



***AlteonOS***

# RELEASE NOTES

*Version 33.0.7.0 Rev.1*  
January 01, 2023

## TABLE OF CONTENTS

<b>CONTENT .....</b>	<b>8</b>
<b>RELEASE SUMMARY.....</b>	<b>8</b>
<b>SUPPORTED PLATFORMS AND MODULES .....</b>	<b>8</b>
<b>UPGRADE PATH .....</b>	<b>9</b>
Before Upgrade – Important! .....	9
Additional Considerations .....	9
Downgrade .....	10
<b>WHAT'S NEW IN 33.0.7.0 .....</b>	<b>10</b>
GEL Dashboard Enhancements.....	10
Ansible for Content Rules.....	11
Service and Real Server PPS Statistics .....	11
Keepalive in Proxy Mode .....	11
Security Message for Unsecure Management Protocols .....	11
PIP Source Port Utilization Warning .....	11
AppWall Dynamic Resource Allocation .....	12
<b>WHAT'S NEW IN 33.0.6.0 .....</b>	<b>12</b>
OCSP Health Check .....	12
AppShape++ Commands .....	12
<b>WHAT'S NEW IN 33.0.5.0 .....</b>	<b>13</b>
Session Reuse for SSL Health Checks .....	13
6420 DPDK Support .....	13
BGP AS DOT Notation Support.....	13
Integrated AppWall .....	13
WebSocket.....	13
API Security .....	14
Advanced Base64 Attack in HTTP Headers .....	15
<b>WHAT'S NEW IN 33.0.4.50 .....</b>	<b>16</b>
DPDK Support for 6420.....	16
<b>WHAT'S NEW IN 33.0.4.0 .....</b>	<b>16</b>
ADFS Health Check .....	16
PMTU Support .....	17
GEL Entitlement Migration Workflow .....	17
Integrated AppWall .....	17
WebSocket.....	17

API Security .....	18
Advanced Base64 Attack in HTTP Headers .....	19
<b>WHAT'S NEW IN 33.0.3.0 .....</b>	<b>20</b>
HTTP/3 Gateway .....	20
Bot Manager in Transparent Mode.....	21
BGP ECMP Traffic Load Balancing.....	21
DNS over TLS (DoT) Gateway to DNS over UDP.....	21
vRA/vRO Plug-in.....	22
DNSSEC Support for SOA Record (GSLB) .....	22
SameSite Cookie Attribute .....	22
FIPS Card Support for 7612 .....	22
Client NAT (PIP) Statistics MIB .....	22
PPS Statistics per Service and Filter.....	23
Single IP Mode Configuration in WBM .....	23
APSolite Vision ADC Analytics Support in the WAF Security Events Dashboard .....	23
APSolite Vision Support for WAF Admin and WAF Viewer User Roles for Integrated AppWall .....	24
Integrated AppWall .....	24
WebSocket.....	24
Base64 Heuristic Detection.....	26
Multiple Encoded Attacks.....	26
HTTP Header Inspection with the Database Filter .....	26
Maximum Active Connection Alert .....	27
<b>WHAT'S NEW IN 33.0.2.0 .....</b>	<b>28</b>
Enable VMA Source Port for FTP.....	28
Route to Resolved FQDN IP Address .....	28
Security Hardening .....	29
BIOS and GRUB Password .....	29
Ubuntu18 Support.....	29
Close Connection on Fastage .....	29
Integrated AppWall .....	30
64 bit Support.....	30
Enhanced Security Attacks Protection.....	30
Visibility .....	30
Traffic Event Support for H2 Gateway Traffic .....	30
Alteon PPS Statistics per Device .....	30
Interface MIB Enhancement .....	30
Sideband Policy Statistics .....	31

Ansible Module for "command" Execution.....	31
HTTP/3 Gateway – POC .....	31
<b>WHAT'S NEW IN 33.0.1.50 .....</b>	<b>31</b>
Mid-session DNS Resolving .....	31
DNS over HTTPS (DoH) Gateway to DNS over UDP .....	32
AppShape++ Commands .....	32
<b>WHAT'S NEW IN 33.0.1.0 .....</b>	<b>33</b>
ERT Active Attackers Feed (EAAF).....	33
LinkProof Dashboard in APSolute Vision .....	34
Ansible Modules .....	35
Enable/disable/shutdown for a Specific Real Server Member of a Group.....	35
Configuration BGP peers Radware Internal -- GitHub (Enhancement) .....	35
Public Cloud HA Enhancements .....	36
AWS Route Table Update on Failover.....	36
Session Mirroring for SingleIP Alteon Devices in Azure .....	36
Mellanox ConnectX-4 Support.....	37
Cipher Configuration on Management .....	37
Bot Manager Additions .....	37
Client IP Support in Traffic Event .....	38
DPDK Support for 8420 .....	38
AppWall Features .....	38
<b>WHAT'S NEW IN 33.0.0.0 .....</b>	<b>41</b>
BOT Manager .....	41
Bot Manager per Content Rule Level.....	41
Bot Manager Policy Capabilities .....	41
Bot Manager in Unified Events .....	42
Block Bot Manager Policy Configuration for a Redirect/Discard Service .....	42
Integrated AppWall .....	42
Monitor Mode for SSL Traffic Enhancements .....	42
AppWall on 9800 Standalone .....	43
Google Cloud (GCP) Support.....	43
BGP Enhancements .....	43
IPv6 .....	43
BGP Authentication.....	44
BGP Graceful Restart (RFC 4724) – ADC-VX.....	44
BGP Community Support – ADC-VX .....	44

Multiple RW and RO SNMP Communities .....	45
Static Routes on the Management Interface .....	45
Traffic Distribution for Alteon VA .....	45
Disable ARP for VIPs .....	46
Any MSS Values.....	46
<b>WHAT'S CHANGED IN 33.0.7.0 .....</b>	<b>46</b>
MP CPU Reservation .....	46
Cookie Insert Path .....	46
Server Group and Real Server Description .....	46
AppWall Integrated .....	46
Multiple IPs included in XFF HTTP header .....	46
<b>WHAT'S CHANGED IN 33.0.6.0 .....</b>	<b>47</b>
SSH Library Upgrade to Support SHA2 MAC Algorithm .....	47
Proxy ARP Entries .....	47
EAAF for Alteon Feed Eligibility Based on GEL Entitlement .....	47
OpenSSL Upgrade .....	47
AppWall Integrated .....	47
<b>WHAT'S CHANGED IN 33.0.5.0 .....</b>	<b>48</b>
GEL Allocation Granularity .....	48
Syslog Server for Integrated WAF .....	48
HTTP/HTTPS Health Check .....	48
Number of Alteon DNS Responders.....	48
Ping6 Response .....	48
EAAF UI.....	49
QAT Driver/Engine Upgrade.....	49
OpenSSL Upgrade .....	49
AppWall Integrated .....	49
<b>WHAT'S CHANGED IN 33.0.4.0 .....</b>	<b>49</b>
Empty Group Association to FQDN Server and Virtual Service.....	49
HTTP Header Length .....	50
Treck Version.....	50
Remove Vulnerable Expat Library .....	50
Include "remote address" at the TACACS request.....	50
Ignore Non-existing Fields in JSON .....	50
Event Counter Default Change.....	50
AppWall Integrated .....	50
<b>WHAT'S CHANGED IN 33.0.3.0 .....</b>	<b>51</b>
Maximum Number of Content Rules per Service .....	51

SSL Policy ID length .....	51
Additional Disk for Alteon VA on VMware Ubuntu18.....	51
Remove Repetitive Sideband PIP Configuration Warning .....	52
<b>WHAT'S CHANGED IN 33.0.2.0 .....</b>	<b>52</b>
Additional Disk for Alteon VA on VMware .....	52
OpenSSL Version .....	53
Maximum Number of vADCs for 5208.....	53
AppWall Enhancements .....	53
SSL Private Key Store Encryption using AES .....	53
Application Service Engine Logs Enhancements.....	53
APM Removal from WBM.....	54
<b>WHAT'S CHANGED IN 33.0.1.0 .....</b>	<b>54</b>
Cluster Persistency Data Sync .....	54
SSLi Dynamic Certificate Cache Key .....	54
Default Management Port Access on a Data Port in ADC-VX .....	55
OpenSSL Version .....	55
Server Failure Reason on Block State .....	55
Trace Log Update .....	55
Bot Manager Updates.....	55
Security Notice when Telnet is Enabled .....	55
Warning Messages and Notifications .....	55
Traffic Events Update .....	56
AppWall Features .....	56
<b>WHAT'S CHANGED IN 33.0.0.0 .....</b>	<b>57</b>
DNS Resolver Enhancements.....	57
DNS Cache per IP version.....	57
Response for Unsupported Record Types (first introduced in version 32.6.3.50) .....	57
OpenSSL Version .....	57
Treck Version.....	57
<b>MAINTENANCE FIXES .....</b>	<b>58</b>
Fixed in 33.0.7.0 .....	58
General Bug Fixes .....	58
AppWall Bug Fixes .....	59
Fixed in 33.0.6.50 .....	60
General Bug Fixes .....	60
Fixed in 33.0.6.0 .....	61
General Bug Fixes .....	61

