AlteonOS

RELEASE NOTES

Version 32.2.0.0
January 17, 2019

TABLE OF CONTENTS

CONTENT

Radware announces the release of AlteonOS version 32.2.0.0. These release notes describe new and changed features introduced in this version on top of version 32.1.1.0.

RELEASE SUMMARY

Release Date: December 31st, 2018

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

SUPPORTED PLATFORMS AND MODULES

This version is supported by the following platforms:

- 4208, 4208S
- 5224, 5224XL
- 5208, 5208 XL/Extreme, 5208S
- 6024, 6024 XL/Extreme, 6024S, 6024SL, 6024 FIPS II
- 6420, 6420 XL/Extreme, 6420S, 6420SL
- 6420p, 6420p XL/Extreme
- 7612S, 7612SL
- 7220S, 7220SL
- 8420, 8420 XL/Extreme, 8420S, 8420SL
- 8820, 8820 XL/Extreme, 8820S , 8820SL
- 9800, 9800S, 9800SL
- Alteon VA running on VMware ESX 6.0, 6.5 (*new*), KVM, Hyper-V and OpenXen
- Alteon VA on AWS
- Alteon VA on Azure
- Alteon VA on Nutanix
- Alteon VA on Oracle Cloud

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

Alteon 32.2.0.0 is supported by APSolute Vision version 4.10 and later.

OpenSSL version:

- XL/Extreme models: 1.0.2p
- S/SL models, standard models and VA: 1.1.1 (official OpenSSL release for TLS v1.3)

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS version 32.1.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.

- .

Downgrade

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

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

WHAT'S NEW IN 32.2.0.0

This section describes the new features and components introduced in this version on top of Alteon version 32.1.1.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.2.0.0.

Application Dashboard and Reporting

The Application Dashboard and Reporting screens are available starting with this version, using APSolute Vision 4.10 and later.

These screens are a centralized set of dashboards that graphically display the health and performance of your applications.

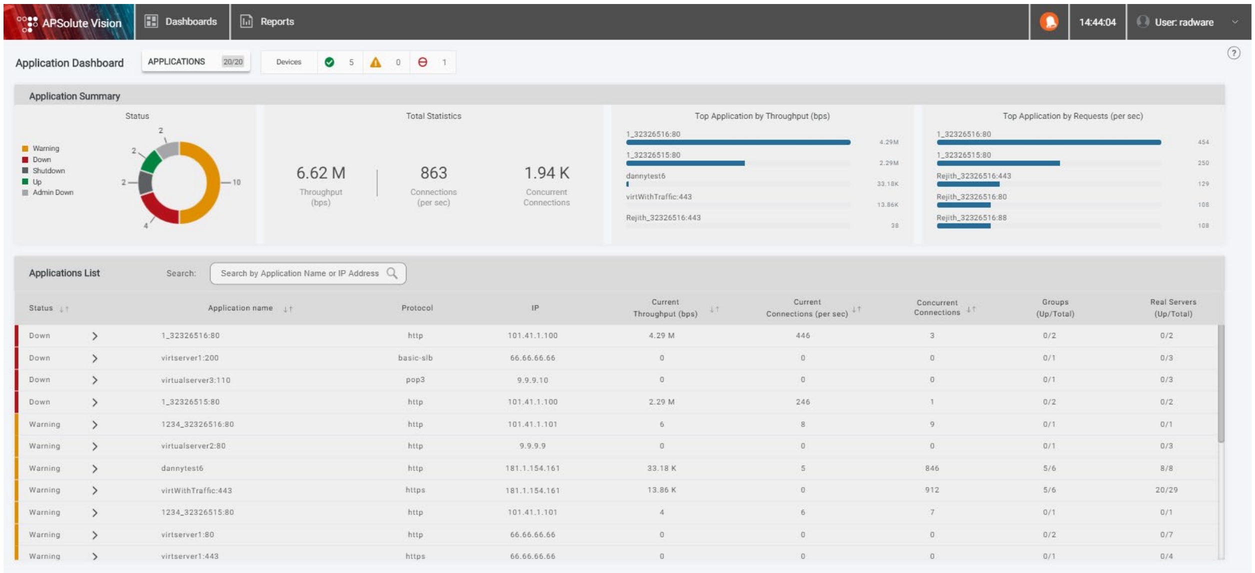
The Application Dashboard provides insights into the application health and performance data, letting you to proactively plan capacity, and to troubleshoot and detect anomalies.

The Reporting capability lets you define, generate, schedule, and send reports, either manually or automatically in PDF, HTML, or CSV format.

The Application Dashboard and Reports provide real-time as well as historical data (up to three months).

Application Dashboard Main Screen

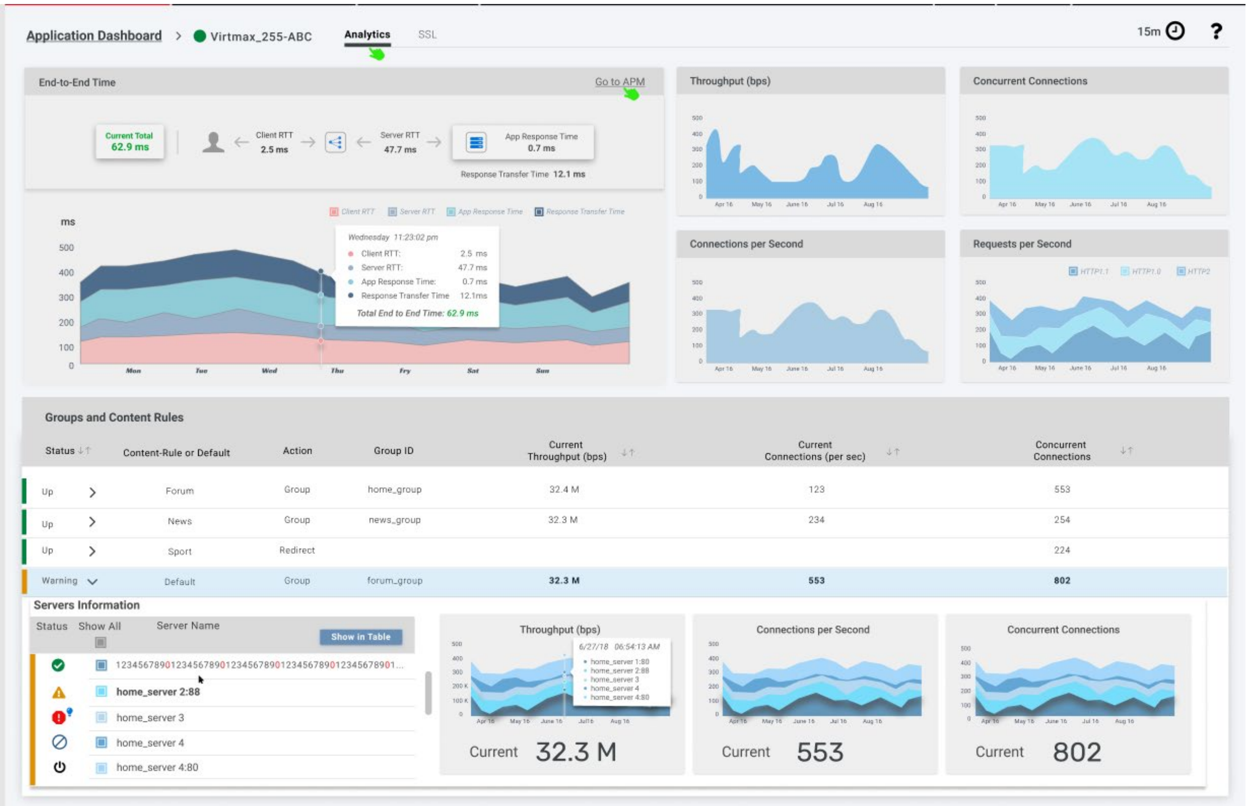
The Application Dashboard main screen displays a summary of all the applications on your managed Alteon devices, from where you can identify at a glance unhealthy applications, the top applications by throughput/requests per second, and some other key information per application.



Status	Application name	Protocol	IP	Current Throughput (bps)	Current Connections (per sec)	Concurrent Connections	Groups (Up/Total)	Real Servers (Up/Total)
Down	1_32326516:80	http	101.41.1.100	4.29 M	446	3	0/2	0/2
Down	virtserver1:200	basic-slb	66.66.66.66	0	0	0	0/1	0/3
Down	virtualserver3:110	pop3	9.9.9.10	0	0	0	0/1	0/3
Down	1_32326515:80	http	101.41.1.100	2.29 M	246	1	0/2	0/2
Warning	1234_32326516:80	http	101.41.1.101	6	8	9	0/1	0/1
Warning	virtualserver2:80	http	9.9.9.9	0	0	0	0/1	0/3
Warning	dannytest6	http	181.1.154.161	33.18 K	5	846	5/6	8/8
Warning	virtWithTraffic:443	https	181.1.154.161	13.86 K	0	912	5/6	20/29
Warning	1234_32326515:80	http	101.41.1.101	4	6	7	0/1	0/1
Warning	virtserver1:80	http	66.66.66.66	0	0	0	0/2	0/7
Warning	virtserver1:443	https	66.66.66.66	0	0	0	0/1	0/4

Per Application – Analytics

Clicking on an individual application opens a more detailed view on the application and its groups and servers, helping you troubleshoot any health and performance issues.



Groups and Content Rules

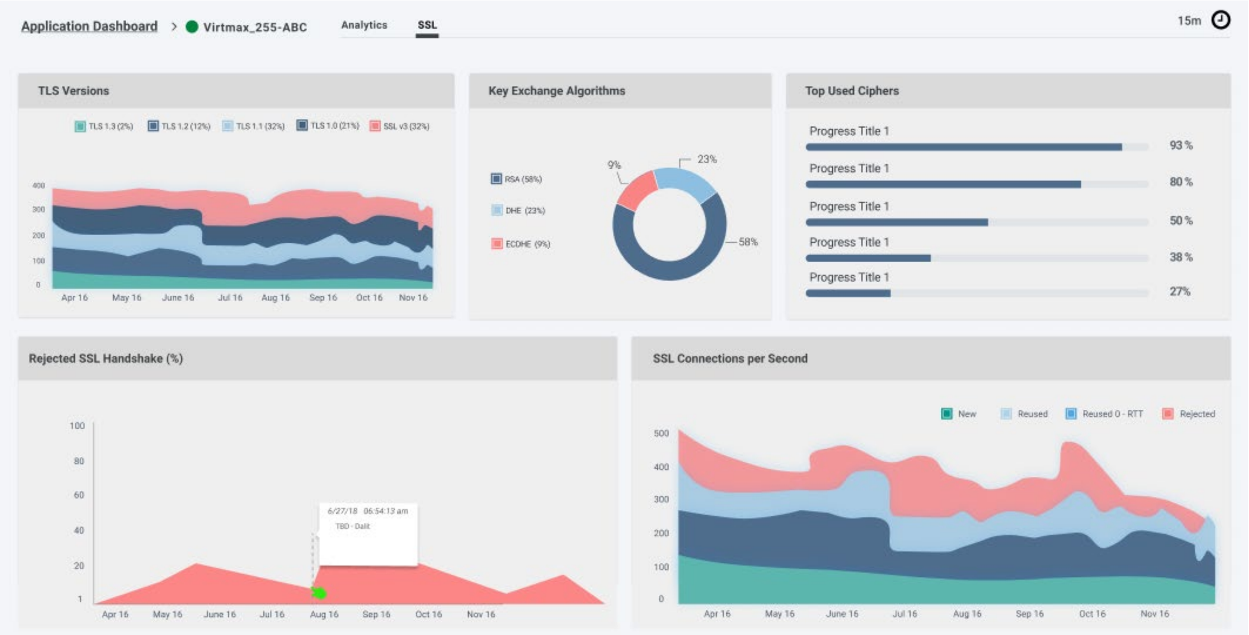
Status ↓↑		Content-Rule or Default	Action	Group ID	Current Throughput (bps) ↓↑	Current Connections (per sec) ↓↑	Concurrent Connections ↓↑
Up	>	Forum	Group	home_group	32.4 M	123	553
Up	>	News	Group	news_group	32.3 M	234	254
Up	>	Sport	Redirect				224
Warning	⌄	Default	Group	forum_group	**32.3 M**	**553**	**802**

Servers Information

Status	Show All □	Server Name
✓	■	123456789012345678901234567890123456789012345678901...
⚠	■	**home_server 2:88**
!	■	home_server 3
⊘	■	home_server 4
⏻	■	home_server 4:80

Per Application – SSL

Clicking on the *SSL* tab opens the client-side SSL information of the application:



Note: The Application Dashboard information is based on counter-based information retrieved from Alteon once a minute in a JSON format. This JSON can be also used for integration with external SIEMs (such as Splunk and ELK).

