

**ACOS 7.0.3**

# **New Features and Enhancements**

May, 2026



© 2026 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

## PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

[a10-virtual-patent-marking](#).

## TRADEMARKS

A10 Networks, Inc. trademarks are listed at: [a10-trademarks](#)

## CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc.. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

## DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

## ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

## FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting [www.a10networks.com](http://www.a10networks.com).

# Table of Contents

<b>Enhancements in ACOS 7.0.3</b> .....	<b>5</b>
AI Firewall .....	5
Introducing AI Firewall .....	5
Application Delivery Controller .....	8
IPAM Integration with Sideband Support .....	8
DNS Cache Memory Optimization .....	10
Increased FQDN Length Support .....	10
Enhanced URL Switching Failure Handling .....	11
Dynamic Selection of Non-HTTP and Non-SSL Traffic Paths .....	12
Hybrid KEM Support for TLS 1.3 .....	14
Enhanced RADIUS Health Monitoring .....	15
Carrier Grade NAT .....	17
Hardware-Accelerated DDoS Protection on Non-SPE FTA Platforms .....	17
Firewall Configuration .....	18
Support for ICMP Traffic without a Matching Session .....	19
GUI Enhancements .....	20
GSLB Group Status Tab in GUI .....	20
Platforms .....	21
Thunder Container OpenShift Support .....	21
Disabled Second Management Interface (management2) on Thunder 8665 Platform .....	21
RHEL 9.6 Support for A10 Thunder MVP .....	22
Enhanced Capacity FlexPool License Support for Hardware Appliances .....	22
Introduced New AI Platforms .....	24
Introduced Thunder 3360S Platform .....	24
Introduced Thunder 3765 Platform .....	25
SSL Insight .....	25
Dynamic Steering of Certificate Fetch Operations .....	26
Clear-Text Traffic Replication .....	27

---

Security Updates .....	29
Threat Protection System .....	29
<b>Enhancements in ACOS 7.0.2 .....</b>	<b>30</b>
Application Access Management .....	30
Enhanced Kerberos Encryption with AES128 and AES256 Encryption Algorithms .....	31
aXAPI .....	31
Support Batch Operations .....	32
Carrier Grade NAT .....	32
Hardware-Accelerated DDoS Protection on Non-FTA Platforms .....	32
Platforms .....	33
Introduced Thunder 7465 Platform .....	34
Enhanced Thunder 7460S and 7460S-MAX Platforms .....	34
Ngen Low Latency License for Thunder 1060S .....	35
vThunder Enhancements .....	36
System and Security .....	36
Enhancements to SSH Control-Plane Security .....	37
Enhancements to System Security .....	38
Enhancement to Device Configuration Encryption .....	39
Disk Encryption Support .....	41
Password Configuration Methods for Admin Accounts .....	42
Introduced Configuration Synchronization Between A10 Control and ACOS .....	42
Enhanced axdebug File Size .....	43
SSL Insight .....	44
Enhanced QAT SSL Memory Allocation .....	44
<b>Enhancements in ACOS 7.0.1 .....</b>	<b>46</b>
RHEL Platform Support .....	46
Key Requirements and Support .....	47
New Platform Introduced .....	49
Enhanced ACOS GUI with TPS Integration .....	49

## Enhancements in ACOS 7.0.3

---

This topic provides a brief overview of the new features and enhancements added in the ACOS 7.0.3 release:

For new features and enhancements prior to ACOS 7.x release, see the recent prior ACOS [New Features and Enhancements](#).

The following topic is covered:

<a href="#">AI Firewall</a> .....	5
<a href="#">Application Delivery Controller</a> .....	8
<a href="#">Carrier Grade NAT</a> .....	17
<a href="#">Firewall Configuration</a> .....	18
<a href="#">GUI Enhancements</a> .....	20
<a href="#">Platforms</a> .....	21
<a href="#">SSL Insight</a> .....	25
<a href="#">Security Updates</a> .....	29
<a href="#">Threat Protection System</a> .....	29

## AI Firewall

ACOS 7.0.3 introduces the following new features and enhancements for AI Firewall:

The following topic is covered:

<a href="#">Introducing AI Firewall</a> .....	5
---	---

## Introducing AI Firewall

---

Traditional security controls for AI and Large Language Model (LLM) based applications have primarily operated outside the application delivery path or relied on application-level enforcement. To address the growing threat landscape specific to AI workloads,

A10 Networks introduces AI Firewall, an intelligent content-inspection layer with a centralized AI-traffic governance solution.

AI Firewall performs inline inspection of user prompts and LLM responses, applying security, compliance, and governance policies in real time. It protects AI-enabled applications against prompt injection attacks, jailbreak attempts, sensitive data leakage, and policy violations.

### **Key Features**

The AI Firewall offers the following key features:

- Inline inspection of AI prompts and LLM responses.
- Detection of prompt injection, jailbreaks, policy violations, and data leakage.
- Centralized policy and guardrail management.
- Monitor and Reasoning modes for visibility and policy enforcement.
- User and user-group based guardrail assignment.
- Detailed logging and analytics with advanced filtering.

### **Supported Platforms**

AI Firewall is currently supported only on the following AI-optimized hardware platforms:

- Thunder 1068
- Thunder 7468

These high performance AI platforms, equipped with GPUs, are introduced to address the AI security and networking threats.

### **License Requirement**

The AI firewall feature is a built-in capability available with the ADC or CFW license and can be enabled during license acquisition through the Global License Manager (GLM) portal.

### **CLI Configuration**

The following key command is used to configure AI Firewall.

1. To enable or disable the AI Firewall globally, or to purge the database logs displayed in the AI Firewall GUI dashboard, use the following command:  

```
ACOS(config)# ai firewall {clear-log | disable | enable}
```
2. To enable monitor mode in the AI Firewall for ICAP request and response traffic, configure `aifw-monitor-mode` under the `slb template reqmod-icap` and `slb template respmod-icap`, respectively.
3. To enable reasoning mode in the AI Firewall for ICAP request and response traffic, configure `aifw-reasoning-mode` under the `slb template reqmod-icap` and `slb template respmod-icap`, respectively.

### Show Commands

1. To view the AI Firewall status, use the following command:  

```
ACOS# show ai firewall status
```
2. To view AI engine information, including hardware status, driver version, and GPU details, use the following command:  

```
ACOS# show system ai engine
```
3. To view AI-traffic statistics, including request and response counts, violations, and license usage metrics, use the following command:  

```
ACOS# show ai firewall statistics
```
4. To view the system hardware and the GPU information, use the following command:  

```
ACOS# show hardware
```

### GUI Configuration

To access the AI Firewall GUI, follow these steps:

1. Launch the AI Firewall GUI through the following URL:  

```
https://<thunder-device_ip_address>/gui/aifw/
```
2. In the AI Firewall GUI, you can:
  - Create and manage policies.
  - Configure guardrails.
  - Map guardrails to users and groups.
  - Monitor AI-traffic through logs and analytics.

---

## See Also:

- [AI Firewall User Guide](#)
- [Command Line Interface Reference](#)
- [Global License Manager User Guide](#)
- [Introduced New AI Platforms](#)

## Application Delivery Controller

ACOS 7.0.3 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

<a href="#">IPAM Integration with Sideband Support</a> .....	8
<a href="#">DNS Cache Memory Optimization</a> .....	10
<a href="#">Increased FQDN Length Support</a> .....	10
<a href="#">Enhanced URL Switching Failure Handling</a> .....	11
<a href="#">Dynamic Selection of Non-HTTP and Non-SSL Traffic Paths</a> .....	12
<a href="#">Hybrid KEM Support for TLS 1.3</a> .....	14
<a href="#">Enhanced RADIUS Health Monitoring</a> .....	15

---

## IPAM Integration with Sideband Support

ACOS introduces native IP Address Management (IPAM) integration with sideband connections through aFlex enhancements. This feature allows ACOS to query external IPAM systems and REST-based services while traffic is being processed.

