AlteonOS

RELEASE NOTES

Version 32.4.17.0
January 3, 2024

TABLE OF CONTENTS

CONTENT

Radware announces the release of AlteonOS version 32.4.17.0. These release notes describe new and changed features introduced in this version on top of version 32.4.17.0.

RELEASE SUMMARY

Release Date: January 3, 2023

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
- 5208, 5208 Extreme, 5208S
- 5424S, 5424SL, 5820S, 5820SL
- 6024, 6024 Extreme, 6024S, 6024SL, 6024 FIPS II
- 6420, 6420 Extreme, 6420S, 6420SL
- 6420p, 6420p Extreme
- 7612S, 7612SL
- 7220S, 7220SL
- 8420, 8420 Extreme, 8420S, 8420SL
- 8820, 8820 Extreme, 8820S, 8820SL
- 9800, 9800S, 9800SL
- Alteon VA running on VMware ESXi 6.0, 6.5, 6.7, 7.0, 8.0, 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 32.4.17.0 is supported by APSolute Vision version 4.40 and later, and Cyber Controller 10.0 and later.

Integrated AppWall version: 7.6.22.0

OpenSSL version:

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

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 32.4.17.0:

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 32.4.17.0 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 (for example, 31.0) only support vADCs that run the same version or later.

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 32.4.17.0

Link Layer Discovery Protocol (LLDP)

Starting with this version, the Link Layer Discovery Protocol (LLDP) is also available on the management ports.

NFR ID: 221024-000119

SNMP OID to Monitor Peak Session

The following SNMP OIDs were added for peak session monitoring:

- Peak number of session entries:
  - switchCapPeakSession - 1.3.6.1.4.1.1872.2.5.1.3.9.3.92
- Peak session entries in percentage:
  - switchCapPeakSessionPercentage - 1.3.6.1.4.1.1872.2.5.1.3.9.3.93

NFR ID: 230425-000158

Immediate Backend Bind

When Alteon processes HTTP/S traffic using filters (**Application** set to **HTTP**), the back-end TCP connection is only opened after the first HTTP request is received on the client side. A new flag allows opening the back-end TCP connection as soon as the TCP handshake on the client side is completed and before the first HTTP request arrives.

Enabling immediate bind requires the following conditions:

- A filter set is configured
- All filters in the filter set have **Action** set to **Allow** and **Application** set to **HTTP**.

To enable immediate bind:

- CLI – `/c/slb/filt/adv/frcebind ena`
- WBM – **Application Delivery > Filters > Add/Edit Filter > *HTTP* tab > Force Immediate Backend Bind**

NFR ID: 230822-000111

WHAT'S NEW IN 32.4.16.0

None

WHAT'S NEW IN 32.4.15.0

Integrated AppWall

GraphQL Protocol Support - BETA

We are excited to announce the support for **GraphQL protocol parsing**. GraphQL has gained significant popularity and adoption among clients due to its numerous benefits and advantages over traditional REST APIs.

GraphQL offers a **more efficient and flexible approach** to data fetching, allowing clients to request precisely the data they need in a single request. With its declarative nature, clients can specify the exact structure and shape of the response, reducing over-fetching and minimizing network overhead.

Furthermore, GraphQL enables clients to aggregate data from multiple sources into a unified response, **eliminating the need for multiple round trips to different endpoints**. This reduces latency and improves overall performance, providing a smoother user experience.

By adding GraphQL support to our product, we empower our clients to leverage these advantages and harness the full potential of GraphQL in their applications. With its growing popularity and developer community, GraphQL has become a **preferred choice for modern API development.**

In this release, we not only introduce GraphQL support but also reinforce our commitment to security. **Our enhanced protection for the positive security model ensures that customer GraphQL APIs are guarded against common security vulnerabilities, providing a secure and reliable foundation for applications.**

WHAT’S NEW IN 32.4.14.0

None

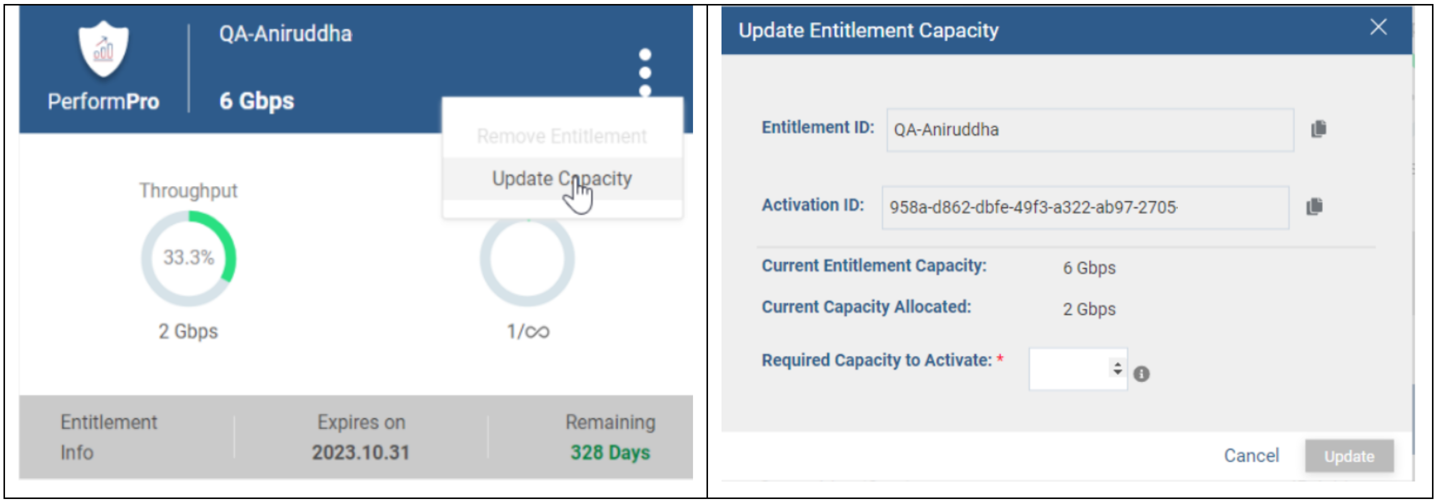
WHAT’S NEW IN 32.4.13.0

GEL Dashboard Enhancements

The following *GEL Dashboard* enhancements are available starting with Cyber Controller version 10.0.0.0, for all supported Alteon versions:

- The Activation ID of the entitlement will only be required when initially activating the entitlement. The Activation ID will no longer be required when removing an entitlement or as part of updating the entitlement capacity (Split use case).
- Entitlement capacity update (for Split use-cases only) is now available in the *Entitlement* card, providing a clearer indication of the current capacity activation and capacity allocation of the entitlement.

  The *GEL Dashboard* also prevents decreasing the activated capacity below the allocated capacity.



Entitlement ID: QA-Aniruddha

Activation ID: 958a-d862-dbfe-49f3-a322-ab97-2705

Current Entitlement Capacity: 6 Gbps

Current Capacity Allocated: 2 Gbps

Required Capacity to Activate: *

Ansible for Content Rules

New Ansible modules were added for:

- Content Class configuration. Supports configuring entries of type Host, Path, File Name, File Type, Header, and Cookie
- Virtual service Content Rules configuration

Security Message for Unsecure Management Protocols

A security warning message displays when enabling the following unsecure management communication protocols using CLI or WBM:

- SNMP v1/v2
- SSH V1+V2
- TLS1.0
- TLS 1.1

NFR ID: 220415-000006

PIP Source Port Utilization Warning

Alteon can now send an alert when the PIP table utilization has passed the specified threshold with a 5-minute alert frequency.

- Using CLI: `/cfg/slb/adv/pipthr`
- Using WBM:**<virtual service> setting > session management > PIP Table Alert Threshold**

The feature is disabled by default.

Alert example:

```
2022-12-01T14:15:37-08:00 ALERT   slb: PIP Allocation reached 93%
threshold on ingress port 17 for traffic pattern SIP:
60.60.10.162:36244 RIP: 172.198.50.12:80 PIP: 10.10.10.100:tcp VIP:
172.198.50.101 (aux table 110). Increase the PIP address range for
better PIP port distribution.
```

NFR ID: 211102-000066

WHAT'S NEW IN 32.4.12.0

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 32.4.11.0

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

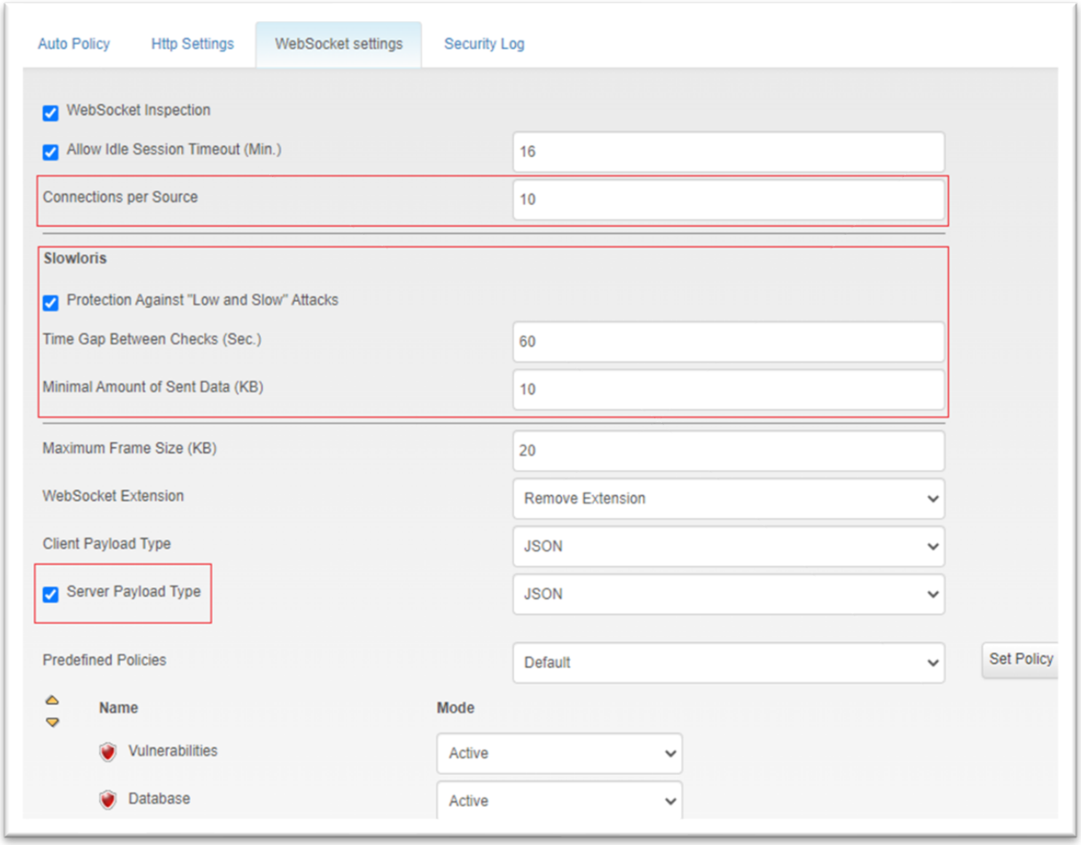
WebSocket

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.) 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

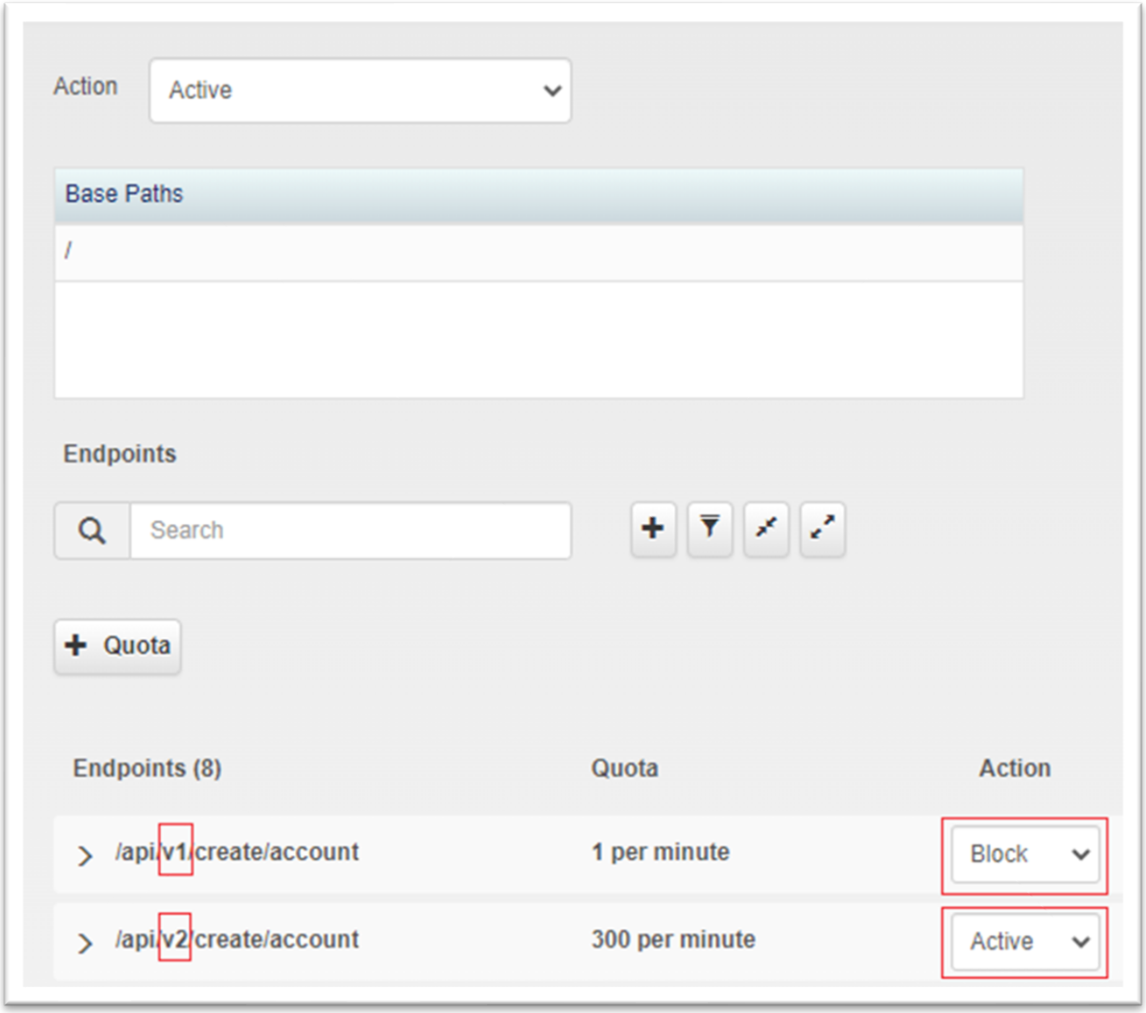
Name	Mode
Vulnerabilities	Active
Database	Active

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 32.4.10.0

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

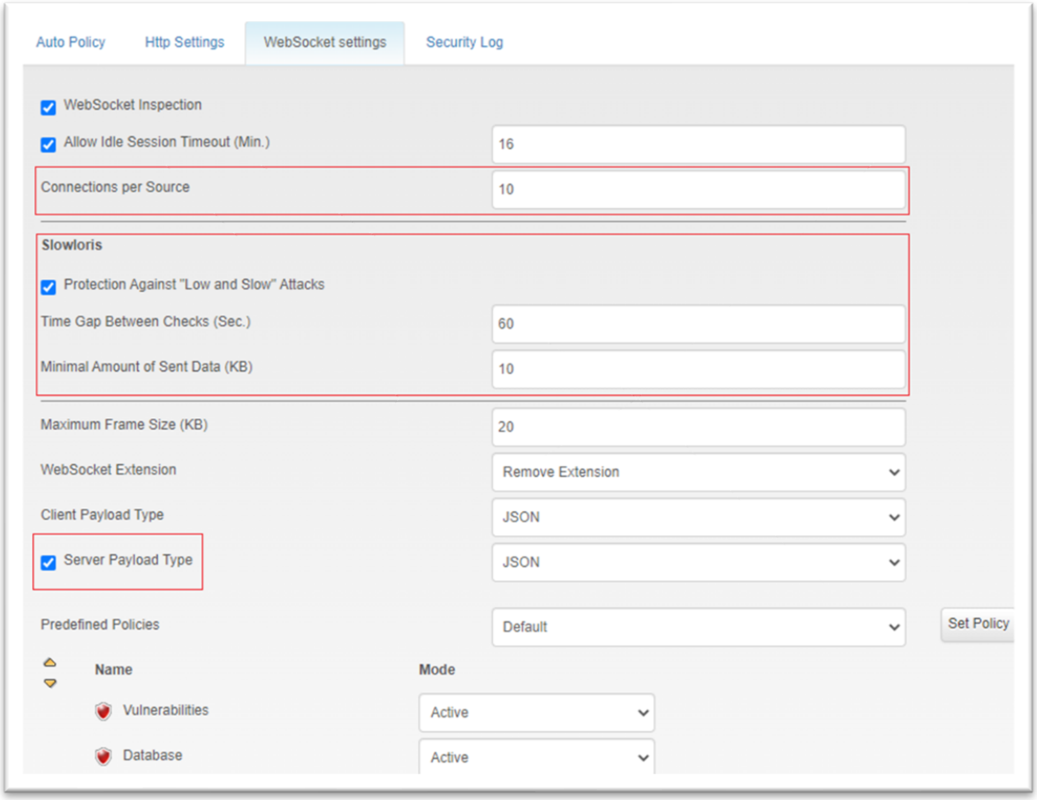
WebSocket

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

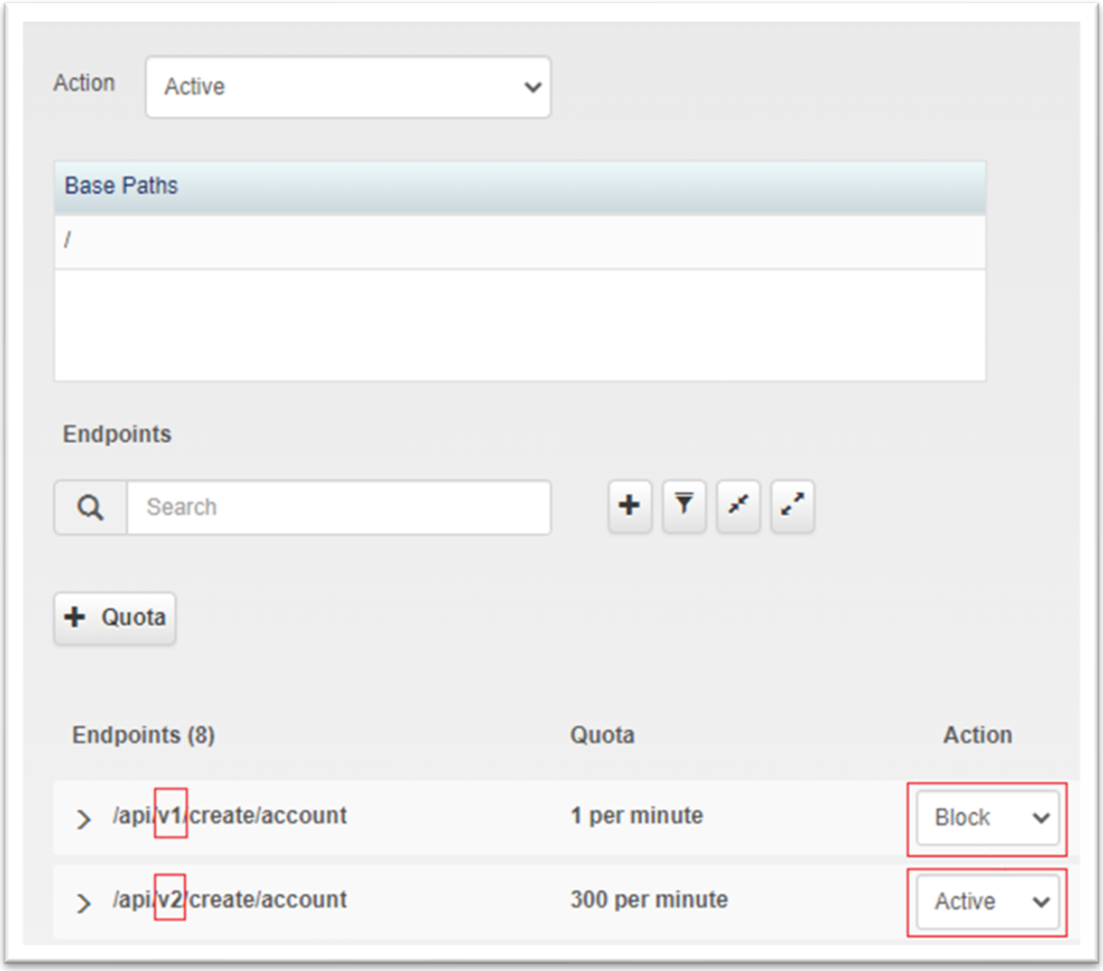
Name	Mode
Vulnerabilities	Active
Database	Active

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 32.4.9.0

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

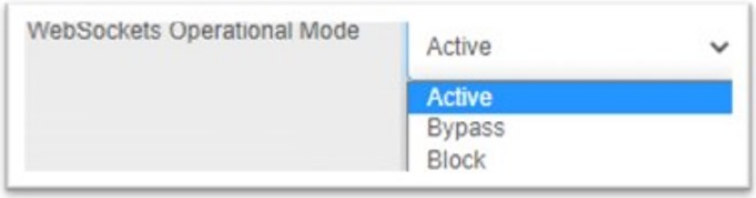
In this version, WebSocket protocol support is added.

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.

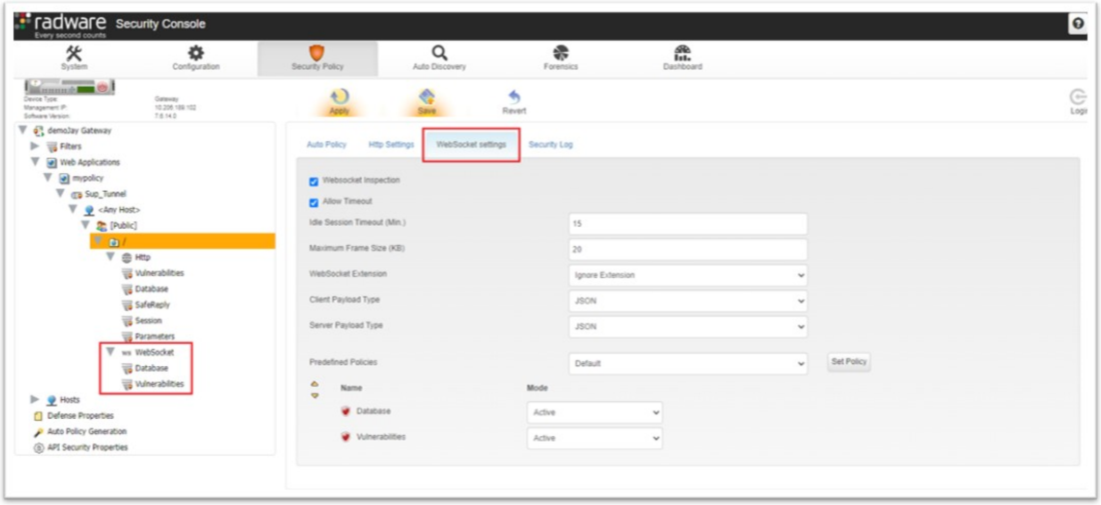
AppWall WebSocket support:

- 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



☑ Websocket Inspection

☑ Allow Timeout

Idle Session Timeout (Min.): 15

Maximum Frame Size (KB): 20

WebSocket Extension: Ignore Extension

Client Payload Type: JSON

Server Payload Type: JSON

Predefined Policies: Default

Name	Mode
Database	Active
Vulnerabilities	Active

Base64 Heuristic Detection

The way to detect a Base64 payload is not so obvious. If Base64 detection is not processed 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.

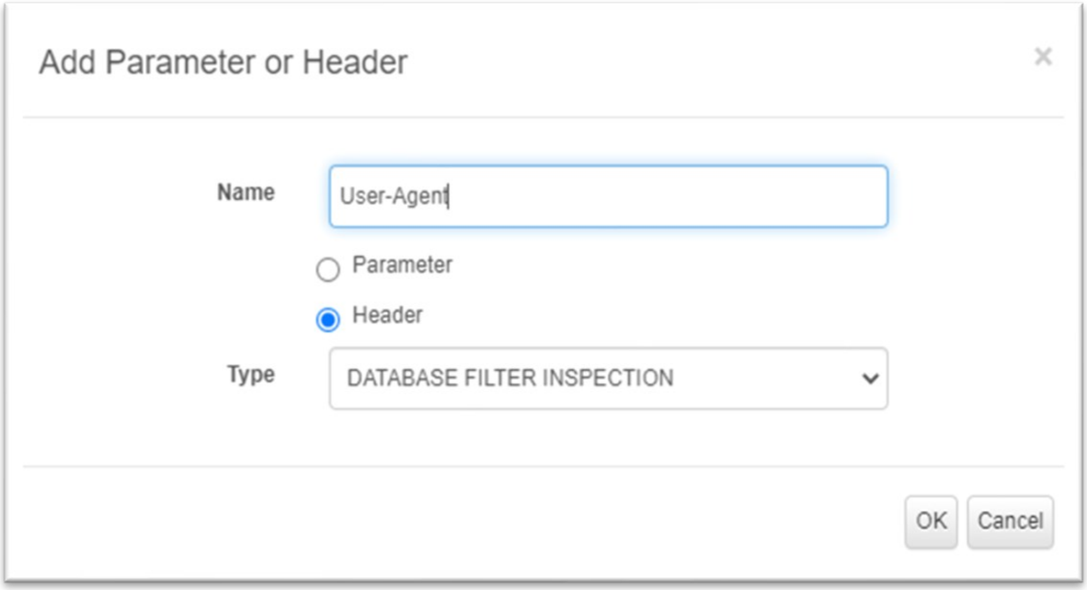
Multiple Encoded Attacks

In the previous release, we introduced support for multiple-encoded attacks for any parameter. In this version, Radware added 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

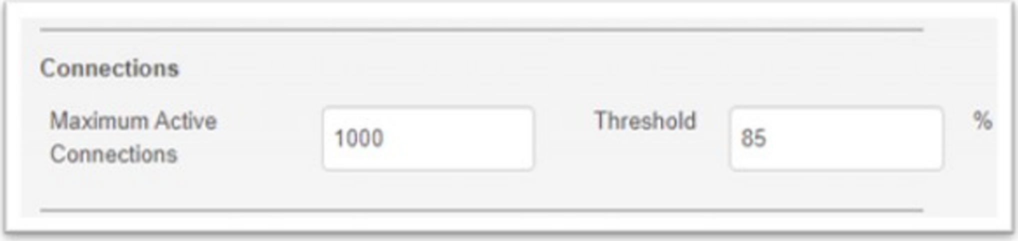
● Header

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.

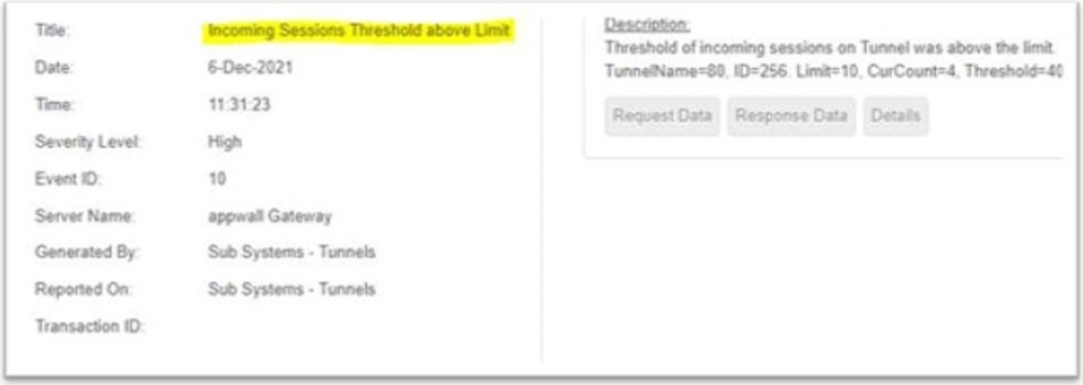
In this version, we added the option to configure a threshold (in percentage) of active connections. When the threshold is reached, an alert is sent in the Forensics Security events before the maximum number of allowed active connections is reached and the connections queue gets completely full.



Connections

Maximum Active Connections: 1000

Threshold: 85 %

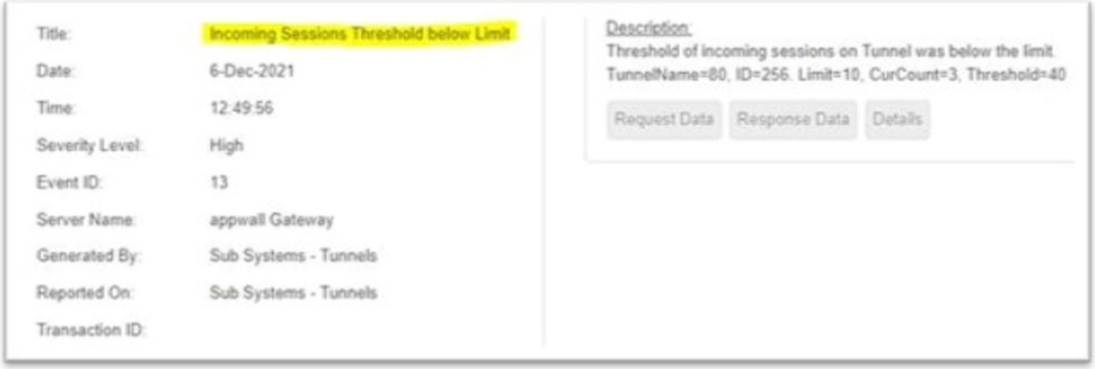


Title:	Incoming Sessions Threshold above Limit
Date:	6-Dec-2021
Time:	11:31:23
Severity Level:	High
Event ID:	10
Server Name:	appwall Gateway
Generated By:	Sub Systems - Tunnels
Reported On:	Sub Systems - Tunnels
Transaction ID:	

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 32.4.8.0

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 32.4.7.0

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.