The URL for the JSON request is: https://<device IP>/reporter/virtualServer

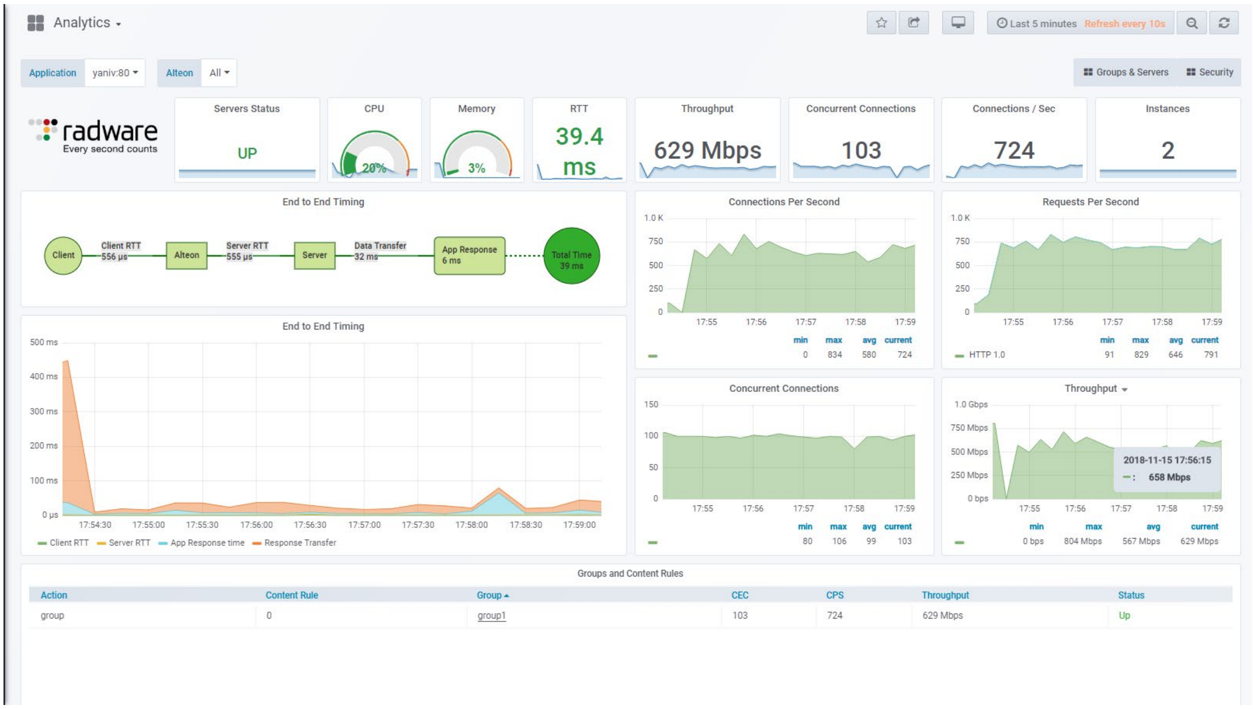
Refer to the *Reporting* section in the *WBM Alteon Application Guide* for detailed information on the JSON structure and data.

Alteon Cluster on Azure

This version introduces Alteon VA application clusters on Azure.

Using the solution template that is available in the Azure marketplace, you can configure a cluster of Alteon VAs that process your application's traffic. As the traffic load increases, additional Alteon VAs members are added to the cluster, and when the load goes down, unnecessary members are removed. The cluster has an IP address through which you can change the configuration of the Alteon VAs cluster members, while a serverless Azure function running in the background synchronizes the configuration changes among the cluster members.

The Alteon VA cluster on Azure is deployed with advanced analytics capabilities, providing an easy view to monitor an application's status and detect anomalies. The following are examples of the Application Analytics dashboard and SSL performance activity dashboard:



Connections Per Second

	min	max	avg	current
	0	834	580	724

Requests Per Second

	min	max	avg	current
HTTP 1.0	91	829	646	791

Concurrent Connections

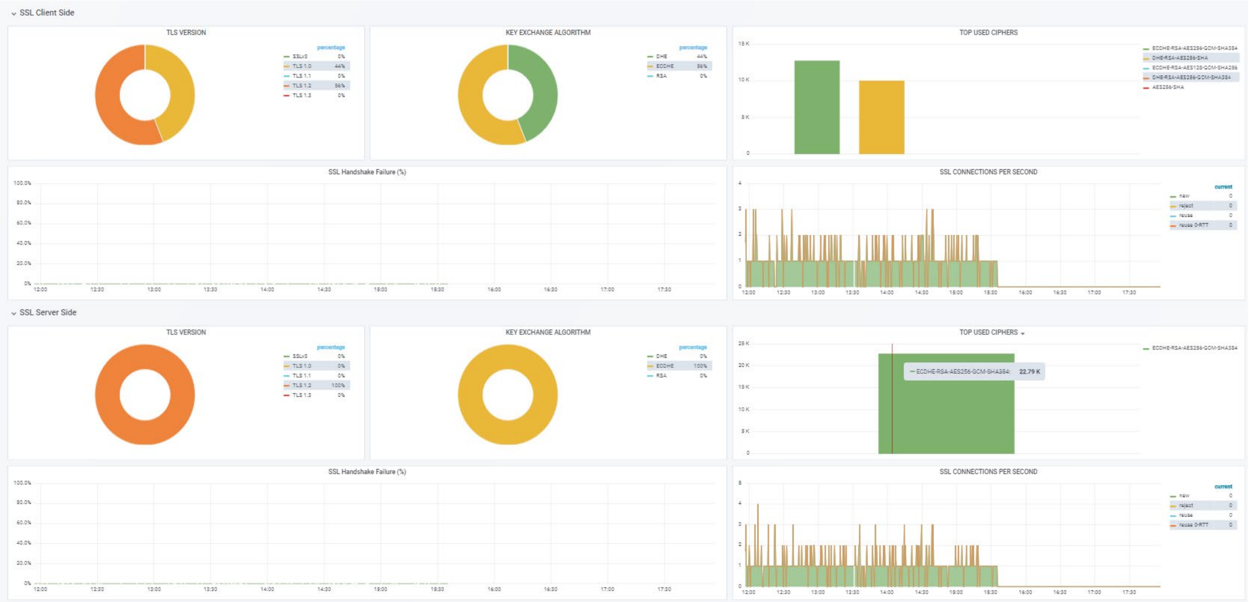
	min	max	avg	current
	80	106	99	103

Throughput

	min	max	avg	current
	0 bps	804 Mbps	567 Mbps	629 Mbps

Groups and Content Rules

Action	Content Rule	Group ▴	CEC	CPS	Throughput	Status
group	0	group1	103	724	629 Mbps	Up



SSL

TLS 1.2 Session Tickets Support

TLS pre-version 1.3 offers two session resumption mechanisms:

- Session ID – The server keeps track of recent negotiated sessions using unique session IDs.
- Session Ticket – The session key and associated information, encrypted by a key (STEK), which is only known by the server, are stored by the client. This removes load from servers.

TLS 1.3 only offers the Session Ticket resumption mechanism.

Alteon now also supports the Session Ticket resumption mechanism for TLS 1.2, 1.1, and 1.0.

If TLS 1.2 Session Ticket support is enabled on Alteon, but the remote side does not support Session Tickets, Alteon reverts to the session ID reuse mechanism.

Using the Session Ticket mechanism for TLS versions 1.2, 1.1, 1.0 can be controlled at the device level and per SSL policy. Note that reuse is controlled separately for the front-end and back-end.

- If the SSL Policy Session Reuse parameter is set to **Inherit**, all reuse parameters are taken from the global settings, and the SSL policy level TLS 1.2 Session Ticket parameter is ignored.
- If the SSL Policy Session Reuse parameter is set to **Disable**, the SSL policy level TLS 1.2 Session Ticket parameter is ignored.
- If the SSL Policy Session Reuse parameter is set to **Enable**, the SSL policy level TLS 1.2 Session Ticket parameter controls the behavior.

Notes:

- Even though it is named TLS 1.2 Session Ticket, when enabled it also allows use of Session Tickets for TLS 1.1 or 1.0 handshakes.

Session Ticket Key Mirroring

Mirroring the key (STEK) used by Alteon to encrypt the Session Tickets on the standby Alteon device allows for fast TLS session resumption after failover.

The STEK is securely synchronized using a passphrase configured on both devices.

To enable STEK mirroring and configure passphrase:

- Web UI: *Network/High Availability* page, *Stateful Failover* tab
- CLI: `cfg/slb/sync/tcktkey` menu

Note: STEK sync is supported only in switch-level failover HA modes (Switch HA, Legacy VRRP Active-Standby and Hot Standby)

OCSP Stapling

Alteon now supports OCSP Stapling on both the front-end and back-end:

- On the front-end SSL connection, Alteon performs as an SSL server and can staple its certificate before forwarding it to the client, if the client requested staple in the Client SSL Hello.
- On the back-end SSL connection, Alteon performs as an SSL client and can request (if enabled) a stapled certificate from the server.

OCSP Stapling activation is performed via the Authentication Policy:

- An Authentication Policy must be created for either the client or server side depending on where you want to employ OCSP Stapling
- OCSP must be enabled as the Certificate Validation method
- A new parameter, OCSP Mode, is available and determines whether to enable OCSP Stapling or not. Its values have a different effect for Client and Server Authentication Policies:

OCSP Mode	Client Authentication Policy	Server Authentication Policy
OCSP Server	Alteon communicates with the OCSP server to validate client certificate.	Alteon communicates with the OCSP servers to retrieve the revocation status for the certificate it received from the server.
OCSP Stapling	Alteon sends to the client the server certificate accompanied by the OCSP staple retrieved from the OCSP server, attesting the certificate is not revoked.	Alteon requires the OCSP status from the back-end server (OCSP staple).

OCSP Mode	Client Authentication Policy	Server Authentication Policy
Both	Alteon validates the client certificate and staples the server certificate it sends to the client.	Alteon requires the OCSP status from the server (OCSP staple). If the OCSP staple is not received, or the received response is not valid, Alteon communicates with the OCSP servers to retrieve the revocation status for the certificate it received from the server

- Configure the relevant OCSP parameters.
- The Authentication Policy must be attached to relevant SSL policy.

AppWall

New Fingerprint-based Tracking Mechanism

The Activity Tracking module can be set to one of two tracking modes:

- IP-based tracking (available both in Passive and Active modes) is not intrusive.
- Device Fingerprint-based tracking (available only in Active mode) is intrusive.

Device fingerprint technology employs various tools and methodologies to gather IP-agnostic information about the source, including running JavaScript on the client side. Once the JavaScript is processed, an AJAX request is generated from the client side to AppWall with the fingerprint information.

Previously, when an HTTP request is received from a new source, the browser received from AppWall a 302 Redirect response to a fingerprint page. Once the browser received that page, it executed the embedded JavaScripts that generated a fingerprint that was sent back to AppWall as an AJAX call. Only then, AppWall redirected the browser to the originally requested resource in the secured Web application.

As of this version, AppWall embeds the Fingerprint JavaScript into the original server response, avoiding the dual redirect process. The JavaScript process is then executed as the last step of the page rendering process in the browser. Thus, there is no end-user visibility into the redirect process, the fingerprint page is not shown, and there is no latency experienced by the user.

WebSocket Support

WebSockets is a protocol that allows the transfer of different types of data, such as XML, JSON, other types of text, and binary data. As of this version, AppWall detects the WebSocket switching protocol process and bypasses the connection to avoid a scenario of blocking a WebSocket because of lack of conformity with the HTTP RFC. This setting can be configured in the Tunnel HTTP properties section. By default, bypassing WebSockets is disabled.

New Web UI Interface

As of this version, the common operational use cases of AppWall management are offered also as pure Web interface instead of the Java applet. The new interface is launched via the Edit Security Policy link in **Security > Web Security > Secured Web Applications** pane and via the New AppWall Configuration link in the **Security > Web Security** pane.

The Web UI runs on a modern technology with a React client side and with a back-end REST API layer based on the Node.JS server. The REST API calls generated from the client-side application are authenticated using JWT (JSON Web Token), properly securing access to the server side.

The highlights of the supported functionality in the new Web UI include:

Configuration:

- Add/Edit/Delete a protected Web server
- Add/Edit/Delete HTTP and HTTPS tunnels
    - TCP properties
    - Parsing properties
    - Message size
    - Active/Passive mode
- Add/Edit/Delete a Web application
- Add/Edit/Delete an application path
- Vision server configuration
- Certificate management
- License management
- IP groups management
- Activity Tracking
- Source Blocking Management
- Cluster Manager settings and adding nodes
- Backup/restore configuration

Security Policies:

- Host based policy:

    - CSRF
    - Activity Tracking
- Security Filters Policy:
    - Global Security Filter settings
    - Enable/disable security filters in application path
    - Manage security filters refinements
- Role based policy

Forensics

- Publishing rules
- Security, Initialization, admin and system logs with filtering options

Dashboard

- Dashboard summary view: resource utilization, traffic volume
- Reporting widgets: Events by Filters, Events by Apps
- Dashboard view of tunnels with stats

New AS++ Command – whereis

The new whereis AS++ command lets you retrieve the geographical location of a specific IP address.

The command supports both IPv4 and IPv6 addresses.

Syntax: `whereis <IP> [continent | country_code | state | city | zip | latitude | longitude]`

When no flag is provided, the command returns all the parameters (continent, country code, state, zip, latitude and longitude) in a TCL list.

Notes:

- For DPS devices, a Perform or Secure subscription is required.
- If there is no valid license or the location of the IP address is unknown, the command returns empty list/parameter.
- If the invalid IP address is invalid, the traffic is failed.

WHAT'S CHANGED IN 32.2.0.0

Alteon VA Enhancements

Footprint Reduction

Alteon VA is now available with a small footprint (2 GB RAM) on Azure or AWS on top of its availability on other hypervisors that were introduced in version 32.1. This makes the usage of Alteon VA on public Clouds more cost effective (for example, you can now utilize the t2.small instance on an AWS instead of m3.medium instances in previous versions).

With 2GB RAM, some of the system capacity tables were reduced as follows:

- Real servers: 1024
- Health checks: 4096
- Content rules: 150
- Filters: 75
- HTTP modification rules: 1000
- Data classes: 100

The Alteon VA with a small footprint is not recommended for advanced Layer 7 processing, such as force proxy, SSL offload, AppShape++ scripts, and so on.

Improved Performance on Azure

Starting with this version, Alteon VA supports SR-IOV on Azure.

With this capability, Alteon VA can utilize up to 15 vCPUs providing improved Layer 7 and SSL performance.

GEL Support Enhancements

GEL License Activation

When activating the GEL license on Alteon instances, there is no longer a need to enter the DPS package. You just need to enter the throughput (in case no subscription add-on is required), and Alteon extracts from the entitlement the relevant DPS package.

DPS Package Upgrade

When upgrading a DPS package license of an entitlement, all of the Alteon devices automatically upgrade their licenses to the new DPS package with no need for manual intervention to change their licenses.

LLS Availability on Azure

You can now also deploy vDirect with the Local License Server (LLS) on the Microsoft Azure Cloud. This is important if all of your Alteon VAs are running on Azure, and need an LLS on the same network.

Password Generator

The password generator also accepts the Entitlement ID to generate the password for upgrades. This enables the support of Alteon VAs running a GEL license that do not have their MAC addresses registered in the install base.

SSL Key Replacement

It is now possible to replace an existing key, using the same ID, via Web UI.