When enabled, ACOS uses aFlex to make inline HTTP or HTTPS sideband requests to an external IPAM system using client information such as the source IP address. The response from IPAM is received in real time and can be used immediately to control how traffic is handled, including service selection, policy enforcement, or service chaining.

By performing IPAM lookups directly in the data path, you can build simple, attribute-based traffic policies that adapt dynamically based on external information such as user group, device type, or security classification stored in IPAM.

### Key Benefits

- Enables real-time and context-aware traffic handling based on external attributes
- Provides flexibility in service chaining based on dynamic client identity
- Extends aFlex capabilities to include external decision sources

### aFlex Command and Events

The following new event is introduced to enable policy decisions immediately after TCP connection establishment:

- `CLIENT_ACCEPTED_CHECK`

The following new sideband HTTP commands are introduced to initiate and manage inline HTTP or HTTPS requests to external systems:

- `SIDE_HTTP::task`
- `SIDE_HTTP::response_code`
- `SIDE_HTTP::response_header`
- `SIDE_HTTP::response_body`

### Limitations

- Sideband HTTP or HTTPS requests are executed in the slow path only.
- Only one `SIDE_HTTP::task` can be active per client connection at any given time. If initiated again, it overwrites the previous task.

---

### See Also:

- [Application Delivery and Server Load Balancing Guide](#)
- [aFlex Scripting Language Reference](#)

## DNS Cache Memory Optimization

---

ACOS introduces an enhancement to optimize DNS cache memory usage by dynamically allocating memory based on the actual DNS response size. This optimization reduces memory consumption while preserving existing DNS cache behavior and configuration.

This enhancement is especially beneficial in deployments with variable DNS response sizes, where fixed allocation may lead to unnecessary memory overhead. There is no impact on DNS cache functionality, CLI commands, or operational workflows.

### Show command

To view DNS cache memory allocation information, use the following command:

```
ACOS(config)# show dns cache statistics
```

See Also:

- [Command Line Interface Reference](#)

## Increased FQDN Length Support

---

ACOS now supports longer Fully Qualified Domain Names (FQDNs) for selected Server Load Balancing (SLB) features. The maximum supported hostname length has been updated to **253 characters**.

This update ensures that ACOS devices support modern application configuration that rely on long or nested domain names. The extended FQDN length aligns ACOS behavior with current DNS standards. This feature is applicable only to SLB functionality and does not impact other modules. Existing configurations that use shorter hostnames will continue to function as configured.

### CLI Configuration

- To configure an SLB real server using a long hostname, use the following command:

```
ACOS(config)# slb server <server_name> <hostname>
```

- To configure an SLB service-group member using a long hostname, use the following command:

```
ACOS(config)# slb service-group <name> { tcp | udp }
ACOS(config-service-group)# member <server-name> <port> <hostname>
```

- To configure an SLB link-probe template with a long destination hostname, use the following command:

```
ACOS(config)# slb template link-probe <name>
ACOS(config-link-probe)# destination hostname <hostname>
```

- To perform health monitoring and verify network connectivity using a long hostname, use the following command:

```
ACOS(config)# ping <hostname>
```

### Show command

To view DNS cache entries associated with longer hostnames, use the following command:

```
ACOS(config)# show ip dns-cache <hostname>
```

### Limitations

Configurations that use longer FQDNs are not backward compatible. Downgrading to an earlier ACOS release may result in configuration validation failures.

### See Also:

[Command Line Interface Reference](#)

## Enhanced URL Switching Failure Handling

ACOS enhances HTTP URL switching by providing a consistent and predictable failure-handling mechanism when a request is mapped to a service group that is unavailable. The ACOS device can be configured to respond directly with HTTP 503 or HTTP 504 when a URL-matched service group is down. This provides clear and predictable error handling when backend services are down.

Previously, if a matched service group was down, ACOS relied on a default service group configured under the virtual port (vPort). This could cause unintended request routing, session termination, or inconsistent error responses.

With this enhancement, administrators can configure URL-switching rules to return a user-defined error code (503 or 504) without using a fallback service group or aFlex. The failure is handled per request, meaning only the affected request fails. By default, the TCP connection is preserved using HTTP keep-alive, allowing subsequent requests on the same connection to continue normally.

### CLI Configuration

- To configure URL switching to return an HTTP error code when the matched service group is down, use the following command under an HTTP template:

```
ACOS(config)# slb template http URL-switch
ACOS(config)# url-switching contains /auth service-group Auth-SG sg-
down-respond-code 503
ACOS(config)# url-switching contains /drive service-group Token-SG sg-
down-respond-code 504
```

---

**NOTE:** This feature is disabled by default and takes effect only when the `sg-down-respond-code` option is explicitly configured.

---

- To optionally terminate the client TCP connection after sending the HTTP response:

```
ACOS(config)# slb template http URL-switch
ACOS(config)# url-switching contains /auth service-group Auth-SG sg-
down-respond-code 503 terminate-client-conn
```

### See Also:

- [Application Delivery Controller Guide](#)
- [Command Line Interface Reference](#)

---

## Dynamic Selection of Non-HTTP and Non-SSL Traffic Paths

---

ACOS extends traffic steering capabilities to support dynamic path selection for traffic that does not match the expected protocol on Layer 7 virtual ports in service chaining deployments.

Traffic identified as non-HTTP or non-SSL can be evaluated at runtime, and the appropriate service-group can be selected dynamically using aFlex.

This feature provides the following capabilities:

- Dynamically selects a service-group for non-HTTP traffic received on HTTP or HTTPS virtual ports
- Dynamically selects a service-group for non-SSL traffic received on SSL-enabled virtual ports
- Supports preservation or explicit translation of destination ports as part of traffic steering logic
- Improves flexibility and control in service chaining deployments, especially in mixed-protocol environments.

### **aFlex Command and Events**

The following new events are introduced to enable dynamic handling of non-HTTP and non-SSL traffic:

- `HTTP_NON_HTTP`
- `CLIENTSSL_NON_SSL`

When both events are applicable, the `CLIENTSSL_NON_SSL` event is executed before the `HTTP_NON_HTTP` event. Thus, ensuring SSL-related processing takes precedence.

The following new global command is added to control destination port handling:

- `translate_dest_port`

The following new SSL command is added to redirect non-SSL traffic from the generic proxy to the HTTP proxy:

- `SSL::bypass_to_http`

The following command is used within the new events to dynamically select the service-group:

- `pool`

---

See Also:

- [Application Delivery and Server Load Balancing Guide](#)
- [aFlex Scripting Language Reference](#)

## Hybrid KEM Support for TLS 1.3

---

ACOS supports Hybrid Key Exchange Mechanism (Hybrid-KEM) for TLS 1.3 in software SSL mode. This mechanism leverages TLS library v3 and combines Post-Quantum Cryptographic (POC) and traditional algorithms to provide protection against traditional and quantum computing threats.