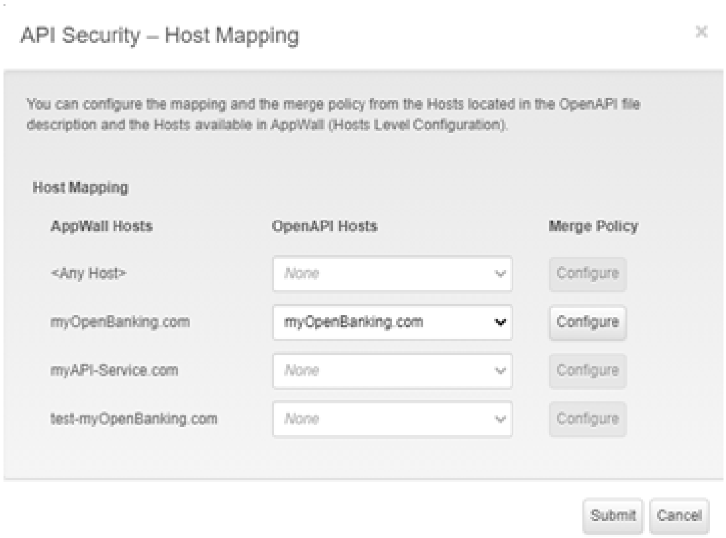
Important: The default management cipher is now set to "main" and supports the following suites:

```
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).

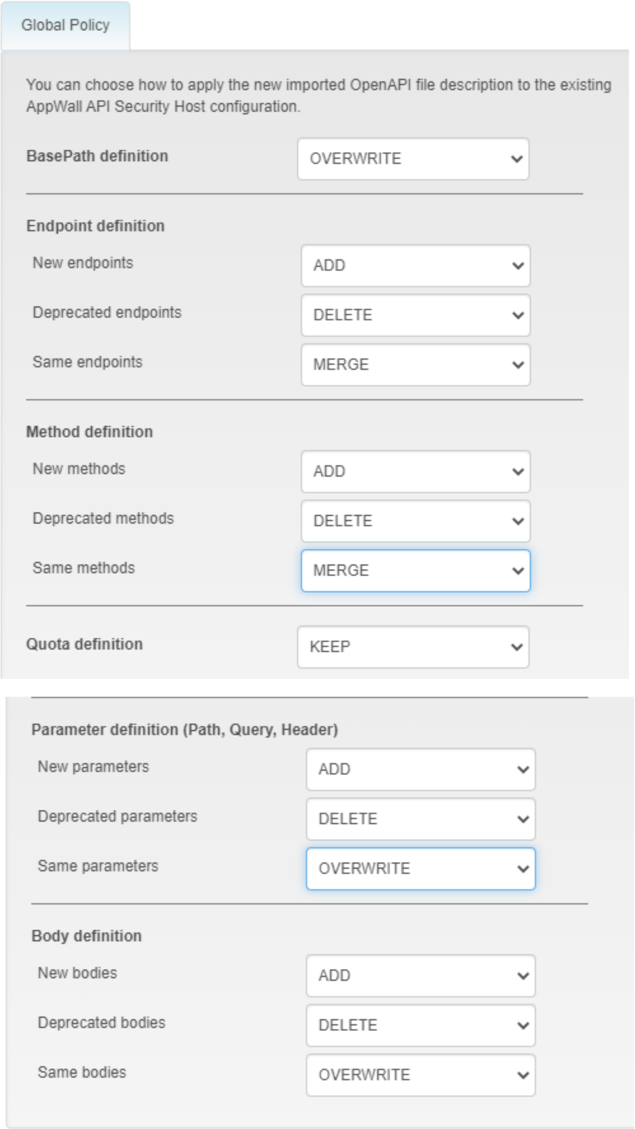
Host Mapping

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

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

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



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

BasePath definition OVERWRITE

Endpoint definition

New endpoints ADD

Deprecated endpoints DELETE

Same endpoints MERGE

Method definition

New methods ADD

Deprecated methods DELETE

Same methods MERGE

Quota definition KEEP

Parameter definition (Path, Query, Header)

New parameters ADD

Deprecated parameters DELETE

Same parameters OVERWRITE

Body definition

New bodies ADD

Deprecated bodies DELETE

Same bodies OVERWRITE

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

WHAT'S NEW IN 32.4.6.0

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 32.4.5.0

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

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 32.4.4.0

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.

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.

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 the 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.

WHAT'S NEW IN 32.4.3.0

Alteon VA – Azure Government support – HA support

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

Synchronization of Cluster Persistent Data (first introduced in version 32.4.2.60)

Synchronization of persistence information between Alteon devices that are members of the same Active-Active clusters (2-tier clusters) ensures persistency between a client and server so that the server provides the client with services even in cases where the Alteon device for a specific client fails. The Alteon cluster member that receives the new connections from the client can continue to forward new connections to the persistent server.

The Cluster Persistent Data Sync option synchronizes client IP address and SSL ID persistency. The data is synchronized between cluster members over unicast UDP communication. New persistent entries are sent to all other cluster members. In addition, aggregated data (32 entries per message) is sent at every user-defined keep-alive interval (default 30 seconds). When a new Alteon is added to the cluster, or a device that went down comes back up, updates are triggered from all the existing members.

Note: Before configuring cluster persistent data synchronization:

- Session Persistency must be set to Client IP address for virtual services
- High Availability must be disabled
- Sync Persistent Sessions must be disabled

To configure cluster persistent data synchronization (Web UI: **Network > High Availability > Cluster Persistent Data Sync**; CLI: `/cfg/slb/sync/cluster`)

1. Enable the Cluster Persistent Data Sync option
2. Add the IP addresses of all the cluster members

NFR ID: 190911-000454 (prod00272010)

WHAT'S NEW IN 32.4.2.0

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)

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)

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 ‘‘Refine’’ includes only new events generated after the upgrade. Filtering ‘‘Not Refine”" events includes all events from before the upgrade, refined and not. Radware advises to use this filter together with a time range filter.

WHAT’S NEW IN 32.4.1.6

IPv6 Support

The following products and product features now support IPv6:

- AppWall Activity Tracking
- AppWall Reverse DNS Lookup
- Radware vDirect

WHAT’S NEW IN 32.4.1.0

This section describes the new features and components introduced in this version on top of Alteon version 32.4.0.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.4.1.0.

Traffic Events Enhancements

Traffic Events Volume Control

Starting with this version, you can control the traffic event log volume by limiting the number of events per second generated per application. The limit is defined in the traffic event policy, based on the traffic event severity (Normal/Exception), as either Unlimit, Event/Sec Limit, or Disable (do not send). With this capability, the log storage capacity can be protected and predictable.

The default is set to 100 events/second for both Normal and Exception events (in previous versions, before this feature was introduced, the default was Unlimited).

Satisfied End-to-End Time Threshold Setting

By default, the satisfied End-to-End time threshold is set to 500 ms and the frustrated End-to-End time threshold is set to 2000 ms.

Using the Traffic Event log, a transaction that exceeds the frustrated End-to-End time threshold severity is set to Exception.

Starting with this version, you can define the satisfied End-to-End time threshold globally (using the `/cfg/slb/adv/satisrt` command) and per application (using the `/cfg/slb/virt/service/satisrt` command).

The frustrated End-to-End time threshold is calculated as the Satisfied threshold multiplied by four.

New SLB Metric – Highest Random Weights (HRW)

The Highest Random Weights (HRW) Hash Load Balancing Metric can ensure client IP address persistency in an Active-Active cluster scenario.

Usually Layer 3 session stickiness to a real server is preserved on Alteon via the session table and the persistency entries (p-entries). To ensure that Layer 3 stickiness is preserved when the active Alteon fails, the preserved session table and persistency entries must be synchronized (mirrored) between the cluster peers. In an Active-Active cluster such synchronization is not practical, and a different mechanism is required to preserve Layer 3 connections and Layer 3 session stickiness to a real server for a scenario where an Alteon instance fails.

The HRW method performs hash on the client IP plus server IP. Thus, when a new connection arrives, hash is performed for the combination of client IP address with each of the servers. The server that results in the highest hash value is selected.

When a real server becomes unavailable or is removed, all session entries mapped to it are removed and load balancing is performed again for those sessions. HRW then selects the new highest result for each client and all sessions of each specific client are mapped to a new server. This is consistent across all cluster members.

Note: If a new server is defined and shortly afterwards failover occurs, sessions that started before the addition of the new server might be redirected to the wrong server (if the new server yields a higher hash value).

NFR ID: prod00272235

DAST (AppWall feature) for D-line Products

Fortify’s WebInspect Dynamic Application Security Testing (DAST) Integration – AppWall integrated with Alteon supports importing the security vulnerabilities report from WebInspect (v19.1.0) to generate a virtual patching security policy tailored to the specific application's security vulnerabilities.

*The DAST feature is available for D-line products only.

WHAT’S NEW IN 32.4.0.0

This section describes the new features and components introduced in this version on top of Alteon version 32.4.0.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.4.0.0.

Documentation in HTML Format

Starting with this version, the documentation set is available from the Radware Customer Portal in both PDF and HTML format. You can access the new HTML documentation either from the Documentation Download page for a given version, or you can perform a search for text from the Customer Portal search feature.

Application Traffic Log Dashboard (Advanced Analytics)

The Application Traffic Log dashboard is available starting with this version, using APSolute Vision version 4.30 or later.

It provides deep-level analytics based on transaction information, improves troubleshooting and speeds up the root cause analysis, it provides user insights, and enables anomaly detection.

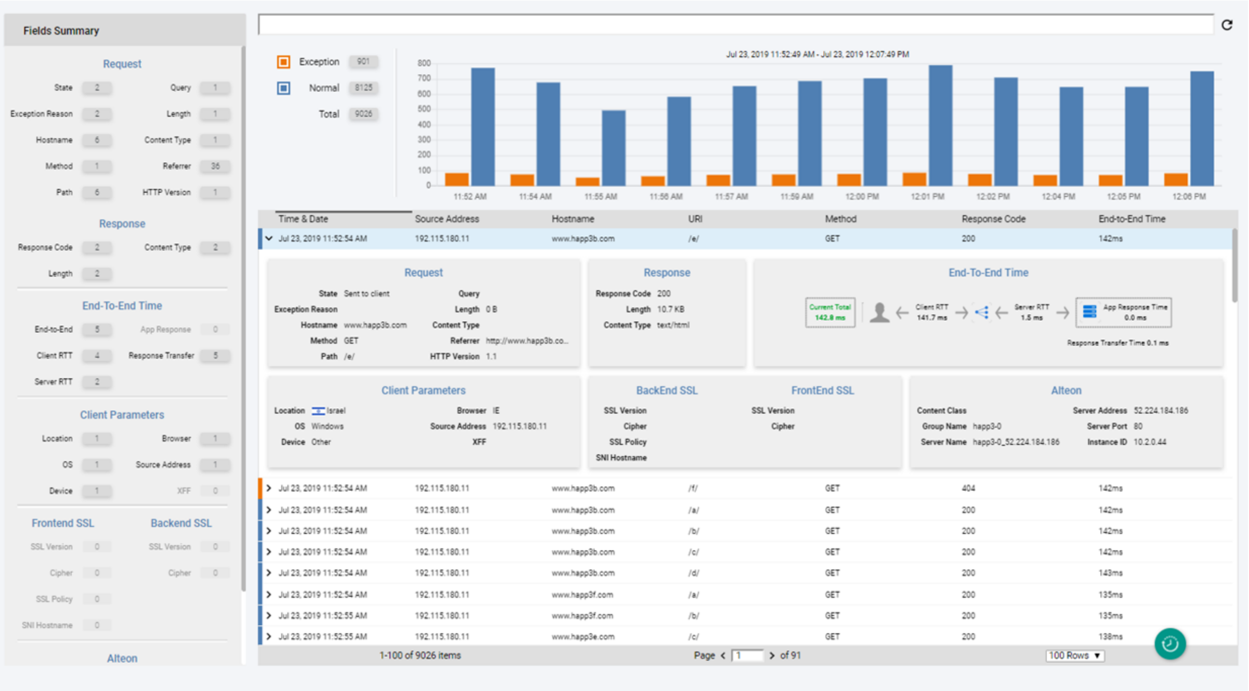
Using the Traffic Log dashboard, you get clear insights to the traffic patterns that your application handles.

The dashboard includes the following components:

- A filter area – Filters events using Lucene Query syntax.
- A histogram – Displays the number of events per severity (Normal/Exception) that match the filter criteria, within the selected period.
- A Traffic Event Log table – Displays the list of events that match the filter criteria, with expanded capability-per-event for detailed information.
- A Fields Summary area – Provides 5 Top values per each and every field of the transaction

Exception events can quickly be identified, including:

- Failed Front-end and Back-end SSL handshake connections
- Transactions ended with 4xx and 5xx response codes
- Transactions with high end-to-end time latency
- Service unavailable use-cases



Fields Summary

Request

State	2	Query	1
Exception Reason	2	Length	1
Hostname	6	Content Type	1
Method	1	Referrer	36
Path	6	HTTP Version	1

Response

Response Code	2	Content Type	2
Length	2		

End-To-End Time

End-to-End	5	App Response	0
Client RTT	4	Response Transfer	5
Server RTT	2		

Client Parameters

Location	1	Browser	1
OS	1	Source Address	1
Device	1	XFF	0

Frontend SSL		Backend SSL	
SSL Version	0	SSL Version	0
Cipher	0	Cipher	0
SSL Policy	0		
SNI Hostname	0		

Alteon

Jul 23, 2019 11:52:49 AM - Jul 23, 2019 12:07:49 PM

Exception	901
Normal	8125
Total	9026

Time & Date	Source Address	Hostname	URI	Method	Response Code	End-to-End Time
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3b.com	/e/	GET	200	142ms

Request

State	Sent to client	Query	
Exception Reason		Length	0 B
Hostname	www.happ3b.com	Content Type	
Method	GET	Referrer	http://www.happ3b.co...
Path	/e/	HTTP Version	1.1

Response

Response Code	200
Length	10.7 KB
Content Type	text/html

End-To-End Time

Current Total 142.8 ms ← Client RTT 141.7 ms → ← Server RTT 1.5 ms → App Response Time 0.0 ms

Response Transfer Time 0.1 ms

Client Parameters

Location	Israel	Browser	IE
OS	Windows	Source Address	192.115.180.11
Device	Other	XFF	

BackEnd SSL

SSL Version
Cipher
SSL Policy
SNI Hostname

FrontEnd SSL

SSL Version
Cipher

Alteon

Content Class		Server Address	52.224.184.186
Group Name	happ3-0	Server Port	80
Server Name	happ3-0_52.224.184.186	Instance ID	10.2.0.44

Time & Date	Source Address	Hostname	URI	Method	Response Code	End-to-End Time
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3b.com	/f/	GET	404	142ms
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3b.com	/a/	GET	200	142ms
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3b.com	/b/	GET	200	142ms
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3b.com	/c/	GET	200	142ms
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3b.com	/d/	GET	200	143ms
Jul 23, 2019 11:52:54 AM	192.115.180.11	www.happ3f.com	/a/	GET	200	135ms
Jul 23, 2019 11:52:55 AM	192.115.180.11	www.happ3f.com	/b/	GET	200	135ms
Jul 23, 2019 11:52:55 AM	192.115.180.11	www.happ3e.com	/c/	GET	200	138ms

1-100 of 9026 items   Page < 1 > of 91   100 Rows ▼

Notes:

- The Traffic Event dashboard is available only for Alteon devices installed with version 32.4 or later.
- Advanced Analytics requires a valid Perform-subscription or Secure-subscription license

WAF Support in Standalone Form-Factor

Integrated AppWall is now also available on Alteon platforms running in Standalone mode. This includes the following platforms: 4208 /S, 5208 /S, 5424 S/SL, 5820 S/SL, 6024 /S/SL/FIPS 7220, 7612.

To provision these capabilities on a Standalone model, perform the following steps:

1. Install the appropriate AppWall licenses on the Alteon platform.
2. Allocate the appropriate number of cores for AppWall. Note that device reset is required to activate core allocation to AppWall.
   - From WBM: **Configuration > System > Core Allocation**
   - From CLI: `/cfg/sys/resources`

Note: When boot configuration is set to factory default, the device reboot removes the allocated AppWall cores.

Single IP Support on Common Alteon VA Environments

Starting with version 32.4, the option to run Alteon VA in single IP mode is available on AWS, VMware, and KVM on top of its current availability in Azure.

Single IP mode is automatically selected when an Alteon VA has a single NIC attached to it.

Configuring an Alteon VA running in single IP mode is very straightforward, as VIPs, PIPs, and interface configuration are done automatically behind the scenes.

There are also cases of public clouds that provide instances with only a single NIC, and using this capability enables the support of such environments.

SCTP Support

The Stream Control Transmission Protocol (SCTP) is a Transport Layer protocol, serving in a similar role to the popular protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). SCTP is a reliable transport protocol operating on top of a potentially unreliable connectionless packet service such as IP. It offers acknowledged error-free non-duplicated transfer of datagrams (messages). Detection of data corruption, loss of data and duplication of data is achieved by using checksums and sequence numbers. A selective retransmission mechanism is applied to correct loss or corruption of data.

The decisive difference from TCP is multi-homing and the concept of several streams within a connection. In TCP, a stream is referred to as a sequence of bytes, but in SCTP, a stream represents a sequence of messages (and these may be very short or long).

Radware defines a single-home SCTP association as a connection between two single IP addresses. A multi-home SCTP association is a connection between multiple addresses. Both client and server can supply additional addresses on top of the one that is carried in the Layer 3 header.

The client sends the additional IP addresses in the INIT packet while the server sends the additional IP addresses in the INIT-ACK packet.

When NAT is performed for SCTP, the INIT and INIT-ACK packets should be updated and the SCTP association should be supported.

SCTP Load Balancing with Alteon

Alteon now supports Layer 4 load balancing for SCTP. The following SCTP communication types are supported:

- Single-homed SCTP **(a connection between two single IP addresses)**
- Multi-homed SCTP **(connection between multiple addresses belonging to the same client and server entities)**
- NAT for outbound SCTP

New Alteon Platforms (Alteon D-5424/D-5820)

The Alteon Application Switch D-5424/D-5820 is a very high port density ADC with up to 40 Gbps throughput.

These platforms support the latest encryption standards (ECC) with an HW SSL acceleration integrated by default, and have superior performance coupled with a wide range of connectivity options, high performing and reliable storage (SSD), high memory size, advanced capabilities, and OnDemand scalability.

They are suitable for small to medium-sized enterprises that require a high-performing solution.

Alteon D-5424/ D-5820 Highlights

- On-demand throughput scalability: 12 Gbps, 22 Gbps, and 40 Gbps
- Platform flavors:
  - Alteon D-5424S / D-5820S up to:
    - 10K RSA SSL CPS
    - 7K EC SSL CPS
    - 10Gbps bulk encryption
  - Alteon D-5424SL / D-5820SL up to:
    - 20K RSA SSL CPS
    - 12K EC SSL CPS
    - 10Gbps bulk encryption
- Port density:
  - Alteon D-5424S/SL
    - Four (4) 10 GE SFP+
    - Sixteen (16) 1 GE SFP
    - Eight (8) 1 GE RJ45
    - Two (2) management port – 1Gbe copper
    - One (1) console RJ45
  - Alteon D-5820 S/SL
    - Eight (8) 10 GE SFP+

    - Twelve (12) 1 GE SFP
    - Eight (8) 1 GE RJ45
    - Two (2) management port – 1Gbe copper
    - One (1) console RJ45
- RAM: 32 GB
- Storage: 128GB SSD
- Single AC power supply – dual power supply is optional (currently DC PS is not available)
- Capabilities: Deliver, Perform, and Secure capability packages

Notes:

- Upgrades between S flavors to SL flavors are based on software license only.
- The ADC-VX form factor is not yet supported (planned for end of 2019).
- Shipping will start on September 20, 2019.

SSL

SNI-based Decisions without SSL Decryption

There are scenarios that require making host-based decisions for SSL traffic without decrypting it using the Server Name Indicator (SNI). Previously, this capability was available only for outbound SSL Inspection. Starting with this version, this was extended to support the following scenarios:

- **Inbound SSL Inspection Bypass**–− When virtual hosting is present (multiple hosts on the same service IP address), in order to bypass SSL inspection for some of the hosts:
    a. Configure a front-end filter that handles bypassed hosts, using an SSL Content Class to match the hosts that should be bypassed, and no SSL policy.
    b. Configure additional front-end filter/s that handle traffic that must be inspected with an SSL policy and the necessary certificate/certificate group.
    c. Configure a Multi-protocol Filter Set and attach to it the front-end filters.
- **Redirect or block SSL traffic to certain sites**–− Allows redirecting SSL traffic to a specific server group or WAN Links group, or block SSL traffic based on hostname or web category, without SSL decryption.
    a. Configure an SSL Content Class that matches the hostnames for which you want to define a certain policy (for example, Office365 hostnames) or a URL Filter policy that matches the categories for which you want to define the policy.
    b. Configure SSL Content Class that includes a single Host entry set to “.” – this matches all the rest of the SSL traffic (“any”).

c. Configure filter SSL (Application set to HTTP) and attach to it the SSL Content Class or URL Filter Policy that matches the specific hosts/web categories. If it is a URL Filter Policy, the URL Filtering Mode must also be set to SSL.

   - If the requirement is to redirect this traffic to specific servers or WAN Link/s, the filter must be of type Redirect or Outbound LLB and the specific WAN Link group must be configured.
   - If the requirement is to block such traffic, the filter must be of type **Deny**.

d. Configure an additional SSL filter (Application set to HTTP) that handles the rest of the SSL traffic and attach to it the "any" SSL Content Class.

e. Configure a Multi-protocol Filter Set and attach to it the above filters. Note that the above filters do not include an SSL policy.

- **Virtual Hosting without SSL decryption**–− It is possible to redirect traffic of different hosts on the same virtual service to different server groups, without decrypting the SSL.

  a. Configure SSL Content Classes that match the hostnames you want to redirect.

  b. Configure Content Rules and attach them to an HTTPS/SSL virtual service.

  Notes:

  - No SSL policy is attached to the virtual service
  - All Content Classes attached to a virtual service must be of the same type – either HTTP or SSL.

OpenSSL Update

The OpenSSL version is updated in this release as follows:

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

AppWall–- Redirect Validation

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 "dynamic file inclusion" mechanisms implemented in the application. The vulnerability occurs due to the use of user-supplied input without proper validation.

AppWall's Redirect Validation scans all parameters in the request (including JSON, URL and body parameters) and looks for external or internal redirect attempts to include files.

You can add trusted domains and trusted URIs for which the Redirect Validation are not applied. These can be added manually by clicking **Add** in the trusted domains and trusted URIs list.

OCSP Multiple Servers

OCSP multiple servers increase availability by letting you configure a secondary (backup) static OCSP server and by supporting a retry mechanism that prevents OCSP communication failure because of a temporary issue (number of retries is configurable).

WHAT'S CHANGED IN 32.4.17.0

Reduce Default Traffic Event Sampling

The default sampling rate for traffic events has been decreased from 100% to 20% to mitigate its performance impact. In a production environment, it is advisable to start with this low rate and adjust it according to specific needs and performance considerations. Note that this modification applies solely to new traffic event policies and does not influence existing policies.

Further, beginning with this version, the sampling rate no longer affects Security events and EAAF events.

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

Exclusion of URL Categorization from Secure Subscription License

Starting with this version, the URL Categorization capability is excluded from the Secure Subscription license and is now accessible through the SecURL Gateway license.

Existing deployments utilizing URL Categorization with Secure Subscriptions will remain unaffected when upgrading to this version or any subsequent releases. These deployments can continue to utilize URL Categorization with Secure Subscriptions until their upcoming renewal without any disruption.

License Validation During Config Import

When uploading a configuration file to Alteon with enabled capabilities for which the corresponding license is not installed on Alteon, the configuration upload fails and remains in diff. Starting with this version, a clear error will also appear via the CLI and WBM listing the missing licenses to support the required configuration.

Integrated AppWall

HTML Decoding

- Support for decoding the HTML-encoded query parameter value in the HTTP request.

Vulnerability Partial Scan

- Support for partial inspection for each of the request zones: URL, Headers, Body, or Parameters. Each zone can be configured as fully scanned, partially scanned, or disabled for scanning.

GraphQL Protection

- Support for importing and exporting SDL files.

WHAT’S CHANGED IN 32.4.16.0

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

GSLB Network Number Increase

The maximum number of GSLB networks was increased from 2048 to 4096 for VA, Standalone, and vADCs with 11 CUs or greater. For vADCs with less than 11 CUs, the maximum number of GSLB networks was increased from 1024 to 2048.

NFR ID: 230111-000065

"wget" Package Update

The WGET library was upgraded to version 1.21.4.

NFR ID: 220808-000107

Integrated AppWall

GraphQL Protection

- Support for Extension, Directive and Variable list.
- Support for requests located in the query parameters.
- Security inspection with Database filter, Vulnerabilities filter and Redirect Validation Host protection.

Custom Pattern

The customer pattern has been improved to support multiple conditions. We can now define different patterns located in different zones of the requests.

It provides a more accurate option to define Custom Pattern and reduce false positives.

Limit Number of Headers to Parse

In the Tunnel Properties, we can limit the maximum number of headers to be parsed.

Base64 Decoding

The Base64 heuristic detection can decode payload with suffix.

Redirect Validation Host Protection

In the Defense Properties, the configuration of the Redirect Validation Host protection is exposed. The signatures used for LFI, RFI, SSRF and their delimiters can be edited.

WHAT'S CHANGED IN 32.4.16.0

Reduce Default Traffic Event Sampling

The default sampling rate for traffic events has been decreased from 100% to 20% to mitigate its performance impact. In a production environment, it is advisable to start with this low rate and adjust it according to specific needs and performance considerations. Note that this modification applies solely to new traffic event policies and does not influence existing policies.

Further, beginning with this version, the sampling rate no longer affects Security events and EAAF events.

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

Integrated AppWall

HTML Decoding

- Support for decoding the HTML-encoded query parameter value in the HTTP request.

Vulnerability Partial Scan

- Support for partial inspection for each of the request zones: URL, Headers, Body, or Parameters. Each zone can be configured as fully scanned, partially scanned, or disabled for scanning.

GraphQL Protection

- Support for importing and exporting SDL files.

WHAT’S CHANGED IN 32.4.15.0

BWM Shaping

The BWM shaping capability is no longer supported and has been hidden from the CLI and WBM. If the capability is configured already on a device before upgrading to this version, it will continue to work as configured after upgrade.

Alteon Embedded Dashboard Removal

Starting with this version, the Alteon embedded dashboard is no longer available from WBM. For enhanced analytics, which include historical data and reporting, Radware recommends using the ADC analytics capability available via APSolute Vision or Cyber Controller.

Advanced Virtual Wire Health Check Enhancements

The advanced virtual wire health check now works in conjunction with port trunks (Static and LACP).

Change in AppWall SNMP Trap OID

The SNMP trap OID for the integrated AppWall server status was wrong and is now fixed:

- appwallUpTrap (AppWall server is up) OID is now .1.3.6.1.4.1.1872.2.**5**.7.0.166
- appwallDownTrap (AppWall server is down) OID is now .1.3.6.1.4.1.1872.2.**5**.7.0.167

Integrated AppWall

Multiple Improvements

- **Automatic Disable for Auto Discovery and Auto Policy**: A timer was added to disable Auto Discovery and Auto Policy after 30 days.
- More security coverage in the **Directory Listing** host protection.
- Support for **Tor Exit Nodes** in the GEO updates subscription (Anonymous Proxy renamed).
- **SSRF Security Event** name change.
- Increase **default configuration value for Fast Upload**.
- **Redirect Validation default configuration change.**
- **Default Security filters in a new Virtual Directory**: Database filter, Vulnerabilities filter and HTTPMethod are proposed by default.
- **Base64 support**: Option for “Heuristic Detection” and “Force scan of original value” has been removed from AppWall management Console (available in the Configuration file and REST Management APIs).

WHAT'S CHANGED IN 32.4.14.0

Combined Image Upload Option Removed from WBM

The Alteon combined image is utilized to install both ADC-VX and vADC instances for Alteon platforms in a single step. However, the option to upload a combined image has been removed from the WBM in this version and is only supported via the CLI. If you want to upload an image via WBM, you must upload the ADC-VX and vADC images separately.

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

AppWall Integrated

1. **API Security**

   In this version multiple enhancements are provided for API Security protection:

   - **Support for Preflight request (CORS mechanism):** Usually the preflight requests are automatically sent by browsers. This consists of sending automatic requests with the HTTP method OPTION and the header "Access-Control-Request-Method". If the method OPTION is not defined in the OpenAPI file description, the requests are blocked by the API protection. Support of preflight requests will now accept these client requests coming from the browser.
   - **Case insensitivity during the API Catalog endpoints inspection.** By default, the inspection is case sensitive. It can be deactivated to be case insensitive.
   - **Circular reference**: OpenAPI files that include circular references are now supported.
   - The **Forensics Security Events** present more detailed descriptions related to the nested parameters, for example into a JSON body.
   - When a Security violation occurs, AppWall propose a more accurate and **advanced refinements option** that will improve the False Positive management.
   - The **AppWall Techdata** has been updated to include the OpenAPI files that have been previously uploaded.

2. **Custom Pattern per Application Path**

   Custom Patterns help to define a personal signature. Custom Patterns can now be defined per Application Path, not only globally.

3. **Server-Side Request Forgery**

   The Unvalidated Redirect protection is improved in terms of performance and security coverage.

4. **Multiple IPs Included in XFF HTTP Header**

   In version 7.6.18.0, AppWall allowed globally configuring how to read XFF HTTP headers when they contain multiple IPs. From this version, this can be configured per AppWall Tunnel (referred to as SECWA in the Alteon WAF).

5. **Global Security Event Suppression**

   AppWall provides mechanisms to protect from a Security Events flood:

   - Automatic Event suppression configured manually per Security Event.
   - Automatic Event suppression configured dynamically per Security Event.

   In this version, AppWall provides an additional mechanism:

   - Automatic Event suppression configured dynamically per multiple Security Events.

6. **Database Security Filter**

   Database Filter inspection can be excluded for Query/Body Parameter names. The configuration is available globally or per Application Path.

7. **Multiple Enhancements on AppWall REST API for DevOps**

   Multiple new AppWall REST APIs have been delivered.

   For details, please consult the on-line product documentation.

WHAT’S CHANGED IN 32.4.13.0

MP CPU Reservation

In VX mode, the MP core is shared between multiple vADCs. By default, Alteon reserves MP processing power for all vADCs that an MP core can carry. For example, if an MP CPU can carry 10 vADCs and only four (4) are configured, Alteon reserves 60% of the core for future vADCs.

In this version, you now can disable this reservation to allow the existing vADCs to utilize the full resources of the core. Note that if you disable the reservation, when you add a new vADC, the MP resources available are reallocated, so the resources allocated to the previous vADCs will go down. In the above example, if previously each vADC received 25% core, now it will receive 20%.

Cookie Insert Path

When virtual service persistency mode is Cookie Insert, the default for the Path field is now "/" (previously was empty).

Upon software upgrade to this version the existing configuration is preserved.

AppWall Integrated

Multiple IPs included in XFF HTTP header

Content Delivery Network (CDN) support helps define the real source IP. By default, AppWall reads the right-most IP. Optionally, the left-most IP can be defined as the real IP.

WHAT'S CHANGED IN 32.4.12.0

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.

AppWall Integrated

- 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 32.4.11.0

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 requires 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 upgrading 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.

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.

AppWall Integrated

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.

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.

WHAT'S CHANGED IN 32.4.10.0

Empty Group Association to FQDN Server and Virtual Service

A group without servers can now be associated with 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.

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 it 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 32.4.9.0

None

WHAT'S CHANGED IN 32.4.8.0

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 32.4.7.0

Default Management Port Access on a Data Port in ADC-VX

Starting with this version, management access on the data port is disabled on a vADC by default. This change was done to align with the standalone behavior. The change is applicable for new configurations (an existing configuration will not be affected after upgrade).

NFR ID: 201204-000112

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

AppWall Features

1. In the Tunnel configuration, AppWall now defines multiple properties related to the HTTP parser per URI. The following changes have been added in this version:
   a. By default, when adding a new URI, the following parameters are validated:
      i. Allow Parameter without an equal sign
      ii. Fast Upload for large HTTP requests
      iii. Fast Upload for large HTTP requests with files
   b. The option “Use IIS Extended Unicode Measures (Block Unicode Payloads)” has been removed from the AppWall management console but is still available from the configuration file.
2. The BruteForce Security Filter prevents remote users from attempting to guess the username and password of an authorized user. The option “Shared IP auto-Detection” check box has been removed from the AppWall management console to limit false positives.
3. Remote File Inclusion (RFI) and Local File Inclusion (LFI) are file inclusion vulnerabilities that allow an attacker to include a file or expose sensitive internal content, usually exploiting a “dynamic file inclusion” mechanism implemented in the application. In the Hosts protection section, by default, Redirect Validation is in passive mode with the option “Protect against external URL” activated.
4. The Tunnel IP (VIP), the Port and the Host have been added to the system log event titled "Large number of parameters in request".

WHAT'S CHANGED IN 32.4.6.0

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.

Starting 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 32.4.5.0

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 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

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

WHAT'S CHANGED IN 32.4.4.0

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.

OpenSSL Upgrade

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

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

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 32.4.3.50

TLS Version Default

Starting with this version, TLS 1.1 is disabled by default.

Note: The default TLS 1.1 setting is not set to disabled if was enabled prior to this version.

WHAT’S CHANGED IN 32.4.3.0

Syslog Enhancements

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 manually disabling 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 – 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 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).

WHAT'S CHANGED IN 32.4.2.0

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)

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.

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)

OpenSSL Version

The OpenSSL version for both management and data path was updated as follows:

- XL/Extreme and FIPS II models: 1.0.2u
- S/SL models, standard models and VA: 1.1.1d

WHAT’S CHANGED IN 32.4.1.0

Smart Session Table Adjustment

Based on research Radware performed, more than 99% of the Alteon platforms in the field use less than 10% of their session table capacity.

Alteon allocates static memory for the entire session table in advance even if Alteon uses only a few thousand entries.

In order to increase Alteon free memory, the session table has been reduced to 50% of its capacity.

The session table will not be changed automatically in the following cases:

- The user changes the default value (100%) of the session table.
- The session table peak is above 35% since the last reboot.

Platform	RAM Size	100% Session Table	50% Session Table	Free Memory Saving (free memory improvement) *
4208	8GB	6M	3M	706 MB (+53%)
5208	16GB	12M	6M	1,358 MB (+34%)
5424	32GB	22M	11M	2,482 MB (+24%)
5820	32GB	22M	11M	2,482 MB (+24%)
6024	32GB	20M	10M	2,260 MB (+19%)

Platform	RAM Size	100% Session Table	50% Session Table	Free Memory Saving (free memory improvement) *
6420	32GB	46M	23M	4,894 MB (+210%)
7612	96GB	46M	23M	4,603 MB (+11%)
7220	96GB	46M	23M	4,603 MB (+11%)
8420	128GB	76M	38M	8,596 MB (+16%)
9800	192GB	140M	70M	7,901 MB (+8%)

*Based on the platform's default RAM size

The session table size can also be changed manually with the following CLI command:

```
/c/slb/adv/sesscap

Enter capacity (400 , 200 , 100 , 75 , 50 , 25 , 12) of entries
sessions table: <Session table capacity>
```

Alteon User Password Encryption Enhancement

Starting with this version, the user password is encrypted with SHA512 with dynamic Salt.

Important: Due to this support, it is now mandatory to define the configuration sync Authentication Passphrase on both HA peers (using `/cfg/slb/sync/auth`). During upgrade, a default passphrase will be set if there is no passphrase. It is recommended to update that default passphrase after the upgrade.

NFR ID: prod00272191

Audit Log via Telnet and SSH

The audit log now includes the CLI protocol from which the configuration change was performed (either Telnet or SSH).

NFR ID: prod00272163

BGP Support for Four-octet AS Number

The range of the "AS" value for BGP was extended from a 2-byte to a 4-byte value.

NFR ID: prod00268252

OpenSSL Update

The OpenSSL version is updated in this release as follows:

- S/SL platform models, regular platform models, and Alteon VA now use OpenSSL 1.1.1c

- XL/Extreme platform models, as well as 6024 FIPS II, use OpenSSL 1.0.2s

Full Layer 3 Tunnel Support (IP-in-IP and GRE) – Phase 2

IP-in-IP and GRE tunnel protocols for the data path is now supported.

NFR IDs: prod00259678, prod00259680

Failover Delay

In a high availability environment, a failover delay is now available on the backup in order to eliminate failover flapping when a virtual service failover occurs.

When the failover delay is defined, once the master priority decreases, the backup waits for the configured delay time before it becomes the master.

The delay is used whenever the priority is decreased because of real/gateway/interface tracking.

Note: This capability is available for both service and switch mode and is not available for VRRP.

NFR ID: 191006-000024

WHAT’S CHANGED IN 32.4.0.5

Fixed AppWall Performance Degradation

Fixed a severe performance degradation of AppWall integrated with Alteon after upgrading to version 32.4.0.0.

The performance degradation was only related to services that have Secwa attached and impact the traffic that goes through AppWall.

WHAT’S CHANGED IN 32.4.0.0

HTTP/2 Proxy General Availability

The full HTTP/2 Proxy capability that allows load balancing HTTP/2 traffic to HTTP/2 real servers, is now Generally Available (it was previously available as Beta only).

The following capabilities are supported for HTTP/2 Proxy:

- SSL offloading
- Back-end SSL
- Layer 4 load balancing

- XFF header insertion
- Server Health Check over HTTP/2

To configure HTTP/2 Gateway for a virtual service:

1. Define the HTTP/2 policy, as follows:
   a. Select **Configuration > Application Delivery > Application Services > HTTP. HTTP/2**.
   b. In the Policy table, click **+** to add an entry. The relevant *Add* tab displays.
   c. Click **Enable HTTP/2 Policy** to enable the policy, once defined.
   d. In the **Policy ID** field, enter an ID for the new policy.
   e. In the *Backend* tab, select **Backend HTTP/2** to enable HTTP/2 proxy.
   f. Click **Submit**.
2. Define the required HTTPS virtual service, including an SSL Policy. The server group used for this service must use the HTTP/2 health check. Predefined clear text (h2c) and SSL (h2) HTTP/2 health checks are available.
3. In the virtual service *HTTP* tab, select the HTTP/2 policy to use with this service.

Alteon VA Enhancements

Support for Mellanox CX5 Alteon VA over VMware

Mellanox CX5 100G NICs are supported on the Alteon VA running VMware in pci pass-through mode.

Improved Performance on AWS

The performance of Alteon VA running on AWS was improved by supporting SRIOV on AWS.

Alteon VA, when running on AWS instances, supports SRIOV (enhanced network) reaching 10 Gbps (such as m4.10xlarge can reach 10 Gbps L4 throughput).

By running Alteon VA on instances supporting SRIOV (enhanced networking), the Layer 7 and SSL performance can be significantly improved utilizing the Alteon DPDK capabilities to run multiple SPs using the Alteon TDVA.

Extended GEL Throughput Points

The granularity of the Alteon instances running a GEL instance was extended.

Alteon instances running GEL license can now be assigned the following throughput points:

- 25M, 50M, 75M, 100M, 200M, 300M, 500M, 800M
- 1G, 2G, 3G, 5G, 8G, 10G, 15G
- 20G, up to 60G in increments of 10G (10G, 20G,….60G)

- 100G, 160G, 230G

Layer 7 Performance Improvement

Layer 7 performance (L7 RPS, L7 BW, and SSL bulk encryption) of the following Alteon platforms has been improved:

- Alteon D-4208
- Alteon D-7612 / D-7220
- Alteon D-9800

The new tech spec includes the updated numbers. You can find it on Radware portal or Radware official Web site.

Note: The improvement takes effect only when Layer 4 HW hash is enabled.

SSL Inspection Wizard Enhancement (vDirect Based)

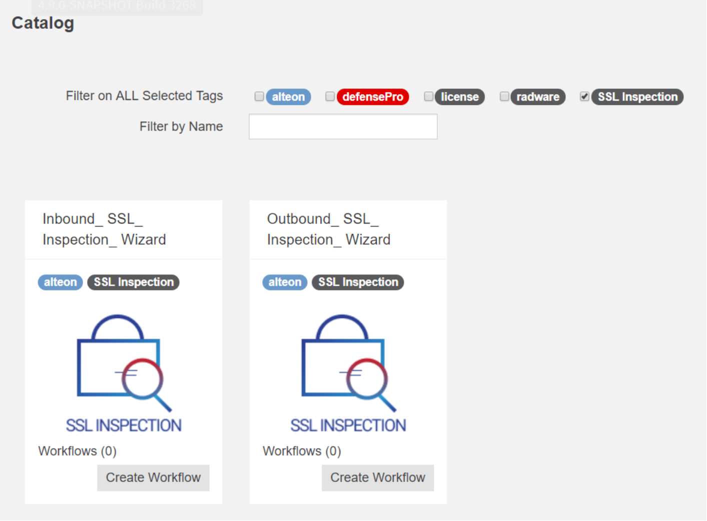
An updated wizard for quick and easy configuration of an outbound SSL Inspection solution is now available using vDirect workflow version 1.1.0-1 available on APSolute Vision 4.30.

The updated wizard provides full-transparent deployment (where Alteon acts as bump-in-the-wire) on top of the Layer 3 deployment which was available in workflow version 1.0.0.

Notes:

- Full-transparent mode is available for Alteon VA, Standalone, and vADC
- Layer 3 mode is available for both Alteon VA and Standalone
- 2-box deployment is not yet supported

To access the wizard, access vDirect from APSolute Vision, navigate to the catalog, and filter by SSL inspection:



Catalog

Filter on ALL Selected Tags □ alteon □ defensePro □ license □ radware ☑ SSL Inspection

Filter by Name

Inbound_ SSL_ Inspection_ Wizard

alteon SSL Inspection

SSL INSPECTION

Workflows (0)

Create Workflow

Outbound_ SSL_ Inspection_ Wizard

alteon SSL Inspection

SSL INSPECTION

Workflows (0)

Create Workflow

Management Login Using the SSH key

In addition to the basic user/password authentication, Alteon also supports SSH public key authentication. Public key authentication improves security considerably as it frees users from remembering complicated passwords (or worse, writing them down). It also provides cryptographic strength that even extremely long passwords cannot offer.

SSH public key authentication offers usability benefits as it allows users to implement single sign-on across the SSH servers they connect to. Public key authentication also allows for an automated, password-less login that is a key enabler for the countless secure automation processes.

Note: SSH public key authentication support is available only for local users.

NFR ID: prod00235977

AppWall

The Geolocation database and IP Groups now support IPv6 addresses and can be used in Web User Roles.

Application Dashboard and Basic Analytics License Enforcement

Starting with this version, Alteon basic analytic (metric-based reporting) requires the Perform package license.

Note: The Application dashboard is available in APSolute Vision and is also based on Alteon basic analytics capabilities. Ensure that the Alteon devices for which you require application dashboard monitoring are installed with the Perform package.

Virtual Service Traffic Event Logs Additions

In addition to the HTTP, SSL, and Layer 4 connection separated events, Alteon now also supports Unified events.

Using Unified events, an event is sent per transaction including HTTP, SSL, and Layer 4 information during the same event, allowing easier integration with third-party SIEM products (like ELK or Splunk)

Unified events also identify two types of events:

- Normal Severity – Transactions that ended successfully (as expected)
- Exception severity – Transactions that ended with an anomaly that may have an impact on the service. The following exception reasons are identified:
  - Service unavailable – When a group is unavailable or overloaded
  - HTTP response code 4xx
  - HTTP response code 5xx

- Failure of Front-end or Back-end SSL handshakes
- End-to-end time passed a threshold (currently, the E2E time threshold is set to 2 seconds)

Notes:

- Traffic event logging requires a valid Perform-subscription or Secure subscription license.
- Traffic event logging impacts performance. To reduce performance impact, use sampling.
- The unified events are only available for HTTP/HTTPS virtual service in force proxy.
- Unified events can only be sent over TCP/TLS syslog.

MAINTENANCE FIXES

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

Fixed in 32.4.17.0

General Bug Fixes

Item	Description	Bug ID
1.	A real server health check failed even when there was response to the health check packets.	AL-141245
2.	There was a problem with config sync of a TrustedCA certificate.	AL-141314
3.	Added a debug command and debug logs for helping to debug an SP panic involving a filter configuration.	AL-141609
4.	vADC2 and vADC3 auto-rebooted due to a software safe restart	AL-141629
5.	After upgrading to version 33.0.9.50, SP1 has high CPU utilization on vADC4.	AL-141699
6.	The overload status was activated when at least one LOGEXP health check operand detected an overload.	AL-141752
7.	A BGP flap occurred due to a non-reachable IP address used in getlog.	AL-141862
8.	A compression limit above 10000 MB was not correctly pushed to a vADC.	AL-141877
9.	In some edge cases, the watcher process had an invalid process ID 0. The fix is not to try to recover process ID 0.	AL-141935

Item	Description	Bug ID
10.	After analyzing a customer-reported reboot, added a protection code to prevent access to released memory.	AL-142166
11.	The MP crashed upon apply when <real/group/virtual server> used a new health check object ID with the same content and with the same index.	AL-142245
12.	There was an application persistency issue after adding a new virtual server or configuration.	AL-142267
13.	Many panics or core dumps were generated.	AL-142305
14.	There was an incorrect session count with the pbind cookie.	AL-141311 AL-142316

AppWall Bug Fixes

Item	Description	Bug ID
1.	`Corrupted Configuration File Detected` message displayed.	AW-50153
2.	Failed upload of Open API file on Radware Cloud.	AW-50162
3.	AppWall crashed during production and Web portals were down.	AW-50190
4.	Request to remove uncheckable checkbox from WAF GUI.	AW-50061
5.	Integrated AppWall WebSocket frame size value issue.	AW-50078
6.	Help to investigate Alteon integrated AppWall crash.	AW-50116
7.	AppWall crashed due to configuration corruption.	AW-50119
8.	AppWall fixed content length was injected to the response body and not as a header.	AW-50131
9.	AppWall GUI is showed connection error and the error message "Cannot connect to management server".	AW-50132
10.	Attacks were not blocked by AppWall.	AW-50168
11.	File Upload issue - Possible AppWall issue on version 7.6.21.10.	AW-50184
12.	Integrated WAF security events were not being retained.	AW-50192
13.	Web service was not working when Tunnel is in Passive mode.	AW-50224

Fixed in 32.4.16.50

General Bug Fixes

Item	Description	Bug ID
1.	Services went down after revert apply failed.	AL-141582 AL-141587
2.	On a 5424 platform with 16/24GB RAM, setting the MTU was blocked.	AL-141480 AL-141481
3.	After running /boot/rsrcs/cur, an increased disk size was not reflected.	AL-141467 AL-141471
4.	An Alteon 5208XL platform rebooted with a software safe restart.	AL-141418 AL-141420 AL-141421
5.	After disabling and enabling a BGP peer, the vADC rebooted.	AL-141346 AL-141351
6.	When rebooting a vADC, the vADC was not accessible for approximately five (5) minutes, even though it appeared as UP on the ADC-VX .	AL-141328
7.	After the DNS cache timer expired, Alteon did not query for the FQDN origin if the answer was a CNAME.	AL-141234 AL-141237
8.	Persistent session mirroring did not properly mirror the group names to the backup device when the group names had the same first character.	AL-141217 AL-141218
9.	There was an error in JSON Fancy Names.	AL-141200 AL-141203
10.	Was not able to connect to Alteon via SSH in rare scenarios because the maximum number of sessions exceeded.	AL-141162 AL-141167
11.	When clsaging "both" and clfstage "both" are enabled, a memory leak occurred which eventually led to the health checks failing.	AL-141153 AL-141154

Item	Description	Bug ID
12.	With two gateways configured with same IP address, the route table created two entries whenever the gateway flapped, resulting in filling up the route table, which in turn led to device reboot when Alteon failed to add a route for the gateway.	AL-141147 AL-141148
13.	When an aggregate route was redistributed from one peer to another, the original AS number was added as AS_SEt segment in the AS_PATH attribute. In the code, there were some issues in parsing the AS_PATH segments when there were two or more segments.	AL-141136 AL-141137
14.	The Secured Web Applications view for a user with the user role "Web AppSecurity Owner" hung with a "Loading..." message.	AL-141127 AL-141129
15.	The Mexico time zone switched to DST (daylight savings time) before the actual Mexico DST (April to October). After upgrade, the Mexico time zone did not switch to DST.	AL-141061 AL-141063
16.	The group backup server status was DOWN when queried via SNMP.	AL-140990 AL-140991
17.	When a fragmented packet matched a filter with "reverse enabled" , the device rebooted.	AL-140962 AL-140963 AL-140968
18.	On DPDK platforms, the MNG port bonding mode was incorrect. It was set to round-robin instead of active-backup.	AL-140815 AL-140816
19.	The backup WAN link server did not come online while processing a DNS query.	AL-140647 AL-140649
20.	Changing the vADC management address caused the ADC-VX management address to be removed in ifconfig.	AL-139801 AL-139802

AppWall Bug Fixes

Item	Description	Bug ID
14.	Latency on masked responses.	AW-49841

Fixed in 32.4.16.0

General Bug Fixes

Item	Description	Bug ID
1.	There was a connectivity issue after changing the management IP address.	AL-52913
2.	Upgrading from version 32.6.8 to version 32.6.12 to avoid a memory leak resulted in a further degradation.	AL-138917
3.	Problems occurred with an SSL certificate with a Subject Alternative Name with more than 1024 characters.	AL-139072
4.	Using APSolute Vision, there was a back-end SSL handshake failure exception.	AL-139138 AL-139176
5.	A virtual service froze after an apply operation .	AL-139206
6.	An IPv6 remote real health check failed via a DSSP health check.	AL-139250 AL-139252
7.	WBM was not available after the mmgmt certificate was updated .	AL-139285
8.	A failed real server mistakenly displayed the current sessions counts.	AL-139380
9.	There was an issue with a non-configured peer.	AL-139423
10.	The IPv6 Network filter for an unspecified address (::/128) overlapped with an IPv4 network filter.	AL-139452
11.	There was an issue session capacity and session mirroring .	AL-139483
12.	When syncing from backup to master, virtual services were deleted on the master, affecting the service.	AL-139501 AL-139504
13.	On an Alteon D-6024S platform, the RX and TX PPS statistics value seemed stuck in the prefmon file.	AL-139589
14.	vADC-2 was restarting on both ADC-VX instances in a High Availability environment.	AL-139628
15.	Sessions through transparent SSLi failed when sending traffic to a VRRP MAC.	AL-139640
16.	The Alteon embedded dashboard was visible even though it no longer should be available.	AL-139649

Item	Description	Bug ID
17.	Alteon TRP MIB file (CHEETAH-TRAP-MIB.mib) was missing a definition for session table threshold traps.	AL-139664
18.	An IP address deleted in Smart NAT was not released.	AL-139868 AL-139869
19.	The /info/vADC command output incorrect throughput for the vADC.	AL-139891
20.	Traffic graphs on the dashboard were not updated during a performance test.	AL-139913
21.	There was an issue with vADC High Availability if a high number of CUs are assigned.	AL-139974
22.	A real server in shutdown mode that was in a network rule could not be synced to a peer.	AL-140030
23.	For IP ACLs enabled at the Alteon level, when applying changes to AppWall, the sync process from the device where the AppWall change was applied adds/removes IP addresses not configured manually on the destination device for the sync process.	AL-140057
24.	Could not download tech data.	AL-140105
25.	When TACACS with OTP was enabled, could not log in to Alteon with first attempt providing credentials.	AL-140136
26.	The /oper/slb/group/shut (connection shutdown) did not work correctly.	AL-140182
27.	Issue using AppShape++ to add a PIP if the client IP address was in the same subnet as the server.	AL-140230
28.	After upgrading from version 33.5.4.0 to version 33.5.5.1, the NAT health check configuration was missing.	AL-140261
29.	Application Service Engine Out-of-sync issue	AL-140274
30.	When connecting to a Alteon 5424 platform with a specific server name, after disabling then enabling a port, the device did not come up again.	AL-140281
31.	After running automation with an API call that failed,· accessing the WBM on Alteon VA produced a 50X error.	AL-140413
32.	Inconsistent restart information between ADC-VX and vADC in TechData.	AL-140563

Item	Description	Bug ID
33.	The RST packets originated after an inactivity timeout from the proxy were sent with wrong source MAC instead of the proxymac.	AL-140573

AppWall Bug Fixes

Item	Description	Bug ID
1.	Latency on masked responses.	AW-49841
2.	Standalone AppWall VA crashed (version 7.6.20.0)	AW-49833
3.	AppWall Security event showed wrong destination port.	AW-49938
4.	AppWall crashed when it is inline.	AW-49871

Fixed in 32.4.15.50

General Bug Fixes

Item	Description	Bug ID
1.	Sessions through transparent SSLi failed when sending traffic to a VRRP MAC.	AL-139637
2.	A failed real server displayed the current session count.	AL-139375
3.	Using APSolute Vision, there was a back-end SSL Handshake Failure exception.	AL-139173 AL-139179 AL-139181
4.	When syncing from Backup to Master, virtual services were deleted on the Master device.	AL-138536

Fixed in 32.4.15.0

General Bug Fixes

Item	Description	Bug ID
1.	The Websec module fluctuated between down and up.	AL-49480
2.	The APP response was not calculated correctly when there were matches to the content class	AL-49489
3.	DNS vulnerability CVE-2004-0789 was fixed.	AL-49491

Item	Description	Bug ID
		AL-49492
4.	The FQDN real indexes changed during get config.	AL-49504
5.	When the capture -M command was run on very large secrets files, the disk became full. Now the secrets file size is limited during capture -M execution.	AL-49514
6.	Alteon SSH failed a security audit.	AL-51828
7.	The CDP group table became empty when deleting one entry case.	AL-51868
8.	The static NAT for GRE traffic in point-to-point was incorrect.	AL-51875
9.	The VLAN 2090 error was assigned to more than 32 PIPs.	AL-51888
10.	The /oper/slb/sessdel command did not work for ESP sessions.	AL-51896
11.	There was a corruption in the NAT rule configuration.	AL-51897
12.	The LinkProof Smart NAT ID disappeared.	AL-51905
13.	On a KVM VA, health checks to AppWall and nodejs failed in single IP mode.	AL-52628 AL-52629
14.	The appwallUp and appwallDown traps were sent with the wrong OIDs.	AL-52639 SL-52642
15.	In the Ansible SSL policy configuration, added the option "none" to fe_intermediate_ca_chain_type.	AL-52648
16.	The /info/sys/log command issues an error when the ramdisk is full. This was due to an issue with the FRR log rotation logic.	AL-53587
17.	Implemented a new CLI command "/c/slb/virt x/service 53 dns/undirect ena|dis" to bypass BWM processing in the response path for the DNS UDP stateless service.	AL-53595
18.	Hid the internal address from the BE session table.	AL-53605
19.	The DNS responder replied to the DNS response with a malformed packet.	AL-54031
20.	Alteon failed to support the OID for Temperature sensor 3 and Temperature sensor 4.	AL-54703
21.	Using WBM, when dbind was set to enabled, when changing SSL-related configurations (as such the SSL policy), the dbind setting was changed to forceproxy.	AL-54708

Item	Description	Bug ID
22.	On a vADC, the perf_rec_2.tmp.old file utilized all of the disk space.	AL-54723
23.	In an SLB with pbind environment, when a service was configured with AppShape++ and alwayson, upon receiving the traffic the device rebooted.	AL-54730
24.	There was a discrepancy in the output hard disk between the CLI and WBM.	AL-54735
25.	In an ADC-VX environment, when VLAN sharing was enabled on a 5424 platform, traffic destined to the vADC was dropped.	AL-54745 AL-54746
26.	With virt sync disabled and a virtual service configured with a content rule, during configuration sync, devices being synced lost the content rule association with the virtual service.	AL-54749
27.	A vADC rebooted because of a software safe restart.	AL-54763
28.	In WBM, the password strength (pwscrit) menu was not included.	AL-54768
29.	On an Alteon VA, even though the disk space was increased, logs were issued regarding the storage capacity.	AL-54773
30.	The SSL inspection advanced virtual wire check was down when the IDS ports belonged to trunks.	AL-54914
31.	When a syslog message sent from Alteon did not use LF as delimiters, the vDirect traffic event was not triggered .	AL-54923
32.	The health check run-time instance was shared unexpectedly when several cntrules with different groups were defined under the same virtual service.	AL-54932
33.	Logs were added in relevant places that failed during key/certificate modification.	AL-55159
34.	Alteon sent incorrect parameters to the customer-hosted CAPTCHA/Block page.	AL-55168
35.	An error alarm was issued for PIP port usage.	AL-138281
36.	Exporting RSA key as a TEXT was encrypted using DES-ED	AL-138518
37.	When sending an FQDN update, the SSL-related configuration that was sent was still in progress and caused a configuration issue.	AL-138541

Item	Description	Bug ID
38.	Unexpected reboot	AL-138555
39.	Both Alteon devices panic at the same time, multiple times.	AL-138689 AL-138691
40.	Alteon sent a duplicate response for each ICMPv6 request sent to the device's interface IP address.	AL-138758

AppWall Bug Fixes

Item	Description	Bug ID
5.	Attack recorded in Passive state.	DE81421
6.	The Websec module down/up statistic was fluctuating.	DE81882
7.	Customer request was blocked with transactionID 0 and no event being generated.	DE82183
8.	Query about discrepancy between documentation and error message on Parameters Filter refinement.	DE82374
9.	Traffic was not sent to the back-end when integrated WAF had the “Subsystem stopped” Init event, reported on “Subsystems – Escalation”.	DE82382
10.	Filtering forensics view by URI returns nothing and cause web page freeze.	DE82455
11.	Customer unable to visualize the GeoMap dashboard in AppWall 7.6.17.1.	DE82787
12.	Server Request failed with status code 500.	DE82865
13.	API Discovery caused overwrite of HTTP Properties.	DE83555
14.	The DefensePro connection failed when the user clicked the Check button, even though AppWall was able to reach the DefensePro device.	AW-11611
15.	The DefensePro connection failed when the user added a DefensePro device.	AW-11615
16.	In rare cases, when a security apply is performed, AppWall can get stuck for 35 seconds.	AL-49522
17.	The **GeoLocations.dat** file should not have been included when config backup is taken from the Alteon WBM or CLI.	AW-14707

Fixed in 32.4.14.50

General Bug Fixes

Item	Description	Bug ID
1.	Alteon SSH failed a security audit.	DE79481
2.	The CDP group table became empty when deleting one entry case.	DE81636
3.	The static NAT for GRE traffic in point-to-point was incorrect.	DE81780 DE81786
4.	Alteon failed to support the OID for Temperature sensor 3 and Temperature sensor 4.	DE81861
5.	The VLAN 2090 error was assigned to more than 32 PIPs.	DE81973
6.	The DNS responder replied to the DNS response with a malformed packet.	DE82040
7.	The SSL inspection advanced virtual wire check was down when the IDS ports belonged to trunks.	DE82094
8.	Using WBM, when dbind was set to enabled, when changing SSL-related configurations (as such the SSL policy), the dbind setting was changed to forceproxy.	DE82162 DE82168
9.	On a vADC, the perf_rec_2.tmp.old file utilized all of the disk space.	DE82196
10.	In an SLB with pbind environment, when a service was configured with AppShape++ and alwayson, upon receiving the traffic the device rebooted.	DE82280
11.	The FQDN real indexes changed during get config.	DE82348
12.	Logs were added in relevant places that failed during key/certificate modification.	DE82361
13.	There was a discrepancy in the output hard disk between the CLI and WBM.	DE82392
14.	When a syslog message sent from Alteon did not use LF as delimiters, the vDirect traffic event was not triggered .	DE82415
15.	When the capture -M command was run on very large secrets files, the disk became full. Now the secrets file size is limited during capture -M execution.	DE82469 DE82475

Item	Description	Bug ID
16.	Alteon sent incorrect parameters to the customer-hosted CAPTCHA/Block page.	DE82738
17.	On a KVM VA, health checks to AppWall and nodejs failed in single IP mode.	DE82826

Fixed in 32.4.14.0

General Bug Fixes

Item	Description	Bug ID
1.	On DPDK virtual platforms, traffic passing thorough BWM shaping contracts caused invalid buffer access and caused the vADC to reboot.	DE79045
2.	SANs fields greater than 1024 bytes were accepted while generating a CSR.	DE80138 DE80141
3.	After upgrading from version 30.5.3.0 to 32.4.6.0, VLANs displayed as Down.	DE80315
4.	After downloading and uploading a configuration via REST API, SlbNewCfgFQDNServerTable was empty.	DE80344
5.	An SSLi issue caused the device to reboot.	DE80416
6.	An incorrect GSLB DNS query refused a response for non-existing domains.	DE80449
7.	Logging the times command caused the device to reboot.	DE80601
8.	There was an AppShape++ namespace conflict when using rule Ids that end with digits.	DE80625
9.	SNMP trap 193 is returned for a disk space issue when it was not included it its MIB	DE80685
10.	The Secured Web Applications (secwa) pane did not display on a standalone device.	DE80691
11.	On an ADC-VX, the MP caused a reboot.	DE80815
12.	From the CLI, could not connect to real server via Telnet.	DE81208
13.	Using WBM, could not change the protocol TCP/UDP for port 389.	DE81258 DE81259

Item	Description	Bug ID
14.	The label in the output regarding MP memory for the `/i/sys/capacity` command was not clear. Changed the label from “mp memory” to “total device memory”.	DE81365
15.	The last digit of the year was missing in the output for some OIDs because arrayLength-1 was assigned with a Null character.	DE81374
16.	A RADIUS UDP health check was sent for RADIUS AA instead of the expected TCP health check when a non-standard destination port was defined.	DE81514
17.	When there is a shared resource (file) that is being accessed by two different operations (for example, putcfg and snmp), there was a bug in the state machine that is responsible for the synchronization, causing the device to reboot.	DE81556
18.	There were DNS errors in the Alteon MP logs.dns due to DNS resolution not being case-insensitive.	DE81598 DE81604
19.	Back-end SSL with client authentication using static RSA caused a bad MAC address.	DE81671 DE81676 DE81679

AppWall Bug Fixes

Item	Description	Bug ID
1.	Cannot change the tunnel operational mode to Passive.	DE78282
2.	Sensitive Parameters are not getting masked in Security Details but are getting masked in Raw Request Data.	DE78706
3.	AppWall GUI gets stuck and affects the Alteon GUI as well in versions 32.4.13 and 33.5.3 and 33.0.6.5.	DE79700
4.	Error in the GUI when accessing Vulnerabilities.	DE79955
5.	File Upload security filter is detecting false-positive.	DE80620
6.	AppWall is trimming requests payload based on Content-Length header value.	DE81172
7.	AppWall does not send complete hostname in the security syslog message.	DE81249

Fixed in 32.4.13.50

General Bug Fixes

Item	Description	Bug ID
1.	Could not configure filtpbkp in hot-standby mode. Modified the CLI validation to resolve the issue.	DE78562 DE79212
2.	Interface 256 could not be selected for switch HA advertisements.	DE78888 DE78890
3.	Using WBM, an update to the cipher list was greater than 256 characters and was not accepted.	DE78976 DE78978
4.	The Unit label for a rule level timeout was different between WBM and the CLI.	DE79008 DE79010
5.	There was high SP memory utilization during a low traffic period.	DE79054 DE79056
6.	Getting the vADC partition size failed and caused the vADC to hang on restart.	DE79115 DE79116
7.	After running /stats/slb/pip, the SNMP OID was missing from the output.	DE79216 DE79218
8.	VPN connectivity failed because of the IKE and the ESP sessions being bound to different servers.	DE79224 DE79225 DE79227
9.	Could not enter the hyphen (-) character in the New Host to Replace field on the **Application Delivery > Virtual Services >Virtual Services of Selected Virtual Server > HTTP Content Modifications >HTTP Rules >URL Match & URL Action** pane.	DE78528 DE79233
10.	Using WBM, the hard disk capacity displayed incorrectly because secondary disk size was not counted.	DE79247 DE79250
11.	SNMP walk failed because the OID did not increase.	DE79426 DE79427 DE79429

Item	Description	Bug ID
12.	An AppShape++ script trying to insert a script greater than 50k characters into the **cmdLogMP-1-1** file caused the device to reboot.	DE79538 DE79540
13.	If PIP processing or session mirroring is enabled if the Alteon device is identified as the backup device with server processing disabled, the frame received from the server needs to be forwarded.	DE79587 DE79593
14.	System analytics were sent with null data.	DE79613 DE79615
15.	When setting the time zone by name and not changing the default NTP time zone, a warning is issued after the Apply.	DE79794 DE79796
16.	When **clsaging both** is enabled with tunnels, the device rebooted.	DE79825 DE79827
17.	The application services engine was not synchronized with the current configuration and the change was not saved.	DE79838 DE79840
18.	In an SLB and PIP environment, there was a discrepancy in the PIP statistics between /st/slb/pip and /st/slb/aux.	DE80121 DE80122 DE80124
19.	The traceroute response packet was sent by Alteon with the wrong interface.	DE80186 DE80188

Fixed in 32.4.13.0

General Bug Fixes

Item	Description	Bug ID
1.	On an Alteon VA device, in some cases SSH and WBM connections failed due to the non-availability of free virtual memory.	DE76265
2.	The Throughput threshold license caused an error even though the high threshold had not been reached.	DE76313
3.	When accessing the tunnel meta header of a frame for non-tunnel traffic with filter reverse session support, the device rebooted.	DE76380 DE76384

Item	Description	Bug ID
4.	Bandwidth Management (BWM) did not restrict upload bandwidth.	DE76718
5.	Configuring 3044 real servers caused high MP CPU and LACP problems.	DE76788 DE76789
6.	The device ran out of Heap memory, causing it to reboot.	DE76885
7.	In an SLB environment with dbind forceproxy and dbind ena, the device rebooted unexpectedly.	DE77024
8.	Changing the SIP from network class to subnet/network in a filter was not updated in the configuration.	DE77187 DE77188
9.	When configuring the action in an HTTP modification rule, the Alteon action was not validated correctly.	DE77277
10.	No data was received from Alteon for LinkProof Analytics	DE77437
11.	The device rebooted because of an issue with nsgroup auto-completion.	DE77456
12.	The device rebooted because of hardware Watchdog issues.	DE77487
13.	The DNS persistence cache cleared on Apply of GSLB changes. An alert was added to display when this occurs.	DE77516 DE77517
14.	Generating tech data could take a long time.	DE77625
15.	vDirect issued an error for table SpMemUseStatsTableEntry using SNMP.	DE77641
16.	MP CPU utilization was high, causing the device to reboot.	DE77727
17.	With a BWM rate limiting contract assigned to a forceproxy service, when AppXcel sent a frame to the client/server, the contract information stored in the frame was overwritten with the default contract, causing a failure with BWM enforcement.	DE77824
18.	After changing the user role from User to Web AppSecurity Viewer without submitting the change, associating a Web application resulted in an error message which was not clear.	DE77899 DE77900
19.	Importing the configuration resulted in a missing bitmap handling.	DE77914
20.	The device rebooted with the following error: SIGSEGV(11) thread STAT(tid=71)	DE77944 DE77945

Item	Description	Bug ID
21.	When applying configuration changes unrelated to the SLB module, the nbind session table entry erroneously cleared.	DE77950
22.	When performing a simultaneous operation of import and apply config, changes were displaying in diff.	DE77995
23.	There was an issue with the Connection module handling traceroute packets.	DE78002
24.	When a packet capture running on a data port stopped, the device rebooted.	DE78058
25.	The vADC iprep setting was lost after performing a reboot.	DE78114
26.	The device rebooted when executing a diff from SNMP.	DE78153
27.	In an outbound LB environment, the source port of the connections was changed, leading to traffic failure.	DE78210
28.	The device rebooted because of the Hardware watchdog	DE78676
29.	A random reboot was analyzed and fixed.	DE78923 DE78924

AppWall Bug Fixes

Item	Description	Bug ID
1.	The database filter removed part of the refinements, and only regex refinements remained.	DE75781
2.	There were cases (only in version 7.6.17 for a few signatures) where traffic was blocked although the signatures were refined.	DE76455
3.	In rare cases, POST requests were blocked.	DE76522
4.	In the integrated AppWall platform, the security events were not using the correct syslog facility.	DE77260
5.	In rare cases and under specific conditions, AppWall restarted.	DE77492
6.	GEO blocking was conducted to false positive.	DE77880

Fixed in 32.4.12.50

General Bug Fixes

Item	Description	Bug ID
1.	A misleading license error message was issued.	DE76142 DE76413 DE76147
2.	A search operation did not work correctly.	DE76186 DE76190
3.	In WBM, after Submit, SSH keys is incorrectly displayed as Do Not Erase.	DE76218 DE76219 DE76223
4.	The management port status of eth0 and eth1 displayed incorrectly.	DE76256
5.	After upgrade, running the /boot/cur command displays the image download date incorrectly.	DE76393 DE76397
6.	In WBM, the configured Server Side Idle Timeout values were not displayed.	DE76500 DE76504 DE76505
7.	Generating applogs resulted in high MP CPU utilization. A new warning message regarding this is now issued when running the /maint/applog/showlog command.	DE76527 DE76531
8.	Traffic was sent to a real server when the real server health check failed due to its related buddy server failing.	DE76545 DE76549
9.	Features that in the background automatically created virtual servers sometimes caused the High Availability configuration to be different between the HA devices.	DE76553 DE76557
10.	Changing a health check for LDAP(s) caused a reboot.	DE76641 DE76645
11.	Configuration sync issued caused the device to reboot.	DE76656 DE76660
12.	IPC module issue caused the device to reboot.	DE76757

Item	Description	Bug ID
		DE76758
13.	Syslog servers and protocol definitions were saved in the vADC configuration but were not actually used when delegated from the ADC-VX to the vADCs.	DE76963 DE76968
14.	When generating techdata, the techdata creation failed.	DE77063 DE77067

Fixed in 32.4.12.0

General Bug Fixes

Item	Description	Bug ID
1.	Using SSH, there was no matching key exchange method found when connecting from Ubuntu 20.	DE70421 DE70426
2.	An Alteon cluster running on Azure had high availability issues.	DE72942
3.	PCI compliance with Alteon SSH failed.	DE74373
4.	The device restarted by a software panic.	DE74394 DE74395 DE74399
5.	vADC buffer memory related to SSL caused a reboot.	DE74588
6.	An SSH management connectivity issue occasionally caused a reboot.	DE74604 DE74605 DE74609
7.	On a vADC, the GET /config/SlbCurCfgEnhVirtServicesTable message was received during config sync and all hash tables were initialized (zeroed), causing a reboot.	DE74687
8.	A vADC stopped processing production traffic.	DE74787
9.	Alteon VA devices deployed in Hyper-V experienced high CPU usage compared to other hypervisors.	DE74931
10.	After inserting a 1 G GBIC, message logs did not display.	DE75057
11.	After rebooting, configuration sync failed, and the configuration was stuck in diff with the same error.	DE75225 DE75226

Item	Description	Bug ID
12.	When trying to use Single IP in Azure, a message was issued that the user should use Multiple IP address mode.	DE75283
13.	After an Apply failure due to an empty passphrase for certificates, after reboot the entire configuration went into diff.	DE75334
14.	There was duplicate entry validation error for two domains where one had a hostname, and the other did not have a hostname.	DE75354
15.	When using the Russia time zone, the incorrect time displayed for the /info/sys/time command and in AppWall Forensics.	DE75400
16.	On a vADC, when executing SSL stats commands, the vADC rebooted.	DE75444 DE75445
17.	After the primary real server was activated in a group, the session handled by the backup real server was fastaged.	DE75534
18.	An SSH management connectivity issue occasionally caused a reboot.	DE75548 DE75549
19.	When gathering the device output, memory stats information did not appear in the techdata.	DE75685
20.	The client certificate went through OCSP verification even though it is in OCSP stapling mode.	DE75805
21.	SNMP polling resulted in an incorrect response.	DE75837
22.	The DNS Cache per IP version feature was not working	DE75976 DE75977

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

Item	Description	Bug ID
6.	Protected applications behind AppWall went down suddenly.	DE75232
7.	Under certain conditions, no explanation is provided in the Forensics API Security event.	DE75513
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
10.	Failure to update the GEO file.	DE74563
11.	In API Protection, AppWall identifies parameters as "required" even when they are not in the uploaded file.	DE74572
12.	Failure occurs with unexpected headers in the server response.	DE74998
