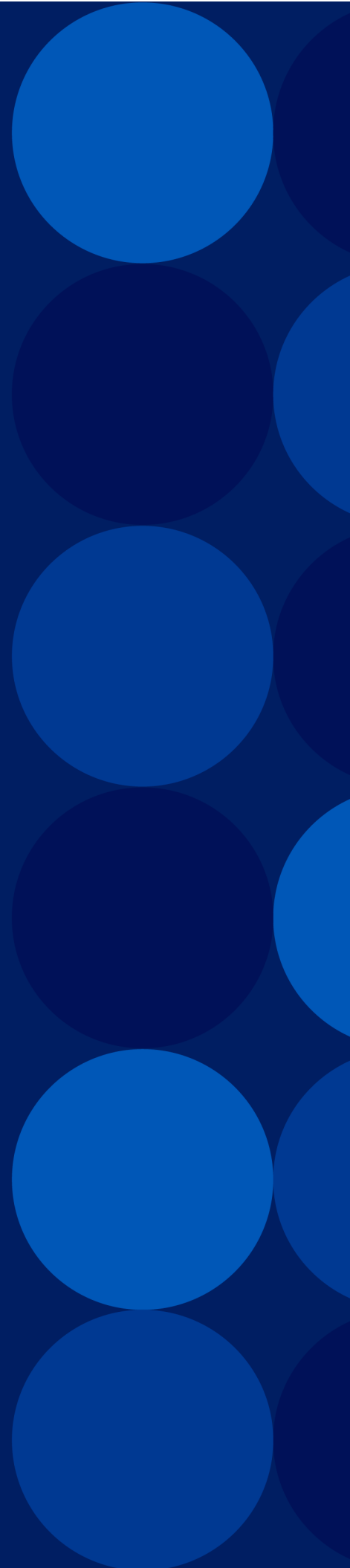


ACOS 7.0.3

Release Notes

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.

Table of Contents

Changes to Default Behavior	7
Default Behavior Changes Introduced in ACOS 7.x.x	8
SNMP High-Availability OIDs Deprecated	8
TLS Protocol and Algorithm Deprecated	8
Disabled Second Management Interface (management2) on Thunder 8665 Platform	9
License Restoration Changes	9
Kerberos RC4-HMAC Encryption Algorithm Deprecated	9
Shared Poll Mode Deprecated	10
SNMP CM Subagent Deprecated	10
Harmony Controller Integration Deprecated	10
Carrier-Grade NAT and Firewall Features Deprecated	11
FIPS Deprecated	11
SSH Insight, Old Software SSL and Nitrox V in SSL Module Deprecated	11
Forward Proxy Bypass Case Insensitive Feature Changes	12
run-hw-diag Command Deprecated	12
System TLS 1.3 Management Feature Deprecated	12
DNSSEC Thales HSM Deprecated	13
DHCP Behavior Changes	13
Import Certificate Changes	13
Feature Preview	14
Platforms Compatibility Matrix	15
Hardware Product Licenses	16
SKUs and Licenses	17
Third-party Licenses for Webroot and ThreatSTOP	18
Modular Licenses	19
Upgrading to ACOS 7.0.3	22
General Guidelines	23

Prerequisites	24
Upgrade Path	25
Upgrade Requirements	25
System Partitions	26
Review Boot Order	29
Disable Shared Polling Mode	32
RHEL Support License Installation	32
Download Software Image	33
Perform a Backup	34
Pre-Upgrade Tasks	36
Upgrade Instructions	40
Post-Upgrade Tasks	44
Upgrade Rollback	47
Upgrading to ACOS 7.0.3 Using aVCS	49
Backing Up the System	50
Full Chassis Upgrade (with or without VRRP-A)	51
Staggered Upgrade (with or without VRRP-A)	52
Manual Upgrade (with VRRP-A)	56
Upgrading Scaleout Cluster from ACOS 5.2.1-Px to 6.x.x	60
Upgrading Scaleout/aVCS Cluster from ACOS 6.0.x to 6.0.7	61
Migrating Existing Thunder Platforms to Thunder Modular Platforms	62
Migrating from Thunder Device (ACOS 6.0.x) to Thunder Modular Device (ACOS 7.0.x)	62
Migrating Configuration Between Thunder Modular Devices (ACOS 7.0.x)	65
Software and Hardware Limitations	67
Software Limitations	68
Downgrading a Scaleout Cluster from ACOS 5.2.x to 4.1.4-GR1-Px	69
SSL Handshake Cannot Happen with Low DH-Param Value	69
Active FTP on vThunder (Virtual Thunder) for Azure	70
Active VM Limitation for Recovering floating-ip	70

aFlex Limitations	70
Application Access Management aFlex Limitations	70
Application Access Management Limitations	71
aXAPI Functionality Limitations	71
Delayed IP Migration on Azure Cloud	71
Form-based Relay Pages Limitations	71
Health Monitor is Displayed Twice in Startup Configuration	72
Incoming Axdebug/Debug Packets Are Not Captured on Azure	73
IPsec VPN Restrictions and Limitations	73
Known GUI Limitations	73
L3V Interface Disabled After Upgrading	74
Local Lagging	74
NAT Pool Statistics Limitation	74
Passive FTP on vThunder for AWS and Azure Does Not Work	74
Server-SSL Template Binding	75
SSLi Single Partition with Explicit Proxy Source NAT	76
VCS on vThunder for AWS and Azure Does Not Work	76
VCS and GSLB Limitations	76
VPN Tunnel Cannot Be Up with SLB Virtual Server Enabled on Azure	77
VRRP-A Configuration Sync Limitation	77
vThunder Cannot Ping Standby Interface in VPPR-A Deployments	77
WAF Template Configuration Missing After Upgrading to 5.x	77
Web-category License Corrupt After Upgrading to 4.x	77
Encrypted Password Configuration Missing After Upgrading to ACOS 7.0.x	78
Hardware Limitations	80
Auto-Negotiation Limitations	80
Combo Console/LOM Interface Requires Splitter Cable	80
Show Interface Media Return "ERROR"	81
Thunder 7650 Limitations	81
Thunder 14045 Limitations	82
Thunder 940/1040 Limitations	83

