteon VA from version 32.4.4.3 to 33.0.1.50, Alteon VA lost its configuration followed by and AX-Out-Of-Sync.	DE69699
27.	When creating a content class a panic occurred.	DE69768

Item	Description	Bug ID
28.	In a tunnel environment, all configured tunnel static route tables did not display under the route dump.	DE69831
29.	Ansible facts gathered from standalone devices did not provide the correct image list.	DE69869
30.	After reboot, Alteon falsely reported that the MGMT IP address was changed.	DE69944
31.	The special character '\' was added to the REGEX string '\\'.	DE69957
32.	Alteon 5208 rebooted because of a software panic.	DE69994 DE69996
33.	Alteon displayed a configuration as pending, but would not accept an apply or save. This was because a group associated with fqdnreal was empty.	DE70058
34.	The dns-responder with DNSSEC did not work on Cavium platforms since version 32.6.0.0.	DE70111 DE70113
35.	In an Alteon HA environment with a virtual service configured with an AppShape++ rule, the Alteon backup rebooted when the configuration was synched to the backup.	DE70163
36.	An Alteon D-5208S platform abnormally rebooted because of a software panic.	DE70232

AppWall Bug Fixes

Item	**Description**	**Bug ID**
1.	AppWall displayed an “Initialization error” after the navigation to Security filters.	DE68858
2.	AppWall API management: HTTP tunnel PUT method changed to contain all the mandatory fields. Creation of the PATCH Method.	DE69722

Fixed in 32.6.6.50

General Bug Fixes

Item	Description	Bug ID
1.	The exporter port 46000 was accessible through the Management IP address, and as a result it appeared in the vulnerability scan.	DE66271
2.	An Internal out-of-sync configuration was detected.	DE68009
3.	In an HA environment, after the backup device rebooted, FTP	DE68024

Item	Description	Bug ID
	data sessions disappeared intermittently on the backup device.	DE68026
4.	Config sync failed with EC certificates in the configuration.	DE68186
5.	After user-defined ciphers, the Application Services engine was not synchronized with the current configuration.	DE68193 DE68415
6.	On an Alteon VA device, in some instances if eth0 was removed and then re-attached, Alteon VA displayed more links than the actual interfaces.	DE68222
7.	When the MRST flag was set to on, it was not possible to disable a data port.	DE68250 DE68255
8.	A port disabled in a saved configuration needed to be toggled twice to bring it up after reboot.	DE68269 DE68272
9.	On an Alteon VA platform, sometimes resource allocation was not working correctly when the VA was deployed with multiple cores but with a disabled multi-queue for the image.	DE68276 DE68278 DE68281
10.	Alteon forwarding or routing packets without SRC MAC translation led to a MAC flap issue.	DE68298 DE68301
11.	Using the WBM, after creating a vADC, the vADC stayed in the init state.	DE68400 DE68403
12.	Alteon responded to Non-RFC compliant responses for DNS requests.	DE68407 DE68410
13.	When the WANlink server was operationally disabled and then re-enabled, the WANlink peak statistics were incorrect.	DE68440 DE68443
14.	Removed the unnecessary syslog message that appeared in vADCs on each Apply.	DE68575 DE68577
15.	Using APSolute Vision, newly created vADCs were not manageable.	DE69611 DE68614
16.	After upgrading to version 32.6.5.0, vADCs could not be managed by the APSolute Vision server.	DE68790 DE68792 DE68795
17.	On an Alteon 5424 (ODS-LS2) platform, the real server capacity in standalone and ADC-VX modes was increased in 8192.	DE68843 DE68845 DE68848

Item	Description	Bug ID
18.	A software panic occurred followed by an AX Out-of-sync.	DE68882 DE68885
19.	Was not enable to sync the configuration between devices in the beta code.	DE68913 DE68916
20.	Issue with FQDN servers. Logs were added to help with this issue.	DE68927 DE68929 DE68932
21.	A panic occurred with with a loss of the configuration. Fixed included not tracing empty DNS responses.	DE68943 DE68945 DE68948
22.	The SIP INVITE went to the wrong real server.	DE68969 DE68972
23.	An empty user agent caused a panic.	DE69044 DE69047
24.	During the tunnel handling routine, Alteon reboots with IP fragmented traffic.	DE69715 DE69178
25.	BM JS injection occurred when no BM was configured.	DE69191 DE69194 DE69198 DE69201

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall blocked requests when Host protections (CSRF/URL Rewrite/Redirect validations) had the “Inherit” status.	DE67920
2.	Debug log added to link the Source Blocking scoring and the related security event.	DE66587
3.	Wrong IP blocked with Source Blocking.	DE68383
4.	Wrong host displayed in syslog security event.	DE68396
5.	Wrong hostname displayed in the Forensics security events when blocked by the Application Security policy.	DE68487
6.	In specific scenarios, AppWall restarted when the Host protector was in Inherit mode.	DE70250

Fixed in 32.6.6.0

General Bug Fixes

Item	Description	Bug ID
1.	The L4oper user could not view the Virtual Servers pane.	DE65789
2.	Too many core files took up too much disk space, resulting in techdata failing.	DE66123
3.	The device became full with too many open files, causing it to run slowly.	DE66426
4.	Alteon sent malformed SNMPv3 traps when aes128 or aes256 were configured as the privacy protocol.	DE66748
5.	STP packets dropped by the ND caused a loop.	DE66779 DE66781
6.	Panic analysis.	DE66955
7.	When passing the client certificate via the HTTP header in a multiline in compatible mode, the last hyphen (-) was removed.	DE67195 DE67197
8.	The router ID was not visible for between routers for traceroute.	DE67258 DE67260
9.	There was a WBM error for the SLBVIEW user.	DE67375
10.	Using WBM, the DNS responder VIP displayed as up even if it was disabled by configuration.	DE67544
11.	With VMAsport enabled, SSL-ID based persistency was not maintained correctly.	DE67631 DE67633
12.	When traffic matches a filter that is configured with layer7 loopup, Alteon panicked.	DE67655
13.	Incorrect units displayed for uploading/downloading bandwidth for WANlink real servers.	DE67713
14.	The network driver process was stuck and caused Linux core 0 to be stuck. This caused the MP to be stuck.	DE67717
15.	When deleting a group and the FQDN associated with that group, the group was deleted twice from the AX database.	DE67721 DE67723
16.	There was a non-existing Rlogging policy on a disabled traffic event policy.	DE67729
17.	In WBM, the real server table displayed as empty.	DE67821
18.	Using AppShape++, when attaching/detaching a content class SSL from a filter, the AppShape++ command was removed	DE67833

Item	Description	Bug ID
	and recreated, but the order was incorrect.	
19.	AppWall init completion took a very long time.	DE67869
20.	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.	DE67900
21.	There was a crash in the external "nano messages" package.	DE67939
22.	The AppWall process took more time to start than expected.	DE68030 DE68032 DE68034
23.	In a virtual environment, configuration sync from the ADC-VX failed.	DE68061
24.	An empty AVP prevented AppShape++ from parsing a RADIUS transaction.	DE68081
25.	Some Fastview configuration files were not updated as part of the new feature using FastView JS injection capabilities.	DE68088
26.	When the hold timer expired, Alteon sent a notification with a cease.	DE68094 DE68314 DE68317

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
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 32.6.5.50

General Bug Fixes

Item	Description	Bug ID
1.	In an RSTP environment, the port state transition from DISACRD to FORWARD was delayed.	DE66168 DE66171
2.	The SSL Hello health check caused a memory leak which led to a panic.	DE66190 DE66193
3.	The CRL could be considered expired before the true expiration time because of the time zone.	DE66217 DE66220
4.	Alteon VA in DPDK mode crashed when BWM processing with BW shaping was enabled.	DE66398 DE66401
5.	After configuring a deny route for a DSR VIP with tunnels set to real servers, the MP panicked.	DE66472 DE66475
6.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66479 DE66482 DE66570 DE66572 DE66575
7.	Using WBM, when users of type 'user' was disabled, they could still successfully log in.	DE66530 DE66533
8.	Could not create a new BWM policy on a 4208 device.	DE66622 DE66625
9.	Panic analysis.	DE66640 DE66643
10.	On a Cavium platform, there was a memory leak when using ECDHE-RSA-AES256-SHA384 as the back-end cipher and the server triggered SSL renegotiation.	DE66696 DE66699
11.	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.	DE66704 DE66707
12.	After a Trust CA group was configured, no other certificates could be deleted even if they were not part of the Trust CA group.	DE66721 DE66724

