



AlteonOS **RELEASE NOTES**

Version 34.0.3.0
January 3, 2024



TABLE OF CONTENTS

CONTENT	6
RELEASE SUMMARY.....	6
SUPPORTED PLATFORMS AND MODULES	6
UPGRADE PATH	7
Before Upgrade – Important!.....	7
Additional Considerations.....	8
Downgrade	8
WHAT’S NEW IN 34.0.3.0	9
New Alteon Automation Engine.....	9
Traffic Capture Enhancements	11
Memory Options for 6300 Platform	11
Alteon Cluster Management HA.....	11
Link Layer Discovery Protocol (LLDP)	12
PIP Advertising via BGP.....	12
SNMP OID to Monitor Peak Session	12
Immediate Backend Bind	13
Exclude DNS Responders from Config Sync.....	13
WHAT’S NEW IN 34.0.2.0	13
6300 Platform Enhancements.....	13
Alteon Kubernetes Connector Enhancements (version 1.4.0).....	14
Ingress Resource Support	14
Static IP for AKC Service	14
Alteon High Availability.....	15
LDAP User Authentication	15
CDP (CRL Distribution Point) High Availability	15
Ansible Enhancements.....	15
Red Hat Certification	15
New Ansible Modules.....	15
AWS HA Enhancements	16
Cluster Manager Enhancements.....	16
New GEL LLS Notifications	16
HTTP IP Header Configuration on Filter	17
WHAT’S NEW IN 34.0.1.0	17

New Alteon 6300 Platform.....	17
Alteon VA Subscription Model.....	18
Alteon Cluster Management for VMware Environment.....	18
Alteon Support in Cyber Controller High-Availability.....	19
VXLAN Support.....	20
Low and Slow (Slowloris) Attack Protection for TLS.....	20
BGP ECMP Support on Load Balanced Traffic.....	21
Support for IPv6 Subnet Prefix of 64.....	21
sysName LLDP Support.....	21
GEL Entitlement Description.....	21
Integrated AppWall.....	21
GraphQL Protocol Support - BETA.....	21
WHAT'S NEW IN 34.0.0.0.....	22
GEL Support in Standalone Mode.....	22
Alteon Kubernetes Connector Enhancements.....	22
Overload Protection for Integrated WAF.....	23
Slowloris Attack Protection.....	24
Layer 7 Modification on HTTP/2 traffic.....	24
Out-of-the-box Certificate Pinned Sites List.....	25
Sideband and SecurePath Updates in Unified Events.....	26
GEL Dashboard Enhancements.....	26
Control and Export of Management Port Packet Capture from WBM.....	26
WHAT'S CHANGED IN 34.0.3.0.....	27
Reduce Default Traffic Event Sampling.....	27
End to End time Enhancements.....	27
OpenSSL Upgrade.....	27
Startup Wizard Enhancement.....	27
FastView Feature Deprecation.....	27
Exclusion of URL Categorization from Secure Subscription License.....	28
License Validation During Config Import.....	28
Integrated AppWall.....	28
HTML Decoding.....	28
Vulnerability Partial Scan.....	28
GraphQL Protection.....	28
WHAT'S CHANGED IN 34.0.2.0.....	29
vRO Plugin Update.....	29
OpenSSL Upgrade.....	29
Quick Application Wizard Enhancement.....	29

GSLB Network Number Increase	29
Password Policy Enhancements	29
"wget" Package Update	30
SecurePath Policies Number Increase	30
Integrated AppWall	30
GraphQL Protection	30
Custom Pattern	30
Limit Number of Headers to Parse	30
Base64 Decoding	30
Redirect Validation Host Protection	30
WHAT'S CHANGED IN 34.0.1.0	30
Network HSM (Thales/Gemalto) Enhancements	30
BWM Shaping	31
UDP Virtual Service Down Response	31
Updated Option to Enable/Disable Weak Algorithms in SSH	31
Alteon Embedded Dashboard Removal	31
Advanced Virtual Wire Health Check Enhancements	31
Change in AppWall SNMP Trap OID	31
Integrated AppWall	32
Multiple Improvements	32
WHAT'S CHANGED IN 34.0.0.0	32
UDP Stateless and TCP Services on the Same VIP	32
Integrated WAF SUS and GEO DB Update Via Proxy	32
Combined Image Upload Option Removed from WBM	32
Service and Real PPS Collection Interval	33
OpenSSL Upgrade	33
Integrated AppWall	33
API Security	33
Custom Pattern per Application Path	33
Server-Side Request Forgery	33
Multiple IPs Included in XFF HTTP Header	34
Global Security Event Suppression	34
Database Security Filter	34
Multiple Enhancements on AppWall REST API for DevOps	34
MAINTENANCE FIXES	34
Fixed in 34.0.3.0	34

General Bug Fixes	34
AppWall Bug Fixes	37
Fixed in 34.0.2.10	37
AppWall Bug Fixes	37
Fixed in 34.0.2.0	37
General Bug Fixes	37
AppWall Bug Fixes	40
Fixed in 34.0.1.0	40
General Bug Fixes	40
AppWall Bug Fixes	42
Fixed in 34.0.0.0	43
General Bug Fixes	43
AppWall Bug Fixes	46
KNOWN LIMITATIONS	46
RELATED DOCUMENTATION	46



CONTENT

Radware announces the release of AlteonOS version 34.0.3.0. These release notes describe new and changed features introduced in this version on top of version 34.0.2.0.

RELEASE SUMMARY

Release Date: January 3, 2024

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

SUPPORTED PLATFORMS AND MODULES

This version is supported by the following platforms:

- 4208, 4208S
- 5208, 5208S
- 5424S, 5424SL, 5820S, 5820SL
- 6024, 6024S, 6024SL, 6024 FIPS II
- 6300
- 6420p, 6420, 6420S, 6420SL
- 7612S, 7612SL
- 7220S, 7220SL
- 7100S, 7100SL, 7100DS
- 7700S, 7700SL, 7700DS
- 8420, 8420S, 8420SL
- 8820, 8820S, 8820SL
- 9800, 9800S, 9800SL
- Alteon VA running on VMware ESXi 6.0, 6.5, 6.7, 7.0, 8.0, KVM, Hyper-V, and OpenXen
- Alteon VA on AWS
- Alteon VA on Azure
- Alteon VA on Nutanix
- Alteon VA on Oracle Cloud
- Alteon VA on Google Cloud

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

Alteon 34.0.3.0 is supported by APSolute Vision version 4.30 and later, and Cyber Controller 10.0 and later.

Integrated AppWall version: 7.6.22.0

OpenSSL version:

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

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 28.x, 29.x, 30.x, 31.x, 32.x, 33.x and 34.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 34.0.3.0:

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 34.0.3.0 using the recovery process. Note: You must save the configuration before starting this process.
29.0.x (x=<8)	> 29.0.9.0 > 30.5.3.0 > this version	
29.0.x (x > 8)	> 30.5.3.0 > this version	
29.5.x (x=<7)	> 29.5.8.0 > 30.5.3.0 > this version	
29.5.x (x>7)	> 30.5.3.0 > this version	
30.x =< 30.5.2.0	> 30.5.3.0 > this version	
30.x > 30.5.2.0	Direct upgrade to this version	
31.x	Direct upgrade to this version	
32.x	Direct upgrade to this version	
33.x	Direct upgrade to this version	
34.x	Direct upgrade to this version	



Additional Considerations

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

Important!

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

Downgrade

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

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



WHAT'S NEW IN 34.0.3.0

This section describes the new features and components introduced in this version on top of Alteon version 34.0.2.0.

New Alteon Automation Engine

The new Alteon Automation Engine available starting with Cyber Controller 10.4 facilitates the efficient execution of complex operations and frequently recurring tasks using templates and minimizes manual errors and overhead associated with administrative tasks.

Templates are predefined sets of configuration settings that you can apply to multiple instances and reuse as needed. Templates help you follow best practices and ensure compliance across the organization. By using templates, you can specify and enforce security settings, network configurations, and other relevant parameters in a consistent and systematic way. With Alteon Automation Ansible-based templates, you can perform tasks such as onboarding Alteon instances and deploying new applications in a standardized way, saving time and effort in managing complex environments. You do not need to be an expert in application delivery and security to manage complex and advanced services. You just need to know which template to use for a service to enable and update it. This way, you do not have to ask the subject matter experts (SMEs) and architects for help with configuration and management issues. This reduces the number of escalations and the total time spent and improves the operational efficiency of the IT organization.

Alteon Automation revolutionizes the conventional manual service management approach by transforming it into an automated process that is managed through an intuitive UI. This UI does not require any familiarity or expertise with the managed solutions. The expertise and knowledge to manage advanced ADC services are built into the templates and workflows available through this easy-to-use UI.

For instance, when operators execute a template that deploys a new instance of a service or application, they are guided via a graphical interface to provide the unique parameters of the service, such as IP address, server IP, and SSL key. The bulk of the service configuration is standardized based on application and business requirements by the creator of the template. All these standardized components are automatically added to the solution configuration.

The 'Run Action' dialog box is shown with the 'Parameters' tab selected. It contains the following fields:

- VIP ***: A text input field with the placeholder 'Type Here'.
- Server Port**: A text input field with the value '0'.
- Service Port ***: A text input field with the placeholder 'Type Here'.
- SSL certificate ***: A text input field with the placeholder 'Type Here'.