AppWall Bug Fixes .....	63
Fixed in 33.0.5.50 .....	64
General Bug Fixes .....	64
Fixed in 33.0.5.0 .....	65
General Bug Fixes .....	65
AppWall Bug Fixes .....	66
Fixed in 33.0.4.50 .....	67
General Bug Fixes .....	67
Fixed in 33.0.4.0 .....	68
General Bug Fixes .....	68
AppWall Bug Fixes .....	70
Fixed in 33.0.3.50 .....	70
General Bug Fixes .....	70
AppWall Bug Fixes .....	72
Fixed in 33.0.3.0 .....	72
General Bug Fixes .....	72
AppWall Bug Fixes .....	74
Fixed in 33.0.2.50 .....	74
General Bug Fixes .....	74
AppWall Bug Fixes .....	76
Fixed in 33.0.2.0 .....	77
General Bug Fixes .....	77
AppWall Bug Fixes .....	78
Fixed in 33.0.1.50 .....	79
General Bug Fixes .....	79
Fixed in 33.0.1.0 .....	80
General Bug Fixes .....	80
AppWall Bug Fixes .....	86
Fixed in 33.0.0.0 .....	86
General Bug Fixes .....	86
AppWall Bug Fixes .....	91
<b>KNOWN LIMITATIONS .....</b>	<b>92</b>
<b>RELATED DOCUMENTATION .....</b>	<b>92</b>

## CONTENT

Radware announces the release of AlteonOS version 33.0.7.0. These release notes describe new and changed features introduced in this version on top of version 33.0.6.50.

## RELEASE SUMMARY

Release Date: December 29, 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
- 6420, 6420p, 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 33.0.7.0 is supported by APSolute Vision version 4.30 and later, and Cyber Controller 10.0 and later.

**Integrated AppWall version:** 7.6.18.0

### OpenSSL version:

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

## UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 28.x, 29.x, 30.x, 31.x, and 32.x. General upgrade instructions are found in the *Alteon Installation and Maintenance Guide*.

### Before Upgrade – Important!

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

The following table describes the specific upgrade path from each version to 33.0.7.0:

Current Version	Upgrade Path	Notes
28.x	> 29.0.9.0 > 30.5.3.0 > this version	As an alternative, you can upgrade directly to 33.0.7.0 using the recovery process. <b>Note:</b> 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	

### 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, 8420, and 9800, vADCs running 33.0.3.50 version require ADC-VX running 33.0.0.0 and later.

## Downgrade

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

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

## WHAT'S NEW IN 33.0.7.0

### GEL Dashboard Enhancements

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

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

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

The screenshot displays the GEL Dashboard interface. On the left, a card for 'QA-Aniruddha' shows a throughput of 33.3% (2 Gbps) and a capacity of 1/∞. A dropdown menu is open, showing 'Remove Entitlement' and 'Update Capacity'. On the right, the 'Update Entitlement Capacity' modal is shown, containing the following fields:

- Entitlement ID: QA-Aniruddha
- Activation ID: 958a-d862-dbf3-a322-ab97-2705
- Current Entitlement Capacity: 6 Gbps
- Current Capacity Allocated: 2 Gbps
- Required Capacity to Activate: \* (input field with a dropdown arrow and an information icon)

At the bottom of the modal are 'Cancel' and 'Update' buttons. Below the modal, a table shows entitlement information:

Entitlement Info	Expires on	Remaining
	2023.10.31	328 Days

## Ansible for Content Rules

New Ansible modules were added for:

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

## Service and Real Server PPS Statistics

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

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

## Keepalive in Proxy Mode

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

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

**NFR ID:** 220624-000086

## Security Message for Unsecure Management Protocols

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

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

**NFR ID:** 220415-000006

## PIP Source Port Utilization Warning

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

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

The feature is disabled by default.

Alert example:

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

**NFR ID:** 211102-000066

## AppWall Dynamic Resource Allocation

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

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

## WHAT'S NEW IN 33.0.6.0

### OCSP Health Check

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

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

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

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

### 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.

## WHAT'S NEW IN 33.0.5.0

### Session Reuse for SSL Health Checks

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

### 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.

### BGP AS DOT Notation Support

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

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

**NFR ID:** 211205-000073

### 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.

The screenshot shows the 'WebSocket settings' configuration page. Key settings include: 'WebSocket Inspection' checked, 'Allow Idle Session Timeout (Min.)' at 16, 'Connections per Source' at 10, 'Slowloris' protection checked with a 60-second gap and 10 KB minimal data, 'Maximum Frame Size (KB)' at 20, 'WebSocket Extension' set to 'Remove Extension', 'Client Payload Type' and 'Server Payload Type' both set to 'JSON', 'Predefined Policies' set to 'Default', and 'Vulnerabilities' and 'Database' both set to 'Active' mode.

## 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 33.0.4.50

This section describes the new features and components introduced in this version on top of Alteon version 33.0.4.0.

### DPDK Support for 6420

Starting with this version, the Alteon 6420 platform uses the DPDK infrastructure. This allows for integration of more advanced capabilities. For example, it supports new BGP library (FRR) and it allows using Alteon 6420 with an external HSM.

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

#### Performance Impact:

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

## WHAT'S NEW IN 33.0.4.0

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

### 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:

1. Before being able to use external health check scripts, you must enable this functionality (`/maint/debug/extscrhcd ena`) and **reboot the device**.
2. 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**)
3. Creating a health check of type ADFS. This involves associating a script from the External HC Scripts Health Check repository.

**NFR ID:** 201129-000071

## PMTU 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

## 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**).

## 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.

The screenshot shows the 'WebSocket settings' tab in a configuration interface. The settings include:

- WebSocket Inspection:** Checked.
- Allow Idle Session Timeout (Min.):** 16.
- Connections per Source:** 10.
- Slowloris:**
  - Protection Against "Low and Slow" Attacks:** Checked.
  - 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:** Checked.
- Predefined Policies:** Default.
- Mode:**
  - Vulnerabilities:** Active.
  - Database:** Active.

A 'Set Policy' button is located at the bottom right of the settings area.

## 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 33.0.3.0

This section describes the new features and components introduced in this version on top of Alteon version 33.0.2.0.

### HTTP/3 Gateway

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

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

Alteon supports the HTTP/3 to HTTP/1.1 gateway, which can allow Web sites to enjoy the advantages of HTTP/3 transport over the Internet, without any modification to the Web site.

#### Notes:

- The HTTP/3 gateway is supported on virtual services only.
- Content-aware server selection and content modification, including AppShape++, as well as content inspection (WAF, Bot Manager) are not supported.
- Client authentication with QUIC is not supported.
- The server certificate must be signed by a trusted certification authority for the HTTP/3 service to work..
- The Chrome browser does not access the service via HTTP/3 if the responses from the server has the Cache-Control header set to **Private**. The value of the cache control can be changed on the Web site or by Alteon via HTTP Content Modification or an AppShape++ script.

To enable HTTP/3 access for an application on Alteon, the following configuration is required:

1. Configure a regular HTTPS service for that application (which can also support HTTP/2 traffic).

To advertise to the client that HTTP/3 is supported, in responses insert the Alt-Svc (alternate service) header mentioning support of HTTP/3 and the port on which it is available. For example: `Alt-Svc: h3=":50781"`

2. Configure another HTTPS service on the same virtual server for the service port mentioned in Alt-Svc header, and set Protocol to UDP.

*An HTTP/3 policy and a QUIC policy must be defined and attached to this service*

## Bot Manager in Transparent Mode

Bot Manager integration with Alteon has been available starting with version 32.6.3.0 to protect virtual services. Starting with this version, Bot Manager protection is also available in transparent mode using filters. This lets you add the Bot Manager solution as part of Inbound SSL inspection as well as other transparent deployments.

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

**NFR ID:** 210706-000031

## BGP ECMP Traffic Load Balancing

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

You can specify ECMP to work with different peer types (iBGP, eBGP or both), or disable it.

### Notes:

- ECMP for BGP is available only when using the new FRR BGP library (FRR mode)
- This version support ECMP only for IPv4 traffic

**NFR ID:** 210304-000102

## DNS over TLS (DoT) Gateway to DNS over UDP

DNS over TLS (DoT) is a network security protocol for encrypting and wrapping Domain Name System (DNS) queries and answers via the Transport Layer Security (TLS) protocol. The goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data via man-in-the-middle attacks.

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

**Note:** Gateway between DoT and DNS over TCP was previously supported (simple TLS offload).

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

An AppShape++ script is required to handle forwarding the decrypted DNS over TCP query to the sideband DNS over UDP connection and handling sideband connection response. The script can also handle cases where a truncated DNS response is received from the UDP servers (retransmitting the DNS query to the back-end servers over TCP).

**NFR ID:** 201204-000103

## **vRA/vRO Plug-in**

A vRA/vRO plug-in is now available for direct Alteon configuration. The plug-in currently includes one-predefined workflow for configuration of an HTTP or HTTPS virtual service.

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

## **DNSSEC Support for SOA Record (GSLB)**

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

**NFR ID:** 210805-000092

## **SameSite Cookie Attribute**

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

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

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

Alteon now allows the following:

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

## **FIPS Card Support for 7612**

The Nitrox III FIPS SSL card is now supported for the Alteon 7612 platform.

