radware

AlteonOS

RELEASE NOTES

Version 32.2.14.0
September 30, 2022

TABLE OF CONTENTS

CONTENT

Radware announces the release of AlteonOS version 32.2.14.0. These release notes describe new and changed features introduced in this version on top of version 32.2.13.0.

RELEASE SUMMARY

Release Date: September 30, 2022

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

SUPPORTED PLATFORMS AND MODULES

This version is supported by the following platforms:

- 4208, 4208S
- 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

  Note: Memory usage has increased on Alteon versions 31.0.0.0 and later. Therefore, a 6420 platform with a default memory of 32 GB reaches 100% SP utilization very quickly. To use this version of Alteon on a 6420 platform, upgrade the RAM memory to at least 64 GB (factory installed or FUU).
- 7612S, 7612SL
- 7220S, 7220SL
- 8420, 8420 XL/Extreme, 8420S, 8420SL
- 8820, 8820 XL/Extreme, 8820S, 8820SL
- 9800, 9800S, 9800SL
- Alteon VA running on VMware ESXi 6.0, 6.5, 6.7, 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 32.2.14.0 is supported by APSolute Vision version 4.10.100 and later.

Integrated AppWall version: 7.6.17.0

OpenSSL version:

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

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 28.*x*, 29.*x,* 30.x, 31.x and 32.x.

General upgrade instructions are found in the *Alteon Installation and Maintenance Guide*.

Before Upgrade – Important!

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

The following table describes the specific upgrade path from each version to 32.2.14.0:

Current Version	Upgrade Path	Notes
28.*x*	> 29.0.9.0 > 30.5.3.0 > this version	As an alternative, you can upgrade directly to 32.2.14.0 using the recovery process. **Note**: You must save the configuration before starting this process.
29.0.*x* (*x*=<8)	> 29.0.9.0 > 30.5.3.0 > this version	
29.0.*x* (*x* > 8)	> 30.5.3.0 > this version	
29.5.*x* (*x*=<7)	> 29.5.8.0 > 30.5.3.0 > this version	
29.5.*x* (*x*>7)	> 30.5.3.0 > this version	
30.*x* =< 30.5.2.0	> 30.5.3.0 > this version	
30.*x* > 30.5.2.0	Direct upgrade to this version	
31.*x*	Direct upgrade to this version	
32.*x*	Direct upgrade to this version	

General Considerations

- Hypervisors (ADC-VX) running a certain version (for example, 31.0) only support vADCs that run the same version or later.

Downgrade

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

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

WHAT'S NEW IN 32.2.14.0

None

WHAT'S NEW IN 32.2.13.0

Integrated AppWall

Signature Operation Mode

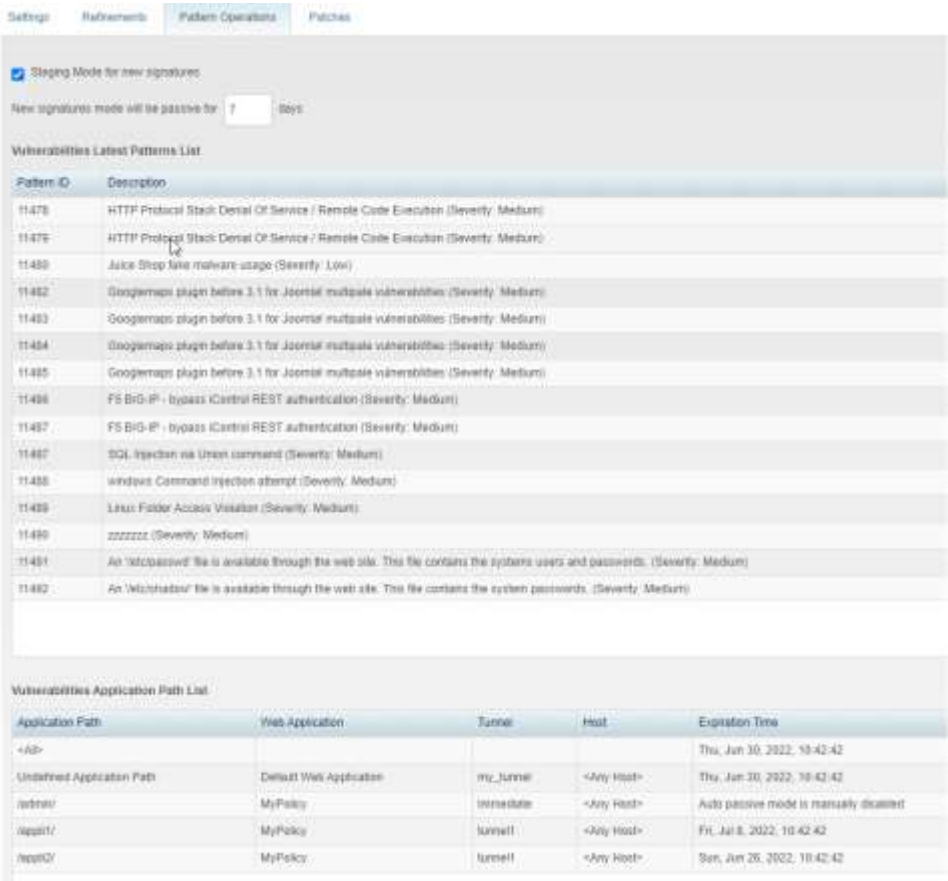
When AppWall retrieves an updated signature file (automatically or manually), it contains new signatures. Sometimes, these new signatures can generate false positives and block legitimate customer traffic.

In order not to block legitimate traffic, the new signatures will automatically be in *Passive* mode during a configurable period of time (7 days by default). There is no impact on the existing configuration (what is refined, stay refined). Only the new signatures are in *Passive* mode.

During the configurable period of time, the security engineer can evaluate the new signatures and eventually refine them. At the end of the time period, the new signatures automatically move from *Passive* to *Active* mode. This can be configured globally (all Application Paths will inherit from the global settings) or specifically per Application Path.

Signature Operation Mode can be turned off, globally or on a specific Application Path, if the customer wants to be protected immediately, after the signature update, if the application is exposed to a 0-day attack.

Note: Signature Operation Mode is available for Database Security filters and Vulnerabilities Security filter.



WebSocket

In this version, a few more options to configure WebSocket protection were added:

- Per Application Path: You can define if WebSocket protection is Active, Passive or Bypass.
- For the WebSocket payload, we can combine the structured and unstructured format (Text, JSON and XML can be combined with Binary).

Server-Side Request Forgery

In this version we reinforced SSRF protection. We complete the security coverage with more patterns.

Previously, we were only able to refine a URI or domain name. We can now also refine a specific parameter name.

We added also new REST API of the Unvalidated Redirect module in order to configure the pattern list related to LFI, RFI and SSRF.

WHAT'S NEW IN 32.2.12.0

Integrated AppWall

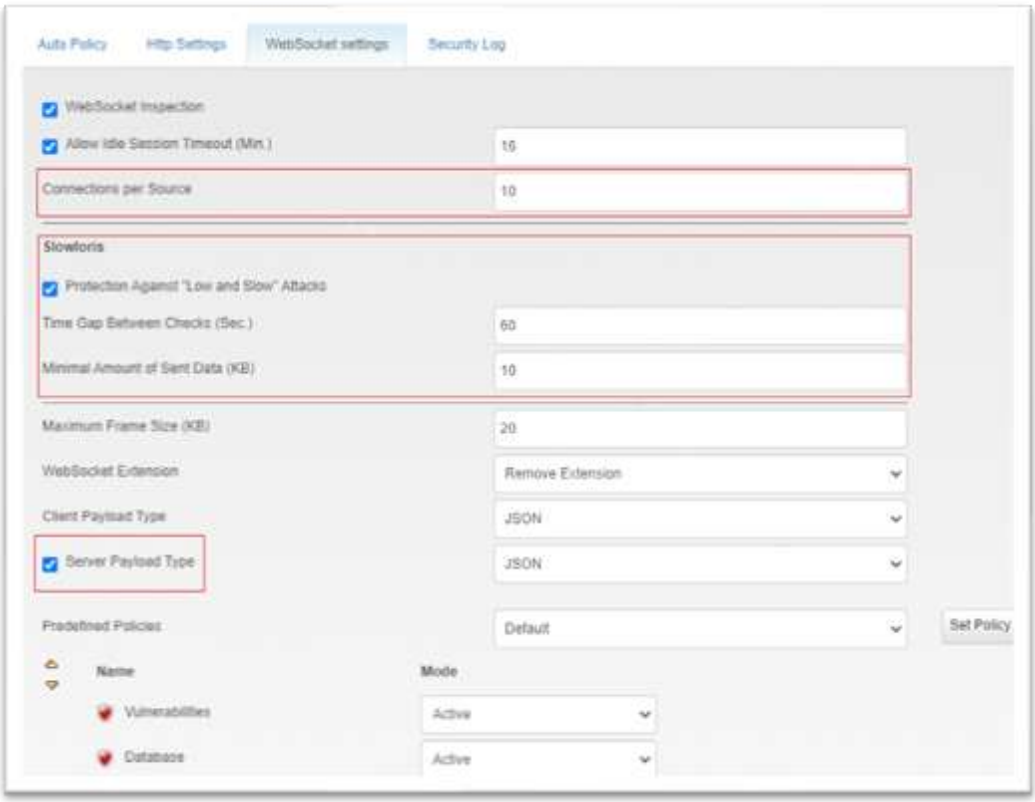
WebSocket

In the previous version support of the WebSocket protocol was introduced. In this version, the following WebSocket support was added:

- **Connection per source** - where the maximum number of connections that a source can open to a specific WebSocket application is defined.
- **Low & Slow attack mitigation** where we configure the following:
  - Time Gap Between Checks - The time span during which the AppWall is counting the traffic rate on the inspected connection.
  - Minimal traffic volume threshold to trigger protection.

Two minor changes were also introduced:

- The enforcement of the WebSocket server response payload type can be optional.
- When the WebSocket is in "block" mode in the Tunnel configuration, the client connection is closed with a Security Page and not with a TCP reset.

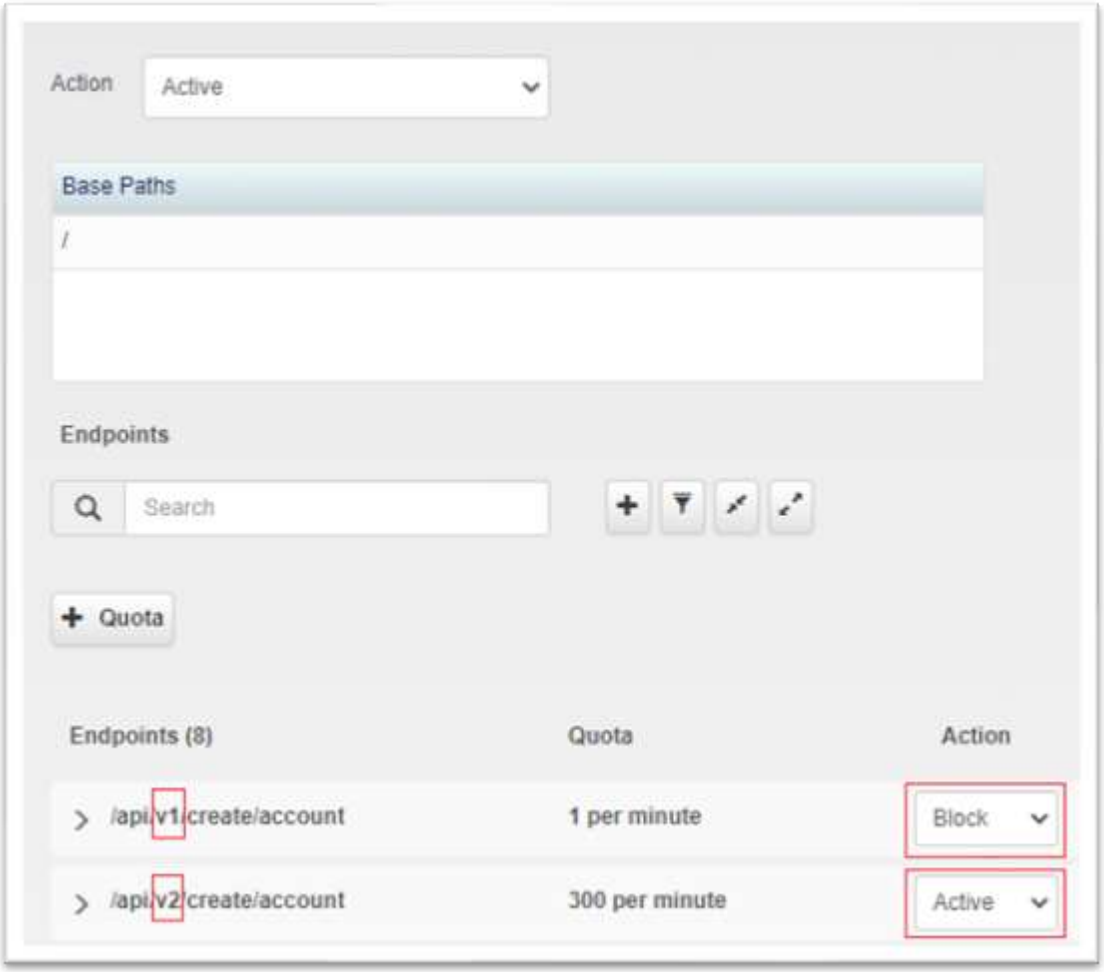


API Security

In the API Security module, a new "Block" action for the endpoint's schema enforcement is added.

Previously, "Active", "Passive" and "Bypass" actions were supported. The new "Block" action will immediately block the client request. It manages use cases such as:

- When an endpoint is deprecated (for example, because of a bug) and the customer does not want any request to reach the API service, the deprecated endpoint can be in Block mode where the new endpoint can be in Active mode
- When an endpoint presents some security risks (for example, data leakage, 0-days attacks, injections) and the customer wants to immediately block any incoming request to this endpoint until it is fixed.



Advanced Base64 Attack in HTTP Headers

Following previous deliveries related to Base64 Heuristic Detection and Multiple Encoded attacks, in this version, we added support for multiple-encoded attacks in the HTTP header, such as harmful Injections, with the AppWall Database filter.

WHAT'S NEW IN 32.2.11.0

SameSite Cookie Attribute

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

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

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

Alteon now allows the following:

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

Integrated AppWall

WebSocket

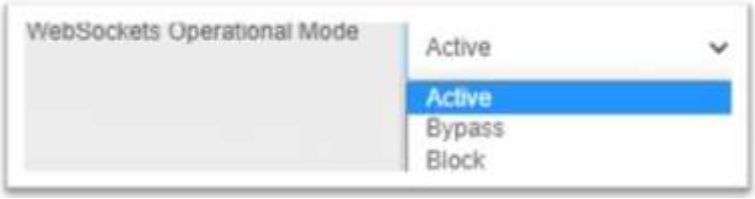
In this version, WebSocket protocol support is added.

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

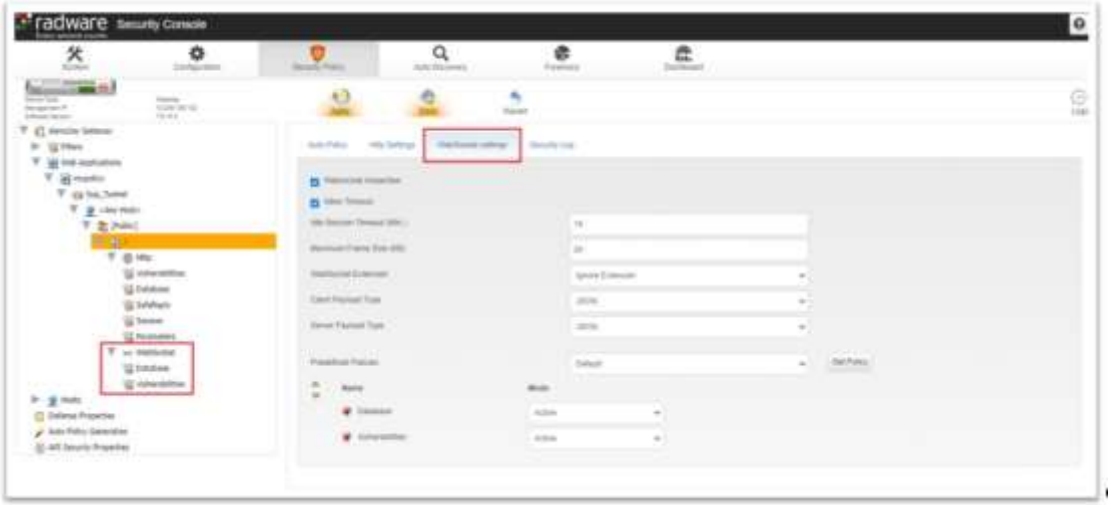
The WebSocket protocol enables interaction between a client application and a web server with lower overhead, facilitating real-time data transfer from and to the server. This is made possible by providing a standardized way for the server to send content to the client without being first requested by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

AppWall WebSocket support:

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



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



Base64 Heuristic Detection

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

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

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

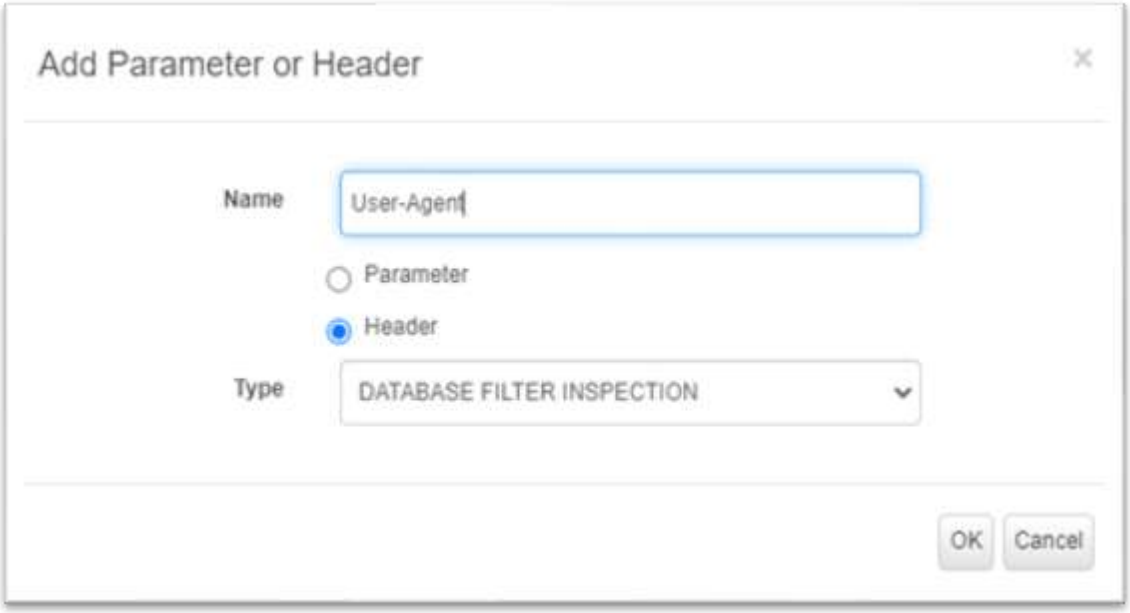
Multiple Encoded Attacks

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

HTTP Header Inspection with the Database Filter

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

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



Maximum Active Connection Alert

AppWall can limit the number of connections for every AppWall tunnel (referred to as SECWA in the Alteon WAF). When AppWall receives the maximum limit of active connection in a tunnel, no new connections are opened.
In this version, we added the option to configure a threshold (in percentage) of active connections. When the threshold is reached, an alert is sent in the Forensics Security events before the maximum number of allowed active connections is reached and the connections queue gets completely full.

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

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

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

WHAT'S NEW IN 32.2.10.0

Integrated AppWall

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

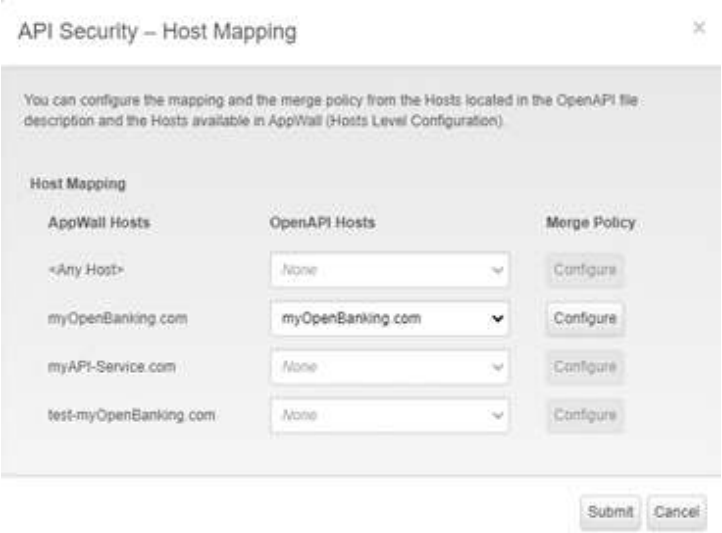
For example, the attacker can encode a parameter value with Base64 multiple times that contains an SQL Injection.

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

WHAT'S NEW IN 32.2.9.0

AppWall Features

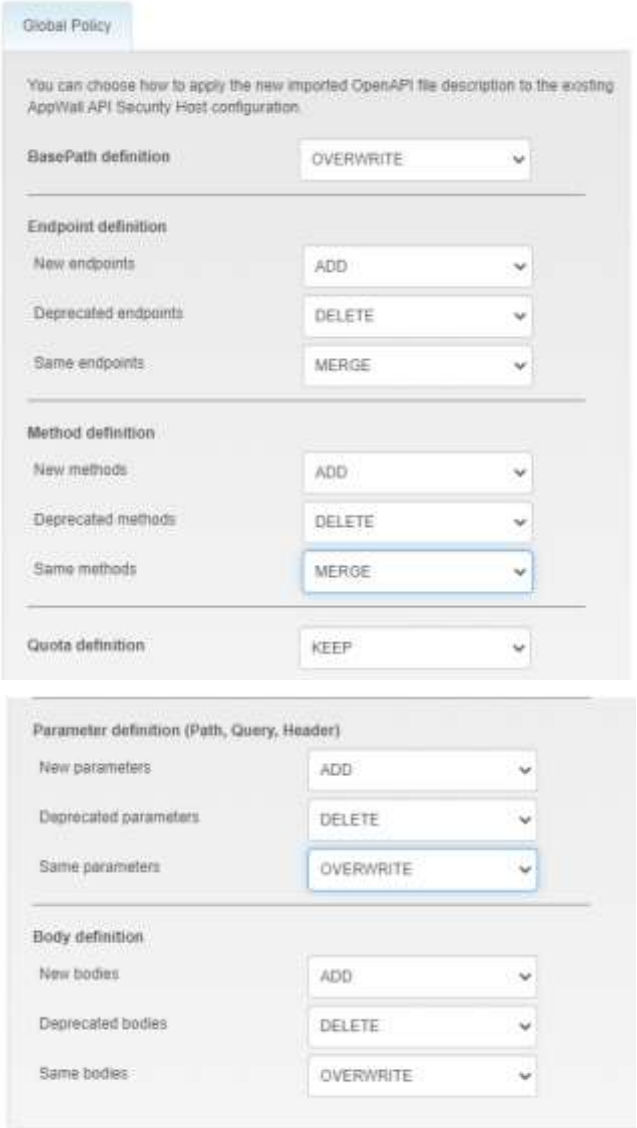
1. API Security hosts protection has been updated with two new functionalities:
   a. **Host Mapping**: During the process of uploading a new OpenAPI file, it is now possible to choose to which AppWall Hosts to attach the OpenAPI file definition. An explicit use case is when DevOps usually assesses the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



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

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

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



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

WHAT'S NEW IN 32.2.8.0

None

WHAT'S NEW IN 32.2.7.0

DNS Nameserver (NS) Records Support

For security reasons, some DNS cache servers require authoritative nameservers to answer NS queries for the domains for which it is authoritative.

Alteon now answers such queries for the domains for which it is authoritative if the nameservers were configured for that domain. In addition, if the nameserver hostname is in the same domain as the hostname for which the NS query arrived, and the user specified an IPv4 and/or IPv6 address for the nameservers, the answer will also include A and/or AAAA records for each nameserver in the ADDITIONAL section (glue records).

The following configuration is required for the GSLB/LinkProof participating Alteons:

- **Define Nameserver Group/s** – A list of hostnames that serve as nameservers for the same hostnames. For each nameserver, you can also define IPv4 and IPv6 addresses.
- When configuring a hostname, either via a virtual service or a DNS Rule, attach the relevant nameserver group.

NFR ID: 200327-000083

Secure Password Policy

Starting with this version, the administrator can enforce password strengths criteria for the passwords of local users (both predefined and user-defined).

When password strength is configured, it is applied to passwords of newly created users as well as password changes for existing users.

The password strength criteria are not applied to the default predefined Admin user.

NFR ID: 200227-000015

WHAT'S NEW IN 32.2.6.0

Integrated AppWall – API Security

The usage of APIs in Web applications and services is on the rise, and security concerns and needs are not entirely covered by traditional protections in WAF. AppWall's API security module provides protections that cover security concerns and the need for working with APIs.

API Security can be automatically configured by importing an OpenAPI document to AppWall. AppWall automatically updates the API security module for hosts configured under the Host Level Configuration that match the ones defined in the OpenAPI document. All API endpoints will be added to the endpoint list of the host, allowing API requests to these endpoints automatically. API requests to the allowed endpoints are still scanned by AppWall's security protections for embedded attacks.

Alteon VA – VMware ESXi 7.0 Support

Starting with this version, Alteon VA supports the recently released VMware ESXI version 7.0 on top of the earlier version.

SHA2 and AES-256 Support for SNMPv3

Starting with this version, the following SNMPv3 support was added for stronger security

- **authentication type** – Support for SHA256
- **privacy type** – Support for AES256

NFR ID: prod00268561

TCP SACK Control on Management Port

Enabling the TCP SACK improves the performance on management ports. However, this can expose the device to the following vulnerabilities:

- CVE-2019-11477
- CVE-2019-11478

For additional information about these vulnerabilities. please access the Radware Knowledge Base.

TCP SACK can be enabled/disabled via CLI using the following command (enabled by default):

```
/maint/debug/tcpsack  <ena/dis>
```

This requires a reboot

This feature is relevant on following Alteon platforms: 5208, 5224, 6420, 8420.