13.	AppWall Management REST for Allow-List misinterpreted a wildcard in the configuration.	DE75050

Fixed in 32.4.11.50

General Bug Fixes

Item	Description	Bug ID
1.	On an Ubuntu 18 VA device, when selecting a time zone GMT offset greater than 4 hours, the GEL license activation failed.	DE73644
2.	Application delivery features were not available via API for the slbviewer user role.	DE74196 DE74197 DE74201
3.	When an IPv6 virtual server used IPv4 servers for load balancing and if any SLB config apply was performed, the existing sessions were closed.	DE74224 DE74225 DE74229
4.	An Alteon 5224 device rebooted because of a power cycle.	DE74350 DE74351 DE74355
5.	There was a Switch HA failover issue.	DE74512 DE74513 DE74517

Item	Description	Bug ID
6.	The wrong time zone offset was sent to the NTP server.	DE74634 DE74635 DE74639 DE74975
7.	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.	DE74759 DE74763
8.	The MP CPU utilization was high with DNS packets (dport 53).	DE74807 DE74808 DE74812
9.	When configuring network settings, an internal error was issued.	DE74817 DE74821
10.	On an ADC-VX, an LACP issue was caused by high MP CPU utilization.	DE74843 DE74847
11.	When the device started after a reboot, it stopped performing ARP base health checks.	DE74864 DE74865 DE74869
12.	Using SNMPv3, the “Unknown user name” is now issued for invalid usernames and invalid passwords.	DE74946 DE74947 DE74951
13.	The maximum supported length of the RADIUS password is 16 characters. Authentication failed If the password was configured with more than 16 characters.	DE74797 DE74801
14.	From WBM, when the SSH key was set to be deleted, after clicking Submit it was immediately deleted before the device was rebooted.	DE75018 DE75019 DE75023
15.	The device rebooted because of a software panic.	DE75036 DE75037 DE75041
16.	The Ext.HC script did not generate traffic.	DE75006

Item	Description	Bug ID
17.	Changing vADC CUs caused syslogs to be removed.	DE75087 DE75091
18.	AppWall LDAP connection failures were caused due to the multiple creation of MP processes.	DE75154 DE75158
19.	On an Alteon VA, packets larger than the negotiated MTU size were forwarded.	DE75426 DE75519
20.	The /oper/slb/group command displayed different output when two SSH sessions were opened to a single device.	DE75483

Fixed in 32.4.11.0

General Bug Fixes

Item	Description	Bug ID
1.	A user was allowed to configure a duplicate Static ARP entry using WBM, but not the CLI.	DE72183
2.	Bandwidth utilization was displayed incorrectly as Mbps, when it should have been MBps.	DE72623
3.	An Alteon NG 5424-S rebooted because of a BSP problem with the monotonic timer.	DE72987
4.	Alteon VA version 33.0.4.0 using Ubuntu12 rebooted on the execution of the Display Certificates Group configuration.	DE73036
5.	There was an error with traps for IPv6-related events.	DE73066
6.	A request to make to increase the height of the "Configuration Sync - Peers" in WBM.	DE73189
7.	A DNS responder with delegation for TCP session did not close.	DE73210 DE73211
8.	In a WANlink environment, traffic was processed by ISP, which was down.	DE73233
9.	Disk space exceeded the high threshold with 80 % usage because of the AppWall cores.	DE73248
10.	On a version 30.5.22.0 vADC, FQDN resolution update failed.	DE73305

Item	Description	Bug ID
11.	A health check timeout failure caused a reboot due to a race condition when freeing the object.	DE73534 DE73535
12.	Fixed Ansible documentation in alteon-device-facts.	DE73621
13.	Continuous operations on real server groups (additions, deletions, amendments) could lead to an internal OOS state.	DE73663
14.	In an Alteon VA environment, occasionally empty syslog messages were generated when the size exceeded 1300 bytes.	DE73747
15.	On a vADC, inbound host-based LLB rules were not created using the LinkProof menu due to RBAC issues.	DE73772 DE73773
16.	Trying to add vADC licenses to the ADC-VX when vadcadv had a custom flavor caused an error.	DE74075

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 32.4.10.50

General Bug Fixes

Item	Description	Bug ID
1.	The IPv6 static route failed if the respected interface was configured with the same Apply.	DE67580 DE67581
2.	Mirrored session statistics were not updated for Smart NAT Inbound traffic.	DE71992 DE71993 DE71997

Item	Description	Bug ID
3.	When the real and virtual server statistics were incremented or decremented the logs were not updated.	DE72084 DE72085 DE72089
4.	Using WBM, expired certificates could not be exported because there was a validation check on the “validation period” (1 to 3650).	DE72165 DE72166 DE72170
5.	Upgrade failed because of incorrect resource allocation (SP and AW cores).	DE72281 DE72285
6.	When trying to change the Traffic/AppWall capacity units (CUs) for a single vADC, an error occurred.	DE72343 DE72347
7.	In an IPV6 environment, when Static NAT was configured, ICMP traffic failed.	DE72399 DE72400 DE72404
8.	IPsec sessions abruptly aged out due to an incorrect interpretation of TCP flags.	DE72424 DE72428
9.	An Open SSL vulnerability (CVE 2022-0778) was fixed.	DE72460 DE72464
10.	When updating a configuration with idbynum enabled, an error occurred.	DE72507
11.	An HA failover caused SIP packets to be lost.	DE72527 DE72531
12.	When there was an overflow of the Current Sessions value, unexpected statistics of Available Sessions and DNS answer resulted .	DE72556 DE72557 DE72561
13.	In CLI, Bandwidth Utilization displayed as MBps, when it should have been Mbps.	DE72622
14.	After upgrade, the configuration was not preserved.	DE72652 DE72656

Item	Description	Bug ID
15.	In and ADC-VX environment, when executing putconfig and tech data collection at the same time on a vADC, the vADC rebooted.	DE72661 DE72665
16.	When there was a TCB block leak, DSSP health checks failed.	DE72724 DE72728
17.	The Ansible module description of vip_health_check_mode was incorrect.	DE72818 DE72822
18.	Using APSolute Vision the Alteon EAAF data base of was not updated.	DE72825 DE72829
19.	VRRP did not sending advertisements because the VR state was incorrected checked.	DE72841
20.	The AppWall nodejs module flapped on virtual platforms in the following cases: 1. When there are more than 10 vADCs 2. When vADCs are configured with the basic flavor.	DE72860 DE72864
21.	The Persistency gmetric was not working correctly.	DE72967
22.	Cookie-based real server selection caused a reboot. Defensive code was added to address the issue.	DE73087 DE73088
23.	On a version 30.5.22.0 vADC, FQDN resolution update failed.	DE73309
24.	On an Alteon VA, intermediate certificates were not fetched.	DE73341 DE73344

Fixed in 32.4.10.0

General Bug Fixes

Item	Description	Bug ID
1.	The special Regex character '\' '\\' should be added.	DE69955
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.	DE69964
3.	The MP CPU utilization was high when applying the configuration, causing a network interrupt.	DE70611
4.	A mixed type SNS request failed (dnsrespoder VIP IPv4 and query type IPv6, and vice versa).	DE70701 DE70702

Item	Description	Bug ID
5.	An unexpected VRRP failback when preemption is disabled.	DE70745 DE70746
6.	A panic occurred due to memory corruption.	DE70772
7.	Alteon displayed inaccurate SFP Tx and Rx power values.	DE70784
8.	The max_cipher_list_length was increased from 16000 to 20000.	DE70965
9.	The “Threshold of incoming sessions" event was generated when the total active connections were much lower than the maximum value.	DE71106
10.	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.	DE71266
11.	After resetting a non-debug Alteon VA platform, GEL licenses sometimes were lost when they passed non-GEL applicable validations.	DE71293
12.	Fixed the License Manager connection failure algorithm.	DE71352
13.	The LINK LED remained ON even when the optical cable was pulled off or the ACT LED was not working.	DE71472
14.	The file descriptor was allocated and not released during execution of SP/MP profiling./maint/debug/cpuProfiling/	DE71501
15.	A MAC flap occurred because of VRRP advertisements sent by the backup Alteon device.	DE71520 DE71521
16.	When an AppShape++ script was applied with cmd logging enabled, Alteon rebooted.	DE71527
17.	The GEL license logs were generated every 5 minutes, causing memory leaks.	DE71580
18.	Support of stapling and client certificate verification added.	DE71592 DE71593
19.	Alteon could be down when a specific traffic pattern request interacted with the redirect service using dynamic tokens.	DE71618
20.	On a vADC device, the MP CPU reached 100%.	DE71655
21.	When a DPDK image reset, an unexpected DNS server IP address was added by BSP.	DE71755

Item	Description	Bug ID
22.	After the AppWall health check failed, the MP restarted AppWall every 15 seconds .	DE71819
23.	The Application Services engine was not synchronized with the current configuration.	DE71838 DE71839
24.	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.	DE71898
25.	Could not allocate memory to run the diff command.	DE71905
26.	Could not create an LLB inbound rule.	DE71972 DE71973
27.	Attempting to delete a server or CA certificate group explicitly or implicitly resulted in an AX internal OOS failure.	DE72198 DE72199

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 FileUpload filter and reported as PUT.	DE70675
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

Fixed in 32.4.9.50

General Bug Fixes

Item	Description	Bug ID
1.	With IDS chain configured, ICMP responses from the server were not forwarded to the client.	DE70043 DE70044

Item	Description	Bug ID
2.	In an HA environment with a virtual service configured with an AppShape++ rule, the backup device rebooted when that configuration was synched to the backup.	DE70161 DE70162
3.	FQDN real server IP addresses incorrectly ended with a period (".").	DE70252 DE70256
4.	Rebooting an ADC-VX caused vADCs to be stuck in the initialization stage.	DE70261 DE70262 DE70266
5.	The ICMPv4 real server health check failed while a CLI ping worked correctly. A v4 debug command was added.	DE70301 DE70305
6.	A user was locked out after making a password change.	DE70323 DE70327
7.	The TLS 1.3 protocol did not display in the Backend SSL policy.	DE70443 DE70444 DE70448
8.	The XFF code in the HTTP/2 proxy used the VIP instead of the Client IP address.	DE70458 DE70459 DE70463
9.	The AppWall check did not recognize that AppWall was frozen and did not restart AppWall.	DE70468 DE70472
10.	Configuration sync failed due to a long certificate group ID.	DE70486 DE70490
11.	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.	DE70512 DE70513 DE70517
12.	A panic occurred during a packet capture.	DE70541 DE70542 DE70546

Item	Description	Bug ID
13.	The HTTP/2 health check did not contain the ALPN protocol in the SSL handshake.	DE70590 DE70595
14.	After an unexpected reboot of Alteon VA on ESXi 7.0, could not save changes after Apply, and received error messages.	DE70598 DE70602
15.	After upgrade, empty groups with no real server added to them could shift the group index map.	DE70630 DE70631 DE70635
16.	The ARP table information was not the same between the CLI and WBM.	DE70687 DE70688 DE70692
17.	Could not manually delete a session table entry for VPN traffic.	DE70801 DE70802 DE70806
18.	Uppercase characters were, incorrectly, added to HTTP headers for HTTP/2 proxy, which generated the following error: `Upper case characters in header name`	DE70810 DE70811 DE70815
19.	An SLB apply took longer to execute when it was run as SLB config apply.	DE70997 DE70998
20.	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.	DE71069 DE71070 DE71074
21.	When running dbind disable service, a panic occurred when Alteon received the RST packet from the server.	DE71112 DE71113 DE71117
22.	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.	DE71132 DE71133 DE71137
23.	Enabling IPv6 on a virtual server caused a panic.	DE71148

Item	Description	Bug ID
		DE71152

AppWall Bug Fixes

Item	Description	Bug ID
1.	Under some conditions, long header Hostnames led to a syslog failure.	DE70821
2.	The APSolute Vision AppWall dashboard displayed wrong data	DE70207

Fixed in 32.4.9.0

General Bug Fixes

Item	Description	Bug ID
1.	Wrong management of TSO buffers and logs flood from the AE module caused a panic.	DE66432
2.	On an Alteon-VA platform with BWM configured, when switching from DPDK to TUNTAP, in some instances a software panic occurred.	DE68859
3.	Alteon 6420 running on version 32.4.6.50 rebooted due to a software panic	DE68955
4.	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.	DE69008
5.	A MAC flap occurred because of HA advertisements sent by the backup Alteon device.	DE69140
6.	Because of a vulnerability, upgraded to the latest Nginx version.	DE69160 DE69161
7.	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.	DE69251
8.	On an Alteon 6024 platform, the primary and secondary devices rebooted automatically due to a stack overflow.	DE69294

Item	Description	Bug ID
9.	upThroughputBitsPs and downThroughputBitsPS were incorrectly calculated.	DE69332
10.	When attaching or detaching an SSL policy, the wrong port changed.	DE69393
11.	On an Alteon 6420 platform, there was a data transmission problem with packet fragmentation with a one-minute delay.	DE69402
12.	On a 7612 platform, after a vADC was enabled there was a large VS address delay.	DE69412
13.	After upgrading from 32.6.3.50 to 32.6.6.0, there was latency/delays.	DE69416
14.	When a DNS Response was received with new IP addresses and new real servers created, the Save flag was set to ON.	DE69420
15.	In a BGP, BFD environment, BFD connections went down when BWM processing was enabled, leading to BGP adjacency going down.	DE69438
16.	Config apply took more than 10 minutes.	DE69477
17.	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.	DE69495 DE69496
18.	When configuring cntclss values, a max length validation failure did not display the correct error.	DE69508
19.	Ansible Alteon device fact gathering failed due to an unsupported field in some Alteon versions.	DE69528
20.	In an ADC-VX environment, trying to create vADC 10 caused a panic.	DE69547
21.	Could not view the connection statistics in both WBM and CLI.	DE69592
22.	Could not configure the user role WSAdmin in SA mode.	DE69638 DE69639
23.	In an SLB environment with VLAN level proxy configured, in some instances the MAC flapped after an SLB config apply.	DE69666
24.	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.	DE69698

Item	Description	Bug ID
25.	When creating a content class, a panic occurred.	DE69766 DE69767
26.	In a tunnel environment, all configured tunnel static route tables did not display under the route dump.	DE69830
27.	Ansible facts gathered from standalone devices did not provide the correct image list.	DE69868
28.	After reboot, Alteon falsely reported that the MGMT IP address was changed.	DE69942 DE69943
29.	The special character '\' was added to the REGEX string '\\'.	DE69956
30.	Alteon 5208 rebooted because of a software panic.	DE69995
31.	Alteon displayed a configuration as pending, but would not accept an apply or save. This was because a group associated with fqdnreal was empty.	DE70057
32.	The dns-responder with DNSSEC did not work on Cavium platforms since version 32.6.0.0.	DE70112
33.	An Alteon D-5208S platform abnormally rebooted because of a software panic.	DE70230 DE70231 DE70235 DE70236

AppWall Bug Fixes

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

Fixed in 32.4.8.50

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.	DE66269 DE66270
2.	An Internal out-of-sync configuration was detected.	DE68007 DE68008
3.	In an HA environment, after the backup device rebooted, FTP data sessions disappeared intermittently on the backup device.	DE68025
4.	Config sync failed with EC certificates in the configuration.	DE68185
5.	After user-defined ciphers, the Application Services engine was not synchronized with the current configuration.	DE68191 DE68192
6.	After user-defined ciphers, the Application Services engine was not synchronized with the current configuration.	DE68220 DE68221
7.	When the MRST flag was set to on, it was not possible to disable a data port.	DE68251 DE68254
8.	A port disabled in a saved configuration needed to be toggled twice to bring it up after reboot.	DE68268 DE68271
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.	DE68277 DE68280
10.	Alteon forwarding or routing packets without SRC MAC translation led to a MAC flap issue.	DE68296 DE68297
11.	Using the WBM, after creating a vADC, the vADC stayed in the init state.	DE68399 DE68402
12.	Alteon responded to Non-RFC compliant responses for DNS requests.	DE68405 DE68406 DE68409
13.	When the WANlink server was operationally disabled and then re-enabled, the WANlink peak statistics were incorrect.	DE68438

Item	Description	Bug ID
		DE68439 DE68442
14.	Using APSolute Vision, newly created vADCs were not manageable.	DE68610 DE68613
15.	Password Strength not available in WBM but was available in the CLI.	DE68777 DE69778 DE68781 DE68783
16.	After upgrading to version 32.6.5.0, vADCs could not be managed by the APSolute Vision server.	DE68791 DE68794
17.	On an Alteon 5424 (ODS-LS2) platform, the real server capacity in standalone and ADC-VX modes was increased in 8192.	DE68844 DE68847
18.	A software panic occurred followed by an AX Out-of-sync.	DE68880 DE68881
19.	Was not enable to sync the configuration between devices in the beta code.	DE68912 DE68914 DE68915
20.	Issue with FQDN servers. Logs were added to help with this issue.	DE68928 DE68931
21.	A panic occurred with a loss of the configuration. Fixed included not tracing empty DNS responses.	DE68944 DE68947
22.	The SIP INVITE went to the wrong real server.	DE68967 DE68968 DE68971
23.	Received the following error: `Configuration Error column slbCurCfgEnhContRuleBotMProcessing not found` For the fix, removed an unneeded entry that was ported by mistake.	DE69120 DE69121 DE69124

Item	Description	Bug ID
24.	During the tunnel handling routine, Alteon reboots with IP fragmented traffic.	DE69174 DE69177
25.	BM JS injection occurred when no BM was configured.	DE69197 DE69200
26.	While configuring CNTCLSS values, a maximum length validation failure did not display the correct error.	DE69507

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 32.4.8.0

General Bug Fixes

Item	Description	Bug ID
1.	The L4oper user could not view the Virtual Servers pane.	DE65787 DE65788
2.	The device became full with too many open files, causing it to run slowly.	DE66424 DE66425
3.	In OpenStack Alteon VA deployments, after upgrade sometimes the physical MAC was shuffled.	DE66510
4.	When passing the client certificate via the HTTP header in a multiline in compatible mode, the last hyphen (-) was removed.	DE67196

Item	Description	Bug ID
5.	The router ID was not visible for between routers for traceroute.	DE67259
6.	There was a WBM error for the SLBVIEW user.	DE67373 DE67374
7.	Using WBM, the DNS responder VIP displayed as up even if it was disabled by configuration.	DE67542 DE67543
8.	With VMAsport enabled, SSL-ID based persistency was not maintained correctly.	DE67632
9.	When traffic matches a filter that is configured with layer7 lookup, Alteon panicked.	DE67653
10.	Incorrect units displayed for uploading/downloading bandwidth for WANlink real servers.	DE67711 DE67712
11.	The network driver process was stuck and caused Linux core 0 to be stuck. This caused the MP to be stuck.	DE67716
12.	When deleting a group and the FQDN associated with that group, the group was deleted twice from the AX database.	DE67722
13.	There was a non-existing Rlogging policy on a disabled traffic event policy.	DE67728
14.	Added the extended FMAC option and the HA-ID to this version as it was not ported to the 32.4.x series.	DE67748 DE67749
15.	In WBM, the real server table displayed as empty.	DE67820
16.	Using AppShape++, when attaching/detaching a content class SSL from a filter, the AppShape++ command was removed and recreated, but the order was incorrect.	DE67831 DE67832
17.	AppWall init completion took a very long time.	DE67868
18.	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.	DE67899
19.	There was a crash in the external "nano messages" package.	DE67938
20.	The AppWall process took more time to start than expected.	DE68028 DE68029 DE68033

Item	Description	Bug ID
21.	In a virtual environment, configuration sync from the ADC-VX failed.	DE68059 DE68060
22.	An empty AVP prevented AppShape++ from parsing a RADIUS transaction.	DE68079 DE68080
23.	Some FastView configuration files were not updated as part of the new feature using FastView JS injection capabilities.	DE68087
24.	When the hold timer expired, Alteon sent a notification with a cease.	DE68092 DE68093 DE68313 DE68318

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 32.4.7.50

General Bug Fixes

Item	Description	Bug ID
1.	Too many core files took up too much disk space, resulting in techdata failing.	DE66121 DE66122
2.	In an RSTP environment, the port state transition from DISACRD to FORWARD was delayed.	DE66166 DE66167

Item	Description	Bug ID
3.	The SSL Hello health check caused a memory leak which led to a panic.	DE66189 DE66192
4.	The CRL could mistakenly be considered expired before the true expiration time because of the time zone.	DE66216 DE66219
5.	The exporter port 46000 was accessible through the Management IP address, and as a result it appeared in the vulnerability scan.	DE66269 DE66270 DE66273
6.	Alteon VA in DPDK mode crashed when BWM processing with BW shaping was enabled.	DE66396 DE66397
7.	After configuring a deny route for a DSR VIP with tunnels set to real servers, the MP panicked.	DE66470 DE66471 DE66474
8.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66478 DE66481
9.	Using WBM, when users of type 'user' was disabled, they could still successfully log in.	DE66527 DE66529 DE66532
10.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66571 DE66574
11.	Could not create a new BWM policy on a 4208 device.	DE66620 DE66621 DE66624
12.	Panic analysis.	DE66639 DE66642
13.	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.	DE66695 DE66698
14.	A panic analysis resulted in the following fix:	DE66702 DE66703

Item	Description	Bug ID
	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.	DE66706
15.	After a Trust CA group was configured, no other certificates could be deleted even if they were not part of the Trust CA group.	DE66719 DE66720 DE66723
16.	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.	DE66729 DE66732
17.	When AES128 or AES256 were configured as the privacy protocol, Alteon sent malformed SNMPv3 traps	DE66746 DE66747
18.	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.	DE66803 DE66806
19.	BGP neighborship did not get established because of issues with the AS number functionality.	DE66811 DE66814
20.	Using WBM, when refreshing the Virtual Services tab, the VS status displayed as Warning instead of UP.	DE66881 DE66884
21.	The user was unable to access Alteon WBM.	DE66890 DE66893
22.	Panic analysis.	DE66953 DE66954 DE66957
23.	Starting with this version, the SNMPv3 target address table is available in the Ansible module.	DE67002 DE67005
24.	When the SP CPU was activated, a false `Throughput threshold exceed` message displayed.	DE67122 DE67125
25.	Using WBM, real servers and groups are not displayed for HA tracking.	DE67274 DE67275 DE67278
26.	In WBM, HAID did not display properly.	DE67453

Item	Description	Bug ID
		DE67456

Fixed in 32.4.7.0

General Bug Fixes

Item	Description	Bug ID
1.	Could not enable the extended_log via Ansible.	DE63839
2.	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.	DE63989
3.	In the USM pane, added support for SHA2 and AES-256.	DE64024
4.	The real health check displayed different times in CLI and WBM.	DE64030
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	DE64089
6.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64150
7.	The MGMT port status was DOWN but the Link and operational status was UP.	DE64229
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.	DE64245
9.	Alteon VA had an internal leak that caused connections to drop out.	DE64254
10.	In an HA environment, when the RADIUS service was enabled with mirroring and associated with an AppShape++ script , RADIUS authentication timed out.	DE64318
11.	Applying part of the nginx when disabling the Web proxy took too much time.	DE64338
12.	When pbind clientip and vmasport were enabled, the persistent session was not permanently deleted.	DE64353

Item	Description	Bug ID
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."	DE64375 DE64377
14.	Added a REGEX to accept the dot (.), slash (/), and backslash (\) characters.	DE64454
15.	Added a REGEX for the path fields that accept special characters.	DE64462
16.	Config sync transmit was aborted between two devices when the sync request was received from a third device.	DE64484
17.	Predefined HTTP headers were used when POST HTTP health checks were sent without taking into the account the actual body length.	DE64521
18.	After receiving the same routes in BGP updates when Alteon failed to set a protocol owner, Alteon deleted the RIB.	DE64531
19.	Using WBM, ephemeral servers did not display in the Configuration menu.	DE64583
20.	After performing /boot/shutdown, TLS version 1.1 was incorrectly being set to enabled.	DE64594
21.	In a BGP environment, when BGP peers were directly connected, the BGP state stayed as Connect even though the local interface was disabled.	DE64645
22.	Using a logical expression health check resulted in an unexpected real server state.	DE64688
23.	Upgrading an ADC-VX generated the following error message on the console: write error: Broken pipe	DE64701
24.	The management Web server did not work due to a bug with the access SSL key on FIPS.	DE64729
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.	DE64755
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.	DE64784

Item	Description	Bug ID
27.	The Layer 2 system configuration had an incorrect BoardType for 7216NCX.	DE64886
28.	When real servers were down, Alteon sent traps with the wrong OID.	DE64897
29.	In an SLB environment, when the primary server failed, the secondary backup displayed as "UP" instead of "BLOCKED".	DE64921
30.	On a 7220 platform, when Alteon received a packet with a size greater than 1500, it panicked.	DE64944
31.	In DPS Perform mode, AppWall was not pushed to vADCs.	DE64994
32.	The weighted least connection was not correct.	DE65004
33.	When there was a state transition from backup to master, GARP was not sent.	DE65037
34.	There was an incorrect rule ID for retrieving statistics from the SP.	DE65175
35.	Added the FastView smfhub self-healing mechanism.	DE65199
36.	Defect that tracked DE65346 -- Device auto rebooted with reason of hardware watchdog.	DE65230
37.	Accessing a device using APSolute Vision or WBM caused a memory leak and eventually led to a panic.	DE65238
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.	DE65281
39.	Even though there were no open connections, new SSH connections were ignored with a "max connection reached" error.	DE65299
40.	The comparison function used to compare the SSL policy name was incorrect.	DE65315
41.	Added more information to the debug log when an ASSERT occurs on an ndebug image.	DE65342
42.	After performing config apply, GSLB DNS responses returned a remote IP address instead of a local VIP.	DE65362
43.	The MP CPU utilization was high when querying virtual stats.	DE65376

Item	Description	Bug ID
44.	A connection drop occurred because a virtual service was reset due to a virtual index mismatch after applying new configuration changes.	DE65401 DE65403
45.	SIP UDP service run by AppShape++ failed (it was used for persistency and/or Layer 7 manipulation).	DE65432
46.	On 5208/ODS-VL/VL2/non-DPDK platforms, a ping failed because the ARP reply was not transmitted back to requester by the ND. This caused the config sync to fail.	DE65439
47.	The Alteon Data interface with port range 40k-45k mistakenly was accessible from outside world.	DE65481 DE65483
48.	Even though the SP/MP profiling logic was disabled by default, Alteon panics with SP profiling logic being triggered.	DE65489
49.	Whenever multiple requests were sent with a cookie in a single session for multiple services, Alteon did not decrement the current session properly.	DE65499 DE65501
50.	Alteon displayed the diff and diff flash without any configuration changes.	DE65534
51.	Using RCA, there was an incorrect virt-sever ID display.	DE65565 DE65604
52.	AppWall crashed when not receiving the i/o time.	DE65572
53.	The SP performed unequal traffic distribution.	DE65602
54.	When burst traffic was sent to Alteon, some p-sessions remained in the zombie/stale state.	DE65661 DE65662
55.	Added support for the IF IP to connect to the service dashboard.	DE65679
56.	Added a maint debug CLI command to export the virtual stat service table to understand the cause of the virtual stats not working.	DE65703
57.	A new Regex command forbade a hyphen (-) by mistake.	DE65718 DE65719
58.	When an ARP entry is deleted, sending queued packets to the ARP entry after ARP resolution sometimes leads to an MP freeze and eventually leads to an MP panic.	DE65741

Item	Description	Bug ID
59.	In an RTSP environment, the RTSP service stopped working and all the SYN packets were dropped.	DE65745
60.	When all 24 GBICs were inserted, the Watcher timed out when ports were initiated.	DE65783
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.	DE65830
62.	Performing gtcfg via SCP resulted in a panic.	DE65855 DE65856
63.	Added the HW platform type MIBs for 6024, 5208, and 8420 to the MIB tree.	DE65863 DE65864
64.	On an Alteon VA, when displaying port speed and mode, Any was displayed.	DE65877
65.	When vmasport was enabled, the service ceased working.	DE65894 DE65895
66.	The AppWall service did not restart after being ended by the MP.	DE65915
67.	When BFD and tunneling were enabled, a panic occurred.	DE65999
68.	Using SNMP, OIDs errorCountersSpTable and eventCountersSpTable could cause Alteon to not be accessible via SSH or WBM.	DE66028
69.	With the command logging feature enabled, Apply/Save resulted in a panic.	DE66101
70.	While initiating the SSL client connection for the SSL health check, the vADC MP crashed.	DE66138
71.	Adding and deleting real servers or groups resulted in an AX Out-Of-Sync error.	DE66177
72.	The CRL could mistakenly be considered expired before the true expiration time because of the time zone.	DE66215
73.	Panic analysis.	DE66638

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 32.4.6.50

General Bug Fixes

Item	Description	Bug ID
1.	The random salt was a predictable random number generation function generating a similar sequence.	DE63658 DE63661
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.	DE63981
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.	DE63988
4.	In the USM pane, added support for SHA2 and AES-256.	DE64023
5.	The realhc stat had a different time between the CLI and WBM.	DE64029
6.	A 4208 platform displayed the option to convert into virtual (VX/ADC) mode.	DE64088
7.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64149
8.	When the MGMT port status was Down, the Link and Operational statuses were incorrectly Up.	DE64227 DE64228
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.	DE64243

Item	Description	Bug ID
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.	DE64316 DE64317
11.	Applying an operation took an inordinate amount of time.	DE64337
12.	A persistent session was not permanently deleted when pbind clientip and vmasport were enabled.	DE64352
13.	Added a REGEX to accept, dot (.), slash (/), and backslash (\) characters.	DE64452 DE64453
14.	Added a REGEX for the path fields that accept special characters.	DE64461
15.	There was a fix for CVE-2021-3449.	DE64468
16.	When the sync request was received from a third device, the config sync transmit was aborted between two devices.	DE64483
17.	Predefined HTTP headers were used when POST HTTP health checks were sent without accounting for the actual body length.	DE64520
18.	When Alteon failed to set a protocol owner, Alteon deleted the RIB after receiving the same routes in BGP updates.	DE64529 DE64530
19.	Using WBM, the ephemeral servers did not display in the Configuration menu.	DE64582
20.	After performing /boot/shutdown, TLS version 1.1 was incorrectly being set to enabled.	DE64593
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.	DE64643 DE64644
22.	Using a logical expression health check resulted in an unexpected real server state.	DE64687
23.	When upgrading an ADC-VX, the error message "write error: Broken pipe" displayed on the console.	DE64700
24.	The management Web server did not work due to a bug with the access SSL key on FIPS.	DE64728
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.	DE64753 DE64754

Item	Description	Bug ID
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.	DE64783
27.	There was an incorrect BoardType for 7216NCX in the I2 system configuration.	DE64885
28.	When real servers were down, Alteon sent traps with the wrong OID.	DE64895 DE64896
29.	In an SLB environment, when the primary server failed, the secondary backup displayed as UP instead of BLOCKED.	DE64920
30.	On a 7220 platform, when Alteon received a packet greater than 1500, Alteon panicked.	DE64942 DE64943
31.	AppWall was not pushed to a vADC in DPS Perform mode.	DE64993
32.	The weighted least connection was not correct.	DE65003
33.	When there was a state transition from backup to master, a GARP was not sent.	DE65035 DE65036
34.	There was an incorrect rule_id for retrieving statistics from the SP.	DE65173 DE65174
35.	On an Alteon VA, FastView treatments stopped working.	DE65197
36.	Using APSolute Vision or WBM to access a device caused a memory leak and eventually led to a panic.	DE65237
37.	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.	DE65280
38.	New SSH connections were ignored with a "max connection reached" error, even though there are no open connections.	DE65298
39.	The comparison function used to compare SSL policy names was incorrect.	DE65314
40.	Added more information to the debug log when ASSERT occurs on an ndebug image.	DE65340
41.	For SIP UDP traffic running with AppShape++ scripts (for persistency and Layer 7 manipulation), UDP sessions stopped working.	DE65431

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 32.4.6.0

General Bug Fixes

Item	Description	Bug ID
1.	Upon Submit, there was a Quick Service setup wizard internal error.	DE57038
2.	In WBM, the equivalent to the filterpbkp CLI command was missing.	DE59728
3.	Alteon did not forward traffic when LACP was disabled, and worked as expected when LACP was enabled.	DE61523
4.	There was no support for query type return errors even if the domain was found.	DE61642
5.	When starting up a vADC startup, the admin context froze and the Watcher killed the process, resulting in a panic.	DE61769
6.	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.	DE61942
7.	Port mirroring increased the SP CPU utilization.	DE62269
8.	Failed to access the Alteon WBM and the SSH connectivity was lost.	DE62310
9.	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.	DE62391

Item	Description	Bug ID
10.	Even after changing the log level from debug to error, warning messages continued to be issued.	DE62434
11.	With specific browsers, HTTP2 traffic with an uncommon form in the header was not answered.	DE62609
12.	Exporting a configuration from ADC-VX did not work.	DE62634
13.	Incorrect MTU syslog messages were issued for vADCs.	DE62661
14.	The packet capture timestamp was incorrect.	DE62731
15.	On an ADC-VX, the HW Watchdog rarely rebooted due to an unknown trigger.	DE62749
16.	While exporting techdata, IPv6 connectivity went down for a short while and then came back up.	DE62822
17.	When uploading a Layer 2 packet capture from an ADC-VX to the FTP server, Alteon panicked.	DE62852
18.	Using Ansible, could not configure the TLS 1_3 parameter.	DE62870
19.	There was vADC auto-reboot issue because of a software panic.	DE62945
20.	A config sync from a non-HA device to an HA-configured device caused the loss of the HA configurations.	DE62948 DE62952
21.	Health check tables were not supported for the l4 admin and slb admin users.	DE62975
22.	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.	DE63058
23.	A non-supported configuration caused a crash.	DE63072
24.	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.	DE63193
25.	In Ansible, it was not possible to remove one VLAN from all interfaces because the value "0" was not accepted.	DE63217
26.	When multiple VIPs are configured with srcnet, the ptmout value was not being considered.	DE63481
27.	When VIRT6 went down, when deleting the IPv6 SLB virt, Alteon panicked.	DE63543

Item	Description	Bug ID
28.	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.	DE63552 DE63557
29.	SSL statistics in the CLI and WBM did not match on Alteon running version 32.4.5.0.	DE63566 DE63571
30.	Fetching the routing table via REST API when the routing table was full caused a panic.	DE63588
31.	When a real server had an rport set to 0 and an rport ser to x, the service became unavailable.	DE63619
32.	After SSL Offloading was enabled, Alteon stopped accepting connections.	DE63630
33.	After changing the admin password and Applying, there were configuration sync issues with the peer.	DE63759
34.	Using CLI, after running the /stats/slb/virt command, backup real servers did not display.	DE63800 DE63803
35.	After changing a group on an FQDN server, the servers were bound to the older group as well as the new group.	DE63833
36.	After a signal panic, Alteon stopped booting.	DE63891
37.	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.	DE63905 DE64069
38.	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.	DE63982
39.	Alteon VA did not initiate a BGP connection to a peer.	DE63987
40.	SHA2 and AES-256 support for SNMPv3 is missing in version 32.4.5.50.	DE64022
41.	On the 4208 platform, the option to convert to virtual mode (ADC-VX) was mistakenly available.	DE64087
42.	After Alteon received a packet and tried to open a session entry, an incorrect initialization of a pointer resulted in a NULL access and Alteon panicked.	DE64188

Item	Description	Bug ID
43.	Peer Alteon devices panicked due to vulnerability to CVE-2021-3449.	DE64469