At the bottom right, there are 'Cancel' and 'Run' buttons.

The Automation Engine enables you to customize and create templates that suit your needs, in addition to the ones provided out-of-the-box for the most common tasks in application delivery.

The 'Alteon Automation' interface is displayed. On the left, the 'Templates' section shows a list of predefined templates:

Favorite	Name	Category	Origin	Description
☆	Deploy_HTTP_app_OOB	Application Deployme...	Predefined	
☆	Deploy_HTTPS_app_OOB	Application Deployme...	Predefined	
☆	Device_onboarding_OOB	Device Onboarding	Predefined	
☆	Deploy_TCP_UDP_app_OOB	Application Deployme...	Predefined	

On the right, the 'Jobs' section shows a list of running and completed jobs:

Running (0)		Completed (8)	
Name	Description	Template Name	Execution Mode
job7		Deploy_HTTP_app_OOB	Immediate
555555		Deploy_HTTP_app_OOB	Immediate
4444		Deploy_HTTP_app_OOB	Immediate
3333		Deploy_HTTP_app_OOB	Immediate
2		Deploy_HTTP_app_OOB	Immediate
1		Deploy_HTTP_app_OOB	Immediate
job2		Deploy_HTTP_app_OOB	Immediate
job1		Deploy_HTTP_app_OOB	Immediate

The new Alteon Automation Engine lets you leverage the power of automation to streamline your processes and optimize their outcomes by providing

- Centralized templates repository
- RBAC – You can control the user roles that can run a specific template and the devices on which a user can run templates
- Tracking template run and outcome
- Auditing



Traffic Capture Enhancements

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

This new feature enhances troubleshooting capabilities.

NFR ID: 230413-000074

Memory Options for 6300 Platform

Starting with this version, the Alteon 6300F and 6300M platforms support memory upgrade from 32 GB to 64 GB and 128 GB. The memory upgrade will be available as factory installed or as a field upgrade.

The extended memory enables use of more vADCs, from the current maximum of eight (8, to 10 in Default mode, and up to 26 in Maximum mode.

Alteon Cluster Management HA

Starting with Cyber Controller version 10.4, you can use the Alteon Cluster Manager (ACM) in a Cyber Controller HA installation. This ensures that ACM will continue operating after Cyber Controller failover. Note that Alteon Cluster Manager must not be used in a Cyber Controller HA scenario if the Cyber Controller version is earlier than 10.4.

There are a few issues to consider when using Alteon Cluster Manager in an HA scenario:

- When a Cyber Controller instance becomes active (bootup or failover) the Alteon Cluster Manager service cold starts – it becomes active only after 10 minutes. This capability is required to reduce the risk of a split brain (both Cyber Controller instances in an HA pair acting as the active instance). The cold start capability reduces the chance of this condition occurring when the Primary Cyber Controller reboots or when the communication disconnection between the Cyber Controller instances is temporary (under 10 minutes).
- If Cyber Controller failover occurs while a cluster provisioning, cluster scale-out, or cluster scale-in job is in process, it can result in zombie VMs – VMs that are provisioned in vCenter but are not registered in the Alteon Cluster Manager. Currently this condition must be solved by removing the zombie VMs from vCenter.

Note that zombie VMs can occur also in standalone Cyber Controller mode, if Cyber Controller reboots while a cluster provisioning, cluster scale-out, or cluster scale-in job is in process.

- The process of upgrading the software version on a pair of Cyber Controller instances in HA mode currently requires decoupling the HA pair (disabling HA), upgrading the individual Cyber Controller instance and recoupling the pair. When the Cyber Controller pair is decoupled, the ACM process remains active only on the Cyber Controller instance that was Primary before the decoupling, as explained above. It is important when re-enabling the HA that the same Cyber Controller is defined as Primary.

Link Layer Discovery Protocol (LLDP)

Starting with this version, the Link Layer Discovery Protocol (LLDP) is also available on the management ports.

NFR ID: 221024-000119

PIP Advertising via BGP

Alteon can now advertise client NAT (PIP) addresses to its BGP peers. This feature is applicable only for FRR BGP mode.

This feature allows to enable advertising the different types of PIPs – port-based PIPs, VLAN-based PIPs, and virtual service-based ones.

To enable PIP advertising via CLI:

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

```
[PIP Redistribution Menu]
```

```
pip - PIP Advertisement Menu
```

```
ppip - Enable/disable advertising port based PIP addresses
```

```
vpip - Enable/disable advertising vlan based PIP addresses
```

```
extpip - Enable/disable advertising extra PIP addresses
```

```
cur - Display current PIP redistribution configuration
```

To enable PIP advertising via WBM got to **Network > Layer 3 > Dynamic Routing > BGP page**.

To enable advertising PIP addresses that are configured at virtual service level, enable advertising extra PIP addresses, and configure the specific addresses you want to advertise. You can specify up to 128 PIP addresses (IPv4 and IPv6 together).

NFR ID: 230420-000126

SNMP OID to Monitor Peak Session

The following SNMP OIDs were added for peak session monitoring:

- Peak number of session entries:
 - switchCapPeakSession - 1.3.6.1.4.1.1872.2.5.1.3.9.3.92
- Peak session entries in percentage:
 - switchCapPeakSessionPercentage - 1.3.6.1.4.1.1872.2.5.1.3.9.3.93

NFR ID: 230425-000158

Immediate Backend Bind

When Alteon processes HTTP/S traffic using filters (**Application** set to **HTTP**), the back-end TCP connection is only opened after the first HTTP request is received on the client side. A new flag allows opening the back-end TCP connection as soon as the TCP handshake on the client side is completed and before the first HTTP request arrives.

Enabling immediate bind requires the following conditions:

- A filter set is configured
- All filters in the filter set have **Action** set to **Allow** and **Application** set to **HTTP**.

To enable immediate bind:

- CLI – `/c/slb/filt/adv/frcebind ena`
- WBM – **Application Delivery > Filters > Add/Edit Filter > HTTP tab > Force Immediate Backend Bind**

NFR ID: 230822-000111

Exclude DNS Responders from Config Sync

The DNS Responders are by default synchronized to a peer Alteon device. Now it is possible to exclude them from configuration synchronization.

To disable syncing DNS responders:

- CLI: `cfg/slb/sync/resvips d`
- WBM: Go to **Network > High Availability > Configuration Sync**, select the *Modules to Sync* tab, and disable **DNS Responders**.

WHAT'S NEW IN 34.0.2.0

This section describes the new features and components introduced in this version on top of Alteon version 34.0.1.0.

6300 Platform Enhancements

Alteon D-6300 is available with two configurations:

- D-6300F – Fixed configuration with a 4x25G NIC card and the SSL acceleration card. It is available with 40G L4 throughput license.
- D-6300M – Modular platform with four slots:
 - Slot 1: 2x25G or 4x10G NIC card
 - Slot 2: 2x25G or 4x10G NIC card
 - Slot 3: Optional QAT
 - Slot 4: Optional 8x1G NIC card

The D-6300M is available with L4 throughput licenses of 60G and 90G.

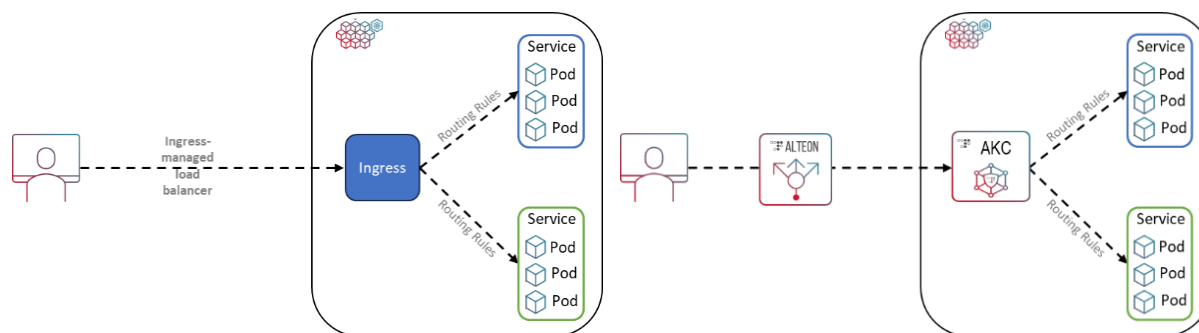
With this release, the D-6300 platform supports ADC-VX mode with up to eight (8) vADCs.

Alteon Kubernetes Connector Enhancements (version 1.4.0)

Ingress Resource Support

The Ingress resource in Kubernetes allows external access to services within a cluster by exposing HTTP and HTTPS routes. The routing of traffic is governed by rules defined in the Ingress resource. An Ingress controller is responsible for fulfilling the Ingress, usually with a load balancer.

When AKC is deployed in your Kubernetes clusters, it now allows provisioning Alteon as an external load balancer fulfilling the Ingress – providing Layer 7 load balancing and SSL/TLS termination.