SSL Inspection Wizard Enhancement

A wizard for quick and easy configuration of an inbound SSL Inspection solution is now available via APSolute Vision (version 4.10 and later). The wizard is implemented using a Radware vDirect workflow.

The wizard supports a Layer 3 environment in either a single or 2-box deployment, and can be run on either a standalone, Alteon VA, or vADC.

To access the wizard, do one of the following:

- Select the Alteon device from the APSolute Vision device tree.
  1. Go to **Configuration > Application Delivery > SSL > Inbound SSL inspection**.
  2. Click the **Inbound SSL Inspection Wizard** link. A vDirect page with the workflow opens in a separate browser page.
  3. Run the **Inbound_ SSL_ Inspection_ Wizard** workflow.
- From APSolute Vision, open the vDirect page:
  1. Navigate to **Operations > Catalog**.
  2. Filter by the **SSL inspection** tag (optional).
  3. Run the **Inbound_ SSL_ Inspection_ Wizard** workflow.

LinkProof MAC Overwrite

LinkProof can now handle scenarios where the WAN Link router is in fact a router cluster, but without a floating MAC address (GARP announcements use the active router MAC address and not the floating MAC address).

To support this scenario, when a new MAC address is received for a WAN Link that differs from the MAC address already in the ARP table for that WAN Link IP address, Alteon overwrites the MAC address in all session entries belonging to this WAN Link. This ensures that traffic is sent to the MAC address of the active router.

NFR ID: prod00262807

Allow Local and Remote Authentication

When Alteon management users are authenticated using remote authentication (RADIUS or TACACS), you can now also allow local users. When this capability is enabled (new User Authentication Priority parameter set to Local First) Alteon will first try to authenticate the user locally and if it fails will use remote authentication.

NFR ID: prod00235979

Health Check Enhancements

Graceful Health Check Edit

When a health check attached to a group or real server is changed (either by attaching a new health check ID or by editing the health check parameters), after **Apply** the status of the health check is preserved. Previously the status of an edited health check immediately after **Apply** failed, causing the server's status to temporarily change to **Down**.

Note: The status of the health check is not preserved after the change in the following cases:

- If the destination port of the health check is changed, either by changing it directly on the health check object or by changing it on the virtual service or real server.
- If the host name is configured as **Inherit** in the HTTP/HTTPS health check and the virtual service hostname is changed.
- If a basic health check is replaced by a logical expression health check, if the old basic health check had a user-defined destination port that was different from service/server port.

NFR ID: prod00252740, prod00261070

Advanced Virtual Wire Health Check

The Advanced virtual wire health check can be used to check the connectivity between the ingress and egress interfaces of a virtual wire device in an SSL inspection deployment.

As opposed to the OOTB virtual wire health check (used by the on-device outbound SSL inspection wizard), the advanced virtual wire health check can also be used in a manual configuration. It does not require static ARP and it runs on the TCP port defined on the filter rport or the health check dport.

AppWall

AppWall in Transparent Mode

The ability to provide WAF capability in transparent mode via filters was introduced in version 32.1.1.0 with several configuration restrictions.

In this version, there is no longer any restriction to the syntax of the Secure Web Application name or the SSL policy ID. However, on filters with an attached SecureWeb Application, it is required to configure the Multi-protocol Filter Set ID:

- If the same Secure Web Application is attached to several filters, all filters must set the filter set ID to the same value.
- If different Secure Web Applications are attached to different filters, a different filter set ID must be set for each filter.

Support for transparent AppWall configuration via WBM has also been added.

Syslog Message Enrichment

The threat category and attack name fields were added to the syslog messages generated by AppWall to external SIEM solutions.

Defense Messaging

Defense Messaging to DefensePro version 8.x was certified to support both a Layer 3 source IP address and Layer 7 XFF based source IP.

User Name Format

AppWall now adds support for defining the username format as it is being sent to the user datastore. Now there are three optional formats:

- username@domain
- domain\username
- username

This new function is supported for both RADIUS and LDAP servers.

SSL Statistics and MIBs

MIB and WBM support has been added for SSL front-end and back-end SSL statistics, including the cipher usage statistics. They are available in the following panes:

- **Monitoring > Application Delivery > Virtual Servers > Service [x] > View Service**

- **Monitoring > Application Delivery > Filters > View Filter**

The SSL summary statistics are available through **Monitoring > Application Delivery > SSL**.

MAINTENANCE FIXES

Fixed in 32.2.0.0

Item	Description	Bug ID
1.	Using WBM, in the Service Status View pane, the real servers incorrectly displayed.	prod00267276
2.	Using WBM, in the Service Status View pane, the filter option in the displayed data did not work as expected.	prod00267217
3.	Using WBM, the complete IPv6 Management IP address did not display.	prod00267208
4.	In an SLB environment, when real servers were moved from one server group to the other, although the real servers were moved away from a group, the old sessions still remained and did not age out.	prod00267134
5.	In an SLB environment, after the primary real server went down and the backup real server and group took over, the service became inaccessible.	prod00267089
6.	Alteon did not handle a specific condition related to FQDN and went into an inconsistent state.	prod00267062
7.	In a Global SLB environment, when the network gmetric used a network class as the source IP address, the DNS response was incorrect.	prod00267044
8.	In an inbound link load balancing Smart NAT environment, the Availability metric in the SmartNAT GSLB rule was not processed, causing an improper ISP links order.	prod00267020
9.	Using WBM, from the *Certificate Repository* pane, you could not perform a search in the table.	prod00266986
10.	In a configuration sync environment, after a routine configuration change, the MP CPU reached 100%.	prod00266964
11.	In an SLB environment, when overlapping IP addresses were defined in a network class configuration with exclude enabled, and when an exclude range was a subset of the other exclude range, the filter defined with this network class fired incorrectly for an excluded IP address, causing the filter to misfire.	prod00266924

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

Item	Description	Bug ID
22.	When the NTP was set over a data port and the NTP server was down, an incorrect SNMP Trap (Critical Temperature Trap) was sent when the NTP request timed out.	prod00266743
23.	In an Azure environment, when the RADIUS server was on a different network other than the management network, RADIUS authentication did not work.	prod00266675
24.	In an SLB environment, after configuring the real server weight using the CLI command `/c/slb/real x/weight`, a panic occurred.	prod00266636
25.	In an SLB environment with an acceleration environment, due to connections being reset, some application outages and traffic failures were observed.	prod00266633
26.	In an SLB environment, on a real server, due to packet drops in the SPs, TCP latency occurred for health check packets.	prod00266603
27.	In in Outbound Link Load Balancing environment, the transparent health check to a destination server was sent from an inappropriate port/VLAN (WAN Link).	prod00266602
28.	While using a REST API call to export the configuration, Alteon ignored the path and name specified in the API request. Alteon generated a name and transferred the file to the root folder of the SCP server instead.	prod00266593
29.	When importing a key which is not encrypted (plain text), due to minimal passphrase that was set, the import caused all onboarding of HTTPS applications that use non-encrypted certificates to fail.	prod00266573
30.	In a monitoring environment, invalid TRAP OIDs were sent for the SP CPU Pressure On/Off. **Note**: The correct MIB OID has been added to the trap.c and GENERIC-TRAP-MIB.MIBs: altSwSpCpuPressureActivatedTrap - 1.3.6.1.4.1.1872.2.5.7.0.214 altSwSpCpuPressureDeactivatedTrap - 1.3.6.1.4.1.1872.2.5.7.0.215	prod00266559
31.	In a VRRP environment with an SLB configuration, the session move operation did not get synchronized to the backup, leading to session mirroring not working, causing statistics discrepancies on the backup devices.	prod00266543

Item	Description	Bug ID
32.	In an SSL environment, when changing the cipher suite from TLS 1.2 to the User Defined " TLS_ECDHE-RSA-AES128-GCM-SHA256" cipher, the AX configuration was corrupted and the service to which the SSL policy was attached stopped working.	prod00266530
33.	In a Layer 7 environment, if the original request did not contain any query, Alteon did not remove the query separator "?" in the redirect URI.	prod00266453
34.	Using WBM, in the *Outbound LLB Rule* pane, the IP address/network could not be edited.	prod00266452
35.	In a VRRP environment, when health checks failed on the backup, statistics discrepancies (incorrect number of sessions to the real servers) occurred on the backup device.	prod00266339
36.	In an SLB environment, when there was a change in the virtual server configuration (disable/enable), the session move operation via CLI did not move the session to a different real server.	prod00266338
37.	When the time zone was set to Asia/Jerusalem (GMT offset +02:00), as the daylight saving setting was not taken into account, Alteon displayed the incorrect time from the month of October.	prod00266305
38.	In an SLB environment with HA, after the failover, uneven load distribution occurred on the new master device.	prod00266157
39.	Using WBM, In the certificate repository, when importing an intermediate CA, the size displayed as 0. **Note:** After the fix, the size is not calculated and is displayed blank.	prod00266154
40.	In an SLB environment, when real servers were allocated to multiple virtual services and a **Revert Apply** was performed, the session table was deleted automatically.	prod00266012
41.	Using WBM, with the "User" role, configuration sync could be performed even though the "User" account should not be able to do this.	prod00266008
42.	While running a vDirect script on Alteon devices, it took more than 20 minutes to display the output or the script timed out with no result.	prod00265982
43.	In an SSL environment, the user was unable to change the ciphers string under the advanced HTTPS health check.	prod00265975

Item	Description	Bug ID
44.	Using WBM, in the **Configuration > Setup > High Availability** pane, there was no option to delete VR Group settings.	prod00265973
45.	Using WBM, in an SLB environment when configuring a virtual service, the cookie configuration changed after making a change to the virtual server even if the user did not modify the persistent binding (pbind) cookie settings.	prod00265867
46.	Using WBM, when duplicating a real server, sometimes the "ERR json parse failed" message was returned.	prod00265865
47.	Using WBM, from the health check pane **Configuration > Application Delivery > Health Check > add** , the **Always Perform Health Check** field displayed twice.	prod00265861
48.	Using WBM, you could not set the action as Discard for a virtual server.	prod00265857
49.	When performing SNMP monitoring on SSL offloading stats (FE/BE), due to a memory corruption, a panic occurred and the device rebooted a few times.	prod00265843
50.	In an Alteon integrated AppWall environment, SSL sessions were not created for specific tunnels.	prod00265812
51.	When **agTftpCfgFileName** was more than 83 characters, exporting the configuration with SCP through the REST API server failed.	prod00265672
52.	If the data-class entry contained a backslash (\) character and configuration sync was performed, the configuration was not synced correctly.	prod00265617
53.	In an SLB environment, when the client connected directly but through different VLANs for forward and backward traffic, the SP CPU utilization became high even though the amount of traffic was not increased, causing a degradation.	prod00265558
54.	In a Global SLB environment, when a configuration **Apply** was performed during the periodic statistics calculation, when the internal data structures used in GSLB were reset and repopulated, an illegal access occurred, causing a panic.	prod00265544
55.	When a new virtual server with a service-based proxy address and a corresponding VPR were both configured within the same **Apply** operation, Alteon did not display the VPR status in the VRRP and the ARP cache.	prod00265538

Item	Description	Bug ID
56.	In an SLB environment, if the configuration had a disabled virtual server and one of the services of the virtual server had a non-existent AppShape++ script, the configuration could not be saved.	prod00265537
57.	Using WBM, when using the SSL Inspection Wizard, when performing a revert, in certain conditions a REST API 405 error displayed even though the Revert was successful.	prod00265381
58.	In an HA environment, during configuration sync, the real server configuration under HA triggers were not synced to the peer correctly.	prod00265322
59.	In an SLB forceproxy environment with IP service and filters configured, when performing an **Apply**, Alteon attempted to add a service mapping entry (needed for IP address and Port translation) for a filter, but instead accessed data meant for the virtual service, causing a panic.	prod00265289
60.	In a BGP environment, you could not import the default gateway alone or any other "range of IP"/"IP" separately.	prod00265280
61.	In an SSL environment, when configured with client-IP, SSL-ID persistency and with SSL-ID traffic, a panic occurred.	prod00265243
62.	When dumping the FDB entries in the SP using the `/maint/debug/spfdb` command, only 8K entries were dumped when the Max size of the FDB per SP was actually 16K.	prod00265212
63.	In an SNMP monitoring environment, when accessing the MIB OID 1.3.6.1.4.1.1872.2.5.4.3.14 corresponding to runtime instances of a health check, a panic occurred.	prod00265181
64.	Using WBM, when logging in as a TACACS user, the following error message displayed: `mgmt: The language defined at the TACACS server is not recognized. Using global language.`	prod00265166
65.	In an HA environment with session mirroring enabled after failover, the new master did not mirror sessions to the new backup.	prod00265127
66.	In an Alteon integrated with AppWall environment, when the Accept-Language header was missing, AppWall responded with a 302-response code.	prod00265072
67.	If the IDSChain was not working for subsequent fragments or did not forward fragment IP frames that matched the filter, the RADIUS Server communication broke.	prod00265053

Item	Description	Bug ID
68.	Using WBM, in the Layer 7 Load Balancing Content Class Configuration pane, if the content class string contained a backslash (escape characters), the REGEX text field value displayed incorrectly.	prod00265029
69.	In a monitoring environment, fetching the Layer 3 Interface statistics using REST API did not work.	prod00264975
70.	Using CLI, with verbose 1 set, when a health check that was associated to a server group or real server was deleted, a prompt for user input did not display.	prod00264970
71.	When PIP was configured under a DNS-UDP stateless service, as it is not applicable it was ignored. **Note:** As a fix, a warning message has been added only in CLI.	prod00264906
72.	In an HA environment, the backslash ("\") character in the LDAP user name was not synced to the peer device, and WBM did not display them.	prod00264903
73.	Using WBM, when a real server was deleted from a GSLB network, as these entries could not be reused even after deletion, once all the maximum 128 entries were exhausted, the following error message displayed: `Real server precedence table is full`	prod00264835
74.	The image upload on the management port using SCP was slower than using FTP.	prod00264763
75.	In an AppWall integrated with Alteon environment, for a virtual server that had an AppWall tunnel, Alteon stopped processing traffic.	prod00264676
76.	In an SLB environment with health checks configured, with an HTTP health check there was no difference in the failure status regardless of the failure reason. If the checked file was removed (404 code), the file required authentication (401 code) or an internal server error (500 code), for all cases the following error displayed: `Reason: Server's response is not as expected`.	prod00264674
77.	In an Alteon HA environment, when configuration sync failed with a Global SLB/Link Load Balancing configuration, after the failure the new configuration moved automatically to the current configuration without performing an Apply operation.	prod00264673
78.	In a DNS environment, Alteon does not include the edns0 client subnet in the DNS response.	prod00264633