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 32.4.5.50

General Bug Fixes

Item	Description	Bug ID
1.	Snmpbulkwalk on the capacityUsageStats node returned invalid OID output.	DE62232 DE62233
2.	In rare circumstances during tsdmp or techdata export, a panic would occur.	DE62553 DE62557
3.	In an HA environment, synching the configuration to the peer device with sync tunnel config flag disabled results in the peer panicking.	DE61965 DE61966 DE62008 DE62013

Item	Description	Bug ID
		DE62014
4.	A ticket from a failed connection required passing over the authentication policy on the next connection.	DE62484 DE62487
5.	After upgrading to version 31.0.13.0, uneven load balancing started.	DE62336 DE62468
6.	In a DSR and multi-rport configuration environment, the /stat/slb/virt X command returned statistics as 0.	DE62344 DE62348
7.	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.	DE61875 DE61881
8.	Using WBM, there was a display issue when modifying a virtual service with actionredirect.	DE61595 DE61600
9.	When while handling malicious DNS packet with compression pointer loops, Alteon panicked.	DE62131 DE62136
10.	There were no Mibs for the health check count to display them for the command /info/sys/capcityswitchCapHealthCheck MaxEntswitchCapHealthCheckCurEnt.	DE61741 DE61742
11.	Using WBM, when configuring the Nameserver group under DNS Authority, the table name in the mapping file was incorrect.	DE61479 DE61484 DE61485
12.	vADCs did not process SSL traffic.	DE61692 DE61695
13.	There was no support for query type return errors even if the domain was found.	DE61253 DE61254
14.	When the user sent traffic, a throughput high alert message was issued even though the throughput was less than the configured throughput threshold limit.	DE61981
15.	When Alteon had high MP memory utilization, restarting caused configuration loss. Alteon came up with the default configuration.	DE61206 DE61207
16.	When resolving a DNS PTR record, IP matching was skipped (for both hostlk enabled and disabled) if the service hostname	DE60810 DE60941

Item	Description	Bug ID
	was not configured. Now, the service hostname check is skipped only if the hostlk is disabled.	
17.	When a syslog file had long log messages, the /info/sys/log command did not display any log messages.	DE60886 DE60887
18.	During configuration export, creating the AppWall configuration failed, and as a result the entire operation failed.	DE60950 DE60951
19.	The default STP group was not available for a newly added physical VM port.	DE61298
20.	The serial number was missing in the output for the /info/sys/general command.	DE61675 DE61676
21.	When sending an OCSP request over the management port, there were two leaks.	DE60850 DE60851
22.	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.	DE61343 DE61344
23.	In a DPDK VA environment with two NUMAs, packets were not tunnel-processed when they were VMAed to and SP of a different NUMA.	DE60627 DE60630
24.	If Alteon received a request when all real servers were down, the group with all the real servers' indexes less than 33 and the RR, BW, or response metric failed to select a real server, even if they came up.	DE61140 DE61145
25.	When the management WBM listener connection control block was closed during its validation, a 50X WBM error displayed.	DE60914 DE60915
26.	Following a set of SNMP operations, on some occasions Alteon panicked from a memory corruption with a boot reason power cycle.	DE61044 DE61045
27.	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	DE61095 DE61096
28.	When the SSH connection with the correct password was attempted for a locked user, the user lockout status was checked too late.	DE60702 DE60703

Item	Description	Bug ID
29.	AppWall was stuck and did not process traffic but was not restarted by the MP.	DE61474 DE61475
30.	When the default gateway MAC was changed, Alteon sent return traffic to the incorrect or old MAC.	DE60784 DE60785
31.	Using WBM, a 50X error occurred due to buffer leak in an HTTPS request.	DE60765 DE60766
32.	Alteon sometimes would crash when it received the same apply filter deletion and network class deletion that was assigned to the PIP that was defined for the real server.	DE61030 DE61031
33.	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.	DE60362

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 32.4.5.0

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.	DE60939

Item	Description	Bug ID
2.	On an Alteon standalone integrated with AppWall, the AppWall syslog messages were not sent.	DE60563
3.	A virtual service application-id configuration diff did not sync to an HA pair.	DE60453
4.	The Alteon Capacity information for HDD did not display a newly added HDD.	DE60409
5.	Using CLI, when using the /maint/debug/enhancedMP/health command, a panic would sometimes occur.	DE60349
6.	AppWall was down and the MP did not kill it, resulting in AppWall staying down indefinitely.	DE60158 DE60367
7.	Starting with this version, the Certificate Group Duplicate button is removed because it is not usable for certificate groups.	DE60328 DE60331
8.	Using Alteon VA, WBM displayed the port type as "Giga Ethernet Copper" irrespective of the actual port type used.	DE59941
9.	Using WBM, an 50X error occurred due to a leak in buffers on an HTTPS request.	DE60800
10.	Periodic statistics logging was corrupting the configuration environment during Apply/Save, which resulted in a panic.	DE60308
11.	Some DNS requests were not answered or were delayed.	DE60089
12.	A deadlock due to non-async signal functions caused a reboot.	DE59877
13.	There were negative values in OIDs related to Total Octets in content rules statistics.	DE59837
14.	The /info/sys/capacity command did not display current virtual and real services.	DE60172
15.	When trying to free the session entry allocated for an AX-processed session, a panic occurred.	DE60182
16.	A vADC displayed all default user account passwords in a dump.	DE59871
17.	In an MSTP with trunk environment, Alteon failed to communicate with another device.	DE59893
18.	When a user was in lockout, the information message was not consistent, causing a security problem.	DE59811
19.	Using the CLI, when executing the /c/l3/ha/switch/pref command, if the SSH/Telnet connection terminated, a panic occurred.	DE59573

Item	Description	Bug ID
20.	DNS query responses were not handled for query types MX and CNAME.	DE60208
21.	Starting with this version, added the Expiry Time field for the cookie in the Services pane.	DE60050
22.	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.	DE59784
23.	The bandwidth metric sometimes did not work if all the WAN links in a group were configured with health checks.	DE59357
24.	SAN input for DNS without a period (".") was not allowed.	DE60100
25.	The DNS query on a Backup device gave an incorrect response.	DE59543
26.	The total IP range limit value mentioned in the validation error for network classes was incorrect. It should have been 4294967294 instead of 4294967295.	DE59460
27.	vADCs were in running state but were not able to be accessed via MGMT until they were disabled and then re-enabled.	DE59085
28.	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.	DE59493 DE59498
29.	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.	DE59595
30.	The WAN link server displayed an overflow message for a clear issue for an edge condition.	DE59397
31.	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.	DE58834 DE58837
32.	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.	DE59150
33.	Maxcon support for 1 million was erroneously not implemented in the 30.5 series.	DE58163

Item	Description	Bug ID
34.	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.	DE59368
35.	Due to a network outage, Alteon panicked due to an IPv6 gateway failure.	DE59416
36.	An IPv4 filter session sometimes would be deleted before it aged out if the session memory was previously used by an IPv6 session.	DE60388
37.	On a 5208 platform, Ethernet ports connected to FireEye stayed down.	DE60233
38.	When real servers associated with a deleted FQDN real were deleted, AX was not updated.	DE58109

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 32.4.4.50

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.	DE59743
2.	Using the CLI, when executing the /c/l3/ha/switch/pref command, if the SSH/Telnet connection terminated, a panic occurred.	DE59568

Item	Description	Bug ID
3.	When more than nine (9) Ethernet ports were configured, incorrect information displayed when greping the port information.	DE59561 DE59562
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.	DE59489 DE59490
5.	As a fix, the FIPS domain name length was changed from 14 to 32 characters.	DE59703 DE59704
6.	After configuring an IPv6 address as a syslog host, the IPv6 VIP stopped working because the address was removed from the nbrcache entry.	DE59665 DE59666
7.	The DNS IPv6 EDNS client subnet IP address was incorrect.	DE59581 DE59584
8.	When a real server went down, the virtual statistics summary display was incorrect.	DE58515 DE59516
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.	DE59289 DE59290
10.	On a 5424 platform with an unlimited SSL license, the info/sys/general command incorrectly displayed “S” and not “SL”.	DE59026 DE59027
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.	DE58915 DE58916
12.	Even after setting the throughput threshold limit to "0," throughput alerts were issued.	DE58821 DE58822
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.	DE59458 DE59459
14.	When TACACS with clog was enabled, during a techdata/tsdmp operation, unnecessary logs were issued to the syslog.	DE58757 DE58762 DE58763
15.	The description for MIB altSwSpCpuPressureDeactivatedTrap was incorrect.	DE58771 DE58772

Item	Description	Bug ID
16.	When sending ICMP traffic to Alteon, the ICMP session was dumped to the syslog server as UDP.	DE59281 DE59283
17.	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.	DE58600 DE58601
18.	When sending client traffic to an IPv6 VIP with sharing enabled for the VR server, Alteon did not respond.	DE58952 DE58981 DE58983
19.	After upgrading from version 30.5 to version 32.2, LinkProof NG static NAT did not perform reverse NAT.	DE58609 DE58610
20.	Alteon used a console with a 9600 baud rate, and the MP issued information faster than the console could receive it.	DE58739 DE58740
21.	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.	DE58991 DE58992
22.	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.	DE59596
23.	When DSSP messages were received on the backup device, a software panic occurred.	DE58704 DE58705
24.	The Alteon device was not indicated as the next hop in a traceroute from the client machine to the ISP router.	DE58628
25.	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.	DE58382 DE58383
26.	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.	DE58574 DE58579 DE58580
27.	After upgrade, there was a false detection of session table corruption, resulting in an autorecovery.	DE59003 DE59004
28.	SSL traffic without SNI could not be handled without decrypting the traffic.	DE58839

Item	Description	Bug ID
29.	When configured with a 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.	DE59151
30.	While a session having proxy port was being freed, a panic occurred.	DE58194 DE59840
31.	When deleting an LSA from a neighbor's retransmission list, a panic occurred for link-state ACK packets.	DE59107 DE59112 DE59113
32.	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.	DE58361 DE58366 DE58367
33.	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.	DE58108

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 32.4.4.0

General Bug Fixes

Item	Description	Bug ID
1.	In an HTTP Modification rule, when clicking the path option, the Path field was not visible.	DE58291
2.	In an ADC-VX environment, after executing the techdata, tsdump, or td-stats all commands, the MP CPU reached 100% utilization.	DE58251

Item	Description	Bug ID
3.	The Alteon NTP time jumped one month ahead.	DE58134
4.	At boot time, when AppWall crashed, Alteon also crashed.	DE58059
5.	When user configuring a scripted health check for port 25 (SMTP), during runtime the syslog was flooded with health check failure logs.	DE57868
6.	On receiving an ICMP_UNREACH packet, when matching an existing session with no real server, a panic occurred.	DE57861
7.	When a VRRP group was configured, sharing did not work properly.	DE57849
8.	In AppShape++ scripting, an early and unnecessary variable validation was removed from the validator function.	DE57765
9.	After upgrading from version 31.0.10.50 to 32.2.3.50, the GSLB. DNS Summary Statistics displayed with a 0.	DE57678
10.	In Layer 2 mode when flooding to more than one port, fragmented packets (both in order and out-of-path) were lost.	DE57639 DE57642
11.	In an ADC-VX environment, after enabling /cfg/slb/ssl/adv/bereuse, after a reset or reboot the value changed back to disabled.	DE57633
12.	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.	DE57567
13.	Due to an incorrect version comparison, TLS 1.1 displayed as disabled by default.	DE57562
14.	The length of the hostname in the HTTP healthcheck field was increased to 128 characters as required.	DE57549
15.	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.	DE57538
16.	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.	DE57518
17.	Alteon incorrectly validated unsupported path attributes (currently the BGP community path attribute).	DE57513

Item	Description	Bug ID
18.	Using WBM, the percent character (%) in the passphrase for private keys did not work.	DE57486 DE57489
19.	Using WBM, could not renew existing certificates because of internal indexing issues.	DE57471
20.	When a DPDK initialization failed on any error except a queue error, it reverted to tuntap.	DE57372
21.	On a 9800 platform, after saving a configuration the following error displayed: mgmt: Flash Write Error	DE57350
22.	Using WBM, removing a target address from the SNMV3 did not remove the address from the AppWall UI server list.	DE57315
23.	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.	DE57305
24.	When the MP froze, the Watcher did not also kill the AW process of this MP.	DE57294
25.	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.	DE57270
26.	After rebooting a master and it comes up with an RSTP setup, an ARP packet was sent and received over the backup's block port.	DE57252
27.	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.	DE57225
28.	After rebooting a vADC, the GSLB/LinkProof licenses were disabled.	DE57176 DE57179
29.	After performing a recovery, the session capacity value was incorrect.	DE57148
30.	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.	DE57061
31.	On a FIPS card, a session terminated while it was still pending for a task.	DE57052 DE57056

Item	Description	Bug ID
32.	After a period of no traffic, the race condition timing could lead to an AppWall restart.	DE56992
33.	OSPF was not able to send a link state update (redistributed route) to peed when the gateway went down.	DE56966
34.	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.	DE56947
35.	A configuration with many real servers caused a delay in context switching, resulting in LACP messages not being handled.	DE56934
36.	Using WBM, when trying to modify the throughput limit, an error occurred. Added a REGEX to support all the throughput licenses.	DE56922
37.	After version upgrade, GEL licenses were rejected.	DE56888 DE56896
38.	In an HA environment with vADCs, when trying to send more OSPF routes to the peer device, a panic occurred.	DE56837
39.	An incorrect FIPS license string (deprecated) caused a flow of FIPS tests.	DE56813
40.	When a service was configured in a non-existing VIRT, it remained unnoticed until the VIRT was defined.	DE56795
41.	When mgmt was disabled and the syslog defined on mgmt, the new syslogs did not display in /info/sys/log.	DE56734
42.	There was a RADIUS Authentication failure because secret was not configured. No warning was issued for this.	DE56723
43.	After inserting a 1G SX Multimode transceiver, the following error displayed: “Cannot work with 1G transceivers.”	DE56714
44.	Alteon DPDK platforms dropped out-of-order fragmented packets.	DE56701
45.	The vconsole internally used Terminal MultiPlexer (TMUX), which is not available on DPDK-based platforms.	DE56693
46.	When trying to upload tech data when the management network was slow, an SCP timeout error occurred.	DE56656
47.	After applying the /info/sys/general command, the output was incorrectly 7612 S instead of 7612 SL.	DE56609

Item	Description	Bug ID
48.	While deleting an IPv6 configuration, a panic occurred. Added defensive validations.	DE56598
49.	Using WBM, the Monitoring > System > Capacity > Application Delivery page did not display capacity information.	DE56487
50.	Port 2233 was visible to public networks. The new behavior is that port is visible to a local host only (for example: 127.0.0.1:2233).	DE56400
51.	Using the CLI, after configuring a local add as a nwclass ID, after reboot, the configuration was not applied.	DE56337
52.	Using WBM, the configured Server Certificate group in a configuration did not display.	DE56292
53.	Configuring the data class IP address with mask 0 caused a panic. Because mask 0 is invalid, the fix was to ignore it.	DE56282
54.	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.	DE56081
55.	On an ADC-VX, an NTP timeout occurred.	DE55857 DE55862

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
8.	Activity tracking refinement issue.	DE56277
9.	Multiple events from different sessions are seen with same transaction ID	DE56260

Fixed in 32.4.3.50

General Bug Fixes

Item	Description	Bug ID
1.	Using WBM, you could not renew existing certificates because of internal indexing issues.	DE57475
2.	When a DPDK init failed on any error except a queue error, the configuration reverted to TUN/TAP.	DE57376
3.	On a 9800 platform, after saving a configuration, the following error displayed: `mgmt: Flash Write Error`	DE57354
4.	Using WBM, removing the target address from SNMPv3 did not remove the address from the AppWall UI server list.	DE57319
5.	When SNMP OID hwApplicationSwitchNameInfo was probed, the port state incorrectly changed to DISABLED by referring to wrong port flag state. This led to a gateway health check failure.	DE57309
6.	The Watcher did not kill the AppWall process that was related to the MP.	DE57298
7.	SLB traffic ignored a real server's weight for the roundrobin group metric when the real server rindex was included in a different word index group (rindex value /32).	DE57274
8.	If the Interface IP address and floating IP address were swapped and applied, the IF IP address was added to the IPv6 Neighbor Cache table as the new IF IP address but was deleted as the old floating IP address.	DE57229
9.	After reboot a vADC, the GSLB/LinkProof license was disabled.	DE57183
10.	When performing a recovery session, the incorrect capacity value was displayed.	DE57152
11.	Per RFC 3416, the SNMP Get Next values should be in lexicographical order, but this was not implemented for the FDBtable and other tables. This issue was fixed only for the FDBtable.	DE57065
12.	After a certain amount of time with no traffic, race condition timing could lead to an AppWall restart.	DE56996
13.	OSPF was not able to send a link state update (redistributed route) if there was a link failure or route change.	DE56970

Item	Description	Bug ID
14.	In an SLB environment with HA and session mirroring enabled, the real server current session statistics and redirect statistics were displayed incorrectly after issuing the command /i/slb/virt x summary on the backup device. It resulted in traffic failure when the backup became the active.	DE56951
15.	A configuration with many real servers caused a delay in context switching, resulting in LACP messages not to be handled.	DE56938
16.	Added REGEX to support all throughput licenses.	DE56926
17.	After upgrade, GEL licenses were rejected.	DE56900
18.	When Alteon tried to send more OSPF routes to a peer device, a panic occurred.	DE56834
19.	While trying to access SSH, a bad FIPS license string (which was also deprecated) caused a flow of FIPS tests.	DE56817
20.	When a service was configured in a non-existing VIRT, it remained unnoticed until the VIRT was defined.	DE56799
21.	RADIUS Authentication failed because the secret password was not configured. In addition, no warning was issued for this issue.	DE56727
22.	After inserting a 1 G SX Multimode transceiver, the following error displayed: `Cannot work with 1G transceivers.`	DE56718
23.	Alteon DPDK platforms dropped the out-of-order fragmented packets.	DE56705
24.	When uploading Techdata when the management network was slow, an SCP timeout error occurred.	DE56660
25.	After applying the /info/sys/general command, the output of the command incorrectly displayed "7612 S" instead of "7612 SL".	DE56613
26.	While deleting an IPv6 configuration and adding defensive validations, a panic occurred.	DE56602
27.	To aid with a configuration that requires many real server health checks, the maximum and current values for real services was added to the /info/sys/capacity output.	DE56491
28.	When using the CLI to configure a local add as network class ID, after reboot the configuration was not applied.	DE56341

Item	Description	Bug ID
29.	When small IPv6 TCP packets were received by the MP out of order via a data port, the memory associated with the packets did not return (after usage) to the pool of free small packets, causing problems for features allocating such packets.	DE56330
30.	Using WBM, a configured server certificate group did not display.	DE56296
31.	A check was added for packet captures to prevent a one-time crash that occurred when an unchained buffer was treated as a chained buffer on non-DPDK platforms.	DE55731

Fixed in 32.4.3.0

General Bug Fixes

Item	Description	Bug ID
1.	Could not save a configuration change and received the error `Flash Write Error`.	DE57354
2.	If there was no default Gateway defined or the Gateway failed, after a security scan there was total service outage.	DE56257
3.	When a burst of packets was 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.	DE56155
4.	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.	DE56138
5.	In an IPv6 environment, a specific virtual service could not be DNS-resolved by GSLB.	DE55999
6.	In an IPv6 environment, a specific virtual service could not be DNS-resolved by GSLB.	DE55994
7.	The HTTP modification rule for a host match did not accept a dot (.) in the match term.	DE55935
8.	The translation to Chinese for the value slbNewCfgEnhVirtServApplicationType.13 was incorrectly translated as "basic slbit"; it should have been "SMTP."	DE55927 DE55930

Item	Description	Bug ID
9.	Stuck sessions in AX caused another of issues, resulting in a panic.	DE55834
10.	Alteon lost communication with the LLS and entered the grace period.	DE55779
11.	Using WBM, the dot (.) character was not supported in an SSL policy name.	DE55721
12.	After an upgrade to version 31.0.12.0, a panic occurred because of null pointer access.	DE55711
13.	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.	DE55670
14.	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.	DE55654
15.	On an Alteon 5412XL platform, the same cookie load-balanced to multiple real servers.	DE55599
16.	In an AppWall integrated in Alteon environment, a new secwa did not display in the AppWall Console.	DE55472
17.	The configuration migration tool duplicated the GSLB network for Inbound LLB rules.	DE55451
18.	When HAID 2 was configured, /info/slb/virt display the wrong virtual MAC address.	DE54763
19.	Layer 7 SNI-based LLB did not work with BWM enabled in Enforcement mode.	DE54456

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 were not synced to the backup.	DE56051

Item	Description	Bug ID
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 32.4.2.60

General Bug Fixes

Item	Description	Bug ID
1.	In an ADC-VX environment, when a packet capture was exported to an SCP server, the capture status remained as “upload in progress” until the device rebooted.	DE55387
2.	In an Alteon VA environment running version 32.4.0.5, SP 1 initially configured with memory = 0 KB.	US55632
3.	A DNS request accessed the cache unexpected.	DE55410
4.	The packet capture tool did not capture all of the packet sent from SP to MP, resulting in an expected health check.	DE54439
5.	There was an Alteon SSL inspection and IWSVA integration issue.	DE54475
6.	On a FIPS-II 6024 platform, there was a memory leak.	DE55609
7.	There was a health check issue with a buddy real server.	DE55482
8.	With GEL active license revalidation, there was an MP freeze issue.	DE55437

Item	Description	Bug ID
9.	A type discrepancy in the URLF subcategory printing caused Alteon to reboot.	DE55362
10.	There was no support for non-interactive mode for the "/c/slb/sync/auth passphrase xxxxxx" command, causing a missing configuration sync authentication toggle.	DE55339
11.	Could not apply the TACACS configuration during a timeout cycle.	DE55316
12.	Live packet capture did not work.	DE55277 DE55283
13.	A type discrepancy in the URLF subcategory printing caused Alteon to reboot.	DE55266
14.	Using AppWall integrated with Alteon, all Web applications stopped.	DE55240
15.	Routes through GRE/IPinIP tunnels did not display after running the /i/sys/capacity command.	DE55217
16.	Site resources were not cached by FastView	DE55134
17.	After connecting to the GEL server, the Alteon console was flooded with some junk logs every 18 seconds.	DE54946
18.	Using the /info/l2/vlan command, the jumbo frame information was incorrect.	DE54896
19.	Using WBM, you could not create a service using TCP 995.	DE54874 DE54880
20.	Allow filters failed to decrypt IPv6 traffic.	DE54820
21.	The error message "Someone else is doing the diff [flash] try again!" was issued.	DE54816
22.	When HAID 2 was configured, /info/slb/virt displayed the wrong Virtual MAC ID.	DE54764
23.	After upgrading, Alteon was not able to push the intermediate certificate and failed to apply the configuration.	DE54735
24.	After Revert Apply, the gateway flapped in Alteon running version 31.0.9.0.	DE54687
25.	Config sync was unsuccessful. The Application Services Engine was not synchronized with the current configuration.	DE54678

Item	Description	Bug ID
26.	The WBM menu was disabled, but you could use CLI to modify settings.	DE54658 DE54664
27.	Performing proxy processing on an OSPFv6 packet caused a panic and reboot.	DE54650
28.	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.	DE54639
29.	A BGP peer established a connection and changed back to the Connect state.	DE54627
30.	Could not upgrade from Alteon VA version 32.2.0.0 to version 32.2.3.0.	DE54612
31.	When GW 1 was deleted, DNS health checks were not generated but ICMP health checks were generated.	DE54590
32.	APSolute Vision sent an incorrect REST query to Alteon.	DE54493
33.	There was error while applying a configuring for a network class.	DE54484
34.	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	DE54460
35.	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.	DE54430
36.	Using WBM, downloaded techdata and core dumps were corrupt.	DE54415 DE54421
37.	The SNMP overload health check mechanism stopped working when it was added to the logExp health check.	DE54412
38.	The fragmented CPU size was increased from 16K to 64K.	DE54403

Item	Description	Bug ID
39.	Using the WBM, a VLAN name of 32 characters was allowed, while in the CLI, only 31 characters was allowed.	DE54391
40.	In the Real Server configuration pane, the HA master displayed FQDN instances.	DE54393
41.	After device reset, WBM and APSolute Vision were not accessible.	DE55140
42.	There was a bug in the Advisory Tool upgrade.	DE54380

AppWall Bug Fixes

Item	Description	Bug ID
1.	The communication properties option in the wizard was not relevant. It has been removed.	DE51197 prod00272955
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 upgrading 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 32.4.2.0

General Bug Fixes

Item	Description	Bug ID
1.	After upgrading the Alteon software version, the application Intermittently was not working.	prod00277501
2.	On an Alteon VA, Alteon reset the connection when traffic failed over.	prod00277059
3.	IPv6 SNMP queries over the data port were not working because checking for management access with the ingress data port failed.	prod00277282

Item	Description	Bug ID
4.	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%.	prod00277362
5.	AppWall for Alteon was not parsing parameters whose values matched the string "banana" (%F0%9F%8D%8C).	prod00274209
6.	When using HTTP/2 after login, traffic stops working.	prod00278070
7.	Connections to a VIP closed abruptly.	prod00276584
8.	During stress traffic, a panic occurred.	prod00278081
9.	The Alteon 6024 platform rebooted due to a panic.	prod00276360
10.	The Alteon NG+ license did not apply the 5 vADC license.	prod00276639
11.	The port speed capability was not handled for the MR platform XGE interface while dumping the port configuration and port auto-negotiation configuration options, resulting ins no diff configuration.	prod00275660
12.	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.	prod00275473
13.	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.	prod00276340
14.	The priorities for remote real servers among different GSLB networks 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.	prod00277208
15.	After upgrading to version 31.0.11.0, SSL offload did not work properly.	prod00276274
16.	SSL traffic caused a panic.	prod00278067

Item	Description	Bug ID
17.	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.	prod00275640
18.	In an SLB environment with a pbind client IP address, persistence was not maintained.	prod00275950
19.	Trend Micro's IWSVA (AV) in ICAP mode (with Alteon acting as ICAP client) was only partially working.	prod00277015
20.	With AES used for privacy and/or encryption, the initialization vector was not set properly, causing AES encryption to fail.	prod00276313
21.	When logged in as a TACACS or RADIUS user, could not modify or create SNMPv3 authentication or privacy passwords.	prod00277012
22.	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.	prod00277394
23.	During SNMP polling, a panic occurred.	prod00277993
24.	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.	prod00277517
25.	When changing to the default configuration, the runtime session capacity was not reflected.	prod00276875
26.	During an upgrade to version 32.2.30 or later, the configuration became stuck in diff.	prod00276743
27.	When an HTTP modification string was configured with multiple escape sequences, Alteon did not insert an escape sequence.	prod00276936
28.	In a GSLB environment, Alteon became stuck with high MP CPU utilization.	prod00276520
29.	When the management port was disabled, syslog messages were not sent on the data port.	prod00278037
30.	In a DSR environment, there was a discrepancy between /info/swkey and virtual server statistics.	prod00277932

Item	Description	Bug ID
31.	When processing the second fragment destined for the Alteon interface when the redirect filter was configured, Alteon panicked.	prod00277481
32.	Using WBM, you could not edit the IP address for a new Outbound LLB Rule.	prod00277386
33.	BGP 4 Byte ASN was not compatible with Cisco Nexus 9K and Huawei routers.	prod00276711
34.	An invalid hypervisor type was set for virtual platforms.	prod00276260
35.	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.	prod00276501
36.	Using WBM, could not configure BGP 4-byte-ASN.	prod00276810
37.	Traffic was forwarded to a failed WAN real server.	prod00276356
38.	The remote system refused the connection, impacting Azure NA self-service.	prod00277311
39.	When the Alteon HA state changed from Master to Backup, the gateway and real server's health checks failed.	prod00278210
40.	When changing from ena to dis and vice versa, could not apply the /cfg/l3/ha/switch/filtpbkp command.	prod00277753
41.	Could not log in to AppWall.	prod00275567
42.	On DPDK platforms, Interface errors for port statistics were issued.	prod00278281
43.	ICAP responses were not forwarded to the client.	prod00276506
44.	In an IPv6 SLB environment with an IPv6 HTTP health check and IPv6 HA configured, the memory allocated for HTTP HC was not freed, which led to a memory leak.	prod00276962
45.	When AES was used for privacy and/or encryption, the initialization vector was not set properly, causing AES encryption failure.	prod00276312
46.	On an ADC-VX, the device banner and /boot/cur show different active Alteon versions.	prod00276979
47.	On a vADC, incorrect Throughput Alert messages were issued.	prod00275924

Item	Description	Bug ID
48.	While STG information was sent from an ADC-VX to a vADC, a panic occurred.	prod00278078
49.	When importing a configuration with BGP, Alteon issued Notice messages with non-ASCII characters.	prod00275647
50.	On an ADC-VX, the device banner and /boot/cur show different active Alteon versions.	prod00276977
51.	Added GSLB site IP address validation.	prod00277095
52.	After a panic, the Admin context went into a reboot loop.	prod00276327
53.	There were many FLOOD entries being created in the FDB table for the PIP MAC. This caused some of the traffic to fail.	prod00277246
54.	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.	prod00276616
55.	Using WBM, during configuration sync, continuous fetching of the virtual server table caused a panic.	prod00277467
56.	Could not sync or apply changes.	prod00276399
57.	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.	prod00277337
58.	When the primary WAN link went down and the backup WAN link took over, an incorrect syslog message displayed.	prod00276691
59.	A confusing configuration resulted while implementing LDAP(S) health check.	prod00275745
60.	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.	prod00276795
61.	Using WBM on a vADC, could not renew an SSL certificate.	prod00276405
62.	An HTTP header modification value set to None was considered as valid input.	prod00277186

Item	Description	Bug ID
63.	After HA failover, Alteon lost router connectivity in order to reach real servers.	prod00277715
64.	Enabling and disabling HTTP/2 caused service impact.	prod00275418
65.	The backup group status in a content rule displayed an incorrect status when the backup group was not directly associated to any service.	prod00276758
66.	In an Azure environment, Alteon VA crashed.	prod00276481
67.	Using WBM, when "Return to Last Hop" was set for a virtual server, an additional field type was also set internally.	prod00276933
68.	The Intermediate CA certificate could not be imported due to unexpected max limit.	prod00278075
69.	Using Alteon VA, there were multiple core dumps that resulted in the file system becoming full.	prod00277683
70.	An explicit proxy caused unexpected behavior for HTTP/HTTPS traffic.	prod00278421
71.	An unexpected LACP changed state resulted in the device switching to BACKUP state.	prod00278167
72.	Using vADC, generating a new Web Management Certificate caused a panic.	prod00278260
73.	After upgrading to version 32.2.3.0, the device constantly rebooted due to a panic.	prod00278289
74.	After upgrading to version 32.2.3.50, SSL inspection and ICAP Integration were not working properly.	prod00278451

AppWall Bug Fixes

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

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

Item	Description	Bug ID
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

Fixed in 32.4.1.50

Item	Description	Bug ID
1.	ICAP responses were not forwarded to the client.	prod00276488
2.	Using WBM, added a "renew" parameter as part of query string to allow renewal of SSL keys and certificates.	prod00276278
3.	Incorrect throughput alert messages displayed on vADCs.	prod00275809
4.	With AES was used for privacy/encryption, the initialization vector was not set properly, causing an AES encryption failure.	prod00276222
5.	Could not sync or apply changes.	prod00276402
6.	Using the preempt disabled feature, a primary real server that is moved to the OPER DIS state by the health check module when the backup is UP for the service continues to be in OPER DIS state even when the "backup" and "preempt dis" configuration is removed from it.	prod00276615
7.	After upgrading to version 31.0.11.0, SSL offload did not work correctly.	prod00276282
8.	Using WBM, could not configure BGP 4-byte-ASN.	prod00276813
9.	When upgrading to version 32.2.30 or later, the configuration became stuck in diff.	prod00276747

Item	Description	Bug ID
10.	Using WBM, when the Return to Last Hop was set for a virtual server, an additional field type also was set internally.	prod00276934
11.	The port speed capability was not handled for the MR platform XGE interface while dumping the port configuration and port auto-negotiation configuration options, resulting in no diff configuration.	prod00275659
12.	Enabling and disabling HTTP/2 impacted service.	prod00275411
13.	In an IPv6 SLB environment with an IPv6 HTTP health check and IPv6 HA configured, the memory allocated for the HTTP health check was not freed, which led to a memory leak.	prod00276961
14.	Using WBM, the HTTP health check edit pane did not display the configured settings and values	prod00275724
15.	The device banner and /boot/cur displayed different active Alteon versions on the ADC-VX.	prod00276981
16.	When a starting packet capture through WBM, incorrect data displayed when running /c/sys/alerts when the packet capture filter string was set to more than 128 characters.	prod00275472
17.	An IWSVA (AV) in ICAP mode (with Alteon acting as the ICAP client) was only partially working.	prod00277014
18.	Implementing LDAP(S) health checks has been improved.	prod00275744
19.	Added GSLB site IP address validation.	prod00277094
20.	When a device came up after reboot, the HA status displayed as "NONE" because the HA state was recorded based on current HA service group state for which an Apply was in process.	prod00275639
21.	In a GSLB environment, the device became stuck with high MP CPU.	prod00276546
22.	In an SLB environment, when the session move operation is executed, in some scenarios this operation was not reset on one of the SPs, which leads all subsequent session move operations to fail on that particular SP.	prod00276344