To make an Ingress secure, you must provide a Secret that has a TLS private key and certificate. The Ingress resource can only use one TLS port, 443, and it assumes that the TLS connection ends at the Ingress point (Alteon in this case), and the traffic to the Service and its Pods is not encrypted.

When fulfilling Ingress, Alteon provides load balancing at the Pod level. Alteon sends traffic directly to the Pods, bypassing the internal load balancing mechanism of the Kubernetes cluster. This is achieved using BGP and requires that the Calico Container Network Interface (CNI) plug-in is used with the K8s cluster.

Static IP for AKC Service

By default, AKC allocates a VIP for a newly deployed Kubernetes service from IPAM. Now it is possible for the operator that deploys the Kubernetes service to manually allocate a specific IP address by using the following annotation: `akc.radware.com/static-ip: <virtual-ip>`

NFR ID: 230609-000038

Alteon High Availability

You can now configure both primary and backup Alteons in the AKC Configurator, to ensure that the Alteons continue to be updated with all changes occurring in the Kubernetes clusters even when the primary Alteon fails.

LDAP User Authentication

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

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

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

NFR ID: 221012-000007

CDP (CRL Distribution Point) High Availability

Until this version, when multiple CDPs (URIs) are defined within the same CDP group, each one is checked ('AND' function) and the certificate is validated only if it is not listed in any of the CDPs. In such a case, if any CDP becomes unavailable, the certificate is not validated.

Starting with this version, Alteon lets you list two CDPs (URIs) as two separate endpoints within one CDP group. In such a case, they work as high-availability support ('OR' function), where if one CDP is unavailable, the certificate is validated by the second CDP.

Ansible Enhancements

Red Hat Certification

The Alteon Ansible collection is now certified by Red Hat and appears in the Red Hat Ecosystem Catalog under Certified Ansible Collections as [radware_alteon_collection](#).

NFR ID: 220707-000144, 230213-000142

New Ansible Modules

The following Ansible modules were added:

- `alteon_config_sideband_policy`: supports Sideband Policy configuration
- `alteon_config_secure_path_policy`: supports SecurePath Policy configuration
- `alteon_config_security_global`: supports enabling/disabling SecurePath at device level

In addition, new fields were added to `alteon_config_virtual_service` to support configuring Sideband and SecurePath policies per virtual service.



AWS HA Enhancements

To enable transferring the public IP address from the primary Alteon device to the backup device in case of failover, Alteon must have access to the AWS account running the Alteon VA virtual machines.

Until now, for Alteon to have access to the AWS account, the user was required to configure on the Alteon instances the AWS Access Key and Secret Key.

A new, more secure option is now available to provide Alteon with the necessary access by creating an IAM role/policy that enables communication between Alteon VA and AWS and applying the role to both primary and secondary Alteon instances. **NFR ID:** 230608-000005

Cluster Manager Enhancements

During the creation of a new cluster, a more detailed BGP configuration is available, including enabling BFD. This requires Cyber Controller version 10.3.0.

NFR ID: 230706-000040

New GEL LLS Notifications

Starting with version 10.3.0.0, Cyber Controller can now send alerts in case one of the following issues occur in its GEL Local License Server (LLS):

- The LLS is not able to communicate with Flexera for more than the defined time.
Default: 12 hours
- The LLS database has grown more than the defined size.
Default: 1 GB

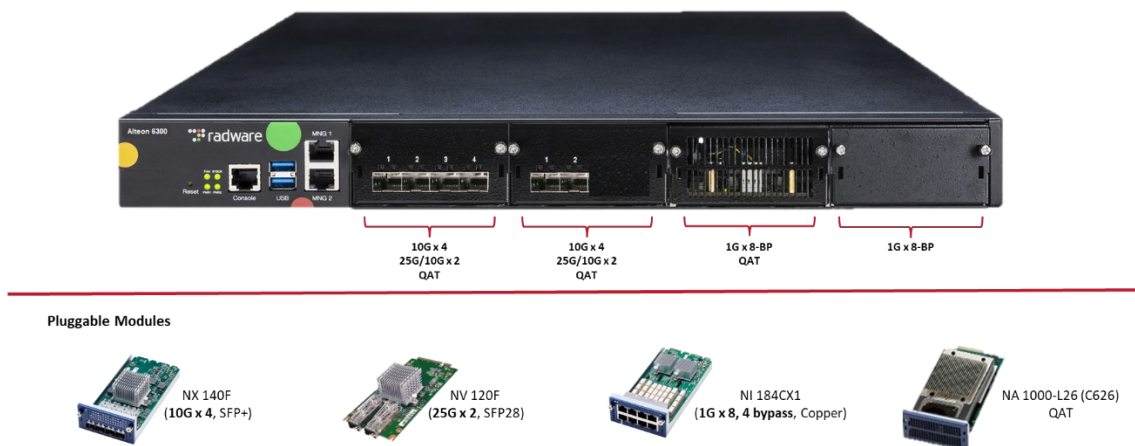
HTTP IP Header Configuration on Filter

In a SecurePath deployment on filters, starting with this version you can define the HTTP IP header for where the original client IP address is specified.

WHAT'S NEW IN 34.0.1.0

This section describes the new features and components introduced in this version on top of Alteon version 34.0.0.0.

New Alteon 6300 Platform



The Alteon 6300 platform is Radware's latest addition to the Alteon appliance family, a mid-range ADC with modular NIC and QAT cards. This cutting-edge platform represents a significant milestone as it introduces modularity to the existing Alteon lineup. Designed to meet the evolving needs of modern applications, the Alteon 6300 offers unmatched flexibility and scalability. With its modular architecture, it offers the following benefits:

- **Deployment** – Customers have the freedom to select and pay exclusively for the interface ports they require.
- **Flexibility** – Customers have the flexibility to interchange installed interface modules within and among different 6300 platforms.
- **Scalability** – Customers have the option to incorporate additional interface modules to accommodate their expansion needs.
- **Cost effective** – No need to pay for unused interface ports.

Known limitations:

- Only the SA option is released. ADC-VX mode is scheduled to be part of the next release

- There is no support for Jumbo frames
- There is no support for BGP FRR

Alteon VA Subscription Model

Radware announces the introduction of its Alteon Virtual Appliance (VA) through an annual subscription.

The new time based VA replaces the perpetual license. The perpetual VA license is removed from Radware price list.

This time-based VA offers customers with the following benefits:

- **Lower initial investment** – Lower entry barrier for users who may not have the resources for a substantial one-time payment.
- **Predictable budgeting** – Users know exactly how much they will be spending on a recurring basis, making it easier to manage cash flow and expenses.
- **Risk mitigation** – Subscriptions provide an opportunity to try out a product or service without committing to a long-term investment.
- **Cost flexibility** – Provides flexibility in managing costs, as users can adjust their subscription level or cancel if needed, rather than making a large upfront investment

Alteon Cluster Management for VMware Environment

The new Alteon Cluster Management capability, available in Radware Cyber Controller starting with version 10.0.2.0, allows for provisioning, management, and maintenance of Alteon auto-scaling clusters in the VMware environment.

An Alteon auto-scaling cluster is a group of Alteon VA instances that can dynamically adjust the number of active nodes based on the traffic load and performance requirements. It improves the availability and reliability of the ADC service by automatically distributing the requests among multiple nodes and avoiding single points of failure.

The Alteon auto-scaling cluster enhances the scalability and efficiency of the ADC service and allows handling the following type of scenarios:

- **Gradual growth** – An ADC cluster can start with a couple of Alteon devices that meet the initial traffic needs. As the application traffic increases, the scaling cluster handles it by automatically adding more Alteon instances to meet the requirement.
- **Planned or un-planned traffic surge** – When the ADC cluster is suddenly presented with a significant increase in traffic that exceeds the current cluster capacity, additional Alteon instances are temporarily provisioned to handle that increase. Once the traffic load goes back down, the additional instances are automatically decommissioned.

The ADC Cluster Management solution includes the following components:

- VMware cloud infrastructure
- BGP routers with ECMP support to distribute VIP traffic between Alteon instances in the same cluster

- Alteon VA versions 33.0.8.0, 33.5.4.0, 34.0.0.0 and later.