The mechanism supports crypto agility by allowing:

- Preferred use of Hybrid-KEM algorithms when configured
- Automatically fall back to traditional ECDHE algorithms

It is ideally suited in the following scenarios:

- TLS 1.3 SSL offload deployments and hybrid environments that require post-quantum readiness.
- Data center and enterprise ADC environments that are transitioning to Post-Quantum Cryptography (PQC).

### Limitations

- SSLi or explicit proxy use cases are not supported.
- Deprecated protocols and algorithms (SSLv3, TLS 1.0/1.1, SHA 1, MD5) are not supported.
- Dual key share mode increases CPU utilization due to multiple key share generations.
- RSA 1024 bits and smaller key sizes are not supported.

### CLI Configuration

Hybrid KEM support for TLS 1.3 is available only in software SSL mode using TLS library v3.

- To enable TLS library v3 in software SSL mode, configure the following commands:

```
ACOS (config) # slb common  
ACOS (config-common) # ssl-module software  
ACOS (config-common) # tls-lib-v3-enable
```

- To configure Hybrid-KEM and traditional key exchange groups on Client SSL and Server SSL templates, use the `supported-group` command. This command supports Hybrid-KEM groups and traditional groups.

### Example

The following command configures the client SSL template with `x25519MLKEM768` Hybrid-KEM group and `secp384r1` traditional key exchange group.

```
ACOS(config)# slb template client-ssl cssl_pqc
ACOS(config-client-ssl)# supported-group X25519MLKEM768
ACOS(config-client-ssl)# supported-group secp384r1
```

### Show Commands

To verify Hybrid-KEM configuration and SSL statistics, use the following show command:

```
ACOS(config)# show slb ssl-counters
```

---

### See also:

- [Application Delivery Controller Guide](#)
- [Command Line Interface Reference](#)

---

## Enhanced RADIUS Health Monitoring

ACOS now supports enhanced RADIUS health monitoring, including support for accounting requests, to improve validation of backend RADIUS services. This enhancement extends health monitoring to include accounting services and introduces additional configuration flexibility to reduce false failure detection.

The RADIUS health monitor supports:

- Validation of RADIUS accounting services
- Optional disabling of RADIUS `response-code` validation
- Explicit configuration of the `nas-ip-address` attribute
- Support for both IPv4 and IPv6 `nas-ip-address` values

These capabilities allow you to distinguish between basic service reachability and authentication success for RADIUS services.

You can disable `response-code` validation for `access-request` and `accounting-request` messages. When response-code validation is disabled, the health monitor skips response-code checks and uses the receipt of valid responses to determine the server's UP or DOWN status.

In addition, you can also configure the `nas-ip-address` used in RADIUS health monitor requests. If this option is not configured, the health monitor automatically uses the IP address of the outgoing interface as the NAS-IP-Address.

### CLI Configuration

- To configure a health monitor with only an `access-request` port and no expected response codes, use the following command:

```
ACOS(config-health:monitor)# method radius username <username> password <examplepassword> secret <secret-from-radius-server> port <port-num>
```

- To configure a health monitor with an `accounting-request` port and expected response codes, use the following command:

```
ACOS(config-health:monitor)# method radius username <username> password <examplepassword> secret <secret-from-radius> accounting-port <port-num> expect response-code <code-list>
```

- To configure a health monitor with `access-request` and `accounting-request` ports without response-code validation, use the following command:

```
ACOS(config-health:monitor)# method radius username <username> password <examplepassword> secret <secret-from-radius> accounting-port <port-num>
```

- To configure `nas-ip-address` with response-code validation, use the following command:

```
ACOS(config-health:monitor)# method radius username <username> password <examplepassword> secret <secret-from-radius> nas-ip-address <nas-ip> expect response-code <code-list>
```

- To configure `nas-ip-address` without response-code validation, use the following command:

```
ACOS(config-health:monitor)# method radius username <username> password <examplepassword> secret <secret-from-radius> nas-ip-address <nas-ip>
```

### Show Command

The following show command has been enhanced to display the `nas-ip-address` and `accounting-port` details of the health monitor:

- `show health monitor <health_monitor>`

---

### See Also:

- [Application Delivery Controller Guide](#)
- [Command Line Interface Reference](#)

## Carrier Grade NAT

ACOS 7.0.3 introduces the following new feature and enhancement for Carrier Grade NAT (CGN or CGNAT):

The following topic is covered:

[Hardware-Accelerated DDoS Protection on Non-SPE FTA Platforms](#) .....17

---

## Hardware-Accelerated DDoS Protection on Non-SPE FTA Platforms

---

ACOS supports hardware accelerated DDoS protection only on the Thunder 7650 non-SPE FTA platforms. LSN selective filtered entries can now be offloaded to the Broadcom (BCM) switch, meaning anomalous traffic can be blocked directly at the hardware level. This offload significantly reduces CPU load during volumetric DDoS attacks and improves overall system performance.

**NOTE:** This feature is not supported on other non-SPE FTA platforms.

---

### Key Points:

- A standalone license, `HW_ACCELERATED_BLOCKING` must be installed to enable hardware blocking. Without the license, selective filtering is supported entirely in software by the CPU. With the license, the entries are offloaded to the hardware.

- Once the hardware entry limit of 700 is reached, additional entries are not offloaded to hardware and are instead handled in software.
- Hardware blocking is supported at L3 level and at L4 level for TCP and UDP traffic only.

### CLI Configuration

Offloading selective filtering entries to the hardware does not require a separate CLI configuration. It uses the same configuration as selective filtering for LSN. This feature is supported only on the Thunder 7650 non-SPE FTA platforms.

To configure a limit for selective filtering entries on the hardware for non-SPE FTA platforms, use the following command:

```
ACOS(config)#cgnv6 ddos-protection max-hw-entries number
```

**NOTE:** The maximum number of hardware entries is limited to 700 by default. Configuration change is not required unless a lower limit needs to be enforced. This limit is system-wide and not per partition.

### Show Command

The following show command has been enhanced to display different counters:

```
show counters cgnv6 ddos-protection
```

See Also:

- [IPv4-to-IPv6 Transition Solutions Guide](#)
- [Command Line Interface Reference](#)

## Firewall Configuration

ACOS 7.0.3 introduces the following new features and enhancements for Firewall Configuration (CFW):

The following topic is covered:

[Support for ICMP Traffic without a Matching Session](#) ..... 19

## Support for ICMP Traffic without a Matching Session

---

ACOS supports processing specific ICMP traffic without an existing firewall session in asymmetric firewall deployments. In such deployments, the firewall may observe traffic in only one direction, which can cause legitimate ICMP response packets to be dropped due to the absence of a matching session.

When this feature is enabled, the firewall ensures that valid `ICMP echo replies` and `ICMP error messages` received on the inside-interface are forwarded correctly, even if the initiating request was not seen by the firewall.

For ICMP echo replies, ACOS dynamically creates a new session, forwards the packets, and processes subsequent packets using normal session handling logic.

For ICMP error messages, ACOS forwards the packet without creating a session, as these messages consist of a single packet.

The feature supports both IPv4 and IPv6 and is primarily intended for IPv6 environments, where asymmetric routing scenarios are more common.

### CLI Configuration

- To allow ICMP echo replies without an existing session, use the following command:

```
ACOS(config)# fw allow-icmp-echo-reply-fwd
```

- To allow ICMP error messages without an existing session, use the following command:

```
ACOS(config)# fw allow-icmp-err-msg-fwd
```

### Limitations

- This feature is intended only for asymmetric routing deployments.
- The feature supports only client-side ICMP echo replies and ICMP error messages.
- The firewall does not validate ICMP echo replies if the corresponding requests do not traverse the firewall.