23.	The Alteon NG+ license did not apply the 5-vADCs license.	prod00276642

Item	Description	Bug ID
24.	After syncing the configuration from the secondary device to primary device, virtual routers, Switch HA, and/or Service HA may flap or go into the INIT state if there was a configuration difference between two devices	prod00276500
25.	An invalid hypervisor type was set for virtual platforms.	prod00276262
26.	When importing a configuration with BGP, notice messages were issued with non-ASCII characters.	prod00275646
27.	Using LinkProof for Alteon, intermittent ICMP packet was dropped. After pinging from same sequence number, the ping reply packet intermittently dropped.	prod00276800
28.	Fixed a panic scenario based on case prod00275591.	prod00276363
29.	The backup group status in a content rule displayed the incorrect status when the backup group was not directly associated to any service.	prod00276756
30.	Traffic was forwarded to a failed WAN real server.	prod00276355
31.	BGP 4-byte ASNs were not compatible with Cisco Nexus 9K and Huawei routers.	prod00276714
32.	Using WBM, added a "renew" parameter as part of query string to allow renewal of SSL keys and certificates.	prod00276408
33.	Connections to a VIP randomly closed.	prod00276583
34.	There was a disparity of the MAC address between the primary and backup devices.	prod00275354
35.	When the primary WAN link went down and the backup WAN link took over, an incorrect syslog message was issued.	prod00276694
36.	In an Azure environment, Alteon did not load with SRIOV NICs.	prod00274518
37.	There were many flood entries created in the FDB table for the PIP MAC, causing some of the traffic to fail.	prod00277242

Fixed in 32.4.1.6

Item	Description	Bug ID
1.	Enabling and disabling HTTP/2 caused a service impact.	prod00274166
2.	Could not reach above 51K CPS when TD was enabled.	N/A
3.	Alteon HA did not behave as expected.	prod00273952

Item	Description	Bug ID
4.	The AppWall WBM was vulnerable to XSS.	prod00273963
5.	During bootup, while loading the configuration from flash, the Apply failed.	prod00273263
6.	Long parameters bypassed by the DB filter displayed in the AppWall Security log.	prod00274169
7.	Using AppWall, there were many "Invalid Version string at HTTP protocol identifier" security events.	prod00273330
8.	AppWall sent syslog messages to APSolute Vision with 10.10.10.10 reported as the source IP address.	prod00274506
9.	Using AppWall, when generating coupons, there was latency when traffic was processed.	prod00274887
10.	In a GSLB environment, the device stuck in high MP CPU.	prod00275031
11.	In the Forensics log the illegal pattern in the security evet was not marked in red, as expected.	prod00275143
12.	Apply and Diff could not be performed because of "Could not allocate memory for diff" errors.	prod00275686
13.	After upgrading from version 32.4.0.5 to 32.4.1.4, a rare condition caused WAF to reload multiple times, leading to service outage.	prod00276512
14.	Improper error handling enforcement of a missing parameter in a REST API call allowed creation of a real server without an IP address.	prod00276523

Fixed in 32.4.1.0

Item	Description	Bug ID
1.	A long certificate name was not accepted when attached to back-end policy.	prod00272989
2.	Time syslog timestamp format for Alteon WAF was incorrect.	prod00274427
3.	Incorrect statistics in AppWall dashboard.	prod00274417
4.	A vADC panicked.	prod00274736
5.	The Submit button in Network > Layer 3 > Tunnels is always highlighted.	prod00274001

Item	Description	Bug ID
6.	In the APSolute Vision Analytics Dashboard, there was an Alteon SP CPU display issue.	prod00274444
7.	Using WBM, could not configure the sync passphrase.	prod00274035
8.	There were many RFI security events although "Redirect Validation" was disabled.	prod00274442
9.	Long parameters bypassed by the DB filter displayed in the AppWall Security log.	prod00274169
10.	Using WBM, could not change the default of factory configuration to save the management configuration.	US64628
11.	With Layer 7 Application Acceleration, some connections were dropped in the middle.	DE50652
12.	When Alteon sent syslog messages, a panic occurred.	prod00272885
13.	Using LinkProof NG, when the upload/download limits for the WAN link were configured to be greater than 455 Mbps, WAN link bandwidth utilization displayed incorrect statistics.	prod00273017
14.	When the DNS virtual service protocol is UDP Stateless, HTTP and FTP services failed for IPv6 traffic.	prod00273833
15.	Using config sync, disabling virt synchronization removed virtual servers from the backup device.	prod00273197
16.	After resetting the admin password from the console, the password displayed in clear text in diff flash.	prod00274144
17.	Using WBM, there was an HTTP modification rule configuration issue.	prod00273398
18.	While running a scan over SSH, Alteon panicked.	prod00274798
19.	Health checks failed due to a corruption in the small/medium/jumbo packet free pool list because of a synchronization problem in the ARP module.	prod00274562
20.	A MAC flap on Layer 2 occurred when the DUT was connected on one port and the server was connected on a different port.	prod00273066
21.	Using WBM, when VIPs were added to/removed from the HA service list, Alteon panicked.	prod00273660
22.	A configurational change to shutdown did not display correctly under /cfg/slb/group x/cur.	prod00272734

Item	Description	Bug ID
23.	IEEE 802.3 standard protocol packets (such as STP packets that run over LLC) sometimes were 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 they were transmitted with the unstripped CRC to other entities in the network.	prod00272403
24.	The GSLB DNS client network rules real server selection pane was too small.	prod00272846
25.	Using WBM, when changing the "DNS Responder VIP" from "dis" to ena" and vice versa, Alteon did not update the flags that are used to identify the config change. Because of this, Alteon found no config change during Apply and an issue occurred.	prod00273457
26.	A vADC panicked, became stuck, and was not able to handle any traffic.	prod00274806
27.	When viphlth was enabled, there was no response to ICMP health checks directed at VIPs.	prod00274664
28.	Configuration sync failed with a timeout.	prod00273098
29.	Using WBM, a Notify View ISO could not be configured without creating a custom Notify Tag.	prod00273729
30.	After upgrading to version 32.2.1.0, session logs were not generated.	prod00272746
31.	Was not able to configure service 111 for TCP and UDP.	prod00272611
32.	After running /stat/slb/clear, only part of the filter statistics was cleared, and the others remained cleared.	prod00272889
33.	Alteon was rebooted unexpectedly by Watchdog.	prod00273481
34.	A packet capture's TCP stream displayed corrupted data due to TSO allocated buffers.	prod00269187
35.	After upgrading to version 32.2.1, the MP CPU utilization spiked.	prod00273888
36.	SIP INVITE and fragmented packets were not forwarded to real servers.	prod00273234
37.	While loading the configuration from flash, an Apply failure occurred during bootup time.	prod00274183

Item	Description	Bug ID
38.	SNMP data of polling interface details incorrectly displayed the interface type.	prod00273385
39.	After reverting an unsaved configuration, the HA State remained INIT and was not updated automatically.	prod00272981
40.	When enabling an HTTP/2 policy, a panic occurred.	prod00273788
41.	Using Passive FTP, an RTS session was created instead of a filter session for FTP data traffic.	prod00272723
42.	Alteon HA did not display expected behavior.	prod00274960
43.	Handled CVE 2019-11477, CVE 2019-11478, and CVE 2019-11479 using a Linux Kernal patch.	prod00273354
44.	Using WBM, the Maximum Session Number was not changed after adding a CU. It only was changed in CLI.	prod00274758
45.	Using WBM, an Invalid EC Key Size (6). error displayed while generating an SSL certificate an RSA key.	prod00272085
46.	When VLAN 1 was disabled and an Apply was done for any config change, the ping response to the interface was delayed, causing a timeout.	prod00273595
47.	With lower BFD rx-int configured, when there was a change in the session table type between ABT and PBT, the BFD session went down, causing deletion of the BGP session. This issue has been addressed by yielding control to the SP to send BFD packets.	prod00272730
48.	While running a scan over SSH, Alteon panicked.	prod00274826
49.	A vADC could not handle any data traffic including a health check. The vADC did not restart after an SP panic/freeze.	prod00274320
50.	Alteon indirectly caused a vulnerability to the DNS cache poisoning attack.	prod00269191
51.	When idbynum was enabled, there were issues with Revert Apply.	prod00273941
52.	After a device reset, could not connect to the Alteon VA management IPv6 address.	prod00275196
53.	After a power cycle, Alteon rebooted.	prod00272653
54.	NTP requests were not sent in an OSPF network.	prod00274315

Item	Description	Bug ID
55.	After a Submit via QAS, a service's rport was overwritten.	prod00272877
56.	In a GSLB environment, Alteon did not resolve a DNS query even though the remote real servers were UP.	prod00272896
57.	Using APSolute Vision, importing a certificate in Alteon did not work with the ADC + Certificate Administrator role.	prod00274711
58.	In a GSLB with VRRP/HA environment, after applying a configuration, the DSSP health checks failed.	prod00273186
59.	After Applying configuration changes, VIPs stopped responding.	prod00272782
60.	A vADC panicked.	prod00274792
61.	There was a service failure/RIP leakage due to sessions abruptly aging out.	prod00275794

Fixed in 32.4.0.0

Item	Description	Bug ID
1.	On a 6024 platform with 128GB RAM, in an environment that uses jumbo frames (with /cfg/l2/mtu set to greater than 1500), the config sync send operation fails when all the jumbo packets are consumed due to an SNMP memory leak.	prod00273909
2.	Alteon sends multiple requests to the RADIUS server for one login to WBM.	prod00270429
3.	In an AppWall integrated in Alteon environment, the details for refinement of pattern id: 10487 displayed SQL information incorrectly.	prod00267554
4.	When an SNMP health check was configured, the weight was displayed but not displayed when the SNMP heath check was part of a LOGEXP.	prod00268456
5.	In a high availability environment, even though the configuration was the same on both the active and standby devices, a warning message related to the HA configuration mismatch was issued.	prod00268006
6.	In an SLB environment with forceproxy, and an ICAP and SSL Inspection configuration, when the ICAP server terminated or was not responding, a panic occurred.	prod00267961

Item	Description	Bug ID
7.	In an SLB environment with the group metric "svcleastconns" and multi rports, load distribution to real server was not performed correctly.	prod00267434
8.	In Alteon Virtualization environment on an ADC-VX, when an API request queried the default image "agDefaultImageVer", an incorrect/gibberish response was received.	prod00267830
9.	When an LDAP bind request packet length exceeded 127 (for contents greater than 116, including LDAP markers), multi-byte representation was not used, which caused Alteon to not generate the advanced health check type LDAP as expected.	prod00269896
10.	You could modify an HTTP head host modification rule using CLI, but not with WBM.	prod00268689
11.	In an SLB environment with forceproxy, after configuration sync (the associated real server was removed) from the master to the backup device, the device rebooted.	prod00269017
12.	In an SLB environment, when the primary group became operational, the backup group's session table was removed.	
13.	As part of the fix, the session entry is removed if the real server is not enabled under the group. In this scenario, this condition failed because the session's real server that is backed up is removed from the group when the primary real server becomes operational. This leads to removal of the backup real server's session entry when the primary real server comes up.	prod00270616
14.	When the number of basic health check components used in a logical expression-based health check object was changed, and the new expression had fewer objects than the old expression, a software panic occurred.	prod00268237
15.	PIP count validations for limiting the number of ARP/NBR entries in non-HA mode were not available. This allowed the user to add more than the maximum allowed entries in non-HA mode, and when the user switched to HA mode, the validations issued errors.	
16.	As a fix, added the same set of validations for non-HA mode. In addition, maximum PIPs are now 2K and the number of ARP and NBR entries are 2K each.	prod00268391

Item	Description	Bug ID
17.	The "new cached bytes" field in the statistics for the acceleration engine cache mechanism, displayed the wrong value.	prod00271431
18.	When the configuration script was only partially run and then the diff command was run, services went down on the master device.	prod00270097
19.	The binary health check failed with a timeout even through the checked server replied with unexpected value.	prod00271038
20.	In a hot-standby VRRP environment, when port 1 was disabled on the backup, Alteon attempted to disable the port as part of the hot standby algorithm irrespective of the current status of port. The functions called during the flow used ND APIs and they resulted in high MP CPU.	
21.	As part of the fix, disabling the port again is prevented if the port is already in the disabled state.	prod00271917
22.	After enabling compression, file download failed.	prod00272083
23.	On a vADC and standalone, entering the command blkport disable caused a panic.	prod00270660
24.	When Alteon was connected to a Cisco device using a LAG (Link Aggregation Group) that had two member ports in it, and the Cisco device was acting as the gateway for Alteon, with STG on and the LACP block port enabled, when one of the ports was moved out of LACP LAG, the interface went down.	prod00266987
25.	In an HA environment, when performing a reset (/boot/reset) on the master device (which disables the ports), the real servers went down, and Layer 4 sessions were deleted on both the master device and the backup device.	prod00267151
26.	Using WBM, on the **Monitoring > System > Maintenance** pane, when the resolution changed, the Export button for techdata was slightly misplaced.	prod00267869
27.	After creating a Notify Tag from **Configuration > System > SNMP > SNMPv3 > Notify Tags**, opening the new Notify Tag displayed the content of a different Notify Tag.	prod00269990

Item	Description	Bug ID
28.	In an SLB environment, when the HTTP/2 policy was set to ON, with a group that included one real server and one backup real server configured, when the active real server went down, traffic was not shifted to the real server configured as the backup and the client received a 503 error.	prod00268742
29.	Irrespective of the LACP port configurations, Alteon with STP set to OFF did not transparently pass BPDU from a Cisco Nexus with MSTP.	prod00269096
30.	When running a vDirect script in Alteon, received a timeout.	prod00270590
31.	In an OSPF environment, Alteon was unable to update any change of the OSPF parameter to the peer.	prod00268277
32.	When a data port was used for NTP and the packets were received from non-configured NTP servers, the syslog was filled with the message "NTP illegal packet length" for the dropped NTP packets.	prod00268905
33.	In a virtualization environment on a vADC, SP memory displayed as HIGH all the time even though the device had no traffic and no SLB configuration.	prod00268395
34.	Using WBM, could not assign a VLAN to an interface.	prod00271063
35.	If a bandwidth management contract is associated to a traffic pattern and the TOS overwrite feature is enabled, a packet capture did not reflect the DSCP field modification.	prod00270092
36.	When RTSRCMAC is enabled and the gateway is disabled, Alteon does not return UDP/SIP virtual traffic to the client.	prod00270953
37.	Using WBM, default group 1 displayed without any changes made to it, while in CLI the group did not display unless changes were made to it.	prod00271520
38.	In an ADC-VX environment, WBM, SSH, and the console were not available until the device was rebooted.	prod00271286
39.	In an FTP Passive environment, the incorrect ACK number was updated for the PASV retransmitted packet.	prod00272219
40.	The SNMP configuration commands in CLI /c/sys/ssnmp/rcomm and /c/sys/ssnmp/wcomm accepted NULL string, resulting in errors on adding or removing real server from the group.	prod00268504

Item	Description	Bug ID
41.	In an SSL environment with certificates that will expire after 100 years were displayed as expired.	prod00267055
42.	In a virtualization environment, when a vADC was deleted and when a new vADC was created with same vADC number, the old configuration was restored in the newly created vADC.	prod00267319
43.	Using WBM, even though a user was logged in as 'admin', the user could not disable a real server operationally.	prod00267835
44.	Using WBM, when configuring an SSL service, the certificate and the group were set and configured even when the user selected the 'any' option, causing the newly configured APP to run slowly.	prod00268686
45.	In a VRRP environment, changes to the VRs' priority during migration failover ended with an apply lock and high MP memory usage.	prod00268859
46.	In an SLB environment with DNS Responder VIPs, with mixed delegation/non-delegation traffic, a panic occurred.	prod00269132
47.	In a filter configuration, the default value of "matchdev" differed between WBM and CLI.	prod00270628
48.	Even though access to the device management port was restricted using the access list (/cfg/sys/access/mgmt/add), it was not working correctly.	prod00268808
49.	Using WBM, in an SLB environment, in the Content Rule pane for a virtual service, an invalid URI was accepted for the redirect URI configuration, while in CLI the same configuration resulted in an error.	prod00267553
50.	In an SLB environment, when you disabled or enabled a real server operationally in a server group, a syslog message for these actions was not generated.	prod00267984
51.	Using WBM, Alteon panicked when generating techdata.	prod00271232
52.	WBM did not display the virtual service configuration after synchronization.	prod00270172
53.	The EDNS+Source network-based name resolution failed for certain source addresses. The GSLB query failed when it contained the EDNS extension with the client subnet address, which fails to match the network class configuration.	prod00270958

Item	Description	Bug ID
54.	If the link was down when the STG was off and "blockport" was enabled, the incorrect port state was assigned to a LAG member port after reboot.	prod00271623
55.	After changing all of the IP addresses of a single network to different IP address, non-existing MACs remained in ARP table.	prod00272483
56.	Using WBM, an AppShape++ script with the incorrect syntax was allowed, which corrupted the configuration upon save.	prod00270694
57.	In an SLB environment with high availability, even though the PIP network class range was enabled to receive GARP (/c/l3/ha/nwclgarp ena), the GARP was not sent for all IP addresses from the proxy network class range.	prod00268507
58.	Using WBM, when creating route maps, the following parameters had incorrect values for the route map object: Local Preference, Metric, and Weight	prod00264252
59.	In an SLB environment with forceproxy, the TCP policy/pushack behaved as being disabled even though it was set to enabled, causing a TCP retransmission problem.	prod00267405
60.	In a virtualization environment, when configuring synchronization, the MP CPU of the vADC stayed at more than 80% utilization for a long time.	prod00269754
61.	In an SLB environment, when the FQDN real server was changed, Alteon did not update for more than half an hour since the change was made, and it changed only after the FQDN real was disabled and then enabled.	prod00268655
62.	When the user enabled vmasport and entered Apply, Alteon rebooted due to a software panic.	prod00270607
63.	In a monitoring environment, when continuously polling for the following set of OIDs with GET REQUESTs, a panic occurred: slbStatLinkpflpTable,pip6CurCfgTable,pip6NewCfgTable, pip6CurCfgPortTable,pip6NewCfgPortTable,pip6CurCfgVlanTable, pip6CurCfgVlanTable,pip6NewCfgVlanTable)	prod00268930
64.	When the services were moved from master node to backup node, there were no SNMP traps sent to the Monitoring server.	
65.	Note: These traps were omitted when implementing the new feature "Extended HA".	

Item	Description	Bug ID
66.	Trap, syslog, and log messages have been updated/extended/replaced with new messages.	prod00267570
67.	In a SLB configuration with high availability, the configuration of the backup real server and/or backup group was not synced to the peer device.	prod00268047
68.	The STG-VLAN configuration failed to apply on reboot because the number of parameters exceeded 64.	
69.	Fix: After upgrade, perform the configuration and save, then reboot.	prod00271342
70.	The Info/slb/group command displayed the incorrect VLAN for unavailable servers.	prod00270186
71.	When configuring a health check ID and real server ID together with a length greater than 35, due to a bug in the health check script a panic occurred.	prod00271594
72.	After an interface related VLAN was deleted and then added back, the Layer 3 interface stayed down.	prod00272243
73.	In a BGP environment, when network class changes were applied, the device panicked.	prod00270720
74.	In an HA environment with same network class associated to Smart NAT and a real server, the ARPs for some of the PIPs in the network class range were not answered by Alteon.	prod00268646
75.	In an SLB environment with forceproxy configured and with the HTTP/2 gateway implementation, SP memory usage was high.	prod00267930
76.	When Alteon received the IPv6 address as a full-length address (more than 32 characters including colons, for example: 2101:2101:2100:2100:2101:2100:2100:2101) and processed an IPv6 fragmented packet, a panic occurred.	prod00267494
77.	In an HA environment, a filter proxy was added to the ARP table with the device MAC instead of the HA MAC, causing Alteon to not forward dynamic NATed DNS response to the internal DNS server.	prod00267724
78.	Using WBM or SNMP, when a GSLB network prefix we configured, the IPv6 mask configuration did not get set properly. This caused improper matching of the GSLB network during DNS request processing.	prod00269774

Item	Description	Bug ID
79.	In an SSH environment, image download using SCP was slow compared to FTP download.	prod00269085
80.	Error received configuring a real server.	prod00269759
81.	When submitting the SECWA configuration, AppWall issued the following error:	
82.	You are not authorized to edit this Web Application.	prod00269189
83.	After running the command /c/slb/cur, if the configuration contained any AppShape++ script associated to a filter, a panic occurred.	prod00270300
84.	In an SLB environment, when the real service port (rport under virtual service) was configured with a value less than 5 (except for multiple rport/IP service scenario), the traffic failed for such rports.	
85.	As a fix, validation has been added to allow rport 0-multirport or 1-ipservice or 5-65534.	prod00269098
86.	In a BGP environment, when deny route redistribution was disabled for a BGP peer, even though the BGP peer went down and came back up, Alteon stopped sending advertisements.	prod00267679
87.	Using WBM, HA Real Server Tracking could not be configured.	prod00268052
88.	The current and total session counters were not accurate in server group statistics.	prod00271254
89.	On an Alteon D 6024 platform, could not assign more than 7200 CPS with the entire 40 CU.	prod00270205
90.	After a vADC rebooted from a panic, that part of the configuration was lost.	prod00271651
91.	When the filter action was "nat", the client NAT IP address options were missing from the Dynamic NAT tab	prod00272365
92.	Using WBM, the user lost access to a vADC.	prod00270782
93.	Using WBM, when monitoring servers and logged in as a real server operator, when the user tried to disable the server operational status from the Application Delivery > Server Resources > Real Servers pane, the status of that real server did not change.	prod00267518

Item	Description	Bug ID
94.	In an SLB filters environment, the IPv6 redirect filter used the proxy port to forward the packet to the server, while the redirect IPv4 filter did not.	prod00267952
95.	IPv4 PIP did not respond to ICMP requests.	prod00266690
96.	When managing Alteon logged in as notacacs or noradius, the following issues occurred:	
97.	When backdoor users logged in, the user was allowed or disallowed to change the admin password based on the previous user login.	
98.	The who command displayed nothing or displayed the previous user login name.	
99.	When logging in with the "noradius" user and admin password, Alteon disallowed changing the admin password.	prod00267750
100.	WBM did not display data.	prod00269798
101.	After disabling the Layer 3 filter, the health check started failing.	prod00269932
102.	In SLB environment with force proxy enabled, when the server group names exceeded 50 characters and first 50 characters being the same/identical, Alteon stopped processing the traffic.	prod00269641
103.	Out-of-order TCPv6 segments from the client to the MP caused a panic.	prod00270533
104.	A gmetric network does not work with the IPv6 nwclass having an element with a prefix 96 or less.	prod00270436
105.	In an SSH environment, when export/import of configuration (gtcfg/ptcfg) operations was performed, SSH sessions became stuck and remained so.	prod00267717
106.	The Alteon secondary device was inaccessible via the mgmt port and console.	prod00271313
107.	Using the command /info/slb/sess/dump, the configuration sync fails while dumping huge SLB sessions onto the console.	prod00271270
108.	The timezone was not correct in the techdata dump.	prod00269193
109.	In AppWall, after changing the publishing rules, the configuration was deleted when synching from the master to the backup,	prod00271705

Item	Description	Bug ID
110.	Using WBM, Alteon panicked when generating techdata.	prod00272026
111.	After rebooting the device, with configuration changes in diff, received errors after Apply.	prod00270718
112.	In a virtualization environment, vADCs were accessible over HTTPS, even though HTTPS access was disabled in the configuration.	prod00267647
113.	Using WBM, when trying to set the group real server status to connection Shutdown, the status kept displaying as enabled.	prod00267517
114.	In an SLB environment with filter sessions, when the primary server became available, even though backup clear (clrbkp) was enabled, the sessions that were bound to the backup server were not cleared on the filter.	prod00268273
115.	In an HA environment where the proxy configured under a filter was the same as the floating IP address, the filter's proxy entries were added to the ARP table with the device MAC on the backup server without checking the HA state, causing the backup server to reply to ARP queries.	prod00267748
116.	Using the CLI, in an SLB monitoring environment, in the virtual server statistics the highest sessions displayed were greater than the total sessions.	prod00268786
117.	Using the CLI, after running the command /c/l3/ha/service/dis, the incorrect description displayed.	prod00268975
118.	When the LDAPS module received the response from the server, the timestamp was not updated properly. As a result, the response time was calculated incorrectly, resulting a very long response time.	prod00270546
119.	When a client connected to Alteon using SSH with RADIUS authentication, a panic occurred.	prod00268122
120.	In an ADC-VX environment, when fetching the SSL chip status reboot, a panic occurred.	prod00271319
121.	Using WBM, the dashboard displayed the wrong throughput for a virtual server, even though there was no traffic for the virtual server.	prod00270114
122.	When RADIUS authentication was enabled with SSH user logins (usually with some scripts), vADCs panicked occurred due to NULL memory access.	prod00269221

Item	Description	Bug ID
123.	The VRRP status remained as Active-Active even if related VRs were erased, when that status should have changed to Active-Standby.	prod00271765
124.	A real server under /info/slb/group displayed in the BLOCKED state. When a group was not attached to any service or filter, no svc-pool entry was created for it. As a result, the wrong group was displayed with the /info/slb/group command.	
125.	Fix: If at least one group is configured for the real server with no svc-entry corresponding to the group, the svc-pool entry is preserved with the default health check and group ID. In addition, if there is not any svc-entry corresponding to the group that is being queried, the default health check for the real server is displayed.	prod00272043
126.	XML fragmented files over SIP were not forwarded to real servers. As a fix, the maximum dechunk datagram was resized from 8200 to 16400.	prod00270951
127.	In an SLB environment, when a content rule group contained a remote real server with a DSSP health check, an inconsistent DSSP health check status displayed.	
128.	**Note**: Config Apply is now not allowed if the content rule group contains a remote real server with the DSSP health check but the same real server is not part of the default service group.	prod00268432
129.	Using WBM, when adding interfaces to a VM, Flow Continuation Ingress ports could not be validated.	prod00265359
130.	When OCSP used DNS over management, after 64K DNS requests, failures occurred, causing Alteon to close the connection during SSL handshake.	prod00267964
131.	When Alteon sent a zero byte just before the EOM terminating sequence of 0x0d0a2e0d0a (part of the capture file) and the server did not answer, Alteon did not receive 250 responses from the server after sending e-mail contents (syslog messages).	prod00267296

Fixed in 32.2.1.0

Item	Description	Bug ID
1.	In an SLB environment with primary and standby devices, after syncing the configuration from primary to standby, the virtual service configuration did not display in the WBM of the standby device.	prod00270171
2.	In SLB monitoring using the APIs, the status of a real server that is part of a content rule and its health check failure reason could not be fetched using the API SlbStatEnhContRuleActionGroupEntry.	prod00270081
3.	In an SLB environment, although only 29 real servers were configured, when trying to configure a real server (with duplicate), the following error message was issued: `The maximum of 1023 Real Servers has been reached. To add new real server, first delete any unused Real Servers and apply.`	prod00269765
4.	In a virtualization environment, during configuration synchronization, the MP CPU of the vADC stayed at more than 80% for a long time.	prod00269753
5.	In an SLB environment with cookie persistent mode and forceproxy, the svclstconns metric always selected the same server as a collection of active connections, causing unequal load distribution for the service	prod00269642
6.	In an SLB environment with force proxy enabled, when the server group names exceeded 50 characters and first 50 characters were the same, after upgrading, Alteon stopped processing the traffic.	prod00269640
7.	When RADIUS authentication was enabled and a user logged in using SSH (probably using scripts), a vADC panic occurred due to NULL memory access.	prod00269220
8.	In an AppWall integrated with Alteon environment, when submitting a SECWA configuration, AppWall issued the following error: You are not authorized to edit this Web Application.	prod00269188
9.	In an AppWall integrated with Alteon environment, you could enable SSL for the authsrv (/c/security/websec/authsrv/ldap 1/ssl ena) even though SSL will not be used.	prod00269183

Item	Description	Bug ID
	As a fix, this command has been removed the from CLI.	
10.	Irrespective of the LACP port configurations, Alteon with STP off did not pass transparently BPDU from Cisco Nexus with MSTP.	prod00269094
11.	In an SSH environment, downloading an image using SCP was slow compared to downloading through FTP.	prod00269084
12.	In an SLB environment with DNS Responder VIPs, with mixed delegation/non-delegation traffic, a panic occurred.	prod00269062
13.	In an SLB environment with forceproxy, after configuration sync (with associated real server removed) from the master to the backup device, the device rebooted.	prod00269015
14.	Using CLI, an incorrect description was displayed for the command /c/l3/ha/service/dis	prod00268974
15.	In a monitoring environment, a panic occurred when continuously polling for a set of OIDs (slbStatLinkpfIpTable,pip6CurCfgTable, pip6NewCfgTable, pip6CurCfgPortTable, pip6NewCfgPortTable, pip6CurCfgVlanTable, pip6NewCfgVlanTable) with GET REQUESTs.	prod00268928
16.	When a data port was used for NTP, and the packets were received from non-configured NTP servers, the syslog message NTP illegal packet length for the dropped NTP packets was issued.	prod00268904
17.	In a VRRP environment, changes to a VR's priority during migration failover ended with an apply lock and high MP memory usage.	prod00268858
18.	In an SLB environment, when the HTTP2 policy was enabled with a group of one real server and one backup real server configured, when the active real server went down, traffic was not shifted to the real server configured as the backup, and the client received a 503 error.	prod00268741
19.	Using CLI, In an SLB monitoring environment, in the virtual server statistics the displayed highest sessions were greater than the total sessions.	prod00268723
20.	An HTTP head host modification rule could be changed or modified using CLI but not using WBM	prod00268688

Item	Description	Bug ID
21.	Using WBM, when configuring an SSL service, the certificate and the group were set and configured even when the user chose the 'any' option. This caused the newly configured APP to function slowly.	prod00268685
22.	In an SLB environment, when a FQDN real server was changed, Alteon was not updated for more than a half an hour after the change, and it changed only after the FQDN real server was disabled and then enabled.	prod00268654
23.	In an HA environment with the same network class associated to a SmartNAT and also a real server, the ARP for a few of the PIPs in the network class range were not answered.	prod00268645
24.	In an HA with SLB environment, even though the PIP Network Class Range was enabled to receive GARP `(/c/l3/ha/nwclgarp ena)`, the GARP was not sent for all IP addresses from the proxy network class range.	prod00268505
25.	The SNMP CLI configuration commands /c/sys/ssnmp/rcomm and `/c/sys/ssnmp/wcomm` in accepted a NULL string, resulting in errors when adding or removing real servers from a group using WBM.	prod00268503
26.	In an environment with health checks, when the SNMP health check was configured, the weight displayed but it did not display when the SNMP heath check was part of a LOGEXP.	prod00268455
27.	In an SLB environment, when a content rule group contained a remote real server with the DSSP health check, an inconsistent DSSP health check status displayed. **Note**: A **Config Apply** action is now not allowed if the content rule group contains a remote real server with a DSSP health check and the DSSP health check is not part of the default service group.	prod00268431
28.	In a virtualization environment on a vADC, the SP memory displayed as HIGH all of the time, while the device had no traffic and no SLB configuration.	prod00268394
29.	In an SLB environment, a filter configured with the protocol as "50" was not restored after rebooting the device.	prod00268390

Item	Description	Bug ID
30.	In an SLB environment, when the real service port (the rport of a virtual service) was configured with a value less than 5 (except for multiple rports/IP addresses service scenarios), the traffic on these rports failed. For the fix, a validation has been added to allow rport 0-multirport or 1-ipservice or 5-65534.	prod00268324
31.	In an SLB environment with filter sessions, when the primary became available, even though backup clear (clrbkp) was enabled, the sessions that were bound to the backup server were not cleared on the filter.	prod00268272
32.	When the FastView license expired, Alteon also lost the compression license.	prod00268238
33.	When the number of basic health check components used in the logical expression-based health check object was changed, such that the new expression had fewer objects than the old expression, a software panic occurred.	prod00268236
34.	When a client connected to Alteon using SSH with RADIUS authentication, a panic occurred.	prod00268120
35.	Using WBM, HA Real Server Tracking could not be configured.	prod00268053
36.	In an HA environment with an SLB configuration, configuration of the backup real server and/or backup group was not synced to the peer device.	prod00268048
37.	In a virtualization environment, when a vADC was deleted and when a new vADC was created with same vADC number, the old configuration was restored in the newly created vADC.	prod00268003
38.	When Alteon sent a zero byte just before the EOM terminating sequence of 0x0d0a2e0d0a (observed in the capture file) and the server did not answer with anything, Alteon did not receive a 250 response from the server after sending the e-mail content (syslog messages).	prod00268002
39.	When OCSP used DNS over management, after 64K DNS requests, failures occurred, causing Alteon to close the connection during SSL handshake.	prod00267963
40.	In an SLB environment with forceproxy and an ICAP and SSL Inspection configuration, if the ICAP server terminated or did not respond, a panic occurred.	prod00267959

Item	Description	Bug ID
41.	In an Alteon Integrated with WAF environment, the Parameter name within the parameters filter did not match the REGEX.	prod00267953