To order Alteon 7612 FIPS, order the D-7216S platform required and the separate FIPS II card part number (factory installed).

## **Client NAT (PIP) Statistics MIB**

Client NAT (PIP) statistics (`/state/slb/pip`) per network class and subnet are now available in the following Alteon PIP MIBs:

- `slbStatPipAddressTable` – Statistics for PIP per Service and per Real Server in address/subnet mode.
- `slbStatPipNwClassTable` – Statistics for PIP per Service and per Real Service in network class mode.
- `slbStatPipTable` – Statistics for PIP per Port/VLAN as well as PIP per Service and per Real Server in address/subnet mode.

**NFR ID:** 201224-000071

## PPS Statistics per Service and Filter

PPS statistics is now available for the following:

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

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

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

**NFR ID:** 200706-000123

## Single IP Mode Configuration in WBM

Alteon VA Single IP configuration is now available via the WBM. It lets you configure:

- Alteon VA with a single IP address data port.
- Alteon VA with a management IP address and a single IP address data port.
- Alteon VA with multiple IP addresses (disable single IP).

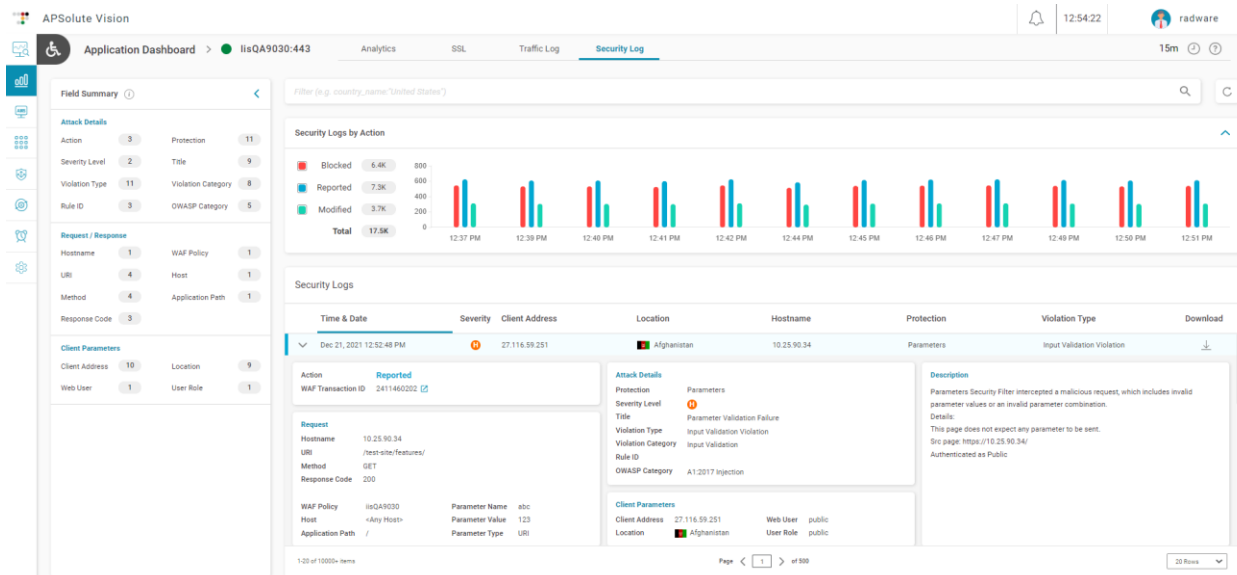
## APSolute Vision ADC Analytics Support in the WAF Security Events Dashboard

The *Security Events* dashboard is now available as part of the application dashboards. This dashboard is available for applications protected by WAF, and enables the user to view protected traffic, identify false positives, and provide detailed explanations of security attacks. With the dashboard, you can correlate between the security event and its traffic event (using the WAF transaction ID) to obtain more information on the transition that initiated the attack.

This dashboard requires one of the following APSolute Vision licenses:

- **vision-GEL-Secure** (available as part of GEL Secure Cloud or Pro)
- **AW analytics** for APSolute Vision plus ADC analytics

**Note:** The Refinement capability is currently not available as part of the security event.



## APolute Vision Support for WAF Admin and WAF Viewer User Roles for Integrated AppWall

The following WAF user roles are now available via APSolute Vision to manage integrated AppWall:

- AppWall Admin
  - Within Alteon, have access only to AppWall Management
  - Within integrated AppWall Management,- have access and manageability capability for all AppWall Management functions
  - Have access to AppWall Analytics
- AppWall Viewer
  - Within Alteon, have access only to AppWall Management
  - Within integrated AppWall Management, have view-only capability for all AppWall Management functions
  - Have access to AppWall Analytics

NFR: 201217-000089

## Integrated AppWall

### WebSocket

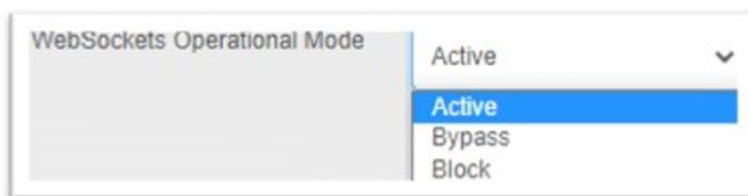
In this version, WebSocket protocol support is added.

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

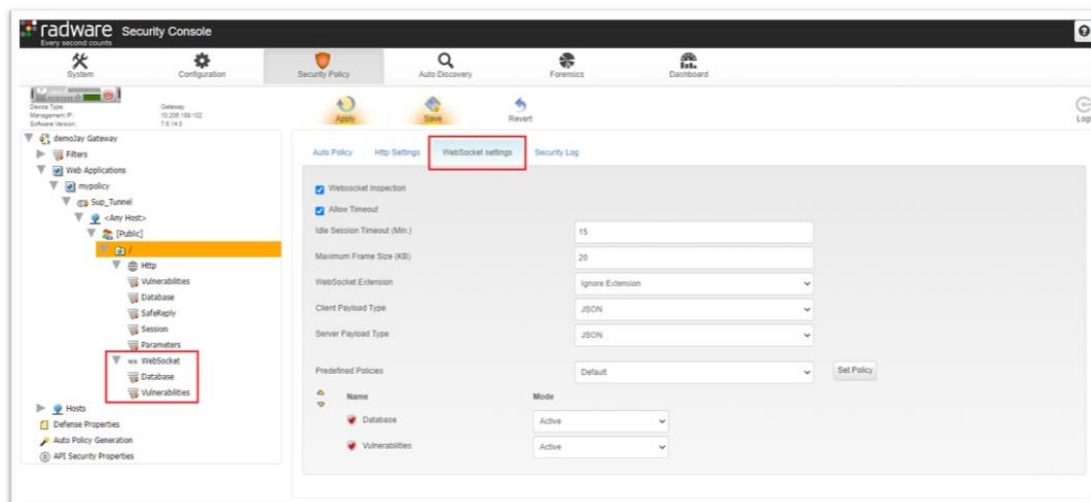
The WebSocket protocol enables interaction between a client application and a web server with lower overhead, facilitating real-time data transfer from and to the server. This is made possible by providing a standardized way for the server to send content to the client without being first requested by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

AppWall WebSocket support:

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



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



### ***Base64 Heuristic Detection***

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

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

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

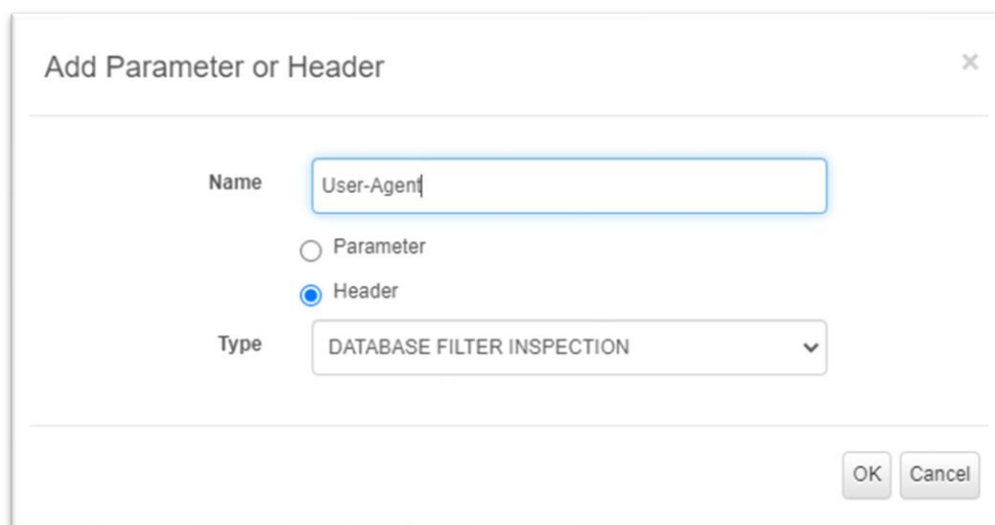
### ***Multiple Encoded Attacks***

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

### ***HTTP Header Inspection with the Database Filter***

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

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



The screenshot shows a dialog box titled "Add Parameter or Header". It contains a text input field for "Name" with the value "User-Agent". Below this are two radio buttons: "Parameter" and "Header", with "Header" selected. Below the radio buttons is a dropdown menu for "Type" with the value "DATABASE FILTER INSPECTION". At the bottom right are "OK" and "Cancel" buttons.