Item	Description	Bug ID
79.	In an SLB environment with AppShape++ scripts, when adding an AppShape++ script to a virtual server without creating the service on that virtual server and performing an **Apply**, an **Apply** error did not occur, and any further configuration change on the virtual server and performing **Apply**, the `Pending configuration` message always displayed.	prod00264597
80.	Alteon allowed management access via data ports on IPv6 even though the access was disabled.	prod00264531
81.	In an HA environment, after synchronizing the configuration from the master device, the health checks for a real server failed/toggled on the backup device.	prod00264498
82.	Due to a debug tool that was configured for OpenSSL, HTTPS health checks caused 100% CPU usage on the MP, introducing delays in HTTPS health checks.	prod00264468
83.	When configured a URI under a CDP group with the left parenthesis ("(:) character in the URI and with traffic, a panic occurred	prod00264433
84.	In an HA environment with SLB configured, after configuration sync, when Alteon attempted to configure the backup real server as a backup group, the backup real servers in the group were removed on the peer device.	prod00264432
85.	In an IPv6 environment, even though IPv6 local networks were configured, Alteon sent a server response to the default gateway instead of sending it directly to the connected client. As a result, a real server could not be reached from the subnet.	prod00264431
86.	In an SLB environment, incorrect statistics were displayed while fetching virtual service statistics (`via /stats/slb/virt`), the statistics for a real server (Current, Highest, Total sessions) displayed as 0, even though the real server handled the connections.	prod00264430
87.	On an Alteon VA platform, although the new VLANs were defined to contain default ports, after the reboot, the configuration was always pending in the diff operation.	prod00264390
88.	In a forceproxy SSL environment, internally when MP and AX went out of synchronization, Alteon continued to send an old certificate even after installing a new certificate.	prod00264339

Item	Description	Bug ID
89.	Using WBM, from the **Configuration > Application Delivery > LinkProof > Inbound LLB Rules** pane, there were several issues during configuration.	prod00264289
90.	Using WBM, with SLB monitoring, when a content rule was used with a real port, the session counter displayed incorrectly.	prod00264285
91.	Using WBM, in an Inbound Link load balancing environment, the NAT address configuration was missing in the Global SLB's client network rule page.	prod00264245
92.	Using WBM, when attempting to configure HTTP modification for header removal, Alteon forced the user to input the header value.	prod00264244
93.	Using WBM, in an SSL environment in the Export tab, even though the "certificate and key" option was selected to export, only one **Export** button displayed.	prod00264233
94.	In an HA environment with script health checks configured, after deleting/adding/modifying a script and performing configuration sync, there was a discrepancy in the health checks between the master and the backup device.	prod00264172
95.	In an SLB environment, when a real server with the same IP address was configured for different groups, and each of the groups were configured with the same logical expression health check, Alteon failed to evaluate the logical expression except the group in which the real server came up first. The rest of the real servers remained down in respective groups.	prod00264146
96.	In an environment with a configuration where the client packet comes into Alteon through one VLAN (ingress) and after server processing, the response packet leaves to the client in another VLAN (egress), duplicate IP FDB entries got created for external IP addresses.	prod00264048
97.	In an SSL environment with Cavium cards, after upgrading a couple of certificates and performing **Apply**, a panic occurred.	prod00264047
98.	Using CLI, when executing a non-existing or hidden command with the /maint/pktcap menu, an error was not issued. **Note:** As a fix, all the hidden commands under `/maint/pktcap` were removed and cannot be executed.	prod00264010
99.	In an SLB environment with filter processing enabled, VMAed traffic source MAC learning did not occur, causing traffic to be flooded on all the VLAN ports, causing higher throughput utilization.	prod00264009

Item	Description	Bug ID
100.	In an SLB environment with multiple rports, when a new real server was created with addports and if it was associated to more than one service, if any of the service health checks was toggled, Alteon forwarded client requests to the server on the service port rather than on the real server's service port (rport = addport of the real server).	prod00263992
101.	In an SLB environment, when a particular sequence of SLB configuration steps involving a HTTP virtual service and another virtual server along with **Apply**, the configuration became corrupted.	prod00263986
102.	In an SLB environment, when a group was configured with one or more real servers (by manual configuration), when deleting or removing real server(s) from the group, the following Apply error displayed: `Error: Real server group 100 associated to virtual server 100 service 80 is not defined`	prod00263985
103.	For the BWM-history-related e-mail, when the SMTP 'To' user was not configured, but when Alteon tried a number of times to send this e-mail, after a while Alteon did not respond to SSH/HTTPs via management.	prod00263983
104.	Using WBM, when a configuration dump was performed on a FIPS device, the following error displayed: `Error: Configuration import/export via HTTP is already running.`	prod00263982
105.	In an SLB environment, you could not configure a virtual server with a different protocol and Alteon returned the following error: `Error: Virtual server v1 has the same SIP SLB group id as virtual server v1-udp`.	prod00263980
106.	In a virtualization environment with HA, when p-session sync updates were received from the master, the backup attempted to become the master. This was no longer an issue when the p-session sync was configurationally disabled.	prod00263979
107.	In an AppWall integrated with Alteon environment, when troubleshooting some false-positive "HTTP reply not RFC-compliant" events were issued that indicated that Request Data and Reply Data under Forensics were identical.	prod00263587
108.	There was a discrepancy between the peak compressions usage command output (/info/swkey) and syslog messages.	prod00261525

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

AppWall

Item	Description	Bug ID
1.	Fixed a rare failure in the HTTP parsing process.	DE43435
2.	Fixed a rare failure in HTTP Response parsing process.	DE43438
3.	The client IP address was not sent in the security page.	DE42288
4.	For some types of security violations, the case number shown in the security page was 0.	DE41895
5.	When the server response body was in JSON format, the BruteForce security filter failed to block the IP address for a bad login after the IP address reached the threshold limit.	DE44726
6.	BruteForce security events syslog messages had the wrong event type value: learning instead of security.	DE45524
7.	Fixed PCI compliance Report data in APSolute Vision in the 6.5.5 section referring to Improper error handling.	DE23276
8.	Primary LDAP server failure detection and failover to the secondary server did not work under certain conditions.	DE42480
9.	When a non-authenticated user attempted to access a Web page, the Authentication Gateway redirected the user to the login process and upon successful authentication, redirected it back to the originally requested page. The redirection back to the originally requested page did not preserve the original HTTP request parameters.	DE42479
10.	Under rare conditions, Alteon stopped processing traffic on a VIP with an Application security policy.	DE42240
11.	When the Authentication Gateway received requests from an old version of the Internet Explorer browser, AppWall redirected successfully authenticated users to the authentication process.	DE42339
12.	In Monitor deployment mode and in Alteon OOP mode, both Request and Response data in the security logs for non-RFC-compliant HTTP Reply displayed Response data.	DE40221

Item	Description	Bug ID
13.	Added a terminating chunk to a 302 chuck encoding reply with an empty body.	DE43566
14.	Was unable to refine forensic events for SafeReply credit cards.	DE44273
15.	Login monitoring settings in HTTP custom headers were ignored.	DE43567
16.	For AppWall running on Alteon version 32.0.1.0, adding a DefensePro the Defense Messaging configuration using port 443 failed.	DE42698
17.	Fixed issues with AppWall policy synchronization between the master and backup Alteon platforms.	DE44274 DE44670
18.	A rare failure could occur when an HTTP response could not be properly parsed.	DE44316
19.	A long JSON value within a query parameter could cause a failure.	DE44890
20.	For the Database Security Filter ignored parameters, the logs displayed the length of parameter name instead of the parameter param value.	DE44869
21.	Fixed the “Server Name” field value in the Security logs for AppWall running on Alteon.	DE45098
22.	Fixed a possible failure in AppWall once applying a policy change.	DE34945
23.	REGEX support was added for both.	DE44273
24.	API calls for NTP servers sometimes were not be successful.	DE41308
25.	The Database.kcf file was not replaced during the upgrade process to version 7.5.8.	DE42077
26.	The ptcfg command did not work properly in Alteon. A "Failed to create AW configuration File" message was shown.	DE44559

Fixed in 32.1.0.0

Version 32.1.0.0 includes all field bugs available in version 31.0.6.0.

Item	Description	Bug ID
1.	Using the CLI, when executing the command `/stat/spx/allcpu`, the SP CPU statistics that displayed was 0%.	prod00263872
2.	In an SLB environment with ICAP messages chunked, due to parser issues in Alteon, a panic occurred.	prod00263781

Item	Description	Bug ID
3.	Using WBM, when creating a new HTTP or HTTPS service, Alteon added an extra command for FTP for the service.	prod00263714
4.	In an SLB environment, when enabling an SNMP health check for a group with the roundrobin metric, a panic occurred.	prod00263635
5.	In a Geo Proximity environment, a software upgrade caused an invalid GEO configuration, which led to an outage.	prod00263469
6.	In an SLB Filter environment with dbind forceproxy, dport configured with a range and rtsrcmac enabled did not handle the return traffic for port range except the starting port. For example, for dport range 8080-8443, traffic worked only for 8080 but not the other ports in the range.	prod00263325
7.	In an SLB environment, when the Script health check was configured with nonat for a virtual service, the incorrect source IP address was used by Alteon.	prod00263231
8.	In a VRRP active-standby configuration, when configuration sync was performed, though the corresponding virtual service was UP, the virtual router (VSR) went into the INIT state.	prod00263222
9.	In an SLB environment with FQDN servers configured: • The DNS response was received during a Revert Apply or configuration sync, causing a problem. • When a Revert Apply or configuration sync was performed during service, the DNS response caused a problem.	prod00263196
10.	Using WBM, in the **Monitoring > LinkProof > WAN Links > Per WAN Link IP/ID and Monitoring > LinkProof > WAN Link Groups** pane, the statistics did not display correctly.	prod00263121
11.	In the *Monitoring* perspective, sometimes empty e-mails were randomly generated.	prod00263061
12.	In an SLB environment with rtscmac enabled, the source MAC address of a virtual server would change during the same session, causing packets to be blocked by ISP.	prod00263043
13.	Using WBM, in the **Configuration > Application Delivery > SSL > Certificate Repository > Intermediate Certificate** pane, the key type of the intermediate certificate was displayed as unknown.	prod00262965

Item	Description	Bug ID
14.	In an SLB environment with IPv4 virtual servers and an IPv6 real server, when using IP version conversion and some SLB related-configuration changes were made, misleading syslog messages were issued.	prod00262937
15.	In a Layer 7 environment, the redirection URI under Content Classes took the variable query $QUERY keyword only after the custom queries.	prod00262866
16.	In an SLB environment with SSL offload, and with forceproxy enabled and rtsrcmac enabled, and with a filter enabled on the server port, when the server packets were dropped in the SP after server processing, SSL offloading did not work properly.	prod00262841
17.	Using CLI in an SLB Monitoring environment, the octet count displayed by the virtual server statistics command `/stats/slb/virt x` was incorrect.	prod00262825
18.	Alteon failed to import encrypted private keys that had a long password (> 40 characters).	prod00262772
19.	In an SLB SIP environment with AppShape++ scripts, a SIP parser issue occurred.	prod00262760
20.	In an SLB monitoring environment with names configured for real servers, when displaying the real server group statistics with the CLI command `/stats/slb/group`, the real server name was listed instead of the IP address. The fix was to change the heading to "IP Address/Name". The real server name displays if it is configured. Otherwise, the IP address displays. This also applies to the commands `/stats/slb/virt` and `/stats/slb/sp x/virt`.	prod00262715
21.	Using WBM in an SLB environment, you could not configure POP3 over SSL (TCP port 995).	prod00262692
22.	After disabling the default user, the command `/cfg/sys/access/user` did not display the correct value.	prod00262676
23.	In an SLB environment with filters, even though rtsrcmac (Return to Source MAC) was enabled for a filter, ICMP reply packets corresponding to the filter session were routed to the VLAN gateway instead of the client port.	prod00262649

Item	Description	Bug ID
24.	Using WBM in an SLB environment, when a virtual router and Proxy IP address under a virtual server were the same, the following error displayed: `The IP Address of Virtual Router 2 conflicts with the Client NAT (PIP) IP address`	prod00262620
25.	During a Nessus security scan on Alteon, due to opening and closing SSH connections frequently, a panic occurred.	prod00262619
26.	Using WBM in an SSL environment, you could not generate a CSR.	prod00262589
27.	Using the CLI, the command `/info/l3/ha` output information was misleading (it displayed VRRP information).	prod00262578
28.	In an SLB environment with an IP service configured with the svcleast metric, traffic was distributed to the same server, leading to uneven load balancing of the traffic.	prod00262568
29.	In an SLB environment with content classes configured, when selecting a different group's real server per the content class, rather than a group-real server being configured on the virtual service, the front-end session abruptly aged out/terminated, causing service issues.	prod00262567
30.	When logged in with a backdoor-enabled user and with RADIUS enabled, after running the `/oper/passwd` command to change the user's password, the displayed username was incorrect, the syslog message was generated was with incorrect username, and the **Who** command displayed the incorrect username.	prod00262566
31.	In an environment with a slower client (LG K220) and a faster server, after enabling HTTP2, high SP CPU usage occurred.	prod00262565
32.	Using WBM, in a DNS Proxy configuration, you could not roll back the default group configuration to 'none'.	prod00262545
33.	After using the CLI command `/info/transceiver`, Alteon either rebooted unexpectedly or Alteon's traffic was stuck for about 13-15 seconds.	prod00262540
34.	Due to an ND issue, a panic occurred and caused a reboot.	prod00262521
35.	Due to an unauthorized Rx queue disable mode of I210 MACs, Alteon dropped some packets.	prod00262519
36.	Using WBM in an SLB SSL environment, attempting to create a new authentication policy also added the passinfo default configuration, causing the Apply to fail.	prod00262518

