



AlteonOS

RELEASE NOTES

Version 33.5.7.0
January 3, 2024

TABLE OF CONTENTS

CONTENT	8
RELEASE SUMMARY	8
SUPPORTED PLATFORMS AND MODULES	8
UPGRADE PATH	9
Before Upgrade – Important!	9
Additional Considerations	9
Downgrade	10
WHAT'S NEW IN 33.5.7.0	10
Traffic Capture Enhancements	10
Link Layer Discovery Protocol (LLDP)	10
PIP Advertising via BGP	10
SNMP OID to Monitor Peak Session	11
Immediate Backend Bind	11
WHAT'S NEW IN 33.5.6.0	11
LDAP User Authentication	11
WHAT'S NEW IN 33.5.5.0	12
Alteon Support in Cyber Controller High-Availability	12
BGP ECMP Support on Load Balanced Traffic	12
GEL Entitlement Description	12
Integrated AppWall	12
GraphQL Protocol Support - BETA	12
WHAT'S NEW IN 33.5.4.0	13
GEL Support in Standalone Mode	13
Layer 7 Modification on HTTP/2 traffic	13
Control and Export of Management Port Packet Capture from WBM	13
WHAT'S NEW IN 33.5.3.0	14
SecurePath Connector Enhancements	14
Alteon 7100/7700 Platforms	14
GEL Dashboard Enhancements	14
Built-in DNS over HTTPS Gateway	15
Latency Control for Integrated WAF	15
Alteon VA Support for AMD Processors	16
Cookie Insert Enhancement	16
Ansible for Content Rules	16

Service and Real Server PPS Statistics	16
Keepalive in Proxy Mode	16
Security Message for Unsecure Management Protocols	16
PIP Source Port Utilization Warning	17
AppWall Dynamic Resource Allocation	17
WHAT'S NEW IN 33.5.2.0	17
SecurePath Connector	17
GEL Management Administrative Modes	18
AppShape++ Commands	19
Latency Control for Integrated WAF	19
OCSP Health Check	20
Additional SSL Policy Parameters	20
Generic HTTP Sideband	20
WHAT'S NEW IN 33.5.1.0	21
Heat Templates for OpenStack Installations	21
GEL Entitlement Split Across License Servers	21
6420 DPDK Support	22
Selective WAF Content Inspection	23
Session Reuse for SSL Health Checks	24
BGP AS DOT Notation Support	24
HTTP/3 Gateway Enhancement	24
Chinese Crypto Algorithms Enhancement	24
Integrated AppWall	24
WebSocket	24
API Security	25
Advanced Base64 Attack in HTTP Headers	26
WHAT'S NEW IN 33.5.0.0	27
vRA/vRO Workflows	27
HTTP/3 Gateway	27
Layer 7 Services	27
HTTP/3 Service Advertise Parameter	27
Hardware Acceleration	28
Chinese Crypto Algorithms (SM2, SM3 and SM4) Support	28
64GB RAM on 5424/5820	29
BGP IPv6 ECMP Traffic Load Balancing	29
ADFS Health Check	29
Ansible Modules	29
GEL Entitlement Migration Workflow	30

Source NAT for Health Checks	30
PMTU Discovery Support.....	30
FIPS Card Support for 7220	31
Integrated AppWall	31
WebSocket	31
API Security	32
Advanced Base64 Attack in HTTP Headers	33
Filter Tunnel Command	33
WHAT'S CHANGED IN 33.5.7.0	34
Reduce Default Traffic Event Sampling	34
OpenSSL Upgrade	34
Exclusion of URL Categorization from Secure Subscription License	34
License Validation During Config Import	34
Integrated AppWall	34
HTML Decoding	34
Vulnerability Partial Scan	35
GraphQL Protection	35
WHAT'S CHANGED IN 33.5.6.0	35
OpenSSL Upgrade	35
GSLB Network Number Increase	35
Password Policy Enhancements	35
"wget" Package Update	36
SecurePath Policies Number Increase	36
Integrated AppWall	36
GraphQL Protection	36
Custom Pattern	36
Limit Number of Headers to Parse.....	36
Base64 Decoding.....	36
Redirect Validation Host Protection	36
WHAT'S CHANGED IN 33.5.5.0	36
Network HSM (Thales/Gemalto) Enhancements	36
BWM Shaping.....	37
UDP Virtual Service Down Response	37
Alteon Embedded Dashboard Removal.....	37
Advanced Virtual Wire Health Check Enhancements	37
Change in AppWall SNMP Trap OID	37
Integrated AppWall	37

Multiple Improvements	37
WHAT'S CHANGED IN 33.5.4.0	38
Integrated WAF SUS and GEO DB Update Via Proxy.....	38
Combined Image Upload Option Removed from WBM	38
Service and Real PPS Collection Interval	38
OpenSSL Upgrade	38
AppWall Integrated	38
WHAT'S CHANGED IN 33.5.3.0	40
MP CPU Reservation	40
Tech Data Ready Notification.....	40
VMA Default	40
Cookie Insert Path.....	40
Server Group and Real Server Description.....	40
External Health Check.....	40
AppWall Integrated	41
Multiple IPs included in XFF HTTP header	41
WHAT'S CHANGED IN 33.5.2.0	41
SSH Library Upgrade to Support SHA2 MAC Algorithm.....	41
Proxy ARP Entries.....	41
External Health Check.....	41
EAAF for Alteon Feed Eligibility Based on GEL Entitlement.....	41
FastView GUI Configuration Removal	41
OpenSSL Upgrade	42
AppWall Integrated	42
WHAT'S CHANGED IN 33.5.1.0	42
GEL Enhancements	42
GEL Dashboard	42
GEL Allocation Granularity.....	42
Syslog Server for Integrated WAF.....	42
HTTP/HTTPS Health Check.....	43
Number of Alteon DNS Responders	43
Ping6 Response	43
EAAF UI.....	43
QAT Driver/Engine Upgrade	44
OpenSSL Upgrade	44
AppWall Integrated	44
WHAT'S CHANGED IN 33.5.0.0	44

Empty Group Association to FQDN Server and Virtual Service	44
HTTP Header Length	44
Treck Version	44
Remove Vulnerable Expat Library.....	45
Include "remote address" at the TACACS request	45
Ignore Non-existing Fields in JSON	45
Event Counter Default Change	45
AppWall Integrated	45
MAINTENANCE FIXES	46
Fixed in 33.5.7.0	46
General Bug Fixes	46
AppWall Bug Fixes	48
Fixed in 33.5.6.10	49
AppWall Bug Fixes	49
Fixed in 33.5.6.0	49
General Bug Fixes	49
AppWall Bug Fixes	51
Fixed in 33.5.5.0	51
General Bug Fixes	51
AppWall Bug Fixes	53
Fixed in 33.5.4.0	54
General Bug Fixes	54
AppWall Bug Fixes	57
Fixed in 33.5.3.0	57
General Bug Fixes	57
AppWall Bug Fixes	60
Fixed in 33.5.2.0	60
General Bug Fixes	60
AppWall Bug Fixes	62
Fixed in 33.5.1.0	63
General Bug Fixes	63
AppWall Bug Fixes	65
Fixed in 33.5.0.0	66
General Bug Fixes	66
AppWall Bug Fixes	68
Fixed in 33.0.3.0	69

General Bug Fixes	69
AppWall Bug Fixes	71
Fixed in 33.0.2.50	72
General Bug Fixes	72
AppWall Bug Fixes	73
Fixed in 33.0.2.0	74
General Bug Fixes	74
AppWall Bug Fixes	75
Fixed in 33.0.1.50	76
General Bug Fixes	76
Fixed in 33.0.1.0	78
General Bug Fixes	78
AppWall Bug Fixes	82
Fixed in 33.0.0.0	83
General Bug Fixes	83
AppWall Bug Fixes	88
KNOWN LIMITATIONS	88
RELATED DOCUMENTATION	88



CONTENT

Radware announces the release of AlteonOS version 33.5.7.0. These release notes describe new and changed features introduced in this version on top of version 33.5.6.10.

RELEASE SUMMARY

Release Date: January 3, 2024

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
- 5208, 5208S
- 5424S, 5424SL, 5820S, 5820SL
- 6024, 6024S, 6024SL, 6024 FIPS II
- 6420p, 6420, 6420S, 6420SL
- 7612S, 7612SL
- 7220S, 7220SL
- 7100S, 7100SL, 7100DS
- 7700S, 7700SL, 7700DS
- 8420, 8420S, 8420SL
- 8820, 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
- Alteon VA on Google Cloud

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

Alteon 33.5.7.0 is supported by APSolute Vision version 4.30 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, 32.x and 33.x. General upgrade instructions are found in the *Alteon Installation and Maintenance Guide*.

Before Upgrade – Important!

1. Before performing an upgrade, back up your current configuration.
2. To ensure a successful upgrade, run the [Upgrade Advisor Tool](#) with your current configuration and the target version. Then, perform the required actions as instructed in the report output. The Upgrade Advisory Tool includes all the limitation and upgrade considerations specifically relevant to the source configuration, version, device details and target version. Make sure to update the Upgrade Advisory Tool DB before performing the analysis. The Upgrade Advisor Tool is available on the Customer Portal.
3. Read the [Upgrade Limitations](#) in these Release Notes for new upgrade limitations related to this version.

The following table describes the specific upgrade path from each version to 33.5.7.0:

Current Version	Upgrade Path	Notes
28.x	> 29.0.9.0 > 30.5.3.0 > this version	As an alternative, you can upgrade directly to 33.5.7.0 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	
33.x	Direct upgrade to this version	

Additional Considerations

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

Important!

- For Alteon 5208, 5424, 5820, 6024, 7612, 7220, and 9800, vADCs running this version require ADC-VX running at a minimum version 33.0.0.0.
- For Alteon 8420, vADCs running this version require ADC-VX running at a minimum version 33.0.1.0.
- For Alteon 6420, vADCs running this version require ADC-VX running at a minimum version 33.0.4.50.

Downgrade

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

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

WHAT'S NEW IN 33.5.7.0

Traffic Capture Enhancements

A new capability is added to the Alteon packet capture, enabling correlation between the front-end and back-end connections of captured traffic. This correlation is established based on the client IP address or Virtual Server IP.

This new feature enhances troubleshooting capabilities.

NFR ID: 230413-000074

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

PIP Advertising via BGP

This feature is applicable only for FRR BGP mode. It supports the PIP advertisements at the global level applicable for all BGP peers.

```
/cfg/l3/bgp/piprdst/
```

```
[PIP Redistribution Menu]
```

pip - PIP Advertisement Menu
ppip - Enable/disable advertising port based PIP addresses
vpip - Enable/disable advertising vlan based PIP addresses
extpip - Enable/disable advertising extra PIP addresses
cur - Display current PIP redistribution configuration

You can define up to 128 extra PIPs (both IPv4 and IPv6 together) that can be advertised to BGP peers.

NFR ID: 230420-000126

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 33.5.6.0

LDAP User Authentication

Alteon now provides user authentication and authorization using a Lightweight Directory Access Protocol (LDAP) server.

Alteon lets you map between an LDAP object and an Alteon User Role to allow RBAC per user.



Radware recommends enabling administrator backdoor (`/cfg/sys/access/user/admbd`) and security backdoor (`/cfg/sys/ldap/secbd`) to allow Alteon access using the default admin user when the LDAP server is not accessible.

NFR ID: 221012-000007

WHAT'S NEW IN 33.5.5.0

Alteon Support in Cyber Controller High-Availability

Alteon now supports Cyber Controller in a High-Availability environment.

When Alteon is managed by Cyber Controller version 10.0.2 or later, Cyber Controller updates each registered Alteon device with the IP addresses of both Cyber Controller servers, including their roles (primary or secondary) and statuses (active or inactive). Alteon continuously queries the Cyber Controller servers to identify any change in their statuses.

With that knowledge, Alteon can be configured to send WAF security events, traffic events, and EAAF events to the Active Cyber Controller server, as well as retrieving the ERT Active Attacker Deed from the Active Cyber Controller server.