This feature is also available for versions 31.0.14.0, 32.2.6.0, 32.4.4.0.

WHAT'S NEW IN 32.2.5.0

Synchronization of Cluster Persistent Data (first introduced in version 32.2.4.60)

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

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

Note: Before configuring cluster persistent data synchronization:

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

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

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

NFR ID: 190911-000454 (prod00272010)

WHAT'S NEW IN 32.2.4.0

This section describes the new features and components introduced in this version on top of Alteon version 32.2.3.50.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.2.4.0.

High Availability Enhancements

New tracking options (VIP and server group) were added to Alteon High Availability capability. These options are not available in the legacy VRRP mode.

In this version, these new options are configurable via CLI only:

- **VIP Tracking**

A user can mark the VIPs to track, and when any of these VIPs is unavailable (at least one of its services is unavailable) a failover will occur.

The user has the option to determine the criteria for the VIP to fail over according to its services, meaning to limit the failover only if specific services of that virtual services are not available.

NFR ID: 191006-000023

- **Group Tracking**

  A user can select a real servers group to track, and when that group is not available a failover will occur.

  A group is considered as not available according to the number of available real servers as configured for the Group status threshold parameters.

  Radware recommends using the group tacking option mainly when working with filters, where a virtual service is not relevant, and as result the VIP tracking option cannot be used.

  NFR ID: 190911-000428 (prod00269501)

AppShape++ Enhancements

The following AppShape++ capabilities were added:

- The **httponly** flag is added to the **persist cookie insert** and **persist cookie rewrite** commands. This flag informs the browser not to display the cookie through client-side scripts (document.cookie and others).

  NFR ID: 190911-000550 (prod00271354)

- The 308 response code option is added to **http::redirect** command. 308 is the Permanent Redirect response code and it indicates that the resource requested has been definitively moved to the URL given by the Location headers.

  NFR ID: 190925-000125 (prod00253762)

AppWall Enhancements

Anti-Scraping Thresholds per URI

Anti-Scraping now supports defining thresholds per URI. In Anti-Scraping mode, the Activity Tracking module counts the HTTP transaction rate to the defined application scope (domain/page) per user per second. You can define different thresholds and different blocking time settings for each (up to 30) protected URI.

Forensics Filters

Forensics events can now be filtered by: URI, Parameter Name, and Refinements. Filtering by refinements display either refined events or events not refined.

Note: When upgrading from previous versions, filtering by 'Refined' includes only new events generated after the upgrade. Filtering 'Not Refined" events includes all events from before the upgrade, refined and not. Radware advises to use this filter together with a time range filter.

WHAT'S NEW IN 32.2.3.0

This section describes the new features and components introduced in this version on top of Alteon version 32.2.2.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.2.3.0.

Smart Session Table Adjustment

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

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

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

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

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

Platform	RAM Size	100% Session Table	50% Session Table	Free Memory Saving (free memory improvement) *
4208	8GB	6M	3M	706 MB (+53%)
5208	16GB	12M	6M	1,358 MB (+34%)
5424	32GB	22M	11M	2,482 MB (+24%)
5820	32GB	22M	11M	2,482 MB (+24%)
6024	32GB	20M	10M	2,260 MB (+19%)
6420	32GB	46M	23M	4,894 MB (+210%)
7612	96GB	46M	23M	4,603 MB (+11%)
7220	96GB	46M	23M	4,603 MB (+11%)
8420	128GB	76M	38M	8,596 MB (+16%)
9800	192GB	140M	70M	7,901 MB (+8%)

*Based on the platform's default RAM size

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

```
/c/slb/adv/sesscap

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

New SLB Metric – Highest Random Weights (HRW)

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

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

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

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

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

NFR ID: prod00272235

WHAT'S NEW IN 32.2.2.0

This section describes the new features and components introduced in this version on top of Alteon version 32.2.1.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.2.2.0.

Documentation in HTML Format

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

Management Login with SSH Key

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

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

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

OpenSSL Upgrade

The OpenSSL version is updated in this release as follows:

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

OCSP Multiple Servers

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

WHAT'S NEW IN 32.2.1.0

This section describes the new features and components introduced in this version on top of Alteon version 32.2.0.0.

For more details on all features described here, see the *Alteon Application Guide* and the *Alteon Command Reference* for AlteonOS version 32.2.1.0.

Virtual Service Traffic Events

Traffic events are now also available for virtual services. These traffic events provide a detailed connection and transaction-based view of the traffic processed by virtual services. The traffic events enable you to quickly identify problems and discover their root cause.

The events are in CEF format and can be integrated with third-party SIEM products.

The following type of traffic events can be sent:

- SSL connection events
- SSL handshake failure events
- HTTP transaction events (request and response)
- Layer 4 connection events

The traffic events are sent to a specified group of syslog servers over the UDP/TCP/TLS protocol (via data ports).

Note: Traffic event logging is available with the Perform subscription and Secure subscription.

To perform traffic event logging per virtual service, do the following:

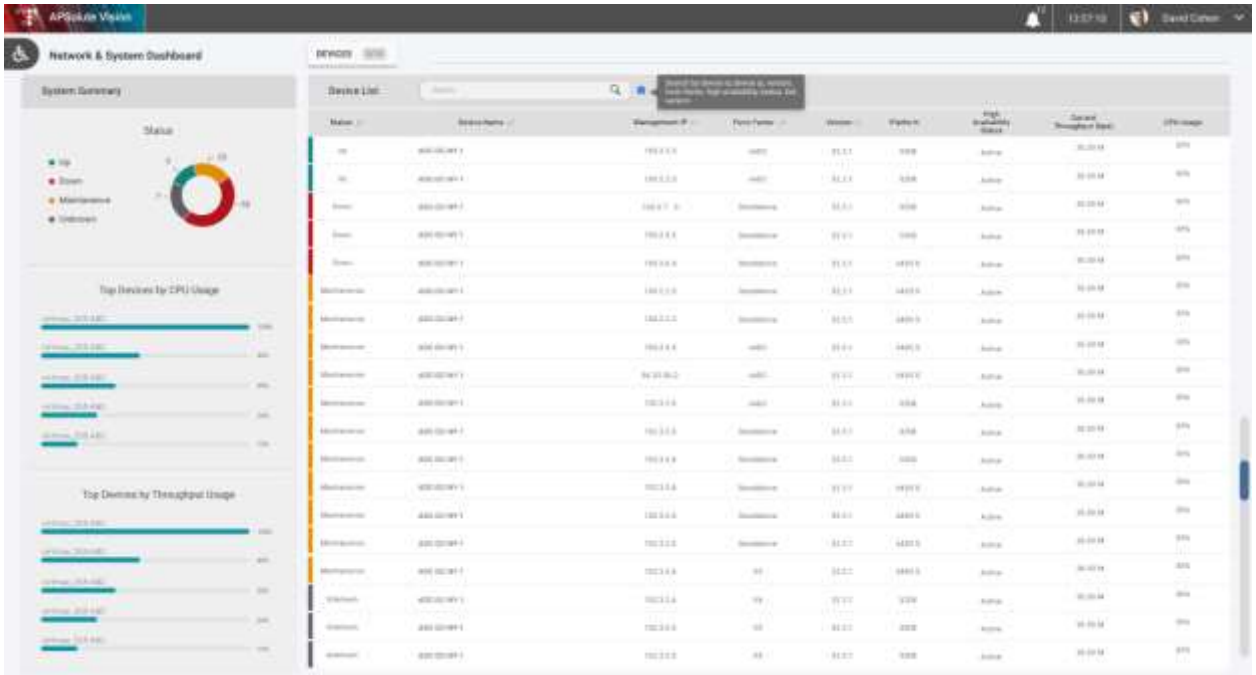
1. Enable the Traffic Event Log globally from **Application Delivery > Application Services > Traffic Event Policy**.
2. Define Traffic Event policies from **Application Delivery > Application Services > Traffic Event Policy/+** that specify the events you want to see, and attach a remote logging object that defines the group of syslog servers and protocol to which these events should be sent.
3. Attach the Traffic Event policy to the virtual services that require logging.

ADC Analytics: System and Network Dashboard and Reports

Starting with this version, the Alteon *System and Network* dashboard and *Reporting* are available using APSolute Vision 4.20 or later. These screens are a centralized set of dashboards that graphically display the health and performance of your system, enabling 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 dashboards and reports provide real-time as well as historical data (up to three months).

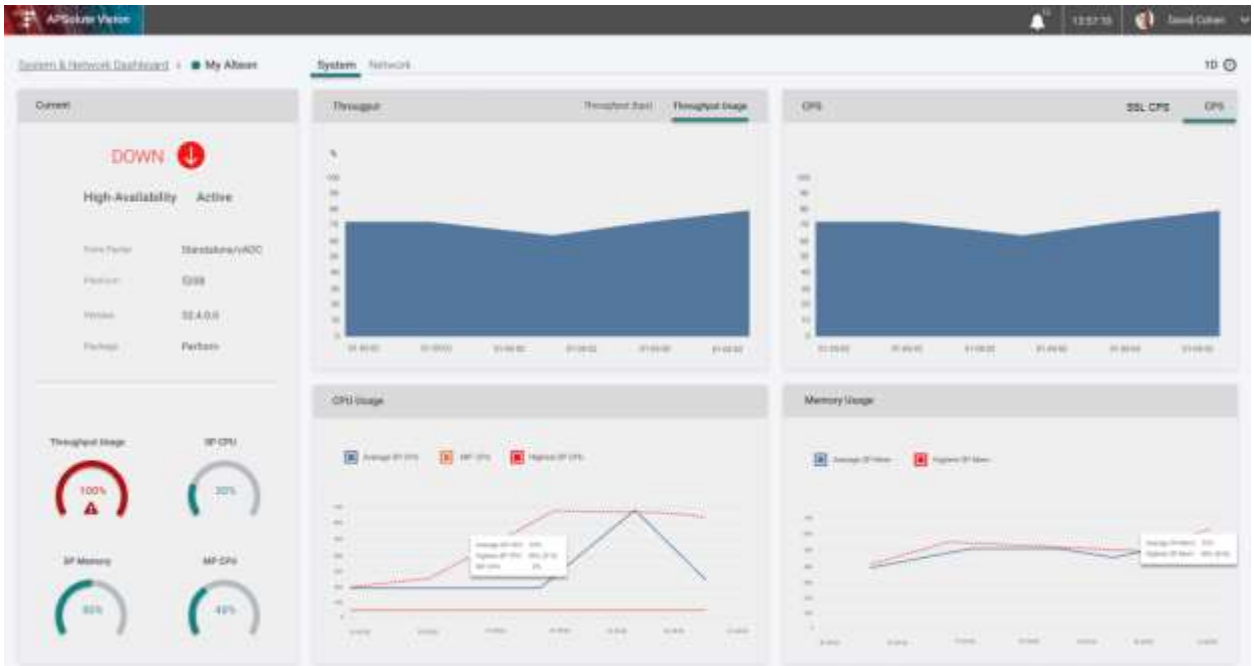
System and Network Dashboard Main Screen

The System and Network Dashboard main screen displays a summary of all the Alteon devices (32.2.1.0 and later) managed by APSolute Vision. From here you can identify at a glance the top devices by throughput or CPU in addition to other key information per device.



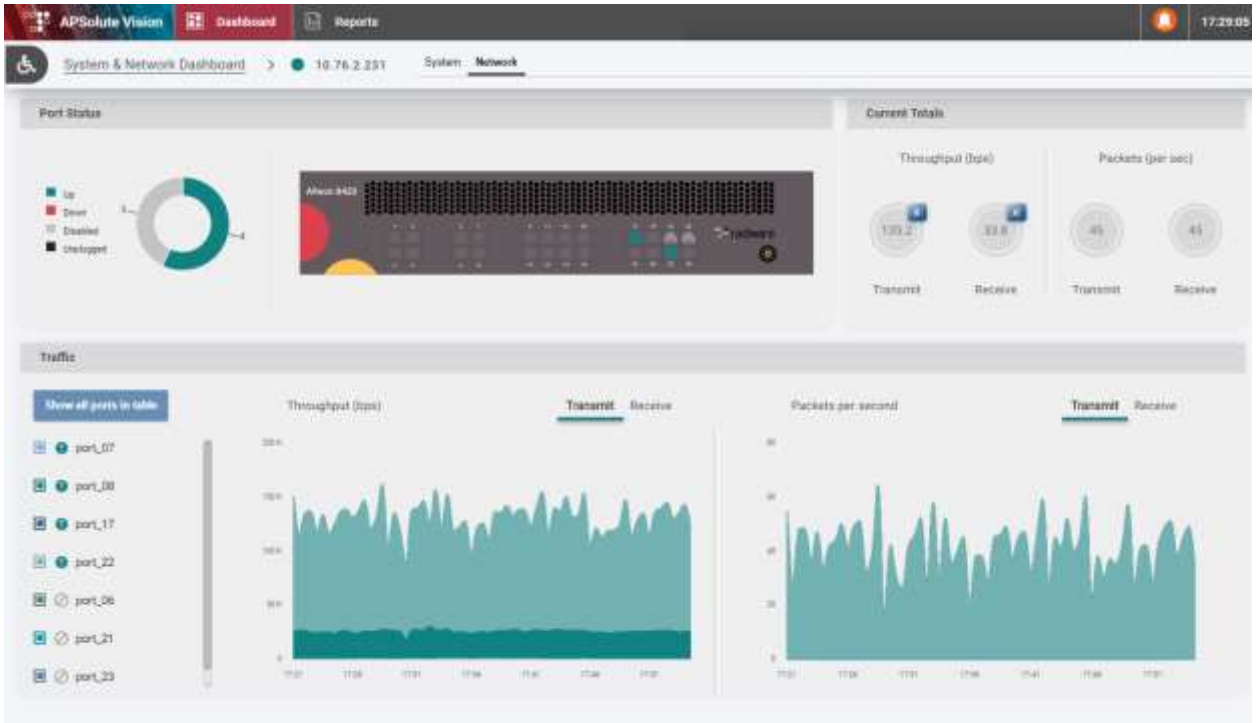
System Dashboard Screen

Clicking on an individual device opens a more detailed view of the system, such as MP/SP CPU, throughput utilization, SSL CPS, and its groups and servers, helping you troubleshoot any health and performance issues, and more.



Network Dashboard Screen

Clicking on the *Network* tab displays a screen with the device ports' statuses and TX and RX statistics:



SSL Enhancements

OCSP Enhancements

This version introduces the following OCSP enhancements:

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

  NFR ID: prod00253069

- Support for the HTTP GET method – Previously only the POST method was available.

Support Subject Alternative Name Field

Alteon now supports generating a CSR or certificate with Subject Alternative Names. Multiple domain names can be configured using the following format:

`DNS:domain1.com, DNS:www.domain2.com,…`

NFR ID: prod00267481

Display Certificate Serial Number in Certificate Repository

The certificate serial number is now extracted and displayed in the certificate repository. This is displayed in both CLI (`/cfg/slb/ssl/certs/cert <n>/cur`) and WBM (**Configuration > Application Delivery > SSL > Certificate Repository**).

NFR ID: prod00261471

ICAP Enhancements

This version introduces the following enhancements to ICAP support:

- Ability to send only certain HTTP requests/responses to ICAP server inspection, using AppShape++ script.

  The ADAPT: disable command was added for this purpose:

  - **ADAPT::disable** – Disables ICAP processing for the current HTTP request if called in an HTTP_REQUEST or current response if called in an HTTP_RESPONSE.
  - **ADAPT::disable request** – Disables ICAP processing for the current request. The request will be forwarded according to filter action without being scanned by the ICAP service. This command can be called in HTTP_REQUEST events.
  - **ADAPT::disable response** – Disables ICAP processing for the current response when called in HTTP_RESPONSE events, or for the response to a current request when called in an HTTP_REQUEST. The response will be forwarded according to filter action without being scanned by the ICAP service.

- Ability to provide the ICAP servers with the original client IP address.

  Alteon lets you include an ICAP header that carries the client IP address. A user can specify whether the client IP address should be taken from the HTTP/S original packet source IP address or from the X-Forwarded-For header. The default ICAP header name used for this is X-Client-IP, but it can change.

AppWall Enhancements

Alteon 32.2.1.0 includes integrated AppWall module version 7.6.4 that introduces the following enhancements.

HTTP Strict Transport Security Support

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps protect websites against protocol downgrade attacks and click hijacking. It allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure HTTPS connections, and never via the insecure HTTP protocol.

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page, and routing them to another page, most likely owned by another application or domain.

AppWall's HSTS feature allows adding HTTP response headers to different hosts to improve security in places where the application is lacking the required measures.

For more information, see https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Two options of predefined headers are available: **Strict-Transport-Security** protects against protocol downgrade attacks and **Content-Security-Policy** protects against clickjacking.

In addition to the predefined header values, the user can also add different headers in the response if desired.

Cookie Security Enhancement

A cookie returned from a web server can have attributes and flags, for example, "secure" and "httponly" flags, that control the way the browser sends the cookie back to the server on the next requests. The "secure" flag tells the browser to send the cookie only on a secure connection (i.e. https), and the "httponly" flag tells the browser not to enable the page to read this cookie in commands like *document.cookie*.

For security reasons, for some relevant cookies, it should be considered modifying the returned cookie from the server to contain the "secure" or "httponly" flags even if the server did not set them.

The *Reply Cookie Flags* option allows the user to update the returned cookie to contain a **Secure** or **HTTP Only** flag.

Security Page Enhancement

The status code and status message of the security page returned can now be defined. The configuration file WebApp.cfg contains information for the status code and the status message returned by AppWall for an internal security page.

The default value for the status code is 200 and the default for the status message is *OK*. Valid values: 200-599.

New Web UI

The integrated AppWall module configuration and monitoring is now fully supported via new React-based Web UI and totally replaces the previous AppWall Management Application based on Java.

The new interface is launched via the Edit Security Policy link in the **Security > Web Security > Secured Web Applications** pane and via the New AppWall Configuration link in the **Security > Web Security** pane.

Logging Enhancements

Logs per Health Check

Whenever a server goes down because of a health check failure, Alteon sends a notification (syslog message or SNMP trap). However, when a logical expression health check is used and one of the individual health checks fails without causing a logical expression health check failure, there is no notification (the status of each individual health check can be viewed using the **info** command).

Starting with this version, if an individual health check that is part of a logical expression health check fails, a notification is sent for it.

NFR ID: prod00252738

Alteon Session Logs via Management Port

Alteon can now write the session log messages to a predefined file path on the disk, and these logs can be exported using the CLI or WBM on both data and management ports.

To use this feature, enable it in CLI `(cfg/sys/syslog/sesslog/mode disk)` or in WBM (**Configuration > System > Logging and Alerts > Session Log**).

Limitation: Export using SCP fails when the file size is around 300/400 MB (DE47803, DE47808)

Workaround: Use FTP when the file size more than 300 MB.

NFR ID: prod00266536

Keys Import on Alteon 6024 FIPS

On FIPS-certified devices, keys should be created directly on the FIPS device to be protected against discovery. Such keys can be synchronized with a similar FIPS device via a special trust process.

In a scenario where a service moves from regular SSL security to a FIPS-enhanced security, Radware recommends generating a new key for the service on the FIPS device and acquire a new certificate for this key. However, if the original key and certificate must be used, Alteon now lets you import a clear-text key and certificate.

NFR ID: prod00267640

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.

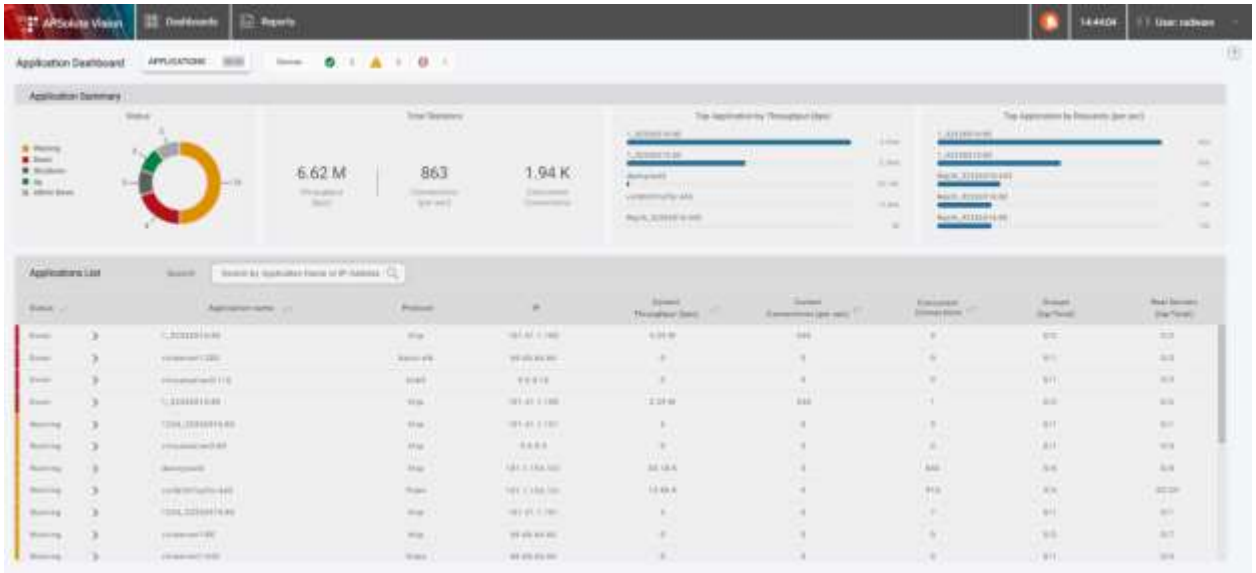
The Application Dashboard provides insights into the application health and performance data, letting you to proactively plan capacity, and to troubleshoot and detect anomalies.

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).

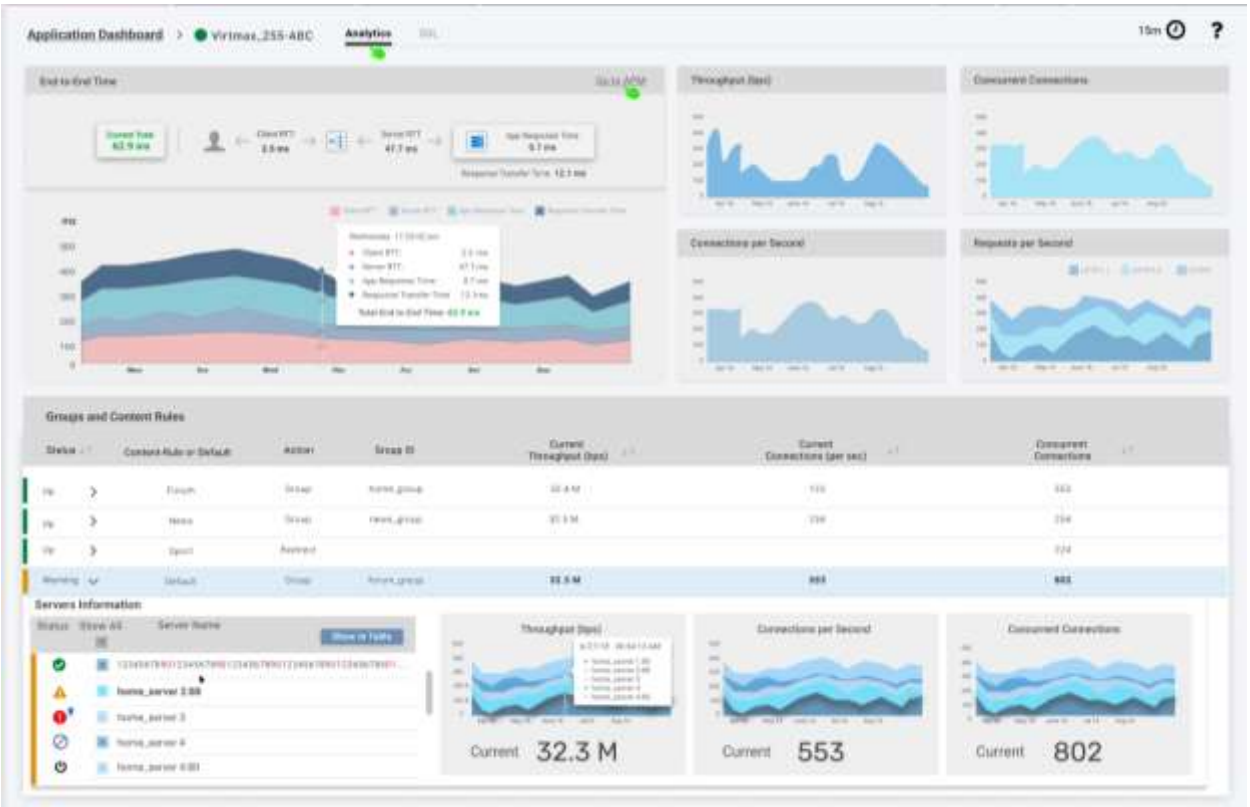
Application Dashboard Main Screen

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.



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.



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: **Error! Hyperlink reference not valid.** IP>/reporter/virtualServer

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

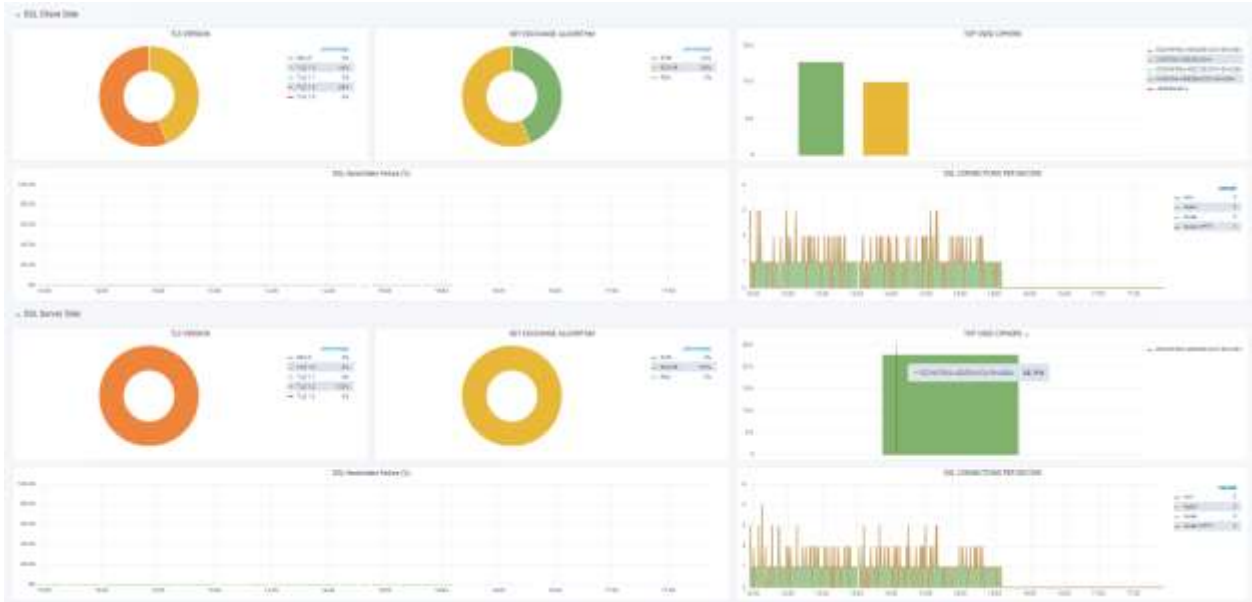
Alteon Cluster on Azure

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:


Analytics
radware
Every second counts
Servers Status
UP
CPU
Memory
RTT
39.4 ms
Throughput
629 Mbps
Concurrent Connections
103
Connections / Sec
724
Instances
2
End to End Timing
Connections Per Second
Requests Per Second
Concurrent Connections
Throughput



Real Servers Auto Scaling support on AWS

