



AlteonOS

RELEASE NOTES

Version 33.5.2.0
September 30, 2022

TABLE OF CONTENTS

CONTENT	5
RELEASE SUMMARY.....	5
SUPPORTED PLATFORMS AND MODULES	5
UPGRADE PATH	6
Before Upgrade – Important!.....	6
Additional Considerations.....	6
Downgrade	7
WHAT’S NEW IN 33.5.2.0	7
SecurePath Connector	7
GEL Management Administrative Modes.....	8
AppShape++ Commands	9
Latency Control for Integrated WAF.....	9
OCSP Health Check.....	10
Additional SSL Policy Parameters.....	10
Generic HTTP Sideband	10
WHAT’S NEW IN 33.5.1.0	11
Heat Templates for OpenStack Installations.....	11
GEL Entitlement Split Across License Servers	11
6420 DPDK Support.....	12
Selective WAF Content Inspection.....	13
Session Reuse for SSL Health Checks.....	13
BGP AS DOT Notation Support	14
HTTP/3 Gateway Enhancement.....	14
Chinese Crypto Algorithms Enhancement	14
Integrated AppWall	14
WebSocket	14
API Security	15
Advanced Base64 Attack in HTTP Headers	16
WHAT’S NEW IN 33.5.0.0.....	17
vRA/vRO Workflows.....	17
HTTP/3 Gateway	17
Layer 7 Services	17
HTTP/3 Service Advertise Parameter.....	17
Hardware Acceleration.....	18

Chinese Crypto Algorithms (SM2, SM3 and SM4) Support	18
64GB RAM on 5424/5820	19
BGP IPv6 ECMP Traffic Load Balancing	19
ADFS Health Check	19
Ansible Modules	19
GEL Entitlement Migration Workflow	20
Source NAT for Health Checks	20
PMTU Discovery Support.....	20
FIPS Card Support for 7220.....	21
Integrated AppWall	21
WebSocket	21
API Security	22
Advanced Base64 Attack in HTTP Headers	23
Filter Tunnel Command.....	23
WHAT'S CHANGED IN 33.5.2.0	24
SSH Library Upgrade to Support SHA2 MAC Algorithm.....	24
Proxy ARP Entries.....	24
External Health Check.....	24
EAAF for Alteon Feed Eligibility Based on GEL Entitlement	24
FastView GUI Configuration Removal	24
OpenSSL Upgrade	25
AppWall Integrated.....	25
WHAT'S CHANGED IN 33.5.1.0	25
GEL Enhancements	25
GEL Dashboard	25
GEL Allocation Granularity.....	25
Syslog Server for Integrated WAF.....	25
HTTP/HTTPS Health Check.....	26
Number of Alteon DNS Responders	26
Ping6 Response	26
EAAF UI.....	26
QAT Driver/Engine Upgrade	27
OpenSSL Upgrade	27
AppWall Integrated.....	27
WHAT'S CHANGED IN 33.5.0.0	27
Empty Group Association to FQDN Server and Virtual Service	27
HTTP Header Length	27
Treck Version	27

Remove Vulnerable Expat Library.....	28
Include "remote address" at the TACACS request	28
Ignore Non-existing Fields in JSON	28
Event Counter Default Change	28
AppWall Integrated	28
MAINTENANCE FIXES	29
Fixed in 33.5.2.0	29
General Bug Fixes	29
AppWall Bug Fixes	31
Fixed in 33.5.1.0	32
General Bug Fixes	32
AppWall Bug Fixes	34
Fixed in 33.5.0.0	34
General Bug Fixes	34
AppWall Bug Fixes	37
Fixed in 33.0.3.0	37
General Bug Fixes	37
AppWall Bug Fixes	39
Fixed in 33.0.2.50	41
General Bug Fixes	41
AppWall Bug Fixes	42
Fixed in 33.0.2.0	43
General Bug Fixes	43
AppWall Bug Fixes	44
Fixed in 33.0.1.50	45
General Bug Fixes	45
Fixed in 33.0.1.0	47
General Bug Fixes	47
AppWall Bug Fixes	51
Fixed in 33.0.0.0	52
General Bug Fixes	52
AppWall Bug Fixes	57
KNOWN LIMITATIONS	57
RELATED DOCUMENTATION	57

CONTENT

Radware announces the release of AlteonOS version 33.5.2.0. These release notes describe new and changed features introduced in this version on top of version 33.5.1.0.