Item	Description	Bug ID
13.	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.	DE66730 DE66733
14.	When AES128 or AES256 were configured as the privacy protocol, Alteon sent malformed SNMPv3 traps	DE66751
15.	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.	DE66802 DE66804
16.	BGP neighboship did not get established because of issues with the AS number functionality.	DE66810 DE66812 DE66815
17.	Using WBM, when refreshing the Virtual Services tab, the VS status displayed as Warning instead of UP.	DE66880 DE66882 DE66885
18.	The user was unable to access Alteon WBM.	DE66891 DE66894
19.	Panic analysis.	DE66958
20.	Starting with this version, the SNMPv3 target address table is available in the Ansible module.	DE67003 DE67006
21.	When the SP CPU was activated, a false `Throughput threshold exceed message` displayed.	DE67123 DE67126
22.	There was an overflow of RAM disk memory allocated for logs.	DE67130 DE67132 DE67135
23.	Using WBM, real servers and groups are not displayed for HA tracking.	DE67279
24.	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.	DE67288
25.	In WBM, HAID did not display properly.	DE67452 DE67454 DE67457

Fixed in 32.6.5.0

General Bug Fixes

Item	Description	Bug ID
1.	The random salt was a predictable random number generation function generating a similar sequence.	DE63667
2.	Could not enable the extended_log via Ansible.	DE63840
3.	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.	DE63991
4.	The real health check displayed different times in CLI and WBM.	DE64032
5.	On a 4208 platform, the option to convert to virtual (ADC-VX/ADC) mode displayed the following error message: The operation cannot be performed	DE64091
6.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64152
7.	The MGMT port status was DOWN but the Link and operational status was UP.	DE64232
8.	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.	DE64247
9.	In an HA environment, when the RADIUS service was enabled with mirroring and associated with an AppShape++ script , RADIUS authentication timed out.	DE64320
10.	An internal link on Alteon VA caused connections to drop.	DE64252 DE64256
11.	Applying part of the nginx when disabling the Web proxy took too much time.	DE64341
12.	When pbind clientip and vmasport were enabled, the persistent session was not permanently deleted.	DE64355
13.	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.	DE64379

Item	Description	Bug ID
14.	Added a REGEX to accept the dot (.), slash (/), and backslash (\) characters.	DE64458
15.	Added a REGEX for the path fields that accept special characters.	DE64465
16.	Config sync transmit was aborted between two devices when the sync request was received from a third device.	DE64487
17.	Predefined HTTP headers were used when POST HTTP health checks were sent without taking into the account the actual body length.	DE64523
18.	After receiving the same routes in BGP updates when Alteon failed to set a protocol owner, Alteon deleted the RIB.	DE64533
19.	Using WBM, ephemeral servers did not display in the Configuration menu.	DE64585
20.	After performing /boot/shutdown, TLS version 1.1 was incorrectly being set to enabled.	DE64596
21.	In a BGP environment, when BGP peers were directly connected, the BGP state stayed as Connect even though the local interface was disabled.	DE64647
22.	Using a logical expression health check resulted in an unexpected real server state.	DE64690
23.	Upgrading an ADC-VX generated the following error message on the console: write error: Broken pipe	DE64703
24.	The management Web server did not work due to a bug with the access SSL key on FIPS.	DE64731
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.	DE64758
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.	DE64786
27.	The Layer 2 system configuration had an incorrect BoardType for 7216NCX.	DE64888
28.	When real servers were down, Alteon sent traps with the wrong OID.	DE64899
29.	In an SLB environment, when the primary server failed, the secondary backup displayed as "UP" instead of "BLOCKED".	DE64924

Item	Description	Bug ID
30.	On a 7220 platform, when Alteon received a packet with a size greater than 1500, it panicked	DE64946
31.	In DPS Perform mode, AppWall was not pushed to vADCs.	DE64992 DE64996
32.	The weighted least connection was not correct.	DE65007
33.	When there was a state transition from backup to master, GARP was not sent.	DE65039
34.	There was an incorrect rule ID for retrieving statistics from the SP.	DE65177
35.	Added the FastView smfhub self-healing mechanism.	DE65203
36.	Defect that tracked DE65346 -- Device auto rebooted with reason of hardware watchdog.	DE65234
37.	Accessing a device using APSolute Vision or WBM caused a memory leak and eventually led to a panic.	DE65240
38.	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.	DE65283
39.	Even though there are no open connections, new SSH connections were ignored with a "max connection reached" error.	DE65301
40.	The comparison function used to compare the SSL policy name was incorrect.	DE65317
41.	Added more information to the debug log when an ASSERT occurs on an ndebug image.	DE65344
42.	After performing config apply, GSLB DNS responses returned a remote IP address instead of a local VIP.	DE65364
43.	The MP CPU utilization was high when querying virtual stats.	DE65379
44.	A connection drop occurred because a virtual service was reset due to a virtual index mismatch after applying new configuration changes.	DE65405
45.	SIP UDP service run by AppShape++ failed (it was used for persistency and/or Layer 7 manipulation).	DE65435
46.	After attaching a second hard disk to Alteon VA, the DPDK network driver did not load.	DE65458
47.	The Alteon Data interface with port range 40k-45k mistakenly was accessible from outside world.	DE65485

Item	Description	Bug ID
48.	Even though the SP/MP profiling logic was disabled by default, Alteon panics with SP profiling logic being triggered.	DE65491
49.	Whenever multiple requests were sent with a cookie in a single session for multiple services, Alteon did not decrement the current session properly.	DE65504
50.	Alteon displayed the diff and diff flash without any configuration changes.	DE65535
51.	Using RCA, there was an incorrect virt-sever ID display.	DE65564 DE65566
52.	AppWall crashed when not receiving the i/o time.	DE65573
53.	The SP performed unequal traffic distribution.	DE65605
54.	When burst traffic was sent to Alteon, some p-sessions remained in the zombie/stale state.	DE65663
55.	Added support for the IF IP to connect to the service dashboard.	DE65678 DE65680
56.	Added a maint debug CLI command to export the virtual stat service table to understand the cause of the virtual stats not working.	DE65705
57.	A new Regex command forbade a hyphen (-) by mistake.	DE65720
58.	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.	DE65742
59.	In an RTSP environment, the RTSP service stopped working and all the SYN packets were dropped.	DE65744 DE65746
60.	When all 24 GBICs were inserted, the Watcher timed out when ports were initiated.	DE65782 DE65784
61.	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.	DE65831
62.	Performing gtcfg via SCP resulted in a panic.	DE65857
63.	Multi-line notices via ansible did not work.	DE65861
64.	Added the HW platform type MIBs for 6024, 5208, and 8420	DE65865

Item	Description	Bug ID
	to the MIB tree.	
65.	When vmasport was enabled, the service ceased working.	DE65896
66.	The AppWall service did not restart after being ended by the MP.	DE65917
67.	The /c/port xxx/gig/cur command displayed breakout details, even though breakout was not applicable.	DE65935 DE65937
68.	When the rlogging TCP health check is running via the MGMT port, Alteon sometimes panics.	DE65957
69.	When BFD and tunneling were enabled, a panic occurred.	DE66001
70.	Using SNMP, OIDs errorCountersSpTable and eventCountersSpTable could cause Alteon to not be accessible via SSH or WBM.	DE66030
71.	With the command logging feature enabled, Apply/Save resulted in a panic.	DE66100 DE66102
72.	While initiating the SSL client connection for the SSL health check, the vADC MP crashed.	DE66139
73.	Adding and deleting real servers or groups resulted inan AX Out-Of-Sync error.	DE66179

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

Fixed in 32.6.4.50

General Bug Fixes

Item	Description	Bug ID
1.	The random salt was a predictable random number generation function generating a similar sequence.	DE63662