Alteon VA on AWS now supports real servers running as part of an AWS Auto Scaling group. Using this capability, Alteon VA automatically adds or removes real servers from the real servers group as the AWS Auto Scaling capability adds or removes application servers. This solution is comprised of an Alteon Auto Scaling AWS lambda function together with the Alteon FQDN capabilities.

For further details, refer to the *Alteon VA on AWS Getting Started Guide*.

Real Servers Auto Scaling Support on VMware

Alteon VA, through vDirect now supports real servers auto scaling controlled by VRO.

vDirect adds or removes real servers in real servers group of the Alteon devices automatically ass servers are added or removed by the VRO. This is supported starting vDirect version 4.70

For further details, refer to the *vDirect user guide*.

New Alteon Platform Series (9800)

The Alteon Application Switch 9k series includes high-end performance application delivery appliances, providing superior SSL performance with support for the latest encryption standards (ECC). High-performance coupled with a wide range of connectivity options, high performing and reliable storage (SSD), advanced capabilities, and OnDemand scalability make this series suitable for carriers, mobile operators, and large enterprises.

Alteon D-9800 Highlights

- On-demand throughput scalability: 240 Gbps and 320 Gbps
- Platform flavors:
  - 9800 – Up to 35K RSA SSL CPS/35K EC SSL CPS and 30 Gbps bulk encryption
  - 9800S – Up to 100K RSA SSL CPS/50K EC SSL CPS and 50 Gbps bulk encryption
  - 9800SL – Up to 195K RSA SSL CPS/115K EC SSL CPS and 75 Gbps bulk encryption
- Port density:
  - Eight (8) 100 GbE QSFP28
  - One (1) management port – 1Gbe copper
  - One (1) console RS232 DB9
- RAM: 192 GB
- Storage: 480 GB SSD
- Dual AC power supply (DC PS is available)
- Capabilities: Deliver and Perform capability packages

Notes:

- Upgrade between the different 9800 models, including between S and SL models, cannot be done in the field (requires factory installation)

- This release does not include Secure package (which is scheduled to be supported in the next release)
- The ADC-VX form factor is not yet supported
- Jumbo frames are currently not supported on Alteon 9800 platforms.

Alteon 6024 NEBS Certification

Alteon 6024 SL with 80 Gbps throughput is now also available with a NEBS version. Separate P/Ns are available for the NEBS product.

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:

- This is supported only on S/SL and regular platform models, and Alteon VA.
- 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 the **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.

Hardware Health Monitor

The hardware health monitoring module scans the system for hardware elements and collects historical statistics on them. These data are then exported as part of the techdata.

By default, hardware health monitoring is enabled and can be disabled using the following CLI command: `/c/sys/hwhealth`

WHAT'S CHANGED IN 32.2.14.0

AppWall Integrated

- Signature Operation Mode:

  A new Operation mode, **Forced Active,** is now available. If the Database Security filter or the Vulnerabilities Security filter are in Passive mode, the RuleID or PatternID configured as **Forced Active** will block the traffic.

  From the AppWall Management Console, in the Database Security filter, the configuration has been consolidated. Two tabs exist today:

  - **Rule Operations** allows the configuration of the Auto Passive Mode, the definition of the Operation Mode for any RuleID, and an aggregated view of the Database Security filter of each Application Path where the Database filter is defined.
  - **Parameter Refinements** allows to exclude RuleIDs per parameters/headers.
- FileUpload Security filter:
  - Support of files with no extension.
  - Advanced support of files upload with content the Content-Type multipart/form-data.

WHAT'S CHANGED IN 32.2.13.0

HTTP/HTTPS Health Check

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

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

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

NFR ID: 211020-000175

QAT Driver/Engine Upgrade

The Intel QAT driver used in Alteon S and SL models has been updated to QAT.L.4.17.0-00002.

OpenSSL Upgrade

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

AppWall Integrated

1. **Database Filter:** In the inspection settings, we can configure the filter to do a partial inspection of the parameters (for example, inspect only the first 150 characters).

2. **Content-type HTTP Header** multipart/form-data can be refined if it does not follow RFC (specific implementation with a different delimiter than in the RFC).
3. **URL-encoded encoding**: More support and refinement options were added in the Parsing properties. Per URI, it can be specified which reserved characters are **un**encoded.
4. **Cookie Reply flag:** We can now enforce the cookie flag SameSite (Strict, LAX or None) on behalf of the origin server.

WHAT'S CHANGED IN 32.2.12.0

AppWall Integrated

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

WHAT'S CHANGED IN 32.2.11.0

None

WHAT'S CHANGED IN 32.2.10.0

OpenSSL Version

The OpenSSL version has been updated to OpenSSL 1.1.1l.

AppWall Enhancements

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

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

WHAT'S CHANGED IN 32.2.9.0

AppWall Features

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

WHAT'S CHANGED IN 32.2.8.0

DNS Resolver Enhancements

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

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

NFR ID: 200723-000119

OpenSSL Version

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

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

Treck Version

The Treck version has been updated to 6.0.1.69.

WHAT'S CHANGED IN 32.2.7.0

Increased Tunnels and Static Tunnel Routes Configuration Capacity

Starting with this version, you can support 8k Layer 3 tunnels and static tunnel routes if memory allows. To increase the number of tunnels and static tunnel routes to 8k, use the CLI command `/c/slb/adv/memmng/tnltbl`. This change requires **Apply**, **Save**, and **Reboot** to become active.

NFR ID: 200322-000001

User Role can be Restricted from Viewing the Syslog Logs

By default, a user with the **User** role can view the syslog logs via the CLI or WBM.

Starting fromwith this version, the Administrator can specify the **User** role to viewto view or not view the syslog logs.

CLI: `/cfg/sys/access/user/usrlog`

WBM: **System > Users > Local Users**

Note: This support is applicable to local users only (both predefined and user-defined). It is not applicable to remote users.

NFR ID: 200814-000008

Enlarge Login Banner Size

The CLI banner length has been increased from 319 characters to 1300 characters (which can be set using the `/cfg/sys/bannr` command).

NFR ID: 200921-000035

WHAT'S CHANGED IN 32.2.6.0

OpenSSL Upgrade

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

Real Server Tracking Logic Changes in WBM

An option to automatically add all the real servers (including those that will be added in the future) was added to the WBM.

NFR ID: 190911-000343

Treck Version Upgrade to 6.0.1.66

In this version, Treck was upgraded from version 6.0.1.44 to 6.0.1.66, which resolves the following CVEs (including Ripple20, and others):

- CVE-2020-11896
- CVE-2020-11897
- CVE-2020-11898
- CVE-2020-11899
- CVE-2020-11900
- CVE-2020-11901
- CVE-2020-11902
- CVE-2020-11903
- CVE-2020-11904
- CVE-2020-11905
- CVE-2020-11906
- CVE-2020-11907
- CVE-2020-11908
- CVE-2020-11909
- CVE-2020-11910
- CVE-2020-11911
- CVE-2020-11912

- CVE-2020-11913
- CVE-2020-11914

WHAT'S CHANGED IN 32.2.5.50

TLS Version Default

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

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

WHAT'S CHANGED IN 32.2.5.0

Syslog Enhancements

Increase of the Number of Syslog Servers to Six

Prior to this version, five syslog servers were supported. Starting with this version, six syslog servers are supported.

NFR ID: 190911-000460

OpenSSL Version

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

TLS Allowed Versions Default

Prior to this version, by default TLS versions 1.1, 1.2, and (where relevant) 1.3 were enabled in newly configured SSL policies. TLS 1.1. is now considered insufficiently secure and allowing it caps the SSL grade provided by Qualys to B. Starting with this version, newly configured SSL policies will have TLS 1.1 disabled by default. Existing SSL policies will preserve the configuration before upgrade. Radware recommends to manually disable TLS 1.1 to achieve a higher SSL grade.

Security Hardening

- Upon authentication failure, the error message does not reflect the reason for the failure.
- All password inputs are masked.
- The log command is available to all user roles using the CLI (to align with the behavior using WBM).
- For upgrades from versions 32.6.1.50 and later, 32.4.3.50 and later, 32.2.5.50 and later, and 31.0.13.50 and later, to any later version, Alteon uses the SHA2 algorithm for the digital signature (in all platforms).

NFR ID: 191126-000098

Client NAT Port Assignment Logic

Starting with this version, it is possible to select the client NAT port assignment algorithm on Alteon running on the vADC form factor. The options are:

- Sequential – Minimizes the probability of fast port reuse, but it can be a security vulnerability
- Random – Provides increased security, but the probability of fast port reuse is higher

This can be done using the command `/cfg/slb/adv/pport` (in WBM, **Application Delivery > Virtual Service > Settings > Session Management** tab).

Notes:

- The change in the client NAT port assignment algorithm will only take place after statistics are cleared (`/oper/slb/clear`).
- On Alteon VA and Alteon platforms in standalone mode, the client NAT port assignment uses an enhanced random mode that also minimizes fast port reuse probability.

NFR ID: 200407-000053

WHAT'S CHANGED IN 32.2.4.0

Health Check Source MAC

When working in legacy VRRP high availability mode, you can now set health check traffic to servers to use the VR MAC for the server's VR owner instead of the interface MAC.

NFR ID: 190911-0 (prod00270223)

Banner Length

The CLI banner length has been increased from 80 characters to the standard banner length of 319 characters (`/cfg/sys/bannr`).

Note: The data type of agCurCfgLoginBanner and agNewCfgLoginBanner was changed from DisplayString (SIZE(0..79)) to OCTECT STRING (SIZE(0..318).

NFR ID: 190912-000126

Alteon VA – Number of Supported NICs (Hyper-V, OpenXEN)

The number of vNICs Alteon VA runs on Hyper-V or OpenXEN was increased from three (3) to eight (8) vNICs (one [1] for management and seven [7] for data).

Integrated AppWall

The following are changes and modifications made to the AppWall module:

- Integrated AppWall module can now report events to Absolute Vision using IPv6 addresses.
- The Forensic events filter by time range now supports hour and minute ranges.

- Integrated AppWall can now synchronize Signature Updates and Geolocation data that was manually installed to a backup HA device. To initiate the synchronization, click **Apply** after installing the new updates on the primary device.
- Disabling the publishing of an event also disables sending the event to APSolute Vision.
- AppWall notifies you of configuration file issues and recommends a solution.
- Fixes and improvements to AppWall's configuration **Apply** mechanism.
- Fixes and improvements to the config sync mechanism.

Server Session Shutdown

Real servers can be shut down gracefully by continuing to send to the server traffic belonging to active connections (Connection Shutdown), and in addition can continue allocating to the server new connections if they belong to persistent session entries (Session Shutdown). Previously, Session Shutdown was only available when persistency mode was cookie or SSL ID. Now this is also available for client IP persistency.

NFR ID: 190911-0000346 (prod00 273440)

OpenSSL Version

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

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

WHAT'S CHANGED IN 32.2.3.0

Alteon User Password Encryption Enhancement

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

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

NFR ID: prod00272191

Audit Log via Telnet and SSH

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

NFR ID: prod00272163

BGP Support for Four-octet AS Number

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

NFR ID: prod00268252

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

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

NFR IDs: prod00259678, prod00259680

Jumbo Frames

Jumbo frames for the 5208, 6420, 8420, Alteon VA, and DPDK platforms now supported.

NFR ID: prod00268780

Failover Delay

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

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

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

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

NFR ID: 191006-000024

WHAT’S CHANGED IN 32.2.2.50

Fixed AppWall Performance Degradation

Fixed a severe performance degradation of AppWall integrated with Alteon after upgrading to version 32.2.2.0.

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

WHAT’S CHANGED IN 32.2.2.0

None

WHAT'S CHANGED IN 32.2.1.0

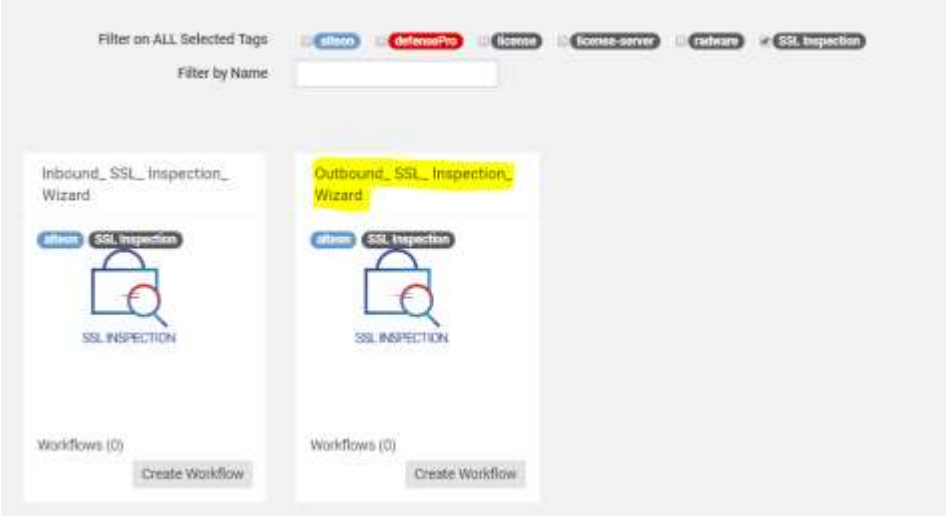
vDirect-Based Outbound SSLi Wizard (Layer 3 Deployment, Single Standalone Device)

A wizard for quick and easy configuration of an outbound SSL Inspection solution is now available via APSolute Vision (version 4.20 and later). The wizard is implemented using a Radware vDirect workflow.

The wizard supports a Layer 3 environment on a single standalone device.

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

To start with the deployment, click **Create Workflow**.



SSL Inspection Deployment Support in VLAN Tag and Trunk

Fallback VLAN an Fallback Trunk Support

Alteon support for Fallback VLAN and Fallback Trunk enables you to connect the Security Inspection Services (SIS) chain of an SSL inspection deployment via switch and not only directly connect to Alteon.

- Fallback VLAN is defined on the filter redirecting to the next SIS in the chain:
  - If the port defined on the fallback port is a tagged port, Alteon injects the traffic with the VLAN tag defined on the fallback VLAN.
  - if the fallback port is tagged but the fallback VLAN is not defined, the injected traffic is injected with PVID tagging
- Fallback Trunk:

- When the fallback port is part of an LACP trunk, the fallback port should be set to any of the ports participate on the trunk. Alteon load balances the injected traffic between the available ports on the trunk.

Trunk and VLAN Support in IDS-Chain

Alteon sends traffic to the IDS server via the defined IDS port and in parallel it injects the traffic to the IDS port in order to continue in the flow. Starting with this version, if the defined IDS port is part of an LACP trunk and, during injection Alteon load balances between the ports in this trunk. If the IDS port is a tagged port, Alteon tags the traffic sent to the IDS server and also injects the traffic to continue in the flow

Note: If the IDS server is connected via a tagged port (IDS port), but the IDS VLAN is not defined, Alteon tags the injected traffic with PVID tagging.

Virtual Service Manageability Enhancements

The following enhancements were added to simplify virtual service manageability:

- *Virtual Service Status* view:
  - Added the virtual server IP address
  - You can now fully expand a service with one click

- Three new CLI commands were added to display the real servers, groups, and virtual services in tabular format. including a search capability (for more information, see the *Alteon Command Reference* or the online CLI command usage help).

  `/info/slb/realtab`

  `/info/slb/grptab`

  `/info/slb/virttab`