A new table is available in Alteon displaying the Cyber Controller IP addresses, roles, and statuses:

From CLI: `/info/sys/cyberc`

From WBM: *Configuration* perspective > **System** > **Cyber Controller**

NFR ID: 220503-000039

BGP ECMP Support on Load Balanced Traffic

Alteon now supports performing ECMP distribution for traffic that it load balances (request traffic to servers and response traffic to clients). In previous versions, Alteon performed ECMP only for routed traffic.

GEL Entitlement Description


Starting with *Cyber Controller 10.2.0*, you can add an editable entitlement description in the *GEL Dashboard* to provide further details that identify the entitlement's purpose.

NFR ID: 221024-000041

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 33.5.4.0

GEL Support in Standalone Mode

Starting with this version, GEL is now available on a Standalone platform.

Now, entitlements can be allocated to VA, vADC, and Standalone platforms.

NFR ID: 221222-000039

Layer 7 Modification on HTTP/2 traffic

Header modification is now supported for HTTP/2 proxy traffic, via HTTP Modification Rules.

Notes:

- Each rule in the rule list must be a header modification rule.
- If the action is Insert, the rule must not contain a condition.
- If the action is Remove or Replace, the following headers cannot be replaced or removed (the values of the header can be changed):
 - Request: ":method", ":scheme", ":authority" and ":path"
 - Response: ":status"
- The header names must not contain uppercase characters.

NFR ID: 221123-000123

Control and Export of Management Port Packet Capture from WBM

You can now control and export the Management port packet capture from WBM.

NFR ID: 221102-000004



WHAT'S NEW IN 33.5.3.0

This section describes the new features and components introduced in this version on top of Alteon version 33.5.2.0.

SecurePath Connector Enhancements

Starting with this version, in addition to SecurePath Connector support in virtual services, it also supports:

- **SecurePath per Content Rule** – This allows setting a specific SecurePath policy and sideband per L7 HTTP matching such as hostname (for the virtual hosting use-case). It also allows bypassing SecurePath processing for specific L7 matching (hosts, paths, and so on).
- **SecurePath on Filter** – This allows using SecurePath in transparent mode deployments.

Note: For the SecurePath configuration in Alteon, you must have at minimum the Perform package.

Alteon 7100/7700 Platforms

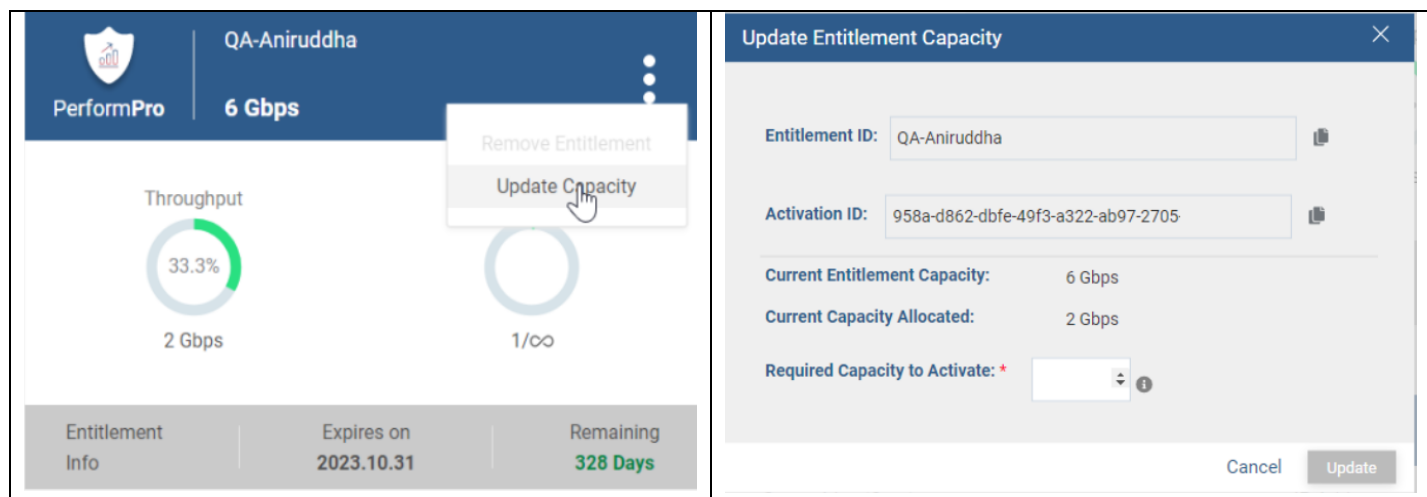
The new Alteon 7100/7700 platforms are based on the existing 7612/7220 platforms, with enhanced CPU. Alteon 7100 is replacing Alteon 7612 and Alteon 7700 is replacing Alteon 7220. In addition to the S and SL models, a new DS model provides increased SSL performance.

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.



Built-in DNS over HTTPS Gateway

Alteon now provides built-in support for translating DoH to Do53 (DNS over UDP or TCP). This provides significant performance improvement versus the previous AppShape++-based solution, as well as simplified configuration.

To activate the built-in DoH gateway:

1. Configure an HTTPS virtual service. Radware recommends enabling HTTP/2 (attach an HTTP/2 policy), as this is the default for DoH.
2. Set the Server Port to 53 (or another non-standard port)
3. Set the **DoH to Do53 Gateway** parameter to the desired translation option (backend): TCP, UDP, or UDP with TCP fallback.
4. If the back-end servers are UDP, you are required to also attach a DNS Sideband policy


Notes:

- This functionality requires the Perform package or higher capabilities
- Configuration of the different DoH and DoT gateway scenarios is detailed in the following [article](#).

Latency Control for Integrated WAF

WAF latency control can now be applied on HTTP requests, responses, or both (in earlier versions it was applied only on HTTP requests).

WAF latency control allows forwarding HTTP messages (request or response) to their destination without waiting for the WAF to complete its inspection if the WAF did not answer within a user-defined timeout. This capability enables giving priority to the customer experience over the application security when the integrated WAF module operates under high loads, which translates into longer latency for the client.



Note: If the request times out and is forwarded to the server without WAF inspection, the response of that transaction will also bypass the WAF module.

Alteon VA Support for AMD Processors

Alteon VA can now run in DPDK mode on AMD-based servers using the VMware hypervisor (ESXi 7.03). It requires an Ubuntu18 Alteon VA installation.

NFR ID: 220214-000059

Cookie Insert Enhancement

When virtual service persistency mode is Cookie Insert, you can now specify the **HTTP only flag** value (default is Disable).

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

Service and Real Server PPS Statistics

The service and real servers PPS statistics can be displayed using the following CLI command:
`/stat/slb/pps`

By enabling the advanced PPS statistics with the `/cfg/slb/adv/pps` command (default: disabled), these statistics can also be stored every 20 minutes into files available as part of the tech data.

Keepalive in Proxy Mode

Alteon now has the ability to issue keepalive messages towards its TCP connection peer when operating in proxy mode. In previous versions, it answered keepalive messages from the peer, but did not generate them.

To activate this functionality, enable it in the TCP policies attached to the relevant virtual service or filter.

NFR ID: 220624-000086

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

AppWall Dynamic Resource Allocation

AppWall tunnels can be manually configured to use from one (1) to three (3) security threads. Usually, there may be more “empty” cores than threads that leads to high utilization of some of the cores, while others are unused.

With the Dynamic Resource Allocation, AppWall automatically adds and removes threads depending on the CPU usage in run-time.

WHAT'S NEW IN 33.5.2.0

This section describes the new features and components introduced in this version on top of Alteon version 33.5.1.0.

SecurePath Connector

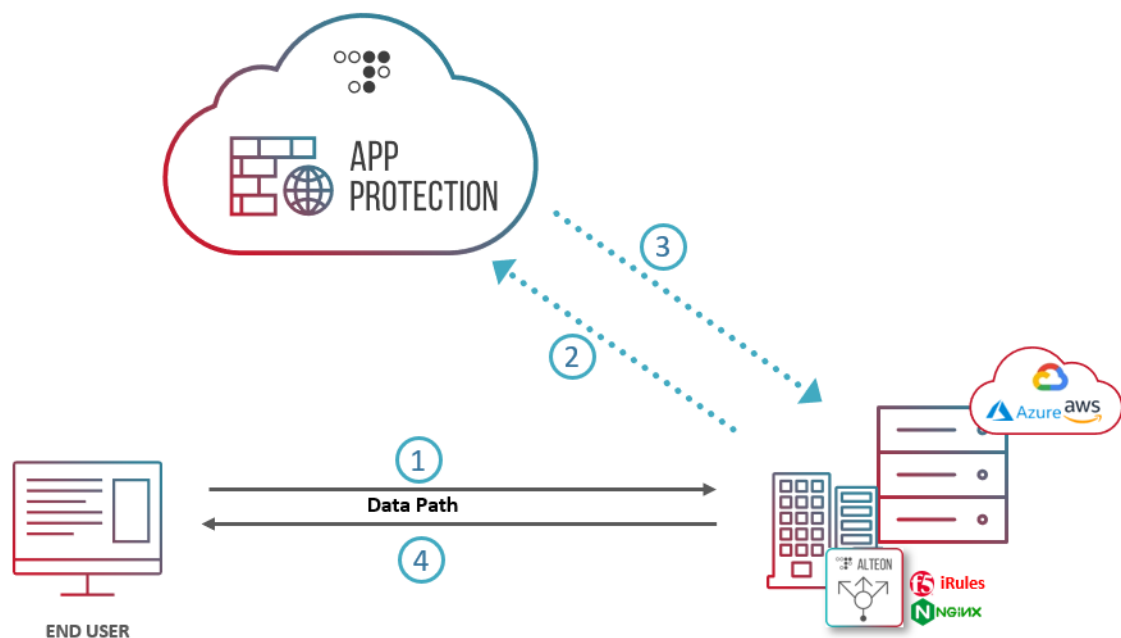
SecurePath integration is an API-based solution for multi-cloud application security. It provides consistent, high-grade, and comprehensive protection for applications hosted across on-premises, private cloud, and public cloud environments, without losing protection quality or operational efficiency.

Radware's cloud application security solution can be deployed in API mode and does not interfere with customer communications, providing Web Application protection, API Security, and Bot Manager Protection in a single solution.

When a client request reaches an application in Alteon which is protected by SecurePath,

1. Alteon sends a copy of the request via the sideband connection to Radware Cloud Security Service endpoint.
2. The Security engine analyzes the data and response to Alteon with the required actions
3. Alteon acts according to the Radware Cloud Security Service response, either allowing the request, blocking it, or challenging the user with a CAPTCHA test.

For the integrated SecurePath to function, you must have at minimum the Perform package, and you must have a license for the required Radware Cloud Security protection (Cloud WAF, BoT Manager).



GEL Management Administrative Modes

Starting with APSolute Vision 5.4, the following administrative modes are available for GEL Management.

- GEL Administrator:
 - Allowed to activate the entitlement, remove the entitlement, and allocate GEL capacity to Alteon devices within the user's scope.
 - Available with APSolute Vision roles: Administrator and Vision administrator
- GEL Operator:
 - Allowed to allocate GEL capacity to Alteon devices within the user's scope

- Available with APSolute Vision roles: Device Administrator, Device Configurator, ADC Administrator and ADC+Certificate administrator.
- GEL Viewer:
 - Can only view the GEL capacity allocation to an Alteon devices within the user's scope without any ability to activate the entitlement, remove or allocate or allocated capacity.
 - Available with all other APSolute Vision roles

AppShape++ Commands


The following AppShape++ commands were added:

- Global commands
 - hex – Transforms text string into hex string.
 - trace – Allows enabling or disabling logging or changing the log level for a specific session.
- CONF commands – Commands that retrieve values of attributes in configuration.
 - CONF::spath – Retrieves the value of the specified attribute in the SecurePath policy.
 - CONF::service – Retrieves the value of the specified attribute in the virtual service.
- HTTP commands
 - HTTP::replace_all – Replace all HTTP content (headers + body)
 - HTTP::cookies – Retrieves all HTTP cookies values
 - HTTP::content_length – Added capability to also modify content length
- Sideband commands
 - SIDEBAND::metadata – Retrieve the metadata inserted in the Sideband request by the main session.
 - SIDEBAND::serialize – Request to serialize the sideband actions (arrange, in proper order and binary format, all the actions that must be performed on the main session).
 - SIDEBAND::add_action – Allows adding actions that should be performed in the main session, based on the sideband response.