Item	Description	Bug ID
37.	Using WBM, when generating a server certificate with SHA256, the certificate was instead generated with SHA1.	prod00262456
38.	Using WBM, in the **Monitoring > Application Delivery > Global Traffic Redirection > Remote Real Virtual Servers** pane, the titles of the table were not displayed in human readable format.	prod00262436
39.	Export of applogs using SCP server with the hostname as the destination failed, but with an IP address as the destination worked.	prod00262426
40.	Using APSolute Vision, the **Generate** and **Export** buttons on the **Monitoring > System > Maintenance** pane were misplaced.	prod00262402
41.	When the gateway was unreachable, and even though Alteon had no interface that was alive interface, Alteon delayed in recognizing a gateway health check failure.	prod00262350
42.	In an SLB environment, when a Script health check was part of a LOGEXP, a different number of health checks packets were sent out per interval for the different health checks combined in the LOGEXP health check.	prod00262279
43.	In an SLB environment, even though the servers were up, Alteon responded with a 503 error	prod00262264
44.	In an SSL environment with certificates, import of certificates in PFX format failed when the passphrase contained special characters such as '@'.	prod00262239
45.	In an SSL environment with certificates, import of certificates in PFX format failed when the passphrase contained special characters such as '@'.	prod00262238
46.	In an SLB environment with HTTP2 enabled on virtual services, sometimes Alteon stopped responding with resource issues.	prod00262190
47.	In a LinkProof environment, Alteon responded to customer requests without changing the server IP address to the Virtual Server IP address and server packets being handled by filter processing, causing the access to fail.	prod00262164
48.	In a gateway-per-VLAN environment, all the traffic to the Alteon interface and virtual server was sent back to the gateway based on the default gateway and not per the VLAN gateway, causing the feature to not work.	prod00262161
49.	Alteon modified the source IP address of hops on the traceroute path of UDP and TCP responses, causing the client to receive an incorrect result.	prod00262158

Item	Description	Bug ID
50.	When logging in to WBM through a data port, the WBM user login information was missing and the incorrect client IP address was logged in the syslog message.	prod00262143
51.	In specific browsers (some versions of Chrome and Opera), which send some non-optimized HTTP2 HPACK header encodings that Alteon does not handle correctly, the PUT method did not work.	prod00262074
52.	After using the CLI command `/c/sys/syslog/cur`, the message `Syslog thread safe mode` displayed when it should not have.	prod00262045
53.	In an SLB environment, the PIP path under the virtual server `(/cfg/slb/virt <vsid>/service <vport> https/pip`) displayed in diff flash even though the settings were set to the default.	prod00262042
54.	When a primary group was configured without real servers associated with an FQDN server, the backup group used FQDN real servers, causing an **Apply** failure.	prod00262017
55.	Using WBM, in an SLB environment, you could not configure a Buddy Server.	prod00262010
56.	When the DNS server was down, Alteon stopped sending health checks with the destination as the hostname.	prod00261970
57.	Using WBM, when creating a Smart NAT dynamic NAT entry, the **Local Address** drop-down list included a **None** option which should have been named **Any**.	prod00261955
58.	Using WBM, when creating a new VRRP virtual router, the check box that is used to enable the virtual router was named **Enable Virtual Routers** instead of **Enable Virtual Router**.	prod00261953
59.	In an SLB environment with rtsrcmac enabled and reverse disabled, a request to a virtual server included an Allow filter, causing SLB traffic to fail.	prod00261909
60.	In previous versions, client IP persistency could not be maintained when the SP CPU was selected based on the client IP address and port (VMAsport enabled).	prod00261812
61.	In an SLB environment, changes to the network class associated to an in-route map required a BGP soft reset for the changes to take effect.	prod00261805
62.	When the audit log was enabled, Alteon sent a blank syslog for the delete operation.	prod00261801

Item	Description	Bug ID
63.	When monitoring Alteon using SNMP, when an SNMP GET was performed for a virtual server with nonat enabled (DSR), the current sessions displayed as NULL.	prod00261791
64.	In a Global SLB environment with the redirect exclusion feature enabled, Alteon selected a service for the DNS response with the action as "redirect" instead of resolving the DNS.	prod00261790
65.	In an SLB environment using CLI, when the xforward command was run for a service, the delayed binding forceproxy setting was not set.	prod00261789
66.	In the Monitoring environment with `/cfg/sys/report` set to on, a panic occurred with SIGSEGV(11) in thread RSTA(tid=81).	prod00261691
67.	When importing the configuration using REST API, Alteon always responded with a success message to the agTftpLastActionStatus query even though the import operation failed.	prod00261680
68.	In a Smart NAT environment, due to a sequence of validations in Global SLB, the warning messages for gmetric were confusing to the user.	prod00261630

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

70.	In a LinkProof NG environment, when the source address was configured for proxy or SmartNAT 'Any' dynamic NAT, the Return to the source MAC address did not work for filter traffic and the return traffic did not behave as expected.	prod00261528
71.	In a LinkProof NG environment, the inbound proximity (gmetric proximity) did not work with Smart NAT.	prod00261523

Item	Description	Bug ID
72.	In a Smart NAT environment, Alteon forwarded the ICMP reply to the client without changing the source IP address to the public IP address. As a result, the VPN gateways could not be pinged using the public IP address.	prod00261521
73.	In an SLB environment with forceproxy, when HTTP content had to be replaced to HTTPS content, Alteon could not match the content-types application/json or application/xml, so Alteon could not replace this part of the HTTP code. As a result, the whole page appeared with issues.	prod00261493
74.	In an SLB environment with forceproxy, the content-based rules with FQDN servers were not working and returned 503 error.	prod00261490
75.	With a data class configured, when attempting to modify the same data class without performing an Apply, there was a discrepancy between the Alteon white list and the vDirect getextendedinfo configuration file. The diff displayed the modifications, but the Apply failed.	prod00261406
76.	On the Cloud WAF portal, with white lists for IP addresses having zero as the last octet, an Apply operation failure occurred.	prod00261121
77.	In the Advanced HTTP health check configuration, although the maximum number of characters for the Body parameter was stated as 1024 characters, only 512 characters were allowed.	prod00261017
78.	Using WBM, when a user logged in using TACACS and performed configuration changes, and later performed Apply/Save operations, the audit logs recorded another user ID and not the user who had logged in.	prod00260978
79.	Using WBM, using $PROTOCOL instead of http:// or https:// in the redirection URL for content rules action redirect or action redirect for a service did not work.	prod00260876
80.	In a DNS environment where DNS responses were received, and with VRRP or HA, performing a configuration sync ended with an FQDN error.	prod00260836
81.	In the SNMP Trap for certificate expiration altSwcertRevokedID, the description was incorrect.	prod00260830
82.	In a VRRP environment, after sync was performed, the server group setting was removed from the peer device.	prod00260808

Item	Description	Bug ID
83.	In WBM, the SLB Viewer user role was allowed to enable/disable physical ports, when this user role should only be able to view Alteon information, SLB statistics, and information, but should not be able to make any configuration changes.	prod00260641
84.	Using WBM, a real server's Description accepted 128 characters while only 31 characters are supported, causing the real server Description not be synced from Active to Standby.	prod00260639
85.	Alerts regarding DUAL PSU failure were generated, but after 6 seconds a notice was issued that the Status was Ok. This issue persisted even after changing to a new PSU.	prod00260597
86.	Using REST API, image upload did not work.	prod00260564
87.	In an SLB environment, when a proxy IP address was defined in a network class, the proxy MAC address was sent with the gateway MAC address to those proxy IP addresses that were not present in the ARP table, causing the applications to fail.	prod00260562
88.	The load time of REST API calls was much slower than the load time in earlier Alteon versions.	prod00260509
89.	In an SLB environment with SSL Hello or HTTPS health checks configured, after upgrading to version 30.2.9.0, real servers configured with these health checks failed.	prod00260485
90.	In an SLB environment with the phash metric, the traffic load was unevenly distributed to real servers with random source IP addresses	prod00260470
91.	In an Outbound Link Load Balancing environment, LinkProof continued to send dispatching traffic towards WAN links whose bandwidth utilization was above 100%.	prod00260455
92.	You could not paste a geo network class configuration as taken from the configuration file and mandate it to add None for the Country and State fields.	prod00260454
93.	In a LinkProof environment configured with the bandwidth metric, Alteon did not select a WAN link based on the bandwidth metric configured on the DNS hostname and the DNS response included WAN links with the bandwidth overloaded.	prod00260453
94.	Using WBM with a WAN Link configuration, there were discrepancies between the upload bandwidth of the Per WAN Link IP and the Per WAN Link ID.	prod00260388

Item	Description	Bug ID
95.	Using WBM, when adding an IPv6 NAT IP address with the default prefix, because the IP address was added with prefix 0 instead of 128, the Apply operation failed.	prod00260360
96.	Using WBM or REST API with certificate repository management, you could not overwrite a certificate.	prod00260330
97.	In a BGP environment, after sending a BGP route update after a set of apply operations and a BGP toggle, a panic occurred.	prod00260322
98.	In a BGP environment, during BGP route update or when the BGP peer went down during BGP peer "cleanup," the platform hung.	prod00260321
99.	For unknown reasons, an unexpected reboot and a panic occurred.	prod00260320
100.	In an SLB environment, ESP traffic was not passed to the back-end servers.	prod00260297
101.	When using REST API to change the next image to boot, the correct image was not set.	prod00260261
102.	Using CLI, when configuring network classes, there were no validations when geo information was added for a network class as a one line command.	prod00260260
103.	Sometimes you could not configure a management port with an IPv6 address that was identical to one generated by SLAAC.	prod00260161
104.	In an SLB environment with delayed binding enabled and APM enabled, because Alteon did not create persistent entries for a few specific clients, Alteon sent the request from a specific Client IP address to a virtual service on Alteon to different real servers, even with the persistent binding Client IP address set on the virtual service.	prod00260097
105.	Using WBM, in an SSL environment, when enabling back-end SSL encryption and the back-end SSL cipher was selected as "user-defined," and then the back-end SSL encryption was disabled, the saved configuration was improper due to a malformed XML.	prod00260026
106.	In an SLB environment with the health check configuration destination set as hostname, the health check failed after performing an apply operation.	prod00259830
107.	When SSH/Telnet connections exceeded the allowed limit, no syslog message generated.	prod00259797

Item	Description	Bug ID
108.	In a failover scenario, when adding or updating more than 256 FDB entries from the MP to the SP, if the SP overloaded, the SP was not able to add the entries to the spfdb table, causing traffic disruptions in the network.	prod00259698
109.	In an AppWall for Alteon VA environment, techdata generation abruptly stopped and a reboot was required.	prod00259694
110.	When Alteon was accessed via SSH, the TCP connections opened for SSH sessions were not closed properly as the client continued to send data and caused stale TCP sessions. This led to SSH access failure to the device.	prod00259686
111.	Using WBM, in **Monitoring > Network > High Availability**, the VRRP labels were incorrect.	prod00259626
112.	In an SLB environment with persistent binding (pbind) configured with a cookie and Client IP, when Layer 4 sessions aged out, the reference count was decremented for the wrong persistent session, causing stale p-sessions.	prod00259581
113.	In a VRRP hot-standby environment, when the hot-standby port was designated as the next-hop port of the static ARP entry for a destination on the backup, a packet to the destination was sent out from that port even though it was in the Blocked state.	prod00259550
114.	In an SLB environment with FQDN real servers configured, on a virtual server with FQDN real servers, Alteon returned a 503 error even though the real servers were up.	prod00259492
115.	In an SLB environment with AppShape++ attached to a particular service, although alwayson was disabled, when the service went down, the request was forwarded to AppXcel.	prod00259436
116.	When attempting to upload a configuration to an RMA device, a panic occurred.	prod00259399
117.	In an SLB environment with AppShape++ configured, after aging, the TCP::close_type AppShape++ command returned an incorrect value in CLIENT_CLOSED, SERVER_CLOSED events.	prod00259384
118.	In an SLB environment with AppShape++ configured, after aging, TCP::close reset AppShape++ command did not send a reset when called from CLIENT_CLOSED, SERVER_CLOSED events.	prod00259334
119.	Using WBM, in a Layer 7 environment when a content class was deleted and a new one was created, some AX-related configuration errors displayed upon Apply/Revert Apply, leading to some AX traffic processing issues with the content class.	prod00259330

Item	Description	Bug ID
120.	In a VRRP environment, the backup Alteon did not change the source MAC and used the proxy MAC while routing the packet on the backup device.	prod00259179
121.	After generating a Tech Support dump or Techdata, the resource allocation table information (`/maint/debug/rsrcdump`) was missing.	prod00258995
122.	After configuring two interfaces, and not on same network, when a SNMP request was sent to one interface IP address, the response came from another interface.	prod00258932
123.	In an HA environment, when the proxy IP range is configured under the network class and a failover occurs, a GARP was not sent for all the proxy IP addresses in the range. **Note**: The following new command was implemented: `/cfg/l3/ha/nwclgarp ena/dis` If the network class range is huge, then the GARP being sent affects the peers ARP table.	prod00258850
124.	In an SLB environment with server groups, although the mhash configuration is only relevant for the minmisses metric, you could also configure it for other metrics (leastconn and svcleast), causing an Apply in these cases to fail.	prod00258826

AppWall

Item	Description	Bug ID
1.	Could not add a Protected URI in CSRF with a double slash.	DE7213
2.	AppWall did not process an empty file with chunked transfer Encoding.	DE38763
3.	The AppWall “Apply” RESTful API returned a failed code with the HTTPS tunnel in Monitor mode, even though the configuration was saved and applied.	DE38490
4.	Under certain conditions, JSON requests were not parsed correctly	DE38161
5.	The signature update did not update automatically.	DE37014
6.	AppWall identified a JSON parsing failure although the JSON was correct.	DE36913
7.	After a response parsing violation, the transaction ID in the security page did not display	DE36297
8.	The Max Reply header size was enforced to 1024 instead of being unlimited.	DE35625

Item	Description	Bug ID
9.	There was a conflict in the Policy Role importing policy Distribution file.	DE39462
10.	Under certain conditions, trimming failed to process.	DE39460
11.	When AppWall logged events about security violations of the Parameters filter, AppWall presented in the security events all the refinements related to the Web Application contain in the Parameter filter. This caused AppWall to log fewer Security events. Usually AppWall can log up to 350 000 events. The Parameters filter created a security event with a size of 53KB. After ~ 4,700 security events, the Security file reached the limit of 250 MB and AppWall deleted 20% of the database and generated new events in the system log.	DE21382

Fixed in 32.0.1.101

Version 32.0.1.101 includes all field bugs available in version 31.0.5.0.