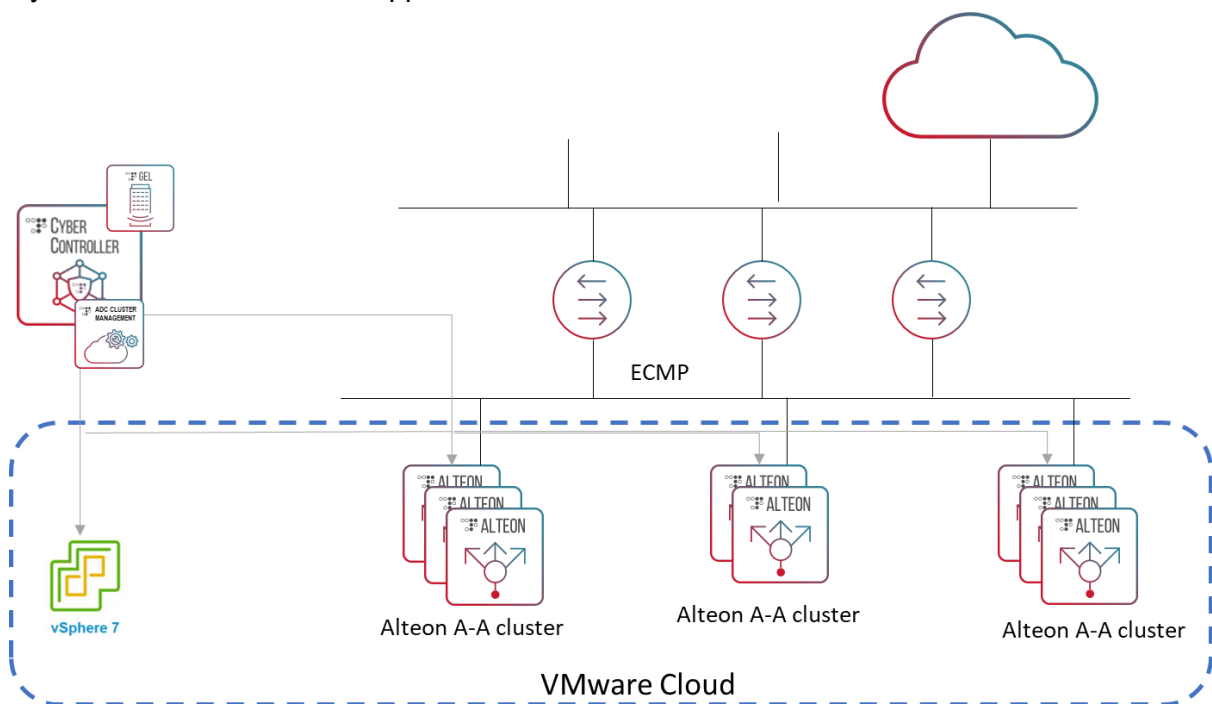
Cyber Controller version 10.0.2.0 and later. Cyber Controller performs the following functions:

- Cluster provisioning** – Provisions on the VMware cloud the Alteon instances required for the cluster
- Cluster scale out/in** – Monitors the resource utilization (CPU and throughput) on the cluster members and based on the thresholds specified by the user, triggers a scale out or scale in event.
- Deploying and updating ADC Services. All Alteon configurations, ADC service level and device level, must only be performed via Cyber Controller, to ensure that the configuration is identical on all cluster members.
- Provide full visibility for ADC Analytics, both system and application level.

For details on this capability please see Alteon Cluster Management User Guide.


Notes:

- WAF is not currently supported by this capability.
- Cyber Controller HA is not supported.



Alteon Support in Cyber Controller High-Availability

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



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

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

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

- From CLI: `/info/sys/cyberc`
- From WBM: *Configuration* perspective > **System** > **Cyber Controller**

NFR ID: 220503-000039

VXLAN Support

In addition to GRE and IP-in-IP, Alteon now supports VXLAN tunnels. The VXLAN support complies with RFC 7348.

Currently Alteon only supports VXLAN tunnels over IPv4.

To configure a VXLAN tunnel:

- From CLI: `/cfg/l3/tunnel /protocol`
- From WBM: *Configuration* perspective > **Network** > **Layer 3** > **Tunnels**

Low and Slow (Slowloris) Attack Protection for TLS

A variant of the Slowloris attack can send “slow SSL.” It sends the handshake data very slowly, one byte at a time, to keep the server waiting for more data, thus overwhelming and slowing down the target.

Alteon can now also protect itself and the application servers from a TLS-based Slowloris attack (protection against “slow HTTP headers” typed of attack was introduced in version 34.0.0.0).

To activate this protection, configure the new **TLS Handshake Timeout** parameter on the *SSL Policy* pane for the virtual services or filters you want to protect. If TLS handshake is not completed within the specified time, the session is closed. The recommended value is 2000 msec (milliseconds).

Statistics on the current number of TLS handshake timeouts per second and total number of timeouts are now available per virtual service, per filter and per device (SSL summary).

BGP ECMP Support on Load Balanced Traffic

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

Support for IPv6 Subnet Prefix of 64

Prior to this version, the maximum supported prefix length for an IPv6 subnet was 96. Now prefixes of length 64 are also supported for traffic matching subnets, and a prefix of 65 for IPv6 subnets in a network class. However, this prefix is only supported for traffic matching (such as source and destination in filters, or the source in virtual servers) and not for PIP/NAT.

NFR ID: 220513-000027

sysName LLDP Support

NFR ID: 221024-000120

Alteon now supports LLDP advertisement TLV Type 5 with the system name.

GEL Entitlement Description

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

NFR ID: 221024-000041

Integrated AppWall


GraphQL Protocol Support - BETA

We are excited to announce the support for **GraphQL protocol parsing**. GraphQL has gained significant popularity and adoption among clients due to its numerous benefits and advantages over traditional REST APIs.

GraphQL offers a **more efficient and flexible approach** to data fetching, allowing clients to precisely request the data they need in a single request. With its declarative nature, clients can specify the exact structure and shape of the response, reducing over-fetching and minimizing network overhead.

Furthermore, GraphQL enables clients to aggregate data from multiple sources into a unified response, **eliminating the need for multiple round trips to different endpoints**. This reduces latency and improves overall performance, providing a smoother user experience.

By adding GraphQL support to our product, we empower our clients to leverage these advantages and harness the full potential of GraphQL in their applications. With its growing popularity and developer community, GraphQL has become a **preferred choice for modern API development**.



In this release, we not only introduce GraphQL support but also reinforce our commitment to security. **Our enhanced protection for the positive security model ensures that customer GraphQL APIs are guarded against common security vulnerabilities, providing a secure and reliable foundation for applications.**

WHAT'S NEW IN 34.0.0.0

This section describes the new features and components introduced in this version on top of Alteon version 33.5.3.0.

GEL Support in Standalone Mode

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

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

NFR ID: 221222-000039

Alteon Kubernetes Connector Enhancements

The Alteon Kubernetes Connector (AKC) provides a solution for Alteon integration with Kubernetes/OpenShift orchestration.

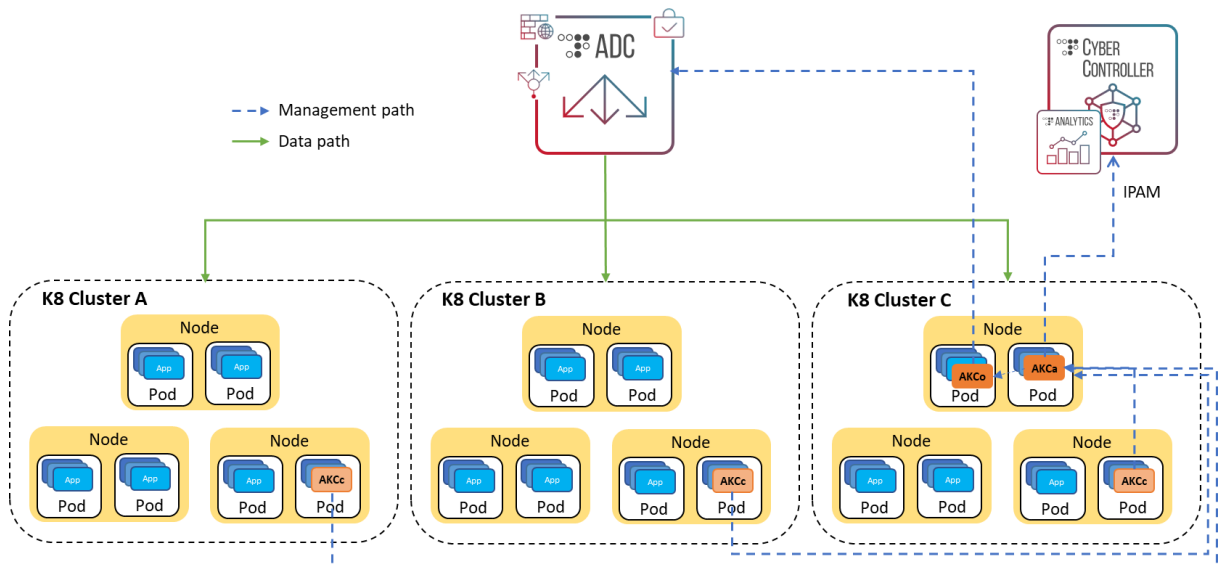
AKC runs inside the Kubernetes clusters, discovers services of type LoadBalancer and translates them to an Alteon ADC configuration. In addition, it monitors the cluster nodes and updates the Alteon configuration when nodes are removed or added to a cluster.

The AKC solution enables Alteon to load balance a service that is deployed in multiple Kubernetes clusters, using a single VIP.

The AKC has three components:

- The AKC Controller that monitors the service objects and nodes in the Kubernetes clusters. Such a component is required in each of the participating Kubernetes clusters.
- The AKC Aggregator that aggregates inputs from all the collectors and communicates the necessary configuration changes to the AKC Configurator. These components should be installed in only one of the clusters.
- The AKC Configurator that translates the changes to Alteon configuration file and pushes it to Alteon.

In addition, the solution uses the vDirect module in Cyber Controller/APSSolute Vision, which handles the IPAM service, required to allocate the service IP (VIP) from an IP pool (currently a single pool supported).