Thunder 5960 Limitations	83
Transceivers Not Purchased From A10 Networks May Show Error Message	84
Thunder 7460S, 7460S-MAX, and 7465 Platforms Limitation	84
Schema Changes Impacting Backward Compatibility	85
/axapi/v3/cgnv6	86
/axapi/v3/vpn/ike-gateway	86
/axapi/v3/vpn/ike-gateway	87
/axapi/v3/vpn/ike-gateway	87
/axapi/v3/system/session/stats	88
/axapi/v3/slb and /axapi/v3/slb/template	90
/axapi/v3/file and /axapi/v3/import	90
/axapi/v3/interface	91
/axapi/v3/web-category	91
/axapi/v3/slb	92
/axapi/v3/glid	93
/axapi/v3/system/glid	94
/axapi/v3/router	97
/axapi/v3/router/isis	98
Various Schema Changes	99
Platform Migration	100
Restore from a Backup	100
A10 Networks Security Advisories	106
APPENDIX Basic Functionality Testing	107

Changes to Default Behavior

This section highlights the major changes to the default or existing behavior in the ACOS 5.x and above releases as compared to earlier releases.

The following topics are covered:

Default Behavior Changes Introduced in ACOS 7.x.x	8
SNMP High-Availability OIDs Deprecated	8
TLS Protocol and Algorithm Deprecated	8
Disabled Second Management Interface (management2) on Thunder 8665 Platform	9
License Restoration Changes	9
Kerberos RC4-HMAC Encryption Algorithm Deprecated	9
Shared Poll Mode Deprecated	10
SNMP CM Subagent Deprecated	10
Harmony Controller Integration Deprecated	10
Carrier-Grade NAT and Firewall Features Deprecated	11
FIPS Deprecated	11
SSH Insight, Old Software SSL and Nitrox V in SSL Module Deprecated	11
Forward Proxy Bypass Case Insensitive Feature Changes	12
run-hw-diag Command Deprecated	12
System TLS 1.3 Management Feature Deprecated	12
DNSSEC Thales HSM Deprecated	13
DHCP Behavior Changes	13
Import Certificate Changes	13

Default Behavior Changes Introduced in ACOS 7.x.x

SNMP High-Availability OIDs Deprecated

Starting from the ACOS 7.0.3 release, all high-availability (HA) related OIDs under axHA (1.3.6.1.4.1.22610.2.4.3.17) in the A10-AX-MIB have been deprecated. Instead, use axVRRP OIDs for HA notifications.

See Also:

- [SNMP MIB Reference](#)

TLS Protocol and Algorithm Deprecated

Starting with the ACOS 7.0.3 release, support for certain legacy SSL/TLS protocols and cryptographic algorithms has been deprecated based on the TLS library in use. Before upgrading, review existing SSL/TLS configurations to ensure that no services depend on deprecated protocols, cipher suites, certificates, or hash algorithms.

The following protocols and algorithms are deprecated for TLS Library v3:

- SSLv3
- TLS 1.0
- TLS 1.1
- SHA 1
- MD5

The following protocols are deprecated for Default TLS Library:

- SSLv3
- TLS 1.0

See also:

[Application Delivery Controller Guide](#)

Disabled Second Management Interface (management2) on Thunder 8665 Platform

In earlier releases, the Thunder 8665 platform included a second management interface (management2) which provided redundancy for the primary management interface.

Starting from the ACOS 7.0.3 release, the second management interface (management2) is disabled on the Thunder 8665 platform. The primary management interface or the data plan interfaces may be used for management access after upgrading.

License Restoration Changes

Starting from the ACOS 7.0.2, the license file is not restored from backup during a system restore. After performing a system reset or restore, you must reinstall or re-request the license from GLM to reactivate licensed features.

See Also

- [System Configuration and Administration Guide](#)

Kerberos RC4-HMAC Encryption Algorithm Deprecated

ACOS supports Kerberos authentication for Application Access Management (AAM). In addition, AAM also supports Windows Kerberos authentication.

Starting with the ACOS 7.0.2 release, the `RC4-HMAC` Kerberos encryption algorithm has been deprecated due to its known security vulnerabilities. To strengthen security, the following Kerberos AES encryption algorithms have been implemented for keytab generation in WIA:

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

This enhancement improves the Kerberos keytab generation process by supporting these more secure encryption algorithms.

For detailed configuration and usage, refer to the [Application Access Management Guide](#).

Shared Poll Mode Deprecated

With ACOS 7.0.1 release, the shared polling mode is deprecated across cThunder and vThunder deployments. To align with the new RHEL platform architecture and to optimize packet processing performance, the shared poll mode is no longer supported in ACOS 7.0.1 and later versions.

NOTE: If shared poll mode is enabled on the device before upgrading to ACOS 7.0.1 or later, the upgrade will fail. A compliance error will be logged to disable this feature before attempting an upgrade.

SNMP CM Subagent Deprecated

The Simple Network Management Protocol (SNMP) subagent `a10cmsubagent` and its associated MIBs under `acosRootStats` (1.3.6.1.4.1.22610.2.4.10) and `acosRootOper` (1.3.6.1.4.1.22610.2.4.11) have been deprecated and are no longer supported.

Harmony Controller Integration Deprecated

Starting from the ACOS 7.0.1 release, integration of Harmony Controller is no longer supported.

Instead, ACOS 7.0.1 supports integration of A10 Control (formerly known as Harmony Controller), starting from version 1.1. Additionally, configuration or registration of the ACOS devices can be performed using either the A10 Control GUI or the ACOS CLI.