```
>> Standalone ADC - Server Load Balancing Information# /info/slb/realtab
** -  Real does not have group/virt configured
-----------------------------------------------------------------------------
| Status    | Real Server ID          | Group ID     | Content Rule   | Virtual Server ID      |
|           | Real Server IP          |              | Content Class  | Virtual Server IP      |
|           | Real Server Type        |              |                | Virtual Service        |
-----------------------------------------------------------------------------
| DOWN      | 1                       | 2            | 0              | **                     |
|           | 10.194.245.112          |              | **             |                        |
|           | local                   |              |                |                        |
-----------------------------------------------------------------------------
| DOWN      | babu                    | babu         | 0              | **                     |
|           | 1.2.2.2                 |              | **             |                        |
|           | local                   |              |                |                        |
-----------------------------------------------------------------------------
| DOWN      | R1                      | G1           | 0              | Myservice              |
|           | 100.3.3.3               |              | **             | 3.30.30.30             |
|           | local                   |              |                | 443 (https)            |
-----------------------------------------------------------------------------
| DOWN      | Real2                   | G2           | 0              | **                     |
|           | 6.6.6.6                 |              | **             |                        |
|           | local                   |              |                |                        |
-----------------------------------------------------------------------------
```

NFR ID: prod00263461, prod00263465

Update Session Entry-based on Gratuitous ARP

When a gratuitous ARP is received from upstream routers, Alteon now updates the source MAC address on relevant session entries.

NFR ID: prod00263371

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.

GEL License Presentation on ADC-VX platforms

The licenses of vADCs with GEL licenses are displayed on Alteon ADC-VX platforms with an indication that vADC is running a GEL license.

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.

Management IP Address in ADC-VX

Starting with this version, when this platform is configured to operate in ADC-VX mode, the management IP address of the Alteon VX and its vADCs must be on the same network. Otherwise, the apply fails.

Dual Power Supply for Alteon 4208

4208 now supports a dual Power Supply

Note: There is no field upgrade of a single PS to dual PS. Upgrading a single PS to dual PS requires going through the buyback process.

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.

Username 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 32.2.14.0

General Bug Fixes

Item	Description	Bug ID
1.	The client certificate went through OCSP verification even though it is in OCSP stapling mode.	DE76180

AppWall Bug Fixes

Item	Description	Bug ID
1.	Request of /v2/config/aw/SecurityEvents/ returned a false response.	DE75916
2.	The forensics search engine was not accurate.	DE74469

Item	Description	Bug ID
3.	Wildcard hostname (*nma.lt) worked incorrectly and caused false positive.	DE74667
4.	Session filter removed the cookie in passive mode.	DE74748
5.	There was no detailed information about a pattern.	DE74850
6.	Protected applications behind AppWall went down suddenly.	DE75232
7.	Under certain conditions, no explanation is provided in the Forensics API Security event.	DE75513
8.	Geo filter (ZZ) to display the Forensics logs for Private networks did not work.	DE75593
9.	In Forensics, the filter according to the Geo-Location did not work.	DE74346

Fixed in 32.2.13.0

General Bug Fixes

Item	Description	Bug ID
1.	The AppWall nodejs module flapped on virtual platforms in the following cases: 1. When there are more than 10 vADCs 2. When vADCs are configured with the basic flavor.	DE72861
2.	There was an error with traps for IPv6-related events.	DE73065
3.	When there was a TCB block leak, DSSP health checks failed.	DE73181

AppWall Bug Fixes

Item	Description	Bug ID
1.	Under certain conditions, Source Blocking reports an “Always Blocked” IP source.	DE72050
2.	The Forensics session and the Dashboard’s Current Activity is not displayed on the AppWall Management Console.	DE73465
3.	For database refinements which involve XML, a false positive is shown, and the request is still blocked.	DE74094

Fixed in 32.2.12.0

General Bug Fixes

Item	Description	Bug ID
1.	A user was locked out after making a password change.	DE70322

Item	Description	Bug ID
2.	Real server health checks were not started when there was a run-time instance with an improper index in the dispatch queue of slice 4.	DE71443
3.	When a DPDK image reset, an unexpected DNS server IP address was added by BSP.	DE71758
4.	After the AppWall health check failed, the MP restarted AppWall every 15 seconds .	DE71822

AppWall Bug Fixes

Item	Description	Bug ID
1.	When adding a host under an existing Webapp using API, an Error 400 was shown.	DE70145
2.	A Corrupted Configuration File Detected error was shown.	DE70260
3.	HTTP DELETE requests were being blocked by AppWall's FileUpload filter and reported as PUT.	DE70675
4.	The Brute Force filter was not working on API-based server responses.	DE70797
5.	A Threshold of incoming sessions event was shown when the total active connections were much lower than the maximum.	DE71105
6.	Under some conditions, long header Hostnames led to a syslog failure.	DE70821
7.	The APSolute Vision AppWall dashboard displayed wrong data	DE70207

Fixed in 32.2.11.0

General Bug Fixes

Item	Description	Bug ID
1.	In an SLB environment with VLAN level proxy configured, in some instances the MAC flapped after an SLB config apply.	DE69665

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall blocked requests when Host protections (CSRF/URL Rewrite/Redirect validations) had the "Inherit" status.	DE67920
2.	Debug log added to link the Source Blocking scoring and the related security event.	DE66587

Item	Description	Bug ID
3.	Wrong IP blocked with Source Blocking.	DE68383
4.	Wrong host displayed in syslog security event.	DE68396
5.	Wrong hostname displayed in the Forensics security events when blocked by the Application Security policy.	DE68487
6.	AppWall displayed an “Initialization error” after the navigation to Security filters.	DE68858
7.	AppWall API management: HTTP tunnel PUT method changed to contain all the mandatory fields. Creation of the PATCH Method.	DE69722

Fixed in 32.2.10.0

General Bug Fixes

Item	Description	Bug ID
1.	Starting with this version, the SNMPv3 target address table is available in the Ansible module.	DE67001
2.	New SSH and HTTPS connections failed when a faulty SSH inbound session existed (associated with an obsolete file descriptor).	DE66477
3.	The SSL Hello health check caused a memory leak which led to a panic.	DE66188

AppWall Bug Fixes

Item	Description	Bug ID
1.	HRS attack: HTTP GET request with BODY was not being blocked while there was a security event.	DE65623
2.	Under some conditions, the AppWall management console WAF stopped working and was not accessible.	DE67515
3.	The AppWall Activity Tracker recognized a legitimate Google search engine as a bad bot.	DE67646
4.	Wrong hosts reported with AppWall Hosts protection.	DE64012
5.	AppWall blocked the server response when a tunnel was in passive mode.	DE65600

Fixed in 32.2.9.0

General Bug Fixes

Item	Description	Bug ID
1.	The random salt was a predictable random number generation function generating a similar sequence.	DE63665
2.	Could not enable the extended_log via Ansible.	DE63838
3.	The real health check displayed different times in CLI and WBM.	DE64028
4.	When pbind clientip and vmasport were enabled, the persistent session was not permanently deleted.	DE64351
5.	Servers were vulnerable to CVE-2021-3449 if they had TLSv1.2 and renegotiation enabled (default). **Fix**: The MP OpenSSL version has been upgraded to 1.1.1k to fix this.	DE64378
6.	Predefined HTTP headers were used when POST HTTP health checks were sent without taking into the account the actual body length.	DE64698
7.	Defect that tracked DE65346 -- Device auto rebooted with reason of hardware watchdog.	DE65346
8.	After performing config apply, GSLB DNS responses returned a remote IP address instead of a local VIP.	DE65360
9.	SIP UDP service run by AppShape++ failed (it was used for persistency and/or Layer 7 manipulation).	DE65430
10.	Even though the SP/MP profiling logic was disabled by default, Alteon panics with SP profiling logic being triggered.	DE65488
11.	When a vADC Layer 2 configuration was applied/pushed to an ADC-VX (with /c/vadc/add or rem), if at the same time a vADC Apply (or config sync) occurred indicated by a flag, a race condition while logging this configuration caused the vADC to freeze while waiting for the flag, and was eventually restarted by the Watcher.	DE65960
12.	When BFD and tunneling are enabled, a panic occurs.	DE66000
13.	While initiating the SSL client connection for the SSL health check, the vADC MP crashed.	DE66137
14.	The MP CPU utilization was high when querying virtual stats.	DE66778

AppWall Bug Fixes

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

Fixed in 32.2.8.0

General Bug Fixes

Item	Description	Bug ID
1.	Upon Submit, there was a Quick Service setup wizard internal error.	DE57036
2.	In WBM, the equivalent to the filterpbkp CLI command was missing.	DE59726
3.	In a DPDK VA environment with two NUMAs, packets were not tunnel-processed when they were VMAed to and SP of a different NUMA.	DE60629
4.	When starting up a vADC startup, the admin context froze and the Watcher killed the process, resulting in a panic.	DE61767
5.	Alteon closed the front-end and back-end SSL connection abruptly. Fixed the classification of second request if there is content class SSL.	DE61780
6.	The WANlink current sessions count for IPv6 SmartNAT were not decremented properly due to using the wrong index. As a result, the /stat/slb/real and /stat/slb/lp/wanlink command displayed accumulated values. It has been fixed by using an appropriate index for updating the statistics.	DE61940

Item	Description	Bug ID
7.	When the user sent traffic, a throughput high alert message was issued even though the throughput was less than the configured throughput threshold limit.	DE61978
8.	Actions changing the configuration (such as Apply, Save, and Diff) were incorrectly allowed for users with viewer/operator classes of service when REST requests were sent.	DE62393
9.	Even after changing the log level from debug to error, warning messages continued to be issued.	DE62436
10.	A ticket from a failed connection required passing over the authentication policy on the next connection.	DE62486
11.	With specific browsers, HTTP2 traffic with an uncommon form in the header was not answered.	DE62608
12.	Exporting a configuration from ADC-VX did not work.	DE62633
13.	Incorrect MTU syslog messages were issued for vADCs.	DE62660
14.	The packet capture timestamp was incorrect.	DE62730
15.	On an ADC-VX, the HW Watchdog rarely rebooted due to an unknown trigger.	DE62748
16.	While exporting techdata, IPv6 connectivity went down for a short while and then came back up.	DE62821
17.	When uploading a Layer 2 packet capture from an ADC-VX to the FTP server, Alteon panicked.	DE62851
18.	Using Ansible, could not configure the TLS 1_3 parameter.	DE62868
19.	There was vADC auto-reboot issue because of a software panic.	DE62942
20.	A config sync from a non-HA device to an HA-configured device caused the loss of the HA configurations.	DE62951
21.	Health check tables were not supported for the l4 admin and slb admin users.	DE62974
22.	Using WBM, from the Virtual Service Monitoring perspective, the health check failure reason differed from the correct one displayed by the CLI when some of the related virtual services for the given virtual server were blocked.	DE63057
23.	A non-supported configuration caused a crash.	DE63069
24.	There was an inconsistency in the current throughput per second statistics units of virtual servers.	DE63093 DE63108

Item	Description	Bug ID
25.	In an HA environment, a config sync operation with a tunnel configuration led to disruption in traffic on the peer device due to a shift in the internal tunnel indices.	DE63190
26.	In Ansible, it was not possible to remove one VLAN from all interfaces because the value "0" was not accepted.	DE63215
27.	When multiple VIPs are configured with srcnet, the ptmout value was not being considered.	DE63480
28.	When VIRT6 went down, when deleting the IPv6 SLB virt, Alteon panicked.	DE63542
29.	When the user changed the dbind settings to disabled along with the SSL configuration, the dbind configuration was set to forceproxy even though it was set to disabled.	DE63556
30.	SSL statistics in the CLI and WBM did not match on Alteon running version 32.4.5.0.	DE63568
31.	Fetching the routing table via REST API when the routing table was full caused a panic.	DE63585
32.	When a real server had an rport set to 0 and an rport ser to x, the service became unavailable.	DE63618
33.	After SSL Offloading was enabled, Alteon stopped accepting connections.	DE63629
34.	After changing the admin password and Applying, there were configuration sync issues with the peer.	DE63758
35.	Using CLI, after running the /stats/slb/virt command, backup real servers did not display.	DE63802
36.	After changing a group on an FQDN server, the servers were bound to the older group as well as the new group.	DE63832
37.	After a signal panic, Alteon stopped booting.	DE63890
38.	After Alteon received a packet and tried to open a session entry, an incorrect initialization of a pointer resulted in a NULL access and Alteon panicked.	DE64148
39.	Peer Alteon devices panicked due to vulnerability to CVE-2021-3449.	DE64467

AppWall Bug Fixes

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

Fixed in 32.2.7.50

General Bug Fixes

Item	Description	Bug ID
1.	Snmpbulkwalk on the capacityUsageStats node returned invalid OID output.	DE62230 DE62231
2.	In rare circumstances during tsdmp or techdata export, a panic would occur.	DE62550 DE62552
3.	In a DSR and multi-rport configuration environment, the /stat/slb/virt X command returned statistics as 0.	DE62341 DE62343
4.	In an HA environment, synching the configuration to the peer device with sync tunnel config flag disabled results in the peer panicking.	DE61960 DE61963 DE62011 DE62012
5.	After upgrading to version 31.0.13.0, uneven load balancing started.	DE62335 DE62467

Item	Description	Bug ID
6.	When a DNS responder service was created, the user was allowed to configure parameters, which caused errors. Now the user can no longer configure parameters in this case.	DE61878 DE61879
7.	Failed to access the Alteon WBM and the SSH connectivity was lost.	DE62307 DE62309
8.	Using WBM, there was a display issue when modifying a virtual service with actionredirect.	DE61598 DE61599
9.	When while handling malicious DNS packet with compression pointer loops, Alteon panicked.	DE62128 DE62129
10.	There were no Mibs for the health check count to display them for the command /info/sys/capcityswitchCapHealthCheckMaxEntswitchCapHealth CheckCurEnt.	DE61739 DE61740
11.	Using WBM, when configuring the Nameserver group under DNS Authority, the table name in the mapping file was incorrect.	DE61482 DE61483
12.	vADCs did not process SSL traffic.	DE61693 DE61694
13.	There was no support for query type return errors even if the domain was found.	DE61640 DE61641
14.	Port mirroring increased the SP CPU utilization.	DE62264 DE62267
15.	There was no support for query type return errors even if the domain was found.	DE61251 DE63650
16.	Alteon closed the front-end and back-end SSL connection abruptly. Fixed the classification of second request if there is content class SSL.	DE61781
17.	When the user sent traffic, a throughput high alert message was issued even though the throughput was less than the configured throughput threshold limit.	DE61979

Item	Description	Bug ID
18.	Alteon did not forward traffic when LACP was disabled and worked as expected when LACP was enabled.	DE61510 DE61518 DE61521
19.	When Alteon had high MP memory utilization, restarting caused configuration loss. Alteon came up with the default configuration.	DE61204 DE61205
20.	When a syslog file had long log messages, the /info/sys/log command did not display any log messages.	DE60884 DE60885
21.	During configuration export, creating the AppWall configuration failed, and as a result the entire operation failed.	DE60948 DE60949
22.	The default STP group was not available for a newly added physical VM port.	DE61295 DE61296
23.	When sending an OCSP request over the management port, there were two leaks.	DE60848 DE60849
24.	If Alteon received a request when all real servers were down, the group with all the real servers' indexes less than 33 and the RR, BW, or response metric failed to select a real server, even if they came up.	DE61143 DE61144
25.	When the management WBM listener connection control block was closed during its validation, a 50X WBM error displayed.	DE60912 DE60913
26.	Following a set of SNMP operations, on some occasions Alteon panicked from a memory corruption with a boot reason power cycle.	DE61039 DE61042 DE61083
27.	In an Alteon HA environment with an SNAT configuration in AppShape++, changing, applying, and synching non-SLB configurations resulted in the following syslog warning: Configuration is not synchronized	DE61093 DE61094
28.	When the SSH connection with the correct password was attempted for a locked user, the user lockout status was checked too late.	DE60700 DE60701
29.	AppWall was stuck and did not process traffic but was not restarted by the MP.	DE61472 DE61478
30.	When the default gateway MAC was changed, Alteon sent return traffic to the incorrect or old MAC.	DE60779 DE60782

Item	Description	Bug ID
31.	Using WBM, a 50X error occurred due to buffer leak in an HTTPS request.	DE60763 DE60764
32.	Alteon sometimes would crash when it received the same apply :filter deletion and network class deletion that was assigned to the PIP that was defined for the real server.	DE61028 DE61029
33.	When SSL hardware acceleration is active via a QAT card, the Acceleration Engine may go out of sync due to unknown conditions during **Config Apply**.	DE60361

AppWall Bug Fixes

Item	Description	Bug ID
1.	Certain transactions were not properly processed leading to a network connection failure of AppWall version 7.6.8 integrated in Alteon version 32.6.1.0.	DE61267
2.	Under rare conditions, a configuration change in AppWall integrated in Alteon may have led to a failure.	DE60598
3.	Enabling base64 decoding in the Database security filter, may have led to an AppWall failure.	DE62625
4.	Saving security events was limited to the latest 200 events	DE60583

Fixed in 32.2.7.0

General Bug Fixes

Item	Description	Bug ID
1.	When resolving a DNS PTR record, IP matching was skipped (for both hostlk enabled and disabled) if the service hostname was not configured. **Fix**: The service hostname check now is skipped only if the hostlk is disabled.	DE60805 DE60808 DE60809
2.	A virtual service application-id configuration diff did not sync to an HA pair.	DE60452
3.	AppWall was down and the MP did not kill it, resulting in AppWall staying down indefinitely.	DE60157 DE60366
4.	Starting with this version, the Certificate Group Duplicate button is removed because it is not usable for certificate groups.	DE60330

Item	Description	Bug ID
5.	Using Alteon VA, WBM displayed the port type as "Giga Ethernet Copper" irrespective of the actual port type used.	DE59940
6.	Using WBM, an 50X error occurred due to a leak in buffers on an HTTPS request.	DE60799
7.	Periodic statistics logging was corrupting the configuration environment during Apply/Save, which resulted in a panic.	DE60307
8.	Some DNS requests were not answered or were delayed.	DE60088
9.	A deadlock due to non-async signal functions caused a reboot.	DE59876
10.	There were negative values in OIDs related to Total Octets in content rules statistics.	DE59834
11.	The /info/sys/capacity command did not display current virtual and real services.	DE60169 DE60171
12.	When trying to free the session entry allocated for an AX-processed session, a panic occurred.	DE60179 DE60181
13.	A vADC displayed all default user account passwords in a dump.	DE59870
14.	In an MSTP with trunk environment, Alteon failed to communicate with another device.	DE59895
15.	When a user was in lockout, the information message was not consistent, causing a security problem.	DE59810
16.	When a user tried to group SFP and non-SFP ports in LACP, the error message that was issued was not clear enough.	DE59740
17.	After configuring an IPv6 address as a syslog host, the IPv6 VIP stopped working because the address was removed from the nbrcache entry.	DE59663
18.	DNS query responses were not handled for query types MX and CNAME.	DE60207
19.	Starting with this version, added the Expiry Time field for the cookie in the Services pane.	DE60047
20.	The source MAC for a generated SYN ACK was erroneously overwritten during the last IP forwarding process in the non-RTSRCMAC scenario for TCP DNS and dbind ena virtual traffic.	DE59782
21.	The bandwidth metric sometimes did not work if all the WAN links in a group were configured with health checks.	DE59355
22.	SAN input for DNS without a period (".") was not allowed.	DE60099
23.	The DNS query on a Backup device gave an incorrect response.	DE59541

Item	Description	Bug ID
24.	vADCs were in running state but were not able to be accessed via MGMT until they were disabled and then re-enabled.	DE59083
25.	On a 5208 XL platform, version 32.2.4.60, Alteon did not receive an information message when saving an image on ADC-VX slots completed.	DE59496
26.	The WAN link server displayed an overflow message for a clear issue for an edge condition.	DE59395
27.	Could not handle SSL traffic without SNI without the traffic being decrypted. **Fix**: Now you can attach an SSL policy with front-end and back-end SSL disabled.	DE58830
28.	With Alteon configured with cookie and multiple rports for real servers, when sending traffic without a cookie, rport persistency was not maintained for the subsequent requests for the same TCP connection. The traffic was load balanced to the lowest rport.	DE59148
29.	Maxcon support for 1 million was erroneously not implemented in the 30.5 series.	DE58162
30.	Configuring a data class with a special character propagated to AX failed due to a parsing error associated to the unsupported ASCII character, resulting in an out-of-sync configuration state.	DE59366
31.	Due to a network outage, Alteon panicked due to an IPv6 gateway failure.	DE59414
32.	An IPv4 filter session sometimes would be deleted before it aged out if the session memory was previously used by an IPv6 session.	DE60386
33.	On a 5208 platform, Ethernet ports connected to FireEye stayed down.	DE60232
34.	When real servers associated with a deleted FQDN real were deleted, AX was not updated.	DE58106
35.	There were two leaks when sending OCSP requests over the management port, which have been fixed.	DE60845

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall WebUI sometimes showed a 500 error.	DE59923

Item	Description	Bug ID
2.	AppWall integrated in Alteon sometimes returned an empty page to a client request.	DE59640
3.	Email notification (STMP) configuration for AppWall integrated in Alteon was wrong.	DE58413
4.	Occasional slowness in AppWall integrated in Alteon due to memory consumption.	DE58350
5.	An event- "Failed to update configuration according to awcfg.xml" sometimes appeared even when the configuration was correct.	DE60488

Fixed in 32.2.6.50

General Bug Fixes

Item	Description	Bug ID
1.	When trying to group SFP and non-SFP ports in LACP, the error message that was issued was not clear.	DE59741
2.	Using the CLI, when executing the /c/l3/ha/switch/pref command, if the SSH/Telnet connection terminated, a panic occurred.	DE59572
3.	Before RIP was assigned to an outgoing packet, the packet included the last four bytes of the IPv6 address, resulting in the leading zero in the address being blocked.	DE59487 DE59488
4.	As a fix, the FIPS domain name length was changed from 14 to 32 characters.	DE59701 DE59702
5.	The DNS IPv6 EDNS client subnet IP address was incorrect.	DE59578 DE59581 DE59582
6.	When a real server went down, the virtual statistics summary display was incorrect.	DE59510 DE59514
7.	On an Alteon VA platform, the jumbo frames feature did not work because the DPDK layer for the VMXNET3 driver did not provide an API call to set the MTU value.	DE59286 DE59288
8.	On a 5424 platform with an unlimited SSL license, the info/sys/general command incorrectly displayed “S” and not “SL”.	DE59025
9.	In a basic SLB environment, when trying to disable a real server operationally that started with the letter "p," Alteon did not correctly prompt the action.	DE58913 DE58914

Item	Description	Bug ID
10.	Even after setting the throughput threshold limit to "0," throughput alerts were issued.	DE58819 DE58820
11.	The total IP range limit value mentioned in the validation error for network classes was incorrect. It should have been 4294967294 instead of 4294967295.	DE59457 DE59458
12.	When TACACS with clog was enabled, during a techdata/tsdmp operation, unnecessary logs were issued to the syslog.	DE58760 DE58761
13.	The description for MIB altSwSpCpuPressureDeactivatedTrap was incorrect.	DE58769 DE58770
14.	When sending ICMP traffic to Alteon, the ICMP session was dumped to the syslog server as UDP.	DE59279 DE59280
15.	Using CLI over an SSH/Telnet connection, when the /c/slb/real x/shut command was executed without input, closing the connection led to a panic.	DE58595 DE58598 DE58599
16.	When sending client traffic to an IPv6 VIP with sharing enabled for the VR server, Alteon did not respond.	DE58979 DE58980
17.	After upgrading from version 30.5 to version 32.2, LinkProof NG static NAT did not perform reverse NAT.	DE58604 DE58607
18.	Alteon used a console with a 9600 baud rate, and the MP issued information faster than the console could receive it.	DE58737 DE58738
19.	When FTP was configured on a non-std data port and the port was same as the customized server data port, the data connection did not work.	DE58989 DE58990
20.	When REST API requests were received after a WBM idle timer timeout, the WBM idle timeout detection mechanism influenced related responses, causing a 401 error.	DE59593 DE59594
21.	When DSSP messages were received on the backup device, a software panic occurred.	DE58699 DE58702 DE58703
22.	The Alteon device was not indicated as the next hop in a traceroute from the client machine to the ISP router.	DE58624 DE58626
23.	After upgrade, in a VRRP environment, Alteon failed to accept the configuration when the same nwclass was associated to more than one VIP and both were part of same VR group.	DE58380 DE58381

Item	Description	Bug ID
24.	Executing the /c/slb/gslb/dnsresvip/ command automatically created an index for a new entry. However, if no other subsequent changes were made to this entry, the diff command did not show the new entry.	DE58577 DE58578
25.	After upgrade, there was a false detection of session table corruption, resulting in an autorecovery.	DE59001 DE59002
26.	SSL traffic without SNI could not be handled without decrypting the traffic. The fix was to allowing attaching the SSL policy while front-end and back-end SSL are disabled.	DE58832
27.	While a session having proxy port was being freed, a panic occurred.	DE58193 DE59841
28.	When deleting an LSA from a neighbor's retransmission list, a panic occurred for link-state ACK packets.	DE59110 DE59111
29.	In an SLB environment, when a filter was configured with reverse enabled for UDP traffic, traffic intermittently failed due to CPU spikes. Traffic never succeeded when the CPU went down.	DE58364 DE58365
30.	After deleting the FQDN server and applying and saving, then deleting the group and applying and saving, then adding a new FQDN server and a new group and applying, the error message "Application services engine is not synchronized with the current configuration" was issued. **Fix**: After removing the FQDN server, the real servers from AX are now also removed.	DE58110

AppWall Bug Fixes

Item	Description	Bug ID
1.	AppWall failed to extract the upgrade image.	DE58085
2.	While accessing the Forensics logs, received a 500 error.	DE59301

Fixed in 32.2.6.0

General Bug Fixes

Item	Description	Bug ID
1.	In an HTTP Modification rule, when clicking the path option, the Path field was not visible.	DE58288 DE58290

Item	Description	Bug ID
2.	In an ADC-VX environment, after executing the techdata, tsdump, or td-stats all commands, the MP CPU reached 100% utilization.	DE58250
3.	The Alteon NTP time jumped one month ahead.	DE58133
4.	At boot time, when AppWall crashed, Alteon also crashed.	DE58058
5.	When user configuring a scripted health check for port 25 (SMTP), during runtime the syslog was flooded with health check failure logs.	DE57867
6.	On receiving an ICMP_UNREACH packet, when matching an existing session with no real server, a panic occurred.	DE57860
7.	When a VRRP group was configured, sharing did not work properly.	DE57848
8.	In AppShape++ scripting, an early and unnecessary variable validation was removed from the validator function.	DE57762
9.	After upgrading from version 31.0.10.50 to 32.2.3.50, the GSLB DNS Summary Statistics displayed with a 0.	DE57675
10.	In Layer 2 mode when flooding to more than one port, fragmented packets (both in order and out-of-path) were lost.	DE57641
11.	In an ADC-VX environment, after enabling /cfg/slb/ssl/adv/bereuse, after a reset or reboot the value changed back to disabled.	DE57632
12.	When an unchained buffer was treated as a chained buffer in non-DPDK platforms, a one-time crash occurred. A check was added to packet captures to prevent this.	DE57568
13.	Due to an incorrect version comparison, TLS 1.1 displayed as disabled by default.	DE57561
14.	The length of the hostname in the HTTP healthcheck field was increased to 128 characters as required.	DE57548
15.	There was a high load on the queues from Alteon to AppWall, a session entered into the pending list twice, and activated after termination. This caused a panic.	DE57537
16.	When PIP mode was configured as address and HA mode as switch, if the same PIP range was associated to more than one service or real server, the PIP ARP limit was reached.	DE57517
17.	Alteon incorrectly validated unsupported path attributes (currently the BGP community path attribute).	DE57512

Item	Description	Bug ID
18.	Using WBM, the percent character (%) in the passphrase for private keys did not work.	DE57488
19.	Using WBM, could not renew existing certificates because of internal indexing issues.	DE57470
20.	When a DPDK initialization failed on any error except a queue error, it reverted to tuntap.	DE57371
21.	On a 9800 platform, after saving a configuration the following error displayed: mgmt: Flash Write Error	DE57349
22.	Using WBM, removing a target address from the SNMV3 did not remove the address from the AppWall UI server list.	DE57314
23.	When the SNMP OID hwApplicationSwitchNameInfo was probed, the port state incorrectly changed to disabled by referring to the wrong port flag state. This led the gateway health check to fail.	DE57304
24.	When the MP froze, the Watcher did not also kill the AW process of this MP.	DE57293
25.	When the real server rindex fell in a different word index group (rindex value /32), SLB traffic ignored the real server's weight for the roundrobin group metric.	DE57269
26.	After rebooting a master and it comes up with an RSTP setup, an ARP packet was sent and received over the backup's block port.	DE57251
27.	The interface IP address and floating IP address were swapped and applied. The IF IP address was added to the IP6 Neighbor Cache table as the new IF IP address, but was deleted as the old floating IP address.	DE57224
28.	After rebooting a vADC, the GSLB/LinkProof licenses were disabled.	DE57178