Item	Description	Bug ID
2.	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.	DE63983
3.	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.	DE63990
4.	In the USM pane, added support for SHA2 and AES-256.	DE64025
5.	The realhc stat had a different time between the CLI and WBM.	DE64031
6.	A 4208 platform displayed the option to convert into virtual (VX/ADC) mode.	DE64090
7.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64151
8.	When the MGMT port status was Down, the Link and Operational statuses were incorrectly Up.	DE64230
9.	In an SLB environment with cookie insert enabled, server responses towards a client that underwent cookie processing had a mismatch of the SRC MAC with an incoming client request.	DE64246
10.	In an HA environment, when the RADIUS service was enabled with mirroring and associated with an AppShape++ script, there was a RADIUS authentication timeout issue.	DE64319
11.	Applying an operation took an inordinate amount of time.	DE64340
12.	A persistent session was not permanently deleted when pbind clientip and vmasport were enabled.	DE64354
13.	Added a REGEX to accept, dot (.), slash (/), and backslash (\) characters.	DE64455
14.	Added a REGEX for the path fields that accept special characters.	DE64460 DE64463
15.	There was a fix for CVE-2021-3449.	DE64470
16.	When the sync request was received from a third device, the config sync transmit was aborted between two devices.	DE64485
17.	Predefined HTTP headers were used when POST HTTP health checks were sent without accounting for the actual body length.	DE64519
18.	When Alteon failed to set a protocol owner, Alteon deleted the	DE64532

Item	Description	Bug ID
	RIB after receiving the same routes in BGP updates.	
19.	Using WBM, the ephemeral servers did not display in the Configuration menu.	DE64584
20.	After performing /boot/shutdown, TLS version 1.1 was incorrectly being set to enabled.	DE64592 DE64595
21.	In a BGP environment, when the BGP peers were directly connected, the BGP state stayed in the Connect state even though the local interface was disabled.	DE64646
22.	Using a logical expression health check resulted in an unexpected real server state.	DE64686
23.	When upgrading an ADC-VX, the error message "write error: Broken pipe" displayed on the console.	DE64699 DE64702
24.	The management Web server did not work due to a bug with the access SSL key on FIPS.	DE64730
25.	When a primary group of real servers was in the Overloaded state, the real servers in the backup group displayed as being in the Blocked state in the virt information.	DE64756
26.	The 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.	DE64782
27.	There was an incorrect BoardType for 7216NCX in the l2 system configuration.	DE64887
28.	When real servers were down, Alteon sent traps with the wrong OID.	DE64898
29.	In an SLB environment, when the primary server failed, the secondary backup displayed as UP instead of BLOCKED.	DE64919 DE64922
30.	On a 7220 platform, when Alteon received a packet greater than 1500, Alteon panicked.	DE64945
31.	AppWall was not pushed to a vADC in DPS Perform mode.	DE64995
32.	The weighted least connection was not correct.	DE65005
33.	When there was a state transition from backup to master, a GARP was not sent.	DE65038
34.	An SP memory leak was caused due to a combination of Bot Manager and the Mux.	DE65051 DE65054

Item	Description	Bug ID
35.	There was an incorrect rule_id for retrieving statistics from the SP.	DE65176
36.	On an Alteon VA, Fastview treatments stopped working.	DE65202
37.	Using APSolute Vision or WBM to access a device caused a memory leak and eventually led to a panic.	DE65236 DE65239
38.	In an SLB environment, a connection closure from the server side with an RST led to traffic failure on the new connection which matched the session that was is in fastage.	DE65282
39.	New SSH connections were ignored with a "max connection reached" error, even though there are no open connections.	DE65300
40.	The comparison function used to compare SSL policy names was incorrect.	DE65316
41.	Added more information to the debug log when ASSERT occurs on an ndebug image.	DE65343
42.	For SIP UDP traffic running with AppShape++ scripts (for persistency and Layer 7 manipulation), UDP sessions stopped working.	DE65434
43.	On 5208 ODS-VL and VL2 non-DPDK platforms, pings fail because the ARP reply was not transmitted back to the requester by the ND. This caused the config sync to fail.	DE65440

AppWall Bug Fixes

Item	Description	Bug ID
1.	An AppWall configuration file became corrupted after a system upgrade.	DE64176
2.	A RuleID was triggered with a request that does not contain a character.	DE64175
3.	A RuleID was triggered with a request that contains a specific Chinese character.	DE64517

Fixed in 32.6.4.0

General Bug Fixes

Item	Description	Bug ID
1.	Upon Submit, there was a Quick Service setup wizard internal error.	DE57034 DE57040

Item	Description	Bug ID
2.	On PSU failure, Alteon displayed a generic message instead of a more specific one.	DE59043
3.	In WBM, the equivalent to the filterpbkp CLI command was missing.	DE59730
4.	In DPDK VA environment with two NUMAs, packets are not tunnel processed when they are VMAed to SP of different NUMA.	DE60631
5.	When the SSH connection with the correct password was attempted for a locked user, the user lockout status was checked too late.	DE60712
6.	When sending an OCSP request over the management port, there were two leaks.	DE60852
7.	Using WBM, there was a display issue when modifying a virtual service with actionredirect.	DE61602
8.	There was no support for query type return errors even if the domain was found.	DE61644
9.	vADCs did not process SSL traffic.	DE61697
10.	When starting up a vADC startup, the admin context froze and the Watcher killed the process, resulting in a panic.	DE61771
11.	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.	DE61944
12.	Port mirroring increased the SP CPU utilization.	DE62271
13.	Failed to access the Alteon WBM and the SSH connectivity was lost.	DE62311
14.	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.	DE62395
15.	Even after changing the log level from debug to error, warning messages continued to be issued.	DE62438
16.	A ticket from a failed connection required passing over the authentication policy on the next connection.	DE62488
17.	With specific browsers, HTTP2 traffic with an uncommon form in the header was not answered.	DE62610

Item	Description	Bug ID
18.	Exporting a configuration from ADC-VX did not work.	DE62635
19.	Incorrect MTU syslog messages were issued for vADCs.	DE62662
20.	The packet capture timestamp was incorrect.	DE62732
21.	On an ADC-VX, the HW Watchdog rarely rebooted due to an unknown trigger.	DE62750
22.	While exporting techdata, IPv6 connectivity went down for a short while and then came back up.	DE62823
23.	When uploading a Layer 2 packet capture from an ADC-VX to the FTP server, Alteon panicked.	DE62849
24.	Using Ansible, could not configure the TLS 1_3 parameter.	DE62871
25.	There was vADC auto-reboot issue because of a software panic.	DE62946
26.	A config sync from a non-HA device to a an HA-configured device caused the loss of the HA configurations.	DE62953
27.	Health check tables were not supported for the l4 admin and slb admin users.	DE62972 DE62977
28.	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.	DE63059
29.	A non-supported configuration caused a crash.	DE63073
30.	There was an inconsistency in the current throughput per second statistics units of virtual servers.	DE63117
31.	In an RTS environment, after upgrading to version 32.6.2.0, RTS sessions were being aged out quickly, resulting in traffic failure.	DE63127
32.	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.	DE63194
33.	The /maint/geo/info command displayed an error message when the ISP GeoDB was not yet loaded onto Alteon.	DE63201 DE63205
34.	In Ansible, it was not possible to remove one VLAN from all interfaces because the value "0" was not accepted.	DE63218
35.	When multiple VIPs are configured with srcnet, the ptmout value was not being considered.	DE63483
36.	When VIRT6 went down, when deleting the IPv6 SLB virt, Alteon panicked.	DE63544