RELEASE SUMMARY

Release Date: September 30, 2022

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

SUPPORTED PLATFORMS AND MODULES

This version is supported by the following platforms:

- 4208, 4208S
- 5208, 5208S
- 5424S, 5424SL, 5820S, 5820SL
- 6024, 6024S, 6024SL, 6024 FIPS II
- 6420p, 6420, 6420S, 6420SL
- 7612S, 7612SL
- 7220S, 7220SL
- 8420, 8420S, 8420SL
- 8820, 8820S, 8820SL
- 9800, 9800S, 9800SL
- Alteon VA running on VMware ESXi 6.0, 6.5, 6.7, 7.0, 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 33.5.2.0 is supported by APSolute Vision version 4.30 and later.

Integrated AppWall version: 7.6.17. 0

OpenSSL version:

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

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 28.x, 29.x, 30.x, 31.x, 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 33.5.1.0:

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 33.5.1.0 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 33.5.2.0

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

SecurePath Connector

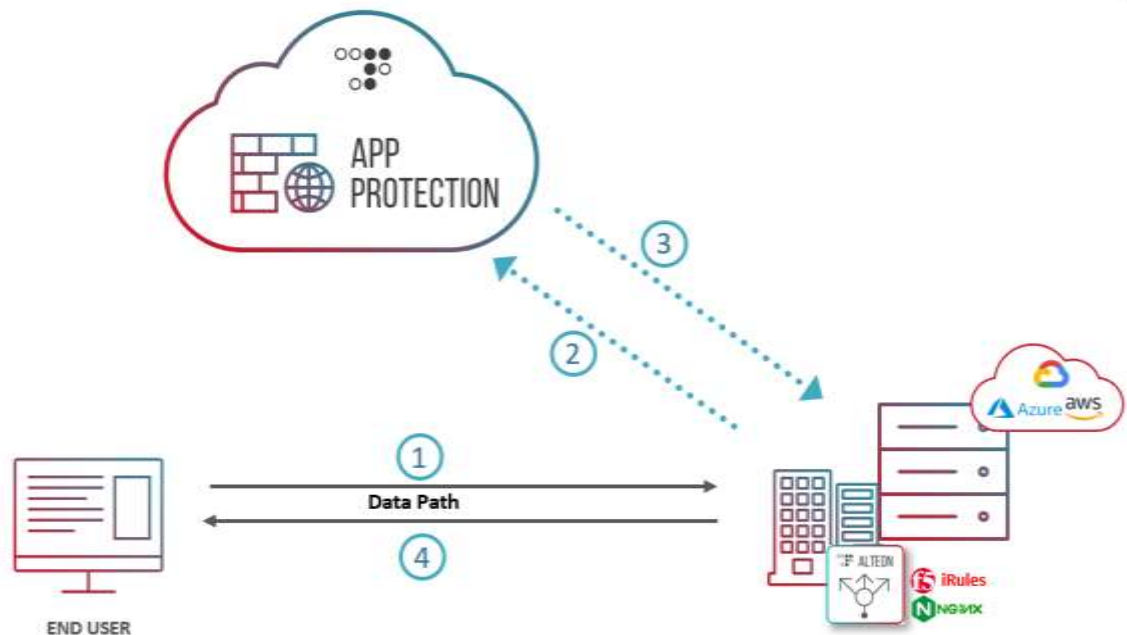
SecurePath integration is an API-based solution for multi-cloud application security. It provides consistent, high-grade, and comprehensive protection for applications hosted across on-premises, private cloud, and public cloud environments, without losing protection quality or operational efficiency.

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,:

6. Alteon sends a copy of the request via the sideband connection to Radware Cloud Security Service endpoint.
7. The Security engine analyzes the data and response to Alteon with the required actions
8. 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 an 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

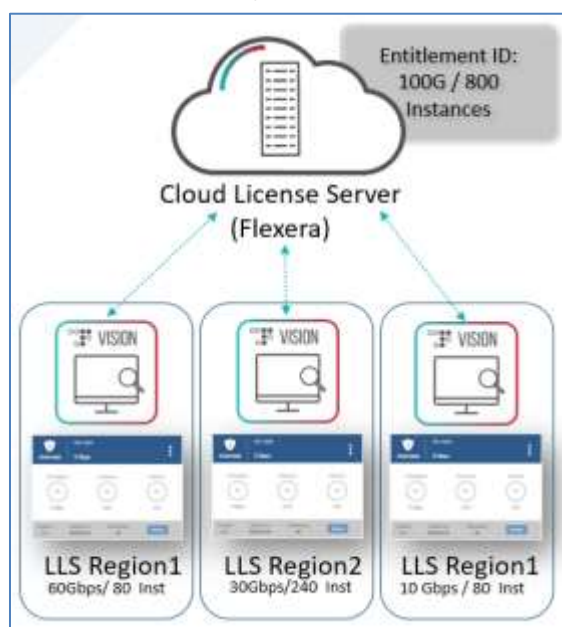
A set of Heat Orchestration Templates (HOTs) is now available for deploying and/or configuring an Alteon device/HA pair from your OpenStack Cloud. The following templates are available:

- 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 split 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 fields for 'Entitlement ID' and 'Activation ID'. Below this is the 'Product Info' section, which includes a table with 'Product' and 'Description' columns. The 'Product' column lists 'Alteon Secure Pro - 1 Gbps Global Elastic License including 8 VAs/vADCs, 1 year subscription Version 2.1, Qty/Copy 1'. The 'Description' column lists 'Alteon Secure- 1 Gbps Global Elastic License - Unlimited VAs/vADCs - 1 year, Price includes support, Operator Tool Box - FastView for Alteon'. The 'Qty' field is highlighted in yellow and shows '100'. Below this, 'Qty remaining' is '100', 'Start date' is 'Feb 10, 2022', and 'Expiration date' is 'Mar 23, 2023'.

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

Activation ID Quantity field on the GEL Dashboard

The screenshot shows the 'Activate Entitlement' dialog box. It has a title bar with a close button. Inside, there is a field for 'Activation ID' with a placeholder 'Paste Activation ID here'. Below this is the 'Activation ID Quantity' field, which 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:

- Virtual service
 - WBM: **Virtual Service > Security tab > Secwa Processing in Flow**
 - CLI: `/cfg/slb/virt <virt id>/service <http | https>/http/aw/awinflow`
- Filter
 - WBM: **Filter > HTTP tab > Secwa Processing in Flow**
 - CLI: `/cfg/slb/filt <filt id>/awinflow`

The content that should bypass WAF processing can be specified via one of the following:

- AppShape++ script attached to the virtual service or filter
- Virtual service Content Rule
 - 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`

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/13/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.

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:

9. 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.) 15

Connections per Source 10

Slowloris

☒ Protection Against "Law 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

Predelined 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.

The screenshot shows the AppWall configuration interface. At the top, there is an 'Action' dropdown menu set to 'Active'. Below it is a 'Base Paths' section with a text input field containing a forward slash '/'. Underneath is an 'Endpoints' section with a search bar and several icons for adding, filtering, and editing. A '+ Quota' button is also present. The main part of the interface is a table with three columns: 'Endpoints (8)', 'Quota', and 'Action'. The table contains two entries. The first entry has the endpoint '/api/v1/create/account', a quota of '1 per minute', and an 'Action' dropdown set to 'Block'. The second entry has the endpoint '/api/v2/create/account', a quota of '300 per minute', and an 'Action' dropdown set to 'Active'. Red boxes highlight the 'v1' and 'v2' in the endpoint paths and the 'Block' and 'Active' in the action dropdowns.

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, SSL 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 33.5.2.0

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

HTTP/HTTPS Health Check

Starting with this version, an IPv4 HTTP/HTTPS health check can be set to terminate the connection using FIN in case of timeout (the default remains RST).

Configuration of this feature is available only via CLI using the `conntout <fin | rst>` command.

Note: Radware recommends closing the connection with RST in case of timeout, for faster response release. Closing with FIN may cause high MP CPU utilization if many real servers are unreachable.

NFR ID: 211020-000175

Number of Alteon DNS Responders

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

NFR ID: 211102-000089

Ping6 Response

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

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

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


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

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

NFR ID: 211102-000064

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 to an FQDN server. With this association, the group name (description) is automatically set on apply (so that the group's configuration will be different than the factory default).

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

NFR ID: 220111-000026, 210302-000006

HTTP Header Length

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

NFR ID: 211209-000097

Treck Version

The Treck version has been updated to 6.0.1.76.