42.	In an SLB filters environment, the IPv6 redirect filter used a proxy port to forward packets to the server, but the IPv4 redirect filter did not.	prod00267951
43.	In an SLB environment, when operationally disabling or enabling a real server in a server group, a syslog message indicating the action was not generated.	prod00267949
44.	In an SLB environment with forceproxy configured and with the HTTP2 Gateway implemented caused high SP memory usage.	prod00267931
45.	Using WBM, in the Monitoring > System > Maintenance pane, when the resolution changed, the Export button for techdata was located in the wrong position.	prod00267870
46.	In an OSPF environment, Alteon was unable to update the peer with any change to the OSPF parameter.	prod00267852
47.	Using WBM, even though a user logged in with the "admin" user, the user could not operationally disable a real server.	prod00267832
48.	In an SSL environment with a certificate repository, after manually importing all of the keys (clear text RSA keys) and certificates to both the master and backup devices, when trying to associate the certificates to their corresponding VIPs, configuration sync failed, an error that a key was missing on the backup device displayed on the master device.	prod00267781
49.	When Alteon was managed with a "notacacs" and "noradius" login, the following issues occurred: • When backdoor users logged in, permissions to change the admin password were based on the previous user login • The who command displayed nothing or displayed the previous user's login name When logging in with the "noradius" user with the admin password, the user could not change the admin password	prod00267749
50.	In an HA environment, when a proxy was configured for a filter was same as a floating IP address, the filter's proxy entries were added to the ARP table of the backup with the device MAC address without checking the HA state, causing the backup to reply to ARP queries.	prod00267746

Item	Description	Bug ID
51.	In an HA environment, the filter proxy was added to the ARP table with the device MAC address instead of the HA MAC address, causing Alteon to not forward dynamic NATed DNS responses to the internal DNS server.	prod00267723
52.	In an SSH environment, when the export/import of configuration operations were performed using gtcfg or ptcfg, SSH sessions became permanently stuck.	prod00267716
53.	Using APSolute Vision, when accessing the *High Availability* tab, the following configuration error was issued: 404 Not Found: REST API lookup failed	prod00267695
54.	In an HA environment, even though the configurations were the same on both the active and standby devices, a warning message related to an HA configuration mismatch was issued.	prod00267681
55.	In a BGP environment, when deny route redistribution was disabled for a BGP peer, although the BGP peer went down and came back up, Alteon stopped sending advertisements.	prod00267678
56.	In a virtualization environment, a vADC was accessible over HTTPS, even though HTTPS access was disabled in the configuration.	prod00267642
57.	Even though access on a device's management port was restricted using an access-list (/cfg/sys/access/mgmt/add), it did not work properly.	prod00267587
58.	When services were moved from the master node to the backup node, no SNMP traps were sent to the Monitoring server. **Note**: These traps were omitted when implementing the new feature "Extended HA". Traps, syslog messages, and log messages have been updated, extended, or replaced with new messages.	prod00267571
59.	Using WBM, in an SLB environment, when configuring a virtual service in the Content Rule pane, an invalid URI was accepted for the redirect URI configuration, while the CLI displayed an error message for that invalid URI.	prod00267552

Item	Description	Bug ID
60.	Using WBM, while monitoring the servers and being logged in as a real server operator, when trying to disable the server operational status through Application Delivery > Server Resources > Real Servers, the status of that real server did not change.	prod00267516
61.	Using WBM, when trying to set the group real server status to connection shutdown, its status kept displaying as enabled.	prod00267515
62.	When Alteon received an IPv6 address with a full-length address (more than 32 characters including colons – for example, 2101:2101:2100:2100:2101:2100:2100:2101) and processed the IPv6 fragmented packet, a panic occurred.	prod00267493
63.	In an SLB environment with the group metric **svcleastconns** and a multi-rport scenario, load distribution to the real server was not proper.	prod00267433
64.	Using WBM in an SLB environment, the virtual server copy did not work properly, and the copied virtual server had different settings for cookie and server group.	prod00267161
65.	When performing an Apply of a configuration imported using REST API, an error was issued.	prod00267152
66.	In an SSL environment, certificates that were set to expire after 100 years displayed as expired.	prod00267056
67.	Pings to PIP/VPR were blocked.	prod00266689
68.	Using WBM, users with user roles Operator, L4 Operator, SLB Operator, and SLB Viewer could execute **Apply** and **Save** commands for a configuration created by the Administrator.	prod00266672
69.	Using WBM, you could modify the privacy and authentication settings for SNMP default users.	prod00265974
70.	Using WBM to create route maps, the following parameters had incorrect values for the route map object: Local preference, Metric, Weight	prod00264251

Fixed in 32.2.0.0

Item	Description	Bug ID
1.	Using WBM, in the Service Status View pane, the real servers incorrectly displayed.	prod00267276

Item	Description	Bug ID
2.	Using WBM, in the Service Status View pane, the filter option in the displayed data did not work as expected.	prod00267217
3.	After upgrading to Alteon version 32.1.x, you needed to log in two times to get access to Alteon VA, ADC-VX, or vADC.	prod00267210
4.	Using WBM, the complete IPv6 Management IP address did not display.	prod00267208
5.	In an SLB environment, when real servers were moved from one server group to the other, although the real servers were moved away from a group, the old sessions still remained and did not age out.	prod00267134
6.	In an SLB environment, after the primary real server went down and the backup real server and group took over, the service became inaccessible.	prod00267089
7.	Using CLI, on a vADC with a QAT SSL card, in the output from the stats/sp x/mem command, the tech support dump (tsdump) did not contain the QAT driver memory usage.	prod00267071
8.	Alteon did not handle a specific condition related to FQDN and went into an inconsistent state.	prod00267062
9.	In a Global SLB environment, when the network gmetric used a network class as the source IP address, the DNS response was incorrect.	prod00267044
10.	In an inbound link load balancing Smart NAT environment, the Availability metric in the SmartNAT GSLB rule was not processed, causing an improper ISP links order.	prod00267020
11.	Using WBM, from the *Certificate Repository* pane, you could not perform a search in the table.	prod00266986
12.	In a configuration sync environment, after a routine configuration change, the MP CPU reached 100%.	prod00266964
13.	In an SLB environment, when overlapping IP addresses were defined in a network class configuration with exclude enabled, and when an exclude range was a subset of the other exclude range, the filter defined with this network class fired incorrectly for an excluded IP address, causing the filter to misfire.	prod00266924

Item	Description	Bug ID
14.	In a Global SLB environment, when the network element was of type subnet, the fromIp was incremented by 1 to skip the network address and the toIp was decremented by 1 to skip the broadcast address, causing a large value for the IP count, and Alteon prevented the subsequent network elements and network classes from being added to the internal tables. This caused a GSLB SIP lookup failure for missing network ranges.	prod00266917
15.	In an SLB environment, filter processing processed the traffic addressed to the SmartNAT dynamic address/PIP addresses, failing the DNS amplification scan.	prod00266909
16.	When the NTP server was configured over IPv6, the IPv6 address was not recognized on routing through the management port IPv6 address.	prod00266888
17.	Using WBM, when deleting a Layer 3 gateway, the gateway entry did not disappear, but a stale entry for the same gateway ID was displayed in the disabled state and with an IP address 0.0.0.0 and VLAN 0.	prod00266880
18.	In an HA environment, when duplicate IP addresses were configured for DNS responder virtual servers and regular virtual server IP addresses on the master device, configuration sync to the peer device did not work, ending with errors.	prod00266879
19.	In a management environment, when different management certificates on the master and backup were configured (/c/sys/access/https/cert), configuration sync failed without a meaningful error message.	prod00266876
20.	In an SLB environment with dynamic address mode with an AppShape++ script (source NAT), Alteon forwarded the traffic to the server with the source MAC address set to the client MAC address instead of the Alteon/HA MAC address.	prod00266869
21.	Using WBM, in the Certificate Repository Import screen, the correct certificate file was not imported when trying to use the Browse button	prod00266868
22.	In a Link Load Balancing (LLB) environment, after restoring the backup configuration using `get config`, the LLB-related configuration `(/c/slb/gslb/network x/wangrp WAN-Group-1)` was lost.	prod00266817
23.	Using WBM, configured AppShape++ script did not display.	prod00266779

Item	Description	Bug ID
24.	When the NTP was set over a data port and the NTP server was down, an incorrect SNMP Trap (Critical Temperature Trap) was sent when the NTP request timed out.	prod00266743
25.	In an Azure environment, when the RADIUS server was on a different network other than the management network, RADIUS authentication did not work.	prod00266675
26.	On a Cavium-FIPS platform, the PKCS12 file of the CA-group was encrypted and larger than 16K in some cases and failed to load.	prod00266654
27.	In an SLB environment, after configuring the real server weight using the CLI command `/c/slb/real x/weight`, a panic occurred.	prod00266636
28.	In an SLB environment with an acceleration environment, due to connections being reset, some application outages and traffic failures were observed.	prod00266633
29.	In an SLB environment, on a real server, due to packet drops in the SPs, TCP latency occurred for health check packets.	prod00266603
30.	In in Outbound Link Load Balancing environment, the transparent health check to a destination server was sent from an inappropriate port/VLAN (WAN Link).	prod00266602
31.	While using a REST API call to export the configuration, Alteon ignored the path and name specified in the API request. Alteon generated a name and transferred the file to the root folder of the SCP server instead.	prod00266593
32.	When importing a key which is not encrypted (plain text), due to minimal passphrase that was set, the import caused all onboarding of HTTPS applications that use non-encrypted certificates to fail.	prod00266573
33.	In a monitoring environment, invalid TRAP OIDs were sent for the SP CPU Pressure On/Off. **Note**: The correct MIB OID has been added to the trap.c and GENERIC-TRAP-MIB.MIBs: altSwSpCpuPressureActivatedTrap - 1.3.6.1.4.1.1872.2.5.7.0.214 altSwSpCpuPressureDeactivatedTrap - 1.3.6.1.4.1.1872.2.5.7.0.215	prod00266559

Item	Description	Bug ID
34.	In a VRRP environment with an SLB configuration, the session move operation did not get synchronized to the backup, leading to session mirroring not working, causing statistics discrepancies on the backup devices.	prod00266543
35.	In an SSL environment, when changing the cipher suite from TLS 1.2 to the User Defined " TLS_ECDHE-RSA-AES128-GCM-SHA256" cipher, the AX configuration was corrupted and the service to which the SSL policy was attached stopped working.	prod00266530
36.	In an environment with AX configured, the primary and secondary vADCs panicked one after the other.	prod00266525
37.	In a Layer 7 environment, if the original request did not contain any query, Alteon did not remove the query separator "?" in the redirect URI.	prod00266453
38.	Using WBM, in the *Outbound LLB Rule* pane, the IP address/network could not be edited.	prod00266452
39.	In a virtualization environment, due to vADC management mask settings not considered for locking, when attempting to get access by the management interface to a vADC, access was given to another vADC.	prod00266409
40.	In a VRRP environment, when health checks failed on the backup, statistics discrepancies (incorrect number of sessions to the real servers) occurred on the backup device.	prod00266339
41.	In an SLB environment, when there was a change in the virtual server configuration (disable/enable), the session move operation via CLI did not move the session to a different real server.	prod00266338
42.	When the time zone was set to Asia/Jerusalem (GMT offset +02:00), as the daylight saving setting was not taken into account, Alteon displayed the incorrect time from the month of October.	prod00266305
43.	In an SLB environment with HA, after the failover, uneven load distribution occurred on the new master device.	prod00266157
44.	Using WBM, In the certificate repository, when importing an intermediate CA, the size displayed as 0. **Note:** After the fix, the size is not calculated and is displayed blank.	prod00266154

Item	Description	Bug ID
45.	In a Cloud environment, when there was a VSAN failure, and when switching to redundant storage from the VMware side caused an I/O failure for a few seconds, the MP was stuck, causing the watcher to trigger the soft reboot and an outage of all Alteon VAs.	prod00266092
46.	In an SLB environment, when real servers were allocated to multiple virtual services and a **Revert Apply** was performed, the session table was deleted automatically.	prod00266012
47.	Using WBM, with the "User" role, configuration sync could be performed even though the "User" account should not be able to do this.	prod00266008
48.	Using WBM, on an ADC-VX, when attempting to log out of WBM, the device kept the user logged in.	prod00266006
49.	While running a vDirect script on Alteon devices, it took more than 20 minutes to display the output, or the script timed out with no result.	prod00265982
50.	In an SSL environment, the user was unable to change the ciphers string under the advanced HTTPS health check.	prod00265975
51.	Using WBM, in the **Configuration > Setup > High Availability** pane, there was no option to delete VR Group settings.	prod00265973
52.	Using WBM, in an SLB environment when configuring a virtual service, the cookie configuration changed after making a change to the virtual server even if the user did not modify the persistent binding (pbind) cookie settings.	prod00265867
53.	Using WBM, when duplicating a real server, sometimes the "ERR json parse failed" message was returned.	prod00265865
54.	Using WBM, from the health check pane **Configuration > Application Delivery > Health Check > add**, the **Always Perform Health Check** field displayed twice.	prod00265861
55.	Using WBM, you could not set the action as Discard for a virtual server.	prod00265857
56.	When performing SNMP monitoring on SSL offloading stats (FE/BE), due to a memory corruption, a panic occurred, and the device rebooted a few times.	prod00265843
57.	In an Alteon integrated AppWall environment, SSL sessions were not created for specific tunnels.	prod00265812

Item	Description	Bug ID
58.	In a virtualization environment for a vADC, after performing a Revert Apply on an ADC-VX, the admin password changed back to the default password (admin) on the vADC.	prod00265710
59.	When **agTftpCfgFileName** was more than 83 characters, exporting the configuration with SCP through the REST API server failed.	prod00265672
60.	If the data-class entry contained a backslash (\) character and configuration sync was performed, the configuration was not synced correctly.	prod00265617
61.	In an SLB environment, when the client connected directly but through different VLANs for forward and backward traffic, the SP CPU utilization became high even though the amount of traffic was not increased, causing a degradation.	prod00265558
62.	In a Global SLB environment, when a configuration **Apply** was performed during the periodic statistics calculation, when the internal data structures used in GSLB were reset and repopulated, an illegal access occurred, causing a panic.	prod00265544
63.	When a new virtual server with a service-based proxy address and a corresponding VPR were both configured within the same **Apply** operation, Alteon did not display the VPR status in the VRRP and the ARP cache.	prod00265538
64.	In an SLB environment, if the configuration had a disabled virtual server and one of the services of the virtual server had a non-existent AppShape++ script, the configuration could not be saved.	prod00265537
65.	In a virtualization environment, one of the vADCs hung and panicked.	prod00265451
66.	In a virtualization environment, when the LACP was configured with 40G ports, during the vADC boot-up frequent gateway health check failures occurred.	prod00265434
67.	Using WBM, when using the SSL Inspection Wizard, when performing a revert, in certain conditions a REST API 405 error displayed even though the Revert was successful.	prod00265381

Item	Description	Bug ID
68.	In a virtualization environment, when the vADC IP address/net mask combination was configured incorrectly and failed to add the relevant gateway, disabling and then enabling vADCs caused Linux ifconfig errors, resulting in management connectivity loss for the ADC-VX. **Note:** This issue was addressed by not allowing invalid gateway settings and ensuring that the ADC-VX and vADC management IP addresses are defined on the same network.	prod00265371
69.	In an HA environment, during configuration sync, the real server configuration under HA triggers were not synced to the peer correctly.	prod00265322
70.	In a virtualization environment with HA configured, during upgrade, one of the vADCs hung and panicked.	prod00265317
71.	In an SLB forceproxy environment with IP service and filters configured, when performing an **Apply**, Alteon attempted to add a service mapping entry (needed for IP address and Port translation) for a filter, but instead accessed data meant for the virtual service, causing a panic.	prod00265289
72.	In a BGP environment, you could not import the default gateway alone or any other "range of IP"/"IP" separately.	prod00265280
73.	On the 6024 platform with 32 GB RAM, the vADC-5 license could not be installed on top of Alteon NG/NG+.	prod00265279
74.	In an SSL environment, when configured with client-IP, SSL-ID persistency and with SSL-ID traffic, a panic occurred.	prod00265243
75.	When dumping the FDB entries in the SP using the `/maint/debug/spfdb` command, only 8K entries were dumped when the Max size of the FDB per SP was actually 16K.	prod00265212
76.	In an SNMP monitoring environment, when accessing the MIB OID 1.3.6.1.4.1.1872.2.5.4.3.14 corresponding to runtime instances of a health check, a panic occurred.	prod00265181
77.	Using WBM, when logging in as a TACACS user, the following error message displayed: `mgmt: The language defined at the TACACS server is not recognized. Using global language.`	prod00265166

Item	Description	Bug ID
78.	In an HA environment with session mirroring enabled after failover, the new master did not mirror sessions to the new backup.	prod00265127
79.	In an Alteon integrated with AppWall environment, when the Accept-Language header was missing, AppWall responded with a 302-response code.	prod00265072
80.	If the IDSChain was not working for subsequent fragments or did not forward fragment IP frames that matched the filter, the RADIUS Server communication broke.	prod00265053
81.	Using WBM, in the Layer 7 Load Balancing Content Class Configuration pane, if the content class string contained a backslash (escape characters), the REGEX text field value displayed incorrectly.	prod00265029
82.	In a monitoring environment, fetching the Layer 3 Interface statistics using REST API did not work.	prod00264975
83.	Using CLI, with verbose 1 set, when a health check that was associated to a server group or real server was deleted, a prompt for user input did not display.	prod00264970
84.	In an HA environment configured with SLB, the mirrored P-session on the backup vADC was bound with the wrong real server group, causing services to get hampered.	prod00264936
85.	When PIP was configured under a DNS-UDP stateless service, as it is not applicable it was ignored. **Note:** As a fix, a warning message has been added only in CLI.	prod00264906
86.	In an HA environment, the backslash ("\") character in the LDAP username was not synced to the peer device, and WBM did not display them.	prod00264903
87.	Using WBM, when a real server was deleted from a GSLB network, as these entries could not be reused even after deletion, once all the maximum 128 entries were exhausted, the following error message displayed: `Real server precedence table is full`	prod00264835

Item	Description	Bug ID
88.	On 4408 and 5208 platforms, when upgrading from versions earlier than 30.2.8.0 to version 30.2.8.0 or later, and the ports were enabled for management access, this resulted in an inconsistent configuration after the upgrade.	prod00264787
89.	The image upload on the management port using SCP was slower than using FTP.	prod00264763
90.	In an AppWall integrated with Alteon environment, for a virtual server that had an AppWall tunnel, Alteon stopped processing traffic.	prod00264676
91.	In an SLB environment with health checks configured, with an HTTP health check there was no difference in the failure status regardless of the failure reason. If the checked file was removed (404 code), the file required authentication (401 code) or an internal server error (500 code), for all cases the following error displayed: `Reason: Server's response is not as expected`.	prod00264674
92.	In an Alteon HA environment, when configuration sync failed with a Global SLB/Link Load Balancing configuration, after the failure the new configuration moved automatically to the current configuration without performing an Apply operation.	prod00264673
93.	In a DNS environment, Alteon does not include the edns0 client subnet in the DNS response.	prod00264633
94.	In an SLB environment with AppShape++ scripts, when adding an AppShape++ script to a virtual server without creating the service on that virtual server and performing an **Apply**, an **Apply** error did not occur, and any further configuration change on the virtual server and performing **Apply**, the `Pending configuration` message always displayed.	prod00264597
95.	Alteon allowed management access via data ports on IPv6 even though the access was disabled.	prod00264531
96.	In an HA environment, after synchronizing the configuration from the master device, the health checks for a real server failed/toggled on the backup device.	prod00264498
97.	Due to a debug tool that was configured for OpenSSL, HTTPS health checks caused 100% CPU usage on the MP, introducing delays in HTTPS health checks.	prod00264468

Item	Description	Bug ID
98.	When configured a URI under a CDP group with the left parenthesis ("(:) character in the URI and with traffic, a panic occurred	prod00264433
99.	In an HA environment with SLB configured, after configuration sync, when Alteon attempted to configure the backup real server as a backup group, the backup real servers in the group were removed on the peer device.	prod00264432
100.	In an IPv6 environment, even though IPv6 local networks were configured, Alteon sent a server response to the default gateway instead of sending it directly to the connected client. As a result, a real server could not be reached from the subnet.	prod00264431
101.	In an SLB environment, incorrect statistics were displayed while fetching virtual service statistics (`via /stats/slb/virt`), the statistics for a real server (Current, Highest, Total sessions) displayed as 0, even though the real server handled the connections.	prod00264430
102.	On an Alteon VA platform, although the new VLANs were defined to contain default ports, after the reboot, the configuration was always pending in the diff operation.	prod00264390
103.	In a forceproxy SSL environment, internally when MP and AX went out of synchronization, Alteon continued to send an old certificate even after installing a new certificate.	prod00264339
104.	Using WBM, from the **Configuration > Application Delivery > LinkProof > Inbound LLB Rules** pane, there were several issues during configuration.	prod00264289
105.	Using WBM, with SLB monitoring, when a content rule was used with a real port, the session counter displayed incorrectly.	prod00264285
106.	Using WBM, in an Inbound Link load balancing environment, the NAT address configuration was missing in the Global SLB's client network rule page.	prod00264245
107.	Using WBM, when attempting to configure HTTP modification for header removal, Alteon forced the user to input the header value.	prod00264244
108.	Using WBM, in an SSL environment in the Export tab, even though the "certificate and key" option was selected to export, only one **Export** button displayed.	prod00264233

Item	Description	Bug ID
109.	In an HA environment with script health checks configured, after deleting/adding/modifying a script and performing configuration sync, there was a discrepancy in the health checks between the master and the backup device.	prod00264172
110.	In an SLB environment, when a real server with the same IP address was configured for different groups, and each of the groups were configured with the same logical expression health check, Alteon failed to evaluate the logical expression except the group in which the real server came up first. The rest of the real servers remained down in respective groups.	prod00264146
111.	In an environment with a configuration where the client packet comes into Alteon through one VLAN (ingress) and after server processing, the response packet leaves to the client in another VLAN (egress), duplicate IP FDB entries got created for external IP addresses.	prod00264048
112.	In an SSL environment with Cavium cards, after upgrading a couple of certificates and performing **Apply**, a panic occurred.	prod00264047
113.	In a virtualization environment when ADC-VX rebooted with a panic, the RADIUS secret became corrupt, and the RADIUS login failed.	prod00264025
114.	Using CLI, when executing a non-existing or hidden command with the /maint/pktcap menu, an error was not issued. **Note:** As a fix, all the hidden commands under `/maint/pktcap` were removed and cannot be executed.	prod00264010
115.	In an SLB environment with filter processing enabled, VMAed traffic source MAC learning did not occur, causing traffic to be flooded on all the VLAN ports, causing higher throughput utilization.	prod00264009
116.	In an SLB environment with multiple rports, when a new real server was created with addports and if it was associated to more than one service, if any of the service health checks was toggled, Alteon forwarded client requests to the server on the service port rather than on the real server's service port (rport = addport of the real server).	prod00263992

Item	Description	Bug ID
117.	In an SLB environment, when a particular sequence of SLB configuration steps involving a HTTP virtual service and another virtual server along with **Apply**, the configuration became corrupted.	prod00263986
118.	In an SLB environment, when a group was configured with one or more real servers (by manual configuration), when deleting or removing real server(s) from the group, the following Apply error displayed: `Error: Real server group 100 associated to virtual server 100 service 80 is not defined`	prod00263985
119.	In a virtualization environment, when autosync was enabled on both ADC-VX and vADCs, configuration changes to the definition of the primary vADC from the ADC-VX triggered the sync to loop between the vADCs.	prod00263984
120.	For the BWM-history-related e-mail, when the SMTP 'To' user was not configured, but when Alteon tried a number of times to send this e-mail, after a while Alteon did not respond to SSH/HTTPs via management.	prod00263983
121.	Using WBM, when a configuration dump was performed on a FIPS device, the following error displayed: `Error: Configuration import/export via HTTP is already running.`	prod00263982
122.	In an SLB environment, you could not configure a virtual server with a different protocol and Alteon returned the following error: `Error: Virtual server v1 has the same SIP SLB group id as virtual server v1-udp.`	prod00263980
123.	In a virtualization environment with HA, when p-session sync updates were received from the master, the backup attempted to become the master. This was no longer an issue when the p-session sync was configurationally disabled.	prod00263979
124.	In an AppWall integrated with Alteon environment, when troubleshooting some false-positive "HTTP reply not RFC-compliant" events were issued that indicated that Request Data and Reply Data under Forensics were identical.	prod00263587
125.	There was a discrepancy between the peak compressions usage command output (/info/swkey) and syslog messages.	prod00261525

Item	Description	Bug ID
126.	In a SmartNAT environment, the concurrent sessions value of the WAN link server was much larger than the displayed session statistics.	prod00261497
127.	Due to a kernel issue, Alteon went into ULP mode and could not be accessed via Telnet, SSH, HTTP, or HTTPS while the Management IP address was reachable only over ICMP.	prod00260720

AppWall

Item	Description	Bug ID
1.	Fixed a rare failure in the HTTP parsing process.	DE43435
2.	Fixed a rare failure in HTTP Response parsing process.	DE43438
3.	The client IP address was not sent in the security page.	DE42288
4.	For some types of security violations, the case number shown in the security page was 0.	DE41895
5.	When the server response body was in JSON format, the BruteForce security filter failed to block the IP address for a bad login after the IP address reached the threshold limit.	DE44726
6.	BruteForce security events syslog messages had the wrong event type value: learning instead of security.	DE45524
7.	Fixed PCI compliance Report data in APSolute Vision in the 6.5.5 section referring to Improper error handling.	DE23276
8.	Primary LDAP server failure detection and failover to the secondary server did not work under certain conditions.	DE42480
9.	When a non-authenticated user attempted to access a Web page, the Authentication Gateway redirected the user to the login process and upon successful authentication, redirected it back to the originally requested page. The redirection back to the originally requested page did not preserve the original HTTP request parameters.	DE42479
10.	Under rare conditions, Alteon stopped processing traffic on a VIP with an Application security policy.	DE42240

Item	Description	Bug ID
11.	When the Authentication Gateway received requests from an old version of the Internet Explorer browser, AppWall redirected successfully authenticated users to the authentication process.	DE42339
12.	In Monitor deployment mode and in Alteon OOP mode, both Request and Response data in the security logs for non-RFC-compliant HTTP Reply displayed Response data.	DE40221
13.	Added a terminating chunk to a 302 chuck encoding reply with an empty body.	DE43566
14.	Was unable to refine forensic events for SafeReply credit cards.	DE44273
15.	Login monitoring settings in HTTP custom headers were ignored.	DE43567
16.	For AppWall running on Alteon version 32.0.1.0, adding a DefensePro the Defense Messaging configuration using port 443 failed.	DE42698
17.	Fixed issues with AppWall policy synchronization between the master and backup Alteon platforms.	DE44274 DE44670
18.	A rare failure could occur when an HTTP response could not be properly parsed.	DE44316
19.	A long JSON value within a query parameter could cause a failure.	DE44890
20.	For the Database Security Filter ignored parameters, the logs displayed the length of parameter name instead of the parameter param value.	DE44869
21.	Fixed the “Server Name” field value in the Security logs for AppWall running on Alteon.	DE45098
22.	Fixed a possible failure in AppWall once applying a policy change.	DE34945
23.	REGEX support was added for both.	DE44273
24.	API calls for NTP servers sometimes were not successful.	DE41308
25.	The Database.kcf file was not replaced during the upgrade process to version 7.5.8.	DE42077

Item	Description	Bug ID
26.	The ptcfg command did not work properly in Alteon. A "Failed to create AW configuration File" message was shown.	DE44559

Fixed in 32.1.0.0

Version 32.1.0.0 includes all field bugs available in version 31.0.6.0.

Item	Description	Bug ID
1.	Using the CLI, when executing the command `/stat/spx/allcpu`, the SP CPU statistics that displayed was 0%.	prod00263872
2.	In an SLB environment with ICAP messages chunked, due to parser issues in Alteon, a panic occurred.	prod00263781
3.	Using WBM, when creating a new HTTP or HTTPS service, Alteon added an extra command for FTP for the service.	prod00263714
4.	In an SLB environment, when enabling an SNMP health check for a group with the roundrobin metric, a panic occurred.	prod00263635
5.	In a Geo Proximity environment, a software upgrade caused an invalid GEO configuration, which led to an outage.	prod00263469
6.	In an SLB Filter environment with dbind forceproxy, dport configured with a range and rtsrcmac enabled did not handle the return traffic for port range except the starting port. For example, for dport range 8080-8443, traffic worked only for 8080 but not the other ports in the range.	prod00263325
7.	In an SLB environment, when the Script health check was configured with nonat for a virtual service, the incorrect source IP address was used by Alteon.	prod00263231
8.	In a VRRP active-standby configuration, when configuration sync was performed, though the corresponding virtual service was UP, the virtual router (VSR) went into the INIT state.	prod00263222
9.	In an SLB environment with FQDN servers configured: • The DNS response was received during a Revert Apply or configuration sync, causing a problem. When a Revert Apply or configuration sync was performed during service, the DNS response caused a problem.	prod00263196

Item	Description	Bug ID
10.	In a virtualization environment on an ADC-VX platform, with vadcadv enabled, when an upgrade was performed from versions earlier than 30.5.3.0/31.0.3.0 to version 32.*x*, the configuration appeared in **diff** after reboot.	prod00263131
11.	Using WBM, in the **Monitoring > LinkProof > WAN Links > Per WAN Link IP/ID and Monitoring > LinkProof > WAN Link Groups** pane, the statistics did not display correctly.	prod00263121
12.	In the *Monitoring* perspective, sometimes empty e-mails were randomly generated.	prod00263061
13.	In an SLB environment with rtscmac enabled, the source MAC address of a virtual server would change during the same session, causing packets to be blocked by ISP.	prod00263043
14.	Using WBM, in the **Configuration > Application Delivery > SSL > Certificate Repository > Intermediate Certificate** pane, the key type of the intermediate certificate was displayed as unknown.	prod00262965
15.	In an SLB environment with IPv4 virtual servers and an IPv6 real server, when using IP version conversion and some SLB related-configuration changes were made, misleading syslog messages were issued.	prod00262937
16.	When upgrading an ADC-VX platform, Alteon became stuck in a loop during the upgrade and experienced a panic, requiring a hard reset.	prod00262927
17.	In a Layer 7 environment, the redirection URI under Content Classes took the variable query $QUERY keyword only after the custom queries.	prod00262866
18.	In an SLB environment with SSL offload, and with forceproxy enabled and rtsrcmac enabled, and with a filter enabled on the server port, when the server packets were dropped in the SP after server processing, SSL offloading did not work properly.	prod00262841
19.	Using CLI in an SLB Monitoring environment, the octet count displayed by the virtual server statistics command `/stats/slb/virt x` was incorrect.	prod00262825
20.	Alteon failed to import encrypted private keys that had a long password (> 40 characters).	prod00262772

Item	Description	Bug ID
21.	In an SLB SIP environment with AppShape++ scripts, a SIP parser issue occurred.	prod00262760
22.	On an Alteon 5208 S platform, depressing the PWR button for a few seconds did not perform a graceful shutdown of the platform.	prod00262716
23.	In an SLB monitoring environment with names configured for real servers, when displaying the real server group statistics with the CLI command `/stats/slb/group`, the real server name was listed instead of the IP address. The fix was to change the heading to "IP Address/Name". The real server name displays if it is configured. Otherwise, the IP address displays. This also applies to the commands `/stats/slb/virt` and `/stats/slb/sp x/virt`.	prod00262715
24.	Using WBM in an SLB environment, you could not configure POP3 over SSL (TCP port 995).	prod00262692
25.	After disabling the default user, the command `/cfg/sys/access/user` did not display the correct value.	prod00262676
26.	In an SLB environment with filters, even though rtsrcmac (Return to Source MAC) was enabled for a filter, ICMP reply packets corresponding to the filter session were routed to the VLAN gateway instead of the client port.	prod00262649
27.	Using WBM in an SLB environment, when a virtual router and Proxy IP address under a virtual server were the same, the following error displayed: `The IP Address of Virtual Router 2 conflicts with the Client NAT (PIP) IP address`	prod00262620
28.	During a Nessus security scan on Alteon, due to opening and closing SSH connections frequently, a panic occurred.	prod00262619