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

Fixed in 32.0.1.100

Version 32.0.1.100 includes all field bugs available in version 31.0.5.0.

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

Fixed in 32.0.1.0

Item	Description	Bug ID
1.	In a Smart NAT environment, due to the sequence of validations in Global SLB, the warning messages for gmetric were confusing to the user. **Note:** The proximity metric for Inbound Link Load Balancing rules with Smart NAT is not yet supported.	prod00260963
2.	In a Smart NAT environment with Global SLB turned off and LinkProof turned on, the validations related to Smart NAT were skipped and no warning messages were issued. **Note:** Proximity is not yet supported for SmartNAT.	prod00260961
3.	In a DNS environment where DNS responses were received, and with VRRP or HA, performing a configuration sync ended with an FQDN error.	prod00260835
4.	In a VRRP environment, after sync was performed, the server group setting was removed from the peer device.	prod00260807
5.	In WBM, the SLB Viewer user role was allowed to enable/disable physical ports, when this user role should only be able to view Alteon information, SLB statistics, and information, but should not be able to make any configuration changes.	prod00260640
6.	Using WBM, a real server's Description accepted 128 characters while only 31 characters are supported, causing the real server Description not be synced from Active to Standby.	prod00260637
7.	Alerts regarding DUAL PSU failure were generated, but after 6 seconds a notice was issued that the Status was Ok. This issue persisted even after changing to a new PSU.	prod00260596
8.	Using REST API, image upload did not work.	prod00260563
9.	In an SLB environment, when a proxy IP address was defined in a network class, the proxy MAC address was sent with the gateway MAC address to those proxy IP addresses that were not present in the ARP table, causing the applications to fail.	prod00260560
10.	The load time of REST API calls was much slower than the load time in earlier Alteon versions.	prod00260508
11.	In an SLB environment with SSL Hello or HTTPS health checks configured, after upgrading to version 30.2.9.0, real servers configured with these health checks failed.	prod00260484

Item	Description	Bug ID
12.	In an SLB environment with the phash metric, the traffic load was unevenly distributed to real servers with random source IP addresses.	prod00260469
13.	In an Outbound Link Load Balancing environment, LinkProof continued to send dispatching traffic towards WAN links whose bandwidth utilization was above 100%.	prod00260451
14.	You could not paste a geo network class configuration as taken from the configuration file and mandate it to add **None** for the **Country** and **State** fields.	prod00260450
15.	In a LinkProof environment configured with the bandwidth metric, Alteon did not select a WAN link based on the bandwidth metric configured on the DNS hostname and the DNS response included WAN links with the bandwidth overloaded.	prod00260449
16.	Using WBM with a WAN Link configuration, there were discrepancies between the upload bandwidth of the **Per WAN Link IP** and the **Per WAN Link ID**.	prod00260386
17.	Using WBM, when adding an IPv6 NAT IP address with the default prefix, because the IP address was added with prefix 0 instead of 128, the Apply operation failed.	prod00260359
18.	Using WBM or REST API with certificate repository management, you could not overwrite a certificate.	prod00260329
19.	In a BGP environment, after sending a BGP route update after a set of apply operations and a BGP toggle, a panic occurred	prod00260319
20.	In a BGP environment, during BGP route update or when the BGP peer went down during BGP peer "cleanup," the platform hung.	prod00260318
21.	For unknown reasons, an unexpected reboot and a panic occurred.	prod00260317
22.	In an SLB environment, ESP traffic was not passed to the back-end servers.	prod00260296
23.	When using REST API to change the next image to boot, the correct image was not set.	prod00260259
24.	Using CLI, when configuring network classes, there were no validations when geo information was added for a network class as a one line command.	prod00260258

Item	Description	Bug ID
25.	In an SLB environment with delayed binding enabled and APM enabled, because Alteon did not create persistent entries for a few specific clients, Alteon sent the request from a specific Client IP address to a virtual service on Alteon to different real servers, even with the persistent binding Client IP address set on the virtual service.	prod00260096
26.	Due to a large file size, the techdata generation failed with the following message: `Unknown Error`	prod00260082
27.	Using WBM, in an SSL environment, when enabling back-end SSL encryption and the back-end SSL cipher was selected as "user-defined," and then the back-end SSL encryption was disabled, the saved configuration was improper due to a malformed XML.	prod00260025
28.	In an SLB environment with the health check configuration destination set as hostname, the health check failed after performing an apply operation.	prod00259829
29.	When SSH/Telnet connections exceeded the allowed limit, no syslog message generated.	prod00259798
30.	In an AppWall for Alteon VA environment, techdata generation abruptly stopped and a reboot was required.	prod00259693
31.	When Alteon was accessed via SSH, the TCP connections opened for SSH sessions were not closed properly as the client continued to send data and caused stale TCP sessions. This led to SSH access failure to the device.	prod00259684
32.	Using WBM, in **Monitoring > Network > High Availability**, the VRRP labels were incorrect.	prod00259625
33.	In an SLB environment with persistent binding (pbind) configured with a cookie and Client IP, when Layer 4 sessions aged out, the reference count was decremented for the wrong persistent session, causing stale p-sessions.	prod00259580
34.	Using WBM, using $PROTOCOL instead of http:// or https:// in the redirection URL for content rules action redirect or action redirect for a service did not work.	prod00259520
35.	In an SLB environment with FQDN real servers configured, on a virtual server with FQDN real servers, Alteon returned a 503 error even though the real servers were up.	prod00259491

Item	Description	Bug ID
36.	In an HA environment, although synchronization was successful, the backup device issued the following error: `HA: Configuration is not synchronized between the HA devices`	prod00259438
37.	In a Geo proximity configuration, you could not set the country **Niger** in an Alteon GEO network class.	prod00259435
38.	In an SLB environment, when submitting a service (that supports non-standard ports) with a standard port, although the Alteon bank-end returned an error, due to the standard port, Alteon internally configured the corresponding service even after issuing the error without informing the user.	prod00259422
39.	When attempting to upload a configuration to an RMA device, a panic occurred.	prod00259398
40.	In an SLB environment with AppShape++ configured, after aging, the TCP::close_type AppShape++ command returned an incorrect value in CLIENT_CLOSED, SERVER_CLOSED events	prod00259383
41.	In an SLB environment with AppShape++ configured, after aging, TCP::close reset AppShape++ command did not send a reset when called from CLIENT_CLOSED, SERVER_CLOSED events.	prod00259333
42.	Using WBM, in a Layer 7 environment when a content class was deleted and a new one was created, some AX-related configuration errors displayed upon Apply/Revert Apply, leading to some AX traffic processing issues with the content class.	prod00259329
43.	In a VRRP environment, the backup Alteon did not change the source MAC address and used the proxy MAC address while routing the packet on the backup device.	prod00259178
44.	After generating a Tech Support dump or Techdata, the resource allocation table information (/maint/debug/rsrcdump) was missing.	prod00258963
45.	After configuring two interfaces, and not on same network, when a SNMP request was sent to one interface IP address, the response came from another interface.	prod00258925
46.	In an HA environment, when the proxy IP range is configured under the network class and a failover occurs, a GARP was not sent for all the proxy IP addresses in the range. **Note**: The following new command was implemented: `/cfg/l3/ha/nwclgarp ena/dis`	prod00258854

Item	Description	Bug ID
	If the network class range is huge, then the GARP being sent affects the peers ARP table.	
47.	Sometimes you could not configure a management port with an IPv6 address that was identical to one generated by SLAAC.	prod00258853
48.	In an SLB environment with AppShape++ attached to a particular service, although alwayson was disabled, when the service went down, the request was forwarded to AppXcel.	prod00258825
49.	In an SLB environment with IPv4 and IPv6 services and IPv6 PIP configured, a panic occurred.	prod00258580
50.	In an SLB environment with server groups, although the mhash configuration is only relevant for the minmisses metric, you could also configure it for other metrics (leastconn and svcleast), causing an Apply in these cases to fail.	prod00258549
51.	In an AppWall for Alteon environment, when an APSolute Vision syslog came from AppWall through the proxy, and LDAP traffic also used the proxy, Web Authentication via AppWall stopped working.	prod00258525
52.	In an SLB environment with session mirroring enabled for virtual services, the session statistics were incorrect on the backup device compared to the primary device.	prod00258381
53.	For DNS Responder virtual servers with DNS over UDP only, DNS resolution failed.	prod00258374
54.	Using WBM, in an SLB monitoring environment, the real server IP addresses for a server group were displayed incorrectly.	prod00258332
55.	When logging into WBM using TACACS and performing configuration changes and later performing Apply/Save operations, in the audit logs another user ID was recorded instead of the user who logged in.	prod00257825
56.	Parameter security events may cause excessive or high event size.	DE21382
57.	Details button was missing in the Database Security Filter view.	DE25177
58.	Under certain conditions, SSL termination causes SSL session traffic interruptions in passive mode.	DE30899
59.	Vulnerability security refinement in a defined Virtual Directory doesn’t block traffic.	DE31063
60.	Failure in the Blocked Source table (Source Blocking) due to a failure in the Fingerprint hash value.	DE31964

Item	Description	Bug ID
61.	After multiple consecutive memory dumps, log partition becomes full.	DE32927
62.	Database security filter blocks legitimate HTTP requests.	DE33867
63.	Compatibility error message with web browser when using Activity Tracking fingerprint based with Vulnerabilities security filter.	DE34015
64.	Failure in the Database security filter after an upgrade with an AppWall version older than 5.7.2.	DE34070
65.	Refinement error message when trying to refine an HTTP reply size header.	DE34119
66.	Duplicate IP Group and Security WebApplication Role when using the API call with import option for policy distribution.	DE34185 DE34453
67.	Hosts based configurations that contain a wildcard are not taken into consideration.	DE35113
68.	Under certain conditions, Database security refinement disappears.	DE35457
69.	Under certain conditions, a failure occurs with huge HTTP response request.	DE32953
70.	After a failed Apply operation, the tunnel cannot be initialized.	DE21581
71.	Failure occurs in Fast Upload	DE33520
72.	AppWall Management Application failures when refreshing the forensics view with a very high of events	DE30806
73.	Go to Policy button in Forensics view generate an AppWall Management Application exception for RFC Violated Security Events.	DE31200
74.	Failure in the AppWall Management Application occurred after creating a complex REGEX in the security policies settings	DE33872
75.	Wrong IP address in the syslog messages	DE34357

Fixed in 32.0.0.0

Version 32.0.0.0 includes all field bugs available in version 31.0.4.0.

KNOWN LIMITATIONS

Alteon VA Limitations

Item	Description	Bug ID
1.	When rebooting an Alteon VA member of the Alteon VA application cluster on Azure, the member boots with the Alteon VA default license and not with the cluster license. As a workaround, do not reboot a single cluster member but spin up a new member of the scale set that inherits the cluster license, and then terminate the member you intended to reboot.	DE45270
2.	The Alteon VA in Azure Cloud boots by default with a single IP address even if the VM has more NICs. In order to switch to a multiple-IP addresses configuration, disable the singleip mode using the `/c/sys/singleip` command.	DE19291
3.	When running the Alteon VA on Azure, changing from single IP address mode to multiple IP address mode on a pair of Alteons running in HA mode, the public IP address of one of the Alteons might get detached from its virtual machine.	DE40936
4.	For Alteon VA to run in PCI pass-through mode on HP servers with VMware virtualization, ESXi 6.0 or higher is required.	NA
5.	On an Alteon VA on HyperV, the image download is limited for a single image. After you already download an upgrade image, if you need to perform another upgrade, you will need to redeploy the Alteon VA.	DE45334
6.	In some cases, the extraction of the upgrade image can last for long time (around 8 minutes).	DE45183
7.	The reboot time of an Alteon VA on Oracle is significantly longer than in other environments.	DE41852
8.	Alteon VA with more than 3 GB RAM works with DPDK and not TUN/TAP (KVM/VMware). This requires that the host processor is the Intel Westmere architecture or higher (Xeon series 36xx, 56xx, and the Core i7-980X).	N/A
9.	Multiple SPs are not supported by the Alteon VA AWS, Azure (using the virtual network driver), Hyper-V and Open XEN	N/A
10.	When working with DPDK with more than 3 GB RAM (KVM/VMware), the SP CPU usage displays high utilization when monitored by external tools. The Alteon internal SP CPU utilization displays the correct value.	NA

Item	Description	Bug ID
11.	When changing the number of vCPUs of an Alteon VA under KVM, you must modify the VM XML file on the host to utilize the correct number of the queues.	NA
12.	LACP is not supported when working in SR-IOV mode.	NA
13.	A NIC is not recognized by an Alteon VA when adding it after the initial boot of the Alteon VA under VMware on a VM operating in TUN/TAP mode.	NA
14.	When changing the number of vCPUs of an Alteon VA under KVM, you must adjust the CPU pinning for performance optimization.	
15.	BWM is not supported on Alteon VA.	DE137
16.	When installing Alteon VA over KVM, the virtual machine name cannot contain spaces.	DE384
17.	Using Alteon VA, the displayed disk size is smaller than the actual configured disk size, even though Alteon VA utilizes the entire disk size configured for it.	
18.	Disabling TD vCPUs should be done through the CLI and not through WBM.	DE13352
19.	When configuring a second Alteon VA on the same host, and the same NUMA that already has a running Alteon VA does not have enough memory, the first Alteon VA might crash.	DE13928
20.	On an Alteon VA platform, deleting or removing a TD can be performed only through CLI and not through WBM.	DE17038