---

### See Also:

- [Firewall Configuration Guide](#)
- [Command Line Interface Reference](#)

## GUI Enhancements

ACOS 7.0.3 introduces the following new feature and enhancement for Graphical User Interface (GUI):

The following topic is covered:

<a href="#">GSLB Group Status Tab in GUI</a> .....	20
--	----

---

### GSLB Group Status Tab in GUI

ACOS has introduced a new information tab in the Global Server Load Balancing (GSLB) Graphical User Interface (GUI) to enhance operational visibility of devices participating in a GSLB group. This enhancement enables users to easily identify the GSLB role (Master or Member) of a device, and to view real-time operational information for all members of a GSLB group directly from the GUI.

The **GSLB > Groups > Status** tab provides a consolidated, read-only view of runtime information for all devices in a GSLB group. For each group member, the Status tab displays the following information:

- Member
- Sys-ID
- Priority
- Attributes
- Status
- Secure Config
- Secure Status
- Address

This enhancement is intended for monitoring and diagnostic purposes only. It does not introduce any changes to existing GSLB configuration workflows, CLI commands, or functional behavior.

---

See Also:

For more information, refer to the **GUI Online Help** by clicking the information icon located at the top-right corner of the ADC device GUI.

## Platforms

ACOS 7.0.3 introduces the following new feature and enhancement for ACOS Platforms:

The following topics are covered:

<a href="#">Thunder Container OpenShift Support</a> .....	21
<a href="#">Disabled Second Management Interface (management2) on Thunder 8665 Platform</a> .....	21
<a href="#">RHEL 9.6 Support for A10 Thunder MVP</a> .....	22
<a href="#">Enhanced Capacity FlexPool License Support for Hardware Appliances</a> .....	22
<a href="#">Introduced New AI Platforms</a> .....	24
<a href="#">Introduced Thunder 3360S Platform</a> .....	24
<a href="#">Introduced Thunder 3765 Platform</a> .....	25

## Thunder Container OpenShift Support

With this release, Thunder Container supports Red Hat OpenShift 4.18.

See Also:

- [cThunder OpenShift Installation Guide](#)

## Disabled Second Management Interface (management2) on Thunder 8665 Platform

ACOS has disabled the second management interface (management2) on Thunder 8665 platform, which was previously used to provide redundant management connectivity.

The primary management interface or the data plane interfaces may be used for management access after upgrading.

---

See Also:

- [Release Notes](#)

## RHEL 9.6 Support for A10 Thunder MVP

---

A10 Thunder Multi-tenant Virtual Platform (MVP) is now updated to run on Red Hat Enterprise Linux (RHEL) 9.6. It provides continued access to the latest operating system security updates and ongoing platform support.

See Also:

- [A10 MVP Thunder Configuration Guide](#)

## Enhanced Capacity FlexPool License Support for Hardware Appliances

---

ACOS 7.0.3 added additional Thunder hardware appliance models to Capacity FlexPool licensing. It also introduced bandwidth-to-core mapping for selected modular platforms with bandwidth tiers. For those platforms, ACOS and A10 Control will determine how the system allocates CPU cores based on the licensed or configured throughput (bandwidth) value. This enhancement ensures that the FlexPool for hardware appliances aligns with the performance of standard modular tiers.

The following table outlines the minimum and maximum bandwidth (BW) limits required for these platforms:

Table 1 : Capacity FlexPool License Support

Platform	Minimum BW	Maximum BW	Bandwidth-to-Core Mapping
Thunder 1060(S)	10G	40G	<ul style="list-style-type: none"> <li>• <math>\geq 10G</math> and <math>&lt; 25G \rightarrow 9</math> cores</li> <li>• <math>\geq 25G \rightarrow</math> Unlimited cores</li> </ul>
Thunder 3350(S)	40G	70G	Not applicable
Thunder 5960	100G	300G	Not applicable

Table 1 : Capacity FlexPool License Support

Platform	Minimum BW	Maximum BW	Bandwidth-to-Core Mapping
Thunder 7460(S)	150G	250G	<ul style="list-style-type: none"> <li>• <math>\geq 150\text{G}</math> and <math>&lt; 200\text{G}</math> <math>\rightarrow</math> 20 cores</li> <li>• <math>\geq 200\text{G}</math> and <math>&lt; 250\text{G}</math> <math>\rightarrow</math> 28 cores</li> <li>• <math>= 250\text{G}</math> <math>\rightarrow</math> Unlimited cores</li> </ul>
Thunder 7460(S-MAX)	250G	270G	Not applicable

**NOTE:**

- Bandwidth changes within the same tier automatically updated and does not require reboot.
- Bandwidth changes across the tier boundary require reboot after user approval.

To improve Capacity FlexPool licensing, the registration process with A10 Control now includes the following system details in the aXAPI payload. ACOS now sends these details to A10 Control during device registration:

- Max CPUs
- Control CPUs
- Current CPUs
- Minimum Bandwidth

**See Also:**

- [Capacity Flex Pool Licensing Guide](#)
- [Release Notes](#)
- [GLM User Guide](#)

## Introduced New AI Platforms

---

The following AI-optimized hardware platforms are introduced in this release:

- Thunder 1068
- Thunder 7468

These high performance AI platforms are designed to address the emerging AI security and networking threats. Powered with GPUs, they provide advanced AI processing capabilities and hardware readiness for future A10 AI solutions. These platforms are packaged with a unified bundle containing ADC and AI Firewall (AIFW) solutions.

---

See Also:

- [A10 Thunder Series TH1068 Installation Reference Guide](#)
- [A10 Thunder Series TH7468 Installation Reference Guide](#)
- [A10 Platform Compatibility Matrix](#)
- [AI Firewall User Guide](#)
- [Optics Data Sheet](#)

## Introduced Thunder 3360S Platform

---

ACOS 7.0.3 now supports Thunder 3360S platform, which is the next generation replacement for TH3350 series. Thunder 3360S is a non-FTA hardware platform. It is designed to support the following deployments:

- ADC
- CFW-ADC
- NGWAF

Additionally, this platform is powered by Intel QuickAssist Technology (QAT). QAT provides ACOS with a hardware-enabled foundation for SSL Insight with TLS 1.3 protocol.

---

See Also:

- [A10 Thunder Series TH3360S Installation Reference Guide](#)
- [A10 Platform Compatibility Matrix](#)
- [Optics Data Sheet](#)

## Introduced Thunder 3765 Platform

---

The A10 Networks Thunder 3765 is a specialized low-latency Application Delivery Controller (ADC) designed for high-frequency trading and financial environments. It delivers ultra-fast traffic processing with latency of less than 2 microseconds ( $\mu\text{s}$ ).

Thunder 3765 Ultra Low Latency 2 (ULL) platform applies optimizations, enabled by hardware acceleration, to significantly reduce packet forwarding latency and jitter for established sessions.

When enabled, the ULL 2:

- Optimizes packet processing paths for faster forwarding.
- Supports granular program policies for efficient traffic handling.

**NOTE:** Thunder 3765 platform supports low latency for up to 2,000 sessions only.

See Also:

- [A10 Thunder Series TH3765 Installation Reference Guide](#)
- [Command Line Interface Reference](#)
- [A10 Platform Compatibility Matrix](#)
- [Optics Data Sheet](#)

## SSL Insight

ACOS 7.0.3 introduces the following new feature and enhancement for SSL Insight (SSLi):

The following topics are covered:

<a href="#">Dynamic Steering of Certificate Fetch Operations</a> .....	26
<a href="#">Clear-Text Traffic Replication</a> .....	27

## Dynamic Steering of Certificate Fetch Operations

---

ACOS enables dynamic steering of SSL handshake–related connections in SSL Insight (SSLi) deployments using aFlex-based service chain selection.