NOTE: A10 Control configuration is not supported via the ACOS GUI.

For more information, see [Remove Harmony Controller Configuration](#).

Carrier-Grade NAT and Firewall Features Deprecated

Starting from the ACOS 7.0.1 release, the following features of Carrier-Grade NAT and Firewall are deprecated:

- **Stateful Firewall** - The CGNv6 stateful-firewall functionality is deprecated and replaced by the Gi Firewall functionality that can be enabled via the CFW license.
- **Firewall and CGNv6 radius Server Commands** - The `cgnv6 lsn radius server` and `fw radius server` commands are deprecated and replaced by the `system radius server` command. If these deprecated commands are used in the existing configurations, they must be replaced with the `system radius server` command prior to upgrading to ACOS 7.0.1 release. If not, these commands will be rejected on booting up with ACOS 7.0.1 release and an error message will be logged.

FIPS Deprecated

Starting from the ACOS 7.0.1 release, Federal Information Processing Standards (FIPS) are no longer supported on A10 Thunder series devices.

SSH Insight, Old Software SSL and Nitrox V in SSL Module Deprecated

In the 6.x and earlier releases, the 4th generation and below platforms supported Nitrox V (N5) on the ACOS. You could switch the SSL module modes related to old software SSL, Nitrox V and SSL client authentication using `direct-client-server-auth` on the ACOS CLI.

Starting with the ACOS 7.0.1 release, only Thunder platforms from 5th generation and above are supported. These platforms do not support Nitrox V (N5) hardware acceleration.

As a result, all features associated with Nitrox V have been deprecated. The following changes apply to both SSL and SSLi deployments:

- The N5-old and N5-new SSL module commands are deprecated.

The previous software SSL module command has been replaced with software-TLS13 module. The term software-TLS13 has been removed, it refers to the software SSL.

- Direct client-server authentication is no longer supported.
- SSH Insight (SSHi) is deprecated.

Forward Proxy Bypass Case Insensitive Feature Changes

In the 6.x and earlier versions, the `forward-proxy-bypass case-insensitive` CLI command disables case sensitivity for matching strings in the SSLi bypass. However, this change did not affect the `forward-proxy-bypass class-list` or the `forward-proxy-bypass exception-class-list` CLI commands.

Starting with 7.0.1 release, `forward-proxy-bypass case-insensitive` applies to the `forward-proxy-bypass class-list` and `forward-proxy-bypass exception-class-list`.

NOTE: Ensure all entries in the class list are defined in lowercase to enable case insensitive matching.

run-hw-diag Command Deprecated

Starting with ACOS 7.0.3, the `run-hw-diag` command, which was used to retrieve hardware diagnostics information on a serial console, is no longer supported on ACOS devices and has been removed.

System TLS 1.3 Management Feature Deprecated

In the 6.x and earlier releases, you could enable or disable TLS 1.3 support globally on the ACOS management interface using ACOS CLI and GUI.

Starting with 7.0.1 release, the `system tls-1-3-mgmt` CLI command has been deprecated or removed from ACOS CLI and GUI. By default, ACOS GUI interface support both the TLS 1.2 and 1.3 options.

DNSSEC Thales HSM Deprecated

Starting from the ACOS 7.0.1 release, ThalesHSM is deprecated and only software based DNSSEC key generation and storage will be used.

Thales SSL Hardware Security Module (HSM) device support is proprietary hardware based DNSSEC encryption and key management. As a result, all the commands and configurations related to thalesHSM are deprecated.

DHCP Behavior Changes

ACOS supports enabling Dynamic Host Configuration Protocol (DHCP) to configure multiple IP addresses on an Ethernet data interface using the `ip address dhcp` command.

Starting with ACOS 7.0.1, the DHCP implementation has been updated due to a version change in the underlying 'dhclient' utility - from version 4.2 in 6.0.x to version 4.4 in 7.0.1. As a result of this update, the DHCP timeout is now set to 60 seconds by default.

Import Certificate Changes

In 6.x and prior releases, ACOS allowed importing PFX (Personal Information Exchange) certificate without enforcing strict validation of cryptographic standards.

Starting from the ACOS 7.0.1 release, stricter validation has been implemented to improve the security. Hence, importing certificates that use old versions or weak algorithms will show backend error messages.

Feature Preview

The following change is planned for a future ACOS release. This information is provided for awareness only and is subject to change.

- After ACOS 7.0.2, the `encrypt` option under the `backup system` command is expected to become the default method for backing up system files, ensuring stronger security by default.

Platforms Compatibility Matrix

For the latest updates on the supported platforms, see [Platform Compatibility Matrix](#).

Hardware Product Licenses

The following topics are covered:

SKUs and Licenses	17
Third-party Licenses for Webroot and ThreatSTOP	18
Modular Licenses	19

SKUs and Licenses

This section describes product SKUs for A10 Thunder Series hardware devices and product licenses for vThunder (Virtual Thunder) devices.

Hardware devices **purchased before February 2016** have no concept of product SKU. Hardware devices **purchased after February 2016** are identified by a product SKU.

vThunder (Virtual Thunder) devices prior to Release 4.1.0 utilized bandwidth licenses; licenses introduced starting from 4.1.0 involve both product and bandwidth usage.