29.	After performing a recovery, the session capacity value was incorrect.	DE57147
30.	As per RFC 3416, the SNMP Get Next values should be in lexicographical format, but Alteon did not follow this for the FDB table and other tables. A fix was made only for the FDB table.	DE57060
31.	On a FIPS card, a session terminated while it was still pending for a task.	DE57049 DE57051
32.	After a period of no traffic, the race condition timing could lead to an AppWall restart.	DE56991

Item	Description	Bug ID
33.	OSPF was not able to send a link state update (redistributed route) to peed when the gateway went down.	DE56965
34.	In an SLB environment with HA and session mirroring enabled, real server current session statistics and redirect statistics displayed incorrectly in the /i/slb/virt x summary on the backup device. This resulted in traffic failure when the backup became the active.	DE56946
35.	A configuration with many real servers caused a delay in context switching, resulting in LACP messages not being handled.	DE56933
36.	Using WBM, when trying to modify the throughput limit, an error occurred. Added a REGEX to support all the throughput licenses.	DE56921
37.	After version upgrade, GEL licenses were rejected.	DE56887
38.	In an HA environment with vADCs, when trying to send more OSPF routes to the peer device, a panic occurred.	DE56836
39.	An incorrect FIPS license string (deprecated) caused a flow of FIPS tests.	DE56812
40.	When a service was configured in a non-existing VIRT, it remained unnoticed until the VIRT was defined.	DE56794
41.	Using WBM, the Edit Security Policy option did not display.	DE56783
42.	When mgmt was disabled and the syslog defined on mgmt, the new syslogs did not display in /info/sys/log.	DE56733
43.	There was a RADIUS Authentication failure because secret was not configured. No warning was issued for this.	DE56722
44.	After inserting a 1G SX Multimode transceiver, the following error displayed: “Cannot work with 1G transceivers.”	DE56713
45.	Alteon DPDK platforms dropped out-of-order fragmented packets.	DE56700
46.	The vconsole internally used Terminal MultiPlexer (TMUX), which is not available on DPDK-based platforms.	DE56691
47.	When trying to upload tech data when the management network was slow, an SCP timeout error occurred.	DE56655
48.	After applying the /info/sys/general command, the output was incorrectly 7612 S instead of 7612 SL.	DE56608
49.	While deleting an IPv6 configuration, a panic occurred. Added defensive validations.	DE56597
50.	Using WBM, the Monitoring > System > Capacity > Application Delivery page did not display capacity information.	DE56486

Item	Description	Bug ID
51.	Port 2233 was visible to public networks. The new behavior is that port is visible to a local host only (for example: 127.0.0.1:2233).	DE56399
52.	Using the CLI, after configuring a local add as a nwclass ID, after reboot, the configuration was not applied.	DE56336
53.	Using WBM, the configured Server Certificate group in a configuration did not display.	DE56289 DE56291
54.	Configuring the data class IP address with mask 0 caused a panic. Because mask 0 is invalid, the fix was to ignore it.	DE56281
55.	When IPv6 TCP small packets were received by the MP out of order via the data port, the memory associated with the packets was not returned (after the usage) to the pool of free small packets, causing problems for features allocating such packets.	DE56080
56.	On an ADC-VX, an NTP timeout occurred.	DE55856 DE55861
57.	In an SLB environment with forceproxy, the TCP policy/pushack worked as disabled even though it was enabled, causing a TCP retransmission problem.	prod00267404

AppWall Bug Fixes

Item	Description	Bug ID
1.	Integrated WAF: Websec module down/up events are shown in the device system logs.	DE57855
2.	Error API call when trying to change a tunnel operational status using AppWall API.	DE57217
3.	AppWall API - Get specific security event resulted in error.	DE57216
4.	Doc bug in AppWall API documentation	DE57200
5.	Integrated WAF: Incorrect information under syslog's DIP field.	DE56918
6.	Alteon is not sending syslog messages for integrated AppWall.	DE56861
7.	WAF XML file breaks Event detains into multiple queries.	DE56386
8.	Activity tracking refinement issue.	DE56277
9.	Multiple events from different sessions are seen with same transaction ID	DE56260

Fixed in 32.2.5.50

General Bug Fixes

Item	Description	Bug ID
1.	Using WBM, you could not renew existing certificates because of internal indexing issues.	DE57474
2.	When AppWall had memory pressure, traffic was bypassed and did not restart after 60 seconds.	DE57400
3.	When a DPDK init failed on any error except a queue error, the configuration reverted to TUN/TAP.	DE57375
4.	On a 9800 platform, after saving a configuration, the following error displayed: `mgmt: Flash Write Error`	DE57353
5.	Using WBM, removing the target address from SNMPv3 did not remove the address from the AppWall UI server list.	DE57318
6.	When SNMP OID hwApplicationSwitchNameInfo was probed, the port state incorrectly changed to DISABLED by referring to wrong port flag state. This led to a gateway health check failure.	DE57308
7.	The Watcher did not kill the AppWall process that was related to the MP.	DE57297
8.	SLB traffic ignored a real server's weight for the roundrobin group metric when the real server rindex was included in a different word index group (rindex value /32).	DE57273
9.	If the Interface IP address and floating IP address were swapped and applied, the IF IP address was added to the IPv6 Neighbor Cache table as the new IF IP address but was deleted as the old floating IP address.	DE57228
10.	After reboot a vADC, the GSLB/LinkProof license was disabled.	DE57182
11.	When performing a recovery session, the incorrect capacity value was displayed.	DE57151
12.	Per RFC 3416, the SNMP Get Next values should be in lexicographical order, but this was not implemented for the FDBtable and other tables. This issue was fixed only for the FDBtable.	DE57058
13.	After a certain amount of time with no traffic, race condition timing could lead to an AppWall restart.	DE56989 DE56995
14.	OSPF was not able to send a link state update (redistributed route) if there was a link failure or route change.	DE56969

Item	Description	Bug ID
15.	In an SLB environment with HA and session mirroring enabled, the real server current session statistics and redirect statistics were displayed incorrectly after issuing the command /i/slb/virt x summary on the backup device. It resulted in traffic failure when the backup became the active.	DE56944 DE56950
16.	A configuration with many real servers caused a delay in context switching, resulting in LACP messages not to be handled.	DE56931 DE56937
17.	Added REGEX to support all throughput licenses.	DE56925
18.	When Alteon tried to send more OSPF routes to a peer device, a panic occurred.	DE56840
19.	While trying to access SSH, a bad FIPS license string (which was also deprecated) caused a flow of FIPS tests.	DE56816
20.	When a service was configured in a non-existing VIRT, it remained unnoticed until the VIRT was defined.	DE56798
21.	Using WBM, the Security Policy option did not display.	DE56787
22.	When the management port was disabled and the syslog was defined on the management port, the new syslogs did not display when issuing the /info/sys/log command.	DE56737
23.	RADIUS Authentication failed because the secret password was not configured. In addition, no warning was issued for this issue.	DE56726
24.	After inserting a 1 G SX Multimode transceiver, the following error displayed: `Cannot work with 1G transceivers.`	DE56717
25.	Alteon DPDK platforms dropped the out-of-order fragmented packets.	DE56704
26.	When uploading Techdata when the management network was slow, an SCP timeout error occurred.	DE56659
27.	After applying the /info/sys/general command, the output of the command incorrectly displayed "7612 S" instead of "7612 SL".	DE56612
28.	While deleting an IPv6 configuration and adding defensive validations, a panic occurred.	DE56601
29.	To aid with a configuration that requires many real server health checks, the maximum and current values for real services was added to the /info/sys/capacity output.	DE56490
30.	When using the CLI to configure a local add as network class ID, after reboot the configuration was not applied.	DE56334 DE56340

Item	Description	Bug ID
31.	When small IPv6 TCP packets were received by the MP out of order via a data port, the memory associated with the packets did not return (after usage) to the pool of free small packets, causing problems for features allocating such packets.	DE56331
32.	Using WBM, a configured server certificate group did not display.	DE56295
33.	A check was added for packet captures to prevent a one-time crash that occurred when an unchained buffer was treated as a chained buffer on non-DPDK platforms.	DE55730

Fixed in 32.2.5.0

General Bug Fixes

Item	Description	Bug ID
1.	Could not save a configuration change and received the error `Flash Write Error`.	DE57353
2.	If there was no default Gateway defined or the Gateway failed, after a security scan there was total service outage.	DE56256
3.	When a burst of packets were sent to the MP for ARP resolution, subsequent packets were dropped when ARP resolution was already in progress for the first packet of a given destination, or when there was an RST from the client followed by a retransmission of a GET request, a connection drop occurred.	DE56152
4.	In an IPv6 environment, when the protocol is set to both for a virtual service, the lookup failed for the virtual service and the client traffic was dropped.	DE56137
5.	In an IPv6 environment, a specific virtual service could not be DNS-resolved by GSLB.	DE55998
6.	In an IPv6 environment, a specific virtual service could not be DNS-resolved by GSLB.	DE55993
7.	The HTTP modification rule for a host match did not accept a dot (.) in the match term.	DE55932 DE55934
8.	The translation to Chinese for the value slbNewCfgEnhVirtServApplicationType.13 was incorrectly translated as "basic slbit"; it should have been "SMTP."	DE55929
9.	Stuck sessions in AX caused another of issues, resulting in a panic.	DE55833

Item	Description	Bug ID
10.	Alteon lost communication with the LLS and entered the grace period.	DE55778
11.	Using WBM, the dot (.) character was not supported in an SSL policy name.	DE55720
12.	After an upgrade to version 31.0.12.0, a panic occurred because of null pointer access.	DE55710
13.	When processing some network elements having consecutive IP addresses as an exclude set, the network class configuration error " total IP range cannot be greater than 4294967295l" was issued.	DE55669
14.	When CDP was configured with a domain name, after the DNS resolution the request was framed using the resolved IP address in the HOST header field instead of the domain name.	DE55652
15.	On an Alteon 5412XL platform, the same cookie load-balanced to multiple real servers.	DE55597
16.	In an AppWall integrated in Alteon environment, a new secwa did not display in the AppWall Console.	DE55470
17.	The configuration migration tool duplicated the GSLB network for Inbound LLB rules.	DE55449
18.	The MP froze during the GEL active license periodic revalidation.	DE55434
19.	A DNS request matched the cache unexpectantly.	DE55407
20.	Layer 7 SNI-based LLB did not work with BWM enabled in Enforcement mode.	DE54451

AppWall Bug Fixes

Item	Description	Bug ID
1.	Source Threshold is not enforced by Activity Tracking's Anti-DDoS in certain cases in 7.6.7.0.	DE56123
2.	Parameter Security filter might fail to load certain Regular Expressions correctly.	DE56110
3.	Rare case where additional changes to AppWall configuration was not synced to the backup.	DE56051
4.	Some Security Events have the wrong Security Event Description.	DE55887
5.	Rare case under heavy traffic causing a parsing mistake that can lead to traffic being blocked.	DE54949

Item	Description	Bug ID
6.	Requests with very large number of parameters may take long to process.	DE54905
7.	Manual SUS update page is not accessible when there is no Internet connection.	DE54670
8.	Special characters cannot be used in paths in AllowList refinements.	DE54755
9.	API documentation for adding a web server into a web farm was not correct.	DE54741
10.	Option to download AppWall forensic events as a CSV file is missing.	DE54924

Fixed in 32.2.4.60

General Bug Fixes

Item	Description	Bug ID
1.	In an ADC-VX environment, when a packet capture was exported to an SCP server, the capture status remained as “upload in progress” until the device rebooted.	DE55387
2.	During ADC-VX upgrade to version 32.4.1.50, the following error message displayed: `"" <<<<<<<<<<<<<< Do you wish to run the analysis ? y or n >>>>>>>>>>>>""if you choose no , there will be no new entry in file`	DE54464
3.	After upgrading to 32.2.4.0 there was a continuous vADC panic.	DE55674
4.	On a FIPS-II 6024 platform, there was a memory leak.	DE55603 DE55607
5.	There was a health check issue with a buddy real server.	DE55480
6.	A type discrepancy in the URLF subcategory printing caused Alteon to reboot.	DE55360
7.	There was no support for non-interactive mode for the "/c/slb/sync/auth passphrase xxxxxx" command, causing a missing configuration sync authentication toggle.	DE55337
8.	Could not apply the TACACS configuration during a timeout cycle.	DE55314
9.	Live packet capture did not work.	DE55281
10.	A type discrepancy in the URLF subcategory printing caused Alteon to reboot.	DE55260 DE55264

Item	Description	Bug ID
11.	Using AppWall integrated with Alteon, all Web applications stopped.	DE55234 DE55238
12.	Routes through GRE/IPinIP tunnels did not display after running the /i/sys/capacity command.	DE55211
13.	Site resources were not cached by FastView	DE55128 DE55132
14.	After connecting to the GEL server, the Alteon console was flooded with some junk logs every 18 seconds.	DE54944
15.	Using WBM, you could not create a service using TCP 995.	DE54878
16.	Allow filters failed to decrypt IPv6 traffic.	DE54824
17.	The error message "Someone else is doing the diff [flash] try again!" was issued.	DE54814
18.	When HAID 2 was configured, /info/slb/virt displayed the wrong Virtual MAC ID.	DE54759
19.	After upgrading, Alteon was not able to push the intermediate certificate and failed to apply the configuration.	DE54733
20.	After Revert Apply, the gateway flapped in Alteon running version 31.0.9.0.	DE54685
21.	Config sync was unsuccessful. The Application Services Engine was not synchronized with the current configuration.	DE54676
22.	The WBM menu was disabled, but you could use CLI to modify settings.	DE54662
23.	Performing proxy processing on an OSPFv6 packet caused a panic and reboot.	DE54648
24.	During a new image upload, if the available disk space was low on a device, an error message was only issued after 94% of the download completed. Now a warning message about low disk space is issued before the download starts. 0	DE54637
25.	A BGP peer established a connection and changed back to the Connect state.	DE54625
26.	Could not upgrade from Alteon VA version 32.2.0.0 to 32.2.3.0 version.	DE54606 DE54610
27.	When GW 1 was deleted, DNS health checks were not generated but ICMP health checks were generated.	DE54588

Item	Description	Bug ID
28.	APSolute Vision sent an incorrect REST query to Alteon.	DE54487 DE54491
29.	There was error while applying a configuring for a network class.	DE54482
30.	There was an Alteon SSL inspection and IWSVA Integration Issue.	DE54469
31.	The Packet Capture tool did not capture all the packets sent from the SP to the MP.	DE54433
32.	When the TACACS server was configured with command logging, Alteon failed to identify the global commands cdump, telnet, traceroute as global commands. Instead, it tried to process from the local menu where it does not exist, resulting in a panic.	DE54424 DE54428
33.	Using WBM, downloaded techdata and core dumps were corrupt.	DE54419
34.	The SNMP overload health check mechanism stopped working when it was added to the logExp health check.	DE54410
35.	The fragmented CPU size was increased from 16K to 64K.	DE54401
36.	Using the WBM, a VLAN name of 32 characters was allowed, while in the CLI, only 31 characters was allowed.	DE54375 DE54386
37.	In the Real Server configuration pane, the HA master displayed FQDN instances.	DE54388
38.	There was a bug in the Advisory Tool upgrade.	DE54376

AppWall Bug Fixes

Item	Description	Bug ID
1.	The communication properties option in the wizard was not relevant. It has been removed.	DE51197 prod00272955
2.	SC6307 – In WBM, VLAN sometimes would not function properly if the VLAN was configured using the Java applet in a previous version, and AppWall was upgraded to newer version.	DE54671
3.	The AllowList REST API call was changed incorrectly after upgrade from version 7.5.8 to version 7.6.6. The REST API call is now fixed.	DE54742
4.	The exported Forensics events was not in the correct XML format.	DE55291

Fixed in 32.2.4.0

General Bug Fixes

Item	Description	Bug ID
1.	Alteon failed to identify cdump, telnet, and traceroute as global commands and tried to get command details from the current menu, resulting in accessing invalid memory and causing a panic.	prod00278132
2.	When using HTTP/2 after login, traffic stops working.	prod00278052
3.	In a LinkProof for Alteon environment, there were Intermittent ICMP packet drops. When pinging from the same sequence number, the ping reply packets dropped intermittently.	prod00274632 prod00276798
4.	In an SLB environment with a pbind client IP address, persistence was not maintained.	prod00275771
5.	When a device came up after reboot, the HA status displayed as NONE because the HA state was recorded based on the current HA service group state for which the apply was in process.	prod00275321
6.	After upgrading to version 32.2.3.0, Alteon rebooted often due to a panic.	prod00277796
7.	After attempting to generate new Web Management Certificate, Alteon crashed.	prod00278178
8.	When the primary WAN link went down and the backup WAN link took over, an incorrect syslog message displayed.	prod00276594
9.	AppWall for Alteon issued the following error message: Server Error: "Get of FilterAdv/Database failed!	prod00277201
10.	A confusing configuration resulted while implementing LDAP(S) health check.	prod00274926 prod00275743
11.	On DPDK platforms, Interface errors for port statistics were issued.	prod00277490
12.	In an Azure environment, Alteon VA crashed.	prod00276479 prod00276485
13.	When an HTTP modification string was configured with multiple escape sequences, Alteon did not insert an escape sequence.	prod00276803
14.	In a DSR environment, there was a discrepancy between /info/swkey and virtual server statistics.	prod00277836
15.	When using HTTP/2 after login, traffic stops working.	prod00278068
16.	Changes to the SSL policy caused a corruption.	prod00278255

Item	Description	Bug ID
17.	On an Alteon VA, Alteon reset the connection when traffic failed over.	prod00277405
18.	ICAP responses were not forwarded to the client.	prod00276507
19.	SSL traffic caused a panic.	prod00278065
20.	BGP 4 Byte ASN was not compatible with Cisco Nexus 9K and Huawei routers.	prod00276712
21.	Traffic was forwarded to a failed WAN real server.	prod00276354
22.	On an Alteon 5424 platform with 24G RAM and software version 32.4.1.10, the maximum sessions remained as 11M even though the sesscap value was 100%.	prod00277363
23.	There were many FLOOD entries being created in the FDB table for the PIP MAC. This caused some of the traffic to fail.	prod00277244
24.	In a GSLB environment, Alteon became stuck with high MP CPU utilization.	prod00276518
25.	While STG information was sent from an ADC-VX to a vADC, a panic occurred.	prod00278077
26.	During an upgrade to version 32.2.30 or later, the configuration became stuck in diff.	prod00276739
27.	An invalid hypervisor type was set for virtual platforms.	prod00276258
28.	Using WBM on a vADC, could not renew an SSL certificate.	prod00276406
29.	Using WBM, a user could change the admin password while being authenticated via TACACS or RADIUS. Usually a user is not allowed to change the admin password when logged in with "admin Privileged" using TACACS or RADIUS.	prod00277354
30.	IPv6 SNMP queries over the data port were not working because checking for management access with the ingress data port failed.	prod00277307
31.	With two vADCs hosted on the same ADC-VX, all applications stopped working.	prod00277921
32.	In an SLB environment, after a config sync was performed with PIP sync disabled. Alteon did not replace the client IP address with a PIP.	prod00277516

Item	Description	Bug ID
33.	The priorities for remote real servers among different GSLB network did not behave as expected. With this version, priority is given to nwclasses matching in added networks. As a result, if there is a SIP match for one of the networks, a network with SIP=any will not be considered. If there is no SIP match for networks with SIP configured, then a network with SIP=any will be considered. Priority is considered among the real servers of the matched network.	prod00276833
34.	Trend Micro's IWSVA (AV) in ICAP mode (with Alteon acting as ICAP client) was only partially working.	prod00277013
35.	Added GSLB site IP address validation.	prod00277093
36.	Using WBM, when starting a packet capture, unexpected data displayed for /c/sys/alerts when the packet capture filter string was set to more than 128 characters.	prod00275469
37.	The Alteon 6024 platform rebooted due to a panic.	prod00276358
38.	An HTTP header modification value set to None was considered as valid input.	prod00277182
39.	Connections to a VIP closed abruptly.	prod00276582
40.	When the management port was disabled, syslog messages were not sent on the data port.	prod00278036
41.	The backup group status in a content rule displayed an incorrect status when the backup group was not directly associated to any service.	prod00276753
42.	In an IPv6 SLB environment with an IPv6 HTTP health check and IPv6 HA configured, the memory allocated for HTTP HC was not freed, which led to a memory leak.	prod00276963
43.	During stress traffic, a panic occurred.	prod00278080
44.	Using WBM, you could not edit the IP address for a new Outbound LLB Rule.	prod00277382
45.	Using WBM, during configuration sync, continuous fetching of the virtual server table caused a panic.	prod00277465
46.	During SNMP polling, a panic occurred.	prod00277992
47.	After HA failover, Alteon lost router connectivity in order to reach real servers.	prod00277716
48.	When changing to the default configuration, the runtime session capacity was not reflected.	prod00276871

Item	Description	Bug ID
49.	When importing a configuration with BGP, Alteon issued Notice messages with non-ASCII characters.	prod00275645
50.	Throughput Threshold alerts displayed despite the threshold level being set 0 (disabled).	prod00276299
51.	Using WBM, could not configure BGP 4-byte-ASN.	prod00276811
52.	After upgrading to version 31.0.11.0, SSL offload did not work properly.	prod00276273
53.	Could not log in to AppWall.	prod00275568
54.	The port speed capability was not handled for the MR platform XGE interface while dumping the port configuration and port auto-negotiation configuration options, resulting ins no diff configuration.	prod00275658
55.	In an SLB environment, when the session move operation was executed, in some cases this operation was not reset on one of the SPs, which resulted in all subsequent session move operations to fail on that particular SP.	prod00276336
56.	Using WBM, when "Return to Last Hop" was set for a virtual server, an additional field type was also set internally.	prod00276930
57.	On a vADC, incorrect Throughput Alert messages were issued.	prod00275925
58.	When the Alteon HA state changed from Master to Backup, the gateway and real server's health checks failed.	prod00278211
59.	When changing from ena to dis and vice versa, could not apply the /cfg/l3/ha/switch/filtpbkp command.	prod00277752
60.	The Alteon NG+ license did not apply the 5 vADC license.	prod00276635
61.	VRs and Switch HA and Service HA configurations sometimes would flap or go into the INIT state after synching the configuration from the secondary device to the primary device if there was a difference in the configuration between the two devices.	prod00276499
62.	After a panic, the Admin context went into a reboot loop.	prod00276326
63.	In an SLB environment with preemption disabled for the primary real server, when it was in the failed state and the backup real server became the primary, the original primary real server became the backup server when its health check came UP, even though preemption was disabled.	prod00277334
64.	Could not sync or apply changes.	prod00276400

Item	Description	Bug ID
65.	Using the preempt disabled feature, a primary real server that was moved to the OPER DIS state by the HC module when the backup was UP for the service, continued to be in the OPER DIS state even when the "backup" and "preempt dis" settings were removed from it.	prod00276614
66.	When processing the second fragment destined for the Alteon interface when the redirect filter was configured, Alteon panicked.	prod00277479
67.	When logged in as a TACACS or RADIUS user, could not modify or create SNMPv3 authentication or privacy passwords.	prod00276999
68.	The Intermediate CA certificate could not be imported due to unexpected max limit.	prod00278074
69.	There was a disparity of the MAC address between the primary and backup devices.	prod00275353
70.	After deploying a TCP optimization policy, the software panicked.	prod00277923
71.	An unexpected LACP changed state resulted in the device switching to BACKUP state.	prod00278165
72.	After upgrading to version 32.2.3.0, the device constantly rebooted due to a panic.	prod00278290
73.	An explicit proxy caused unexpected behavior for HTTP/HTTPS traffic.	prod00278450

AppWall Bug Fixes

Item	Description	Bug ID
1.	Scenarios where the ‘Replace HTTP Reply Messages with Custom Messages’ feature did not function.	DE53496
2.	After performing a ‘Revert’ for AppWall in Alteon, you must refresh the page.	DE50247
3.	For AppWall in Alteon, in some scenarios, the AppWall page is grayed-out for a brief period while applying a new configuration.	DE51355
4.	For AppWall in Alteon, in rare cases, when applying configuration changes, AppWall’s “Login” page is shown and the login will not succeed. In such cases, a restart to AppWall’s service is needed.	DE51346
5.	Source Blocking module might not be enforced on IPv6 sources identified using an HTTP Header, as in the case of CDNs.	DE51975

Item	Description	Bug ID
6.	Auto Discovery should be set manually to “Resume Auto Discovery” when enabling “Auto Policy Generation” on an already-configured application path in the security policy.	DE52165
7.	When using Source Blocking with IPv6 addresses, at least one IPv4 address must exist in the list for the feature to be enabled.	DE49832
8.	Rare case leading AppWall to restart.	DE53577
9.	Scenarios where the 100-Continue header was not sent correctly by AppWall in Alteon, causing the transaction to fail.	DE53201
10.	Rare case when refining parsing properties failed with a server error.	DE53336
11.	Event log filters by date may include additional events in some scenarios.	DE54073
12.	Rare case that led to the error "Server Error: "Get of FilterAdv/Database failed!" in the WebUI for AppWall in Alteon.	DE51538
13.	Scenario where sync fails for AppWall in Alteon.	DE53151
14.	AppWall in Alteon does not parse parameters which value contains Emoji Unicode characters.	DE51007
15.	LDAP group-based authentication may fail in some scenarios.	DE53520
16.	Some scenarios were Redirect Validation was not enforced on specific URL prefixes.	DE53373
17.	A Vulnerability security event is wrongly classified as "HTTP Method Violation".	DE53368
18.	Wrong title in "Threat" field for FastUpload events.	DE53379
19.	LDAP group authentication may fail login in some scenarios.	DE53261
20.	Rare case where transactions were blocked while the tunnel Operational Mode is in Bypass.	DE52453
21.	Wrong tunnel name reported on Source Blocking events in some scenarios.	DE52002
22.	Scenario where Source Blocking stopped blocking blocked sources after a configuration change.	DE52167
23.	LDAP attribute cannot be modified when using LDAP group-based authentication.	DE53760
24.	A specific type of injection was not detected.	DE53785
25.	Scenario where LDAP configuration was not kept after reboot.	DE54019

Item	Description	Bug ID
26.	Rare case where an error was shown in WebUI after adding publishing rules.	DE53413
27.	Filtering Event Log based on predefined forensics view may not work in some cases.	DE54045

Fixed in 32.2.3.50

Item	Description	Bug ID
1.	BGP 4-byte ASNs were not compatible with Cisco Nexus 9K and Huawei routers.	prod00276567
2.	Using WBM, could not configure BGP 4-byte-ASN.	prod00276623
3.	An invalid hypervisor type was set for virtual platforms.	prod00271421
4.	After syncing the configuration from the secondary device to primary device, virtual routers, Switch HA, and/or Service HA may flap or go into the INIT state if there was a configuration difference between two devices	prod00276317
5.	Using APSolute Vision, when Alteon with no AppWall license was configured with ADC Analytics, an MP memory leak occurred, resulting in all MP related processes to not function.	prod00276068
6.	Traffic was forwarded to a failed WAN real server.	prod00276183 prod00276357
7.	When a starting packet capture through WBM, incorrect data displayed when running /c/sys/alerts when the packet capture filter string was set to more than 128 characters.	prod00275357
8.	The backup group status in a content rule displayed the incorrect status when the backup group was not directly associated to any service.	prod00276622
9.	An IWSVA (AV) in ICAP mode (with Alteon acting as the ICAP client) was only partially working.	prod00276988
10.	Connections to a VIP randomly closed.	prod00276581
11.	Fixed a panic scenario based on case prod00275591.	prod00276361
12.	There was a disparity of the MAC address between the primary and backup devices.	prod00275352
13.	In an IPv6 SLB environment with an IPv6 HTTP health check and IPv6 HA configured, the memory allocated for the HTTP health check was not freed, which led to a memory leak.	prod00276964

Item	Description	Bug ID
14.	Using WBM, the HTTP health check edit pane did not display configured settings and values.	prod00275725
15.	When a device came up after reboot, the HA status displayed as "NONE" because the HA state was recorded based on current HA service group state for which an Apply was in process.	prod00275638
16.	With AES was used for privacy/encryption, the initialization vector was not set properly, causing an AES encryption failure.	prod00276311
17.	The device banner and /boot/cur displayed different active Alteon versions on the ADC-VX.	prod00276980
18.	The port speed capability was not handled for the MR platform XGE interface while dumping the port configuration and port auto-negotiation configuration options, resulting in no diff configuration.	prod00275657
19.	After upgrading to version 31.0.11.0, SSL offload did not work correctly.	prod00276281
20.	Using WBM, the HTTP health check edit pane did not display the configured settings and values	prod00275722
21.	Using LinkProof for Alteon, intermittent ICMP packet was dropped. After pinging from same sequence number, the ping reply packet intermittently dropped.	prod00276799
22.	In a GSLB environment, the device became stuck with high MP CPU.	prod00276545
23.	Incorrect throughput alert messages displayed on vADCs.	prod00275927
24.	In an SLB environment, when the session move operation is executed, in some scenarios this operation was not reset on one of the SPs, which leads all subsequent session move operations to fail on that particular SP.	prod00276342
25.	Added GSLB site IP address validation.	prod00277092
26.	The Alteon NG+ license did not apply the 5-vADCs license.	prod00276640
27.	Using the preempt disabled feature, a primary real server that is moved to the OPER DIS state by the health check module when the backup is UP for the service continues to be in OPER DIS state even when the "backup" and "preempt dis" configuration is removed from it.	prod00276613
28.	Alteon VA crashed in an Azure environment.	prod00276482
29.	When importing a configuration with BGP, notice messages were issued with non-ASCII characters.	prod00275644

Item	Description	Bug ID