Item	Description	Bug ID
37.	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.	DE63558
38.	SSL statistics in the CLI and WBM did not match on Alteon running version 32.4.5.0.	DE63572
39.	Fetching the routing table via REST API when the routing table was full caused a panic.	DE63589
40.	When a real server had an rport set to 0 and an rport ser to x, the service became unavailable.	DE63620
41.	After SSL Offloading was enabled, Alteon stopped accepting connections.	DE63631
42.	LACP failed due to TX latency on the network driver.	DE63647
43.	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.	DE63689 DE63693
44.	After changing the admin password and Applying, there were configuration sync issues with the peer.	DE63760
45.	When using the /disk/ramdisk/disk/logs command for Alteon log files, GEL license activation failed.	DE63772
46.	Using CLI, after running the /stats/slb/virt command, backup real servers did not display.	DE63804
47.	After changing a group on an FQDN server, the servers were bound to the older group as well as the new group.	DE63830 DE63834
48.	After a signal panic, Alteon stopped booting.	DE63892
49.	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.	DE63909 DE64071
50.	On a 9800 platform with QAT, SPTHREADS caused a panic.	DE63918 DE63922
51.	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.	DE63984
52.	On the 4208 platform, the option to convert to virtual mode (ADC-VX) was mistakenly available.	DE64099
53.	After Alteon received a packet and tried to open a session entry,	DE64189

Item	Description	Bug ID
	an incorrect initialization of a pointer resulted in a NULL access and Alteon panicked.	
54.	Alteon VA did not initiate a BGP connection to a peer.	DE64237
55.	Peer Alteon devices panicked due to vulnerability to CVE-2021-3449.	DE64473

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

Fixed in 32.6.3.50

General Bug Fixes

Item	Description	Bug ID
1.	Snmpbulkwalk on the capacityUsageStats node returned invalid OID output.	DE62234 DE62235 DE62237
2.	In rare circumstances during tsdmp or techdata export, a panic would occur.	DE62554 DE62558
3.	In an HA environment, synching the configuration to the peer device with sync tunnel config flag disabled results in the peer panicking.	DE61967 DE61968 DE62016

Item	Description	Bug ID
4.	Using WBM, a packet capture caused a panic.	DE62283
5.	After upgrading to version 31.0.13.0, uneven load balancing started.	DE62466
6.	When the ND packet aggregation mechanism was active, a ping response was not sent immediately, resulting in a delay in the ICMP response.	DE62074 DE62075
7.	In a DSR and multi-rport configuration environment, the /stat/slb/virt X command returned statistics as 0.	DE62345 DE62349
8.	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.	DE61882 DE61883
9.	When while handling malicious DNS packet with compression pointer loops, Alteon panicked.	DE62125 DE62132
10.	There were no Mibs for the health check count to display them for the command /info/sys/capcityswitchCapHealthCheckMax EntswitchCapHealthCheckCurEnt.	DE61744
11.	Using WBM, when configuring the Nameserver group under DNS Authority, the table name in the mapping file was incorrect.	DE61486 DE61487
12.	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.	DE61270 DE61277
13.	There was no support for query type return errors even if the domain was found.	DE61255 DE61280
14.	Alteon closed the front-end and back-end SSL connection abruptly. Fixed the classification of second request if there is content class SSL.	DE61784 DE61785
15.	When the user sent traffic, a throughput high alert message was issued even though the throughput was less than the configured throughput threshold limit.	DE61982 DE61983
16.	Alteon did not forward traffic when LACP was disabled and worked as expected when LACP was enabled.	DE61525 DE61526
17.	When Alteon had high MP memory utilization, restarting caused configuration loss. Alteon came up with the default	DE61209

Item	Description	Bug ID
	configuration.	
18.	When resolving a DNS PTR record, IP matching was skipped (for both hostlk enabled and disabled) if the service hostname was not configured. Now, the service hostname check is skipped only if the hostlk is disabled.	DE60938
19.	When a syslog file had long log messages, the /info/sys/log command did not display any log messages.	DE60888 DE60889
20.	During configuration export, creating the AppWall configuration failed, and as a result the entire operation failed.	DE60952 DE60953
21.	The default STP group was not available for a newly added physical VM port.	DE61292 DE61299 DE61300
22.	The serial number was missing in the output for the /info/sys/general command.	DE61677 DE61678
23.	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.	DE61345 DE61346
24.	When the management WBM listener connection control block was closed during its validation, a 50X WBM error displayed.	DE60916 DE60956
25.	Following a set of SNMP operations, on some occasions Alteon panicked from a memory corruption with a boot reason power cycle.	DE61047
26.	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	DE61097 DE61098
27.	AppWall was stuck and did not process traffic but was not restarted by the MP.	DE61476 DE61477
28.	When the default gateway MAC was changed, Alteon sent return traffic to the incorrect or old MAC.	DE60786 DE60787
29.	Using WBM, a 50X error occurred due to buffer leak in an HTTPS request.	DE60798
30.	Alteon sometimes would crash when it received the same apply :filter deletion and network class deletion that was	DE61032

Item	Description	Bug ID
	assigned to the PIP that was defined for the real server.	DE61033
31.	When SSL hardware acceleration is active via a QAT card, the Acceleration Engine may go out of sync due to unknown conditions during **Config Apply**.	DE60363
32.	On a 4208 platform, the link was down for the 1 GB SFP port.	DE61722 DE61723

AppWall Bug Fixes

Item	Description	Bug ID
1.	Certain transactions were not properly processed leading to a network connection failure of AppWall version 7.6.8 integrated in Alteon version 32.6.1.0.	DE61267
2.	Under rare conditions, a configuration change in AppWall integrated in Alteon may have led to a failure.	DE60598
3.	Enabling base64 decoding in the Database security filter, may have led to an AppWall failure.	DE62625
4.	Saving security events was limited to the latest 200 events	DE60583

Fixed in 32.6.3.0

General Bug Fixes

Item	Description	Bug ID
1.	When resolving a DNS PTR record, IP matching was skipped (for both hostlk enabled and disabled) if the service hostname was not configured. **Fix**: The service hostname check now is skipped only if the hostlk is disabled.	DE60812 DE60813
2.	Malformed packets caused a panic on the AppWall monitor.	DE60643
3.	If Alteon received a request when all real servers were down, the group with all real server indexes less than 33, the RR, BW, or response metric failed to select a real server even if they came back up.	DE61146 DE61147 DE61148
4.	On an Alteon standalone integrated with AppWall, the AppWall syslog messages were not sent.	DE60564 DE60560
5.	A virtual service application-id configuration diff did not sync to an HA pair.	DE60454

Item	Description	Bug ID
6.	Using CLI, when using the /maint/debug/enhancedMP/health command, a panic would sometimes occur.	DE60353
7.	Additional logs were added for a 50X error when accessing a vADC.	DE60909
8.	The user lockout status was checked too late when an SSH connection with the correct password was attempted for a locked user.	DE60704
9.	AppWall was down and the MP did not kill it, resulting in AppWall staying down indefinitely.	DE60155 DE60159 DE60364 DE60368
10.	Starting with this version, the Certificate Group Duplicate button is removed because it is not usable for certificate groups.	DE60332
11.	Using Alteon VA, WBM displayed the port type as "Giga Ethernet Copper" irrespective of the actual port type used.	DE59938
12.	Using WBM, an 50X error occurred due to a leak in buffers on an HTTPS request.	DE60760 DE60767
13.	Periodic statistics logging was corrupting the configuration environment during Apply/Save, which resulted in a panic.	DE60309
14.	Some DNS requests were not answered or were delayed.	DE60086
15.	A deadlock due to non-async signal functions caused a reboot.	DE59878
16.	There were negative values in OIDs related to Total Octets in content rules statistics.	DE59838
17.	The /info/sys/capacity command did not display current virtual and real services.	DE60173
18.	When trying to free the session entry allocated for an AX-processed session, a panic occurred.	DE60183
19.	A vADC displayed all default user account passwords in a dump.	DE59872
20.	In an MSTP with trunk environment, Alteon failed to communicate with another device.	DE59897
21.	When a user was in lockout, the information message was not consistent, causing a security problem.	DE59808 DE59812
22.	After configuring an IPv6 address as a syslog host, the IPv6 VIP stopped working because the address was removed from the nbrcache entry.	DE59667