The following [Table 1](#) summarizes the hardware device product SKUs and features available in each product:

Table 1 : ACOS 4.1.0 Hardware Product SKU Matrix

Device	SKU	Features Available Before 4.1.0	Features Available from 4.1.0
A10 Thunder Series hardware device	CGN	CGN, ADC, and SSLi	CGN and ADC
	ADC	ADC, CGN and SSLi	ADC and CGN
	SSLi	SSLi, ADC and CGN	SSLi and related components
	CFW	N/A	CFW, SSLi, ADC, and CGN

The following [Table 2](#) summarizes the vThunder (Virtual Thunder) and Bare Metal product licenses and contents of each product:

Table 2 : ACOS 4.1.0 Product License Matrix

Device	License	Features Available Before 4.1.0	Features Available from 4.1.0
vThunder (Virtual Thunder) device	CGN	CGN and ADC	CGN and ADC
	ADC	ADC and CGN	ADC and CGN
	SSLi	N/A	SSLi and related components
	CFW	N/A	CFW, SSLi, ADC, and CGN

Table 2 : ACOS 4.1.0 Product License Matrix

Device	License	Features Available Before 4.1.0	Features Available from 4.1.0
Bare Metal	CGN	N/A	CGN and ADC
	ADC	N/A	ADC and CGN

For more information about obtaining your product license, refer to your specific vThunder (Virtual Thunder) or Bare Metal installation guide, available on the following [Documentation Portal](#).

Third-party Licenses for Webroot and ThreatSTOP

Third-party licenses for Webroot and ThreatSTOP are also available; contact your local A10 Networks representative for more information.

The following [Table 3](#) summarizes the availability of Webroot and ThreatSTOP licenses for hardware product SKUs:

Table 3 : Webroot and ThreatSTOP Availability Matrix for Hardware

Device	SKU	Webroot and ThreatSTOP Availability
A10 Thunder Series hardware device	CGN	None
	ADC	ThreatSTOP
	SSLi	Webroot and ThreatSTOP
	CFW	Webroot and ThreatSTOP

The following [Table 4](#) summarizes the availability of Webroot and ThreatSTOP licenses for vThunder (Virtual Thunder) and Bare Metal devices:

Table 4 : Webroot and ThreatSTOP Availability Matrix for vThunder (Virtual Thunder) and Bare Metal

Device	License	Webroot and ThreatSTOP Availability
vThunder (Virtual Thunder) device licenses	CGN	None
	ADC	ThreatSTOP
	SSLi	Webroot and ThreatSTOP
	CFW	Webroot and ThreatSTOP
Bare Metal licenses	ADC	ThreatSTOP
	CGN	None

Modular Licenses

[Table 5](#) lists the modular licensing support matrix.

The Modular license (also known as software-driven license) provides the flexibility to select the license based on the allocation of the following device parameters:

- Number of CPU Cores
- Number and type of ports
- Bandwidth
- Memory
- SSL Chipset: Software Only / QAT / N5

These hardware parameters drive the device performance characteristics such as the number of Layer 4/Layer 7 sessions, the number of Connections-Per-Second (CPS), the Packets-Per-Second (PPS), throughput, and so on.

Table 5 : Modular Licenses Support Matrix

Thunder Devices	Modular Licensing Support	Minimum Release
Non-FTA/non-FPGA		
Thunder 5960	✓	6.0.4

Table 5 : Modular Licenses Support Matrix

Thunder Devices	Modular Licensing Support	Minimum Release
Thunder 3350(S)	✓	6.0.4
Thunder 3350(E)		
Thunder 3350	✓	6.0.4
Thunder 3040(S)		
Thunder 1060/1060(C)	✓	6.0.4
Thunder 1040-F		
Thunder 1040(S) (with at least 32GB of Hard Disk)		
Thunder 1040 (with at least 32GB of Hard Disk)		
Thunder 940 (with at least 32GB of Hard Disk)		
FTA/FPGA		
Thunder 14045		
Thunder 8665(S)		
Thunder 7655(S)	✓	6.0.4
Thunder 7650		
Thunder 7445		
Thunder 7440(S)-11		
Thunder 7440(S)		
Thunder 7460(S)	✓	7.0.1
Thunder 7460(S)-MAX	✓	7.0.1

Table 5 : Modular Licenses Support Matrix

Thunder Devices	Modular Licensing Support	Minimum Release
Thunder 7465	✓	7.0.2
Thunder 6655(S)	✓	6.0.4
Thunder 6440		
Thunder 6440(S)		
Thunder 5845		
Thunder 5840(S)-11		
Thunder 5840(S)	✓	6.0.4
Thunder 5540		
Thunder 5440(S)		
Thunder 4440(S)		

Upgrading to ACOS 7.0.3

This section provides detailed instructions for upgrading from ACOS 5.x to the latest version. It includes information on pre-upgrade preparations, the upgrade procedure, post-upgrade tasks, troubleshooting tips, and additional resources.

The Thunder device is provided with preinstalled ACOS software along with the purchased license. When you power ON the device, it boots up with the preinstalled software. To access the latest new features and software fixes as they become available, you must upgrade the ACOS software.

If you are a new ACOS user, check the following documentation on the [A10 Documentation Site](#):

- For instructions on installing new hardware, see [Thunder Physical Appliance](#).
- For instruction on installing vThunder, see [Thunder Virtual Appliance](#).
- For instructions on installing cThunder, see [Thunder Container](#).
- For instructions on installing ACOS on Bare Metal, see [Bare Metal](#).
- For instructions on acquiring a product license, see [Global Licensing Manager](#).
- For initial configuration instructions and quick processes handbook, see [Quick Start Guide](#).

NOTE: The sections in this document are not applicable for TPS. For TPS upgrade instructions, refer to the *TPS Upgrade Guide*.

The following topics are covered:

General Guidelines	23
Prerequisites	24
Pre-Upgrade Tasks	36
Upgrade Instructions	40
Post-Upgrade Tasks	44
Upgrade Rollback	47

General Guidelines

Consider the following recommendations before upgrading the ACOS device:

- Test the upgrade procedure in a non-production environment to ensure its effectiveness.
- ACOS device is upgraded by copying the software image to your device or other system on your local network and then upgrading the device using the CLI or GUI instructions.
- Regardless of whether you have an ADC, CGN, or TPS, a single software image is used to upgrade your ACOS device. However, ensure that the correct product license is obtained and activated.