Latency Control for Integrated WAF

When the integrated WAF module operates under high loads, inspection of certain transactions can take longer than usual, which translates into longer latency for the client and a less than optimal user experience. There are cases when the customer experience has priority over the application security. To provide a solution for such cases, Alteon now allows forwarding HTTP requests to the server without waiting for the WAF to complete its inspection if the WAF did not answer within a user-defined timeout.

This capability can be enabled at the Secured Web Application (secwa) level by configuring the **Timeout** parameter (default is 0, meaning the feature is disabled).



Currently, the timeout is applied only for the request part of a transaction. However, if the request times out and is forwarded to the server without WAF inspection, the response of that transaction will bypass the WAF module.

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.

NFR ID: 211102-000063

Additional SSL Policy Parameters

The following new parameters are now available in SSL policies, for both front-end and back-end SSL:

- Allowed Signature Algorithms – Enables changing the allowed signature algorithms
- Allowed SSL Groups (Curves) – Enables changing the allowed EC curves

Note: The **Allowed SSL Groups** parameter is not available on FIPS platforms (internal HSM card).

Generic HTTP Sideband

A generic HTTP sideband is now supported in virtual services.

With this capability, you can create an HTTP sideband connection to any outside resource, send a custom formatted request, await a response if applicable, act on that response, and so on. The sideband actions and events are manipulated by an AppShape++ script associated to the sideband.

If JS injection to the client browser is required as part of the generic HTTP sideband, JS injection must also be enabled on the service (using the `/cfg/slb/virt/service/http/jsinject` command). This automatically attaches a compression policy to the service to allow for the JS injection functionality.

WHAT'S NEW IN 33.5.1.0

This section describes the new features and components introduced in this version on top of Alteon version 33.5.0.0.

Heat Templates for OpenStack Installations

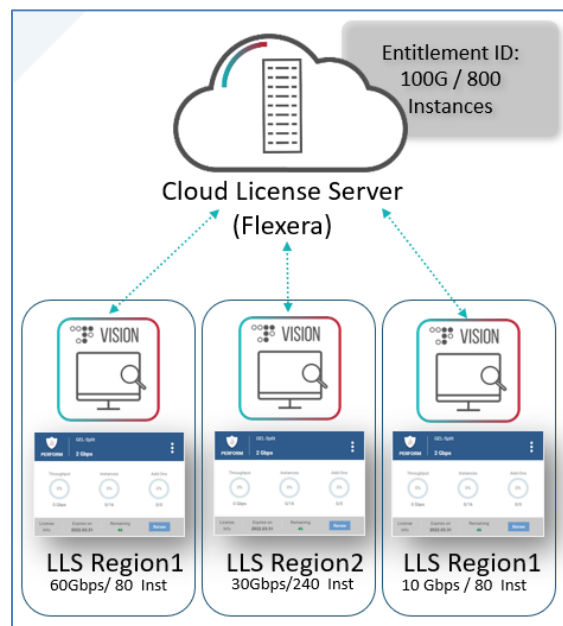
A set of Heat Orchestration Templates (HOTs) is now available for deploying and/or configuring an Alteon device/HA pair from your OpenStack Cloud. The following templates are available:

- Deploy Alteon instance in single IP mode (single port for data and management)
- Deploy Alteon instance with separate management and data ports (virtio)
- Deploy Alteon instance with separate management and data ports (SRIOV)
- Deploy Alteon instance with separate management and two data ports (virtio)
- Deploy Alteon instance with separate management and two data ports (SRIOV)
- Deploy pair of Active-Backup Alteon instances (virtio)
- Deploy pair of Active-Backup Alteon instances (SRIOV)
- Deploy Alteon basic load balancer (single IP mode instance with basic virtual service)

Note: These templates work only with Ubuntu 18 installations.

GEL Entitlement Split Across License Servers

This capability allows splitting the capacity of a single GEL entitlement across several LLS (Local License Server) instances (the capacity for each LLS can be adjusted as needed, as long as it is not currently allocated to Alteon devices).



The minimum split size is 1 Gbps and is available for both online and offline LLS operational modes.

An entitlement that can be split leverages the FlexNet Activation ID Quantity feature. For example, a 100 Gbps Entitlement that is built as an Entitlement of 100G with Quantity=1 can only be deployed on one LLS Server, while an Entitlement built out of 1 Gbps with Quantity=100 can be split across multiple LLS instances.

This allows consuming all activation ID quantities on one LLS Server, if the split is not required, or splitting the quantity among several LLS Servers.

The Entitlement quantity value can be increased as needed to support an Entitlement upgrade.

Starting with APSolute Vision 5.3, the *Activate Entitlement* dialog box includes the **Activation ID Quantity** field to support the Entitlement split.

Entitlement that supports split as it appears in the FlexNet End-User Portal

The screenshot displays the 'ID Info' section with the Entitlement ID and Activation ID. Below is the 'Product Info' section, which includes a table with product details. The 'Qty: 100' is highlighted in yellow. The 'Activation Info' section shows the quantity remaining, start date, and expiration date.

Product information:	Product:	Description:
	Alteon Secure Pro - 1 Gbps	Alteon Secure- 1 Gbps
	Global Elastic License	Global Elastic License
	including 8 VAs/vADCs, 1	Unlimited VAs/vADCs - 1
	year subscription	year, Price includes
	Version 2.1, Qty/Copy 1	support. Operator Tool Box -
		FastView for Alteon -

Activation ID Quantity field on the GEL Dashboard

The screenshot shows the 'Activate Entitlement' dialog box. It contains a text field for 'Activation ID' with a placeholder 'Paste Activation ID here'. Below it, the 'Activation ID Quantity' field is highlighted with a yellow box and contains the value '1'. At the bottom right, there are 'Cancel' and 'Activate' buttons.

Important!: Currently, an Entitlement that supports splitting is only generated per a specific request to Order Management.

Note: For an Entitlement that does not support splitting, the activation ID quantity should remain as "1" when activating the Entitlement.

6420 DPDK Support

Starting with this version, the Alteon 6420 platform uses the DPDK infrastructure. This allows for integration of more advanced capabilities. For example, it allows using the Alteon 6420 platform with an external HSM.

Important!: An upgrade to the version of a 6420 platform working in ADC-VX mode requires that both the ADC-VX and all its vADCs are upgraded to this version, as DPDK- and non-DPDK-based versions cannot be mixed on the same device.

Performance Impact:

On a 6420 platform running in standalone mode, this version currently causes performance degradation of 20% on L4 CPS and RPS numbers.

Selective WAF Content Inspection

By default, parsing of HTTP requests and responses happen after they are processed by the integrated WAF. Starting with this version, you can choose to perform the HTTP parsing before the messages are processed by the integrated WAF. This allows for selecting the content that is sent to the integrated WAF for processing, and more importantly what content *not* to send to the integrated WAF. By bypassing WAF processing for irrelevant content, such as movies and static files, the WAF capacity can be improved.

The timing of HTTP parsing vis-a-vis WAF processing can be set per one the following:

- Virtual service
 - WBM: **Virtual Service > Security tab > Secwa Processing in Flow**
Values: Before Alteon HTTP Parsing (default), After Alteon HTTP Parsing
 - CLI: `/cfg/slb/virt <virt id>/service <http | https>/http/aw/awinflow`
Values: before (default). after
- Filter
 - WBM: **Filter > HTTP tab > Secwa Processing in Flow**
 - CLI: `/cfg/slb/filt <filt id>/awinflow`

You can define the content that should bypass WAF processing using a content rule, as follows:

1. Set WAF processing at the service level to **After Alteon HTTP Parsing** (WBM), or **after** (CLI).
2. Define a content rule with the content to bypass WAF processing.
3. In that content rule, set the WAF processing to **disabled**:
 - WBM: **Virtual Service > Content Rules tab > Content Based Rule > Secure Web Application Processing**
 - CLI: `/cfg/slb/virt <virt id>/service <http | https>/cntrules <id>/secwa`

Note: When WAF processing is set to be performed after HTTP request parsing, AppShape++ events HTTP_REQUEST and HTTP_REQUEST_DATA will be performed prior to WAF processing. This means that if any HTTP modifications are performed via AppShape++, the WAF will receive the modified message.

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.

BGP AS DOT Notation Support

There are several ways to configure/display 4-byte AS numbers. Before this version, Alteon supported only the regular decimal numbers notation (asplain). Starting with this version, Alteon also supports the asdot notation, which represents AS numbers less than 65536 using the asplain notation and AS numbers greater than 65536 with the asdot+ notation. This breaks the AS number in two 16-bit parts, a high-order value, and a low-order value, separated by a dot (.). For example, AS 65538 becomes 1.2.

To use AS DOT notation for Alteon AS numbers as well as peer Remote AS numbers, you must first enable it (`cfg/l3/bgp/asdot`). By default, it is disabled.

NFR ID: 211205-000073

HTTP/3 Gateway Enhancement

Client authentication is now supported on front-end HTTP/3 connections.

Chinese Crypto Algorithms Enhancement

When both TLS and GmSSL protocols are enabled for Frontend SSL on Alteon. If the client also supports both protocols, the TLS protocol and cipher will be selected during the handshake.

Now it is possible to provide the GmSSL protocol and cipher priority via `cfg/slb/ss/sslpol <policy id>/gmprio` command.

Note: This parameter is only visible when running the special SM build and the SM license is installed.

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.

Auto Policy Http Settings **WebSocket settings** Security Log

☒ 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 **Set Policy**

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

Q Search

+

▼

✂

↗

+ Quota

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 33.5.0.0

This section describes the new features and components introduced in this version on top of Alteon version 33.0.3.0.

vRA/vRO Workflows

The vRA/vRO plug-in, available for direct Alteon configuration, now offers more than two dozen out-of-the-box workflows for device onboarding, networking, and virtual servers and service configuration. The plug-in will be available for download on github.

The plug-in was tested for vRA/vRO version 8.5.

HTTP/3 Gateway

The following enhancements were added to the HTTP/3 gateway feature:

Layer 7 Services

The HTTP/3 gateway supports the following Layer 7 services:

- Integrated WAF
- BoT Manager
- DNS over HTTPS proxy
- AppShape++ for content-aware server selection and content modifications.

Note: Content rules and Content Modification rules were not tested for HTTP/3 gateways.

HTTP/3 Service Advertise Parameter

HTTP/3 does not have a designated port like 443 for HTTPS. A browser first connects to the server with HTTP/2 to discover the service. A server that supports HTTP/3 responds with an Alt-Svc header, including the port for HTTP/3, such as Alt-Svc: h3=":50781". If the browser supports HTTP/3, it opens a QUIC connection to the specified port.

In the previous version, this was achieved using AppShape++ or a Content Modification rule.

In this version, a dedicated flag was added for the HTTPS virtual service to advertise the HTTP/3 service (relevant only to HTTP/2 and HTTP/1 services).

- In WBM/APSolution Vision: On the *Virtual Service* pane > *HTTP* tab, enable **Advertise HTTP/3 Service** and configure the HTTP/3 service port
- In CLI: Configure the HTTP/3 service port with the following command: `cfg/slb/virt X/service 443/http/http3port.`

Hardware Acceleration

SSL processing for HTTP/3 (QUIC) can now be offloaded to the hardware acceleration component (QAT), when such a component is present (models S and SL).