## Maximum Active Connection Alert

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

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


Connections		
Maximum Active Connections	<input type="text" value="1000"/>	Threshold <input type="text" value="85"/> %

Title:	Incoming Sessions Threshold above Limit	Description:
Date:	6-Dec-2021	Threshold of incoming sessions on Tunnel was above the limit.
Time:	11:31:23	TunnelName=80, ID=256, Limit=10, CurCount=4, Threshold=40
Severity Level:	High	<input type="button" value="Request Data"/> <input type="button" value="Response Data"/> <input type="button" value="Details"/>
Event ID:	10	
Server Name:	appwall Gateway	
Generated By:	Sub Systems - Tunnels	
Reported On:	Sub Systems - Tunnels	
Transaction ID:		

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

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

Title:	Incoming Sessions Threshold below Limit	Description:
Date:	6-Dec-2021	Threshold of incoming sessions on Tunnel was below the limit.
Time:	12:49:56	TunnelName=80, ID=256, Limit=10, CurCount=3, Threshold=40
Severity Level:	High	<input type="button" value="Request Data"/> <input type="button" value="Response Data"/> <input type="button" value="Details"/>
Event ID:	13	
Server Name:	appwall Gateway	
Generated By:	Sub Systems - Tunnels	
Reported On:	Sub Systems - Tunnels	
Transaction ID:		



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

## WHAT'S NEW IN 33.0.2.0

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

### Enable VMA Source Port for FTP

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

**NFR ID:** 200925-000050

### Route to Resolved FQDN IP Address

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

For this purpose, the following capabilities were added:

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

**Notes:**

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

NFR ID: 201204-000103

## Security Hardening

### *BIOS and GRUB Password*

GRUB is a boot loader package, used for HW configuration.

it is now possible to set a GRUB password which will be required when accessing the GRUB file.

**Note:** The GRUB password is only applicable for the physical Alteon platforms.

NFR ID: 201021-000037

## Ubuntu18 Support

Alteon now supports Alteon VA installations using Ubuntu18 for the following Cloud environments:

- VMware
- OpenStack
- AWS
- Azure
- GCP

### **Notes:**

- The Ubuntu operating system is part of the virtual appliance image, so to upgrade it on an existing Alteon VA, a new installation is required (just upgrading the Alteon software image will not upgrade the operating system).
- Ubuntu18 support was previously supported for VMware, OpenStack and Azure, but without support for integrated AppWall.

## Close Connection on Fastage

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

### **Important Notes:**

- When Close Connection on Fastage is enabled, Radware highly recommends setting the fastage to 0 (the default value) for the session RST to be sent within 2 seconds.
- Requests that arrive during fastage (after the connection is closed by FIN and until Alteon sends an RST and clears the session entries) causes the session to be refreshed, and as a result Alteon does not send the RST. To avoid the session being refreshed and ensure that the RST is sent within the defined fastage time, session drop (`/cfg/slb/adv/sessdrop`) must be set to enabled

- in force proxy mode, when FIN is received from either side (client or server) RST is immediately sent to both the client and server.

**NFR ID:** 210516-000032

## **Integrated AppWall**

### ***64 bit Support***

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

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

### ***Enhanced Security Attacks Protection***

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

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

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

## **Visibility**

### ***Traffic Event Support for H2 Gateway Traffic***

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

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

### ***Alteon PPS Statistics per Device***

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

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

**NFR ID:** 200706-000123

### ***Interface MIB Enhancement***

In this version, it is now possible to configure an alias and name for the management interface. `ifAlias` parameter is now available as read-only as part of the standard MIB. It supports the alias information of both the management and data interfaces.

**NFR ID:** 190911-000253

## **Sideband Policy Statistics**

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

## **Ansible Module for "command" Execution**

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

This MIB accepts CLI commands as text.

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

**NFR ID:** 210505-000103

## **HTTP/3 Gateway – POC**

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

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

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

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

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


For a POC build, contact ADC PM.

## **WHAT'S NEW IN 33.0.1.50**

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

### **Mid-session DNS Resolving**

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



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

**NFR ID:** 200602-000040

## **DNS over HTTPS (DoH) Gateway to DNS over UDP**

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

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

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

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

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

**NFR ID:** 201204-000103

## **AppShape++ Commands**

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

New commands:

- **DNS::construct\_query** – Generates a DNS query as a binary string.
- **DNS::parse\_message** – Parses the input binary data as a DNS message (query or response) into an internal buffer.
- **DNS::message** – Returns the content of the current DNS message.
- **DNS::release\_message** – Releases the memory allocated for the DNS message before the session ends to reduce the memory used.
- **HTTP::content\_length** – Retrieves the value of the Content-length header (size of the message body in bytes).
- **HTTP::headers** – Removes or replaces the entire HTTP headers section in a message (not valid for HTTP messages generated by a device).
- **Sideband::payload** – Retrieves or manipulates payload collected up to this time.

- `Sideband::send` – Sends the specified data message through the sideband connection.
- `UDP::age` – Closes session after a specified period.

New subcommands for `DNS::edns0`

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

New events

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

## WHAT'S NEW IN 33.0.1.0

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

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

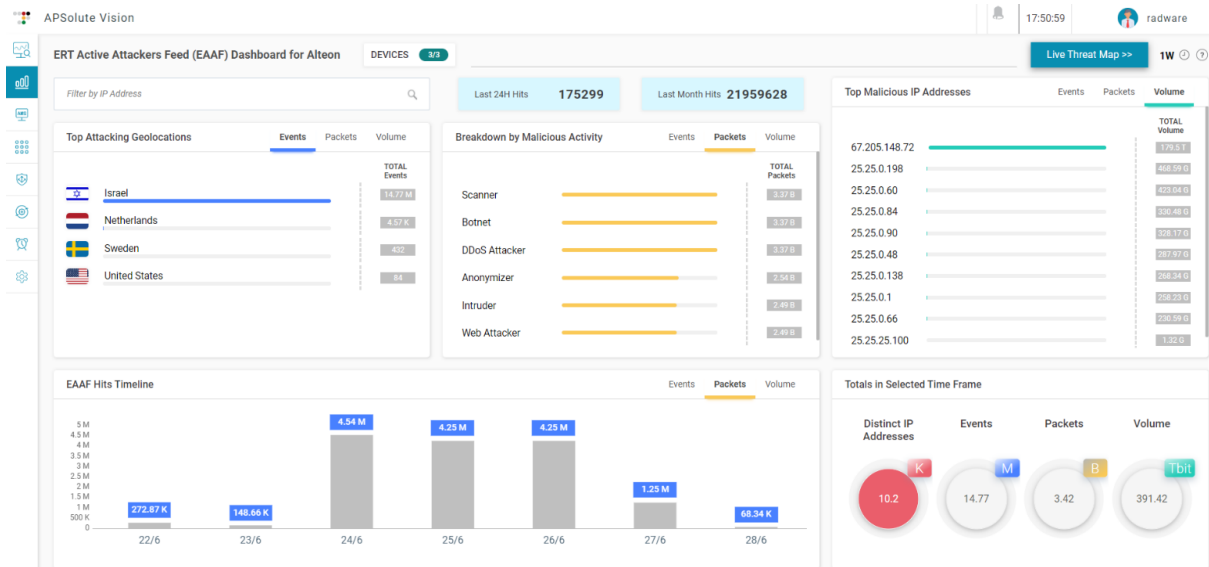
### ERT Active Attackers Feed (EAAF)

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

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

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

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



## LinkProof Dashboard in APSolute Vision

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

The LinkProof analytics in APSolute Vision includes the following:

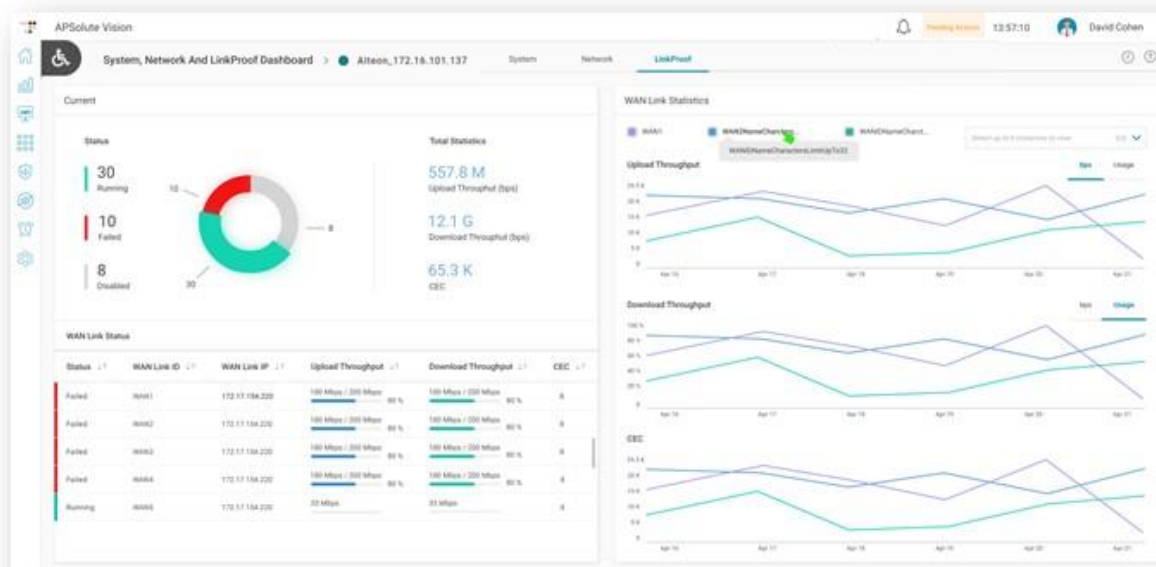
- LinkProof dashboard
  - Current real-time status and performance
  - Performance over time, in a range from 15 minutes to 3 months
- LinkProof reporting template and widgets

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

These metrics are available over JSON using the following link:

[https://<device\\_ip\\_address>/reporter/wanlink](https://<device_ip_address>/reporter/wanlink).