30.	Using WBM, when the Return to Last Hop was set for a virtual server, an additional field type also was set internally.	prod00276929
31.	ICAP responses were not forwarded to the client.	prod00276508
32.	When upgrading to version 32.2.30 or later, the configuration became stuck in diff.	prod00276745
33.	There were many flood entries created in the FDB table for the PIP MAC, causing some of the traffic to fail.	prod00277027

Fixed in 32.2.3.0

Item	Description	Bug ID
1.	Could not log in to AppWall because the AppWall token did not match the Alteon token.	prod00275564
2.	A long certificate name was not accepted when attached to back-end policy.	prod00272989
3.	Site selection rules displayed the MIB name instead of the Rule ID.	prod00272405
4.	NTP requests were not sent in an OSPF network.	prod00274152
5.	When viphlth was enabled, there was no response to ICMP health checks directed at VIPs.	prod00274567
6.	The GSLB DNS client network rules real server selection pane was too small.	prod00272404
7.	After upgrading to version 32.2.2.0, constant VRRP flaps with MP keepaliveFailure occurred.	prod00274443
8.	While loading the configuration from flash, an Apply failure occurred during bootup time.	prod00274156
9.	In a GEL Environment, the Alteon VA prompt license server was constantly reestablishing.	prod00274121
10.	With lower BFD rx-int configured, when there was a change in the session table type between ABT and PBT, the BFD session went down, causing deletion of the BGP session. This issue has been addressed by yielding control to the SP to send BFD packets.	prod00272433
11.	In an AppWall integrated with Alteon environment, the Websocket bypass feature stopped.	prod00274445
12.	While running a scan over SSH, Alteon panicked.	prod00274764
13.	After a device reset, could not connect to the Alteon VA management IPv6 address.	prod00274941

Item	Description	Bug ID
14.	In an AppWall integrated with Alteon environment, there were multiple "Networking Problem" events.	prod00274862
15.	Using WBM, could not change the default of factory configuration to save the management configuration.	US64628
16.	With Layer 7 Application Acceleration, some connections were dropped in the middle.	DE50652
17.	Using LinkProof NG, when the upload/download limits for the WAN link were configured to be greater than 455 Mbps, WAN link bandwidth utilization displayed incorrect statistics.	prod00273016
18.	Health checks failed due to a corruption in the small/medium/jumbo packet free pool list because of a synchronization problem in the ARP module.	prod00274561
19.	SIP INVITE and fragmented packets were not forwarded to real servers.	prod00273235
20.	Using WBM, a Notify View ISO could not be configured without creating a custom Notify Tag.	prod00273725
21.	Using WBM, could not configure the sync passphrase.	prod00274327
22.	After running /stat/slb/clear, only part of the filter statistics was cleared, and the others remained cleared.	prod00272888
23.	A vADC panicked.	prod00274793
24.	Configuration sync failed with a timeout.	prod00273099
25.	Using WBM, when changing the "DNS Responder VIP" from "dis" to ena" and vice versa, Alteon did not update the flags that are used to identify the config change. Because of this, Alteon found no config change during Apply and an issue occurred.	prod00273282
26.	After resetting the admin password from the console, the password displayed in clear text in diff flash.	prod00274145
27.	In a GSLB environment, Alteon did not resolve a DNS query even though the remote real servers were UP.	prod00272897
28.	While running a scan over SSH, Alteon panicked.	prod00274797
29.	After a Submit via QAS, a service's rport was overwritten.	prod00272874
30.	Using config sync, disabling virt synchronization removed virtual servers from the backup device.	prod00273196
31.	A vADC could not handle any data traffic including a health check. The vADC did not restart after an SP panic/freeze.	prod00274323

Item	Description	Bug ID
32.	SNMP data of polling interface details incorrectly displayed the interface type.	prod00273386
33.	A vADC panicked, became stuck, and was not able to handle any traffic.	prod00274804
34.	After reverting an unsaved configuration, the HA State remained INIT and was not updated automatically.	prod00272980
35.	Using WBM, an Invalid EC Key Size (6). error displayed while generating an SSL certificate an RSA key.	prod00273179
36.	After upgrading to version 32.2.1.0, session logs were not generated.	prod00272743
37.	Handled CVE 2019-11477, CVE 2019-11478, and CVE 2019-11479 using a Linux Kernel patch.	prod00273353
38.	Alteon indirectly caused a vulnerability to the DNS cache poisoning attack.	prod00269190
39.	When idbynum was enabled, there were issues with Revert Apply.	prod00273940
40.	When enabling an HTTP/2 policy, a panic occurred.	prod00273687
41.	Using Passive FTP, an RTS session was created instead of a filter session for FTP data traffic.	prod00272718
42.	When Alteon sent syslog messages, a panic occurred.	prod00272887
43.	A MAC flap on Layer 2 occurred when the DUT was connected on one port and the server was connected on a different port.	prod00273062
44.	Using APSolute Vision, importing a certificate in Alteon did not work with the ADC + Certificate Administrator role.	prod00274709
45.	When VLAN 1 was disabled and an Apply was done for any config change, the ping response to the interface was delayed, causing a timeout.	prod00273596
46.	Was not able to configure service 111 for TCP and UDP.	prod00272575
47.	IEEE 802.3 standard protocol packets (such as STP packets that run over LLC) sometimes were incorrectly classified as packets with a length error by the Fortville MAC. The CRC was not stripped from such packets, and the RLEC counter was incremented. These packets later caused problems when they were transmitted with the unstripped CRC to other entities in the network.	prod00272402
48.	Alteon was rebooted unexpectedly by Watchdog.	prod00273479

Item	Description	Bug ID
49.	A packet capture's TCP stream displayed corrupted data due to TSO allocated buffers.	prod00269186
50.	When the DNS virtual service protocol is UDP Stateless, HTTP and FTP services failed for IPv6 traffic.	prod00273832
51.	Using WBM, when VIPs were added to/removed from the HA service list, Alteon panicked.	prod00273658
52.	After Applying configuration changes, VIPs stopped responding.	prod00272576
53.	Using WBM, there was an HTTP modification rule configuration issue.	prod00273396
54.	Using WBM, the Maximum Session Number was not changed after adding a CU. It only was changed in CLI.	prod00274757
55.	After upgrading to version 32.2.1, the MP CPU utilization spiked.	prod00273889
56.	In a GSLB with VRRP/HA environment, after applying a configuration, the DSSP health checks failed.	prod00273181
57.	A configurational change to shutdown did not display correctly under /cfg/slb/group x/cur.	prod00272733

Fixed in 32.2.2.50

Item	Description	Bug ID
1.	SNMP data in the polling interface details incorrectly displayed the interface type	prod00273296
2.	Using WBM, when VIPs were added to/removed from the HA service list, a panic occurred.	prod00273460
3.	When the DNS virtual service protocol was UDP stateless, the HTTP and FTP services failed for IPv6 traffic.	prod00273709
4.	When reverting an unsaved configuration, the HA state remained INIT did not updated automatically.	prod00272958
5.	In a GSLB environment, Alteon did not resolve a DNS query even though the remote real servers were UP.	prod00272749
6.	In an Alteon VA environment, the /stats/slb/clear command did not clear all filter statistics.	prod00272788
7.	Using /cfg/slb/group x/cur, configurationally changing to "shutdown" did not displayed correctly.	prod00272696
8.	Using config sync, disabling virtual synchronization removed virtual servers from the backup device.	prod00273176

Item	Description	Bug ID
9.	Using WBM, generating a certificate resulted in the following error: `Invalid EC Key Size (6)`	prod00272033
10.	After upgrading to version 32.2.1.0, the MP CPU spiked.	prod00273206
11.	After upgrading to version 32.2.1.0, session logs were not generated.	prod00272627
12.	After resetting the admin password from the console, the new admin password displayed in clear text in diff flash.	prod00272628
13.	When VLAN 1 was disabled and applied for any configuration change, the ping response to the interface was delayed, causing a timeout.	prod00273436
14.	SIP INVITE and fragmented packets were not forwarded to real servers	prod00272668
15.	When a Submit occurred via QAS, the rport service was overwritten.	prod00272755
16.	Using LinkProof NG, when uploading or downloading WANlink limits that are configured to greater than 455 Mbps, WANlink bandwidth utilization produced incorrect statistics.	prod00273015
17.	The site selection rules displayed the MIB name instead of the Rule ID.	prod00272850
18.	Using Passive FTP, the RTS session was created instead of the filter session for FTP data traffic.	prod00272727
19.	Using WBM, when changing "DNS Responder VIP" between dis to ena, Alteon did not update the flags that are used to identify the configuration change. Because of this, Alteon did not recognize the configuration change during apply, causing a problem.	prod00273456
20.	When the DUT connected to one port and the server was connected to a different port, a MAC flap occurred on Layer 2.	prod00273068
21.	Alteon rebooted with a power cycle.	prod00272624
22.	In a GSLB with VRRP/High Availability environment, after applying a configuration, DSSP health checks failed.	prod00273182
23.	Was not able to configure service 111 for TCP and UDP.	prod00272610
24.	GSLB DNS client network rules real server selection window is too small.	prod00272847
25.	Alteon rebooted unexpectedly by Watchdog	prod00273482
26.	When enabling an HTTP/2 policy, a panic occurred.	prod00273787

Item	Description	Bug ID
27.	When applying configuration changes, the VIP stopped responding.	prod00272780
28.	Sending syslog messages caused a panic.	prod00272884
29.	Using WBM, the HTTP modification rule configuration had problems.	prod00273397
30.	When a lower BFD rx-int was configured, when there was a change of the session table type between ABT and PBT, the BFD session went down, causing the BGP session to be deleted. This issue was addressed by yielding control to the SP for sending BFD packets	prod00272646

Fixed in 32.2.2.0

Item	Description	Bug ID
1.	Using APSolute Vision, if you configured a virtual server, the Sync button to synchronize the configuration with the backup virtual LB was grayed out.	DE33418
2.	On a 6024 platform with 128GB RAM, In an environment that uses jumbo frames (with /cfg/l2/mtu set to greater than 1500), the config sync send operation fails when all the jumbo packets are consumed due to an SNMP memory leak.	prod00273909
3.	Alteon sends multiple requests to the RADIUS server for one login to WBM.	prod00270429
4.	Tunnels displayed automatically under the "Default Web Application" menu without an option to remove them.	prod00271288
5.	Alteon did not display the ICAP notification page to the client browser.	prod00270816
6.	Updated the online help for IPv6 local networks to "rem6 <Local Network v6 Address entry index>" / "rem <Local Network v4 Address entry index>" .	prod00270457
7.	After applying ab IPinIP tunnel configuration on a DSR service, an error was issued.	prod00269596
8.	In an AppWall in Alteon environment, the generated syslog had missing values.	prod00271339
9.	Using WBM or SNMP, when a GSLB network prefix we configured, the IPv6 mask configuration did not get set properly. This caused improper matching of the GSLB network during DNS request processing.	prod00269737

Item	Description	Bug ID
10.	The VRRP status remained as Active-Active even if related VRs were erased, when that status should have changed to Active-Standby.	prod00271605
11.	In an AppWall in Alteon environment, the download failed when the secwa was applied in inline mode on the Alteon VIP when the file size was more than 50Mb.	prod00270992
12.	A gmetric network does not work with the IPv6 nwclass having an element with a prefix 96 or less.	prod00269710
13.	Using WBM, default group 1 displayed without any changes made to it, while in CLI the group did not display unless changes were made to it.	prod00271477
14.	Using WBM, could not assign a VLAN to an interface.	prod00271061
15.	Using WBM, Alteon panicked when generating techdata.	prod00271962
16.	Using the CLI, creating client network rules with IPv6 was limited to 32 characters.	prod00270733
17.	In AppWall, after changing the publishing rules, the configuration was deleted when synching from the master to the backup,	prod00271685
18.	When RTSRCMAC is enabled and the gateway is disabled, Alteon does not return UDP/SIP virtual traffic to the client.	prod00270859
19.	Using WBM, an AppShape++ script with the incorrect syntax was allowed, which corrupted the configuration upon save.	prod00270537
20.	The current and total session counters were not accurate in server group statistics.	prod00271249
21.	In an AppWall in Alteon environment, activity tracking displayed 10.10.10.10 as the source ID in the security log for IPv6 clients.	prod00269417
22.	AppWall in Alteon security logs were not populated.	prod00272032
23.	When trying to collect the tech support file from the device, the device status changed from Master to Standby due to an "MP keepaliveFailure detected in SP" error.	prod00271714
24.	After changing all of the IP addresses of a single network to different IP address, non-existing MACs remained in ARP table.	prod00272260

Item	Description	Bug ID
25.	In an SLB environment, when the primary group became operational, the backup group's session table was removed. As part of the fix, the session entry is removed if the real server is not enabled under the group. In this scenario, this condition failed because the session's real server that is backed up is removed from the group when the primary real server becomes operational. This leads to removal of the backup real server's session entry when the primary real server comes up.	prod00270615
26.	The Alteon secondary device was inaccessible via the mgmt port and console.	prod00271312
27.	If a bandwidth management contract is associated to a traffic pattern and the TOS overwrite feature is enabled, a packet capture did not reflect the DSCP field modification.	prod00270090
28.	After a vADC rebooted from a panic, that part of the configuration was lost.	prod00271650
29.	The STG-VLAN configuration failed to apply on reboot because the number of parameters exceeded 64. Fix: After upgrade, perform the configuration and save, then reboot.	prod00271341
30.	Using WBM, the user lost access to a vADC.	prod00270783
31.	After a failover, the VRRP backup sent advertisements.	prod00271957
32.	When a user tried to configure a group "metric response" with the dynamic weight SNMP health check, a warning message was issued.	prod00269082
33.	A standalone device rebooted with a software panic.	prod00271231
34.	The binary health check failed with a timeout even through the checked server replied with unexpected value.	prod00271037
35.	After an interface related VLAN was deleted and then added back, the Layer 3 interface stayed down.	prod00272240
36.	After creating a Notify Tag from Configuration > System > SNMP > SNMPv3 > Notify Tags, opening the new Notify Tag displayed the content of a different Notify Tag.	prod00269989
37.	After rebooting the device, with configuration changes in diff, received errors after Apply.	prod00270495

Item	Description	Bug ID
38.	After upgrading from version 30.5.8.0 to 31.0.9.0, vADC-1 booted with configuration in diff. The configuration could be applied but generated the following error: ERROR mgmt: Error: Save not done. Application services engine is not synchronized with the current configuration.	prod00271393
39.	The EDNS+Source network-based name resolution failed for certain source addresses. The GSLB query failed when it contained the EDNS extension with the client subnet address, which fails to match the network class configuration.	prod00270959
40.	A real server under /info/slb/group displayed in the BLOCKED state. When a group was not attached to any service or filter, no svc-pool entry was created for it. As a result, the wrong group was displayed with the /info/slb/group command. Fix: If at least one group is configured for the real server with no svc-entry corresponding to the group, the svc-pool entry is preserved with the default health check and group ID. In addition, if there is not any svc-entry corresponding to the group that is being queried, the default health check for the real server is displayed.	prod00272042
41.	When an LDAP bind request packet length exceeded 127 (for contents greater than 116, including LDAP markers), multi-byte representation was not used, which caused Alteon to not generate the advanced health check type LDAP as expected.	prod00269895
42.	After running the /c/slb/cur command, if the configuration contained any AppShape++ script associated to a filter, Alteon panicked.	prod00270299
43.	XML fragmented files over SIP were not forward to real servers. As a fix, the maximum dechunk datagram was resized from 8200 to 16400.	prod00270949
44.	When the filter action was "nat", the client NAT IP address options were missing from the Dynamic NAT tab	prod00272364
45.	When the LDAPS module received the response from the server, the timestamp was not updated properly. As a result, the response time was calculated incorrectly, resulting a very long response time.	prod00270545

Item	Description	Bug ID
46.	PIP count validations for limiting the number of ARP/NBR entries in non-HA mode were not available. This allowed the user to add more than the maximum allowed entries in non-HA mode, and when the user switched to HA mode, the validations issued errors. As a fix, added the same set of validations for non-HA mode. In addition, maximum PIPs are now 2K and the number of ARP and NBR entries are 2K each.	prod00268389
47.	The Info/slb/group command displayed the incorrect VLAN for unavailable servers.	prod00270185
48.	If the link was down when the STG was off and "blockport" was enabled, the incorrect port state was assigned to a LAG member port after reboot.	prod00271622
49.	On a vADC and standalone, entering the command blkport disable caused a panic.	prod00270659
50.	When running a vDirect script in Alteon, received a timeout.	prod00270588
51.	In an ADC-VX environment, when fetching the SSL chip status reboot, a panic occurred.	prod00271318
52.	WBM did not display the virtual service configuration after synchronization.	prod00270171
53.	After enabling compression, file download failed.	prod00272082
54.	Using the command /info/slb/sess/dump, the configuration sync fails while dumping huge SLB sessions onto the console.	prod00271269
55.	Using WBM, when adding interfaces to a VM, Flow Continuation Ingress ports could not be validated.	prod00265360
56.	In a filter configuration, the default value of "matchdev" differed between WBM and CLI.	prod00270627
57.	Was unable to install a legacy compression license on top of NG/NG+.	prod00271478
58.	After disabling the Layer 3 filter, the health check started failing.	prod00269199
59.	In a hot-standby VRRP environment, when port 1 was disabled on the backup, Alteon attempted to disable the port as part of the hot standby algorithm irrespective of the current status of port. The functions called during the flow used ND APIs and they resulted in high MP CPU. As part of the fix, disabling the port again is prevented if the port is already in the disabled state.	prod00271916

Item	Description	Bug ID
60.	In an ADC-VX environment, the WBM, SSH, and console were not available until device was rebooted.	prod00271285
61.	Out-of-order TCPv6 segments from the client to the MP caused a panic.	prod00270532
62.	Services went down on the master ACOD device. In the syslog there was no indication of failed real servers and there was a significant inconsistency between the syslogs/console logs and tsdump info.	prod00270096
63.	Using WBM, the dashboard displayed the wrong throughput for a virtual server, even though here was no traffic for the virtual server.	prod00270112
64.	When configuring a health check ID and real server ID together with a length greater than 35, due to a bug in the health check script a panic occurred.	prod00271593
65.	In a BGP environment, when network class changes were applied, the device panicked.	prod00270719
66.	The "new cached bytes" field in the statistics for the acceleration engine cache mechanism, displayed the wrong value.	prod00271429
67.	An additional "\" character was inserted in the body of the HTTP Advanced health check	DE47480
68.	With Reverse enabled in a filter and vmasport enabled, the return traffic did not undergo server processing/NATing, causing the server packets to display on the client network.	prod00272714

Fixed in 32.2.1.0

Item	Description	Bug ID
1.	In an SLB environment with primary and standby devices, after syncing the configuration from primary to standby, the virtual service configuration did not display in the WBM of the standby device.	prod00270171
2.	In SLB monitoring using the APIs, the status of a real server that is part of a content rule and its health check failure reason could not be fetched using the API SlbStatEnhContRuleActionGroupEntry.	prod00270081

Item	Description	Bug ID
3.	In an SLB environment, although only 29 real servers were configured, when trying to configure a real server (with duplicate), the following error message was issued: `The maximum of 1023 Real Servers has been reached. To add new real server, first delete any unused Real Servers and apply.`	prod00269765
4.	In a virtualization environment, during configuration synchronization, the MP CPU of the vADC stayed at more than 80% for a long time.	prod00269753
5.	In an SLB environment with cookie persistent mode and forceproxy, the svclstconns metric always selected the same server as a collection of active connections, causing unequal load distribution for the service	prod00269642
6.	In an SLB environment with force proxy enabled, when the server group names exceeded 50 characters and first 50 characters were the same, after upgrading, Alteon stopped processing the traffic.	prod00269640
7.	When RADIUS authentication was enabled and a user logged in using SSH (probably using scripts), a vADC panic occurred due to NULL memory access.	prod00269220
8.	In an AppWall integrated with Alteon environment, when submitting a SECWA configuration, AppWall issued the following error: `You are not authorized to edit this Web Application.`	prod00269188
9.	In an AppWall integrated with Alteon environment, you could enable SSL for the authsrv (/c/security/websec/authsrv/ldap 1/ssl ena) even though SSL will not be used. As a fix, this command has been removed the from CLI.	prod00269183
10.	Irrespective of the LACP port configurations, Alteon with STP off did not pass transparently BPDU from Cisco Nexus with MSTP.	prod00269094
11.	In an SSH environment, downloading an image using SCP was slow compared to downloading through FTP.	prod00269084
12.	In an SLB environment with DNS Responder VIPs, with mixed delegation/non-delegation traffic, a panic occurred.	prod00269062
13.	In an SLB environment with forceproxy, after configuration sync (with associated real server removed) from the master to the backup device, the device rebooted.	prod00269015

Item	Description	Bug ID
14.	Using CLI, an incorrect description was displayed for the command /c/l3/ha/service/dis	prod00268974
15.	In a monitoring environment, a panic occurred when continuously polling for a set of OIDs (slbStatLinkpfIpTable, pip6CurCfgTable, pip6NewCfgTable, pip6CurCfgPortTable, pip6NewCfgPortTable, pip6CurCfgVlanTable, pip6NewCfgVlanTable) with GET REQUESTs.	prod00268928
16.	When a data port was used for NTP, and the packets were received from non-configured NTP servers, the syslog message NTP illegal packet length for the dropped NTP packets was issued.	prod00268904
17.	In a VRRP environment, changes to a VR's priority during migration failover ended with an apply lock and high MP memory usage.	prod00268858
18.	In an SLB environment, when the HTTP2 policy was enabled with a group of one real server and one backup real server configured, when the active real server went down, traffic was not shifted to the real server configured as the backup, and the client received a 503 error.	prod00268741
19.	Using CLI, In an SLB monitoring environment, in the virtual server statistics the displayed highest sessions were greater than the total sessions.	prod00268723
20.	An HTTP head host modification rule could be changed or modified using CLI but not using WBM	prod00268688
21.	Using WBM, when configuring an SSL service, the certificate and the group were set and configured even when the user chose the 'any' option. This caused the newly configured APP to function slowly.	prod00268685
22.	In an SLB environment, when a FQDN real server was changed, Alteon was not updated for more than a half an hour after the change, and it changed only after the FQDN real server was disabled and then enabled.	prod00268654
23.	In an HA environment with the same network class associated to a SmartNAT and also a real server, the ARP for a few of the PIPs in the network class range were not answered.	prod00268645

Item	Description	Bug ID
24.	In an HA with SLB environment, even though the PIP Network Class Range was enabled to receive GARP `(/c/l3/ha/nwclgarp ena)`, the GARP was not sent for all IP addresses from the proxy network class range.	prod00268505
25.	The SNMP CLI configuration commands /c/sys/ssnmp/rcomm and `/c/sys/ssnmp/wcomm` in accepted a NULL string, resulting in errors when adding or removing real servers from a group using WBM.	prod00268503
26.	In an environment with health checks, when the SNMP health check was configured, the weight displayed but it did not display when the SNMP heath check was part of a LOGEXP.	prod00268455
27.	In an SLB environment, when a content rule group contained a remote real server with the DSSP health check, an inconsistent DSSP health check status displayed. **Note**: A **Config Apply** action is now not allowed if the content rule group contains a remote real server with a DSSP health check and the DSSP health check is not part of the default service group.	prod00268431
28.	In a virtualization environment on a vADC, the SP memory displayed as HIGH all of the time, while the device had no traffic and no SLB configuration.	prod00268394
29.	In an SLB environment, a filter configured with the protocol as "50" was not restored after rebooting the device.	prod00268390
30.	In an SLB environment, when the real service port (the rport of a virtual service) was configured with a value less than 5 (except for multiple rports/IP addresses service scenarios), the traffic on these rports failed. For the fix, a validation has been added to allow rport 0-multirport or 1-ipservice or 5-65534.	prod00268324
31.	In an SLB environment with filter sessions, when the primary became available, even though backup clear (clrbkp) was enabled, the sessions that were bound to the backup server were not cleared on the filter.	prod00268272
32.	When the FastView license expired, Alteon also lost the compression license.	prod00268238

Item	Description	Bug ID
33.	When the number of basic health check components used in the logical expression-based health check object was changed, such that the new expression had fewer objects than the old expression, a software panic occurred.	prod00268236
34.	When a client connected to Alteon using SSH with RADIUS authentication, a panic occurred.	prod00268120
35.	Using WBM, HA Real Server Tracking could not be configured.	prod00268053
36.	In an HA environment with an SLB configuration, configuration of the backup real server and/or backup group was not synced to the peer device.	prod00268048
37.	In a virtualization environment, when a vADC was deleted and when a new vADC was created with same vADC number, the old configuration was restored in the newly created vADC.	prod00268003
38.	When Alteon sent a zero byte just before the EOM terminating sequence of 0x0d0a2e0d0a (observed in the capture file) and the server did not answer with anything, Alteon did not receive a 250 response from the server after sending the e-mail content (syslog messages).	prod00268002
39.	When OCSP used DNS over management, after 64K DNS requests, failures occurred, causing Alteon to close the connection during SSL handshake.	prod00267963
40.	In an SLB environment with forceproxy and an ICAP and SSL Inspection configuration, if the ICAP server terminated or did not respond, a panic occurred.	prod00267959
41.	In an Alteon Integrated with WAF environment, the Parameter name within the parameters filter did not match the REGEX.	prod00267953
42.	In an SLB filters environment, the IPv6 redirect filter used a proxy port to forward packets to the server, but the IPv4 redirect filter did not.	prod00267951
43.	In an SLB environment, when operationally disabling or enabling a real server in a server group, a syslog message indicating the action was not generated.	prod00267949
44.	In an SLB environment with forceproxy configured and with the HTTP2 Gateway implemented caused high SP memory usage.	prod00267931
45.	Using WBM, in the Monitoring > System > Maintenance pane, when the resolution changed, the Export button for techdata was located in the wrong position.	prod00267870

Item	Description	Bug ID
46.	In an OSPF environment, Alteon was unable to update the peer with any change to the OSPF parameter.	prod00267852
47.	Using WBM, even though a user logged in with the "admin" user, the user could not operationally disable a real server.	prod00267832
48.	In an SSL environment with a certificate repository, after manually importing all of the keys (clear text RSA keys) and certificates to both the master and backup devices, when trying to associate the certificates to their corresponding VIPs, configuration sync failed, an error that a key was missing on the backup device displayed on the master device.	prod00267781
49.	When Alteon was managed with a "notacacs" and "noradius" login, the following issues occurred: • When backdoor users logged in, permissions to change the admin password were based on the previous user login • The who command displayed nothing or displayed the previous user's login name • When logging in with the "noradius" user with the admin password, the user could not change the admin password	prod00267749
50.	In an HA environment, when a proxy was configured for a filter was same as a floating IP address, the filter's proxy entries were added to the ARP table of the backup with the device MAC address without checking the HA state, causing the backup to reply to ARP queries.	prod00267746
51.	In an HA environment, the filter proxy was added to the ARP table with the device MAC address instead of the HA MAC address, causing Alteon to not forward dynamic NATed DNS responses to the internal DNS server.	prod00267723
52.	In an SSH environment, when the export/import of configuration operations were performed using gtcfg or ptcfg, SSH sessions became permanently stuck.	prod00267716
53.	Using APSolute Vision, when accessing the *High Availability* tab, the following configuration error was issued: `404 Not Found: REST API lookup failed`	prod00267695
54.	In an HA environment, even though the configurations were the same on both the active and standby devices, a warning message related to an HA configuration mismatch was issued.	prod00267681

Item	Description	Bug ID
55.	In a BGP environment, when deny route redistribution was disabled for a BGP peer, although the BGP peer went down and came back up, Alteon stopped sending advertisements.	prod00267678
56.	In a virtualization environment, a vADC was accessible over HTTPS, even though HTTPS access was disabled in the configuration.	prod00267642
57.	Even though access on a device's management port was restricted using an access-list (/cfg/sys/access/mgmt/add), it did not work properly.	prod00267587
58.	When services were moved from the master node to the backup node, no SNMP traps were sent to the Monitoring server. **Note**: These traps were omitted when implementing the new feature "Extended HA". Traps, syslog messages, and log messages have been updated, extended, or replaced with new messages.	prod00267571