Chinese Crypto Algorithms (SM2, SM3 and SM4) Support

The National Password Authority for the People's Republic of China password industry standard approach has announced the SM2/SM3/SM4 and other cryptographic algorithm standards and application specifications. SM is the abbreviation for the national commercial cryptographic algorithm of the People's Republic of China.

- SM2 is a public key cryptography algorithm based on elliptic curve cryptography, including digital signature, key exchange, and public key encryption. It is used to replace international algorithms such as RSA/Diffie-Hellman/ECDSA/ECDH.
- SM3 is a password hash algorithm, operating on 512-bit blocks to produce a 256-bit hash value.
- SM4 is a block cipher used to replace DES/AES and other international algorithms.

The following SSL features are supported on Alteon with SM support:

- Client-side SSL offload:
 - Client Authentication can also be supported but only with the ECDHE-SM2-WITH-SM4-SM3 cipher
- Server-side SSL encryption
- Import of SM2 private key and certificate
- Self-signed SM2 certificate generation

Note: For Alteon support of the SM cipher suite:

- A special image, available only to the Chinese market, must be installed on the Alteon device.
- A special license for SM ciphers must be installed. Without this license, SSL offload is not enabled on the special image.
- The processing of SM ciphers is performed in software only.

NFR ID: 201202-000006

64GB RAM on 5424/5820

The 5424/5820 platforms can now support up to 64 GB RAM, allowing for processing a higher number of concurrent connections. HPP models will now be available for these models.

BGP IPv6 ECMP Traffic Load Balancing

ECMP (Equal Cost Multipath Protocol) for BGP enables Alteon to distribute egress traffic between multiple next hop routers that have an equal cost path to the destination.

ECMP for BGP now also supports IPv6 traffic (IPv4 support was introduced in version 33.0.3.0).

Note: ECMP for BGP is available only when using the new FRR BGP library (FRR mode)

NFR ID: 210304-000102

ADFS Health Check

Active Directory Federation Services (ADFS), is a software component developed by Microsoft, that can run on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access-control authorization model to maintain application security and to implement federated identity. It is part of the Active Directory Services.

Alteon can now monitor the health of an ADFS service using an external shell script.

Note: Currently only the cURL tool is supported in these scripts.

Configuring Alteon to use the external health check (HC) feature for ADFS health monitoring involves the following main steps:

4. Before being able to use external health check scripts, you must enable this functionality (`/maint/debug/extscrhcd ena`) and **reboot the device**.
1. Importing an external health check script to the External HC Scripts repository (`/cfg/slb/advhc/extscript/script`; **Configuration > Application Delivery > Server Resources > External HC Scripts**)
2. Creating a health check of type ADFS. This involves associating a script from the External HC Scripts Health Check repository.

NFR ID: 201129-000071

Ansible Modules

New Ansible modules were added for:

- Configuration of GEL DNS parameters
- Control of port processing capabilities (client/server/proxy processing)

NFR ID: 210215-000073, 210215-000074

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**).

Source NAT for Health Checks

Health checks of servers use as the source IP address the Alteon IP interface to which the servers are connected. Now it is possible to specify a different IP address (NAT) as source the IP address. To achieve this, the following is required:

- Configure the health check NAT address for the IP interface connected to the servers
- Turn on the **Source NAT** flag in the respective health check.

This capability is supported only for IPv4 servers.

Important! When using source NAT for health checks, the IP interfaces must not be synced with the peer device as part of Configuration Sync mechanism (the IP interface sync is disabled by default). In a high availability environment, backup devices also perform health checks (to be ready to take over quickly), so each device must use a different NAT address for the health checks.

NFR ID: 210428-000062

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

FIPS Card Support for 7220

The Nitrox III FIPS SSL card is now supported for the Alteon 7220 platform.

To order Alteon 7220 FIPS, order the D-7220S platform required and the separate FIPS II card part number (factory installed).

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.

Auto Policy Http Settings **WebSocket settings** Security Log

☒ WebSocket Inspection

☒ Allow Idle Session Timeout (Min.)

Connections per Source

Slowloris

☒ Protection Against "Low and Slow" Attacks

Time Gap Between Checks (Sec.)

Minimal Amount of Sent Data (KB)

Maximum Frame Size (KB)

WebSocket Extension

Client Payload Type

☒ Server Payload Type

Predefined Policies

Name	Mode
Vulnerabilities	<input type="text" value="Active"/>
Database	<input type="text" value="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.

The screenshot shows the AppWall configuration interface. At the top, there is an 'Action' dropdown menu set to 'Active'. Below this is a 'Base Paths' section with a text input field containing a forward slash '/'. Underneath is an 'Endpoints' section featuring a search bar, a '+ Quota' button, and four icons: a plus sign, a funnel, a pencil, and a double arrow. The main part of the interface is a table with three columns: 'Endpoints (8)', 'Quota', and 'Action'.

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.

Filter Tunnel Command

Filters are grouped into tunnels. Filter matching is done first on a Layer 1-Layer 4 basis. Once there is a match for a filter, the additional matching is only done inside the tunnel.

The filter tunnel creation logic is as follows:

1. Each non-HTTP filter has its own tunnel.
2. `Filterset` creates a separate filter tunnel.
3. A tunnel is created per physical port plus IP version, and includes all HTTP filters that do not have an SSL policy

4. HTTPS filters are grouped according to the following parameters: Physical port, IP version, SSI policy, Certificate, and SSL Inspection
5. Filters with Application 'none' are added to an HTTP tunnel if it exists. If there is no HTTP tunnel, the filter will not have a tunnel.

A new CLI command was added (`/info/slb/ftunnel`) to better expose the grouping of the filters into tunnels.

WHAT'S CHANGED IN 33.5.7.0

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 33.5.6.0

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

Password Policy Enhancements

The following enhancements were added to the password policy:

- The password policy can now be enforced on the default admin user.
- You can set the password to contain the username or not to contain it.
- You can define the minimum number of times that you cannot use consecutive repetitions of the same number or letter. For example, if this value is set to 4, a password containing “aaaa” or “5555” is not allowed, while a password containing “aaa” is allowed.
- You can define the minimum number of sequential inputs of consecutive letters or numbers (right-to-left or left-to-right) of the QWERTY keyboard that you cannot use. For example, if this value is set to 5, a password containing “qwerty” is not allowed while a password containing “qwer” is allowed.

Note: This rule does not include special characters.

"wget" Package Update

The WGET library was upgraded to version 1.21.4.

NFR ID: 220808-000107

SecurePath Policies Number Increase

The maximum number of SecurePath policies was increased from 50 to 100 for all platforms and form factors.

NFR ID: 230302-000167

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 33.5.5.0

Network HSM (Thales/Gemalto) Enhancements

The Network HSM client was updated to version 10.5.1 (previously it was 7.4).

In addition, a periodic health check is performed on the HSM appliance and if it is down, all SSL/HTTPS virtual services are also down.

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.

UDP Virtual Service Down Response

In previous versions, when UDP requests were sent to a UDP virtual service that was down, Alteon did not respond. When those requests were sent for health check purposes, the lack of answer did not produce an error that the service was down, as UDP clients expect ICMP errors as a response when a UDP service is down.

In this version, Alteon responds with an ICMP error to requests to UDP virtual services that are down. To preserve backward compatibility the `srvdown` flag is used to enable the new behavior under UDP services (**Connection Handling on Service Down** in WBM).

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 33.5.4.0

Integrated WAF SUS and GEO DB Update Via Proxy

Auto-updates for WAF SUS and GEO DB can now be performed through a Proxy server.

Use `/cfg/sys/mgmt/awproxy` to set the interface to route the traffic to the proxy server.

The management interface is defined by default.

NFR ID: 220601-000032

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.

Service and Real PPS Collection Interval

Starting with this version, the service and real PPS collection is enabled by default and collects the information every 20 minutes in .csv format. In addition, the interval can be now adjusted using the `/cfg/slb/adv/pps/interval` command.

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 33.5.3.0

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%.

Tech Data Ready Notification

The generation process of the tech data file can be a lengthy operation. Prior to this version, when the generation process was performed via the WBM, the **Completion** notification indicating the completion of the process disappeared automatically a few seconds after it would first display, and therefore was frequently missed by the end-user. Starting with this version, the **Completion** notification of the tech data generation process does not disappear automatically.

VMA Default

The default of the **Include Destination IP in VMA (vmadip)** parameter was changed to enabled (previously it was disabled), as in most scenarios this provides better traffic distribution and performance. Upon software upgrade to this version the existing configuration is preserved.

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.

Server Group and Real Server Description

The length of the **Description** field for Server Group and Real Server objects has been increased from 31 to 128 characters.

NFR ID: 220225-000012

External Health Check

The external health check capability that was released in version 33.5.2.0 is now supported also on Alteon VAs installed using an Ubuntu18 image.

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 33.5.2.0

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

Proxy ARP Entries

Prior to this release, the number of Proxy IP (PIP) addresses that could be configured on Alteon was limited to 2048 because only 2048 ARP entries were reserved for PIP. This has now been increased to up to 8192 entries for IPv4 PIP addresses and up to 4096 NBR entries for IPv6 PIP addresses.

NFR ID: 220303-000127

External Health Check

The external script capability that was released in version 33.5.0.0 for ADFS health checks can now be used to define generic external health checks.

Notes:

- Currently, curl is the only command-line tool these scripts support.
- To use this capability on a vADC, the ADC-VX must also be updated to version 33.5.2.0.

Limitation: This capability does not currently work on Alteon VAs installed using an Ubuntu18 image.

EAAF for Alteon Feed Eligibility Based on GEL Entitlement

Alteon devices deployed with the GEL Secure Pro license are now eligible for the ERT Active Attacker feed download directly from MIS or via APSolute Vision versions 5.4 and 4.85.20 based on the entitlement ID and without the need to register the devices' MAC addresses.

FastView GUI Configuration Removal

Starting with this version, the FastView configuration is only available via the CLI.

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 33.5.1.0

GEL Enhancements

GEL Dashboard

The following changes were made to the GEL Dashboard (which require APSolute Vision 5.3):

- The Entitlement Card now shows the entitlement type (Pro or Cloud).
- The Perform and Secure Add-ons parameter was removed from the UI (it is not relevant since moving to GEL Pro)

GEL Allocation Granularity

The following Alteon throughput allocation options were added: 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.

NFR ID: 211020-000175

Number of Alteon DNS Responders

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

NFR ID: 211102-000089

Ping6 Response

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

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

```
times <#num_of_times> <#delay_between_times> "ping6 <ipv6_address>"
```


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

```
times 4 0 "ping6 4001::3"
```

NFR ID: 211102-000064

EAAF UI

The EAAF feed location is now configurable from **System > Subscription Management**. You can choose to download the feed directly from the Radware domain (default), or indirectly from APSolute Vision, if Alteon does not have egress access to the Internet.



Note: When Alteon is running in ADC-VX mode, the EAAF location is set at the ADC-VX Admin level.

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.

WHAT'S CHANGED IN 33.5.0.0

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.

Include "remote address" at the TACACS request

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

NFR ID: 210319-000010

Ignore Non-existing Fields in JSON

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

Event Counter Default Change

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

When requested by TAC, enable event counter using the command `/stat/counter/event ena` before issuing TechData. Radware recommends disabling 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.