GEL Limitations

Item	Description	Bug ID
1.	You should return the license to the license server before switching from a local license server to a Cloud license server, and vice versa.	DE36829

WBM Limitations

Item	Description	Bug ID
1.	Using WBM, when configuring port settings for Alteon 9800, it looks like the port speed can be changed, even though this is not possible.	DE45226

Item	Description	Bug ID
2.	Using WBM, incorrect values are displayed for the following counters: • Virtual Service/HTTP/Requests Count • Content Rule Highest Sessions and Total Octets • Virtual Server Total Throughput and CPS	 DE45425 DE45411 DE45166
3.	Using WBM, the Virtual Service "Cipher Usage Statistics FE" table is empty.	DE45108
4.	Using WBM, when configuring a local user on an Alteon in standalone mode, the list of available user roles displays Web Security user roles even though Web Security is not available in standalone mode.	DE37036
5.	When performing a search in the certificate repository, the results display in red even though the certificates are not expired.	DE36046
6.	In the SSL Inspect Wizard, if the Outbound Action is set to Outbound LLB, when attempting to add a Security Devices Flow, internal error occurs. **Workaround**: Deselect the WAN Link Group and then reselect the required group.	DE35159
7.	Using WBM, the backup real server displays as Admin Down in the Service Status View, even though it is Up.	DE43372
8.	Using the SSL Inspection Wizard in WBM, after making configuration changes and performing SAVE/SYNC/REVERT/REVERT APPLY, or switching to a different tab, the following error displays: `REST API Error : 405 Method not found`.	DE36571
9.	Using WBM, when trying to export an Alteon VA configuration that includes private keys with bad a passphrase (for example, one that is too short), although Alteon detects the issue correctly, Alteon cannot export the configuration.	DE31919
10.	Using WBM, during a techdata export, the UI can become unresponsive without any explanatory message.	DE32409
11.	In the SSL Inspection Wizard, when an Inspection Rule is inspected, the following unnecessary message displays in the log: `No Config DE36046uration changes were performed .There is no data to submit`	DE33844
12.	A virtual service with 256 character long ID does not appear in the *Service Status View*.	DE21262

Item	Description	Bug ID
13.	After an idle timeout of a WBM session, if you click **Cancel** instead of entering the credentials in the *Authentication* dialog box, an `incorrect` error message is displayed instead of an `unauthorized` error message.	DE18092
14.	Using WBM, when the Global SLB statistics are cleared, the cleared acknowledgement message displays twice. The duplicate message should be ignored.	DE16456
15.	The *Initial Startup Configuration* does not support configuring tagged VLANs.	
16.	Using WBM, in the *SSL Client Authentication Policy* pane at **Configuration > Application Delivery > SSL > SSL Policy > Client Authentication Policy**, the search in the table does not work on the **Redirect URL on failure** column.	DE16075
17.	Using WBM, when the sync peer is preconfigured and you perform any configuration change to an HTTP/2 policy, the **Sync** button is not automatically highlighted.	DE15480
18.	When editing an SNMPv3 user, you cannot change only the authentication protocol.	DE7889
19.	Using WBM on an Alteon VA platform, you cannot set the IDS port in the real server configuration to a value greater than 2.	DE21296
20.	WBM does not support the Safari browser in MacOS. Instead, you should use Chrome or Firefox.	N/A
21.	In the *STG* monitoring pane, not all values are updated.	prod00214839
22.	Using large configurations, generating a techdata file may cause the MP to reach 100% and WBM disconnects.	prod00212041
23.	Using the *Service Status* view, when the primary real server is down but its backup is up, the backup real server does not display.	prod00211854
24.	Using the *Service Status* view, a real server in *blocking* mode displays as **Up** instead of as **Warning**.	US2349
25.	The **Traffic Contract for Non-IP Traffic** field is not available in the *VLAN configuration* pane.	prod00211136
26.	Using WBM on an Alteon VA platform, in the *VRRP Configuration* pane, the **Advertisement source MAC address mode** field is missing.	prod00216395
27.	WBM has partial support for monitoring and statistics. For full support, use the CLI.	N/A

Item	Description	Bug ID
28.	You cannot renew a server Certificate by changing the **Validation Period**.	prod00218841
29.	Using WBM, the SNMPv3 configuration has the following limitations: • When creating or updating SNMPv3 USM users, the admin password validation is skipped. • When creating SNMPv3 vacmAccess, the security level might not be set properly	prod00204831
30.	In WBM in the *AppShape++ Monitoring* pane, the **Aborts** value is not updated and may display an incorrect value.	prod00204783
31.	In CLI, there is a new display for SP Dynamic Memory usage. In WBM, this display is not available and instead incorrectly shows the old display.	prod00204612
32.	In WBM, DNSSEC has the following limitations: • The DNSSEC responder VIP table may display irrelevant columns such as service and protocol, which can be ignored. • In the *DNS responder VIP Configuration* pane, you must select the virtual Server ID that has DNS TCP and DNS UDP as services. You cannot pre-select the server. The *Virtual Server* pane incorrectly does not display the DNS responder VIP.	prod00204527
33.	In WBM, in the filter configuration, two-way VPN load balancing is missing.	prod00204182
34.	In WBM, the VRRP Virtual Router state displays either **Init**, **Master**, or **Backup** (the **Holdoff** state is missing). To obtain a detailed status, Radware recommends using the CLI.	prod00201915
35.	In WBM, panes in which virtual servers are associated and panes that have virtual server dual lists or select boxes might display DNS responders VIP addresses that are irrelevant. **Workaround**: Ignore or skip these irrelevant VIP addresses.	prod00206278
36.	In WBM, after deleting an object, if the object is associated to other entities, these associations are not automatically removed. You must remove these associations manually so that **Apply** does not fail.	prod00206486
37.	In WBM, the HTTPS body health check configuration can accept only 512 characters, while 1024 characters are allowed.	prod00206608

Item	Description	Bug ID
38.	Enabling or disabling a real server per group is not available using WBM.	prod00206965
39.	Using WBM, when attempting to delete a configuration object and then adding a new object of the same type using the same ID, the **Apply** command must be run between the two operations for the addition to be successful.	prod00201414

Reporting Related Limitations

Item	Description	Bug ID
1.	Summary compression Bytes Saved statistics (/stats/slb/accel/compress/summary) are always shown as zero even when compression is taking place	DE45167
2.	A discrepancy appears between the number of current sessions reported for a filter and the number of sessions for that filter in the session table.	DE35522
3.	The following information is missing from the virtual service JSON (and as a result also from the Application Dashboard): • Statistics on the default action in case of a discard or redirect • Statistic per content rule in case of a redirect action • If the same server group is part of two different content rules in the same application, the statistics in this group appears in the JSON only in one of the content rules.	
4.	In order to check the health of the traffic event log syslog servers do the following: 1. Create a health check script. 2. Set the command to open a UDP connection with the application port a. Set the command to send a string. b. Enable Always Perform Health Check.	DE40881

Item	Description	Bug ID

	3. Attach this health check to each real server in the group.
	For example:
	`/c/slb/advhc/health script_hc SCRIPT`
	`            dest 4 10.171.135.135`
	`            always enabled`
	`/c/slb/advhc/health script_hc SCRIPT/script`
	`            open "514,udp"`
	`            send "HC String"`	

5.	For the HTTP Request Traffic event log, some of the fields have limited length in order to fit a single UDP packet. For more details on the max length of each field, refer to the *Alteon Application Guide*.	N/A
6.	Using the WBM, the default syslog group is not set with the roundrobin metric and by default is not associated to the traffic event policy	DE40966
7.	In the virtual service JSON, the uptime and downtime value of real server is not accurate.	DE37503
8.	A Traffic event log policy that is associated to SSL inspection filter created by the outbound SSL inspection wizard, will be removed on each wizard editing.	

Static NAT Limitations

Item	Description	Bug ID
1.	You can submit a Smart NAT entry with different IP versions (such as IPv4 SNAT and IPv6 WAN link).	DE18862
2.	When adding an IPv6 NAT, in the *Smart NAT* table the local address and NAT address columns display address **0.0.0.0** instead of the IPv6 address.	DE19118, DE20225
3.	Using WBM, an `Invalid mask` error displays when duplicating a dynamic NAT entry	DE44788
4.	Using WBM, when duplicating a No NAT entry and submitting the duplicate entry, an `Invalid IP` error displays.	DE44789

General Limitations

Item	Description	Bug ID
1.	Ciphers CAMELLIA128-SHA, CAMELLIA256-SHA and SEED-SHA do not work on FIPS version	DE40995
2.	FQDN real servers that belong to an unattached group are shown as Up even though they are operationally disabled.	DE45258
3.	When the health check is of type LogExp (logical expression), if the server goes down due to a failure of the "buddy server", when the "buddy server" comes back up, the real server status remains down.	DE31249
4.	When OCSP server certificate validation is enabled, if a host mismatch occurs, SSL handshake fails, even though the Host Mismatch Action is set to Ignore.	DE40742
5.	On a 6420p XL device with a Cavium Nitrox III CNN3550 card, decryption of HTTPS traffic using -M packet capture does not work.	DE36299
6.	SNMP can sometimes stop working on an FIPS image after intensive queries.	DE45382
7.	Synchronization of Session Ticket Encryption Key (STEK) is not working with VRRP Holdoff time.	DE43574
8.	When performing TCP Optimization on traffic processed by filters, you must ensure that filters that have the same Layer 4 parameters also use the same TCP Policy.	DE43521
9.	Outbound SSL Inspection traffic fails when TSO is enabled	DE40097
10.	The /info/slb/sess/real command does not display any results for IPv6 real server, even though sessions exist in the table.	DE44577
11.	The **Handshake only** SSL connection used in non-HTTPS protocols outbound SSL Inspection does not support reuse when TLS version 1.3 is used. Radware recommends to disabling TLS version 1.3 on this internal connection.	DE38869
12.	When outbound SSL inspection for explicit non-HTTPS protocols, such as SMTP is configured, connections to servers that do not support TLS are still counted as SSL connections, and can impact the SSL CPS license enforcement.	DE39332
13.	When performing outbound SSL inspection for FTP, the generated certificate is not cached.	
14.	In an SSL inspection environment with TSO enabled, a traffic drop on the SSL inspection flow occurs.	DE40601

Item	Description	Bug ID
15.	When a real server is overloaded and the health check is edited, although the real server's status changes to Up, it will be counted as a non-active real server. **Workaround**: Operationally ena/dis the server group using the following command: /oper/slb group dis/ena.	DE36774
16.	In an SLB environment, even though the Logical Expression health check includes the “HTTP Health Check with Overload” string, this health check configured as part of a real server or group does not block the Buddy real server. **Note:** This limitation is scheduled to be fixed in the next release.	DE36694
17.	In an SSL environment with valid certificates, sometimes `Certificate expired` messages are displayed.	DE33973
18.	In an HTTP health check with IPv6 and a transparent health check enabled, when the health check fails, the reason is displayed as `Unknown`.	DE33790
19.	Old VPR entries created for a PIP are not removed when switching from Service to Switch HA mode.	DE21032
20.	When a disabled port that is part of a LAG (trunk) is enabled, all the ports in the LAG change their STP states from Listening to Learning and then Forwarding, causing the VLAN to go down and up.	DE24001
21.	The ARP gateway health check fails when **Source MAC learn** is disabled on the gateway VLAN.	DE24508
22.	When configuring the SSL Inspection setup via the SSL Inspection wizard, after performing a **Revert Apply**, the configuration changes are still displayed in diff flash.	DE32129
23.	In an SLB environment, when dbind force proxy enabled for a virtual server, HTTP fragmented traffic fails.	DE32354
24.	The user is locked out after authentication failure. **Limitations**: • The CLI notification for lockout of a user does not display when using an SSH interface connection. • In SSH, Alteon sends two syslog messages for every failed login attempt. In WBM, there is no notification when the user is locked out	DE33285 DE32441 DE33091
25.	When a CA cert is configured as WebManagementCert, and HTTPS traffic is sent, a panic occurs.	DE31510

Item	Description	Bug ID
26.	In an SLB environment using LogExp HC, when the buddy server becomes the backup, the real server that was down due to the buddy still stays down.	DE31249
27.	In an SSL inspection environment with more than one security device flow, the **reverse** setting must be set to **enabled** on all related filters.	
28.	In an SSL inspection environment, if the cache size reaches 100%, traffic failures occur. However, there is a clean mechanism with 10% deletion of the system for an 80% cache size. If the R is being cleaned too quickly (meaning greater than 100Mb per second) traffic failures might still occur.	
29.	In a VRRP environment, centisecond advertisement is not supported. All the intervals must be in seconds. Currently, centiseconds are supported only with IPv6 advertisements and works incorrectly most of the times.	
30.	If you are using different image versions in Master (later than version 30.0.0.0) and Backup (earlier than 30.0.0.0), syslog messages display regarding the mismatch in address count, and advertisement errors are incremented accordingly on the Backup. However, this does not affect the VRRP master-backup scenario. All the functionality is expected to work as before, except for the error counter increment.	
31.	In a high availability configuration a network class used as PIP is not supported well. When multiple PIP addresses are required it is recommended to use PIP of type address.	DE21252
32.	In an SLB environment with a gateway per VLAN configured in a network without a PIP configuration, Alteon forwards server returned packets to clients tagged with different VLAN IDs, causing packets to be discarded by the gateways. Radware recommends setting the **Return to source MAC** value for a relevant virtual service using the **rtsrcmac ena** command, which was introduced in version 30.1.	prod00246941
33.	LACP does not work when MSTP is enabled.	DE13199
34.	In high availability environment, the configuration synchronization failure reason does not appear on the master device when the IPv6 peer IP address is used. **Workaround**: Use the IPv4 peer IP address.	DE19918