During SSLi processing, outbound connections for server certificate retrieval, OCSP queries, and CRL downloads can be directed through a user-defined service chain using the aFlex script. These connections inherit the service chain selected at the SSL handshake stage.

This applies to HTTPS traffic (HTTP/1.1 and HTTP/2) when SSLi inspection is enabled.

### Key Benefits

- Aligns handshake and client traffic under a unified aFlex policy
- Improves visibility and troubleshooting of certificate validation flows
- Removes dependency on static routing for certificate-related traffic

### aFlex Command and Events

This feature uses the existing aFlex `pool` command in the following events:

- CLIENT\_ACCEPTED
- CLIENTSSL\_CLIENTHELLO

The selected pool determines the service group (next-hop) for handshake-related connections and can also influence subsequent client traffic. You can bind the aFlex script to the SLB virtual port to enable this behavior.

For more information about aFlex syntax and related commands, see the *aFlex Scripting Language Reference Guide*.

### Limitations

- The aFlex `pool` command affects only service-group (next-hop) selection. It does not change the destination IP address or port for certificate fetch, OCSP, or CRL

connections.

- Existing aFlex scripts that use the `pool` command in supported events may exhibit behavior changes after upgrade and should be reviewed.
- Explicit Proxy SSLi and Transparent Proxy SSLi are not supported.

---

See Also:

- [SSL Insight Configuration Guide](#)
- [aFlex Scripting Language Reference](#)

## Clear-Text Traffic Replication

---

ACOS supports bidirectional clear-text traffic replication to mirror decrypted traffic to external TAP (collector) systems for monitoring and analysis, without impacting the original traffic flow.

This is used in deployments where encrypted traffic is decrypted, inspected, and optionally replicated.

Clear-text traffic replication can be applied at one of the following stages:

- **Client-side replication:** Traffic is replicated between the client and ACOS. Replication occurs before re-encryption toward the client and is configured using a virtual-port template. It is typically used to monitor outbound responses to client.
- **Server-side Replication:** Traffic is replicated between ACOS and the backend server. Replication occurs after decryption of client traffic and is configured using a service-group. It is typically used to monitor requests sent toward servers.

The client-side and server-side replications are configured independently and are not applied simultaneously on the same virtual port. If both configurations are present, client-side replication takes precedence over server-side replication.

### Key Benefits

- Mirrors bi-directional traffic (request and response) to provides visibility into decrypted application traffic

- Forwards the replicated traffic to configured TAP servers
- Rewrites destination MAC address only for replicated packets.

### Supported Features

- Layer 7 full-proxy TCP applications only (HTTP, HTTPS)
- HTTP/1.1 and HTTP/2
- SSLi Inspection use cases

### CLI Configuration

To configure client-side traffic replication on a virtual port, use the following commands:

```
ACOS(config)# slb template virtual-port client_side_mirror_template
ACOS(config-vport)# traffic-replication tap-sg
```

To configure server-side traffic replication using a service group, use the following commands:

```
ACOS(config)# slb service-group https-sg tcp
ACOS(config-slb svc group)# traffic-replication-type mirror-server-side
```

### Limitations

- Not supported on virtual ports configured with both client-SSL and server-SSL.
- Not supported on Layer 4 virtual ports.
- Clear-text replication occurs before the TCP stack processing, so out-of-order packets or overlapping segments are not reassembled.
- Client-side and server-side replication are configured independently and cannot be applied simultaneously.

---

### See Also:

- [SSL Insight Configuration Guide](#)
- [Application Delivery and Server Load Balancing Guide](#)
- [Command Line Interface Reference](#)

## Security Updates

The following security vulnerabilities are addressed in the ACOS 7.0.3 release:

- Expat Vulnerability
  - CVE-2025-59375: It is a security vulnerability found in libexpat (XML parser library) prior to 2.7.2. It allows attackers to trigger large dynamic memory allocations through a small document that is submitted for parsing.
- HTTPD Vulnerabilities
  - CVE-2025-58098: It is a security vulnerability in Apache HTTP Server that affects versions 2.4.65 and earlier. This is a query string mishandling in Apache HTTP Server with `SSI + mod_cgid` enabling command execution through `#exec`.
  - CVE-2023-38709/CVE-2024-42516: It is a security vulnerability in the core of Apache HTTP Server. This is a Content-Type header manipulation in Apache HTTP Server that allows HTTP response splitting attacks.
- Tar Path Traversal Vulnerability
  - CVE-2025-45582: It is a path traversal vulnerability in GNU Tar through version 1.35 that allows attackers to overwrite critical files through Symlink in Multiple Archive Extraction Steps.

For detailed information about security updates, see [A10 Networks Security Advisories](#).

## Threat Protection System

ACOS 7.0.3 introduces the following new feature and enhancement for Threat Protection System (TPS): [New Features and Enhancements](#)

---

**NOTE:** For TPS-related configuration, refer to [DDoS Mitigation Guide](#). Similarly, for TPS-related CLI commands, refer to [DDoS Command Line Reference Guide](#).

---

## Enhancements in ACOS 7.0.2

---

This topic provides a brief overview of the new features and enhancements added in the ACOS 7.0.3 release:

For new features and enhancements prior to ACOS 7.x release, see the recent prior ACOS [New Features and Enhancements](#).

The following topic is covered:

<a href="#">Application Access Management</a> .....	30
<a href="#">aXAPI</a> .....	31
<a href="#">Carrier Grade NAT</a> .....	32
<a href="#">Platforms</a> .....	33
<a href="#">System and Security</a> .....	36
<a href="#">SSL Insight</a> .....	44

## Application Access Management

ACOS 7.0.2 introduces the following new features and enhancements for Application Access Management (AAM):

---

**NOTE:** For AAM specific configuration steps, refer *Application Access Management Guide*.

---

The following topics are covered:

<a href="#">Enhanced Kerberos Encryption with AES128 and AES256 Encryption Algorithms</a> .	31
---	----

## Enhanced Kerberos Encryption with AES128 and AES256

### Encryption Algorithms

---

ACOS supports AES-based Kerberos encryption algorithms for keytab generation in Windows Integrated Authentication (WIA). This enhancement significantly improves the security of generating Kerberos keytabs by adopting stronger encryption standards that are highly compatible with both Windows Active Directory and MIT Kerberos (krb5). Additionally, the RC4-HMAC Kerberos encryption algorithm has been deprecated due to its known security vulnerabilities:

- aes128-cts-hmac-sha1-96
- aes256-cts-hmac-sha1-96 (default encryption algorithm)

This feature is supported on all platforms and deployment topologies.

#### CLI Configuration

After configuring the Kerberos account and enabling AES encryption on Windows, execute one of the following CLI commands on the ACOS device to choose the Kerberos encryption algorithm used for WIA:

```
ACOS (config-kerberos-spn:client-name) #encryption-algorithm aes128-cts-hmac-sha1-96
```

```
ACOS (config-kerberos-spn:client-name) #encryption-algorithm aes256-cts-hmac-sha1-96
```

The default encryption algorithm is `aes256-cts-hmac-sha1-96`.

---

#### See Also:

- [Application Access Management Guide](#)
- [Command Line Interface Reference](#)

## aXAPI

ACOS 7.0.2 introduces the following new features and enhancements for aXAPI:

The following topic is covered:

[Support Batch Operations](#) .....32

## Support Batch Operations

---

ACOS support batch API to send multiple axAPI requests in a single call, which reduces round-trip time and improves performance.