Item	Description	Bug ID
23.	DNS query responses were not handled for query types MX and CNAME.	DE60209
24.	Starting with this version, added the Expiry Time field for the cookie in the Services pane.	DE60051
25.	The source MAC for a generated SYN ACK was erroneously overwritten during the last IP forwarding process in the non-RTSRCMAC scenario for TCP DNS and dbind-ena virtual traffic.	DE59786
26.	The bandwidth metric sometimes did not work if all the WAN links in a group were configured with health checks.	DE59359
27.	SAN input for DNS without a period (".") was not allowed.	DE60097 DE60101
28.	The DNS query on a Backup device gave an incorrect response.	DE59545
29.	Using CLI over an SSH/Telnet connection, when the /c/slb/real x/shut command was executed without input, closing the connection led to a panic.	DE58602
30.	vADCs were in running state but were not able to be accessed via MGMT until they were disabled and then re-enabled.	DE59087
31.	On a 5208 XL platform, version 32.2.4.60, Alteon did not receive an information message when saving an image on ADC-VX slots completed.	DE59500
32.	The DHCP client ran without any validation.	DE58901
33.	The WAN link server displayed an overflow message for a clear issue for an edge condition.	DE59399
34.	Could not handle SSL traffic without SNI without the traffic being decrypted. **Fix**: Now you can attach an SSL policy with front-end and back-end SSL disabled.	DE58838 DE58841
35.	With Alteon configured with cookie and multiple rports for real servers, when sending traffic without a cookie, rport persistency was not maintained for the subsequent requests for the same TCP connection. The traffic was load balanced to the lowest rport.	DE59145 DE59152
36.	Maxcon support for 1 million was erroneously not implemented in the 30.5 series.	DE58164
37.	Configuring a data class with a special character propagated to AX failed due to a parsing error associated to the unsupported ASCII character, resulting in an out-of-sync configuration state.	DE59370

Item	Description	Bug ID
38.	Due to a network outage, Alteon panicked due to an IPv6 gateway failure.	DE59418
39.	An IPv4 filter session sometimes would be deleted before it aged out if the session memory was previously used by an IPv6 session.	DE60389
40.	There were two leaks when sending OCSP requests over the management port, which have been fixed.	DE60853

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall WebUI sometimes showed a 500 error.	DE59923
2.	AppWall integrated in Alteon sometimes returned an empty page to a client request.	DE59640
3.	Email notification (STMP) configuration for AppWall integrated in Alteon was wrong.	DE58413
4.	Occasional slowness in AppWall integrated in Alteon due to memory consumption.	DE58350
5.	An event- "Failed to update configuration according to awcfg.xml" sometimes appeared even when the configuration was correct.	DE60488

Fixed in 32.6.2.50

General Bug Fixes

Item	Description	Bug ID
1.	When trying to group SFP and non-SFP ports in LACP, the error message that was issued was not clear.	DE59745
2.	Using the CLI, when executing the /c/l3/ha/switch/pref command, if the SSH/Telnet connection terminated, a panic occurred.	DE59574 DE59575
3.	When more than nine (9) Ethernet ports were configured, incorrect information displayed when greping the port information.	DE59556 DE59563 DE59564
4.	Before RIP was assigned to an outgoing packet, the packet included the last four bytes of the IPv6 address, resulting in the leading zero in the address being blocked.	DE59491 DE59492

Item	Description	Bug ID
5.	As a fix, the FIPS domain name length was changed from 14 to 32 characters.	DE59705 DE59706
6.	After configuring an IPv6 address as a syslog host, the IPv6 VIP stopped working because the address was removed from the nbrcache entry.	DE59668
7.	The DNS IPv6 EDNS client subnet IP address was incorrect.	DE59585 DE59586
8.	When a real server went down, the virtual statistics summary display was incorrect.	DE59517 DE59518
9.	On an Alteon VA platform, the jumbo frames feature did not work because the DPDK layer for the VMXNET3 driver did not provide an API call to set the MTU value.	DE59291 DE59292
10.	On a 5424 platform with an unlimited SSL license, the info/sys/general command incorrectly displayed “S” and not “SL”.	DE59029 DE59621
11.	In a basic SLB environment, when trying to disable a real server operationally that started with the letter "p," Alteon did not correctly prompt the action.	DE58917 DE58918
12.	Even after setting the throughput threshold limit to "0," throughput alerts were issued.	DE58823 DE58824
13.	The total IP range limit value mentioned in the validation error for network classes was incorrect. It should have been 4294967294 instead of 4294967295.	DE59461 DE59462
14.	When TACACS with clog was enabled, during a techdata/tsdmp operation, unnecessary logs were issued to the syslog.	DE58764 DE58765
15.	The description for MIB altSwSpCpuPressureDeactivatedTrap was incorrect.	DE58773 DE58774
16.	When sending ICMP traffic to Alteon, the ICMP session was dumped to the syslog server as UDP.	DE59285 DE59287
17.	When sending client traffic to an IPv6 VIP with sharing enabled for the VR server, Alteon did not respond.	DE58984 DE58985
18.	After upgrading from version 30.5 to version 32.2, LinkProof NG static NAT did not perform reverse NAT.	DE58611 DE58612
19.	Alteon used a console with a 9600 baud rate, and the MP	DE58741

Item	Description	Bug ID
	issued information faster than the console could receive it.	DE58742
20.	When FTP was configured on a non-std data port and the port was same as the customized server data port, the data connection did not work.	DE58993 DE58994
21.	When REST API requests were received after a WBM idle timer timeout, the WBM idle timeout detection mechanism influenced related responses, causing a 401 error.	DE59590 DE59598
22.	When DSSP messages were received on the backup device, a software panic occurred.	DE58706 DE58707
23.	The Alteon device was not indicated as the next hop in a traceroute from the client machine to the ISP router.	DE58629 DE58630
24.	After upgrade, in a VRRP environment, Alteon failed to accept the configuration when the same nwclass was associated to more than one VIP and both were part of same VR group.	DE58384 DE58385
25.	Executing the /c/slb/gslb/dnsresvip/ command automatically created an index for a new entry. However, if no other subsequent changes were made to this entry, the diff command did not show the new entry.	DE58581 DE58582
26.	After upgrade, there was a false detection of session table corruption, resulting in an autorecovery.	DE59005 DE59006
27.	When configuring MSTP, a panic occurred because the internal value of the number of ports increased.	DE58409 DE58410
28.	SSL traffic without SNI could not be handled without decrypting the traffic. The fix is to allow attaching the SSL policy while front-end and back-end SSL are disabled.	DE58842
29.	While a session having proxy port was being freed, a panic occurred.	DE58195 DE59839
30.	When deleting an LSA from a neighbor’s retransmission list, a panic occurred for link-state ACK packets.	DE59114 DE59115
31.	In an SLB environment, when a filter was configured with reverse enabled for UDP traffic, traffic intermittently failed due to CPU spikes. Traffic never succeeded when the CPU went down.	DE58368 DE58369

Item	Description	Bug ID
32.	After deleting the FQDN server and applying and saving, then deleting the group and applying and saving, then adding a new FQDN server and a new group and applying, the error message "Application services engine is not synchronized with the current configuration" was issued. **Fix**: After removing the FQDN server, the real servers from AX are now also removed.	DE58107

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall failed to extract the upgrade image.	DE58085
2.	While accessing the Forensics logs, received a 500 error.	DE59301

Fixed in 32.6.2.0

General Bug Fixes

Item	Description	Bug ID
1.	In an HTTP Modification rule, when clicking the path option, the Path field was not visible.	DE58292
2.	In an ADC-VX environment, after executing the techdata, tsdump, or td-stats all commands, the MP CPU reached 100% utilization.	DE58252
3.	The Alteon NTP time jumped one month ahead.	DE58135
4.	When user configuring a scripted health check for port 25 (SMTP), during runtime the syslog was flooded with health check failure logs.	DE57869
5.	When a VRRP group was configured, sharing did not work properly.	DE57850
6.	In AppShape++ scripting, an early and unnecessary variable validation was removed from the validator function.	DE57766
7.	After upgrading from version 31.0.10.50 to 32.2.3.50, the GSLB DNS Summary Statistics displayed with a 0.	DE57679
8.	In Layer 2 mode when flooding to more than one port, fragmented packets (both in order and out-of-path) were lost.	DE57643
9.	In an ADC-VX environment, after enabling /cfg/slb/ssl/adv/bereuse, after a reset or reboot the value	DE57634