In this version, the AKC has added support for the following AlteoN capabilities for the services deployed in Kubernetes:

- **SSL offload.** To enable SSL offload, the following annotations can be used during service deployment to specify the SSL policy and certificate that should be used (these objects must be configured in AlteoN before the service is deployed).
 - `akc.radware.com/sslpol: <ssl policy id>`
 - `akc.radware.com/cert: <certificate id>`
- **The SecurePath connector** that allows providing application security (Cloud WAF, API protection, and BoTM) for the deployed service. The following annotations can be used during service deployment to specify the SecurePath and Sideband policies necessary to activate SecurePath for its traffic (these objects must be configured in AlteoN before the service is deployed).
 - `akc.radware.com/sideband: <sideband policy id>`
 - `akc.radware.com/secpath: <secpath policy id>`

Overload Protection for Integrated WAF

A new mechanism is now available to reduce the load on the WAF process in case of overload by bypassing WAF inspection for some of the transactions.

When the overload protection mechanism is enabled, it looks at the transactions sent within a 10-second sliding window, and when at least 1,000 transactions are received within such a window, the following occurs:

- If the WAF processing time of between 31% and 50% of the transactions within the window is higher than the user-specified threshold, Alteon will start sending to the WAF process only 50% of the transactions.
- If the WAF processing time of between 51% and 75% of the transactions within the window is higher than the user-specified threshold, Alteon will start sending to the WAF process only 10% of the transactions.
- If the WAF processing time of over 76% of the transactions within the window is higher than the user-specified threshold, Alteon will start sending to the WAF process only 1% of the transactions.
- Once 30% or less of the transactions within the window have a WAF processing time higher than the user-specified threshold, Alteon will go back to sending all the transactions to the WAF process.

To enable this mechanism, set the value of the **WAF Overload Threshold** parameter in the relevant virtual service or filter (by default it is disabled, meaning set to 0) as follows:

- From the CLI:
 - For a virtual service: `cfg/slb/virt <id>/service <port>/http/aw overload`
 - For a filter: `cfg/slb/filt <id>/aw overload`
- From the WBM
 - For a virtual service: Use the *New/Edit Virtual Service* pane > *Security* tab
 - For filter: *New/Edit Filter* page, *Security* tab

Note: Filters that have this mechanism enabled must be part of a Filter Set.

Slowloris Attack Protection

Slowloris is an application layer DDoS attack that uses partial HTTP requests to open connections between a single computer and a targeted Web server, and then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.

Alteon can now protect itself and the application servers from a slowloris attack.

To activate the protection, configure the new **HTTP Headers Timeout** parameter for the virtual services or filters you want to protect. If all headers are not received within the specified time, the session is closed. The recommended value is 4000 msec.

Notes:

- The Delayed Bind mode must be Force Proxy when the Slowloris protection is enabled.
- Filters that have this protection enabled must be part of a Filter Set.

Layer 7 Modification on HTTP/2 traffic

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

Notes:

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

NFR ID: 221123-000123

Out-of-the-box Certificate Pinned Sites List

Pinning is the process of associating a host with the expected X509 certificate or public key. This means the client (browser or app) knows which certificate to expect for a certain site, including who signed the certificate.

SSL inspection is not possible for a site with a pinned certificate, as the client will identify the signer of the certificate as not being the original signer, thus terminating the connection.

Traffic to these application domains should be configured for bypass in any SSL Inspection solution if the enterprise wants to allow such traffic for its employees.

To simplify this for customers, Radware provides an out-of-the-box list of known sites with pinned certificates. The following out-of-the-box elements have been added:

- Data class `bypass_hosts_list`, which includes the list of known sites with pinned certificates
- Content class `Cert_Pinning_Bypass_Sni` of type SSL with the `bypass_hosts_list` data class attached
- Content class `Cert_Pinning_Bypass_Hostnames` of type HTTP with the `bypass_hosts_list` data class attached

To bypass the pinned sites, you need to configure the bypass filter and select the relevant Content Class (SNI for Transparent Proxy mode or Hostnames for Explicit Proxy mode).

All these out-of-the-box objects are editable:

- If the data class was edited, it can be reverted to the default.
- After version upgrades, the list could be updated. In such cases, if the `bypass_hosts_list` data class was not edited it is automatically updated. If the data class was edited, it is not updated unless **Revert to Default** is performed.

NFR ID: 221011-000139

Sideband and SecurePath Updates in Unified Events

Unified events now include information related to Sideband and SecurePath (based on AppShape++ script `SIDEBAND::add_action` commands `send_response` and `terminate_session`):

- In SecurePath integration, if the request is identified as an attack and is responded to by Cloud WAF (without reaching the destination server), the event's *severity* is marked as "security" with *reason* "SecurePath Response"
- When generic sideband is used, if the request is responded to by the sideband server (without reaching the destination server), the event's *severity* is marked as "Normal" with *outcome* "Sideband Response"
- When the connection is terminated by the sideband, meaning that the client connection is closed by FIN/RST, the event's *severity* is marked as "Exception" with *outcome* "Failure" and *reason* "Connection Closed by Sideband".
- When there is a Sideband time out, meaning that the client connection is closed by FIN/RST, the event's *severity* is marked as "Exception" with *reason* "Sideband Failure".

GEL Dashboard Enhancements

The following GEL Dashboard enhancements are available starting with Cyber Controller version 10.1.1.0 for all supported Alteon versions:

- An instance's last validation time is now visible in the *Instances* table per the selected entitlement. By default, each instance validates its license with the license server every five (5) minutes.
- The validation status of the license allocated to the Alteon server is now available in the *Instances* table per selected entitlement. Values include:
 - Valid — The Alteon server has received revalidation from the LLS.
 - Revalidation Required — The Alteon license is still valid, but the Alteon server did not receive validation from the LLS for more than two (2) hours, half of the borrow period. If the Alteon server receives revalidation before the end of the four-hour borrow period, the status changes back to Valid.
- Sorting was added to the instance table per selected entitlement. By default, the table is sorted according to the validation status. The table can be sorted by each one of the columns in the table.

Control and Export of Management Port Packet Capture from WBM

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

NFR ID: 221102-000004

WHAT'S CHANGED IN 34.0.3.0

Reduce Default Traffic Event Sampling

The default sampling rate for traffic events has been decreased from 100% to 20% to mitigate its performance impact. In a production environment, it is advisable to start with this low rate and adjust it according to specific needs and performance considerations. Note that this modification applies solely to new traffic event policies and does not influence existing policies.

Further, beginning with this version, the sampling rate no longer affects Security events and EAAF events.

End to End time Enhancements

Request Transfer Time has been added to the End-to-End time breakdown to provide better latency visibility. Request Transfer Time is the time interval from when Alteon receives the first byte from the client until the time at which Alteon sends the last request byte to the server (not including sideband processing time). This time includes the AppWall request processing time, and the AppShape++ request side processing time.

Due to the addition of Request Transfer Time, the End-to-end time is now the sum of the Client RTT, Request Transfer time, Sideband Processing time, Server Response time (which is Server RTT + Application Response time), and Response Transfer time.

The new parameter is updated in the virtual service statistics CLI, WBM, virtual service counter-based JSON, as well as the unified event. Currently, the parameter is not updated at the Application dashboard in either APSolute Vision or Cyber Controller.

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

Startup Wizard Enhancement

The following enhancements were added to the startup wizard:

- Allow configuring the passphrase when the Config sync option is enabled
- When high availability is disabled, auto sync and sync persistent sessions automatically move to disabled.

FastView Feature Deprecation

As of this version, FastView functionality is no longer supported.

- When upgrading from a previous version with FastView enabled, the system will automatically disable FastView and all FastView related configuration will be removed.

- During configuration uploads, if FastView is enabled, the process will not fail. However, the FastView configuration will be ignored, and the remaining configuration will be applied as usual.
- All FastView related command-line interface (CLI) commands have been moved to a hidden state.
- Radware recommends releasing the resources (CUs) allocated to FastView considering this deprecation.

Exclusion of URL Categorization from Secure Subscription License

Starting with this version, the URL Categorization capability is excluded from the Secure Subscription license and is now accessible through the SecURL Gateway license.

Existing deployments utilizing URL Categorization with Secure Subscriptions will remain unaffected when upgrading to this version or any subsequent releases. These deployments can continue to utilize URL Categorization with Secure Subscriptions until their upcoming renewal without any disruption.

License Validation During Config Import

When uploading to Alteon a configuration file that includes enabled capabilities for which the corresponding license is not installed on Alteon, the configuration upload fails and remains in diff. Starting with this version, a clear error will also appear via the CLI and WBM listing the missing licenses to support the required configuration.

Integrated AppWall

HTML Decoding

- Support for decoding the HTML-encoded query parameter value in the HTTP request.

Vulnerability Partial Scan

- Support for partial inspection for each of the request zones: URL, Headers, Body, or Parameters. Each zone can be configured as fully scanned, partially scanned, or disabled for scanning.

GraphQL Protection

- Support for importing and exporting SDL files.

WHAT'S CHANGED IN 34.0.2.0

vRO Plugin Update

The vRO plugin was updated to support vRealize version 8.6.