Item	Description	Bug ID
35.	Alteon does not forward BPDUs between Cisco and Juniper when the VLANs are in different STGs and the STG is set to **off**.	DE19690
36.	In an SLB environment, Layer 7 Direct Server Return (DSR) with FTP does not work.	DE17741
37.	In a BGP environment where Floating IP advertisement is used, when you disable or delete a floating/VR IP address, BGP routes are not updated.	DE16514
38.	In a VRRP unicast environment on an Alteon VA platform (KVM), with Direct Access Mode (DAM) disabled, matrix and mirror enabled, after backup the mirrored sessions are not distributed to all SPs.	DE16513
39.	In a VRRP unicast environment with TSO enabled on the backup and synced to the backup, when the backup becomes the master, even though the TSO enable is synced, manual reboot is required for TSO to work.	DE15820
40.	When performing outbound link load balancing in an IP gateway environment (different IP versions used on LAN and WAN), proximity checks are not initialized.	
41.	When a backup device with FQDN servers comes up after reboot, no ephemeral real servers are present.	
42.	GSLB Proxy Redirection for an HTTPS or SSL service does not work when SSL ID persistency is configured on a virtual service.	DE13265
43.	Using GSLB, availability priority set for a VIP on a remote Alteon is not taken into consideration by the local Alteon.	DE13545
44.	Alteon sends beacons to the APM on the default port *only*.	DE12551
45.	When using a network class for PIP, the range of the network class cannot overlap with the VIP IP address.	DE2065
46.	When the CDP server is not accessible and the CDP **Interval** value is reached, the current CDP is deleted even though it is still valid.	DE2168
47.	Return to the source MAC address only works when Direct Access Mode (DAM) is enabled.	DE792
48.	IPv6 DSR DNS load balancing does not work.	DE2284
49.	The IPv6 DNS client does not work.	DE802

Item	Description	Bug ID
50.	For a virtual service, the insert cookie configuration should be performed either by setting the persistency mode to **insert cookie**, or by using an AppShape++ script with a persistent cookie. Both settings should not be performed together on the same service.	DE881
51.	When audit is enabled on a platform and an audit message contains more than 1000 characters, the message is truncated and the audit may not display all configuration change details in the message.	prod00223697
52.	Some audit messages related to enable/disable might display as deleted when the field is actually being modified. Example command: `/c/sys/access/https/https d` This may display if HTTPS was deleted as it was changed from its default.	prod00223516
53.	Using an AppShape++ script, the UDP::response does not work in SERVER_DATA for DNS.	prod00221228
54.	Under high traffic load, terminated sessions are not removed from the backup platform mirror table.	prod00213645
55.	The IP interface of a VRRP group that includes IPv4 VRs cannot be configured using IPv6.	N/A
56.	While retrieving techdata, the MP CPU utilization may reach 100%, making the management interface inaccessible.	prod00212041
57.	GSLB Proxy Redirection does not work for IPv6 traffic.	prod00215426
58.	GSLB Client Proximity does not work when HTTP traffic is processed in forceproxy mode.	prod00215327
59.	Statistics of IPv6 virtual servers are incorrect on the backup platform.	prod00217544
60.	When activating traffic capture on a platform that is under high load and high SP CPU, failover to the backup platform may occur.	prod00210096
61.	Outbound SIP traffic works only for a standard 5060 port.	prod00217348
62.	SSL decryption of an SSL capture is not supported for IPv6 traffic.	prod00217115
63.	Using redirect filtering, Layer 7 pattern match does not work when delayed binding is enabled.	prod00212657
64.	The OSPF MD5 key is displayed in a config dump as clear text instead of encrypted.	prod00214646

Item	Description	Bug ID
65.	In IPv6 filters, when delayed binding is enabled internally, it functions as forceproxy.	prod00214645
66.	For a VR group that includes both IPv4 and IPv6 VRs, the advertisements are sent only via IPv6 interfaces when the method is unicast.	prod00214159
67.	No warning message is displayed when APM is enabled on a service with no APM license.	prod00213522
68.	When all persistent entries in the Dynamic Data Store (persistence via AppShape++) are purged, sometimes new persistent entries are not mirrored to the backup platform. Radware recommends also purging entries from the backup platform.	prod00212945
69.	If the real server has the description configured, the real server description is shown instead of the real IP address under `/info/slb/cookie`.	prod00220874
70.	When a buddy server does not belong to any service, after **Apply** it and the real server go down for a short time.	prod00212727
71.	When two IPv6 interfaces are configured on the same VLAN and they both have VRs configured, only one interface is in status "up (preferred)", while the other is in status "up (tentative)". **Workaround**: Disable and then enable the interface.	prod00216479
72.	Uploading the configuration taken from a techdata file is not supported. After uploading such a configuration, after rebooting the "bad syntax" error is issued, and most of the configuration is ignored.	prod00216036
73.	The default share value for `/cfg/l3/vrrp/group` and `/cfg/l3/vrrp/vr` is **disabled** in Alteon versions 26.8 and 28.0, and **enabled** starting with version 28.1. After upgrading from versions 26.8 or 28.0 to version 28.1 or later, if the **share** parameter had a default value, you must disable it manually.	prod00177054
74.	The BWM module is not working properly.	prod00190470
75.	For IPv6 virtual routers (VRs), only VRIDs up to 255 can be used.	prod00191837
76.	HTTP Layer 7 processing using legacy delayed binding in enabled mode does not work with fragmented traffic.	prod00198986

Item	Description	Bug ID
77.	SSL ID persistency is not supported in force proxy mode. When upgrading from version 28.1.*x* to 29.5.0.0, if there are virtual services configured with SSL ID persistency and force proxy mode, configuration apply fails until either SSL ID persistency is disabled or force proxy mode is deactivated. Radware recommends performing this before upgrade.	prod00200668
78.	A GSLB configuration with cookie-based persistency between sites does not work for IPv6 requests.	prod00201333
79.	The incorrect APM license value is reported to APSolute Vision.	prod00201942
80.	On an HTTPS service with a non-standard service port and server port 443, in force-proxy mode, real server IP leakage is observed. **Workaround**: Add a proxy IP address or change delayed binding to enabled mode.	prod00202219
81.	When a new configuration is applied, there might be "server up" messages for servers that are not attached to any VIP.	prod00202693
82.	If more than 256 virtual routers (VRs) are configured on the same IP interface, flipping between master and backup device can occur.	prod00202886
83.	Sometimes persistent sessions exist for twice the persistency timeout value.	prod00203494
84.	When processing traffic via a redirect or NAT filter, if an ICMP type 3 code 4 message arrives from the client-side, it is not properly processed.	prod00203850, prod00203888
85.	X-Forwarded-For can be enabled for an HTTPS service without SSL offload (requires delayed binding enabled), even though it cannot be performed.	prod00204113
86.	MP Utilization data sent to the Device Performance Monitoring module is sometimes incorrect.	prod00204922
87.	Generation of a 4096 key size may take up to 30 seconds. During this time, the CPU utilization may reach 100 %.	prod00204939
88.	Trying to upload a very large capture file via FTP/TFTP fails.	prod00205038
89.	Some of the cache statistics are incorrect: • The number of new cached bytes is always reported as 0. • The new cached bytes rate is incorrect. The cached objects average size counters are incorrect.	prod00207290, prod00207297, prod00207299

Item	Description	Bug ID
90.	HTTP/2 Gateway is not supported in conjunction with AppShape++.	
91.	A real server does not accept traffic even though the real server is in the UP state after a 'Shut' real server.	DE37040
92.	Updating a Health check when a real server is Overloaded- keeps the real server inactive.	DE36774
93.	Flapping a service in T2 causes the local real server to go down in T1 permanently.	DE35827

Outbound SSL Inspection VRM Limitations

Item	Description	Bug ID
1.	The Outbound SSL Inspection VRM Dashboard cannot be used when setting the outbound SSL inspection deployment using the wizard.	DE41461
2.	The `Timelion error:Cannot read property` error displays when accessing the SSL Inspection dashboard when for the selected timeframe there is no data in the SSL HS and dynamic certificate storage graphs.(this also occurs on the backup device). This message can be ignored.	DE35752
3.	Enabling the report filter flag for the first time on existing outbound SSL Inspection filters (with traffic running) results in a huge spike for the traffic statistics. The same spike occurs when the filter report flag is set to **ena > dis > ena** while traffic is running	DE35884
4.	The `Service temporarily unavailable` message displays when accessing the dashboard after the APSolute Vision session timed out (DE35646). Gaps might be seen in graph with stress traffic.	DE35251
5.	Clicking on any donut chart (Application by bandwidth, Key exchange, SSL version charts) applies an auto-filter on the dashboard page, causing some charts to display empty. Radware recommends not to use this auto-filter by clicking the donuts.	DE35573
6.	Some SSL Inspection dashboards may display empty. In many cases, this is due to a timing issue between Alteon and APSolute Vision. **Workaround**: Configure Alteon with a time zone (in addition to NTP).	N/A

FastView Limitations

Item	Description	Bug ID
1.	When using FastView for an HTTPS service in conjunction with **Pass SSL Information to Backend Servers**, Radware recommends using the default header names. The FastView fetcher uses default SSL headers to indicate front-end SSL, and not the user-defined custom headers.	DE6100
2.	Using FastView with deferral for images, the images are not displayed. This is scheduled to be fixed in version 31.0.1.0.	DE13859

AppWall Limitations

Item	Description	Bug ID
1.	The AppWall Authentication Gateway and SSO may not be backward-compatible with previous versions. Customers using the Authentication Gateway should contact Radware Technical Support prior to upgrading.	
2.	Under the condition where multiple Database Security Filter refinements match on the same request, only the first refinement is considered. This is relevant when a refinement containing regular expression is created.	
3.	For AppWall integrated in Alteon, when security policies are configured using role-based Authentication policies, the Multiplexing functionality in Alteon must be deactivated.	
4.	When AppWall logs events about security violations to the Parameters filter, all the refinements related to the Web Application contained in the Parameter filter are displayed in the security events. This causes AppWall to log fewer security events. Usually, AppWall can log up to 350,000 events; the Parameters filter creates a security event with a size of 53 KB. After ~ 4,700 security events, the Security file reaches the limit of 250 MB and AppWall deletes 20% of the database and generates new events in the system log.	
5.	AppWall does not support uploading files bigger than 200M (not related to the FileUpload filter).	

Item	Description	Bug ID
6.	For AppWall integrated in Alteon, when Auto Discovery is configured with the default configuration, 8 CUs are allocated to AppWall. Auto Discovery uses 6 CUs. This results in high CPU consumptions. Radware recommends reconfiguring the number of CUs.	
7.	The AppWall hostname cannot contain the underscore (_) symbol as a result of a limitation on all recent Linux distributions. The upgrade process will succeed but will generated a warning. Make sure you rename the host to avoid future upgrade failures.	
8.	In the *Authentication GW* panes, in some rare cases when only the authentication GW license is installed, more filters display than are defined. **Workaround:** For authentication GW functionality, use only the **Allowlist** and **Pathblocking** filters.	DE1929
9.	In some rare cases, the request data in the *Forensics* table does not display information	DE1373
10.	Using WBM in the Firefox Mozilla browser with an HTTPS connection, it might take a very long time to open the applet for Alteon.	DE20462
11.	When using the HTTP timers in the AppWall Tunnel configuration, the TCP timers from Alteon can override the HTTP timers' values.	
12.	In an AppWall integrated HA environment with filter changes in AppWall, after running the sync, the changes are not synced.	DE24995
13.	When importing a configuration backup from an older version, some host settings (such as kerberos.cfg) are missing.	DE24223
14.	When the Authentication Gateway is configured, file upload HTTP POST requests with uploaded files larger than 20 MB fails.	DE19356
15.	Syslog messages sent by AppWall are always sent with facility "Local 6". Now, the events facility is based on the Alteon configuration.	DE21431
16.	Dashboard tunnels traffic activity graphs are not displaying historical data.	DE22455
17.	When processing thousands of security violations per second that are generating security logs, in certain configurations a failure occurs.	DE23791

Item	Description	Bug ID
18.	When a parameter is mapped to both explicit data base security filter refinement and to a regular expression refinement, the order of the refinements enforcements is inconsistent. **Workaround**: In this version, an explicit parameter name refinement will be merged into a regular expression based refinement to avoid the inconsistency and to simplify configuration maintenance.	DE22782, DE21308
19.	After a parameter is mapped to multiple regular expression-based refinements of the data base security filter, mapping of a parameter is not deterministic. **Workaround**: This issue is resolved by merging the regular expression refinements.	DE22863 DE22744
20.	When initially enabled, the session security filter generates a high rate of security violation logs because the cookies that were sent to HTTP clients before enabling the filter were not protected. **Workaround**: In this version, the session security filter identifies those cookies as not validated. To avoid a high rate of false positives, the session security filter is not enabled by default. A high rate of security violation logs may lead to missing Geolocation data in the *Forensics* view because of high processing requirements.	DE22410
21.	When using the HTTP timers in the AppWall Tunnel configuration, the TCP timers from Alteon can override the HTTP timers' values.	
22.	For AppWall integrated in Alteon, when Auto Discovery is configured with the default configuration, 8 CUs are allocated to AppWall. Auto Discovery uses 6 CUs. This results in high CPU consumptions. Radware recommends reconfiguring the number of CUs.	
23.	For AppWall integrated in Alteon, the limit of the concurrent established connection has been removed. AppWall can process more than 64K CEC. The limit depends on the resources availability.	
24.	During the import process of a tunnel policy distribution, if the KVS Policy Role exist with the same name in the current AppWall Security Policy, the current AppWall Security Policy will be replaced by the existing Role definition in the KVS.	

Item	Description	Bug ID
25.	For AppWall integrated in Alteon, when security policies are configured using role-based Authentication policies, the Multiplexing functionality in Alteon must be deactivated.	

Alteon Management via APSolute Vision Limitations

Item	Description	Bug ID
1.	Using APSolute Vision version 3.60 with this Alteon version, the import/export from the *Operations* menu does not work. **Workaround**: Navigate to the individual pages for the export/import of a specific configuration (for example), or upgrade to APSolute Vision version 3.70.	prod00246805
2.	Using APSolute Vision to manage FastView on Alteon, the controls in the Treatment Set screens do not work properly.	DE14140, DE13816
3.	Using APSolute Vision, the following configuration error displays: `mib: gslbStatRemEnhRealServerIpVer  not found`.	DE36993

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*
- *Alteon Troubleshooting 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