NOTE: For TPS upgrade instructions, see *TPS Upgrade Guide*.

- Before starting an SCP-based upgrade with Duo MFA, ensure the following:
 - Duo Unix is properly configured on the authentication server. For more information, [Duo Unix Get Started](#) and [Enable Password Login](#).
 - An SSH/SCP login is attempted to verify whether the authentication method requires a direct passcode, push notification, or SMS passcode.
- During the reboot, the system performs a full reset and will be offline. The actual duration may vary depending on the system parameters.
- Obtain GLM credentials to access A10 Networks [Support](#) and [Documentation](#) Portals. GLM is a self-service portal, and the primary customer contact for A10 Networks can add access to GLM.

Unsupported Upgrade

- The 4th Generation and below hardware platforms cannot be upgraded to ACOS 7.x.x version.
- The Web Application Firewall (WAF) is no longer supported in the ACOS 6.x and above versions. Hence, all WAF configurations will be removed after the upgrade. For more information, see [Web Application Firewall Changes](#).
- The ADC with VRRP-A (traffic distribution with VRID) on the multi-PU platform is no longer supported in the ACOS 6.x and above versions. Hence, all the related

configurations will be removed after the upgrade. For more information, see [ADC Multi-PU Deployment with VRRP-A Changes](#).

Prerequisites

This section outlines essential information that you should know before proceeding with the upgrade process.

Table 6 : Prerequisite Tasks

Tasks	Refer
Check the compatibility of the platform with the supported release version.	Hardware Platforms Support
Check the availability of SKUs or product licenses.	Hardware Product Licenses
Review the ACOS Upgrade path.	Upgrade path
Check the CPU and memory requirements.	Upgrade Requirements
Understand the ACOS partitions and how to take a backup.	System Partitions
Understand how ACOS determines the boot order.	Review Boot Order
Disable Shared Polling Mode	Disable Shared Polling Mode
Install RHEL Support License	RHEL Support License Installation
Preserve the TACACS configuration during upgrade (Optional)	Encrypted Password Configuration Missing After Upgrading to ACOS 7.0.x
Download the ACOS software image.	Download Software Image
Take the system backup.	Perform a Backup
Carefully review the known issues, limitations, and changes to default behavior.	Documentation Site

NOTE: Schedule a maintenance window for the upgrade, taking into account the potential downtime required. Communicate this schedule to relevant stakeholders.

Upgrade Path

This section helps you in identifying the upgrade paths to the latest versions of ACOS releases. Some versions require intermediate upgrades (first hop) before proceeding to the final target version (second or third hop).

Table 7 : ACOS Upgrade Path

Existing Version	First Hop	Second Hop	Third Hop
5.1.x	5.1.x to 5.2.x	5.2.x to 6.x	6.x to 7.0.x
5.2.1-Px	5.2.1-Px to 6.x	6.x to 7.0.x	
6.x	6.x to 7.0.x		

Upgrade Requirements

The minimum system requirements for upgrading to ACOS 7.0.3 are as follows:

- For hardware Thunder platforms: Only 5th and 6th generation platforms can be upgraded
- For Virtual Thunder and Bare Metal platforms:
 - Minimum CPUs: 4
 - Minimum memory: 16GB
 - Minimum disk space: 128GB
 - Configured memory on the device should be at least a multiple of 2GB per CPU.

System Partitions

Each ACOS device contains a single shared partition. By default, this is the only partition on the device and cannot be deleted. If there are no additional partitions on the device, all configuration changes take place in the shared partition.

You can save the configuration of these partitions to either the default startup-config, the current, or a new configuration profile. ACOS provides different options for saving the configuration, depending on the configuration profile and the partition being saved to.

You can use one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

1. Log in to ACOS CLI using your credentials.
2. To view the number of partitions, use the `show partition` command.

```
Total Number of active partitions: 2
Partition Name  Id      L3V/SP    Parent L3V  App Type  Admin Count
-----
---
LV-1           3       L3V      -          ADC       0
SP-1           4       L3V      -          ADC       0
```

3. To view the partitions configuration, use the `show partition-config all` command.

```
ACOS# show partition-config all
```

```

!Current configuration: 278 bytes
!Configuration last updated at 08:30:06 GMT Wed Dec 6 2023
!Configuration last saved at 17:39:49 GMT Mon Dec 4 2023
!64-bit Advanced Core OS (ACOS) version 5.2.1-P8, build 9 (Nov-09-
2023,05:54)
!
multi-config enable
!
system promiscuous-mode
!
partition LV-1 id 3 application-type adc
!
partition SP-1 id 4 application-type adc
!
ve-stats enable
!
!
interface management
.....

```

4. To save the partition configuration, use the `write memory` command. [Table 8](#) summarizes the `write memory` command usage for additional information.

Table 8 : Write Memory Command Usage

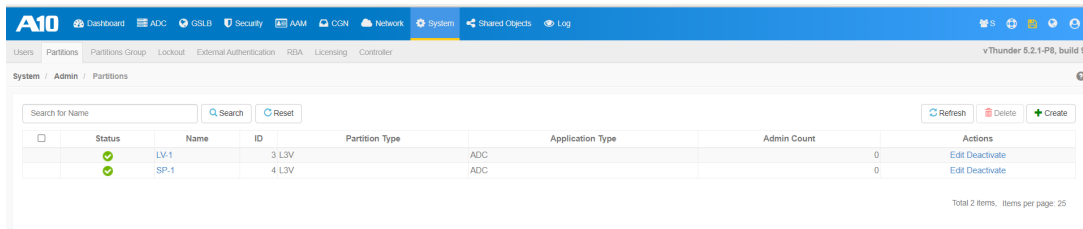
Command	Descriptions
<code>write memory</code>	Save the running configuration to the startup-config or the current profile in the current partition.
<code>write memory all-partitions</code>	<p>Save the running configuration to their respective startup-config or their current profiles of all partitions.</p> <p>NOTE: <u>This is the commonly used command because it works regardless of whether you have the partition or not.</u></p>
<code>write memory</code>	Save the running configuration to the new profile in

Table 8 : Write Memory Command Usage

Command	Descriptions
<code><profile-name></code>	the current partition.
<code>write memory <profile-name> all-partitions</code>	Save the running configuration to the new profile of all partitions.