**NFR: 200424-000128**



## Ansible Modules

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

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

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

**Ansible module name:** `alteon_config_group_real_server`

**NFR ID:** 210204-000099

### ***Configuration BGP peers Radware Internal -- GitHub (Enhancement)***

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

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

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

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

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

NFR ID: 210119-000134

## Public Cloud HA Enhancements

### ***AWS Route Table Update on Failover***

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

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

To configure AWS route table update on Alteon failover:

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

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

### ***Session Mirroring for SingleIP Alteon Devices in Azure***

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

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

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

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

## Mellanox ConnectX-4 Support

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

[https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=a00047733enw&doctype=quickspecs&doclang=EN\\_US&searchquery=&cc=za&lc=en#](https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=a00047733enw&doctype=quickspecs&doclang=EN_US&searchquery=&cc=za&lc=en#)

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

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

**NFR ID:** 200722-000045

## Cipher Configuration on Management

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

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

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

**NFR ID:** 200724-000003

## Bot Manager Additions

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

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

## Client IP Support in Traffic Event

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

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

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

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

## DPDK Support for 8420

Starting with this version, the Alteon 8420 platform uses the DPDK infrastructure. This allows for integration of more advanced capabilities. For example, it allows using Alteon 8420 with an external HSM.

**Important!** Upgrade to this version of an Alteon 8420 platform working in ADC-VX mode requires that both the ADC-VX and all its vADCs are upgraded to this same version, as DPDK and non-DPDK-based versions cannot be mixed on the same device.

## AppWall Features

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

API Security – Host Mapping ×

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

**Host Mapping**

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

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

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

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

Global Policy

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

BasePath definition	OVERWRITE
---------------------	-----------

---

Endpoint definition	
New endpoints	ADD
Deprecated endpoints	DELETE
Same endpoints	MERGE

---

Method definition	
New methods	ADD
Deprecated methods	DELETE
Same methods	MERGE

---

Quota definition	KEEP
------------------	------

---

Parameter definition (Path, Query, Header)	
New parameters	ADD
Deprecated parameters	DELETE
Same parameters	OVERWRITE

---

Body definition	
New bodies	ADD
Deprecated bodies	DELETE
Same bodies	OVERWRITE

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

## WHAT'S NEW IN 33.0.0.0

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

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

### BOT Manager

#### ***Bot Manager per Content Rule Level***

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

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

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

For example:

- A single virtual service that manages two (2) subdomains using two (2) content rules:
  - Content Rule 1 – Matches “**mobile.abc.com**” - Bot Manager policy with the mobile Application Type
  - Content Rule 2 – Matches “**web.abc.com**” - Bot Manager policy with the Web Application Type
- A single virtual service that manages three (3) unrelated applications:
  - Content Rule 1 - matches “**abc.com**” – Bot Manager policy with abc.com SID
  - Content Rule 2 - matches “**xyz.com**” – Bot Manager policy with xyz.com SID
  - Content Rule 2 - matches “**123.com**” – No Bot Manager processing
- Bypass Bot Manager protection for specific cases (such as a specific URL, User-Agent, and so on)

#### ***Bot Manager Policy Capabilities***

- **Custom Response** – With this capability, you can define the required response in Active mode when receiving a CAPTCHA and/or block response. The response includes the response code, and optionally the response body and two (2) headers.

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

### ***Bot Manager in Unified Events***

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

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

### ***Block Bot Manager Policy Configuration for a Redirect/Discard Service***

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

## **Integrated AppWall**

### ***Monitor Mode for SSL Traffic Enhancements***

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

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

## AppWall on 9800 Standalone

Integrated AppWall is now also available on Alteon D-9800/D-9800S/D-9800SL platforms running in Standalone mode.

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

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

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

## Google Cloud (GCP) Support

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

## BGP Enhancements

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

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

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

**Note:** Changing the BGP mode requires rebooting the device.

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

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

## IPv6

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

The user can now do the following:

- Define BGPv6 peers and verify their connection state
- Define IPv6 network filters and associate them to the Route Map access list
- Associate IPv6 network classes to the Route Map access list
- Dump the IPv6 prefixes it has learned via BGP

- View BGPv6 routes in the Alteon routing table

**NFR ID:** 191223-000038, 191223-000051

### ***BGP Authentication***

Alteon now supports the configuration of MD5 based authentication for BGP peers, meaning that each segment sent on the TCP connection between the peers is verified (each transmitted message has an MD5 digest that can be checked by receiving peer).

MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made.

To enable MD5 authentication, configure the appropriate password for each peer (`cfg/13/bgp/peer <peer id>/password`).

**NFR ID:** 200505-000068

### ***BGP Graceful Restart (RFC 4724) – ADC-VX***

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

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

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

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

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

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


**NFR ID:** 190911-000276

### ***BGP Community Support – ADC-VX***

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

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

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



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

**NFR ID:** 190911-000426

### **Multiple RW and RO SNMP Communities**

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

**NFR ID:** 200511-000135

### **Static Routes on the Management Interface**

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

**NFR ID:** 200511-000006

### **Traffic Distribution for Alteon VA**

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

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

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

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

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

## Disable ARP for VIPs

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

## Any MSS Values

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

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

## WHAT'S CHANGED IN 33.0.7.0

### MP CPU Reservation

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

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

### Cookie Insert Path

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

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

### Server Group and Real Server Description

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

NFR ID: 220225-000012

### AppWall Integrated

#### ***Multiple IPs included in XFF HTTP header***

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

## WHAT'S CHANGED IN 33.0.6.0

### 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.

### 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.

### 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 33.0.5.0

### GEL Allocation Granularity

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

**Note:** This requires APSolute Vision 5.3 x.

**NFR ID:** 220109-000019

### Syslog Server for Integrated WAF

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

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

#### Notes:

- After 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 **unencoded**.
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 33.0.4.0

### Empty Group Association to FQDN Server and Virtual Service

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

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

**NFR ID:** 220111-000026, 210302-000006

## HTTP Header Length

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

**NFR ID:** 211209-000097

## Treck Version

The Treck version has been updated to 6.0.1.76.

## Remove Vulnerable Expat Library

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

## Include "remote address" at the TACACS request

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

**NFR ID:** 210319-000010

## Ignore Non-existing Fields in JSON

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

## Event Counter Default Change

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

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

Disabling/enabling the event counter is available in vADC, VA, and Standalone.

## AppWall Integrated

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

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

## WHAT’S CHANGED IN 33.0.3.0

### Maximum Number of Content Rules per Service

The number of content rules that can be defined for a single virtual service has been increased from 128 to 1024. The total number of content rules per device is unchanged.

**NFR ID:** 201018-000024

### SSL Policy ID length

The length of the SSL Policy ID has been increased from 32 characters to 128 characters.

### Additional Disk for Alteon VA on VMware Ubuntu18

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

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

In version 33.0.2.0, Alteon support for Alteon VA disk expansion was added for Ubuntu 12-based running on the VMware ESX server.

Now the disk expansion feature is available for Ubuntu 18-based running on the VMware ESX server. This new feature provides an efficient way to increase the primary disk size of VA while avoiding disk space wastage.

#### Notes:

- On an Alteon VA installed using Ubuntu18-based version 33.0.3.0 and later, you can expand the primary disk twice, and if there is a second disk, it can be expanded four (4) times.
- On an Alteon VA installed using a Ubuntu18-based version less than version 33.0.x, the disk expansion is supported using the same mechanism as for Ubuntu12. As a result:
  - You cannot perform both Alteon VA disk expansion and addition of a secondary disk.
  - Alteon VA disk expansion is allowed only once, so Radware recommends increasing the disk size as fully as needed during the Alteon VA disk expansion procedure.
  - Once Alteon VA disk expansion is performed, you cannot upgrade/downgrade to a version where this feature is not supported.

### Remove Repetitive Sideband PIP Configuration Warning

Client NAT (PIP) is required for sideband and remote logging via data port capabilities. The NAT (PIP) address can be configured per port/VLAN, real server or per sideband policy. If no PIP is configured a validation error will be received on apply. When the PIP was configured per port/VLAN, a warning kept appearing on apply asking the user to make sure that PIP per port/VLAN was configured for the sideband or remote logging real server . This repetitive warning was removed.