The following two endpoints are implemented:

- Batch-Get (`/axapi/v3/batch-get`)- for grouping multiple GET requests
- Batch-Post (`/axapi/v3/batch-post?ignore-errors={true|false}`) - for grouping multiple POST, PUT, DELETE requests.

---

See Also

- [axAPIv3 Reference Guide](#)

## Carrier Grade NAT

ACOS 7.0.2 introduces the following new feature and enhancement for Carrier Grade NAT (CGN or CGNAT):

The following topic is covered:

[Hardware-Accelerated DDoS Protection on Non-FTA Platforms](#) .....32

## Hardware-Accelerated DDoS Protection on Non-FTA Platforms

---

ACOS supports hardware-accelerated DDoS protection on non-FTA platforms having Mellanox ConnectX NICs, such as Thunder 5960. LSN selective filtered entries can now be offloaded to the hardware, meaning anomalous traffic can be blocked directly at the hardware level. This offload significantly reduces CPU load during volumetric DDoS attacks and improves overall system performance.

**Key Points:**

- A standalone license, `HW_ACCELERATED_BLOCKING` must be installed to enable hardware blocking. Without the license, selective filtering entries are enforced entirely in software by the CPU. With the license, the entries are offloaded to the hardware.
- CPU packet prioritization must be enabled.
- Once the hardware entry limit is reached (16k or a lower configured value), additional selective filtering entries are not offloaded to hardware and are instead handled in software.
- Hardware blocking is supported at L3 level and at L4 level for TCP and UDP traffic only.

### CLI Configuration

Offloading selective filtering entries to the hardware does not require a separate CLI configuration. It uses the same configuration as selective filtering for LSN. This feature is supported only on non-FTA platforms equipped with Mellanox ConnectX NICs (for example, Thunder 5960), as well as on SPE platforms.

#### Additional configurations:

- To enable CPU packet prioritization on non-FTA platforms, use the following command:

```
ACOS(config)# system cpu-packet-prio-support enable
```

- To view the selective filtering statistics for hardware offloading, use the following command:

```
ACOS(config)# show counters cgnv6 ddos-protection
```

---

### See Also:

- [IPv4-to-IPv6 Transition Solutions Guide](#)
- [Command Line Interface Reference](#)

## Platforms

ACOS 7.0.2 introduces the following new feature and enhancement for ACOS Platforms:

The following topic is covered:

<a href="#">Introduced Thunder 7465 Platform</a> .....	34
<a href="#">Enhanced Thunder 7460S and 7460S-MAX Platforms</a> .....	34
<a href="#">Ngen Low Latency License for Thunder 1060S</a> .....	35
<a href="#">vThunder Enhancements</a> .....	36

## Introduced Thunder 7465 Platform

---

Thunder 7465 has been introduced as the newly supported next mid-range generation FTA/FPGA supported platform. This platform is designed to support the following deployments:

- CGN
- CFW-CGN
- TPS Detector

---

**NOTE:** For Non-Stop DNS TPS, Thunder 7465 appliances will replace Thunder 6655S and Thunder 7655S.

---

Additionally, the Thunder 7465 provides flexible bandwidth tiers through modular licensing, enabling customers to scale network capacity as needed. It is available with both Modular Perpetual and Modular Subscription licensing models. The 100G DR optics are qualified on this platform.

See Also:

- [A10 Thunder Series TH7460S/TH7460SMAX/TH7465 Installation Reference Guide](#)
- [Global Licensing Manager](#)

## Enhanced Thunder 7460S and 7460S-MAX Platforms

---

Thunder 7460S and 7460S-MAX platforms have been optimized to support Next-Gen Web Application Firewall (NGWAF) deployments.

Additionally, capacity flex pool license support is introduced for TH7460S and TH7460S-MAX through A10 Control. This enhancement enables dynamic bandwidth allocation, optimizing resource utilization based on licensing requirements. The 100G DR optics are qualified on these platforms.

The following table outlines the minimum and maximum bandwidth (BW) limits required for these platforms:

Table 2 : Capacity Flex Pool License Support

Platform	Minimum BW	Maximum BW
Thunder 7460S	150G	250G
Thunder 7460S-MAX	250G	270G

You can adjust the bandwidth using A10 control.

See Also:

- [Next-Gen WAF Configuration Guide](#)
- [Capacity Flex Pool Licensing Guide](#)
- [Release Notes](#)
- [A10 Control User Guide](#)

## Ngen Low Latency License for Thunder 1060S

A new low latency license is introduced **Ngen Low Latency** for Thunder 1060S. This license enables low-latency mode, which applies system-level optimizations to reduce packet forwarding latency and jitter for established sessions.

It is intended for performance-sensitive workloads such as financial services and high-frequency trading (HFT) environments, helping organizations achieve faster transaction processing.

The Ngen low latency license can be acquired from A10 Global License Manager (GLM) and activated on Thunder 1060S platform.

See Also:

- [Global Licensing Manager.](#)
- [Application Delivery Controller Guide](#)

## vThunder Enhancements

---

The following support is introduced in vThunder platform:

- AMD EPYC 4th Gen (Genoa and Turin) processors across BareMetal, KVM, and VMware ESXi deployments.

---

**NOTE:** This capability is for evaluation purposes only and not recommended for production deployments.

---

- Azure Dasv6 series instances with Gen2 EFI VM support.  
Dasv5 AMD Gen1 instances (3rd Gen EPYC) are no longer supported.

---

See Also:

- [vThunder Installation Guide](#)

## System and Security

ACOS 7.0.2 introduces the following new features and enhancements for system and security:

---

**NOTE:** For more information and details, refer *System Configuration and Administration Guide*.

---

The following topics are covered:

<a href="#">Enhancements to SSH Control-Plane Security</a> .....	37
<a href="#">Enhancements to System Security</a> .....	38
<a href="#">Enhancement to Device Configuration Encryption</a> .....	39
<a href="#">Disk Encryption Support</a> .....	41
<a href="#">Password Configuration Methods for Admin Accounts</a> .....	42

<a href="#">Introduced Configuration Synchronization Between A10 Control and ACOS</a> .....	42
<a href="#">Enhanced axdebug File Size</a> .....	43

## Enhancements to SSH Control-Plane Security

---

ACOS supports enhancing the control-plane security to prevent credential theft, lateral movement, unauthorized communication, data exfiltration, reducing attack surface, X11-related vulnerabilities, reducing automated attacks, and avoiding brute-force attempts.

The following SSH functionalities are disabled using the CLI options to enhance security:

- SSH Agent Forwarding
- SSH TCP Port Forwarding
- SSH X11 Forwarding
- Changing Default SSH TCP Port

**NOTE:** These settings apply globally across the ACOS system.

---

### CLI Configuration

- To disable SSH Agent Forwarding, use the following command:

```
ACOS(config)# sshd-config disable-agent-forwarding
```

- To disable SSH TCP Forwarding, use the following command:

```
ACOS(config)# sshd-config disable-tcp-forwarding
```

- To disable SSH X11 Forwarding, use the following command:

```
ACOS(config)# sshd-config disable-x11-forwarding
```

- To change the SSH port number, use the following command:

```
ACOS(config)# sshd-config tcp-port
```

---

See Also:

- [System Configuration and Administration Guide](#)
- [Command Line Interface Reference](#)

## Enhancements to System Security

---

ACOS has enhanced the system-level security to maintain the network integrity, and provide an additional layer of defense against network-based threats. It prevents IP spoofing, packet sniffing, traffic redirection, and DDoS attacks.