MAINTENANCE FIXES

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

Fixed in 33.5.7.0

General Bug Fixes

Item	Description	Bug ID
1.	Changing the vADC management address caused the ADC-VX management address to be removed in ifconfig.	AL-139803
2.	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-140617
3.	The backup WAN link server did not come online while processing a DNS query.	AL-140648
4.	On DPDK platforms, the MNG port bonding mode was incorrect. It was set to round-robin instead of active-backup.	AL-140820
5.	When a fragmented packet matched a filter with "reverse enabled" , the device rebooted.	AL-140964
6.	After a failover, there was a 30 second to one minute delay before all eight IPv4 BGP prefixes were sent out to the neighbors.	AL-140980
7.	The group backup server status was DOWN when queried via SNMP.	AL-140987
8.	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-141062
9.	The Secured Web Applications view for a user with the user role "Web AppSecurity Owner" hung with a "Loading..." message.	AL-141131
10.	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-141135

Item	Description	Bug ID
11.	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-141151
12.	When clisaging "both" and clfstage "both" are enabled, a memory leak occurred which eventually led to the health checks failing.	AL-141152 AL-141155
13.	Was not able to connect to Alteon via SSH in rare scenarios because the maximum number of sessions exceeded.	AL-141166
14.	There was an error in JSON Fancy Names.	AL-141202
15.	Persistent session mirroring did not properly mirror the group names to the backup device when the group names had the same first character.	AL-141211 AL-141213
16.	After the DNS cache timer expired, Alteon did not query for the FQDN origin if the answer was a CNAME.	AL-141239
17.	A real server health check failed even when there was response to the health check packets.	AL-141247
18.	There was a problem with config sync of a TrustedCA certificate.	AL-141313
19.	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-141323
20.	After disabling and enabling a BGP peer, the vADC rebooted.	AL-141345
21.	An Alteon 5208XL platform rebooted with a software safe restart.	AL-141424
22.	After upgrading from version 32.4.x to 32.6.x, the user was forced to reduce the session capacity number.	AL-141461
23.	After running /boot/rsrscs/cur, an increased disk size was not reflected.	AL-141469
24.	On a 5424 platform with 16/24GB RAM, setting the MTU was blocked.	AL-141476
25.	Services went down after revert apply failed.	AL-141585
26.	Added a debug command and debug logs for helping to debug an SP panic involving a filter configuration.	AL-141613
27.	vADC2 and vADC3 auto-rebooted due to a software safe restart	AL-141625 AL-141626
28.	When FastUpload was activated, files larger than the threshold (which therefore were not inspected) failed to upload.	AL-141636

Item	Description	Bug ID
29.	After upgrading to version 33.0.9.50, SP1 has high CPU utilization on vADC4.	AL-141700
30.	The overload status was activated when at least one LOGEXP health check operand detected an overload.	AL-141753
31.	A BGP flap occurred due to a non-reachable IP address used in getlog.	AL-141866
32.	A compression limit above 10000 MB was not correctly pushed to a vADC.	AL-141880
33.	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-141936
34.	After analyzing a customer-reported reboot, added a protection code to prevent access to released memory.	AL-142164
35.	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-142248
36.	Many panics or core dumps were generated.	AL-142307
37.	There was an incorrect session count with the pbind cookie.	AL-142312

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.	<u>AW-50131</u>
9.	AppWall GUI is showed connection error and the error message "Cannot connect to management server".	<u>AW-50132</u>
10.	Attacks were not blocked by AppWall.	<u>AW-50168</u>
11.	File Upload issue - Possible AppWall issue on version 7.6.21.10.	<u>AW-50184</u>

Item	Description	Bug ID
12.	Integrated WAF security events were not being retained.	<u>AW-50192</u>
13.	Web service was not working when Tunnel is in Passive mode.	<u>AW-50224</u>

Fixed in 33.5.6.10

AppWall Bug Fixes

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

Fixed in 33.5.6.0

General Bug Fixes

Item	Description	Bug ID
1.	The content rule was not working with an action group when SecurePath was configured in a virtual service.	AL-138520
2.	Alteon sent a duplicate response for each ICMPv6 request sent to the interface IP address of the device	AL-138753
3.	Upgrading from version 32.6.8 to version 32.6.12 to avoid a memory leak resulted in a further degradation.	AL-138918
4.	Problems occurred with an SSL certificate with a Subject Alternative Name with more than 1024 characters.	AL-139073
5.	Using APSolute Vision, there was a back-end SSL handshake failure exception.	AL-139139 AL-139177
6.	There was cyclic reboot of vADC1 on version 33.0.7.50 when data ports were up.	AL-139199
7.	A virtual service froze after an apply operation .	AL-139207
8.	vADC4 rebooted cyclically after Alteon ADC-VX upgraded to version 33.0.7.50.	AL-139215
9.	An IPv6 remote real health check failed via a DSSP health check.	AL-139254
10.	WBM was not available after the mmgmt certificate was updated .	AL-139286
11.	A failed real server mistakenly displayed the current sessions counts.	AL-139378
12.	There was an issue with a non-configured peer.	AL-139426
13.	The IPv6 Network filter for an unspecified address (::/128) overlapped with an IPv4 network filter.	AL-139450 AL-139454

Item	Description	Bug ID
14.	There was an issue session capacity and session mirroring .	AL-139482
15.	There was an unexpected reboot of an ADC-VX device.	AL-139493
16.	When syncing from backup to master, virtual services were deleted on the master, affecting the service.	AL-139498 AL-139506
17.	The device rebooted.	AL-139516
18.	A standby Alteon advertised BGP routes when any BGP related configuration changes were made, and the “advertise BGP on HA backup peer” option was disabled.	AL-139544
19.	On an Alteon D-6024S platform, the RX and TX PPS statistics value seemed stuck in the prefmon file.	AL-139590
20.	vADC-2 was restarting on both ADC-VX instances in a High Availability environment.	AL-139630
21.	Sessions through transparent SSLi failed when sending traffic to a VRRP MAC.	AL-139641
22.	The Alteon embedded dashboard was visible even though is no longer should be available.	AL-139647
23.	Alteon TRP MIB file (CHEETAH-TRAP-MIB.mib) was missing a definition for session table threshold traps.	AL-139667
24.	An IP address deleted in Smart NAT was not released.	AL-139871
25.	The /info/vADC command output incorrect throughput for the vADC.	AL-139887
26.	Traffic graphs on the dashboard were not updated during a performance test.	AL-139911 AL-139916
27.	There was an issue with vADC High Availability if a high number of CUs are assigned.	AL-139975
28.	A real server in shutdown mode that was in a network rule could not be synced to a peer.	AL-140029
29.	Could not download tech data.	AL-140107
30.	The /oper/slb/group/shut (connection shutdown) did not work correctly.	AL-140186
31.	Issue using AppShape++ to add a PIP if the client IP address was in the same subnet as the server.	AL-140228
32.	After upgrading from version 33.5.4.0 to version 33.5.5.1, the NAT health check configuration was missing.	AL-140259
33.	Application Service Engine Out-of-sync issue	AL-140275

Item	Description	Bug ID
34.	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-140284
35.	After running automation with an API call that failed, accessing the WBM on Alteon VA produced a 50X error.	AL-140414
36.	FRR BGPv6 session not established over the default gateway	AL-140555
37.	Inconsistent restart information between ADC-VX and vADC in TechData.	AL-140565
38.	The RST packets originated after an inactivity timeout from the proxy were sent with wrong source MAC instead of the proxymac.	AL-140574

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 33.5.5.0

General Bug Fixes

Item	Description	Bug ID
1.	On an ADC VA, an SP1 freeze for slb_pbt_age_entries occasionally caused the device to reboot.	AL-49407
2.	The Websec module fluctuated between down and up.	AL-49481
3.	The APP response was not calculated correctly when there were matches to the content class	AL-49483
4.	DNS Vulnerability CVE-2004-0789 was fixed.	AL-49494
5.	The FQDN real indexes changed during get config.	AL-49505
6.	After upgrading to version 33.0.x, the Apply time increased from 12 to 18 seconds.	AL-49512
7.	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-49519
8.	Alteon SSH failed a security audit.	AL-51834

Item	Description	Bug ID
9.	The CDP group table became empty when deleting one entry case.	AL-51871
10.	The static NAT for GRE traffic in point-to-point was incorrect.	AL-51874
11.	The VLAN 2090 error was assigned to more than 32 PIPs.	AL-51886
12.	The /oper/slb/sessdel command did not work for ESP sessions.	AL-51893
13.	The LinkProof Smart NAT ID disappeared.	AL-51902
14.	There was a corruption in the NAT rule configuration.	AL-51904
15.	Updated the REST API Guide to explain how to retrieve the high availability state via REST API when in VRRP mode.	AL-51912
16.	On a KVM VA, health checks to AppWall and nodejs failed in single IP mode.	AL-52632
17.	The appwallUp and appwallDown traps were sent with the wrong OIDs.	AL-52637
18.	In the Ansible SSL policy configuration, added the option "none" to fe_intermediate_ca_chain_type.	AL-52644 AL-52646
19.	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-53591
20.	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-53601
21.	Hid the internal address from the BE session table.	AL-53606
22.	When enabling LACP, the vADC rebooted.	AL-53609
23.	On a 6024 SL platform, as unable to give the response to a TCP-SYN message.	AL-53987
24.	The DNS responder replied to the DNS response with a malformed packet.	AL-54028 AL-54032
25.	Alteon failed to support the OID for Temperature sensor 3 and Temperature sensor 4.	AL-54701
26.	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-54714
27.	On a vADC, the perf_rec_2.tmp.old file utilized all of the disk space.	AL-54721

Item	Description	Bug ID
28.	In an SLB with pbind environment, when a service was configured with AppShape++ and alwayson, upon receiving the traffic the device rebooted.	AL-54726
29.	There was a discrepancy in the output hard disk between the CLI and WBM.	AL-54732
30.	In an ADC-VX environment, when VLAN sharing was enabled on a 5424 platform, traffic destined to the vADC was dropped.	AL-54740
31.	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-54750
32.	A vADC rebooted because of a software safe restart.	AL-54759
33.	In WBM, the password strength (pwscrit) menu was not included.	AL-54769
34.	On an Alteon VA, even though the disk space was increased, logs were issued regarding the storage capacity.	AL-54771
35.	The SSL inspection advanced virtual wire check was down when the IDS ports belonged to trunks.	AL-54919
36.	When a syslog message sent from Alteon did not use LF as delimiters, the vDirect traffic event was not triggered .	AL-54926
37.	The health check run-time instance was shared unexpectedly when several cntrules with different groups were defined under the same virtual service.	AL-54934
38.	Logs were added in relevant places that failed during key/certificate modification.	AL-55161
39.	On an ADC VA, an SP1 freeze for slb_pbt_age_entries occasionally caused the device to reboot.	AL-55166
40.	When sending an FQDN update, the SSL-related configuration that was sent was still in progress and caused a configuration issue.	AL-138537
41.	Unexpected reboot	AL-138554
42.	Both Alteon devices panic at the same time, multiple times.	AL-138690

AppWall Bug Fixes

Item	Description	Bug ID
1.	Attack recorded in Passive state.	DE81421
2.	The Websec module down/up statistic was fluctuating.	DE81882

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

Fixed in 33.5.4.0

General Bug Fixes

Item	Description	Bug ID
1.	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.	DE78514
2.	Interface 256 could not be selected for switch HA advertisements.	DE78887 DE78893
3.	Using WBM, an update to the cipher list was greater than 256 characters and was not accepted.	DE78981

Item	Description	Bug ID
4.	The Unit label for a rule level timeout was different between WBM and the CLI.	DE79013
5.	On DPDK virtual platforms, traffic passing thorough BWM shaping contracts caused invalid buffer access and caused the vADC to reboot.	DE79048
6.	There was high SP memory utilization during a low traffic period.	DE79059
7.	Getting the vADC partition size failed and caused the vADC to hang on restart.	DE79118
8.	After running /stats/slb/pip, the SNMP OID was missing from the output.	DE79215 DE79221
9.	Could not configure filtpbkp in hot-standby mode. Modified the CLI validation to resolve the issue.	DE79223
10.	VPN connectivity failed because of the IKE and the ESP sessions being bound to different servers.	DE79230
11.	The Root Bridge was not properly declared in MSTP.	DE79244
12.	Using WBM, the hard disk capacity displayed incorrectly because secondary disk size was not counted.	DE79253
13.	SNMP walk failed because the OID did not increase.	DE79432
14.	A vADC did not handle traffic when it became the master.	DE79521
15.	An AppShape++ script trying to insert a script greater than 50k characters into the cmdLogMP-1-1 file caused the device to reboot.	DE79543
16.	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.	DE79605
17.	System analytics were sent with null data.	DE79618
18.	There was an issue with FQDN and multiport applications because there was no server name for the FQDN ephemeral real server in the XML sent to AppXcel.	DE79728
19.	When setting the time zone by name and not changing the default NTP time zone, a warning is issued after the Apply.	DE79799
20.	When clsaging both is enabled with tunnels, the device rebooted.	DE79830
21.	The application services engine was not synchronized with the current configuration and the change was not saved.	DE79843