**NFR:** 211202-000224

## WHAT'S CHANGED IN 33.0.2.0

### Additional Disk for Alteon VA on VMware

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

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

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

#### Notes:

- You cannot perform both VA disk expansion and addition of a secondary disk.
- VA disk expansion is allowed only once, so Radware recommends increasing the disk size fully as needed during the VA disk expansion procedure.
- VA disk expansion is supported only on VAs deployed using OVAs of version 31.0.0.0 and later.

- VA disk expansion is supported starting with Alteon versions 32.4.8.0, 32.6.6.0, and 33.0.2.0 and later.
- Once VA disk expansion is performed, you cannot upgrade/downgrade to a version where this feature is not supported.

## OpenSSL Version

The OpenSSL version has been updated to OpenSSL 1.1.1l.

## Maximum Number of vADCs for 5208

With the addition of new features, the RAM consumption increased over time which has resulted in reduction of the number of vADCs supported by 5208 – up to 8 with default 16 GB memory and up to 22 with 32 GB memory.

In this version, due to memory consumption optimization, the maximum number of vADCs of 24 for 32 GB memory is again supported. For the default 16 GB memory, up to 9 vADCs are supported.

## AppWall Enhancements

1. AppWall management API Security hosts protection has been updated. You can now:
  - a. Edit the Path parameter name
  - b. Add/delete a new Endpoint definition
  - c. Add/delete a new Method
  - d. Other UI improvements
2. Database Security Filter performance has been improved in term of time to inspect the request data

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

## SSL Private Key Store Encryption using AES


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

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

**NFR ID:** 200921-000220

## Application Service Engine Logs Enhancements

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



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

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

## APM Removal from WBM

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

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

## WHAT'S CHANGED IN 33.0.1.0

### Cluster Persistency Data Sync

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

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

### SSLi Dynamic Certificate Cache Key

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

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

#### Notes:

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

**NFR ID:** 201210-000099

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

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

**NFR ID:** 201204-000112

## OpenSSL Version

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

## Server Failure Reason on Block State

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

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

## Trace Log Update

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

## Bot Manager Updates

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

## Security Notice when Telnet is Enabled

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

**NFR ID:** 201231-000094

## Warning Messages and Notifications

- A message is sent to the syslog every 15 minutes when a packet capture is running. This periodic syslog can be disabled using the following command: `/maint/pktcap/pcaplog`

- When switch HA is enabled, Radware highly recommends to sync the PIP configuration. On Apply, a warning message displays when switch HA is enabled if PIP synchronization is disabled.
- The legacy Device Performance Monitoring capability (DPM) is not related to ADC Basic Analytics and it is being retired. As DPM has a performance impact, it should not be enabled if not specifically required.

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

## Traffic Events Update

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

## AppWall Features

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

## WHAT'S CHANGED IN 33.0.0.0

### DNS Resolver Enhancements

#### ***DNS Cache per IP version***

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

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

**NFR ID:** 201123-000091

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

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

**NFR ID:** 200723-000119

### OpenSSL Version

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

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

### Treck Version

The Treck version has been updated to 6.0.1.69.

## MAINTENANCE FIXES

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

### Fixed in 33.0.7.0

#### General Bug Fixes

Item	Description	Bug ID
1.	On an Alteon VA device, in some cases SSH and WBM connections failed due to the non-availability of free virtual memory.	DE76267
2.	The Throughput threshold license caused an error even though the high threshold had not been reached.	DE76312 DE76315
3.	When accessing the tunnel meta header of a frame for non-tunnel traffic with filter reverse session support, the device rebooted.	DE76379 DE76382 DE76385
4.	Bandwidth Management (BWM) did not restrict upload bandwidth.	DE76721
5.	Configuring 3044 real servers caused high MP CPU and LACP problems.	DE76791
6.	The power supply failure logs had the wrong status for the power supply.	DE76836
7.	The device ran out of Heap memory, causing it to reboot.	DE76887
8.	In an SLB environment with dbind forceproxy and dbind ena, the device rebooted unexpectedly.	DE77027
9.	Changing the SIP from network class to subnet/network in a filter was not updated in the configuration.	DE77190
10.	When configuring the action in an HTTP modification rule, the Alteon action was not validated correctly.	DE77279
11.	No data was received from Alteon for LinkProof Analytics	DE77439
12.	The device rebooted because of an issue with nsgroup auto-completion.	DE77458
13.	The device rebooted because of hardware Watchdog issues.	DE77489
14.	The DNS persistence cache cleared on Apply of GSLB changes. An alert was added to display when this occurs.	DE77519
15.	Generating tech data could take a long time.	DE77627
16.	vDirect issued an error for table SpMemUseStatsTableEntry using SNMP.	DE77644

Item	Description	Bug ID
17.	MP CPU utilization was high, causing the device to reboot.	DE77726 DE77729
18.	With a BWM rate limiting contract assigned to a forceproxy service, when AppXcel sent a frame to the client/server, the contract information stored in the frame was overwritten with the default contract, causing a failure with BWM enforcement.	DE77826
19.	After changing the user role from User to Web AppSecurity Viewer without submitting the change, associating a Web application resulted in an error message which was not clear.	DE77902
20.	Importing the configuration resulted in a missing bitmap handling.	DE77916
21.	The device rebooted with the following error: SIGSEGV(11) thread STAT(tid=71)	DE77947
22.	When applying configuration changes unrelated to the SLB module, the nbind session table entry erroneously cleared.	DE77953 DE77954
23.	When performing a simultaneous operation of import and apply config, changes were displaying in diff.	DE77997
24.	Defect with the Connection module handling traceroute packets.	DE78004
25.	When a packet capture running on a data port stopped, the device rebooted.	DE78060
26.	The device rebooted when executing a diff from SNMP.	DE78155
27.	In an outbound LB environment, the source port of the connections was changed, leading to traffic failure.	DE78213
28.	The device rebooted because of the Hardware watchdog	DE78659
29.	A random reboot was analyzed and fixed.	DE78926

### **AppWall Bug Fixes**

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

Item	Description	Bug ID
6.	GEO blocking was conduct to false positive.	DE77880

## Fixed in 33.0.6.50

### General Bug Fixes

Item	Description	Bug ID
1.	A misleading license error message was issued.	DE76145 DE76148
2.	A search operation did not work correctly.	DE76188 DE76191
3.	In WBM, after Submit, SSH keys is incorrectly displayed as Do Not Erase.	DE76221 DE76224
4.	The management port status of eth0 and eth1 displayed incorrectly.	DE76254 DE76257
5.	After upgrade, running the /boot/cur command displays the image download date incorrectly.	DE76395 DE76398
6.	In an Alteon SLB environment, external health checks failed when a tag was enabled on the real server port.	DE76484 DE76487
7.	In WBM, the configured Server Side Idle Timeout values were not displayed.	DE76499 DE76502
8.	Generating applogs resulted in high MP CPU utilization. A new warning message regarding this is now issued when running the /maint/applog/showlog command.	DE76529 DE76532
9.	Traffic was sent to a real server when the real server health check failed due to its related buddy server failing.	DE76547 DE76550
10.	Features that in the background automatically created virtual servers sometimes caused the High Availability configuration to be different between the HA devices.	DE76555 DE76558
11.	Changing a health check for LDAP(S) caused a reboot.	DE76643 DE76646
12.	Configuration sync issued caused the device to reboot.	DE76658 DE76661
13.	IPC module issue caused the device to reboot.	DE76760

Item	Description	Bug ID
		DE76763
14.	Syslog servers and protocol definitions were saved in the vADC configuration, but were not actually used when delegated from the ADC-VX to the vADCs.	DE76966 DE76969
15.	When generating techdata, the techdata creation failed.	DE77065 DE77068

## Fixed in 33.0.6.0

### General Bug Fixes

Item	Description	Bug ID
1.	Using SSH, there was no matching key exchange method found when connecting from Ubuntu 20.	DE70424 DE70427
2.	An Alteon cluster running on Azure had high availability issues.	DE72941
3.	Application delivery features were not available via API for the slbviewer user role.	DE74199
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.	DE74227
5.	An Alteon 5224 platform rebooted because of a power cycle.	DE74353
6.	An Alteon 5224 platform rebooted because of a power cycle.	
7.	The device restarted by a software panic.	DE74397 DE64400
8.	After config sync, the Traffic Event Log policy sent a log via the data interface.	DE74451
9.	There was a Switch HA failover issue.	DE74515
10.	vADC buffer memory related to SSL caused a reboot.	DE74590
11.	An SSH management connectivity issue occasionally caused a reboot.	DE74607 DE74610
12.	The wrong time zone offset was sent to the NTP server.	DE74637
13.	On a vADC, the GET /config/SlbCurCfgEnhVirtServicesTable message was received during config sync and all hash tables were initialized (zeroed), causing a reboot.	DE74689