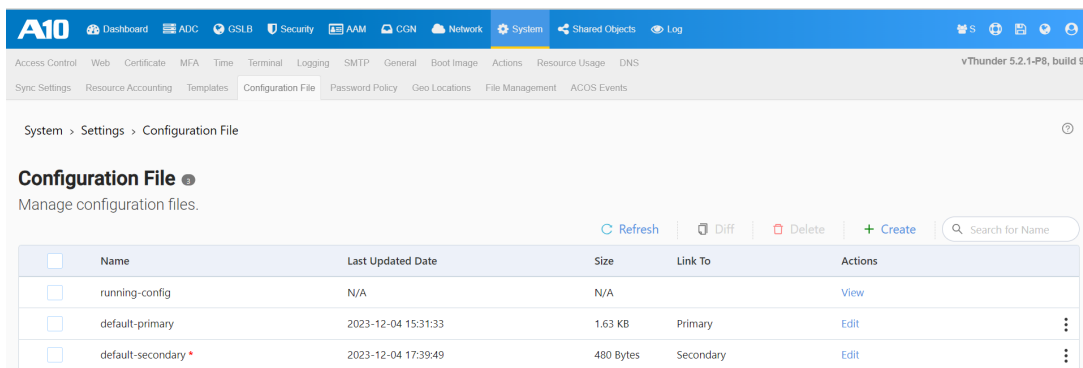
GUI Configuration

1. Log in to the ACOS Web GUI using your credentials.
2. To view the partitions in your system, navigate to **System >> Admin >> Partitions**.



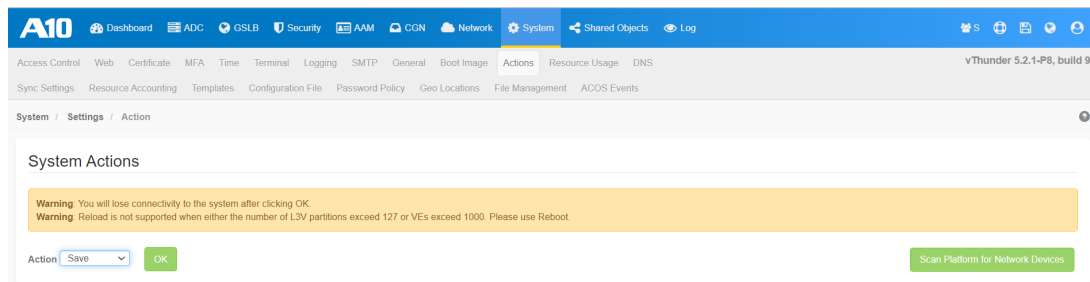
Status	Name	ID	Partition Type	Application Type	Admin Count	Actions
✓	LV-1	3 L3V		ADC	0	Edit Deactivate
✓	SP-1	4 L3V		ADC	0	Edit Deactivate

3. To view the configuration profiles of the partitions, navigate to **System >> Settings >> Configuration File**.



Name	Last Updated Date	Size	Link To	Actions
running-config	N/A	N/A		View
default-primary	2023-12-04 15:31:33	1.63 KB	Primary	Edit
default-secondary*	2023-12-04 17:39:49	480 Bytes	Secondary	Edit

4. To save the partition configuration, navigate to **System >> Settings >> Action**.



5. Select the **Save** option from the **Action** drop-down list.
6. Repeat the same steps by switching to all the partitions from top-right corner **Partition** icon.
7. Click **OK**.

See Also

- For more details on the startup-config and configuration profiles, see "Understanding Configuration Profiles" in the *System Configuration and Administration Guide*.
- For more details on partitions, see *Application Delivery Partition Guide*.
- For more details on all the commands, see *Command Line Interface Reference*.
- For more details on all the GUI options, see *Online Help*.

Review Boot Order

This section describes general guidelines on how ACOS selects the boot image.

Each ACOS device contains multiple locations where software images can be placed. [Table 10](#) provides an overview of the general upgrade process.

- When a new image is loaded onto the ACOS device, select the image device (disk or CF) and the area (primary or secondary) on the device.
- When the device is powered ON or reboot the ACOS device, it always attempts to boot from the disk, using the image area specified in the configuration (primary disk, by default). If a disk fails, the device attempts to boot from the same image area on the backup disk (if applicable to the device model).

Change the boot order when the new image is uploaded to an image area other than the first image area.

NOTE: A10 Networks recommends installing the new image into just one disk image area, either primary or secondary. And retain the old image in the other area. This helps to restore the system in case a downgrade is necessary or if an issue occurs while rebooting the new image.