29.	Using WBM in an SSL environment, you could not generate a CSR.	prod00262589
30.	Using the CLI, the command `/info/l3/ha` output information was misleading (it displayed VRRP information).	prod00262578
31.	In an SLB environment with an IP service configured with the svcleast metric, traffic was distributed to the same server, leading to uneven load balancing of the traffic.	prod00262568

Item	Description	Bug ID
32.	In an SLB environment with content classes configured, when selecting a different group's real server per the content class, rather than a group-real server being configured on the virtual service, the front-end session abruptly aged out/terminated, causing service issues.	prod00262567
33.	When logged in with a backdoor-enabled user and with RADIUS enabled, after running the `/oper/passwd` command to change the user's password, the displayed username was incorrect, the syslog message was generated was with incorrect username, and the **Who** command displayed the incorrect username.	prod00262566
34.	In an environment with a slower client (LG K220) and a faster server, after enabling HTTP2, high SP CPU usage occurred.	prod00262565
35.	Using WBM, in a DNS Proxy configuration, you could not roll back the default group configuration to 'none'.	prod00262545
36.	After using the CLI command `/info/transceiver`, Alteon either rebooted unexpectedly or Alteon's traffic was stuck for about 13-15 seconds.	prod00262540
37.	Due to an ND issue, a panic occurred and caused a reboot.	prod00262521
38.	Due to an unauthorized Rx queue disable mode of I210 MACs, Alteon dropped some packets.	prod00262519
39.	Using WBM in an SLB SSL environment, attempting to create a new authentication policy also added the passinfo default configuration, causing the Apply to fail.	prod00262518
40.	Using WBM, when generating a server certificate with SHA256, the certificate was instead generated with SHA1.	prod00262456
41.	On platforms that do not have QAT, due to irrelevant memory consumption and that memory being set to debug, when new management certificates were configured or created and a configuration sync was performed, a panic occurred.	prod00262436
42.	Using WBM, in the **Monitoring > Application Delivery > Global Traffic Redirection > Remote Real Virtual Servers** pane, the titles of the table were not displayed in human readable format.	prod00262436

Item	Description	Bug ID
43.	Export of applogs using SCP server with the hostname as the destination failed, but with an IP address as the destination worked.	prod00262426
44.	Using APSolute Vision, the **Generate** and **Export** buttons on the **Monitoring > System > Maintenance** pane were misplaced.	prod00262402
45.	When the gateway was unreachable, and even though Alteon had no interface that was alive interface, Alteon delayed in recognizing a gateway health check failure.	prod00262350
46.	In an SLB environment, when a Script health check was part of a LOGEXP, a different number of health checks packets were sent out per interval for the different health checks combined in the LOGEXP health check.	prod00262279
47.	In an SLB environment, even though the servers were up, Alteon responded with a 503 error	prod00262264
48.	In an SSL environment with certificates, import of certificates in PFX format failed when the passphrase contained special characters such as '@'.	prod00262239
49.	In an SSL environment with certificates, import of certificates in PFX format failed when the passphrase contained special characters such as '@'.	prod00262238
50.	In an SLB environment with HTTP2 enabled on virtual services, sometimes Alteon stopped responding with resource issues.	prod00262190
51.	In a LinkProof environment, Alteon responded to customer requests without changing the server IP address to the Virtual Server IP address and server packets being handled by filter processing, causing the access to fail.	prod00262164
52.	In a gateway-per-VLAN environment, all the traffic to the Alteon interface and virtual server was sent back to the gateway based on the default gateway and not per the VLAN gateway, causing the feature to not work.	prod00262161
53.	Alteon modified the source IP address of hops on the traceroute path of UDP and TCP responses, causing the client to receive an incorrect result.	prod00262158

Item	Description	Bug ID
54.	When logging in to WBM through a data port, the WBM user login information was missing, and the incorrect client IP address was logged in the syslog message.	prod00262143
55.	In specific browsers (some versions of Chrome and Opera), which send some non-optimized HTTP2 HPACK header encodings that Alteon does not handle correctly, the PUT method did not work.	prod00262074
56.	After using the CLI command `/c/sys/syslog/cur`, the message `Syslog thread safe mode` displayed when it should not have.	prod00262045
57.	In an SLB environment, the PIP path under the virtual server `(/cfg/slb/virt <vsid>/service <vport> https/pip`) displayed in diff flash even though the settings were set to the default.	prod00262042
58.	When a primary group was configured without real servers associated with an FQDN server, the backup group used FQDN real servers, causing an **Apply** failure.	prod00262017
59.	Using WBM, in an SLB environment, you could not configure a Buddy Server.	prod00262010
60.	When the DNS server was down, Alteon stopped sending health checks with the destination as the hostname.	prod00261970
61.	Using WBM, when creating a Smart NAT dynamic NAT entry, the **Local Address** drop-down list included a **None** option which should have been named **Any**.	prod00261955
62.	Using WBM, when creating a new VRRP virtual router, the check box that is used to enable the virtual router was named **Enable Virtual Routers** instead of **Enable Virtual Router**.	prod00261953
63.	In an SLB environment with rtsrcmac enabled and reverse disabled, a request to a virtual server included an Allow filter, causing SLB traffic to fail.	prod00261909
64.	In a virtualization environment, when the ADC-VX was version 30.2.*x* and the vADC was version 31.0.*x*, there was a compatibility issue without proper information on an LACP trunk, causing port issues.	prod00261865

Item	Description	Bug ID
65.	In previous versions, client IP persistency could not be maintained when the SP CPU was selected based on the client IP address and port (VMAsport enabled).	prod00261812
66.	In an SLB environment, changes to the network class associated to an in-route map required a BGP soft reset for the changes to take effect.	prod00261805
67.	When the audit log was enabled, Alteon sent a blank syslog for the delete operation.	prod00261801
68.	When monitoring Alteon using SNMP, when an SNMP GET was performed for a virtual server with nonat enabled (DSR), the current sessions displayed as NULL.	prod00261791
69.	In a Global SLB environment with the redirect exclusion feature enabled, Alteon selected a service for the DNS response with the action as "redirect" instead of resolving the DNS.	prod00261790
70.	In an SLB environment using CLI, when the xforward command was run for a service, the delayed binding forceproxy setting was not set.	prod00261789
71.	In the Monitoring environment with `/cfg/sys/report` set to on, a panic occurred with SIGSEGV(11) in thread RSTA(tid=81).	prod00261691
72.	When importing the configuration using REST API, Alteon always responded with a success message to the agTftpLastActionStatus query even though the import operation failed.	prod00261680
73.	In a Smart NAT environment, due to a sequence of validations in Global SLB, the warning messages for gmetric were confusing to the user.	prod00261630

Item	Description	Bug ID

74.	When using Alteon as a relay agent, Alteon did not modify the source port when forwarding a request to a server that was on port 68. The server responded back as being on port 68, and Alteon dropped it as Alteon was listening only on port 67.
	Note: To fix this issue, a new CLI command was added: `/cfg/l3/bootp/prsvport`
	When enabled, the source port is preserved.
	New MIBs that were created:
	`ipCurCfgBootpPrsvPort`
	`ipNewCfgBootpPrsvPort`
		prod00261624

75.	In a LinkProof NG environment, when the source address was configured for proxy or SmartNAT 'Any' dynamic NAT, the Return to the source MAC address did not work for filter traffic and the return traffic did not behave as expected.	prod00261528
76.	In a LinkProof NG environment, the inbound proximity (gmetric proximity) did not work with Smart NAT.	prod00261523
77.	In a Smart NAT environment, Alteon forwarded the ICMP reply to the client without changing the source IP address to the public IP address. As a result, the VPN gateways could not be pinged using the public IP address.	prod00261521
78.	In an SLB environment with forceproxy, when HTTP content had to be replaced to HTTPS content, Alteon could not match the content-types application/json or application/xml, so Alteon could not replace this part of the HTTP code. As a result, the whole page appeared with issues.	prod00261493
79.	In an SLB environment with forceproxy, the content-based rules with FQDN servers were not working and returned 503 error.	prod00261490
80.	With a data class configured, when attempting to modify the same data class without performing an Apply, there was a discrepancy between the Alteon whitelist and the vDirect getextendedinfo configuration file. The diff displayed the modifications, but the Apply failed.	prod00261406
81.	On the Cloud WAF portal, with whitelists for IP addresses having zero as the last octet, an Apply operation failure occurred.	prod00261121

Item	Description	Bug ID
82.	In the Advanced HTTP health check configuration, although the maximum number of characters for the Body parameter was stated as 1024 characters, only 512 characters were allowed.	prod00261017
83.	Using WBM, when a user logged in using TACACS and performed configuration changes, and later performed Apply/Save operations, the audit logs recorded another user ID and not the user who had logged in.	prod00260978
84.	In a virtualization environment, when the ADC-VX was version 30.5.*x* and the vADC was version 31.0.*x*, no applogs were generated.	prod00260946
85.	Using WBM, using $PROTOCOL instead of http:// or https:// in the redirection URL for content rules action redirect or action redirect for a service did not work.	prod00260876
86.	In a DNS environment where DNS responses were received, and with VRRP or HA, performing a configuration sync ended with an FQDN error.	prod00260836
87.	In the SNMP Trap for certificate expiration altSwcertRevokedID, the description was incorrect.	prod00260830
88.	In a VRRP environment, after sync was performed, the server group setting was removed from the peer device.	prod00260808
89.	In an SLB environment with the round robin or least connections metric, and with a traffic pattern that had few connections that were opened with relatively long time periods between each other, after migrating all virtual servers from the 5208 platform to the 6420 platform, the round robin metric kept selecting only one specific real server from the server group and did not balance traffic to some servers.	prod00260669
90.	In WBM, the SLB Viewer user role was allowed to enable/disable physical ports, when this user role should only be able to view Alteon information, SLB statistics, and information, but should not be able to make any configuration changes.	prod00260641
91.	Using WBM, a real server's Description accepted 128 characters while only 31 characters are supported, causing the real server Description not to be synced from Active to Standby.	prod00260639

Item	Description	Bug ID
92.	In a virtualization environment, when accessing the device on an ADC-VX using REST API with an incorrect customized Authorization header value, a panic occurred.	prod00260598
93.	Alerts regarding DUAL PSU failure were generated, but after 6 seconds a notice was issued that the Status was Ok. This issue persisted even after changing to a new PSU.	prod00260597
94.	On a 6024 XL platform with 32 GB RAM, in Maximum vADC Density mode, you could not allocate the 12th CPU core (the fourth core for MP processing).	prod00260580
95.	Using REST API, image upload did not work.	prod00260564
96.	In an SLB environment, when a proxy IP address was defined in a network class, the proxy MAC address was sent with the gateway MAC address to those proxy IP addresses that were not present in the ARP table, causing the applications to fail.	prod00260562
97.	The load time of REST API calls was much slower than the load time in earlier Alteon versions.	prod00260509
98.	In an SLB environment with SSL Hello or HTTPS health checks configured, after upgrading to version 30.2.9.0, real servers configured with these health checks failed.	prod00260485
99.	In an SLB environment with the phash metric, the traffic load was unevenly distributed to real servers with random source IP addresses	prod00260470
100.	In an Outbound Link Load Balancing environment, LinkProof continued to send dispatching traffic towards WAN links whose bandwidth utilization was above 100%.	prod00260455
101.	You could not paste a geo network class configuration as taken from the configuration file and mandate it to add None for the Country and State fields.	prod00260454
102.	In a LinkProof environment configured with the bandwidth metric, Alteon did not select a WAN link based on the bandwidth metric configured on the DNS hostname and the DNS response included WAN links with the bandwidth overloaded.	prod00260453
103.	Using WBM with a WAN Link configuration, there were discrepancies between the upload bandwidth of the Per WAN Link IP and the Per WAN Link ID.	prod00260388

Item	Description	Bug ID
104.	Using WBM, when adding an IPv6 NAT IP address with the default prefix, because the IP address was added with prefix 0 instead of 128, the Apply operation failed.	prod00260360
105.	Using WBM, in a virtualization environment on an ADC-VX, the administrator could not change a vADC's administrator password.	prod00260333
106.	Using WBM or REST API with certificate repository management, you could not overwrite a certificate.	prod00260330
107.	In a BGP environment, after sending a BGP route update after a set of apply operations and a BGP toggle, a panic occurred.	prod00260322
108.	In a BGP environment, during BGP route update or when the BGP peer went down during BGP peer "cleanup," the platform hung.	prod00260321
109.	For unknown reasons, an unexpected reboot and a panic occurred.	prod00260320
110.	In an SLB environment, ESP traffic was not passed to the back-end servers.	prod00260297
111.	When using REST API to change the next image to boot, the correct image was not set.	prod00260261
112.	Using CLI, when configuring network classes, there were no validations when geo information was added for a network class as a one-line command.	prod00260260
113.	Sometimes you could not configure a management port with an IPv6 address that was identical to one generated by SLAAC.	prod00260161
114.	In an SLB environment with delayed binding enabled and APM enabled, because Alteon did not create persistent entries for a few specific clients, Alteon sent the request from a specific Client IP address to a virtual service on Alteon to different real servers, even with the persistent binding Client IP address set on the virtual service.	prod00260097
115.	Using WBM, in an SSL environment, when enabling back-end SSL encryption and the back-end SSL cipher was selected as "user-defined," and then the back-end SSL encryption was disabled, the saved configuration was improper due to a malformed XML.	prod00260026

Item	Description	Bug ID
116.	In a virtualization environment on an ADC-VX, when using a REST API call to create a vADC, a panic occurred.	prod00259835
117.	In a virtualization environment on an ADC-VX, when a configuration import (putcfg) operation was performed via SNMP, a panic occurred on the ADC- VX.	prod00259831
118.	In an SLB environment with the health check configuration destination set as hostname, the health check failed after performing an apply operation.	prod00259830
119.	When SSH/Telnet connections exceeded the allowed limit, no syslog message generated.	prod00259797
120.	In a virtualization environment with vADCs on the same ADC-VX cross-connected, ARP responses were dropped, causing a gateway failure.	prod00259735
121.	In a failover scenario, when adding or updating more than 256 FDB entries from the MP to the SP, if the SP overloaded, the SP was not able to add the entries to the spfdb table, causing traffic disruptions in the network.	prod00259698
122.	In an AppWall for Alteon VA environment, techdata generation abruptly stopped and a reboot was required.	prod00259694
123.	When Alteon was accessed via SSH, the TCP connections opened for SSH sessions were not closed properly as the client continued to send data and caused stale TCP sessions. This led to SSH access failure to the device.	prod00259686
124.	In a virtualization environment, after manual reboot on a vADC and when the vADC was disabled/enabled using the ADC-VX, the Apply operation returned the following error message: `vADC management changes due to a previous apply are currently under progress. Please try to apply the new changes after some time.`	prod00259681
125.	Using WBM, in **Monitoring > Network > High Availability**, the VRRP labels were incorrect.	prod00259626
126.	The vulnerability scan on the Alteon ADC-VX management IP address issued the following message: `SSL/TLS Server supports TLSv1.0` **Note**: Configuration for the TLS version was added (affecting management traffic only):	prod00259614

Item	Description	Bug ID
	In CLI: `/cfg/sys/access/https/tlsver` In WBM: **System > Management Access > Management Protocol > HTTPS**	
127.	In an SLB environment with persistent binding (pbind) configured with a cookie and Client IP, when Layer 4 sessions aged out, the reference count was decremented for the wrong persistent session, causing stale p-sessions.	prod00259581
128.	In a VRRP hot-standby environment, when the hot-standby port was designated as the next-hop port of the static ARP entry for a destination on the backup, a packet to the destination was sent out from that port even though it was in the Blocked state.	prod00259550
129.	In an SLB environment with FQDN real servers configured, on a virtual server with FQDN real servers, Alteon returned a 503 error even though the real servers were up.	prod00259492
130.	In an SLB environment with AppShape++ attached to a particular service, although alwayson was disabled, when the service went down, the request was forwarded to AppXcel.	prod00259436
131.	When attempting to upload a configuration to an RMA device, a panic occurred.	prod00259399
132.	In an SLB environment with AppShape++ configured, after aging, the TCP::close_type AppShape++ command returned an incorrect value in CLIENT_CLOSED, SERVER_CLOSED events.	prod00259384
133.	In an SLB environment with AppShape++ configured, after aging, TCP::close reset AppShape++ command did not send a reset when called from CLIENT_CLOSED, SERVER_CLOSED events.	prod00259334
134.	Using WBM, in a Layer 7 environment when a content class was deleted and a new one was created, some AX-related configuration errors displayed upon Apply/Revert Apply, leading to some AX traffic processing issues with the content class.	prod00259330
135.	In a VRRP environment, the backup Alteon did not change the source MAC and used the proxy MAC while routing the packet on the backup device.	prod00259179

Item	Description	Bug ID
136.	In a virtualization environment, after disabling a vADC, the vADC's internal syslogs were deleted from the ADC-VX.	prod00259152
137.	After generating a Tech Support dump or Techdata, the resource allocation table information (`/maint/debug/rsrcdump`) was missing.	prod00258995
138.	Outbound Telnet connections from ADC-VX/vADCs are not terminated when the respective inbound Telnet/SSH connections to the ADC-VX/vADCs are abruptly terminated, causing the user to not be able to access the ADC-VX after closing Telnet sessions abruptly.	prod00258970
139.	After configuring two interfaces, and not on same network, when a SNMP request was sent to one interface IP address, the response came from another interface.	prod00258932
140.	In an HA environment, when the proxy IP range is configured under the network class and a failover occurs, a GARP was not sent for all the proxy IP addresses in the range. **Note**: The following new command was implemented: `/cfg/l3/ha/nwclgarp ena/dis` If the network class range is huge, then the GARP being sent affects the peers ARP table.	prod00258850
141.	In an SLB environment with server groups, although the mhash configuration is only relevant for the minmisses metric, you could also configure it for other metrics (leastconn and svcleast), causing an Apply in these cases to fail.	prod00258826

AppWall

Item	Description	Bug ID
1.	Could not add a Protected URI in CSRF with a double slash.	DE7213
2.	AppWall did not process an empty file with chunked transfer Encoding.	DE38763
3.	The AppWall “Apply” RESTful API returned a failed code with the HTTPS tunnel in Monitor mode, even though the configuration was saved and applied.	DE38490
4.	Under certain conditions, JSON requests were not parsed correctly	DE38161

Item	Description	Bug ID
5.	The signature update did not update automatically.	DE37014
6.	AppWall identified a JSON parsing failure although the JSON was correct.	DE36913
7.	After a response parsing violation, the transaction ID in the security page did not display	DE36297
8.	The Max Reply header size was enforced to 1024 instead of being unlimited.	DE35625
9.	There was a conflict in the Policy Role importing policy Distribution file.	DE39462
10.	Under certain conditions, trimming failed to process.	DE39460
11.	When AppWall logged events about security violations of the Parameters filter, AppWall presented in the security events all the refinements related to the Web Application contain in the Parameter filter. This caused AppWall to log fewer Security events. Usually AppWall can log up to 350 000 events. The Parameters filter created a security event with a size of 53KB. After approximately 4,700 security events, the Security file reached the limit of 250 MB and AppWall deleted 20% of the database and generated new events in the system log.	DE21382

Fixed in 32.0.1.101

Version 32.0.1.101 includes all field bugs available in version 31.0.5.0.

Item	Description	Bug ID
1.	GEL – An Alteon VA deployed by vDirect from a cloned image could not communicate with the License Server.	DE35719
2.	GEL – The license was rejected when the Local License Server (LLS) returned a busy status.	TA64369

Fixed in 32.0.1.100

Version 32.0.1.100 includes all field bugs available in version 31.0.5.0.

Item	Description	Bug ID
1.	In an SLB environment with delayed binding forceproxy and cookie insert persistency, when running traffic with a cookie header, a `503 service unavailable` message was returned without serving the request.	DE37403 (prod00262228, prod00262097)

Fixed in 32.0.1.0

Item	Description	Bug ID
1.	Using WBM, it was not possible to add or edit vADCs	prod00261306
2.	In a Smart NAT environment, due to the sequence of validations in Global SLB, the warning messages for gmetric were confusing to the user. **Note:** The proximity metric for Inbound Link Load Balancing rules with Smart NAT is not yet supported.	prod00260963
3.	In a Smart NAT environment with Global SLB turned off and LinkProof turned on, the validations related to Smart NAT were skipped and no warning messages were issued. **Note:** Proximity is not yet supported for SmartNAT.	prod00260961
4.	In a DNS environment where DNS responses were received, and with VRRP or HA, performing a configuration sync ended with an FQDN error.	prod00260835
5.	In a VRRP environment, after sync was performed, the server group setting was removed from the peer device.	prod00260807
6.	In an SLB environment with the round robin or least connections metric, and with a traffic pattern that had few connections that were opened with relatively long time periods between each other, after migrating all virtual servers from the 5208 platform to the 6420 platform, the round robin metric kept selecting only one specific real server from the server group and did not balance traffic to some servers.	prod00260667

Item	Description	Bug ID
7.	In WBM, the SLB Viewer user role was allowed to enable/disable physical ports, when this user role should only be able to view Alteon information, SLB statistics, and information, but should not be able to make any configuration changes.	prod00260640
8.	Using WBM, a real server's Description accepted 128 characters while only 31 characters are supported, causing the real server Description not to be synced from Active to Standby.	prod00260637
9.	Alerts regarding DUAL PSU failure were generated, but after 6 seconds a notice was issued that the Status was Ok. This issue persisted even after changing to a new PSU.	prod00260596
10.	On a 6024 XL platform with 32 GB RAM, in Maximum vADC Density mode, you could not allocate the twelfth (12th) CPU core (the fourth core for MP processing).	prod00260579
11.	In a virtualization environment, when accessing the device on an ADC-VX using REST API with an incorrect customized Authorization header value, a panic occurred.	prod00260578
12.	Using REST API, image upload did not work.	prod00260563
13.	In an SLB environment, when a proxy IP address was defined in a network class, the proxy MAC address was sent with the gateway MAC address to those proxy IP addresses that were not present in the ARP table, causing the applications to fail.	prod00260560
14.	The load time of REST API calls was much slower than the load time in earlier Alteon versions.	prod00260508
15.	In an SLB environment with SSL Hello or HTTPS health checks configured, after upgrading to version 30.2.9.0, real servers configured with these health checks failed.	prod00260484
16.	In an SLB environment with the phash metric, the traffic load was unevenly distributed to real servers with random source IP addresses.	prod00260469
17.	In an Outbound Link Load Balancing environment, LinkProof continued to send dispatching traffic towards WAN links whose bandwidth utilization was above 100%.	prod00260451

Item	Description	Bug ID
18.	You could not paste a geo network class configuration as taken from the configuration file and mandate it to add **None** for the **Country** and **State** fields.	prod00260450
19.	In a LinkProof environment configured with the bandwidth metric, Alteon did not select a WAN link based on the bandwidth metric configured on the DNS hostname and the DNS response included WAN links with the bandwidth overloaded.	prod00260449
20.	Using WBM with a WAN Link configuration, there were discrepancies between the upload bandwidth of the **Per WAN Link IP** and the **Per WAN Link ID**.	prod00260386
21.	Using WBM, when adding an IPv6 NAT IP address with the default prefix, because the IP address was added with prefix 0 instead of 128, the Apply operation failed.	prod00260359
22.	Using WBM or REST API with certificate repository management, you could not overwrite a certificate.	prod00260329
23.	In a BGP environment, after sending a BGP route update after a set of apply operations and a BGP toggle, a panic occurred	prod00260319
24.	In a BGP environment, during BGP route update or when the BGP peer went down during BGP peer "cleanup," the platform hung.	prod00260318
25.	For unknown reasons, an unexpected reboot and a panic occurred.	prod00260317
26.	In an SLB environment, ESP traffic was not passed to the back-end servers.	prod00260296
27.	When using REST API to change the next image to boot, the correct image was not set.	prod00260259
28.	Using CLI, when configuring network classes, there were no validations when geo information was added for a network class as a one-line command.	prod00260258
29.	In an SLB environment with delayed binding enabled and APM enabled, because Alteon did not create persistent entries for a few specific clients, Alteon sent the request from a specific Client IP address to a virtual service on Alteon to different real servers, even with the persistent binding Client IP address set on the virtual service.	prod00260096

Item	Description	Bug ID
30.	Due to a large file size, the techdata generation failed with the following message: `Unknown Error`	prod00260082
31.	Using WBM, in an SSL environment, when enabling back-end SSL encryption and the back-end SSL cipher was selected as "user-defined," and then the back-end SSL encryption was disabled, the saved configuration was improper due to a malformed XML.	prod00260025
32.	In a virtualization environment on an ADC-VX, when using a REST API call to create a vADC, a panic occurred.	prod00259834
33.	In an SLB environment with the health check configuration destination set as hostname, the health check failed after performing an apply operation.	prod00259829
34.	In a virtualization environment on an ADC-VX, when a configuration import (putcfg) operation was performed via SNMP, a panic occurred on the ADC- VX.	prod00259828
35.	When SSH/Telnet connections exceeded the allowed limit, no syslog message generated.	prod00259798
36.	In a virtualization environment with vADCs on the same ADC-VX cross-connected, ARP responses were dropped, causing a gateway failure.	prod00259734
37.	In an AppWall for Alteon VA environment, techdata generation abruptly stopped and a reboot was required.	prod00259693
38.	When Alteon was accessed via SSH, the TCP connections opened for SSH sessions were not closed properly as the client continued to send data and caused stale TCP sessions. This led to SSH access failure to the device.	prod00259684
39.	Using WBM, in **Monitoring > Network > High Availability**, the VRRP labels were incorrect.	prod00259625
40.	In an SLB environment with persistent binding (pbind) configured with a cookie and Client IP, when Layer 4 sessions aged out, the reference count was decremented for the wrong persistent session, causing stale p-sessions.	prod00259580
41.	Using WBM, using $PROTOCOL instead of http:// or https:// in the redirection URL for content rules action redirect or action redirect for a service did not work.	prod00259520

Item	Description	Bug ID
42.	In an SLB environment with FQDN real servers configured, on a virtual server with FQDN real servers, Alteon returned a 503 error even though the real servers were up.	prod00259491
43.	In an HA environment, although synchronization was successful, the backup device issued the following error: `HA: Configuration is not synchronized between the HA devices`	prod00259438
44.	In a Geo proximity configuration, you could not set the country **Niger** in an Alteon GEO network class.	prod00259435
45.	In an SLB environment, when submitting a service (that supports non-standard ports) with a standard port, although the Alteon bank-end returned an error, due to the standard port, Alteon internally configured the corresponding service even after issuing the error without informing the user.	prod00259422
46.	In a virtualization environment, after manual reboot on a vADC and when the vADC was disabled/enabled using the ADC-VX, the Apply operation returned the following error message: `vADC management changes due to a previous apply are currently under progress. Please try to apply the new changes after some time.`	prod00259410
47.	When attempting to upload a configuration to an RMA device, a panic occurred.	prod00259398
48.	In an SLB environment with AppShape++ configured, after aging, the TCP::close_type AppShape++ command returned an incorrect value in CLIENT_CLOSED, SERVER_CLOSED events	prod00259383
49.	In an SLB environment with AppShape++ configured, after aging, TCP::close reset AppShape++ command did not send a reset when called from CLIENT_CLOSED, SERVER_CLOSED events.	prod00259333
50.	Using WBM, in a Layer 7 environment when a content class was deleted and a new one was created, some AX-related configuration errors displayed upon Apply/Revert Apply, leading to some AX traffic processing issues with the content class.	prod00259329

Item	Description	Bug ID
51.	In a VRRP environment, the backup Alteon did not change the source MAC address and used the proxy MAC address while routing the packet on the backup device.	prod00259178
52.	In a virtualization environment, after disabling a vADC, the vADC's internal syslogs were deleted from the ADC-VX.	prod00259151
53.	The vulnerability scan on the Alteon ADC-VX management IP address issued the following message: SSL/TLS Server supports TLSv1.0 **Note**: Configuration for the TLS version was added (affecting management traffic only): In CLI: `/cfg/sys/access/https/tlsver` In WBM: **System > Management Access > Management Protocol > HTTPS**	prod00258998
54.	Outbound Telnet connections from ADC-VX/vADCs are not terminated when the respective inbound Telnet/SSH connections to the ADC-VX/vADCs are abruptly terminated, causing the user to not be able to access the ADC-VX after closing Telnet sessions abruptly.	prod00258969
55.	After generating a Tech Support dump or Techdata, the resource allocation table information (/maint/debug/rsrcdump) was missing.	prod00258963
56.	After configuring two interfaces, and not on same network, when a SNMP request was sent to one interface IP address, the response came from another interface.	prod00258925
57.	In an HA environment, when the proxy IP range is configured under the network class and a failover occurs, a GARP was not sent for all the proxy IP addresses in the range. **Note**: The following new command was implemented: `/cfg/l3/ha/nwclgarp ena/dis` If the network class range is huge, then the GARP being sent affects the peers ARP table.	prod00258854
58.	Sometimes you could not configure a management port with an IPv6 address that was identical to one generated by SLAAC.	prod00258853

Item	Description	Bug ID
59.	In an SLB environment with AppShape++ attached to a particular service, although alwayson was disabled, when the service went down, the request was forwarded to AppXcel.	prod00258825
60.	In an SLB environment with IPv4 and IPv6 services and IPv6 PIP configured, a panic occurred.	prod00258580
61.	In an SLB environment with server groups, although the mhash configuration is only relevant for the minmisses metric, you could also configure it for other metrics (leastconn and svcleast), causing an Apply in these cases to fail.	prod00258549
62.	In an AppWall for Alteon environment, when an APSolute Vision syslog came from AppWall through the proxy, and LDAP traffic also used the proxy, Web Authentication via AppWall stopped working.	prod00258525
63.	Using WBM, in a virtualization environment on an ADC-VX, the administrator could not change a vADC's administrator password.	prod00258405
64.	In an SLB environment with session mirroring enabled for virtual services, the session statistics were incorrect on the backup device compared to the primary device.	prod00258381
65.	For DNS Responder virtual servers with DNS over UDP only, DNS resolution failed.	prod00258374
66.	Using WBM, in an SLB monitoring environment, the real server IP addresses for a server group were displayed incorrectly.	prod00258332
67.	When logging into WBM using TACACS and performing configuration changes and later performing Apply/Save operations, in the audit logs another user ID was recorded instead of the user who logged in.	prod00257825
68.	SSL Hello health checks using TLS (instead of SSL v2/v3) were not working on XL/Extreme platforms.	DE34416
69.	From WBM, you cannot change the vADC management IP address from within the ADC-VX environment.	prod00216388
70.	Parameter security events may cause excessive or high event size.	DE21382
71.	Details button was missing in the Database Security Filter view.	DE25177

Item	Description	Bug ID
72.	Under certain conditions, SSL termination causes SSL session traffic interruptions in passive mode.	DE30899
73.	Vulnerability security refinement in a defined Virtual Directory doesn't block traffic.	DE31063
74.	Failure in the Blocked Source table (Source Blocking) due to a failure in the Fingerprint hash value.	DE31964
75.	After multiple consecutive memory dumps, log partition becomes full.	DE32927
76.	Database security filter blocks legitimate HTTP requests.	DE33867
77.	Compatibility error message with web browser when using Activity Tracking fingerprint based with Vulnerabilities security filter.	DE34015
78.	Failure in the Database security filter after an upgrade with an AppWall version older than 5.7.2.	DE34070
79.	Refinement error message when trying to refine an HTTP reply size header.	DE34119
80.	Duplicate IP Group and Security WebApplication Role when using the API call with import option for policy distribution.	DE34185 DE34453
81.	Hosts based configurations that contain a wildcard are not taken into consideration.	DE35113
82.	Under certain conditions, Database security refinement disappears.	DE35457
83.	Under certain conditions, a failure occurs with huge HTTP response request.	DE32953
84.	After a failed Apply operation, the tunnel cannot be initialized.	DE21581
85.	Failure occurs in Fast Upload	DE33520
86.	AppWall Management Application failures when refreshing the forensics view with a very high of events	DE30806
87.	Go to Policy button in Forensics view generate an AppWall Management Application exception for RFC Violated Security Events.	DE31200
88.	Failure in the AppWall Management Application occurred after creating a complex REGEX in the security policies settings	DE33872

Item	Description	Bug ID
89.	Wrong IP address in the syslog messages	DE34357

Fixed in 32.0.0.0

Version 32.0.0.0 includes all field bugs available in version 31.0.4.0.

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/1021440

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*

For the latest Alteon product documentation, as well as previous and retired versions, refer to:

https://portals.radware.com/Customer/Home/Downloads/Application-Delivery-Load-Balancing/?Product=Alteon

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