Item	Description	Bug ID
	changed back to disabled.	
10.	When an unchained buffer was treated as a chained buffer in non-DPDK platforms, a one-time crash occurred. A check was added to packet captures to prevent this.	DE57569
11.	Due to an incorrect version comparison, TLS 1.1 displayed as disabled by default.	DE57559 DE57563
12.	The length of the hostname in the HTTP healthcheck field was increased to 128 characters as required.	DE57546 DE57550
13.	There was a high load on the queues from Alteon to AppWall, a session entered into the pending list twice, and activated after termination. This caused a panic.	DE57539
14.	When PIP mode was configured as address and HA mode as switch, if the same PIP range was associated to more than one service or real server, the PIP ARP limit was reached.	DE57519
15.	Alteon incorrectly validated unsupported path attributes (currently the BGP community path attribute).	DE57514
16.	Using WBM, the percent character (%) in the passphrase for private keys did not work.	DE57490
17.	Using WBM, could not renew existing certificates because of internal indexing issues.	DE57472
18.	When a DPDK initialization failed on any error except a queue error, it reverted to tuntap.	DE57373
19.	On a 9800 platform, after saving a configuration the following error displayed: mgmt: Flash Write Error	DE57351
20.	Using WBM, removing a target address from the SNMV3 did not remove the address from the AppWall UI server list.	DE57312
21.	When the SNMP OID hwApplicationSwitchNameInfo was probed, the port state incorrectly changed to disabled by referring to the wrong port flag state. This led the gateway health check to fail.	DE57306
22.	When the MP froze, the Watcher did not also kill the AW process of this MP.	DE57291 DE57295
23.	When the real server rindex fell in a different word index group (rindex value /32), SLB traffic ignored the real server's weight for the roundrobin group metric.	DE57271
24.	After rebooting a master and it comes up with an RSTP	DE57253

Item	Description	Bug ID
	setup, an ARP packet was sent and received over the backup's block port.	
25.	The interface IP address and floating IP address were swapped and applied. The IF IP address was added to the IP6 Neighbor Cache table as the new IF IP address, but was deleted as the old floating IP address.	DE57222 DE57226
26.	After rebooting a vADC, the GSLB/LinkProof licenses were disabled.	DE57180
27.	After performing a recovery, the session capacity value was incorrect.	DE57149
28.	As per RFC 3416, the SNMP Get Next values should be in lexicographical format, but Alteon did not follow this for the FDB table and other tables. A fix was made only for the FDB table.	DE57062
29.	On a FIPS card, a session terminated while it was still pending for a task.	DE57053 DE57057
30.	After a period of no traffic, the race condition timing could lead to an AppWall restart.	DE56993
31.	OSPF was not able to send a link state update (redistributed route) to peed when the gateway went down.	DE56963
32.	In an SLB environment with HA and session mirroring enabled, real server current session statistics and redirect statistics displayed incorrectly in the /i/slb/virt x summary on the backup device. This resulted in traffic failure when the backup became the active.	DE56948
33.	A configuration with many real servers caused a delay in context switching, resulting in LACP messages not being handled.	DE56935
34.	Using WBM, when trying to modify the throughput limit, an error occurred. Added a REGEX to support all the throughput licenses.	DE56919 DE56923
35.	After version upgrade, GEL licenses were rejected.	DE56885 DE56889 DE56897
36.	In an HA environment with vADCs, when trying to send more OSPF routes to the peer device, a panic occurred.	DE56838
37.	An incorrect FIPS license string (deprecated) caused a flow of	DE56810

Item	Description	Bug ID
	FIPS tests.	DE56814
38.	When a service was configured in a non-existing VIRT, it remained unnoticed until the VIRT was defined.	DE56796
39.	When mgmt was disabled and the syslog defined on mgmt, the new syslogs did not display in /info/sys/log.	DE56731 DE56735
40.	There was a RADIUS Authentication failure because secret was not configured. No warning was issued for this.	DE56724
41.	After inserting a 1G SX Multimode transceiver, the following error displayed: “Cannot work with 1G transceivers.”	DE56711 DE56715
42.	Alteon DPDK platforms dropped out-of-order fragmented packets.	DE56702
43.	The vconsole internally used Terminal MultiPlexer (TMUX), which is not available on DPDK-based platforms.	DE56694
44.	The vconsole internally used Terminal MultiPlexer (TMUX), which is not available on DPDK-based platforms.	DE56689
45.	When trying to upload tech data when the management network was slow, an SCP timeout error occurred.	DE56657
46.	After applying the /info/sys/general command, the output was incorrectly 7612 S instead of 7612 SL.	DE56606 DE56610
47.	While deleting an IPv6 configuration, a panic occurred. Added defensive validations.	DE56595 DE56599
48.	Using WBM, the Monitoring > System > Capacity > Application Delivery page did not display capacity information.	DE56483
49.	Using the CLI, after configuring a local add as a nwclass ID, after reboot, the configuration was not applied.	DE56338
50.	Using WBM, the configured Server Certificate group in a configuration did not display.	DE56293
51.	Configuring the data class IP address with mask 0 caused a panic. Because mask 0 is invalid, the fix was to ignore it.	DE56283
52.	When IPv6 TCP small packets were received by the MP out of order via the data port, the memory associated with the packets was not returned (after the usage) to the pool of free small packets, causing problems for features allocating such packets.	DE56078
53.	On an ADC-VX, an NTP timeout occurred.	DE55854

Item	Description	Bug ID
		DE55858 DE55859 DE55863

AppWall Bug Fixes

Item	Description	Bug ID
1.	Integrated WAF: Websec module down/up events are shown in the device system logs.	DE57855
2.	Error API call when trying to change a tunnel operational status using AppWall API.	DE57217
3.	AppWall API - Get specific security event resulted in error.	DE57216
4.	Doc bug in AppWall API documentation	DE57200
5.	Integrated WAF: Incorrect information under syslog’s DIP field.	DE56918
6.	Alteon is not sending syslog messages for integrated AppWall.	DE56861
7.	WAF XML file breaks Event detains into multiple queries.	DE56386

Fixed in 32.6.1.0

General Bug Fixes

Item	Description	Bug ID
1.	If there was no default Gateway defined or the Gateway failed, after a security scan there was total service outage.	DE56258
2.	When a burst of packets were sent to the MP for ARP resolution, subsequent packets were dropped when ARP resolution was already in progress for the first packet of a given destination, or when there was an RST from the client followed by a retransmission of a GET request, a connection drop occurred.	DE56156
3.	In an IPv6 environment, when the protocol is set to both for a virtual service, the lookup failed for the virtual service and the client traffic was dropped.	DE56139
4.	In an IPv6 environment, a specific virtual service could not be DNS-resolved by GSLB.	DE56000
5.	In an IPv6 environment, a specific virtual service could not be DNS-resolved by GSLB.	DE55995

Item	Description	Bug ID
6.	The HTTP modification rule for a host match did not accept a dot (.) in the match term.	DE55936
7.	The translation to Chinese for the value slbNewCfgEnhVirtServApplicationType.13 was incorrectly translated as "basic slbit"; it should have been "SMTP."	DE55931
8.	Stuck sessions in AX caused another of issues, resulting in a panic.	DE55835
9.	Alteon lost communication with the LLS and entered the grace period.	DE55780
10.	Using WBM, the dot (.) character was not supported in an SSL policy name.	DE55722
11.	After an upgrade to version 31.0.12.0, a panic occurred because of null pointer access.	DE55712
12.	When processing some network elements having consecutive IP addresses as an exclude set, the network class configuration error " total IP range cannot be greater than 4294967295l" was issued.	DE55671
13.	When CDP was configured with a domain name, after the DNS resolution the request was framed using the resolved IP address in the HOST header field instead of the domain name.	DE55656
14.	On an Alteon 5412XL platform, the same cookie load-balanced to multiple real servers.	DE55601
15.	In an AppWall integrated in Alteon environment, a new secwa did not display in the AppWall Console.	DE55474
16.	The configuration migration tool duplicated the GSLB network for Inbound LLB rules.	DE55704
17.	The export capture status was stuck at “upload in progress”.	DE55388
18.	Live packet capture was not working.	DE55284
19.	After connecting to the GEL server, the console was flooded with junk logs every 18 seconds.	DE54940
20.	When HAID 2 was configured, /info/slb/virt display the wrong virtual MAC address.	DE54761
21.	Layer 7 SNI-based LLB did not work with BWM enabled in Enforcement mode.	DE54458