The following features are implemented at the system level and impact all control plane traffic:

- Source-Routed Packet Drop - Drops IPv4 and IPv6 source-routed packets to prevent spoofing and traffic redirection.
- Reverse Path Filtering (RPF) - Verifies IPv4 and IPv6 control plane packets by Strict RPF checks to prevent IP spoofing.
- ICMP Redirect Control - Disables ICMP redirect messages from sending to prevent traffic hijacking.
- ICMP Unreachable Filtering - Disables ICMP unreachable messages from sending to prevent traffic redirection, spoofing, and DDoS attacks.

### CLI Configuration

- To drop the IPv4 source-routed packets, use the following command:

```
ACOS(config)# system ip source-route-pkt-drop-enable
```

- To drop the IPv6 source-routed packets, use the following command:

```
ACOS(config)# system ipv6 source-route-pkt-drop-enable
```

- To disable the sending of IPv4 ICMP destination unreachable messages, use the following command:

```
ACOS(config)# system ip icmp-unreachable-disable
```

- To disable the sending of IPv6 ICMP destination unreachable messages, use the following command:

```
ACOS(config)# system ipv6 icmpv6-unreachable-disable
```

- To disable the sending of IPv4 ICMP redirect messages, use the following command:

```
ACOS(config)# system ip icmp-redirect-disable
```

- To disable the sending of IPv6 ICMP redirect messages, use the following command:

```
ACOS(config)# system ipv6 icmpv6-redirect-disable
```

- To enable RPF in strict mode for IPv4 source address, use the following command:

```
ACOS(config)# system ip rpf-check-enable
```

- To enable RPF in strict mode for IPv6 source address, use the following command:

```
ACOS(config)# system ipv6 rpf-check-enable
```

### Show Command

The following show command has been enhanced to display the number of dropped IPv4 and IPv6 source-routed and RPF packets:

- `show slb switch`

### Limitation

- It impacts only the Layer 3 forwarded traffic.
- The commands apply system-wide and impact all control plane packets on the ACOS device. It is not partition-specific.

---

### See Also:

- [System Configuration and Administration Guide](#)
- [Command Line Interface Reference](#)

---

## Enhancement to Device Configuration Encryption

ACOS supports a dynamic hash-key mechanism along with symmetric encryption to ensure that each device configuration is encrypted based on unique device properties. This enhancement allows to set a custom passphrase for encrypting the password. To maintain security and privacy, customers will have complete control over the passphrase.

Additionally, to ensure uniform security across all devices within VCS or VRRP clusters, the same encryption passphrase must be used on all nodes.

**NOTE:** Once the passphrase is set, downgrading to software versions that do not support this feature is not supported.

---

## CLI Configuration

To set the new passphrase, use the following command:

```
ACOS(config)# system update-passphrase
Note: After changing to a new passphrase, you cannot downgrade to the
previous release. Do you want to continue with updating to new passphrase?
[yes/no]: yes
Please enter your new passphrase (minimum 8 characters): passwords
```

## Show Commands

The following show commands are enhanced to display the newly encrypted passwords:

- `show run`
- `show startup-config`

## Limitations

This feature has the following limitations:

- The 'no' functionality is not supported.
- The copying of external configuration to the running configuration is not supported because it is not in an interactive mode.
- aXAPI is not supported.

---

## See Also:

- [System Configuration and Administration Guide](#)
- [Command Line Interface Reference](#)

## Disk Encryption Support

---

ACOS 7.0.2 introduces support for Disk Encryption. This feature helps protect data stored on the device by converting readable data into an unreadable format called *ciphertext*.

When disk encryption is enabled, data-at-rest becomes inaccessible to unauthorized users unless they provide a valid passphrase or decryption key. This enhances data security and helps prevent unauthorized access.

### Supported Devices

- Thunder 3745
- Thunder 3350
- Thunder 5960
- Thunder 1060

### License Requirement

Requires a valid Disk Encryption license. For more information, reach out to the *A10 Sales team*.

### CLI Configuration

To encrypt the disk, use the following command:

```
ACOS(config)#system enable-disk-encryption cipher {aes | serpent |  
twofish} {passphrase <passphrase_string> | passphrase-base64 <base64_  
format_passphrase>}
```

### Limitations

- Upgrading or downgrading is supported only if the disk encryption feature is available in the target ACOS version.
- Both primary and secondary boot images must support disk encryption.

---

See Also:

- [Global Licensing Manager \(GLM\)](#)
- [System Configuration and Administration Guide](#)
- [Command Line Interface Reference](#)

## Password Configuration Methods for Admin Accounts

---

ACOS has enhanced the password configuration method for administrative accounts to secure password confidentiality. This feature ensures that the passwords are hidden or not displayed while they are being entered. It helps to maintain the integrity and confidentiality of sensitive information.

---

See Also:

- [System Configuration and Administration Guide](#)
- [Configuring Application Delivery Partitions](#)
- [Management Access and Security Guide](#)
- [Command Line Interface Reference](#)

## Introduced Configuration Synchronization Between A10 Control and ACOS

---

A configuration synchronization mechanism is introduced to synchronize the configurations from ACOS devices to A10 Control. Instead of relying on periodic manual scans, ACOS now pushes real-time updates to A10 Control using a Kafka-based notification channel.

When any changes are made directly on ACOS devices—whether through CLI or aXAPI—the devices notify A10 Control with the updated configuration version. A10 Control receives the notification and provides an option to synchronize the configuration to send an alert. This ensures that the latest device configuration is visible, reducing the risk of mismatched settings.

### CLI Configuration

- To track or view the configuration changes per partition, the `system config-version` command is used. The parameters of this command are non-configurable and their values are incremented automatically when the configuration changes. The values can be viewed using the `show running-config` command:

```
ACOS(config)# show running-config system config-version
!Section configuration: 102 bytes
!
system config-version
  version 0.22
  updated-at "09-01 17:36:27 IST 2025"
  modified-by admin
!
```

---

**NOTE:** The `version` and `updated-at` parameters can be set using aXAPI.

---

- To configure the interval (in seconds) for the Kafka-based notifications, use the following command:

```
ACOS(config)# system config-mgmt notifications
ACOS(config-notifications)# period <0-60>
```

---

**NOTE:** This command is available only for the shared partition but, once configured, applies system-wide to all partitions

---

### Limitation

VCS, High Availability, and GSLB cluster deployments are not supported.

### See Also:

- [A10 Control Integration Guide](#)
- [Command Line Interface Reference](#)

---

## Enhanced axdebug File Size

---

The `axdebug` feature enables the `axdebug` utility to capture trace packets on ACOS devices. In earlier versions, the capture file size was fixed at 300 MB. Starting with ACOS

7.0.2, users can configure the debug file size within a range of 300 MB to 6000 MB, allowing for larger trace captures. The default file size remains 300 MB.

On multi-PU devices, the system can generate separate debug files for PU1 and PU2, each with a maximum size of 6000 MB. This enhancement offers greater flexibility in trace data collection and helps optimize disk space usage.