Table 9 : Generic Upgrade Process

System	Partition 1	Upgrade	Partition 2
New System	Active	NA	Inactive
1st Upgrade	Active	→	Inactive
2nd Upgrade	Inactive	←	Active
Next Upgrade	Active	→	Inactive
Next Upgrade	Inactive	→	Active

You can follow one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

1. Log in to ACOS CLI using your credentials.
2. To view the boot order, use the `show bootimage` command.

```
ACOS(config)#show bootimage
(* = Default)
Version
-----
Hard Disk primary      5.2.1.45
Hard Disk secondary    5.2.1-P8.9 (*)
```

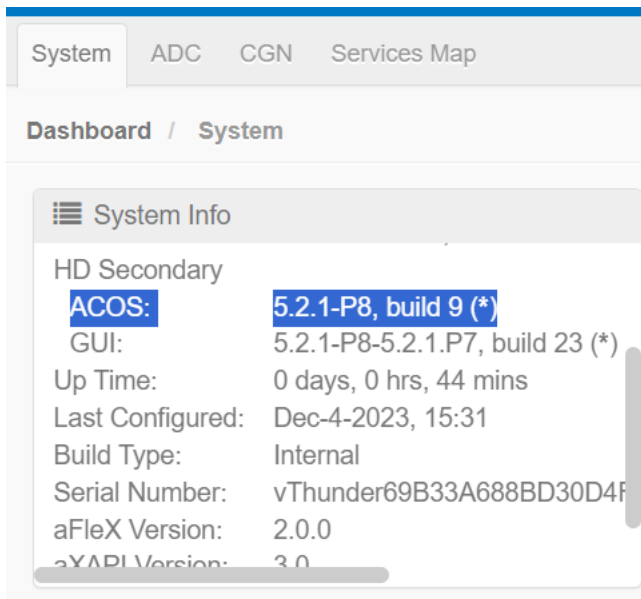
3. To change the boot order, use the `bootimage` command. [Table 9](#) summarizes the `bootimage` command usage.

Table 10 : bootimage Command Usage

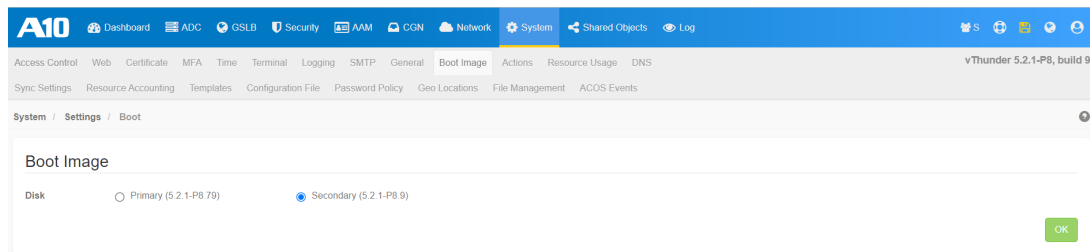
Command	Descriptions
<code>bootimage hd pri</code>	Boot the ACOS device from the primary hard disk the next time the device is rebooted.
<code>bootimage hd sec</code>	Boot the ACOS device from the secondary hard disk the next time the device is rebooted.
<code>bootimage cf pri</code>	Boot the ACOS device from compact flash (cf) and boot the image from the cf primary. NOTE: <u>The cf is used only if the hard disk is unavailable.</u>

GUI Configuration

1. Log in to ACOS Web GUI using your credentials.
2. To view the boot order, navigate to **Dashboard >> System >> System Info**. The default system boot order is displayed with (*).



3. To change the boot order, navigate to **Dashboard >> Settings >> Boot Image**.



4. Choose the boot order and click **OK**.

See Also

- For more details on storage areas in ACOS devices, see "Storage Areas" in the *System Configuration and Administration Guide*.
- For more details on all the commands, see *Command Line Interface Reference*.
- For more details on all the GUI options, see *Online Help*.

Disable Shared Polling Mode

Starting with ACOS 7.0.1, the shared polling mode feature is deprecated. Hence, the shared polling mode must be disabled before upgrading to ACOS 7.0.1 using the following command:

To disable it, execute the following command on your current system:

```
ACOS (config) # system shared-poll-mode disable
```

NOTE: If the shared polling mode is not disabled, the upgrade will fail. A compliance error will be logged, instructing you to disable this feature before attempting an upgrade.

For more information, see [Shared Poll Mode Deprecated](#).

RHEL Support License Installation

Starting with ACOS 7.0.x, a valid Red Hat (RHEL Support) license is mandatory for all new ACOS installations and upgrades. This is due to the platform operating system upgrade from CentOS 7.9 (Community Enterprise Operating System) to Red Hat Enterprise Linux (RHEL). For more information, see [RHEL Platform Support](#).

You can obtain a valid RHEL support license from GLM and install it on the system before upgrading to ACOS 7.0.x.

NOTE: Separate licenses are available for Thunder and vThunder platforms. If RHEL license is not installed on the system, the upgrade will fail.

For license installation instructions, see [Global License Manager User Guide](#).

Download Software Image

ACOS has two device types: FTA and non-FTA. Depending on the device or hardware type, you need to determine the correct software image. All vThunder devices use the non-FTA version.

You can follow the instructions below:

Check the Device Type

Before downloading the image, you need to determine if your device is FTA or non-FTA.

CLI Configuration

Log in to ACOS CLI using your credentials and run the `show hardware` command.

```
ACOS# show hardware | inc FPGA
```

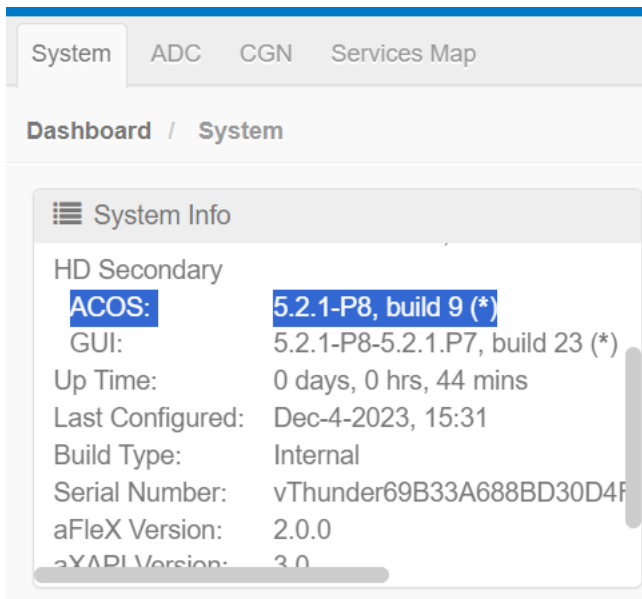
If a response is shown, the device has an FTA.

```
FPGA          : 4 instance(s) present
```

If no response is shown, the device does not have an FTA.