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.	DE74761
15.	A vADC stopped processing production traffic.	DE74789
16.	The MP CPU utilization was high with DNS packets (dport 53).	DE74810
17.	When configuring network settings, an internal error was issued.	DE74819
18.	On an ADC-VX, an LACP issue was caused by high MP CPU utilization.	DE74845
19.	When the device started after a reboot, it stopped performing ARP base health checks.	DE74867
20.	Alteon Bot Manager used 1.1.1.4 in the Host Header while sending POST request to the endpoint.	DE74919
21.	Alteon VA devices deployed in Hyper-V experienced high CPU usage compared to other hypervisors.	DE74934
22.	Using SNMPv3, the "Unknown user name" is now issued for invalid usernames and invalid passwords.	DE74949
23.	The Ext.HC script did not generate traffic.	DE75008
24.	From WBM, when the SSH key was set to be deleted, after clicking <b>Submit</b> it was immediately deleted before the device was rebooted.	DE75021
25.	The device rebooted because of a software panic.	DE75039
26.	After inserting a 1 G GBIC, message logs did not display.	DE75059
27.	Changing vADC CUs caused syslogs to be removed.	DE75089
28.	AppWall LDAP connection failures were caused due to the multiple creation of MP processes.	DE75156
29.	After rebooting, configuration sync failed and the configuration was stuck in diff with the same error.	DE75228
30.	Alteon did not display the Korean language correctly when using local language-Korean.	DE75255
31.	When trying to use Single IP in Azure, a message was issued that the user should use Multiple IP address mode.	DE75285
32.	After an Apply failure due to an empty passphrase for certificates, after reboot the entire configuration went into diff.	DE75336
33.	There was duplicate entry validation error for two domains where one had a hostname and the other did not have a hostname.	DE75356

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.	DE75403
35.	On an Alteon VA, packets larger than the negotiated MTU size were forwarded.	DE75428
36.	On a vADC, when executing SSL stats commands, the vADC rebooted.	DE75447
37.	The /oper/slb/group command displayed different output when two SSH sessions were opened to a single device.	DE75485
38.	After the primary real server was activated in a group, the session handled by the backup real server was fastaged.	DE75537
39.	An SSH management connectivity issue occasionally caused a reboot.	DE75551
40.	When gathering the device output, memory stats information did not appear in the techdata.	DE75688
41.	The client certificate went through OCSP verification even though it is in OCSP stapling mode.	DE75807
42.	SNMP polling resulted in an incorrect response.	DE75836 DE75839

### ***AppWall Bug Fixes***

Item	Description	Bug ID
7.	Request of /v2/config/aw/SecurityEvents/ returned a false response.	DE75916
8.	The forensics search engine was not accurate.	DE74469
9.	Wildcard hostname (*nma.lt) worked incorrectly and caused false positive.	DE74667
10.	Session filter removed the cookie in passive mode.	DE74748
11.	There was no detailed information about a pattern.	DE74850
12.	Protected applications behind AppWall went down suddenly.	DE75232
13.	Under certain conditions, no explanation is provided in the Forensics API Security event.	DE75513
14.	Geo filter (ZZ) to display the Forensics logs for Private networks did not work.	DE75593
15.	In Forensics, the filter according to the Geo-Location did not work.	DE74346
16.	Failure to update the GEO file.	DE74563

Item	Description	Bug ID
17.	In API Protection, AppWall identifies parameters as "required" even when they are not in the uploaded file.	DE74572
18.	Failure occurs with unexpected headers in the server response.	DE74998
19.	AppWall Management REST for Allow-List misinterpreted a wildcard in the configuration.	DE75050

## Fixed in 33.0.5.50

### General Bug Fixes

Item	Description	Bug ID
1.	On an Ubuntu 18 VA device, when selecting a time zone GMT offset greater than 4 hours, the GEL license activation failed.	DE73646
2.	Application delivery features were not available via API for the slbviewer user role.	DE74202
3.	When an IPv6 virtual server used IPv4 servers for load balancing and if any SLB config apply was performed, the existing sessions were closed.	DE74230
4.	An Alteon 5224 platform rebooted because of a power cycle.	DE74356
5.	After config sync, the Traffic Event Log policy sent a log via the data interface.	DE74448 DE74454
6.	There was a Switch HA failover issue.	DE74518
7.	The wrong time zone offset was sent to the NTP server.	DE74640 DE74981
8.	On a vADC, the GET /config/SlbCurCfgEnhVirtServicesTable message was received during config sync and all hash tables were initialized (zeroed), causing a reboot.	DE74692
9.	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.	DE74764
10.	The maximum supported length of the RADIUS password is 16 characters. Authentication failed If the password was configured with more than 16 characters.	DE74799 DE74802
11.	The MP CPU utilization was high with DNS packets (dport 53).	DE74813
12.	When configuring network settings, an internal error was issued.	DE74822

Item	Description	Bug ID
13.	On an ADC-VX, an LACP issue was caused by high MP CPU utilization.	DE74848
14.	When the device started after a reboot, it stopped performing ARP base health checks.	DE74870
15.	Alteon Bot Manager used 1.1.1.4 in the Host Header while sending POST request to the endpoint.	DE74922
16.	Using SNMPv3, the "Unknown user name" is now issued for invalid usernames and invalid passwords.	DE74952
17.	The Ext.HC script did not generate traffic.	DE75011
18.	The device rebooted because of a software panic.	DE75042
19.	Changing vADC CUs caused syslogs to be removed.	DE75092
20.	AppWall LDAP connection failures were caused due to the multiple creation of MP processes.	DE75159
21.	On an Alteon VA, packets larger than the negotiated MTU size were forwarded.	DE75425

## Fixed in 33.0.5.0

### General Bug Fixes

Item	Description	Bug ID
1.	The IPv6 static route failed if the respected interface was configured with the same Apply.	DE67583
2.	A user was allowed to configure a duplicate Static ARP entry using WBM, but not the CLI.	DE72185
3.	Attempting to delete a server or CA certificate group explicitly or implicitly resulted in an AX internal OOS failure.	DE72201
4.	In the outbound SSL wizard, the validation for version 33.0 resulted in the an error.	DE72419
5.	Bandwidth utilization was displayed incorrectly as Mbps, when it should have been MBps.	DE72625
6.	After upgrade, the configuration was not preserved.	DE72654
7.	On a 6024 platform, increasing the session table by size 200% required a minimum 64 RAM.	DE72810
8.	Using Alteon VA, in some cases when running Ubuntu18 OS and DPDK, allocation of SPs was not based on the vCPU configuration.	DE72843 DE72846

Item	Description	Bug ID
9.	An Alteon NG 5424-S rebooted because of a BSP problem with the monotonic timer.	DE72989
10.	Alteon VA version 33.0.4.0 using Ubuntu12 rebooted on the execution of the Display Certificates Group configuration.	DE73038
11.	There was an error with traps for IPv6-related events.	DE73068
12.	A request to make to increase the height of the "Configuration Sync - Peers" in WBM.	DE73188 DE73191
13.	A DNS responder with delegation for TCP session did not close.	DE73213
14.	In a WANlink environment, traffic was processed by ISP, which was down.	DE73235
15.	Disk space exceeded the high threshold with 80 % usage because of the AppWall cores.	DE73251
16.	A health check timeout failure caused a reboot due to a race condition when freeing the object.	DE73537
17.	Continuous operations on real server groups (additions, deletions, amendments) could lead to an internal OOS state.	DE73662 DE73665
18.	In an Alteon VA environment, occasionally empty syslog messages were generated when the size exceeded 1300 bytes.	DE73746 DE73749
19.	On a vADC, inbound host-based LLB rules were not created using the LinkProof menu due to RBAC issues.	DE73775
20.	SSLi did not forward traffic when creating the FW HA, due to 10G not working correctly on VHT.	DE73817
21.	Trying to add vADC licenses to the ADC-VX when vadcadv had a custom flavor caused an error.	DE74077

### **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 33.0.4.50

### General Bug Fixes

Item	Description	Bug ID
1.	Mirrored session statistics were not updated for Smart NAT Inbound traffic.	DE71995 DE71998
2.	When the real and virtual server statistics were incremented or decremented the logs were not updated.	DE72087 DE72090
3.	Using WBM, expired certificates could not be exported because there was a validation check on the “validation period” (1 to 3650).	DE72168 DE72171
4.	Upgrade failed because of incorrect resource allocation (SP and AW cores).	DE72283 DE72286
5.	When trying to change the Traffic/AppWall capacity units (CUs) for a single vADC, an error occurred.	DE72345 DE72348
6.	In an IPV6 environment, when Static NAT was configured, ICMP traffic failed.	DE72402 DE72405
7.	IPsec sessions abruptly aged out due to an incorrect interpretation of TCP flags.	DE72426 DE72429
8.	An Open SSL vulnerability (CVE 2022-0778) was fixed.	DE72462 DE72465
9.	When updating a configuration with idbynum enabled, an error occurred.	DE72513
10.	An HA failover caused SIP packets to be lost.	DE72526 DE72529 DE72532
11.	When there was an overflow of the Current Sessions value, unexpected statistics of Available Sessions and DNS answer resulted .	DE72559 DE72562
12.	When there was a TCB block leak, DSSP health checks failed.	DE72726 DE72729
13.	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.	DE72745 DE72748
14.	The Ansible module description of vip_health_check_mode was incorrect.	DE72820 DE72823