Item	Description	Bug ID
22.	In an SLB and PIP environment, there was a discrepancy in the PIP statistics between /st/slb/pip and /st/slb/aux.	DE80127
23.	SANs fields greater than 1024 bytes were accepted while generating a CSR.	DE80144
24.	The traceroute response packet was sent by Alteon with the wrong interface.	DE80191
25.	After upgrading from version 30.5.3.0 to 32.4.6.0, VLANs displayed as Down.	DE80318
26.	After downloading and uploading a configuration via REST API, SlbNewCfgFQDNServerTable was empty.	DE80347
27.	An SSLi issue caused the device to reboot.	DE80419
28.	An incorrect GSLB DNS query refused a response for non-existing domains.	DE80448 DE80452
29.	Unexpected BFD behavior.	DE80465
30.	Logging the times command caused the device to reboot.	DE80600 DE80604
31.	There was an AppShape++ namespace conflict when using rule lds that end with digits.	DE80628
32.	SNMP trap 193 is returned for a disk space issue when it was not included in its MIB.	DE80688
33.	The Secured Web Applications (secwa) pane did not display on a standalone device.	DE80694
34.	On an ADC-VX, the MP caused a reboot.	DE80819
35.	From the CLI, could not connect to real server via Telnet.	DE81211
36.	Using WBM, could not change the protocol TCP/UDP for port 389.	DE81262
37.	The real server health checks treatment was delayed when an unavailable rlogging server was configured.	DE81275
38.	The label in the output regarding MP memory for the <code>i/sys/capacity</code> command was not clear. Changed the label from "mp memory" to "total device memory".	DE81368
39.	The last digit of the year was missing in the output for some OIDs because arrayLength-1 was assigned with a Null character.	DE81377
40.	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.	DE81518

Item	Description	Bug ID
41.	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.	DE81559
42.	There were DNS errors in the Alteon MP logs.dns due to DNS resolution not being case-insensitive.	DE81601
43.	Back-end SSL with client authentication using static RSA caused a bad MAC address.	DE81674

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 33.5.3.0

General Bug Fixes

Item	Description	Bug ID
1.	A misleading license error message was issued.	DE76146
2.	A search operation did not work correctly.	DE76189
3.	In WBM, after Submit, SSH keys is incorrectly displayed as Do Not Erase.	DE76222
4.	The management port status of eth0 and eth1 displayed incorrectly.	DE76255
5.	On an Alteon VA device, in some cases SSH and WBM connections failed due to the non-availability of free virtual memory.	DE76268

Item	Description	Bug ID
6.	The Throughput threshold license caused an error even though the high threshold had not been reached.	DE76316
7.	When accessing the tunnel meta header of a frame for non-tunnel traffic with filter reverse session support, the device rebooted.	DE76383
8.	After upgrade, running the /boot/cur command displays the image download date incorrectly.	DE76396
9.	In an Alteon SLB environment, external health checks failed when a tag was enabled on the real server port.	DE76481
10.	In WBM, the configured Server Side Idle Timeout values were not displayed.	DE76503
11.	Generating applogs resulted in high MP CPU utilization. A new warning message regarding this is now issued when running the /maint/applog/showlog command.	DE76530
12.	Traffic was sent to a real server when the real server health check failed due to its related buddy server failing.	DE76544
13.	Features that in the background automatically created virtual servers sometimes caused the High Availability configuration to be different between the HA devices.	DE76556
14.	Changing a health check for LDAP(S) caused a reboot.	DE76640 DE76644
15.	Configuration sync issued caused the device to reboot.	DE76659
16.	Bandwidth Management (BWM) did not restrict upload bandwidth.	DE76723
17.	IPC module issue caused the device to reboot.	DE76761
18.	Configuring 3044 real servers caused high MP CPU and LACP problems.	DE76792
19.	The power supply failure logs had the wrong status for the power supply.	DE76837
20.	The device ran out of Heap memory, causing it to reboot.	DE76884 DE76888
21.	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.	DE76967
22.	In an SLB environment with dbind forceproxy and dbind ena, the device rebooted unexpectedly.	DE77028
23.	When generating techdata, the techdata creation failed.	DE77062

Item	Description	Bug ID
		DE77066
24.	Changing the SIP from network class to subnet/network in a filter was not updated in the configuration.	DE77191
25.	When configuring the action in an HTTP modification rule, the Alteon action was not validated correctly.	DE77280
26.	No data was received from Alteon for LinkProof Analytics	DE77436 DE77440
27.	The device rebooted because of an issue with nsgroup auto-completion.	DE77455 DE77459
28.	The device rebooted because of hardware Watchdog issues.	DE77490
29.	The DNS persistence cache cleared on Apply of GSLB changes. An alert was added to display when this occurs.	DE77520
30.	Generating tech data could take a long time.	DE77624
31.	vDirect issued an error for table SpMemUseStatsTableEntry using SNMP.	DE77645
32.	MP CPU utilization was high, causing the device to reboot.	DE77730
33.	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.	DE77827
34.	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.	DE77903
35.	Importing the configuration resulted in a missing bitmap handling.	DE77917
36.	The device rebooted with the following error: SIGSEGV(11) thread STAT(tid=71)	DE77948
37.	When performing a simultaneous operation of import and apply config, changes were displaying in diff.	DE77998
38.	Defect with the Connection module handling traceroute packets.	DE78005
39.	When a packet capture running on a data port stopped, the device rebooted.	DE78061
40.	The device rebooted when executing a diff from SNMP.	DE78156
41.	In an outbound LB environment, the source port of the connections was changed, leading to traffic failure.	DE78214
42.	A random reboot was analyzed and fixed.	DE78927

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 request 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 33.5.2.0

General Bug Fixes

Item	Description	Bug ID
1.	Using SSH, there was no matching key exchange method found when connecting from Ubuntu 20.	DE70425
2.	On an Ubuntu 18 VA device, when selecting a time zone GMT offset greater than 4 hours, the GEL license activation failed.	DE73643
3.	Application delivery features were not available via API for the slbviewer user role.	DE74200
4.	When an IPv6 virtual server used IPv4 servers for load balancing and if any SLB config apply was performed, the existing sessions were closed.	DE74228
5.	An Alteon 5224 platform rebooted because of a power cycle.	DE74354
6.	PCI compliance with Alteon SSH failed.	DE74376
7.	The device restarted by a software panic.	DE74398
8.	After config sync, the Traffic Event Log policy sent a log via the data interface.	DE74452
9.	There was a Switch HA failover issue.	DE74516
10.	vADC buffer memory related to SSL caused a reboot.	DE74587 DE74591
11.	An SSH management connectivity issue occasionally caused a reboot.	DE74608
12.	The wrong time zone offset was sent to the NTP server.	DE74638

Item	Description	Bug ID
13.	On a vADC, the GET /config/SlbCurCfgEnhVirtServicesTable message was received during config sync and all hash tables were initialized (zeroed), causing a reboot.	DE74690
14.	A malformed server caused a miscalculation of the RTO, which led to the retransmission taking a minute, in which time the server closed the connection.	DE74762
15.	A vADC stopped processing production traffic.	DE74790
16.	The MP CPU utilization was high with DNS packets (dport 53).	DE74811
17.	When configuring network settings, an internal error was issued.	DE74820
18.	On an ADC-VX, an LACP issue was caused by high MP CPU utilization.	DE74846
19.	When the device started after a reboot, it stopped performing ARP base health checks.	DE74868
20.	Alteon Bot Manager used 1.1.1.4 in the Host Header while sending POST request to the endpoint.	DE74920
21.	Alteon VA devices deployed in Hyper-V experienced high CPU usage compared to other hypervisors.	DE74935
22.	Using SNMPv3, the “Unknown user name” is now issued for invalid usernames and invalid passwords.	DE74950
23.	The Ext.HC script did not generate traffic.	DE75005
24.	From WBM, when the SSH key was set to be deleted, after clicking Submit it was immediately deleted before the device was rebooted.	DE75022
25.	The device rebooted because of a software panic.	DE75040
26.	After inserting a 1 G GBIC, message logs did not display.	DE75060
27.	Changing vADC CUs caused syslogs to be removed.	DE75090
28.	AppWall LDAP connection failures were caused due to the multiple creation of MP processes.	DE75157
29.	After rebooting, configuration sync failed, and the configuration was stuck in diff with the same error.	DE75229
30.	Alteon did not display the Korean language correctly when using local language-Korean.	DE75256
31.	When trying to use Single IP in Azure, a message was issued that the user should use Multiple IP address mode.	DE75282 DE75286

Item	Description	Bug ID
32.	After an Apply failure due to an empty passphrase for certificates, after reboot the entire configuration went into diff.	DE75333 DE75337
33.	There was duplicate entry validation error for two domains where one had a hostname, and the other did not have a hostname.	DE75357
34.	When using the Russia time zone, the incorrect time displayed for the /info/sys/time command and in AppWall Forensics.	DE75404
35.	On an Alteon VA, packets larger than the negotiated MTU size were forwarded.	DE75429
36.	On a vADC, when executing SSL stats commands, the vADC rebooted.	DE75448
37.	The /oper/slb/group command displayed different output when two SSH sessions were opened to a single device.	DE75486
38.	After the primary real server was activated in a group, the session handled by the backup real server was fastaged.	DE75538
39.	An SSH management connectivity issue occasionally caused a reboot.	DE75552
40.	When gathering the device output, memory stats information did not appear in the techdata.	DE75689
41.	The client certificate went through OCSP verification even though it is in OCSP stapling mode.	DE75804 DE75808
42.	SNMP polling resulted in an incorrect response.	DE75840

AppWall Bug Fixes

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

Item	Description	Bug ID
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 33.5.1.0

General Bug Fixes

Item	Description	Bug ID
1.	Mirrored session statistics were not updated for Smart NAT Inbound traffic.	DE71996
2.	Attempting to delete a server or CA certificate group explicitly or implicitly resulted in an AX internal OOS failure.	DE72202
3.	When the real and virtual server statistics were incremented or decremented the logs were not updated.	DE72088
4.	Using WBM, expired certificates could not be exported because there was a validation check on the "validation period" (1 to 3650).	DE72169
5.	A user was allowed to configure a duplicate Static ARP entry using WBM, but not the CLI.	DE72186
6.	Upgrade failed because of incorrect resource allocation (SP and AW cores).	DE72284
7.	When trying to change the Traffic/AppWall capacity units (CUs) for a single vADC, an error occurred.	DE72346
8.	In an IPV6 environment, when Static NAT was configured, ICMP traffic failed.	DE72403
9.	IPsec sessions abruptly aged out due to an incorrect interpretation of TCP flags.	DE72427
10.	An Open SSL vulnerability (CVE 2022-0778) was fixed.	DE72463
11.	An HA failover caused SIP packets to be lost.	DE72530