59.	Using WBM, in an SLB environment, when configuring a virtual service in the Content Rule pane, an invalid URI was accepted for the redirect URI configuration, while the CLI displayed an error message for that invalid URI.	prod00267552
60.	Using WBM, while monitoring the servers and being logged in as a real server operator, when trying to disable the server operational status through Application Delivery > Server Resources > Real Servers, the status of that real server did not change.	prod00267516
61.	Using WBM, when trying to set the group real server status to connection shutdown, its status kept displaying as enabled.	prod00267515
62.	When Alteon received an IPv6 address with a full length address (more than 32 characters including colons – for example, 2101:2101:2100:2100:2101:2100:2100:2101) and processed the IPv6 fragmented packet, a panic occurred.	prod00267493
63.	In an SLB environment with the group metric **svcleastconns** and a multi-rport scenario, load distribution to the real server was not proper.	prod00267433
64.	Using WBM in an SLB environment, the virtual server copy did not work properly, and the copied virtual server had different settings for cookie and server group.	prod00267161
65.	When performing an Apply of a configuration imported using REST API, an error was issued.	prod00267152

Item	Description	Bug ID
66.	In an SSL environment, certificates that were set to expire after 100 years displayed as expired.	prod00267056
67.	Pings to PIP/VPR were blocked.	prod00266689
68.	Using WBM, users with user roles Operator, L4 Operator, SLB Operator, and SLB Viewer could execute **Apply** and **Save** commands for a configuration created by the Administrator.	prod00266672
69.	Using WBM, you could modify the privacy and authentication settings for SNMP default users.	prod00265974
70.	Using WBM to create route maps, the following parameters had incorrect values for the route map object: Local preference, Metric, Weight	prod00264251

Fixed in 32.2.0.0

Item	Description	Bug ID
1.	Using WBM, in the Service Status View pane, the real servers incorrectly displayed.	prod00267276
2.	Using WBM, in the Service Status View pane, the filter option in the displayed data did not work as expected.	prod00267217
3.	After upgrading to Alteon version 32.1.x, you needed to log in two times to get access to Alteon VA, ADC-VX, or vADC.	prod00267210
4.	Using WBM, the complete IPv6 Management IP address did not display.	prod00267208
5.	In an SLB environment, when real servers were moved from one server group to the other, although the real servers were moved away from a group, the old sessions still remained and did not age out.	prod00267134
6.	In an SLB environment, after the primary real server went down and the backup real server and group took over, the service became inaccessible.	prod00267089
7.	Using CLI, on a vADC with a QAT SSL card, in the output from the stats/sp x/mem command, the tech support dump (tsdump) did not contain the QAT driver memory usage.	prod00267071
8.	Alteon did not handle a specific condition related to FQDN and went into an inconsistent state.	prod00267062
9.	In a Global SLB environment, when the network gmetric used a network class as the source IP address, the DNS response was incorrect.	prod00267044

Item	Description	Bug ID
10.	In an inbound link load balancing Smart NAT environment, the Availability metric in the SmartNAT GSLB rule was not processed, causing an improper ISP links order.	prod00267020
11.	Using WBM, from the *Certificate Repository* pane, you could not perform a search in the table.	prod00266986
12.	In a configuration sync environment, after a routine configuration change, the MP CPU reached 100%.	prod00266964
13.	In an SLB environment, when overlapping IP addresses were defined in a network class configuration with exclude enabled, and when an exclude range was a subset of the other exclude range, the filter defined with this network class fired incorrectly for an excluded IP address, causing the filter to misfire.	prod00266924
14.	In a Global SLB environment, when the network element was of type subnet, the fromIp was incremented by 1 to skip the network address and the toIp was decremented by 1 to skip the broadcast address, causing a large value for the IP count, and Alteon prevented the subsequent network elements and network classes from being added to the internal tables. This caused a GSLB SIP lookup failure for missing network ranges.	prod00266917
15.	In an SLB environment, filter processing processed the traffic addressed to the SmartNAT dynamic address/PIP addresses, failing the DNS amplification scan.	prod00266909
16.	When the NTP server was configured over IPv6, the IPv6 address was not recognized on routing through the management port IPv6 address.	prod00266888
17.	Using WBM, when deleting a Layer 3 gateway, the gateway entry did not disappear, but a stale entry for the same gateway ID was displayed in the disabled state and with an IP address 0.0.0.0 and VLAN 0.	prod00266880
18.	In an HA environment, when duplicate IP addresses were configured for DNS responder virtual servers and regular virtual server IP addresses on the master device, configuration sync to the peer device did not work, ending with errors.	prod00266879
19.	In a management environment, when different management certificates on the master and backup were configured (/c/sys/access/https/cert), configuration sync failed without a meaningful error message.	prod00266876

Item	Description	Bug ID
20.	In an SLB environment with dynamic address mode with an AppShape++ script (source NAT), Alteon forwarded the traffic to the server with the source MAC address set to the client MAC address instead of the Alteon/HA MAC address.	prod00266869
21.	Using WBM, in the Certificate Repository Import screen, the correct certificate file was not imported when trying to use the Browse button	prod00266868
22.	In a Link Load Balancing (LLB) environment, after restoring the backup configuration using `get config`, the LLB-related configuration `(/c/slb/gslb/network x/wangrp WAN-Group-1)` was lost.	prod00266817
23.	Using WBM, configured AppShape++ script did not display.	prod00266779
24.	When the NTP was set over a data port and the NTP server was down, an incorrect SNMP Trap (Critical Temperature Trap) was sent when the NTP request timed out.	prod00266743
25.	In an Azure environment, when the RADIUS server was on a different network other than the management network, RADIUS authentication did not work.	prod00266675
26.	On a Cavium-FIPS platform, the PKCS12 file of the CA-group was encrypted and larger than 16K in some cases and failed to load.	prod00266654
27.	In an SLB environment, after configuring the real server weight using the CLI command `/c/slb/real x/weight`, a panic occurred.	prod00266636
28.	In an SLB environment with an acceleration environment, due to connections being reset, some application outages and traffic failures were observed.	prod00266633
29.	In an SLB environment, on a real server, due to packet drops in the SPs, TCP latency occurred for health check packets.	prod00266603
30.	In in Outbound Link Load Balancing environment, the transparent health check to a destination server was sent from an inappropriate port/VLAN (WAN Link).	prod00266602
31.	While using a REST API call to export the configuration, Alteon ignored the path and name specified in the API request. Alteon generated a name and transferred the file to the root folder of the SCP server instead.	prod00266593

Item	Description	Bug ID
32.	When importing a key which is not encrypted (plain text), due to minimal passphrase that was set, the import caused all onboarding of HTTPS applications that use non-encrypted certificates to fail.	prod00266573
33.	In a monitoring environment, invalid TRAP OIDs were sent for the SP CPU Pressure On/Off. **Note**: The correct MIB OID has been added to the trap.c and GENERIC-TRAP-MIB.MIBs: altSwSpCpuPressureActivatedTrap - 1.3.6.1.4.1.1872.2.5.7.0.214 altSwSpCpuPressureDeactivatedTrap - 1.3.6.1.4.1.1872.2.5.7.0.215	prod00266559
34.	In a VRRP environment with an SLB configuration, the session move operation did not get synchronized to the backup, leading to session mirroring not working, causing statistics discrepancies on the backup devices.	prod00266543
35.	In an SSL environment, when changing the cipher suite from TLS 1.2 to the User Defined " TLS_ECDHE-RSA-AES128-GCM-SHA256" cipher, the AX configuration was corrupted and the service to which the SSL policy was attached stopped working.	prod00266530
36.	In an environment with AX configured, the primary and secondary vADCs panicked one after the other.	prod00266525
37.	In a Layer 7 environment, if the original request did not contain any query, Alteon did not remove the query separator "?" in the redirect URI.	prod00266453
38.	Using WBM, in the *Outbound LLB Rule* pane, the IP address/network could not be edited.	prod00266452
39.	In a virtualization environment, due to vADC management mask settings not considered for locking, when attempting to get access by the management interface to a vADC, access was given to another vADC.	prod00266409
40.	In a VRRP environment, when health checks failed on the backup, statistics discrepancies (incorrect number of sessions to the real servers) occurred on the backup device.	prod00266339
41.	In an SLB environment, when there was a change in the virtual server configuration (disable/enable), the session move operation via CLI did not move the session to a different real server.	prod00266338

Item	Description	Bug ID
42.	When the time zone was set to Asia/Jerusalem (GMT offset +02:00), as the daylight saving setting was not taken into account, Alteon displayed the incorrect time from the month of October.	prod00266305
43.	In an SLB environment with HA, after the failover, uneven load distribution occurred on the new master device.	prod00266157
44.	Using WBM, In the certificate repository, when importing an intermediate CA, the size displayed as 0. **Note:** After the fix, the size is not calculated and is displayed blank.	prod00266154
45.	In a Cloud environment, when there was a VSAN failure, and when switching to redundant storage from the VMware side caused an I/O failure for a few seconds, the MP was stuck, causing the watcher to trigger the soft reboot and an outage of all Alteon VAs.	prod00266092
46.	In an SLB environment, when real servers were allocated to multiple virtual services and a **Revert Apply** was performed, the session table was deleted automatically.	prod00266012
47.	Using WBM, with the "User" role, configuration sync could be performed even though the "User" account should not be able to do this.	prod00266008
48.	Using WBM, on an ADC-VX, when attempting to log out of WBM, the device kept the user logged in.	prod00266006
49.	While running a vDirect script on Alteon devices, it took more than 20 minutes to display the output or the script timed out with no result.	prod00265982
50.	In an SSL environment, the user was unable to change the ciphers string under the advanced HTTPS health check.	prod00265975
51.	Using WBM, in the **Configuration > Setup > High Availability** pane, there was no option to delete VR Group settings.	prod00265973
52.	Using WBM, in an SLB environment when configuring a virtual service, the cookie configuration changed after making a change to the virtual server even if the user did not modify the persistent binding (pbind) cookie settings.	prod00265867
53.	Using WBM, when duplicating a real server, sometimes the "ERR json parse failed" message was returned.	prod00265865
54.	Using WBM, from the health check pane **Configuration > Application Delivery > Health Check > add**, the **Always Perform Health Check** field displayed twice.	prod00265861

Item	Description	Bug ID
55.	Using WBM, you could not set the action as Discard for a virtual server.	prod00265857
56.	When performing SNMP monitoring on SSL offloading stats (FE/BE), due to a memory corruption, a panic occurred, and the device rebooted a few times.	prod00265843
57.	In an Alteon integrated AppWall environment, SSL sessions were not created for specific tunnels.	prod00265812
58.	In a virtualization environment for a vADC, after performing a Revert Apply on an ADC-VX, the admin password changed back to the default password (admin) on the vADC.	prod00265710
59.	When **agTftpCfgFileName** was more than 83 characters, exporting the configuration with SCP through the REST API server failed.	prod00265672
60.	If the data-class entry contained a backslash (\) character and configuration sync was performed, the configuration was not synced correctly.	prod00265617
61.	In an SLB environment, when the client connected directly but through different VLANs for forward and backward traffic, the SP CPU utilization became high even though the amount of traffic was not increased, causing a degradation.	prod00265558
62.	In a Global SLB environment, when a configuration **Apply** was performed during the periodic statistics calculation, when the internal data structures used in GSLB were reset and repopulated, an illegal access occurred, causing a panic.	prod00265544
63.	When a new virtual server with a service-based proxy address and a corresponding VPR were both configured within the same **Apply** operation, Alteon did not display the VPR status in the VRRP and the ARP cache.	prod00265538
64.	In an SLB environment, if the configuration had a disabled virtual server and one of the services of the virtual server had a non-existent AppShape++ script, the configuration could not be saved.	prod00265537
65.	In a virtualization environment, one of the vADCs hung and panicked.	prod00265451
66.	In a virtualization environment, when the LACP was configured with 40G ports, during the vADC boot-up frequent gateway health check failures occurred.	prod00265434

Item	Description	Bug ID
67.	Using WBM, when using the SSL Inspection Wizard, when performing a revert, in certain conditions a REST API 405 error displayed even though the Revert was successful.	prod00265381
68.	In a virtualization environment, when the vADC IP address/net mask combination was configured incorrectly and failed to add the relevant gateway, disabling and then enabling vADCs caused Linux ifconfig errors, resulting in management connectivity loss for the ADC-VX. **Note:** This issue was addressed by not allowing invalid gateway settings and ensuring that the ADC-VX and vADC management IP addresses are defined on the same network.	prod00265371
69.	In an HA environment, during configuration sync, the real server configuration under HA triggers were not synced to the peer correctly.	prod00265322
70.	In a virtualization environment with HA configured, during upgrade, one of the vADCs hung and panicked.	prod00265317
71.	In an SLB forceproxy environment with IP service and filters configured, when performing an **Apply**, Alteon attempted to add a service mapping entry (needed for IP address and Port translation) for a filter, but instead accessed data meant for the virtual service, causing a panic.	prod00265289
72.	In a BGP environment, you could not import the default gateway alone or any other "range of IP"/"IP" separately.	prod00265280
73.	On the 6024 platform with 32 GB RAM, the vADC-5 license could not be installed on top of Alteon NG/NG+.	prod00265279
74.	In an SSL environment, when configured with client-IP, SSL-ID persistency and with SSL-ID traffic, a panic occurred.	prod00265243
75.	When dumping the FDB entries in the SP using the `/maint/debug/spfdb` command, only 8K entries were dumped when the Max size of the FDB per SP was actually 16K.	prod00265212
76.	In an SNMP monitoring environment, when accessing the MIB OID 1.3.6.1.4.1.1872.2.5.4.3.14 corresponding to runtime instances of a health check, a panic occurred.	prod00265181
77.	Using WBM, when logging in as a TACACS user, the following error message displayed: `mgmt: The language defined at the TACACS server is not recognized. Using global language.`	prod00265166

Item	Description	Bug ID
78.	In an HA environment with session mirroring enabled after failover, the new master did not mirror sessions to the new backup.	prod00265127
79.	In an Alteon integrated with AppWall environment, when the Accept-Language header was missing, AppWall responded with a 302-response code.	prod00265072
80.	If the IDSChain was not working for subsequent fragments or did not forward fragment IP frames that matched the filter, the RADIUS Server communication broke.	prod00265053
81.	Using WBM, in the Layer 7 Load Balancing Content Class Configuration pane, if the content class string contained a backslash (escape characters), the REGEX text field value displayed incorrectly.	prod00265029
82.	In a monitoring environment, fetching the Layer 3 Interface statistics using REST API did not work.	prod00264975
83.	Using CLI, with verbose 1 set, when a health check that was associated to a server group or real server was deleted, a prompt for user input did not display.	prod00264970
84.	In an HA environment configured with SLB, the mirrored P-session on the backup vADC was bound with the wrong real server group, causing services to get hampered.	prod00264936
85.	When PIP was configured under a DNS-UDP stateless service, as it is not applicable it was ignored. **Note:** As a fix, a warning message has been added only in CLI.	prod00264906
86.	In an HA environment, the backslash ("\") character in the LDAP user name was not synced to the peer device, and WBM did not display them.	prod00264903
87.	Using WBM, when a real server was deleted from a GSLB network, as these entries could not be reused even after deletion, once all the maximum 128 entries were exhausted, the following error message displayed: `Real server precedence table is full`	prod00264835
88.	On 4408 and 5208 platforms, when upgrading from versions earlier than 30.2.8.0 to version 30.2.8.0 or later, and the ports were enabled for management access, this resulted in an inconsistent configuration after the upgrade.	prod00264787
89.	The image upload on the management port using SCP was slower than using FTP.	prod00264763

Item	Description	Bug ID
90.	In an AppWall integrated with Alteon environment, for a virtual server that had an AppWall tunnel, Alteon stopped processing traffic.	prod00264676
91.	In an SLB environment with health checks configured, with an HTTP health check there was no difference in the failure status regardless of the failure reason. If the checked file was removed (404 code), the file required authentication (401 code) or an internal server error (500 code), for all cases the following error displayed: `Reason: Server's response is not as expected`.	prod00264674
92.	In an Alteon HA environment, when configuration sync failed with a Global SLB/Link Load Balancing configuration, after the failure the new configuration moved automatically to the current configuration without performing an Apply operation.	prod00264673
93.	In a DNS environment, Alteon does not include the edns0 client subnet in the DNS response.	prod00264633
94.	In an SLB environment with AppShape++ scripts, when adding an AppShape++ script to a virtual server without creating the service on that virtual server and performing an **Apply**, an **Apply** error did not occur, and any further configuration change on the virtual server and performing **Apply**, the `Pending configuration` message always displayed.	prod00264597
95.	Alteon allowed management access via data ports on IPv6 even though the access was disabled.	prod00264531
96.	In an HA environment, after synchronizing the configuration from the master device, the health checks for a real server failed/toggled on the backup device.	prod00264498
97.	Due to a debug tool that was configured for OpenSSL, HTTPS health checks caused 100% CPU usage on the MP, introducing delays in HTTPS health checks.	prod00264468
98.	When configured a URI under a CDP group with the left parenthesis ("(:) character in the URI and with traffic, a panic occurred	prod00264433
99.	In an HA environment with SLB configured, after configuration sync, when Alteon attempted to configure the backup real server as a backup group, the backup real servers in the group were removed on the peer device.	prod00264432

Item	Description	Bug ID
100.	In an IPv6 environment, even though IPv6 local networks were configured, Alteon sent a server response to the default gateway instead of sending it directly to the connected client. As a result, a real server could not be reached from the subnet.	prod00264431
101.	In an SLB environment, incorrect statistics were displayed while fetching virtual service statistics (`via /stats/slb/virt`), the statistics for a real server (Current, Highest, Total sessions) displayed as 0, even though the real server handled the connections.	prod00264430
102.	On an Alteon VA platform, although the new VLANs were defined to contain default ports, after the reboot, the configuration was always pending in the diff operation.	prod00264390
103.	In a forceproxy SSL environment, internally when MP and AX went out of synchronization, Alteon continued to send an old certificate even after installing a new certificate.	prod00264339
104.	Using WBM, from the **Configuration > Application Delivery > LinkProof > Inbound LLB Rules** pane, there were several issues during configuration.	prod00264289
105.	Using WBM, with SLB monitoring, when a content rule was used with a real port, the session counter displayed incorrectly.	prod00264285
106.	Using WBM, in an Inbound Link load balancing environment, the NAT address configuration was missing in the Global SLB's client network rule page.	prod00264245
107.	Using WBM, when attempting to configure HTTP modification for header removal, Alteon forced the user to input the header value.	prod00264244
108.	Using WBM, in an SSL environment in the Export tab, even though the "certificate and key" option was selected to export, only one **Export** button displayed.	prod00264233
109.	In an HA environment with script health checks configured, after deleting/adding/modifying a script and performing configuration sync, there was a discrepancy in the health checks between the master and the backup device.	prod00264172
110.	In an SLB environment, when a real server with the same IP address was configured for different groups, and each of the groups were configured with the same logical expression health check, Alteon failed to evaluate the logical expression except the group in which the real server came up first. The rest of the real servers remained down in respective groups.	prod00264146

Item	Description	Bug ID
111.	In an environment with a configuration where the client packet comes into Alteon through one VLAN (ingress) and after server processing, the response packet leaves to the client in another VLAN (egress), duplicate IP FDB entries got created for external IP addresses.	prod00264048
112.	In an SSL environment with Cavium cards, after upgrading a couple of certificates and performing **Apply**, a panic occurred.	prod00264047
113.	In a virtualization environment when ADC-VX rebooted with a panic, the RADIUS secret became corrupt and the RADIUS login failed.	prod00264025
114.	Using CLI, when executing a non-existing or hidden command with the /maint/pktcap menu, an error was not issued. **Note:** As a fix, all the hidden commands under `/maint/pktcap` were removed and cannot be executed.	prod00264010
115.	In an SLB environment with filter processing enabled, VMAed traffic source MAC learning did not occur, causing traffic to be flooded on all the VLAN ports, causing higher throughput utilization.	prod00264009
116.	In an SLB environment with multiple rports, when a new real server was created with addports and if it was associated to more than one service, if any of the service health checks was toggled, Alteon forwarded client requests to the server on the service port rather than on the real server's service port (rport = addport of the real server).	prod00263992
117.	In an SLB environment, when a particular sequence of SLB configuration steps involving a HTTP virtual service and another virtual server along with **Apply**, the configuration became corrupted.	prod00263986
118.	In an SLB environment, when a group was configured with one or more real servers (by manual configuration), when deleting or removing real server(s) from the group, the following Apply error displayed: `Error: Real server group 100 associated to virtual server 100 service 80 is not defined`	prod00263985
119.	In a virtualization environment, when autosync was enabled on both ADC-VX and vADCs, configuration changes to the definition of the primary vADC from the ADC-VX triggered the sync to loop between the vADCs.	prod00263984

Item	Description	Bug ID
120.	For the BWM-history-related e-mail, when the SMTP 'To' user was not configured, but when Alteon tried a number of times to send this e-mail, after a while Alteon did not respond to SSH/HTTPs via management.	prod00263983
121.	Using WBM, when a configuration dump was performed on a FIPS device, the following error displayed: `Error: Configuration import/export via HTTP is already running.`	prod00263982
122.	In an SLB environment, you could not configure a virtual server with a different protocol and Alteon returned the following error: `Error: Virtual server v1 has the same SIP SLB group id as virtual server v1-udp.`	prod00263980
123.	In a virtualization environment with HA, when p-session sync updates were received from the master, the backup attempted to become the master. This was no longer an issue when the p-session sync was configurationally disabled.	prod00263979
124.	In an AppWall integrated with Alteon environment, when troubleshooting some false-positive "HTTP reply not RFC-compliant" events were issued that indicated that Request Data and Reply Data under Forensics were identical.	prod00263587
125.	There was a discrepancy between the peak compressions usage command output (/info/swkey) and syslog messages.	prod00261525
126.	In a SmartNAT environment, the concurrent sessions value of the WAN link server was much larger than the displayed session statistics.	prod00261497
127.	Due to a kernel issue, Alteon went into ULP mode and could not be accessed via Telnet, SSH, HTTP, or HTTPS while the Management IP address was reachable only over ICMP.	prod00260720

AppWall

Item	Description	Bug ID
1.	Fixed a rare failure in the HTTP parsing process.	DE43435
2.	Fixed a rare failure in HTTP Response parsing process.	DE43438
3.	The client IP address was not sent in the security page.	DE42288
4.	For some types of security violations, the case number shown in the security page was 0.	DE41895

Item	Description	Bug ID
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
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

Item	Description	Bug ID
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
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

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

Item	Description	Bug ID
19.	Using CLI in an SLB Monitoring environment, the octet count displayed by the virtual server statistics command `/stats/slb/virt x` was incorrect.	prod00262825
20.	Alteon failed to import encrypted private keys that had a long password (> 40 characters).	prod00262772
21.	In an SLB SIP environment with AppShape++ scripts, a SIP parser issue occurred.	prod00262760
22.	On an Alteon 5208 S platform, depressing the PWR button for a few seconds did not perform a graceful shutdown of the platform.	prod00262716
23.	In an SLB monitoring environment with names configured for real servers, when displaying the real server group statistics with the CLI command `/stats/slb/group`, the real server name was listed instead of the IP address. The fix was to change the heading to "IP Address/Name". The real server name displays if it is configured. Otherwise, the IP address displays. This also applies to the commands `/stats/slb/virt` and `/stats/slb/sp x/virt`.	prod00262715
24.	Using WBM in an SLB environment, you could not configure POP3 over SSL (TCP port 995).	prod00262692
25.	After disabling the default user, the command `/cfg/sys/access/user` did not display the correct value.	prod00262676
26.	In an SLB environment with filters, even though rtsrcmac (Return to Source MAC) was enabled for a filter, ICMP reply packets corresponding to the filter session were routed to the VLAN gateway instead of the client port.	prod00262649
27.	Using WBM in an SLB environment, when a virtual router and Proxy IP address under a virtual server were the same, the following error displayed: `The IP Address of Virtual Router 2 conflicts with the Client NAT (PIP) IP address`	prod00262620
28.	During a Nessus security scan on Alteon, due to opening and closing SSH connections frequently, a panic occurred.	prod00262619
29.	Using WBM in an SSL environment, you could not generate a CSR.	prod00262589
30.	Using the CLI, the command `/info/l3/ha` output information was misleading (it displayed VRRP information).	prod00262578

Item	Description	Bug ID
31.	In an SLB environment with an IP service configured with the svcleast metric, traffic was distributed to the same server, leading to uneven load balancing of the traffic.	prod00262568
32.	In an SLB environment with content classes configured, when selecting a different group's real server per the content class, rather than a group-real server being configured on the virtual service, the front-end session abruptly aged out/terminated, causing service issues.	prod00262567
33.	When logged in with a backdoor-enabled user and with RADIUS enabled, after running the `/oper/passwd` command to change the user's password, the displayed username was incorrect, the syslog message was generated was with incorrect username, and the **Who** command displayed the incorrect username.	prod00262566
34.	In an environment with a slower client (LG K220) and a faster server, after enabling HTTP2, high SP CPU usage occurred.	prod00262565
35.	Using WBM, in a DNS Proxy configuration, you could not roll back the default group configuration to 'none'.	prod00262545
36.	After using the CLI command `/info/transceiver`, Alteon either rebooted unexpectedly or Alteon's traffic was stuck for about 13-15 seconds.	prod00262540
37.	Due to an ND issue, a panic occurred and caused a reboot.	prod00262521
38.	Due to an unauthorized Rx queue disable mode of I210 MACs, Alteon dropped some packets.	prod00262519
39.	Using WBM in an SLB SSL environment, attempting to create a new authentication policy also added the passinfo default configuration, causing the Apply to fail.	prod00262518
40.	Using WBM, when generating a server certificate with SHA256, the certificate was instead generated with SHA1.	prod00262456
41.	On platforms that do not have QAT, due to irrelevant memory consumption and that memory being set to debug, when new management certificates were configured or created and a configuration sync was performed, a panic occurred.	prod00262436
42.	Using WBM, in the **Monitoring > Application Delivery > Global Traffic Redirection > Remote Real Virtual Servers** pane, the titles of the table were not displayed in human readable format.	prod00262436
43.	Export of applogs using SCP server with the hostname as the destination failed, but with an IP address as the destination worked.	prod00262426

Item	Description	Bug ID
44.	Using APSolute Vision, the **Generate** and **Export** buttons on the **Monitoring > System > Maintenance** pane were misplaced.	prod00262402
45.	When the gateway was unreachable, and even though Alteon had no interface that was alive interface, Alteon delayed in recognizing a gateway health check failure.	prod00262350
46.	In an SLB environment, when a Script health check was part of a LOGEXP, a different number of health checks packets were sent out per interval for the different health checks combined in the LOGEXP health check.	prod00262279
47.	In an SLB environment, even though the servers were up, Alteon responded with a 503 error	prod00262264
48.	In an SSL environment with certificates, import of certificates in PFX format failed when the passphrase contained special characters such as '@'.	prod00262239
49.	In an SSL environment with certificates, import of certificates in PFX format failed when the passphrase contained special characters such as '@'.	prod00262238
50.	In an SLB environment with HTTP2 enabled on virtual services, sometimes Alteon stopped responding with resource issues.	prod00262190