Item	Description	Bug ID
15.	Using APSolute Vision the Alteon EAAF data base of was not updated.	DE72827 DE72830
16.	VRRP did not sending advertisements because the VR state was incorrected checked.	DE72842
17.	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.	DE72862 DE72865
18.	After a reboot, the "Service Always Up" configuration for AppShape++ was not preserved.	DE72955 DE72958 DE72961
19.	Cookie-based real server selection caused a reboot. Defensive code was added to address the issue.	DE73090 DE73093
20.	On a version 30.5.22.0 vADC, FQDN resolution update failed.	DE73307 DE73310
21.	On an Alteon VA, intermediate certificates were not fetched.	DE72570 DE73345

## Fixed in 33.0.4.0

### General Bug Fixes

Item	Description	Bug ID
1.	When an AppShape++ script was applied with cmd logging enabled, Alteon rebooted.	DE71526 DE71529
2.	The special Regex character '\ ' should be added.	DE69958
3.	With IDS chain configured, ICMP responses from the server were not forwarded to the client.	DE70047
4.	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.	DE70164
5.	A mechanism was added that prevents false PS (power supply) status indications when there is a dual PS configuration.	DE70369
6.	The MP CPU utilization was high when applying the configuration, causing a network interrupt.	DE70614 DE70617

Item	Description	Bug ID
7.	A mixed type SNS request failed (dnsresponder VIP IPv4 and query type IPv6, and vice versa).	DE70704
8.	An unexpected VRRP failback when preemption is disabled.	DE70748
9.	Alteon displayed inaccurate SFP Tx and Rx power values.	DE70787
10.	The max_cipher_list_length was increased from 16000 to 20000.	DE70968
11.	The "Threshold of incoming sessions" event was generated when the total active connections was much lower than the maximum value.	DE71108
12.	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.	DE71268
13.	After resetting a non-debug Alteon VA platform, GEL licenses some times were lost when they passed non-GEL applicable validations.	DE71295
14.	Fixed the License Manager connection failure algorithm.	DE71354
15.	The LINK LED remained ON even when the optical cable was pulled off or the ACT LED was not working.	DE71474
16.	The file descriptor was allocated and not released during execution of SP/MP profiling./maint/debug/cpuProfiling/	DE71503
17.	A MAC flap occurred because of VRRP advertisements sent by the backup Alteon device.	DE71523
18.	The GEL license logs were generated every 5 minutes, causing memory leaks.	DE71583
19.	Support of stapling and client certificate verification added.	DE71595
20.	Alteon could be down when a specific traffic pattern request interacted with the redirect service using dynamic tokens.	DE71620
21.	On a vADC device, the MP CPU reached 100%.	DE71657
22.	When a DPDK image reset, an unexpected DNS server IP address was added by BSP.	DE71757
23.	After the AppWall health check failed, the MP restarted AppWall every 15 seconds .	DE71821
24.	The remote real server DSSP health check was reported as UP even though the related virtual server had the status of "NO SERVICES UP", due to a WANlink real server health check failure.	DE71900
25.	Could not allocate memory to run the diff command.	DE71911

## ***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 33.0.3.50**

### ***General Bug Fixes***

Item	Description	Bug ID
1.	FQDN real server IP addresses incorrectly ended with a period (".").	DE70254 DE70257
2.	Rebooting an ADC-VX caused vADCs to be stuck in the initialization stage.	DE70264 DE70267
3.	The ICMPv4 real server health check failed while a CLI ping worked correctly. A v4 debug command was added.	DE70300 DE70306
4.	A user was locked out after making a password change.	DE70325 DE70328
5.	After booting Alteon VA with version 33.0.2.50, the initial configuration was not applied.	DE70395 DE70398 DE70401
6.	When copying the x-forwarded-for header, an overflow occurred.	DE70439 DE70442
7.	The TLS 1.3 protocol did not display in the Backend SSL policy.	DE70446 DE70449
8.	The XFF code in the HTTP/2 proxy used the VIP instead of the Client IP address.	FE70461 DE70464

Item	Description	Bug ID
9.	The AppWall check did not recognize that AppWall was frozen and did not restart AppWall.	DE70470 DE70473
10.	Configuration sync failed due to a long certificate group ID.	DE70488 DE70491
11.	When LACP was disabled on ports, the port mask was not updated correctly on both the MP and SP. This wrong port mask in the SP impacted packet forwarding.	FE70515 DE70518
12.	A panic occurred during a packet capture.	DE70544 DE70547
13.	The HTTP/2 health check did not contain the ALPN protocol in the SSL handshake.	DE70593 DE70596
14.	After an unexpected reboot of Alteon VA on ESXi 7.0, could not save changes after Apply, and received error messages.	DE70597 DE70600 DE70603
15.	After upgrade, empty groups with no real server added to them could shift the group index map.	DE70633 DE70636
16.	The ARP table information was not the same between the CLI and WBM.	DE70690 DE70693
17.	When preemption was disabled, an unexpected VRRP failback occurred.	DE70751
18.	A panic occurred due to memory corruption.	DE70774 DE70777
19.	Could not manual delete a session table entry for VPN traffic.	DE70874 DE70807
20.	Uppercase characters were, incorrectly, added to HTTP headers for HTTP/2 proxy, which generated the following error: <code>Upper case characters in header name</code>	DE70813 DE70816
21.	An SLB apply took longer to execute when it was run as SLB config apply.	DE71000 DE71003
22.	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.	DE71072 DE71075
23.	When running dbind disable service, a panic occurred when Alteon received the RST packet from the server.	DE71115 DE71118

Item	Description	Bug ID
24.	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.	DE71135 DE71138
25.	Enabling IPv6 on a virtual server caused a panic.	DE71150 DE71153
26.	Port errors increased in version 32.6.6.50 as compared to version 32.4.6.0 with the same physical cables and topology.	DE72571 DE72574 DE72575 DE72577

### ***AppWall Bug Fixes***

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

### **Fixed in 33.0.3.0**

### ***General Bug Fixes***

Item	Description	Bug ID
1.	Wrong management of TSO buffers and logs flood from the AE module caused a panic.	DE66434
2.	Removed the unnecessary syslog message that appeared in vADCs on each Apply.	DE68578
3.	On an Alteon-VA platform with BWM configured, when switching from DPDK to TUNTAP, in some instances a software panic occurred.	DE68862
4.	Alteon 6420 running on version 32.4.6.50 rebooted due to a software panic	DE68957
5.	Under a heavy load due to BGP traffic, BGP peer sessions were flapping with holdtimer expiry notifications. This has been addressed with a config option and recommended values of keepalive/holdtime.	DE69010
6.	A MAC flap occurred because of HA advertisements sent by the backup Alteon device.	DE69142

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
3.	Wrong IP blocked with Source Blocking.	DE68383
4.	Wrong host displayed in syslog security event.	DE68396
5.	Wrong hostname displayed in the Forensics security events when blocked by the Application Security policy.	DE68487
6.	In specific scenarios, AppWall restarted when the Host protector was in Inherit mode.	DE70250

## Fixed in 33.0.2.0

### General Bug Fixes

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

Item	Description	Bug ID
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
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
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

Item	Description	Bug ID
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

Item	Description	Bug ID
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). <b>Fix:</b> The MP OpenSSL version has been upgraded to 1.1.1k to fix this.	DE64380
15.	Added a REGEX to accept the dot (.), slash (/), and backslash (\) characters.	DE64459 DE64466
16.	Config sync transmit was aborted between two devices when the sync request was received from a third device.	DE64488

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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



Item	Description	Bug ID
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

Item	Description	Bug ID
72.	When HA mode was set to VRRP, VRs with some specific VRIDs were active on the backup vADC because some of the VRID bits were incorrectly used in the HAID calculation, causing the advertisements to be dropped due to a bad HAID.	DE63910 DE64075
73.	On a 9800 platform with QAT, SPTHREADS caused a panic.	DE63923
74.	In some edge cases, AppWall did not come up because of an invalid variable that was not initialized. The fix was to initialize the variable.	DE63980
75.	On the 4208 platform, the option to convert to virtual mode (ADC-VX) was mistakenly available.	DE64100
76.	After Alteon received a packet and tried to open a session entry, an incorrect initialization of a pointer resulted in a NULL access and Alteon panicked.	DE64190
77.	Alteon VA did not initiate a BGP connection to a peer.	DE64238

### ***AppWall Bug Fixes***

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

## KNOWN LIMITATIONS

The list of known limitations, available to customers only, is available at the following link:  
[https://support.radware.com/app/answers/answer\\_view/a\\_id/1027843](https://support.radware.com/app/answers/answer_view/a_id/1027843)

## RELATED DOCUMENTATION

The following documentation is related to this version:

- *Alteon Installation and Maintenance Guide*
- *Alteon VA Installation and Maintenance Guide*
- *Alteon Getting Started Guide*
- *Alteon Web Based Management Application Guide*
- *Alteon Command Line Interface Application Guide*
- *Alteon Command Reference*
- *Alteon REST API User Guide*
- *Alteon AppShape++ SDK Guide*
- *AppWall for Alteon NG User Guide*
- *FastView for Alteon NG User Guide*
- *LinkProof for Alteon NG User Guide*
- *LinkProof NG User Guide*

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

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

© 2023 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.