Item	Description	Bug ID
12.	When there was an overflow of the Current Sessions value, unexpected statistics of Available Sessions and DNS answer resulted.	DE72560
13.	Bandwidth utilization was displayed incorrectly as Mbps, when it should have been MBps.	DE72626
14.	After upgrade, the configuration was not preserved.	DE72655
15.	In an ADC-VX environment, when executing putconfig and tech data collection at the same time on a vADC, the vADC rebooted.	DE72664
16.	When there was a TCB block leak, DSSP health checks failed.	DE72723
17.	During a vADC shut down, the ADC-VX process requests the TD to recycle network driver buffers. This process took more time than was allocated for the TD process to run.	DE72746
18.	On a 6024 platform, increasing the session table by size 200% required a minimum 64 RAM.	DE72811
19.	The Ansible module description of vip_health_check_mode was incorrect.	DE72817
20.	Using APSolute Vision the Alteon EAAF data base of was not updated.	DE72828
21.	Using Alteon VA, in some cases when running Ubuntu18 OS and DPDK, allocation of SPs was not based on the vCPU configuration.	DE72847
22.	The AppWall nodejs module flapped on virtual planforms in the following cases: 1. When there are more than 10 vADCs 2. When vADCs are configured with the basic flavor.	DE72863
23.	An Alteon cluster running on Azure had high availability issues.	DE72946
24.	After a reboot, the "Service Always Up" configuration for AppShape++ was not preserved.	DE72959
25.	An Alteon NG 5424-S rebooted because of a BSP problem with the monotonic timer.	DE72986 DE72990
26.	Alteon VA version 33.0.4.0 using Ubuntu12 rebooted on the execution of the Display Certificates Group configuration.	DE73039
27.	There was an error with traps for IPv6-related events.	DE73069
28.	Cookie-based real server selection caused a reboot. Defensive code was added to address the issue.	DE73091
29.	A request to make to increase the height of the "Configuration Sync - Peers" in WBM.	DE73192

Item	Description	Bug ID
30.	A DNS responder with delegation for TCP session did not close.	DE73214
31.	In a WANlink environment, traffic was processed by ISP, which was down.	DE73236 DE73238
32.	Disk space exceeded the high threshold with 80 % usage because of the AppWall cores.	DE73252
33.	On a version 30.5.22.0 vADC, FQDN resolution update failed.	DE73308
34.	On an Alteon VA, intermediate certificates were not fetched.	DE73343
35.	A health check timeout failure caused a reboot due to a race condition when freeing the object.	DE73538
36.	Fixed Ansible documentation in alteon-device-facts.	DE73620 DE73624
37.	Continuous operations on real server groups (additions, deletions, amendments) could lead to an internal OOS state.	DE73666
38.	In an Alteon VA environment, occasionally empty syslog messages were generated when the size exceeded 1300 bytes.	DE73750
39.	On a vADC, inbound host-based LLB rules were not created using the LinkProof menu due to RBAC issues.	DE73776
40.	SSLI did not forward traffic when creating the FW HA, due to 10G not working correctly on VHT.	DE73818
41.	Trying to add vADC licenses to the ADC-VX when vadcadv had a custom flavor caused an error.	DE74078
42.	The maximum supported length of the RADIUS password is 16 characters. Authentication failed If the password was configured with more than 16 characters.	DE74796 DE74800

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 33.5.0.0

General Bug Fixes

Item	Description	Bug ID
1.	The special Regex character '\ ' should be added.	DE69956
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.	DE69966
3.	FQDN real server IP addresses incorrectly ended with a period (".").	DE70255
4.	Rebooting an ADC-VX caused vADCs to be stuck in the initialization stage.	DE70265
5.	The ICMPv4 real server health check failed while a CLI ping worked correctly. A v4 debug command was added.	DE70304
6.	A user was locked out after making a password change.	DE70326
7.	A mechanism was added that prevents false PS (power supply) status indications when there is a dual PS configuration.	DE70366
8.	After booting Alteon VA with version 33.0.2.50, the initial configuration was not applied.	DE70399
9.	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.	DE70428
10.	When copying the x-forwarded-for header, an overflow occurred.	DE70436 DE70440
11.	The TLS 1.3 protocol did not display in the Backend SSL policy.	DE70447
12.	The XFF code in the HTTP/2 proxy used the VIP instead of the Client IP address.	DE70462
13.	The AppWall check did not recognize that AppWall was frozen and did not restart AppWall.	DE70471
14.	Configuration sync failed due to a long certificate group ID.	DE70489
15.	With IDS chain configured, ICMP responses from the server were not forwarded to the client.	DE70499
16.	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.	DE70516
17.	A panic occurred during a packet capture.	DE70545

Item	Description	Bug ID
18.	The HTTP/2 health check did not contain the ALPN protocol in the SSL handshake.	DE70594
19.	After an unexpected reboot of Alteon VA on ESXi 7.0, could not save changes after Apply, and received error messages.	DE70601
20.	The MP CPU utilization was high when applying the configuration, causing a network interrupt.	DE70615
21.	After upgrade, empty groups with no real server added to them could shift the group index map.	DE70634
22.	The ARP table information was not the same between the CLI and WBM.	DE70691
23.	A mixed type SNS request failed (dnsresponder VIP IPv4 and query type IPv6, and vice versa).	DE70705
24.	An unexpected VRRP failback when preemption is disabled.	DE70749
25.	A panic occurred due to memory corruption.	DE70775
26.	Alteon displayed inaccurate SFP Tx and Rx power values.	DE70788
27.	Could not manually delete a session table entry for VPN traffic.	DE70805
28.	Uppercase characters were, incorrectly, added to HTTP headers for HTTP/2 proxy, which generated the following error: Upper case characters in header name	DE70814
29.	The max_cipher_list_length was increased from 16000 to 20000.	DE70969
30.	An SLB apply took longer to execute when it was run as SLB config apply.	DE71001
31.	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.	DE71073
32.	The "Threshold of incoming sessions" event was generated when the total active connections was much lower than the maximum value.	DE71109
33.	When running dbind disable service, a panic occurred when Alteon received the RST packet from the server.	DE71116
34.	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.	DE71136
35.	Enabling IPv6 on a virtual server caused a panic.	DE71151

Item	Description	Bug ID
36.	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.	DE71265
37.	After resetting a non-debug Alteon VA platform, GEL licenses sometimes were lost when they passed non-GEL applicable validations.	DE71292
38.	Fixed the License Manager connection failure algorithm.	DE71355
39.	The LINK LED remained ON even when the optical cable was pulled off or the ACT LED was not working.	DE71475
40.	The file descriptor was allocated and not released during execution of SP/MP profiling./maint/debug/cpuProfiling/	DE71504
41.	A MAC flap occurred because of VRRP advertisements sent by the backup Alteon device.	DE71524
42.	The GEL license logs were generated every 5 minutes, causing memory leaks.	DE71584
43.	Support of stapling and client certificate verification added.	DE71596
44.	Alteon could be down when a specific traffic pattern request interacted with the redirect service using dynamic tokens.	DE71621
45.	On a vADC device, the MP CPU reached 100%.	DE71654
46.	When a DPDK image reset, an unexpected DNS server IP address was added by BSP.	DE71754
47.	After the AppWall health check failed, the MP restarted AppWall every 15 seconds .	DE71818
48.	The Application Services engine was not synchronized with the current configuration.	DE71842
49.	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.	DE71897
50.	Could not allocate memory to run the diff command.	DE71908

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

Item	Description	Bug ID
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 33.0.3.0

General Bug Fixes

Item	Description	Bug ID
1.	Wrong management of TSO buffers and logs flood from the AE module caused a panic.	DE66434
2.	Removed the unnecessary syslog message that appeared in vADCs on each Apply.	DE68578
3.	On an Alteon-VA platform with BWM configured, when switching from DPDK to TUNTAP, in some instances a software panic occurred.	DE68862
4.	Alteon 6420 running on version 32.4.6.50 rebooted due to a software panic	DE68957
5.	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.	DE69010
6.	A MAC flap occurred because of HA advertisements sent by the backup Alteon device.	DE69142
7.	Because of a vulnerability, upgraded to the latest NGINX version.	DE69163
8.	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.	DE69250
9.	On an Alteon 6024 platform, the primary and secondary devices rebooted automatically due to a stack overflow.	DE69296
10.	On an Alteon 6420 platform, there was a data transmission problem with packet fragmentation with a one-minute delay.	DE69334 DE69404

Item	Description	Bug ID
11.	When attaching or detaching an SSL policy, the wrong port changed.	DE69395
12.	On a 7612 platform, after a vADC was enabled there was a large VS address delay.	DE69414
13.	After upgrading from 32.6.3.50 to 32.6.6.0, there was latency/delays.	DE69418
14.	When a DNS Response was received with new IP addresses and new real servers created, the Save flag was set to ON.	DE69419 DE69422
15.	In a BGP, BFD environment, BFD connections went down when BWM processing was enabled, leading to BGP adjacency going down.	DE69437
16.	Config apply took more than 10 minutes.	DE69480
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.	DE69498
18.	When configuring cntclss values, a max length validation failure did not display the correct error.	DE69510
19.	In an ADC-VX environment, trying to create vADC 10 caused a panic.	DE69550
20.	Could not view the connection statistics in both WBM and CLI.	DE69595
21.	Could not configure the user role WSAdmin in SA mode.	DE69641
22.	In an SLB environment with VLAN level proxy configured, in some instances the MAC flapped after an SLB config apply.	DE69668
23.	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.	DE69697
24.	When creating a content class a panic occurred.	DE69769
25.	REGEX created errors in the WBM infrastructure by using illegal characters. This was fixed in the version.	DE69774 DE69777
26.	In a tunnel environment, all configured tunnel static route tables did not display under the route dump.	DE69829
27.	Ansible facts gathered from standalone devices did not provide the correct image list.	DE69867
28.	ICMP pings to an Alteon IF address running in FRR BGP mode generated duplicate ICMP responses.	DE69884

Item	Description	Bug ID
29.	After reboot, Alteon falsely reported that the MGMT IP address was changed.	DE69945
30.	The special character '\' was added to the REGEX string '\\.	DE69958
31.	Alteon 5208 rebooted because of a software panic.	DE69997
32.	Alteon displayed a configuration as pending but would not accept an apply or save. This was because a group associated with fqdnreal was empty.	DE70056 DE70059
33.	The dns-responder with DNSSEC did not work on Cavium platforms since version 32.6.0.0.	DE70114
34.	An Alteon D-5208S platform abnormally rebooted because of a software panic.	DE70233 DE70238

AppWall Bug Fixes

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

Fixed in 33.0.2.50

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.	DE66272
2.	An Internal out-of-sync configuration was detected.	DE68010
3.	In an HA environment, after the backup device rebooted, FTP data sessions disappeared intermittently on the backup device.	DE68027
4.	Config sync failed with EC certificates in the configuration.	DE68187
5.	After user-defined ciphers, the Application Services engine was not synchronized with the current configuration.	DE68194 DE68542
6.	On an Alteon VA device, in some instances if eth0 was removed and then re-attached, Alteon VA displayed more links than the actual interfaces.	DE68223
7.	When the MRST flag was set to on, it was not possible to disable a data port.	DE68253 DE68256
8.	A port disabled in a saved configuration needed to be toggled twice to bring it up after reboot.	DE68267 DE68270 DE68273
9.	Alteon forwarding or routing packets without SRC MAC translation led to a MAC flap issue.	DE68299 DE68302
10.	When the hold timer expired, Alteon sent a notification with a cease.	DE68315 DE68316
11.	Using the WBM, after creating a vADC, the vADC stayed in the init state.	DE68398 DE68401
12.	Alteon responded to Non-RFC compliant responses for DNS requests.	DE68408 DE68411
13.	When the WANlink server was operationally disabled and then re-enabled, the WANlink peak statistics were incorrect.	DE68441 DE68444
14.	In the output for the /c/slb/virt x/cur and /info/slb/virt x command, and unexpected "ipheader x-forwarded-for" item displayed.	DE68500 DE68503 DE68506