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

Quick Application Wizard Enhancement

The following enhancements were done for the Quick Application Wizard:

- Added: Edit server port translation, HTTP2, WebSocket.
- Changed: Persistency is set to disabled by default; Client NAT is set to disabled by default.
- Removed: Application type 'IP', FastView checkbox,

After upgrade, the above changes will not affect applications that were created by the wizard in previous versions, but additional edits of these applications using the updated wizard will be applied to the applications.

GSLB Network Number Increase

The maximum number of GSLB networks was increased from 2048 to 4096 for VA, Standalone, and vADCs with 11 CUs or greater. For vADCs with less than 11 CUs, the maximum number of GSLB networks was increased from 1024 to 2048.

NFR ID: 230111-000065

Password Policy Enhancements

The following enhancements were added to the password policy:

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

Note: This rule does not include special characters.

NFR ID: 230224-000026

"wget" Package Update

The WGET library was upgraded to version 1.21.4.

NFR ID: 220808-000107

SecurePath Policies Number Increase

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

NFR ID: 230302-000167

Integrated AppWall

GraphQL Protection

- Support for Extension, Directive and Variable list.
- Support for requests located in the query parameters.
- Security inspection with Database filter, Vulnerabilities filter and Redirect Validation Host protection.

Custom Pattern

The customer pattern has been improved to support multiple conditions. We can now define different patterns located in different zones of the requests.

It provides a more accurate option to define Custom Pattern and reduce false positives.

Limit Number of Headers to Parse

In the Tunnel Properties, we can limit the maximum number of headers to be parsed.

Base64 Decoding

The Base64 heuristic detection can decode payload with suffix.

Redirect Validation Host Protection

In the Defense Properties, the configuration of the Redirect Validation Host protection is exposed. The signatures used for LFI, RFI, SSRF and their delimiters can be edited.

WHAT'S CHANGED IN 34.0.1.0

Network HSM (Thales/Gemalto) Enhancements

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

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

BWM Shaping

The BWM shaping capability is no longer supported and has been hidden from the CLI and WBM. If the capability is configured already on a device before upgrading to this version, it will continue to work as configured after upgrade.

UDP Virtual Service Down Response

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

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

Updated Option to Enable/Disable Weak Algorithms in SSH

The command that enables the SSH weak MAC algorithm is now updated to also enable the weak KEX algorithm and the weak Server host key algorithm.

The CLI command was renamed from `/cfg/sys/access/sshd/weakmac` to `/cfg/sys/access/sshd/weakalg`

By default, the value is enabled (to support backward compatibility).

Disabling weak algorithms excludes the following weak SSH algorithms:

- KEX “algorithms diffie-hellman-group-exchange-sha1”, “diffie-hellman-group14-sha1”,
- server host key algorithm “ssh-rsa” and MAC algorithm “hmac-sha1”.

Alteon Embedded Dashboard Removal

Starting with this version, the Alteon embedded dashboard is no longer available from WBM. For enhanced analytics, which include historical data and reporting, Radware recommends using the ADC analytics capability available via APSolute Vision or Cyber Controller.

Advanced Virtual Wire Health Check Enhancements

The advanced virtual wire health check now works in conjunction with port trunks (Static and LACP).

Change in AppWall SNMP Trap OID

The SNMP trap OID for the integrated AppWall server status was wrong and is now fixed:

- appwallUpTrap (AppWall server is up) OID is now .1.3.6.1.4.1.1872.2.5.7.0.166
- appwallDownTrap (AppWall server is down) OID is now .1.3.6.1.4.1.1872.2.5.7.0.167

Integrated AppWall

Multiple Improvements

- **Automatic Disable for Auto Discovery and Auto Policy:** A timer was added to disable Auto Discovery and Auto Policy after 30 days.
- More security coverage in the **Directory Listing** host protection.
- Support for **Tor Exit Nodes** in the GEO updates subscription (Anonymous Proxy renamed).
- **SSRF Security Event** name change.
- Increase **default configuration value for Fast Upload**.
- **Redirect Validation default configuration change**.
- **Default Security filters in a new Virtual Directory:** Database filter, Vulnerabilities filter and HTTPMethod are proposed by default.
- **Base64 support:** Option for “Heuristic Detection” and “Force scan of original value” has been removed from AppWall management Console (available in the Configuration file and REST Management APIs).

WHAT’S CHANGED IN 34.0.0.0

UDP Stateless and TCP Services on the Same VIP

You can now configure both a TCP service and an UDP stateless service on the same VIP and port.

NFR ID: 220520-000151

Integrated WAF SUS and GEO DB Update Via Proxy

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

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

The management interface is defined by default.

NFR ID: 220601-000032

Combined Image Upload Option Removed from WBM

The Alteon combined image is utilized to install both ADC-VX and vADC instances for Alteon platforms in a single step. However, the option to upload a combined image has been removed from the WBM in this version and is only supported via the CLI. If you want to upload an image via WBM, you must upload the ADC-VX and vADC images separately.

Service and Real PPS Collection Interval

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

OpenSSL Upgrade

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

Note: Not relevant for FIPS II models.

Integrated AppWall

API Security

In this version multiple enhancements are provided for API Security protection:

- **Support for Preflight request (CORS mechanism):** Usually the preflight requests are automatically sent by browsers. This consists of sending automatic requests with the HTTP method `OPTION` and the header "Access-Control-Request-Method". If the method `OPTION` is not defined in the OpenAPI file description, the requests are blocked by the API protection. Support of preflight request will now accept these client requests coming from the browser.
 - **Case insensitivity during the API Catalog endpoints inspection.** By default, the inspection is case sensitive. It can be deactivated to be case insensitive.
 - **Circular reference:** OpenAPI files that include circular references are now supported.
 - The **Forensics Security Events** present more detailed descriptions related to the nested parameters, for example into a JSON body.
 - When a Security violation occurs, AppWall propose a more accurate and **advanced refinements option** that will improve the False Positive management.
 - The **AppWall Techdata** has been updated to include the OpenAPI files that have been previously uploaded.

Custom Pattern per Application Path

Custom Patterns help to define a personal signature. Custom Patterns can now be defined per Application Path, not only globally.

Server-Side Request Forgery

The Unvalidated Redirect protection is improved in terms of performance and security coverage.

Multiple IPs Included in XFF HTTP Header

In version 7.6.18.0, AppWall allowed globally configuring how to read XFF HTTP headers when they contain multiple IPs. From this version, this can be configured per AppWall Tunnel (referred to as SECWA in the Alteon WAF).

Global Security Event Suppression

AppWall provides mechanisms to protect from a Security Events flood:

- Automatic Event suppression configured manually per Security Event.
- Automatic Event suppression configured dynamically per Security Event.

In this version, AppWall provides an additional mechanism:

- Automatic Event suppression configured dynamically per multiple Security Events.

Database Security Filter

Database Filter inspection can be excluded for Query/Body Parameter names. The configuration is available globally or per Application Path.

Multiple Enhancements on AppWall REST API for DevOps

Multiple new AppWall REST APIs have been delivered.

For details, please consult the on-line product documentation.

MAINTENANCE FIXES

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

Fixed in 34.0.3.0

General Bug Fixes

Item	Description	Bug ID
1.	Changing the vADC management address caused the ADC-VX management address to be removed in ifconfig.	AL-139804
2.	When rebooting a vADC, the vADC was not accessible for approximately five (5) minutes, even though it appeared as UP on the ADC-VX.	AL-140616
3.	The backup WAN link server did not come online while processing a DNS query.	AL-140651
4.	On DPDK platforms, the MNG port bonding mode was incorrect. It was set to round-robin instead of active-backup.	AL-140819

Item	Description	Bug ID
5.	When a fragmented packet matched a filter with "reverse enabled" , the device rebooted.	AL-140967
6.	After a failover, there was a 30 second to one minute delay before all eight IPv4 BGP prefixes were sent out to the neighbors.	AL-140983
7.	The group backup server status was DOWN when queried via SNMP.	AL-140985 AL-140988
8.	The Mexico time zone switched to DST (daylight savings time) before the actual Mexico DST (April to October). After upgrade, the Mexico time zone did not switch to DST.	AL-141057
9.	The Secured Web Applications view for a user with the user role "Web AppSecurity Owner" hung with a "Loading..." message.	AL-141128
10.	When an aggregate route was redistributed from one peer to another, the original AS number was added as AS_SEt segment in the AS_PATH attribute. In the code, there were some issues in parsing the AS_PATH segments when there were two or more segments.	AL-141134
11.	With two gateways configured with same IP address, the route table created two entries whenever the gateway flapped, resulting in filling up the route table, which in turn led to device reboot when Alteon failed to add a route for the gateway.	AL-141149
12.	When clsaging "both" and clfstage "both" are enabled, a memory leak occurred which eventually led to the health checks failing.	AL-141158
13.	Was not able to connect to Alteon via SSH in rare scenarios because the maximum number of sessions exceeded.	AL-141163
14.	There was an error in JSON Fancy Names.	AL-141198 AL-141201
15.	Persistent session mirroring did not properly mirror the group names to the backup device when the group names had the same first character.	AL-141216
16.	After the DNS cache timer expired, Alteon did not query for the FQDN origin if the answer was a CNAME.	AL-141236
17.	A real server health check failed even when there was response to the health check packets.	AL-141250
18.	There was a problem with config sync of a TrustedCA certificate.	AL-141310