AppWall Bug Fixes

Item	Description	Bug ID
1.	Source Threshold is not enforced by Activity Tracking's Anti-DDoS in certain cases in 7.6.7.0.	DE56123
2.	Parameter Security filter might fail to load certain Regular Expressions correctly.	DE56110
3.	Rare case where additional changes to AppWall configuration was not synced to the backup.	DE56051
4.	Some Security Events have the wrong Security Event Description.	DE55887
5.	Rare case under heavy traffic causing a parsing mistake that can lead to traffic being blocked.	DE54949
6.	Requests with very large number of parameters may take long to process.	DE54905
7.	Manual SUS update page is not accessible when there is no Internet connection.	DE54670
8.	Special characters cannot be used in paths in AllowList refinements.	DE54755
9.	API documentation for adding a web server into a web farm was not correct.	DE54741
10.	Option to download AppWall forensic events as a CSV file is missing.	DE54924

Fixed in 32.6.0.60

General Bug Fixes

Item	Description	Bug ID
1.	During ADC-VX upgrade to version 32.4.1.50, the following error message displayed: `""  <<<<<<<<<<<<< Do you wish to run the analysis ? y or n   >>>>>>>>>>>>""` If you choose no, there will be no new entry in file	DE54468
2.	After upgrading to 32.2.4.0 there was a continuous vADC panic.	DE55676
3.	A DNS request accessed the cache unexpected.	DE55412
4.	The packet capture tool did not capture all of the packet sent from SP to MP, resulting in an expected health check.	DE54441

Item	Description	Bug ID
5.	On a FIPS-II 6024 platform, there was a memory leak.	DE55611
6.	There was a health check issue with a buddy real server.	DE55484
7.	With GEL active license revalidation, there was an MP freeze issue.	DE55439
8.	A type discrepancy in the URLF subcategory printing caused Alteon to reboot.	DE55364
9.	There was no support for non-interactive mode for the "/c/slb/sync/auth passphrase xxxxxx" command, causing a missing configuration sync authentication toggle.	DE55341
10.	Could not apply the TACACS configuration during a timeout cycle.	DE55318
11.	A type discrepancy in the URLF subcategory printing caused Alteon to reboot.	DE55268
12.	Using AppWall integrated with Alteon, all Web applications stopped.	DE55242
13.	Routes through GRE/IPinIP tunnels did not display after running the /i/sys/capacity command.	DE55219
14.	Site resources were not cached by FastView	DE55136
15.	After connecting to the GEL server, the Alteon console was flooded with some junk logs every 18 seconds.	DE54948
16.	Using WBM, you could not create a service using TCP 995.	DE54882
17.	Allow filters failed to decrypt IPv6 traffic.	DE54828
18.	The error message "Someone else is doing the diff [flash] try again!" was issued.	DE54818
19.	When HAID 2 was configured, /info/slb/virt displayed the wrong Virtual MAC ID.	DE54762
20.	After upgrading, Alteon was not able to push the intermediate certificate and failed to apply the configuration.	DE54737
21.	After the SRIOV port was brought UP, the IPv6 gateway did not come up.	DE547218
22.	After Revert Apply, the gateway flapped in Alteon running version 31.0.9.0.	DE54688
23.	Config sync was unsuccessful. The Application Services Engine was not synchronized with the current configuration.	DE54679

Item	Description	Bug ID
24.	The WBM menu was disabled, but you could use CLI to modify settings.	DE54665
25.	Performing proxy processing on an OSPFv6 packet caused a panic and reboot.	DE54651
26.	During a new image upload, if the available disk space was low on a device, an error message was only issued after 94% of the download completed. Now a warning message about low disk space is issued before the download starts.	DE54640
27.	A BGP peer established a connection and changed back to the Connect state.	DE54628
28.	Could not upgrade from Alteon VA version 32.2.0.0 to version 32.2.3.0.	DE54613
29.	When GW 1 was deleted, DNS health checks were not generated but ICMP health checks were generated.	DE54591
30.	APSolute Vision sent an incorrect REST query to Alteon.	DE54494
31.	There was error while applying a configuring for a network class.	DE54478
32.	There was an Alteon SSL inspection and IWSVA Integration Issue.	DE54476
33.	When the TACACS server was configured with command logging, Alteon failed to identify the global commands cdump, telnet, traceroute as global commands. Instead, it tried to process from the local menu where it does not exist, resulting in a panic.	DE54432
34.	Using WBM, downloaded techdata and core dumps were corrupt.	DE54423
35.	The SNMP overload health check mechanism stopped working when it was added to the logExp health check.	DE54414
36.	The fragmented CPU size was increased from 16K to 64K.	DE54405
37.	Using the WBM, a VLAN name of 32 characters was allowed, while in the CLI, only 31 characters was allowed.	DE54394
38.	In the Real Server configuration pane, the HA master displayed FQDN instances.	DE54396
39.	The values of the "Event Class ID" and "Severity" events were incorrectly exchanged in Layer 4 (open + closure) events.	DE54551

Item	Description	Bug ID
40.	When adding a gateway to AllowListRefinements, received an HTTP 409 code.	DE55511
41.	There was a bug in the Advisory Tool upgrade.	DE54370

AppWall Bug Fixes

Item	Description	Bug ID
1.	The communication properties option in the wizard was not relevant. It has been removed.	DE51197
2.	In WBM, VLAN sometimes would not function properly if the VLAN was configured using the Java applet in a previous version, and AppWall was upgraded to newer version.	DE54671
3.	The AllowList REST API call was changed incorrectly after upgrade from version 7.5.8 to version 7.6.6. The REST API call is now fixed.	DE54742
4.	The exported Forensics events was not in the correct XML format.	DE55291

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
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.	The Alteon NG+ license did not apply the 5 vADC license.	prod00276637

Item	Description	Bug ID
10.	On DPDK platforms, Interface errors for port statistics were issued.	prod00278282
11.	Using WBM, when "Return to Last Hop" was set for a virtual server, an additional field type was also set internally.	prod00276932
12.	Using WBM, could not the configure sync passphrase.	prod00274326
13.	Alteon was rebooted unexpectedly by watchdog.	prod00273480
14.	After upgrading from version 31.0.7.0 to version 31.0.10.0, vADC 1 panicked.	prod00274805
15.	Using LinkProof NG, when uploading or downloading WAN link limits are configured above 455 Mbps, WAN link bandwidth utilization displayed incorrect statistics.	prod00273018
16.	Alteon rebooted with a power cycle.	prod00272623
17.	Using WBM, a notify view iso could not be configured without creating a custom notify tag.	prod00273727
18.	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
19.	During SNMP polling, a panic occurred.	prod00277994
20.	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
21.	Using WBM on a vADC, could not renew an SSL certificate.	prod00276404
22.	The Intermediate CA certificate could not be imported due to unexpected max limit.	prod00278076
23.	After upgrading to version 32.2.1.0, MP CPU utilization spiked.	prod00273887
24.	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
25.	In an AppWall for Alteon environment with ADC-VX, changing the password for the local admin for a vADC led to a password	prod00275570

Item	Description	Bug ID
	mismatch.	
26.	Using vADC, generating a new Web Management Certificate caused a panic.	prod00278262
27.	In a GSLB environment, Alteon became stuck with high MP CPU utilization.	prod00276521
28.	A confusing configuration resulted while implementing LDAP(S) health check.	prod00275746
29.	After deploying a TCP optimization policy, the software panicked.	prod00277925
30.	Using WBM, the maximum session number did not change after adding a CU. It only changed using the CLI.	prod00274759
31.	The GSLB DNS client network rules real server selection pane was too small.	prod00272845
32.	Alteon HA did not behave as expected.	prod00274959
33.	When enabling the HTTP/2 policy, a panic occurred.	prod00273689
34.	When running the /stat/slb/clear command, only some of the filter statistics were cleared and the other statistics remained.	prod00272890
35.	Added GSLB site IP address validation.	prod00277096
36.	Connections to a VIP closed abruptly.	prod00276585
37.	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
38.	SIP INVITE and fragmented packets are not forwarded to real servers.	prod00273233
39.	After a panic, the Admin context went into a reboot loop.	prod00276328
40.	After upgrading to version 32.2.1.0, session logs were not generated.	prod00272747
41.	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
42.	Enabling and disabling HTTP/2 caused service impact.	prod00275412
43.	An explicit proxy caused unexpected behavior for HTTP/HTTPS traffic.	prod00278448
44.	When idbynum was enabled, there were issues with Revert	prod00273942