Item	Description	Bug ID
15.	Azure Government Alteon VA boot looped on deployment.	DE68561 DE68564
16.	Using APSolute Vision, newly created vADCs were not manageable.	DE68612 DE68615
17.	After upgrading to version 32.6.5.0, vADCs could not be managed by the APSolute Vision server.	DE68793 DE68796
18.	On an Alteon 5424 (ODS-LS2) platform, the real server capacity in standalone and ADC-VX modes was increased in 8192.	DE68846 DE68849
19.	A software panic occurred followed by an AX Out-of-sync.	DE68883 DE68886
20.	Was not enable to sync the configuration between devices in the beta code.	DE68911 DE68917
21.	Issue with FQDN servers. Logs were added to help with this issue.	DE68930 DE68933
22.	A panic occurred with a loss of the configuration. Fixed included not tracing empty DNS responses.	DE68946 DE68949
23.	The SIP INVITE went to the wrong real server.	DE68970 DE68973
24.	An empty user agent caused a panic.	DE69045 DE69048
25.	During the tunnel handling routine, Alteon reboots with IP fragmented traffic.	DE69173 DE69176
26.	BM JS injection occurred when no BM was configured.	DE69192 DE69195 DE69199 DE69202

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

Item	Description	Bug ID
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

Fixed in 33.0.2.0

General Bug Fixes

Item	Description	Bug ID
1.	The L4oper user could not view the Virtual Servers pane.	DE65790
2.	Self-generated sessions (such as sideband connections and rlogging traffic) now apply the PIP configuration regardless of the PIP port processing settings	DE66411
3.	Too many core files took up too much disk space, resulting in techdata failing.	DE66124
4.	The CRL could mistakenly be considered expired before the true expiration time because of the time zone.	DE66218
5.	The device became full with too many open files, causing it to run slowly.	DE66427
6.	Alteon sent malformed SNMPv3 traps when aes128 or aes256 were configured as the privacy protocol.	DE66749
7.	STP packets dropped by the ND caused a loop.	DE66782
	When passing the client certificate via the HTTP header in a multiline in compatible mode, the last hyphen (-) was removed.	DE67198
8.	The router ID was not visible for between routers for traceroute.	DE67261
9.	There was a WBM error for the SLBVIEW user.	DE67376
10.	Using WBM, the DNS responder VIP displayed as up even if it was disabled by configuration.	DE67545
11.	With VMAsport enabled, SSL-ID based persistency was not maintained correctly.	DE67634
12.	When traffic matches a filter that is configured with Layer7 lookup, Alteon panicked.	DE67656
13.	Incorrect units displayed for uploading/downloading bandwidth for WANlink real servers.	DE67714

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

AppWall Bug Fixes

Item	Description	Bug ID
1.	HRS attack: HTTP GET request with BODY was not being blocked while there was a security event.	DE65623
2.	Under some conditions, the AppWall management console WAF stopped working and was not accessible.	DE67515
3.	The AppWall Activity Tracker recognized a legitimate Google search engine as a bad bot.	DE67646

Item	Description	Bug ID
4.	Wrong hosts reported with AppWall Hosts protection.	DE64012
5.	AppWall blocked the server response when a tunnel was in passive mode.	DE65600

Fixed in 33.0.1.50

General Bug Fixes

Item	Description	Bug ID
1.	In an RSTP environment, the port state transition from DISACRD to FORWARD was delayed.	DE66169 DE66170
2.	The SSL Hello health check caused a memory leak which led to a panic.	DE66191
3.	Alteon VA in DPDK mode crashed when BWM processing with BW shaping was enabled.	DE66399 DE66402
4.	After configuring a deny route for a DSR VIP with tunnels set to real servers, the MP panicked.	DE66473 DE66476
5.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66480 DE66483
6.	Using WBM, when users of type 'user' was disabled, they could still successfully log in.	DE66531 DE66534
7.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66573 DE66576
8.	Could not create a new BWM policy on a 4208 device.	DE66623 DE66626
9.	Panic analysis.	DE66641 DE66644
10.	A panic analysis resulted in the following fix: The Watcher can now run over multiple CPU cores, ensuring that it retrieves the expected CPU time even if an unexpected event occurs on CPU #0.	DE66705 DE66708
11.	After a Trust CA group was configured, no other certificates could be deleted even if they were not part of the Trust CA group.	DE66722 DE66725

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

Fixed in 33.0.1.0

General Bug Fixes

Item	Description	Bug ID
1.	The random salt was a predictable random number generation function generating a similar sequence.	DE63668
2.	Could not enable the extended_log via Ansible.	DE63841
3.	For some edge cases, AppWall did not come up because of an invalid variable that was not initialized. The fix was to initialize the variable.	DE63985
4.	When Alteon initiated the connection to a peer that was not directly connected, the outgoing interface was not selected correctly, resulting in the BGP connection not being initiated. For the fix, the interface used to reach BGP peer is now selected.	DE63992
5.	The real health check displayed different times in CLI and WBM.	DE64033
6.	On a 4208 platform, the option to convert to virtual (ADC-VX/ADC) mode displayed the following error message: The operation cannot be performed	DE64092
7.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64155
8.	The MGMT port status was DOWN but the Link and operational status was UP.	DE64235
9.	In an SLB environment with cookie insert enabled, the server responses to the client undergoing cookie processing had a mismatch of the SRC MAC with an incoming client request.	DE64248
10.	An internal link on Alteon VA caused connections to drop.	DE64257
11.	In an HA environment, when the RADIUS service was enabled with mirroring and associated with an AppShape++ script , RADIUS authentication timed out.	DE64321
12.	Applying part of the nginx when disabling the Web proxy took too much time.	DE64336
13.	When pbind clientip and vmasport were enabled, the persistent session was not permanently deleted.	DE64356
14.	Servers were vulnerable to CVE-2021-3449 if they had TLSv1.2 and renegotiation enabled (default). Fix: The MP OpenSSL version has been upgraded to 1.1.1k to fix this.	DE64380

Item	Description	Bug ID
15.	Added a REGEX to accept the dot (.), slash (/), and backslash (\) characters.	DE64459 DE64466
16.	Config sync transmit was aborted between two devices when the sync request was received from a third device.	DE64488
17.	Predefined HTTP headers were used when POST HTTP health checks were sent without taking into the account the actual body length.	DE64524
18.	After receiving the same routes in BGP updates when Alteon failed to set a protocol owner, Alteon deleted the RIB.	DE64534
19.	Using WBM, ephemeral servers did not display in the Configuration menu.	DE64586
20.	After performing /boot/shutdown, TLS version 1.1 was incorrectly being set to enabled.	DE64597
21.	In a BGP environment, when BGP peers were directly connected, the BGP state stayed as Connect even though the local interface was disabled.	DE64648
22.	Using a logical expression health check resulted in an unexpected real server state.	DE64691
23.	Upgrading an ADC-VX generated the following error message on the console: write error: Broken pipe	DE64704
24.	The management Web server did not work due to a bug with the access SSL key on FIPS.	DE64727 DE64732
25.	When the primary group was in an overloaded state, real servers in the backup group displayed as being in the BLOCKED state in the virtual server information.	DE64759
26.	An ICMP unreachable packet coming from the server side gateway was forwarded to the MP instead of the VMASP, which led to a panic while updating the filter information to the frame's metadata.	DE64787
27.	The Layer 2 system configuration had an incorrect BoardType for 7216NCX.	DE64884 DE64889
28.	When real servers were down, Alteon sent traps with the wrong OID.	DE64900
29.	In an SLB environment, when the primary server failed, the secondary backup displayed as "UP" instead of "BLOCKED".	DE64925

Item	Description	Bug ID
30.	On a 7220 platform, when Alteon received a packet with a size greater than 1500, it panicked.	DE64947
31.	In DPS Perform mode, AppWall was not pushed to vADCs.	DE64997
32.	The weighted least connection was not correct.	DE65009
33.	When there was a state transition from backup to master, GARP was not sent.	DE65041
34.	An SP memory leak was caused due to a combination of Bot Manager and the Mux.	DE65056
35.	There was an incorrect rule ID for retrieving statistics from the SP.	DE65178
36.	Added the FastView smfhub self-healing mechanism.	DE65204
37.	Defect that tracked DE65346 – Device auto rebooted with reason of hardware watchdog.	DE65235
38.	Accessing a device using APSolute Vision or WBM caused a memory leak and eventually led to a panic.	DE65241
39.	In an SLB environment, when a connection closed from the server side with an RST, traffic failed on the new connection that matched the session that was in fastage.	DE65285
40.	Even though there are no open connections, new SSH connections were ignored with a “max connection reached” error.	DE65302
41.	The comparison function used to compare the SSL policy name was incorrect.	DE65318
42.	Added more information to the debug log when an ASSERT occurs on an ndebug image.	DE65338
43.	After performing config apply, GSLB DNS responses returned a remote IP address instead of a local VIP.	DE65365
44.	The MP CPU utilization was high when querying virtual stats.	DE65380
45.	A connection drop occurred because a virtual service was reset due to a virtual index mismatch after applying new configuration changes.	DE65406
46.	SIP UDP service run by AppShape++ failed (it was used for persistency and/or Layer 7 manipulation).	DE65436
47.	After attaching a second hard disk to Alteon VA, the DPDK network driver did not load.	DE65452 DE65459
48.	The Alteon Data interface with port range 40k-45k mistakenly was accessible from outside world.	DE65486

Item	Description	Bug ID
49.	Even though the SP/MP profiling logic was disabled by default, Alteon panics with SP profiling logic being triggered.	DE65492
50.	Whenever multiple requests were sent with a cookie in a single session for multiple services, Alteon did not decrement the current session properly.	DE65505
51.	Alteon displayed the diff and diff flash without any configuration changes.	DE65536
52.	Using RCA, there was an incorrect virt-sever ID display.	DE65567
53.	AppWall crashed when not receiving the i/o time.	DE65571
54.	The SP performed unequal traffic distribution.	DE65606
55.	When burst traffic was sent to Alteon, some p-sessions remained in the zombie/stale state.	DE65664
56.	Added support for the IF IP to connect to the service dashboard.	DE65681
57.	Added a maint debug CLI command to export the virtual stat service table to understand the cause of the virtual stats not working.	DE65706
58.	A new Regex command forbade a hyphen (-) by mistake.	DE65721
59.	When an ARP entry is deleted, sending queued packets to the ARP entry after ARP resolution sometimes leads to an MP freeze and eventually leads to an MP panic.	DE65743
60.	In an RTSP environment, the RTSP service stopped working and all the SYN packets were dropped.	DE65747
61.	When all 24 GBICs were inserted, the Watcher timed out when ports were initiated.	DE65785
62.	When a vADC Layer 2 configuration was applied/pushed to an ADC-VX (with /c/vadc/add or rem), if at the same time a vADC Apply (or config sync) occurred indicated by a flag, a race condition while logging this configuration caused the vADC to freeze while waiting for the flag and was eventually restarted by the Watcher.	DE65832
63.	Performing gtcfg via SCP resulted in a panic.	DE65858
64.	Multi-line notices via ansible did not work.	DE65859
65.	Added the HW platform type MIBs for 6024, 5208, and 8420 to the MIB tree.	DE65866
66.	When vmasport was enabled, the service ceased working.	DE65897
67.	The AppWall service did not restart after being ended by the MP.	DE65918

Item	Description	Bug ID
68.	The /c/port xxx/gig/cur command displayed breakout details, even though breakout was not applicable.	DE65938
69.	When the rlogging TCP health check is running via the MGMT port, Alteon sometimes panics.	DE65955
70.	When BFD and tunneling were enabled, a panic occurred.	DE66002
71.	Using SNMP, OIDs errorCountersSpTable and eventCountersSpTable could cause Alteon to not be accessible via SSH or WBM.	DE66031
72.	With the command logging feature enabled, Apply/Save resulted in a panic.	DE66103
73.	While initiating the SSL client connection for the SSL health check, the vADC MP crashed.	DE66140
74.	Adding and deleting real servers or groups resulted in an AX Out-Of-Sync error.	DE66180

AppWall Bug Fixes

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

Fixed in 33.0.0.0

General Bug Fixes

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

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

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

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

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

AppWall Bug Fixes

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


KNOWN LIMITATIONS

The list of known limitations, available to customers only, is available at the following link:
https://support.radware.com/app/answers/answer_view/a_id/1030724

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*
- *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

© 2024 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners. Printed in the U.S.A.