Item	Description	Bug ID
19.	When rebooting a vADC, the vADC was not accessible for approximately five (5) minutes, even though it appeared as UP on the ADC-VX.	AL-141325
20.	After disabling and enabling a BGP peer, the vADC rebooted.	AL-141350
21.	An Alteon 5208XL platform rebooted with a software safe restart.	AL-141422
22.	After upgrading from version 32.4.x to 32.6.x, the user was forced to reduce the session capacity number.	AL-141463
23.	After running /boot/rsrscs/cur, an increased disk size was not reflected.	AL-141472
24.	On a 5424 platform with 16/24GB RAM, setting the MTU was blocked.	AL-141479
25.	Services went down after revert apply failed.	AL-141581 AL-141583
26.	Added a debug command and debug logs for helping to debug an SP panic involving a filter configuration.	AL-141612
27.	vADC2 and vADC3 auto-rebooted due to a software safe restart	AL-141632
28.	When FastUpload was activated, files larger than the threshold (which therefore were not inspected) failed to upload.	AL-141633
29.	After upgrading to version 33.0.9.50, SP1 has high CPU utilization on vADC4.	AL-141703
30.	The overload status was activated when at least one LOGEXP health check operand detected an overload.	AL-141755
31.	Alteon 6300 shows Websec up/down logs even if was not using AppWall.	AL-141817 AL-141830
32.	A compression limit above 10000 MB was not correctly pushed to a vADC.	AL-141856 AL-141881
33.	In some edge cases, the watcher process had an invalid process ID 0. The fix is not to try to recover process ID 0.	AL-141937
34.	A BGP flap occurred due to a non-reachable IP address used in getlog.	AL-141865
35.	After analyzing a customer-reported reboot, added a protection code to prevent access to released memory.	AL-142167
36.	The MP crashed upon apply when <real/group/virtual server> used a new health check object ID with the same content and with the same index.	AL-142246

Item	Description	Bug ID
37.	Many panics or core dumps were generated.	AL-142306
38.	There was an incorrect session count with the pbind cookie.	AL-142313

AppWall Bug Fixes

Item	Description	Bug ID
1.	Corrupted Configuration File Detected message displayed.	AW-50153
2.	Failed upload of Open API file on Radware Cloud.	AW-50162
3.	AppWall crashed during production and Web portals were down.	AW-50190
4.	Request to remove uncheckable checkbox from WAF GUI.	AW-50061
5.	Integrated AppWall WebSocket frame size value issue.	AW-50078
6.	Help to investigate Alteon integrated AppWall crash.	AW-50116
7.	AppWall crashed due to configuration corruption.	AW-50119
8.	AppWall fixed content length was injected to the response body and not as a header.	AW-50131
9.	AppWall GUI is showed connection error and the error message "Cannot connect to management server".	AW-50132
10.	Attacks were not blocked by AppWall.	AW-50168
11.	File Upload issue - Possible AppWall issue on version 7.6.21.10.	AW-50184
12.	Integrated WAF security events were not being retained.	AW-50192
13.	Web service was not working when Tunnel is in Passive mode.	AW-50224

Fixed in 34.0.2.10

AppWall Bug Fixes

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

Fixed in 34.0.2.0

General Bug Fixes

Item	Description	Bug ID
1.	There was an issue with a DPDK instance in Azure.	AL-49525 AL-50573

Item	Description	Bug ID
2.	A VIP was unreachable after migration from an Alteon 6K platform to a 7K platform.	AL-50582
3.	A vADC MP reached 100% CPU utilization.	AL-54939
4.	Upgrading from version 32.6.8 to version 32.6.12 to avoid a memory leak resulted in a further degradation.	AL-138921
5.	Problems occurred with an SSL certificate with a Subject Alternative Name with more than 1024 characters.	AL-139069
6.	Using APSolute Vision, there was a back-end SSL handshake failure exception.	AL-139140 AL-139178
7.	There was cyclic reboot of vADC1 on version 33.0.7.50 when data ports were up.	AL-139201
8.	A virtual service froze after an apply operation .	AL-139209
9.	vADC4 rebooted cyclically after Alteon ADC-VX upgraded to version 33.0.7.50.	AL-139214 AL-139217
10.	An IPv6 remote real health check failed via a DSSP health check.	AL-139255
11.	WBM was not available after the mmgmt certificate was updated .	AL-139282
12.	A failed real server mistakenly displayed the current sessions counts.	AL-139379
13.	There was an issue with a non-configured peer.	AL-139422
14.	The IPv6 Network filter for an unspecified address (::/128) overlapped with an IPv4 network filter.	AL-139451
15.	There was an issue session capacity and session mirroring .	AL-139481
16.	There was an unexpected reboot of an ADC-VX device.	AL-139494
17.	When syncing from backup to master, virtual services were deleted on the master, affecting the service.	AL-139502 AL-139508
18.	The device rebooted.	AL-139518
19.	A standby Alteon advertised BGP routes when any BGP related configuration changes were made, and the “advertise BGP on HA backup peer” option was disabled.	AL-139548
20.	On an Alteon D-6024S platform, the RX and TX PPS statistics value seemed stuck in the prefmon file.	AL-139591
21.	vADC-2 was restarting on both ADC-VX instances in a High Availability environment.	AL-139631

Item	Description	Bug ID
22.	Sessions through transparent SSLi failed when sending traffic to a VRRP MAC.	AL-139642
23.	The Alteon embedded dashboard was visible even though is no longer should be available.	AL-139651
24.	Alteon TRP MIB file (CHEETAH-TRAP-MIB.mib) was missing a definition for session table threshold traps.	AL-139666
25.	An IP address deleted in Smart NAT was not released.	AL-139872
26.	The /info/vADC command output incorrect throughput for the vADC.	AL-139890
27.	Traffic graphs on the dashboard were not updated during a performance test.	AL-139914
28.	There was an issue with vADC High Availability if a high number of CUs are assigned.	AL-139973
29.	A real server in shutdown mode that was in a network rule could not be synced to a peer.	AL-140027
30.	For IP ACLs enabled at the Alteon level, when applying changes to AppWall, the sync process from the device where the AppWall change was applied adds/removes IP addresses not configured manually on the destination device for the sync process.	AL-140055
31.	Could not download tech data.	AL-140108
32.	The /oper/slb/group/shut (connection shutdown) did not work correctly.	AL-140185
33.	Issue using AppShape++ to add a PIP if the client IP address was in the same subnet as the server.	AL-140231
34.	After upgrading from version 33.5.4.0 to version 33.5.5.1, the NAT health check configuration was missing.	AL-140264
35.	Application Service Engine Out-of-sync issue	AL-140273
36.	When connecting to a Alteon 5424 platform with a specific server name, after disabling then enabling a port, the device did not come up again.	AL-140283
37.	In Integrated AppWall, could not set traffic routing for the DefensePro Signaling Server.	AL-140287
38.	After running automation with an API call that failed, accessing the WBM on Alteon VA produced a 50X error.	AL-140415
39.	FRR BGPv6 session not established over the default gateway	AL-140551

Item	Description	Bug ID
40.	Inconsistent restart information between ADC-VX and vADC in TechData.	AL-140566
41.	The RST packets originated after an inactivity timeout from the proxy were sent with wrong source MAC instead of the proxymac.	AL-140575

AppWall Bug Fixes

Item	Description	Bug ID
1.	Latency on masked responses.	AW-49841
2.	Standalone AppWall VA crashed (version 7.6.20.0)	AW-49833
3.	AppWall Security event showed wrong destination port.	AW-49938
4.	AppWall crashed when it is inline.	AW-49871

Fixed in 34.0.1.0

General Bug Fixes

Item	Description	Bug ID
1.	On an ADC VA, an SP1 freeze for slb_pbt_age_entries occasionally caused the device to reboot.	AL-49410
2.	There were DNS errors in the Alteon MP logs.dns due to DNS resolution not being case-insensitive.	AL-49475 AL-49476 AL-49477
3.	The Websec module fluctuated between down and up.	AL-49482
4.	The APP response was not calculated correctly when there were matches to the content class	AL-49486
5.	DNS Vulnerability CVE-2004-0789 was fixed.	AL-49498
6.	The FQDN real indexes changed during get config.	AL-49506
7.	After upgrading to version 33.0.x, the Apply time increased from 12 to 18 seconds.	AL-49510
8.	When the capture -M command was run on very large secrets files, the disk became full. Now the secrets file size is limited during capture -M execution.	AL-49521
9.	Alteon SSH failed a security audit.	AL-51831
10.	The CDP group table became empty when deleting one entry case.	AL-51872