Remove Vulnerable Expat Library

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

Include "remote address" at the TACACS request

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

NFR ID: 210319-000010

Ignore Non-existing Fields in JSON

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

Event Counter Default Change

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

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

AppWall Integrated

- **SafeReply Filter:** The settings of the SafeReply filter have been moved. Previously, the settings were global when the SafeReply filter was activated. In this version, the settings can be specifically set per Application Path.
- **API Security:** When merging a new OpenAPI schema in an existing configuration, the merge policy can be defined. In this version, during the merge process, the value for the Quota is set, by default, to "Keep".
- **Tunnel Parsing Properties:** In the "Request Boundaries" section, AppWall can accept HTTP GET requests with a Body to mitigate attacks, such as HTTP Request Smuggling attacks. In this version, the "Support Framing for Request Message" option has been removed (doing a TCP reset) rather than presenting a Security Page by the "Allow a GET request with body" option.
- **Auto-Discovery and Auto-Policy:** These two features, Auto-Discovery and Auto-Policy, have been coupled. When activating Auto-Policy in an Application Path, Auto-Discovery is automatically activated. When Auto-Policy in the last Application Path is deactivated, Auto-Discovery will also be automatically deactivated. It is still possible, though, to Activate Auto-Discovery alone. This will require manual deactivation.
- **Forensics Security Events:**

- It is now possible to filter security events per key words found in the security event Description field.
- It is now possible to filter WebSocket Security Events.

MAINTENANCE FIXES

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

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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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.	After the primary real server was activated in a group, the session handled by the backup real server was fastaged.	DE75538
38.	An SSH management connectivity issue occasionally caused a reboot.	DE75552
39.	When gathering the device output, memory stats information did not appear in the techdata.	DE75689
40.	The client certificate went through OCSP verification even though it is in OCSP stapling mode.	DE75804 DE75808
41.	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
8.	Geo filter (ZZ) to display the Forensics logs for Private networks did not work.	DE75593
9.	In Forensics, the filter according to the Geo-Location did not work.	DE74346

Fixed in 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
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 and 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

Item	Description	Bug ID
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 platforms 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
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

Item	Description	Bug ID
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

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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
26.	Alteon displayed inaccurate SFP Tx and Rx power values.	DE70788
27.	Could not manual 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
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 some times 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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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



Item	Description	Bug ID
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 loopup, 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 a different times in CLI and WBM.	DE64033
6.	On a 4208 platform, the option to convert to virtual (ADC-VX/ADC) mode displayed the following error message: The operation cannot be performed	DE64092
7.	When configuring an IP service with nonat enabled, a null pointer access caused a panic.	DE64155
8.	The MGMT port status was DOWN but the Link and operational status was UP.	DE64235
9.	In an SLB environment with cookie insert enabled, the server responses to the client undergoing cookie processing had a mismatch of the SRC MAC with an incoming client request.	DE64248
10.	An internal link on Alteon VA caused connections to drop.	DE64257
11.	In an HA environment, when the RADIUS service was enabled with mirroring and associated with an AppShape++ script , RADIUS authentication timed out.	DE64321
12.	Applying part of the nginx when disabling the Web proxy took too much time.	DE64336
13.	When pbind clientip and vmasport were enabled, the persistent session was not permanently deleted.	DE64356
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 some times leads to an MP freeze and eventually leads to an MP panic.	DE65743
60.	In an RTSP environment, the RTSP service stopped working and all the SYN packets were dropped.	DE65747
61.	When all 24 GBICs were inserted, the Watcher timed out when ports were initiated.	DE65785
62.	When a vADC Layer 2 configuration was applied/pushed to an ADC-VX (with /c/vadc/add or rem), if at the same time a vADC Apply (or config sync) occurred indicated by a flag, a race condition while logging this configuration caused the vADC to freeze while waiting for the flag, and was eventually restarted by the Watcher.	DE65832
63.	Performing gtcfg via SCP resulted in a panic.	DE65858
64.	Multi-line notices via ansible did not work.	DE65859
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 applyfilter deletion and network class deletion that was assigned to the PIP that was defined for the real server.	DE61034
12.	Following a set of SNMP operations, on some occasions Alteon panicked from a memory corruption with a boot reason power cycle.	DE61048
13.	In an Alteon HA environment with an SNAT configuration in AppShape++, changing, applying, and synching non-SLB configurations resulted in the following syslog warning: Configuration is not synchronized	DE61099

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

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

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

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

AppWall Bug Fixes

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


KNOWN LIMITATIONS

The list of known limitations, available to customers only, is available at the following link:
https://support.radware.com/app/answers/answer_view/a_id/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*
- *FastView for Alteon NG User Guide*

- 
- [LinkProof for Alteon NG User Guide](#)
 - [LinkProof NG User Guide](#)

North America
Radware Inc.
575 Corporate Drive
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: 972 3 766 8666

© 2022 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.