51.	In a LinkProof environment, Alteon responded to customer requests without changing the server IP address to the Virtual Server IP address and server packets being handled by filter processing, causing the access to fail.	prod00262164
52.	In a gateway-per-VLAN environment, all the traffic to the Alteon interface and virtual server was sent back to the gateway based on the default gateway and not per the VLAN gateway, causing the feature to not work.	prod00262161
53.	Alteon modified the source IP address of hops on the traceroute path of UDP and TCP responses, causing the client to receive an incorrect result.	prod00262158
54.	When logging in to WBM through a data port, the WBM user login information was missing, and the incorrect client IP address was logged in the syslog message.	prod00262143
55.	In specific browsers (some versions of Chrome and Opera), which send some non-optimized HTTP2 HPACK header encodings that Alteon does not handle correctly, the PUT method did not work.	prod00262074

Item	Description	Bug ID
56.	After using the CLI command `/c/sys/syslog/cur`, the message `Syslog thread safe mode` displayed when it should not have.	prod00262045
57.	In an SLB environment, the PIP path under the virtual server (`/cfg/slb/virt <vsid>/service <vport> https/pip`) displayed in diff flash even though the settings were set to the default.	prod00262042
58.	When a primary group was configured without real servers associated with an FQDN server, the backup group used FQDN real servers, causing an **Apply** failure.	prod00262017
59.	Using WBM, in an SLB environment, you could not configure a Buddy Server.	prod00262010
60.	When the DNS server was down, Alteon stopped sending health checks with the destination as the hostname.	prod00261970
61.	Using WBM, when creating a Smart NAT dynamic NAT entry, the **Local Address** drop-down list included a **None** option which should have been named **Any**.	prod00261955
62.	Using WBM, when creating a new VRRP virtual router, the check box that is used to enable the virtual router was named **Enable Virtual Routers** instead of **Enable Virtual Router**.	prod00261953
63.	In an SLB environment with rtsrcmac enabled and reverse disabled, a request to a virtual server included an Allow filter, causing SLB traffic to fail.	prod00261909
64.	In a virtualization environment, when the ADC-VX was version 30.2.*x* and the vADC was version 31.0.*x*, there was a compatibility issue without proper information on an LACP trunk, causing port issues.	prod00261865
65.	In previous versions, client IP persistency could not be maintained when the SP CPU was selected based on the client IP address and port (VMAsport enabled).	prod00261812
66.	In an SLB environment, changes to the network class associated to an in-route map required a BGP soft reset for the changes to take effect.	prod00261805
67.	When the audit log was enabled, Alteon sent a blank syslog for the delete operation.	prod00261801
68.	When monitoring Alteon using SNMP, when an SNMP GET was performed for a virtual server with nonat enabled (DSR), the current sessions displayed as NULL.	prod00261791

Item	Description	Bug ID
69.	In a Global SLB environment with the redirect exclusion feature enabled, Alteon selected a service for the DNS response with the action as "redirect" instead of resolving the DNS.	prod00261790
70.	In an SLB environment using CLI, when the xforward command was run for a service, the delayed binding forceproxy setting was not set.	prod00261789
71.	In the Monitoring environment with `/cfg/sys/report` set to on, a panic occurred with SIGSEGV(11) in thread RSTA(tid=81).	prod00261691
72.	When importing the configuration using REST API, Alteon always responded with a success message to the agTftpLastActionStatus query even though the import operation failed.	prod00261680
73.	In a Smart NAT environment, due to a sequence of validations in Global SLB, the warning messages for gmetric were confusing to the user.	prod00261630

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

75.	In a LinkProof NG environment, when the source address was configured for proxy or SmartNAT 'Any' dynamic NAT, the Return to the source MAC address did not work for filter traffic and the return traffic did not behave as expected.	prod00261528
76.	In a LinkProof NG environment, the inbound proximity (gmetric proximity) did not work with Smart NAT.	prod00261523
77.	In a Smart NAT environment, Alteon forwarded the ICMP reply to the client without changing the source IP address to the public IP address. As a result, the VPN gateways could not be pinged using the public IP address.	prod00261521

Item	Description	Bug ID
78.	In an SLB environment with forceproxy, when HTTP content had to be replaced to HTTPS content, Alteon could not match the content-types application/json or application/xml, so Alteon could not replace this part of the HTTP code. As a result, the whole page appeared with issues.	prod00261493
79.	In an SLB environment with forceproxy, the content-based rules with FQDN servers were not working and returned 503 error.	prod00261490
80.	With a data class configured, when attempting to modify the same data class without performing an Apply, there was a discrepancy between the Alteon white list and the vDirect getextendedinfo configuration file. The diff displayed the modifications, but the Apply failed.	prod00261406
81.	On the Cloud WAF portal, with white lists for IP addresses having zero as the last octet, an Apply operation failure occurred.	prod00261121
82.	In the Advanced HTTP health check configuration, although the maximum number of characters for the Body parameter was stated as 1024 characters, only 512 characters were allowed.	prod00261017
83.	Using WBM, when a user logged in using TACACS and performed configuration changes, and later performed Apply/Save operations, the audit logs recorded another user ID and not the user who had logged in.	prod00260978
84.	In a virtualization environment, when the ADC-VX was version 30.5.*x* and the vADC was version 31.0.*x*, no applogs were generated.	prod00260946
85.	Using WBM, using $PROTOCOL instead of http:// or https:// in the redirection URL for content rules action redirect or action redirect for a service did not work.	prod00260876
86.	In a DNS environment where DNS responses were received, and with VRRP or HA, performing a configuration sync ended with an FQDN error.	prod00260836
87.	In the SNMP Trap for certificate expiration altSwcertRevokedID, the description was incorrect.	prod00260830
88.	In a VRRP environment, after sync was performed, the server group setting was removed from the peer device.	prod00260808

Item	Description	Bug ID
89.	In an SLB environment with the round robin or least connections metric, and with a traffic pattern that had few connections that were opened with relatively long time periods between each other, after migrating all virtual servers from the 5208 platform to the 6420 platform, the round robin metric kept selecting only one specific real server from the server group and did not balance traffic to some servers.	prod00260669
90.	In WBM, the SLB Viewer user role was allowed to enable/disable physical ports, when this user role should only be able to view Alteon information, SLB statistics, and information, but should not be able to make any configuration changes.	prod00260641
91.	Using WBM, a real server's Description accepted 128 characters while only 31 characters are supported, causing the real server Description not to be synced from Active to Standby.	prod00260639
92.	In a virtualization environment, when accessing the device on an ADC-VX using REST API with an incorrect customized Authorization header value, a panic occurred.	prod00260598
93.	Alerts regarding DUAL PSU failure were generated, but after 6 seconds a notice was issued that the Status was Ok. This issue persisted even after changing to a new PSU.	prod00260597
94.	On a 6024 XL platform with 32 GB RAM, in Maximum vADC Density mode, you could not allocate the 12th CPU core (the fourth core for MP processing).	prod00260580
95.	Using REST API, image upload did not work.	prod00260564
96.	In an SLB environment, when a proxy IP address was defined in a network class, the proxy MAC address was sent with the gateway MAC address to those proxy IP addresses that were not present in the ARP table, causing the applications to fail.	prod00260562
97.	The load time of REST API calls was much slower than the load time in earlier Alteon versions.	prod00260509
98.	In an SLB environment with SSL Hello or HTTPS health checks configured, after upgrading to version 30.2.9.0, real servers configured with these health checks failed.	prod00260485
99.	In an SLB environment with the phash metric, the traffic load was unevenly distributed to real servers with random source IP addresses	prod00260470

Item	Description	Bug ID
100.	In an Outbound Link Load Balancing environment, LinkProof continued to send dispatching traffic towards WAN links whose bandwidth utilization was above 100%.	prod00260455
101.	You could not paste a geo network class configuration as taken from the configuration file and mandate it to add None for the Country and State fields.	prod00260454
102.	In a LinkProof environment configured with the bandwidth metric, Alteon did not select a WAN link based on the bandwidth metric configured on the DNS hostname and the DNS response included WAN links with the bandwidth overloaded.	prod00260453
103.	Using WBM with a WAN Link configuration, there were discrepancies between the upload bandwidth of the Per WAN Link IP and the Per WAN Link ID.	prod00260388
104.	Using WBM, when adding an IPv6 NAT IP address with the default prefix, because the IP address was added with prefix 0 instead of 128, the Apply operation failed.	prod00260360
105.	Using WBM, in a virtualization environment on an ADC-VX, the administrator could not change a vADC's administrator password.	prod00260333
106.	Using WBM or REST API with certificate repository management, you could not overwrite a certificate.	prod00260330
107.	In a BGP environment, after sending a BGP route update after a set of apply operations and a BGP toggle, a panic occurred.	prod00260322
108.	In a BGP environment, during BGP route update or when the BGP peer went down during BGP peer "cleanup," the platform hung.	prod00260321
109.	For unknown reasons, an unexpected reboot and a panic occurred.	prod00260320
110.	In an SLB environment, ESP traffic was not passed to the back-end servers.	prod00260297
111.	When using REST API to change the next image to boot, the correct image was not set.	prod00260261
112.	Using CLI, when configuring network classes, there were no validations when geo information was added for a network class as a one line command.	prod00260260
113.	Sometimes you could not configure a management port with an IPv6 address that was identical to one generated by SLAAC.	prod00260161

Item	Description	Bug ID
114.	In an SLB environment with delayed binding enabled and APM enabled, because Alteon did not create persistent entries for a few specific clients, Alteon sent the request from a specific Client IP address to a virtual service on Alteon to different real servers, even with the persistent binding Client IP address set on the virtual service.	prod00260097
115.	Using WBM, in an SSL environment, when enabling back-end SSL encryption and the back-end SSL cipher was selected as "user-defined," and then the back-end SSL encryption was disabled, the saved configuration was improper due to a malformed XML.	prod00260026
116.	In a virtualization environment on an ADC-VX, when using a REST API call to create a vADC, a panic occurred.	prod00259835
117.	In a virtualization environment on an ADC-VX, when a configuration import (putcfg) operation was performed via SNMP, a panic occurred on the ADC- VX.	prod00259831
118.	In an SLB environment with the health check configuration destination set as hostname, the health check failed after performing an apply operation.	prod00259830
119.	When SSH/Telnet connections exceeded the allowed limit, no syslog message generated.	prod00259797
120.	In a virtualization environment with vADCs on the same ADC-VX cross-connected, ARP responses were dropped, causing a gateway failure.	prod00259735
121.	In a failover scenario, when adding or updating more than 256 FDB entries from the MP to the SP, if the SP overloaded, the SP was not able to add the entries to the spfdb table, causing traffic disruptions in the network.	prod00259698
122.	In an AppWall for Alteon VA environment, techdata generation abruptly stopped and a reboot was required.	prod00259694
123.	When Alteon was accessed via SSH, the TCP connections opened for SSH sessions were not closed properly as the client continued to send data and caused stale TCP sessions. This led to SSH access failure to the device.	prod00259686

Item	Description	Bug ID
124.	In a virtualization environment, after manual reboot on a vADC and when the vADC was disabled/enabled using the ADC-VX, the Apply operation returned the following error message: `vADC management changes due to a previous apply are currently under progress. Please try to apply the new changes after some time.`	prod00259681
125.	Using WBM, in **Monitoring > Network > High Availability**, the VRRP labels were incorrect.	prod00259626
126.	The vulnerability scan on the Alteon ADC-VX management IP address issued the following message: `SSL/TLS Server supports TLSv1.0` **Note**: Configuration for the TLS version was added (affecting management traffic only): In CLI: `/cfg/sys/access/https/tlsver` In WBM: **System > Management Access > Management Protocol > HTTPS**	prod00259614
127.	In an SLB environment with persistent binding (pbind) configured with a cookie and Client IP, when Layer 4 sessions aged out, the reference count was decremented for the wrong persistent session, causing stale p-sessions.	prod00259581
128.	In a VRRP hot-standby environment, when the hot-standby port was designated as the next-hop port of the static ARP entry for a destination on the backup, a packet to the destination was sent out from that port even though it was in the Blocked state.	prod00259550
129.	In an SLB environment with FQDN real servers configured, on a virtual server with FQDN real servers, Alteon returned a 503 error even though the real servers were up.	prod00259492
130.	In an SLB environment with AppShape++ attached to a particular service, although alwayson was disabled, when the service went down, the request was forwarded to AppXcel.	prod00259436
131.	When attempting to upload a configuration to an RMA device, a panic occurred.	prod00259399
132.	In an SLB environment with AppShape++ configured, after aging, the TCP::close_type AppShape++ command returned an incorrect value in CLIENT_CLOSED, SERVER_CLOSED events.	prod00259384
133.	In an SLB environment with AppShape++ configured, after aging, TCP::close reset AppShape++ command did not send a reset when called from CLIENT_CLOSED, SERVER_CLOSED events.	prod00259334

Item	Description	Bug ID
134.	Using WBM, in a Layer 7 environment when a content class was deleted and a new one was created, some AX-related configuration errors displayed upon Apply/Revert Apply, leading to some AX traffic processing issues with the content class.	prod00259330
135.	In a VRRP environment, the backup Alteon did not change the source MAC and used the proxy MAC while routing the packet on the backup device.	prod00259179
136.	In a virtualization environment, after disabling a vADC, the vADC's internal syslogs were deleted from the ADC-VX.	prod00259152
137.	After generating a Tech Support dump or techdata, the resource allocation table information (`/maint/debug/rsrcdump`) was missing.	prod00258995
138.	Outbound Telnet connections from ADC-VX/vADCs are not terminated when the respective inbound Telnet/SSH connections to the ADC-VX/vADCs are abruptly terminated, causing the user to not be able to access the ADC-VX after closing Telnet sessions abruptly.	prod00258970
139.	After configuring two interfaces, and not on same network, when a SNMP request was sent to one interface IP address, the response came from another interface.	prod00258932
140.	In an HA environment, when the proxy IP range is configured under the network class and a failover occurs, a GARP was not sent for all the proxy IP addresses in the range. **Note**: The following new command was implemented: `/cfg/l3/ha/nwclgarp ena/dis` If the network class range is huge, then the GARP being sent affects the peers ARP table.	prod00258850
141.	In an SLB environment with server groups, although the mhash configuration is only relevant for the minmisses metric, you could also configure it for other metrics (leastconn and svcleast), causing an Apply in these cases to fail.	prod00258826

AppWall

Item	Description	Bug ID
1.	Could not add a Protected URI in CSRF with a double slash.	DE7213
2.	AppWall did not process an empty file with chunked transfer Encoding.	DE38763

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

Fixed in 32.0.1.101

Version 32.0.1.101 includes all field bugs available in version 31.0.5.0.

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

Fixed in 32.0.1.100

Version 32.0.1.100 includes all field bugs available in version 31.0.5.0.

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

Fixed in 32.0.1.0

Item	Description	Bug ID
1.	Using WBM, it was not possible to add or edit vADCs	prod00261306
2.	In a Smart NAT environment, due to the sequence of validations in Global SLB, the warning messages for gmetric were confusing to the user. **Note:** The proximity metric for Inbound Link Load Balancing rules with Smart NAT is not yet supported.	prod00260963
3.	In a Smart NAT environment with Global SLB turned off and LinkProof turned on, the validations related to Smart NAT were skipped and no warning messages were issued. **Note:** Proximity is not yet supported for SmartNAT.	prod00260961
4.	In a DNS environment where DNS responses were received, and with VRRP or HA, performing a configuration sync ended with an FQDN error.	prod00260835
5.	In a VRRP environment, after sync was performed, the server group setting was removed from the peer device.	prod00260807
6.	In an SLB environment with the round robin or least connections metric, and with a traffic pattern that had few connections that were opened with relatively long time periods between each other, after migrating all virtual servers from the 5208 platform to the 6420 platform, the round robin metric kept selecting only one specific real server from the server group and did not balance traffic to some servers.	prod00260667
7.	In WBM, the SLB Viewer user role was allowed to enable/disable physical ports, when this user role should only be able to view Alteon information, SLB statistics, and information, but should not be able to make any configuration changes.	prod00260640

Item	Description	Bug ID
8.	Using WBM, a real server's Description accepted 128 characters while only 31 characters are supported, causing the real server Description not to be synced from Active to Standby.	prod00260637
9.	Alerts regarding DUAL PSU failure were generated, but after 6 seconds a notice was issued that the Status was Ok. This issue persisted even after changing to a new PSU.	prod00260596
10.	On a 6024 XL platform with 32 GB RAM, in Maximum vADC Density mode, you could not allocate the twelfth (12th) CPU core (the fourth core for MP processing).	prod00260579
11.	In a virtualization environment, when accessing the device on an ADC-VX using REST API with an incorrect customized Authorization header value, a panic occurred.	prod00260578
12.	Using REST API, image upload did not work.	prod00260563
13.	In an SLB environment, when a proxy IP address was defined in a network class, the proxy MAC address was sent with the gateway MAC address to those proxy IP addresses that were not present in the ARP table, causing the applications to fail.	prod00260560
14.	The load time of REST API calls was much slower than the load time in earlier Alteon versions.	prod00260508
15.	In an SLB environment with SSL Hello or HTTPS health checks configured, after upgrading to version 30.2.9.0, real servers configured with these health checks failed.	prod00260484
16.	In an SLB environment with the phash metric, the traffic load was unevenly distributed to real servers with random source IP addresses.	prod00260469
17.	In an Outbound Link Load Balancing environment, LinkProof continued to send dispatching traffic towards WAN links whose bandwidth utilization was above 100%.	prod00260451
18.	You could not paste a geo network class configuration as taken from the configuration file and mandate it to add **None** for the **Country** and **State** fields.	prod00260450
19.	In a LinkProof environment configured with the bandwidth metric, Alteon did not select a WAN link based on the bandwidth metric configured on the DNS hostname and the DNS response included WAN links with the bandwidth overloaded.	prod00260449
20.	Using WBM with a WAN Link configuration, there were discrepancies between the upload bandwidth of the **Per WAN Link IP** and the **Per WAN Link ID**.	prod00260386

Item	Description	Bug ID
21.	Using WBM, when adding an IPv6 NAT IP address with the default prefix, because the IP address was added with prefix 0 instead of 128, the Apply operation failed.	prod00260359
22.	Using WBM or REST API with certificate repository management, you could not overwrite a certificate.	prod00260329
23.	In a BGP environment, after sending a BGP route update after a set of apply operations and a BGP toggle, a panic occurred	prod00260319
24.	In a BGP environment, during BGP route update or when the BGP peer went down during BGP peer "cleanup," the platform hung.	prod00260318
25.	For unknown reasons, an unexpected reboot and a panic occurred.	prod00260317
26.	In an SLB environment, ESP traffic was not passed to the back-end servers.	prod00260296
27.	When using REST API to change the next image to boot, the correct image was not set.	prod00260259
28.	Using CLI, when configuring network classes, there were no validations when geo information was added for a network class as a one line command.	prod00260258
29.	In an SLB environment with delayed binding enabled and APM enabled, because Alteon did not create persistent entries for a few specific clients, Alteon sent the request from a specific Client IP address to a virtual service on Alteon to different real servers, even with the persistent binding Client IP address set on the virtual service.	prod00260096
30.	Due to a large file size, the techdata generation failed with the following message: `Unknown Error`	prod00260082
31.	Using WBM, in an SSL environment, when enabling back-end SSL encryption and the back-end SSL cipher was selected as "user-defined," and then the back-end SSL encryption was disabled, the saved configuration was improper due to a malformed XML.	prod00260025
32.	In a virtualization environment on an ADC-VX, when using a REST API call to create a vADC, a panic occurred.	prod00259834
33.	In an SLB environment with the health check configuration destination set as hostname, the health check failed after performing an apply operation.	prod00259829

Item	Description	Bug ID
34.	In a virtualization environment on an ADC-VX, when a configuration import (putcfg) operation was performed via SNMP, a panic occurred on the ADC- VX.	prod00259828
35.	When SSH/Telnet connections exceeded the allowed limit, no syslog message generated.	prod00259798
36.	In a virtualization environment with vADCs on the same ADC-VX cross-connected, ARP responses were dropped, causing a gateway failure.	prod00259734
37.	In an AppWall for Alteon VA environment, techdata generation abruptly stopped and a reboot was required.	prod00259693
38.	When Alteon was accessed via SSH, the TCP connections opened for SSH sessions were not closed properly as the client continued to send data and caused stale TCP sessions. This led to SSH access failure to the device.	prod00259684
39.	Using WBM, in **Monitoring > Network > High Availability**, the VRRP labels were incorrect.	prod00259625
40.	In an SLB environment with persistent binding (pbind) configured with a cookie and Client IP, when Layer 4 sessions aged out, the reference count was decremented for the wrong persistent session, causing stale p-sessions.	prod00259580
41.	Using WBM, using $PROTOCOL instead of http:// or https:// in the redirection URL for content rules action redirect or action redirect for a service did not work.	prod00259520
42.	In an SLB environment with FQDN real servers configured, on a virtual server with FQDN real servers, Alteon returned a 503 error even though the real servers were up.	prod00259491
43.	In an HA environment, although synchronization was successful, the backup device issued the following error: `HA: Configuration is not synchronized between the HA devices`	prod00259438
44.	In a Geo proximity configuration, you could not set the country **Niger** in an Alteon GEO network class.	prod00259435
45.	In an SLB environment, when submitting a service (that supports non-standard ports) with a standard port, although the Alteon bank-end returned an error, due to the standard port, Alteon internally configured the corresponding service even after issuing the error without informing the user.	prod00259422

Item	Description	Bug ID
46.	In a virtualization environment, after manual reboot on a vADC and when the vADC was disabled/enabled using the ADC-VX, the Apply operation returned the following error message: `vADC management changes due to a previous apply are currently under progress. Please try to apply the new changes after some time.`	prod00259410
47.	When attempting to upload a configuration to an RMA device, a panic occurred.	prod00259398
48.	In an SLB environment with AppShape++ configured, after aging, the TCP::close_type AppShape++ command returned an incorrect value in CLIENT_CLOSED, SERVER_CLOSED events	prod00259383
49.	In an SLB environment with AppShape++ configured, after aging, TCP::close reset AppShape++ command did not send a reset when called from CLIENT_CLOSED, SERVER_CLOSED events.	prod00259333
50.	Using WBM, in a Layer 7 environment when a content class was deleted and a new one was created, some AX-related configuration errors displayed upon Apply/Revert Apply, leading to some AX traffic processing issues with the content class.	prod00259329
51.	In a VRRP environment, the backup Alteon did not change the source MAC address and used the proxy MAC address while routing the packet on the backup device.	prod00259178
52.	In a virtualization environment, after disabling a vADC, the vADC's internal syslogs were deleted from the ADC-VX.	prod00259151
53.	The vulnerability scan on the Alteon ADC-VX management IP address issued the following message: SSL/TLS Server supports TLSv1.0 **Note**: Configuration for the TLS version was added (affecting management traffic only): In CLI: `/cfg/sys/access/https/tlsver` In WBM: **System > Management Access > Management Protocol > HTTPS**	prod00258998
54.	Outbound Telnet connections from ADC-VX/vADCs are not terminated when the respective inbound Telnet/SSH connections to the ADC-VX/vADCs are abruptly terminated, causing the user to not be able to access the ADC-VX after closing Telnet sessions abruptly.	prod00258969

Item	Description	Bug ID
55.	After generating a Tech Support dump or techdata, the resource allocation table information (/maint/debug/rsrcdump) was missing.	prod00258963
56.	After configuring two interfaces, and not on same network, when a SNMP request was sent to one interface IP address, the response came from another interface.	prod00258925
57.	In an HA environment, when the proxy IP range is configured under the network class and a failover occurs, a GARP was not sent for all the proxy IP addresses in the range. **Note**: The following new command was implemented: `/cfg/l3/ha/nwclgarp ena/dis` If the network class range is huge, then the GARP being sent affects the peers ARP table.	prod00258854
58.	Sometimes you could not configure a management port with an IPv6 address that was identical to one generated by SLAAC.	prod00258853
59.	In an SLB environment with AppShape++ attached to a particular service, although alwayson was disabled, when the service went down, the request was forwarded to AppXcel.	prod00258825
60.	In an SLB environment with IPv4 and IPv6 services and IPv6 PIP configured, a panic occurred.	prod00258580
61.	In an SLB environment with server groups, although the mhash configuration is only relevant for the minmisses metric, you could also configure it for other metrics (leastconn and svcleast), causing an Apply in these cases to fail.	prod00258549
62.	In an AppWall for Alteon environment, when an APSolute Vision syslog came from AppWall through the proxy, and LDAP traffic also used the proxy, Web Authentication via AppWall stopped working.	prod00258525
63.	Using WBM, in a virtualization environment on an ADC-VX, the administrator could not change a vADC's administrator password.	prod00258405
64.	In an SLB environment with session mirroring enabled for virtual services, the session statistics were incorrect on the backup device compared to the primary device.	prod00258381
65.	For DNS Responder virtual servers with DNS over UDP only, DNS resolution failed.	prod00258374
66.	Using WBM, in an SLB monitoring environment, the real server IP addresses for a server group were displayed incorrectly.	prod00258332

Item	Description	Bug ID
67.	When logging into WBM using TACACS and performing configuration changes and later performing Apply/Save operations, in the audit logs another user ID was recorded instead of the user who logged in.	prod00257825
68.	SSL Hello health checks using TLS (instead of SSL v2/v3) were not working on XL/Extreme platforms.	DE34416
69.	From WBM, you cannot change the vADC management IP address from within the ADC-VX environment.	prod00216388
70.	Parameter security events may cause excessive or high event size.	DE21382
71.	Details button was missing in the Database Security Filter view.	DE25177
72.	Under certain conditions, SSL termination causes SSL session traffic interruptions in passive mode.	DE30899
73.	Vulnerability security refinement in a defined Virtual Directory doesn't block traffic.	DE31063
74.	Failure in the Blocked Source table (Source Blocking) due to a failure in the Fingerprint hash value.	DE31964
75.	After multiple consecutive memory dumps, log partition becomes full.	DE32927
76.	Database security filter blocks legitimate HTTP requests.	DE33867
77.	Compatibility error message with web browser when using Activity Tracking fingerprint based with Vulnerabilities security filter.	DE34015
78.	Failure in the Database security filter after an upgrade with an AppWall version older than 5.7.2.	DE34070
79.	Refinement error message when trying to refine an HTTP reply size header.	DE34119
80.	Duplicate IP Group and Security WebApplication Role when using the API call with import option for policy distribution.	DE34185 DE34453
81.	Hosts based configurations that contain a wildcard are not taken into consideration.	DE35113
82.	Under certain conditions, Database security refinement disappears.	DE35457
83.	Under certain conditions, a failure occurs with huge HTTP response request.	DE32953
84.	After a failed Apply operation, the tunnel cannot be initialized.	DE21581

Item	Description	Bug ID
85.	Failure occurs in Fast Upload	DE33520
86.	AppWall Management Application failures when refreshing the forensics view with a very high of events	DE30806
87.	Go to Policy button in Forensics view generate an AppWall Management Application exception for RFC Violated Security Events.	DE31200
88.	Failure in the AppWall Management Application occurred after creating a complex REGEX in the security policies settings	DE33872
89.	Wrong IP address in the syslog messages	DE34357

Fixed in 32.0.0.0

Version 32.0.0.0 includes all field bugs available in version 31.0.4.0.

KNOWN LIMITATIONS

The list of known limitations, available to customers only, is available at the following link:
https://support.radware.com/app/answers/answer_view/a_id/1021441

RELATED DOCUMENTATION

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

North America	International
Radware Inc.	Radware Ltd.
575 Corporate Drive	22 Raoul Wallenberg St.
Mahwah, NJ 07430	Tel Aviv 69710, Israel
Tel: +1-888-234-5763	Tel: 972 3 766 8666