### CLI Configuration

Set the axdebug buffer file using the following command:

```
ACOS (config) #axdebug  
ACOS (config) #file-size <300-6000>
```

See Also:

- [Command Line Interface Reference](#)

## SSL Insight

ACOS 7.0.2 introduces the following new feature and enhancement for SSL Insight (SSLi):

The following topic is covered:

[Enhanced QAT SSL Memory Allocation](#) ..... 44

## Enhanced QAT SSL Memory Allocation

---

ACOS supports customizing the pre-allocated QAT (Intel QuickAssist Technology) SSL memory, which is used by SSL hardware offload engines. This enhancement provides safe and flexible control over QAT memory allocation, helping maintain high SSL performance and optimal resource usage.

Additionally, it ensures that memory sizes cannot be set below the required thresholds and prevents misconfiguration that may disable the active SSL engine.

You can use `system ssl-hardware` to set the size of the SSL hardware memory blocks:

- `ssl_mem` - Shared Direct Memory Access (DMA) buffer.

Memory used by QAT engines to move SSL data efficiently between system memory and hardware, reducing CPU load.

- `ssl_context` - Per-engine cipher context memory.

Dedicated memory for storing SSL cipher states per engine, ensuring fast and secure cryptographic operations.

---

**NOTE:** This feature is supported only on Thunder devices with QAT SSL hardware offload engines such as Thunder 1060S, Thunder 7655S, Thunder 8665S.

---

### CLI Configuration

- To configure the size of the SSL hardware memory blocks (`ssl_mem` and `ssl_context`), use the following command:

```
ACOS (config) # system ssl-hw-memory
ACOS (config-ssl-hw-memory) # ssl_mem size<0-20480>
ACOS (config-ssl-hw-memory) # ssl_context_N size<0-20480>
```

The `N` in `ssl_context_N` represents the SSL engine number (2 to 10), for example `ssl_context_2` represents engine 2 memory, `ssl_context_3` represents engine 3 memory and so on. `ssl_context` represents memory for engine 1.

---

**NOTE:** The command takes effect only when you save the configuration using the `write memory` command and then reboot the device using the `reboot` command.

---

### Show Command

To view the status and allocation of the SSL hardware memory blocks, use the `show system ssl-hw-memory` command.

---

### See Also:

- [SSL Insight Configuration Guide](#)
- [Command Line Interface Reference](#)

# Enhancements in ACOS 7.0.1

---

This topic provides a brief overview of the new features and enhancements added in the ACOS 7.0.1 release:

For new features and enhancements prior to ACOS 7.x release, see the recent prior ACOS [New Features and Enhancements](#).

The following topic is covered:

<a href="#">RHEL Platform Support</a> .....	46
<a href="#">New Platform Introduced</a> .....	49
<a href="#">Enhanced ACOS GUI with TPS Integration</a> .....	49

## RHEL Platform Support

ACOS has upgraded its platform operating system from Community Enterprise Operating System (CentOS v7.9) to Red Hat Enterprise Linux (RHEL). This enhancement applies to both on-premises (Thunder) and cloud-based (vThunder and cThunder) deployments.

- **Enhanced Security and Compliance:** Offers robust security features and regulatory compliance capabilities. Built on the RHEL foundation, it ensures that your systems meet the latest industry standards.
- **Improved Stability and Support:** Provides higher reliability and access to the latest updates and patches for improved support and faster addressing of CVEs.
- **Future-Platform Support:** Sets the stage for compatibility with next-generation hardware, including:
  - Advanced Micro Devices (AMD) and Advanced RISC Machines (ARM).
  - NVIDIA ConnectX-7 400G network interface card support to enable high-throughput networking across BareMetal, KVM, and VMware platforms.
  - Intel’s Data Plane Development Kit (DPDK) 23.11 Long Term Support (LTS) version to provide enhanced performance and extended support.

- **Artificial Intelligence (AI) Readiness:** Establishes a foundation for integrating Artificial Intelligence (AI) platforms in future ACOS releases.

## Key Requirements and Support

---

### System Requirements

- Mandates the following system requirements during boot-up system checks and upgrades:
  - Minimum 4 vCPUs
  - Minimum 16 GB memory (must be multiple of 2 GB per vCPU)
  - Minimum 128 GB of total disk space (for QCOW2, VHD, or OVA)
  - Shared poll mode is disabled

For more information, see [Upgrade Guide](#).

### License Requirement

Requires a valid Red Hat Support license for all new ACOS installations and upgrades to ACOS 7.0.1 and later versions. Separate licenses are available for Thunder and vThunder platforms.

For instructions on obtaining and installing a Red Hat Support license, see [Global License Manager User Guide](#).

### Platforms Supported

See [Platform Compatibility Matrix](#).

### vThunder Platform Compatibility

- vThunder compatibility support in cloud:
  - AWS
  - Azure (latest waagent version supported)
  - OCI

- vThunder compatibility support in on-prem:
  - RHEL KVM
  - VMware ESXi

### Limitations

- Upgrade from ACOS 6.0.x to ACOS 7.0.x is not supported or recommended on cloud platforms. Use fresh image deployments only.
- Unified Extensible Firmware Interface (UEFI)–based Generation 2 (GEN2) virtual machines are not supported.
- Deployment on vThunder Hyper-V, OpenStack, and Google Cloud Platform (GCP) is not supported.

For more information, see the respective vThunder [Installation Guide](#).

### Thunder Container Compatibility

In ACOS 7.0.1, OpenShift 4.16 is introduced for Thunder Container which provides the following scalability enhancements:

- Increases CPU core range from 0–127 to 0–1023.
- Increases maximum thread count from 96 to 256.
- Adds automatic detection of cgroupv2.

For more information, see [cThunder Installation Guide](#).

### Unsupported Features

In ACOS 7.0.1, Internal Thunder Observability Agent (iTOA) and External Thunder Observability Agent (TOA) is not supported.

### Deprecated Features

As ACOS 7.0.1 sets the stage for compatibility with next-generation hardware, and foundation for future AI-based platforms, various legacy features have been deprecated and/or changed.

For more information, see [Changes to Default Behavior](#).

## New Platform Introduced

Introducing 6th Gen Modular Appliances - Thunder 7460S and 7460S-MAX:

- TH7460S: Designed for moderate SSL workloads.
- TH7460S-MAX: Optimized for high-performance SSL workloads.

Both platforms support ADC and CFW-ADC (SSLi + CAP (Cloud Access Proxy) + Firewall + ADC) use cases.

Additionally, the `system forced-group-speed` command is introduced specifically for these platforms. It configures fixed group speeds (1G, 10G, or 25G) on Ethernet ports 01–24, since these ports do not support auto speed detection.

### CLI Configuration

To set the speed for a group of four ethernet ports (quads) simultaneously, use the following command:

```
ACOS(config)# system forced-group-speed <ethXX_to_ethYY> <1g | 10g | 25g>
```

See Also:

- [A10 Thunder Series TH7460S/7460-MAX Installation Reference Guide](#)
- [Platform Compatibility Matrix](#)
- [Global Licensing Manager](#)
- [System Configuration and Administration Guide](#)
- [Command Line Interface Reference](#)
- [Migrating Existing Thunder Platforms to Thunder Modular Platforms](#)

## Enhanced ACOS GUI with TPS Integration

ACOS GUI has improved the user experience with the integration of Threat Protection System (TPS) functionality. As a part of this enhancement, a new **Detector** menu is introduced, that allows you to view the template configurations and other settings of the TPS device.

---

**NOTE:**

- The **Detector** menu is visible only after a valid TPS product license is installed.
  - TPS template configurations and settings can be edited or deleted only using the CLI.
- 

For more information, see *ACOS Online Help*.



©2026 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: [www.a10networks.com/company/legal/trademarks/](http://www.a10networks.com/company/legal/trademarks/).