Item	Description	Bug ID
11.	The static NAT for GRE traffic in point-to-point was incorrect.	AL-51876
12.	The VLAN 2090 error was assigned to more than 32 PIPs.	AL-51885
13.	The /oper/slb/sessdel command did not work for ESP sessions.	AL-51889
14.	There was a corruption in the NAT rule configuration.	AL-51898
15.	The LinkProof Smart NAT ID disappeared.	AL-51908
16.	Updated the REST API Guide to explain how to retrieve the high availability state via REST API when in VRRP mode.	AL-51914
17.	On a KVM VA, health checks to AppWall and nodejs failed in single IP mode.	AL-52635
18.	The appwallUp appwallDown traps were sent with the wrong OIDs.	AL-52638
19.	In the Ansible SSL policy configuration, added the option "none" to fe_intermediate_ca_chain_type.	AL-52647
20.	The /info/sys/log command issues an error when the ramdisk is full. This was due to an issue with the FRR log rotation logic.	AL-53589
21.	Implemented a new CLI command "/c/slb/virt x/service 53 dns/undirect ena dis" to bypass BWM processing in the response path for the DNS UDP stateless service.	AL-53598
22.	Hid the internal address from the BE session table.	AL-53607
23.	On a vADC, enabling LACP caused the device to reboot.	AL-53612
24.	Back-end SSL with client authentication using static RSA caused a "bad" MAC address..	AL-54021 AL-54022 AL-54024
25.	Alteon failed to support the OID for Temperature sensor 3 and Temperature sensor 4.	AL-54702
26.	Using WBM, when dbind was set to enabled, when changing SSL-related configurations (as such the SSL policy), the dbind setting was changed to forceproxy.	AL-54715
27.	On a vADC, the perf_rec_2.tmp.old file utilized all of the disk space.	AL-54722
28.	In an SLB with pbind environment, when a service was configured with AppShape++ and alwayson, upon receiving the traffic the device rebooted.	AL-54728
29.	There was a discrepancy in the output hard disk between the CLI and WBM.	AL-54738

Item	Description	Bug ID
30.	In an ADC-VX environment, when VLAN sharing was enabled on a 5424 platform, traffic destined to the vADC was dropped.	AL-54744
31.	With virt sync disabled and a virtual service configured with a content rule, during configuration sync, devices being synced lost the content rule association with the virtual service.	AL-54751
32.	A vADC rebooted because of a software safe restart.	AL-54760
33.	In WBM, the password strength (pwscrit) menu was not included.	AL-54764
34.	On an Alteon VA, even though the disk space was increased, logs were issued regarding the storage capacity.	AL-54775
35.	The SSL inspection advanced virtual wire check was down when the IDS ports belonged to trunks.	AL-54915 AL-54917
36.	When a syslog message sent from Alteon did not use LF as delimiters, the vDirect traffic event was not triggered .	AL-54922
37.	The health check run-time instance was shared unexpectedly when several cntrules with different groups were defined under the same virtual service.	AL-54929 AL-54931
38.	Logs were added in relevant places that failed during key/certificate modification.	AL-55158 AL-55165
39.	Alteon sent incorrect parameters to the customer-hosted CAPTCHA/Block page.	AL-55167 AL-55173
40.	Did not receive the complete URL in the data received post.	AL-130949
41.	When sending an FQDN update, the SSL-related configuration that was sent was still in progress and caused a configuration issue.	AL-138539
42.	Unexpected reboot	AL-138556
43.	Both Alteon devices panic at the same time, multiple times	AL-138694
44.	Alteon sent a duplicate response for each ICMPv6 request sent to the device's interface IP address.	AL-138757

AppWall Bug Fixes

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

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

Fixed in 34.0.0.0

General Bug Fixes

Item	Description	Bug ID
1.	On a 6024 SL platform, as unable to give the response to a TCP-SYN message.	DE76488
2.	RSTP was not working properly	DE78382
3.	Could not configure filtpbcp in hot-standby mode. Modified the CLI validation to resolve the issue.	DE78555
4.	Interface 256 could not be selected for switch HA advertisements.	DE78894
5.	Using WBM, an update to the cipher list was greater than 256 characters and was not accepted.	DE78975 DE78982
6.	The Unit label for a rule level timeout was different between WBM and the CLI.	DE79014

Item	Description	Bug ID
7.	On DPDK virtual platforms, traffic passing thorough BWM shaping contracts caused invalid buffer access and caused the vADC to reboot.	DE79049
8.	There was high SP memory utilization during a low traffic period.	DE79060
9.	Getting the vADC partition size failed and caused the vADC to hang on restart.	DE79122
10.	After running /stats/slb/pip, the SNMP OID was missing from the output.	DE79222
11.	VPN connectivity failed because of the IKE and the ESP sessions being bound to different servers.	DE79231
12.	Could not enter the hyphen (-) character in the New Host to Replace field on the Application Delivery > Virtual Services >Virtual Services of Selected Virtual Server > HTTP Content Modifications >HTTP Rules >URL Match & URL Action pane.	DE79234
13.	The Root Bridge was not properly declared in MSTP.	DE79245
14.	Using WBM, the hard disk capacity displayed incorrectly because secondary disk size was not counted.	DE79254
15.	SNMP walk failed because the OID did not increase.	DE79433
16.	A vADC did not handle traffic when it became the master.	DE79515
17.	An AppShape++ script trying to insert a script greater than 50k characters into the cmdLogMP-1-1 file caused the device to reboot.	DE79544
18.	If PIP processing or session mirroring is enabled if the Alteon device is identified as the backup device with server processing disabled, the frame received from the server needs to be forwarded.	DE79607
19.	System analytics were sent with null data.	DE79612 DE79619
20.	There was an issue with FQDN and multiport applications because there was no server name for the FQDN ephemeral real server in the XML sent to AppXcel.	DE79729
21.	When setting the time zone by name and not changing the default NTP time zone, a warning is issued after the Apply.	DE79793 DE79800
22.	When clsaging both is enabled with tunnels, the device rebooted.	DE79831
23.	The application services engine was not synchronized with the current configuration and the change was not saved.	DE79844

Item	Description	Bug ID
24.	In an SLB and PIP environment, there was a discrepancy in the PIP statistics between /st/slb/pip and /st/slb/aux.	DE80128
25.	SANs fields greater than 1024 bytes were accepted while generating a CSR.	DE80145
26.	The traceroute response packet was sent by Alteon with the wrong interface.	DE80192
27.	After upgrading from version 30.5.3.0 to 32.4.6.0, VLANs displayed as Down.	DE80314
28.	After downloading and uploading a configuration via REST API, SlbNewCfgFQDNServerTable was empty.	DE80348
29.	An SSLi issue caused the device to reboot.	DE80415 DE80420
30.	An incorrect GSLB DNS query refused a response for non-existing domains.	DE80453
31.	Unexpected BFD behavior.	DE80466
32.	Logging the times command caused the device to reboot.	DE80605
33.	There was an AppShape++ namespace conflict when using rule lds that end with digits.	DE80629
34.	SNMP trap 193 is returned for a disk space issue when it was not included in its MIB.	DE80689
35.	The Secured Web Applications (secwa) pane did not display on a standalone device.	DE80695
36.	On an ADC-VX, the MP caused a reboot.	DE80820
37.	From the CLI, could not connect to real server via Telnet.	DE81212
38.	Using WBM, could not change the protocol TCP/UDP for port 389.	DE81263
39.	The real server health checks treatment was delayed when an unavailable rlogging server was configured.	DE81271
40.	The label in the output regarding MP memory for the /i/sys/capacity command was not clear. Changed the label from "mp memory" to "total device memory".	DE81369
41.	The last digit of the year was missing in the output for some OIDs because arrayLength-1 was assigned with a Null character.	DE81378
42.	A RADIUS UDP health check was sent for RADIUS AA instead of the expected TCP health check when a non-standard destination port was defined.	DE81519

Item	Description	Bug ID
43.	When there is a shared resource (file) that is being accessed by two different operations (for example, putcfg and snmp), there was a bug in the state machine that is responsible for the synchronization, causing the device to reboot.	DE81560
44.	There were DNS errors in the Alteon MP logs.dns due to DNS resolution not being case-insensitive.	DE81599
45.	Back-end SSL with client authentication using static RSA caused a bad MAC address.	DE81675

AppWall Bug Fixes

Item	Description	Bug ID
1.	Cannot change the tunnel operational mode to Passive.	DE78282
2.	Sensitive Parameters are not getting masked in Security Details but are getting masked in Raw Request Data.	DE78706
3.	AppWall GUI gets stuck and affects the Alteon GUI as well in versions 32.4.13 and 33.5.3 and 33.0.6.5.	DE79700
4.	Error in the GUI when accessing Vulnerabilities.	DE79955
5.	File Upload security filter is detecting false-positive.	DE80620
6.	AppWall is trimming requests payload based on Content-Length header value.	DE81172
7.	AppWall does not send complete hostname in the security syslog message.	DE81249


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/1036876

RELATED DOCUMENTATION

The following documentation is related to this version:

- *Alteon Installation and Maintenance Guide*
- *Alteon VA Installation and Maintenance Guide*
- *Alteon Getting Started Guide*
- *Alteon Web Based Management Application Guide*
- *Alteon Command Line Interface Application Guide*

- 
- *Alteon Command Reference*
 - *Alteon REST API User Guide*
 - *Alteon AppShape++ SDK Guide*
 - *AppWall for Alteon NG User Guide*
 - *LinkProof for Alteon NG User Guide*
 - *LinkProof NG User Guide*

For the latest Alteon product documentation, as well as previous and retired versions, refer to:

<https://portals.radware.com/Customer/Home/Downloads/Application-Delivery-Load-Balancing/?Product=Alteon>

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

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

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