Item	Description	Bug ID
	Apply.	
45.	When importing a configuration with BGP, Alteon issued Notice messages with non-ASCII characters.	prod00275648
46.	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
47.	When the DNS virtual service protocol was UDP stateless, the HTTP and FTP services failed for IPv6 traffic.	prod00273830
48.	There were many FLOOD entries being created in the FDB table for the PIP MAC. This caused some of the traffic to fail.	prod00277247
49.	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
50.	Using WBM, you could not edit the IP address for a new Outbound LLB Rule.	prod00277384
51.	On a vADC, incorrect Throughput Alert messages were issued.	prod00275923
52.	When the Alteon HA state changed from Master to Backup, the gateway and real server's health checks failed.	prod00278209
53.	In a GSLB with VRRP/HA environment, after applying a configuration, the DSSP health checks failed.	prod00273187
54.	In an SLB environment with a pbind client IP address, persistence was not maintained.	prod00276271
55.	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
56.	After resetting the admin password from the console, the new password was seen in clear text in diff flash.	prod00274143
57.	In an Azure environment, Alteon VA crashed.	prod00276480
58.	Using WBM, could not configure BGP 4-byte-ASN.	prod00276809
59.	When the primary WAN link went down and the backup WAN link took over, an incorrect syslog message displayed.	prod00276690
60.	When logged in as a TACACS or RADIUS user, could not modify or create SNMPv3 authentication or privacy passwords.	prod00277002
61.	In a GEL environment, the Alteon VA prompt license server was	prod00274364

Item	Description	Bug ID
	constantly reestablished.	
62.	Alteon was affected by CVE 2019-11477, CVE 2019-11478, and CVE 2019-11479. This is now fixed.	prod00273355
63.	Alteon Indirectly caused a vulnerability to a DNS cache poisoning attack.	prod00274788
64.	When sending syslog messages, a panic occurred.	prod00272886
65.	After the device reset, it failed to connect the Alteon VA management IPv6 address.	prod00275197
66.	A vADC could not handle any data traffic that included a health check. The vADC do not restart after an SP panic/freeze.	prod00274322
67.	Using WBM, during configuration sync, continuous fetching of the virtual server table caused a panic.	prod00277466
68.	The backup group status in a content rule displayed an incorrect status when the backup group was not directly associated to any service.	prod00276757
69.	While STG information was sent from an ADC-VX to a vADC, a panic occurred.	prod00278079
70.	Config sync or disabling virt synchronization removed virtual servers from the backup device.	prod00273198
71.	When AES was used for privacy and/or encryption, the initialization vector was not set properly, causing AES encryption failure.	prod00276314
72.	A configuration change to the shutdown definition was not displayed correctly using the /cfg/slb/group x/cur command.	prod00272735
73.	NTP requests were not sent in an OSPF network.	prod00274317
74.	On the APSolute Vision Analytics Dashboard, there was an Alteon SP CPU display issue.	prod00274472
75.	When changing to the default configuration, the runtime session capacity was not reflected.	prod00276873
76.	During an upgrade to version 32.2.30 or later, the configuration became stuck in diff.	prod00276741
77.	On an ADC-VX, the device banner and /boot/cur show different active Alteon versions.	prod00276978
78.	Using WBM, there was an HTTP modification rule configuration issue.	prod00273399

Item	Description	Bug ID
79.	The Alteon 6024 platform rebooted due to a panic.	prod00274800
80.	When processing the second fragment destined for the Alteon interface when the redirect filter was configured, Alteon panicked.	prod00277545
81.	There was a disparity of the MAC address between the primary and backup devices.	prod00275355
82.	On an Alteon VA, Alteon reset the connection when traffic failed over.	prod00277406
83.	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
84.	SSL traffic caused a panic.	prod00278066
85.	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
86.	Throughput Threshold alerts displayed despite the threshold level being set 0 (disabled).	prod00276301
87.	Using Passive FTP, an RTS session was created instead of a filter session for FTP data traffic.	prod00272720
88.	During bootup time while loading the configurations from flash, the Apply failed.	prod00274184
89.	ICAP responses were not forwarded to the client.	prod00276505
90.	The priorities for remote real servers among different GSLB network did not behave as expected. 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.	prod00276835
91.	BGP 4 Byte ASN was not compatible with Cisco Nexus 9K and Huawei routers.	prod00276710
92.	In an IPv6 SLB environment with an IPv6 HTTP health check and IPv6 HA configured, the memory allocated for HTTP HC was	prod00276967

Item	Description	Bug ID
	not freed, which led to a memory leak.	
93.	SNMP data in the polling interface details incorrectly represented the interface type.	prod00273384
94.	During an internal cleanup operation, a vADC panicked and restarted.	prod00274791
95.	Trend Micro's IWSVA (AV) in ICAP mode (with Alteon acting as ICAP client) was only partially working.	prod00277016
96.	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
97.	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
98.	An HTTP header modification value set to None was considered as valid input.	prod00277184
99.	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
100.	When changing from ena to dis and vice versa, could not apply the /cfg/l3/ha/switch/filtpbkp command.	prod00277754
101.	After reverting an unsaved configuration, the HA state remained INIT and was not updated automatically.	prod00272982
102.	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
103.	During stress traffic, a panic occurred.	prod00278082
104.	When viphlth was enabled, there was no response to ICMP health checks to VIP IP addresses.	prod00274665
105.	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
106.	When a device came up after reboot, the HA status displayed as	prod00278452

Item	Description	Bug ID
	NONE because the HA state was recorded based on the current HA service group state for which the apply was in process.	
107.	After upgrading to version 31.0.11 0 SSL offload did not work properly.	prod00276275
108.	After upgrading to version 31.0.11.0, SSL offload did not work properly.	prod00275661
109.	In a GSLB environment, Alteon did not resolve a DNS query even though the remote real servers were UP.	prod00272895
110.	After applying configuration changes, a VIP stopped responding.	prod00272783
111.	After running a scan over SSH, the device panicked.	prod00274827
112.	A packet capture's TCP stream displayed corrupted data.	prod00273699
113.	On an Alteon 5424 platform with 24G RAM and software version 32.4.1.10, the maximum sessions remained as 11M even though the sesscap value was 100%.	prod00277364
114.	IPv6 SNMP queries over the data port were not working because checking for management access with the ingress data port failed.	prod00277308
115.	In a DSR environment, there was a discrepancy between /info/swkey and virtual server statistics.	prod00277933
116.	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
117.	Traffic was forwarded to a failed WAN real server.	prod00276353
118.	When the management port was disabled, syslog messages were not sent on the data port.	prod00278038
119.	Using APSolute Vision, importing a certificate Alteon did not work with the ADC + Certificate Administrator role.	prod00274710
120.	Could not log in to AppWall.	prod00275566
121.	After upgrading to version 32.2.3.0, the device constantly rebooted due to a panic.	prod00278288
122.	An invalid hypervisor type was set for virtual platforms.	prod00276259
123.	HTTP health check edit page via BBI does not show configured settings and values	prod00275723
124.	With two vADCs hosted on the same ADC-VX, all applications stopped working.	prod00277922

Item	Description	Bug ID
125.	Using WBM, generating a certificate resulted in an invalid EC key size (6). error.	prod00272976
126.	Using QAS, after a Submit the rport of the service was overwritten.	prod00272878
127.	Using switch HA, an unexpected failback sometimes occurred.	prod00274832
128.	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
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

Item	Description	Bug ID
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 were 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
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*

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