GUI Configuration

Log in to ACOS Web GUI using your credentials and navigate to **Dashboard >> System >> System Info**.



Download the Software Image

1. Log in to [A10 Networks Support](#) using your GLM credential.
2. Download the ACOS upgrade package as specified below:
 - For FTA enabled platforms, use the image with the file name: ACOS_FTA_<version>.upg
 - For non-FTA enabled platforms (including vThunder), use the image with the file name: ACOS_non_FTA_<version>.upg

Perform a Backup

It is essential to perform a complete backup of your data, including configuration settings, databases, and any customizations. This backup will prove invaluable in case of unexpected issues during the upgrade, and you want to restore it.

You can follow one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

1. Log in to the ACOS CLI using your credentials.
2. Create a backup of the system (startup-config file, aFlex scripts, and SSL certificates and keys). In this example, the backup is created on the remote server using SCP.

```
ACOS(config)# backup system
scp://exampleuser@192.168.3.3/home/users/exampleuser/backups/backupfile.tar.gz
```

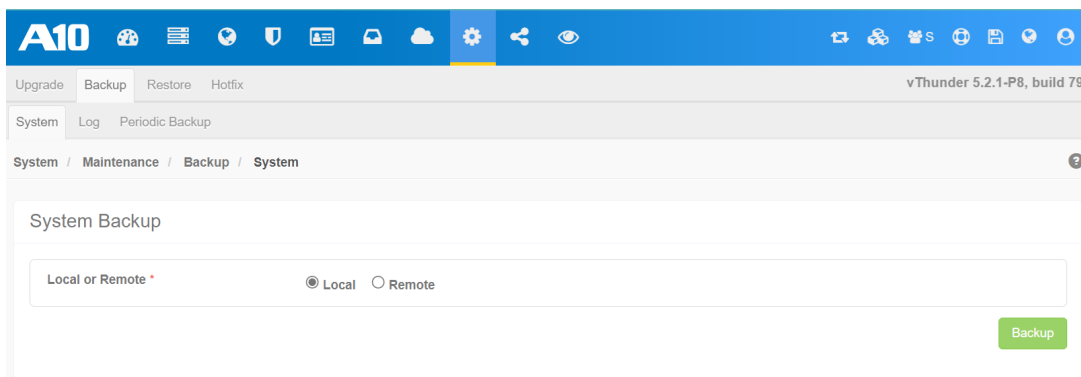
3. Create a backup of the log entries in the syslog buffer and set a periodic (daily) backup.

The connection to the remote server will be established using SCP on the management interface (`use-mgmt-port`).

```
ACOS(config)# backup log period 1 use-mgmt-port
scp://exampleuser@192.168.3.3/home/users/exampleuser/backups/backuplog.tar.gz
```

GUI Configuration

1. Log in to ACOS Web GUI using your credentials.
2. Navigate to **System >> Maintenance >> Backup**.



3. Select one of the following tabs:
 - *System* — In this tab, you can perform an immediate backup of the configuration file (s), aFlex scripts, and SSL certificates and keys.
 - *Log* — In this tab, you can perform an immediate backup of the log entries in the ACOS device's syslog buffer (along with any core files on the system).

- *Periodic Backup* — In this tab, you can perform a scheduled backup of either the system or log files.
4. Choose if you want to back up the files on the local or remote location.
 5. Enter the host and location, and the protocol used to access the host.
 6. Click **Backup**.

See Also

- For more details on system backup, see *System Administrators and Configuration Guide*.
- For more details on restoring backup, see [Restore from a Backup](#).
- For more details on all the commands, see *Command Line Interface Reference*.
- For more details on all the GUI options, see *Online Help*.

Pre-Upgrade Tasks

Before upgrading ACOS software, you must perform some basic checks. Keep the below information handy to ensure a seamless upgrade.

You can follow one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

Log in to ACOS CLI using your credentials and perform the following checks:

Validate the Platform Compatibility

Check if you have vThunder or Thunder device using the following command:

```
ACOS# show hardware | inc Gateway
```

If the device is vThunder, the following response is displayed.

```
Thunder Series Unified Application Service Gateway vThunder
```

If the device is Thunder, the following response is displayed.

Thunder Series Unified Application Service Gateway **TH5840S**

NOTE: Make sure that the device is 4th generation or later platform.

Check the Software Version

Check if the current software version is 5.x using the following command:

```
ACOS> show version | inc ACOS
64-bit Advanced Core OS (ACOS) version 5.2.1-p5, build 114 (Jul-14-
2022,05:11)
```

Check the Disk Space

Check the disk space and verify minimum disk requirements using the following command:

```
ACOS(config)# show disk
Total(MB)      Used(MB)      Free(MB)      Usage
-----
20480         10421         10058         50%
Hard Disk Primary Status : OK
```

Check the Memory Usage

Check the memory usage using the following command:

```
ACOS(config)#show memory | inc Memory
Memory: 8127392      4742619      3384773      58.30%
```

Check the System Boot Order

Check the default system boot order to determine the new destination using the following command:

```
ACOS(config)#show bootimage | inc *
Hard Disk primary      5.2.1-p5.114 (*)
```

Save the Partition Configuration

Save all primary, secondary, and partition configurations using the following command:

```
ACOS(config)# write memory all-partitions
Building configuration...
Write configuration to default primary startup-config
Write configuration to profile "pri_default" on partition GSLB
[OK]
```

Perform Backup

See **CLI Configuration** steps in [Backing Up the System](#).

Perform Basic Testing

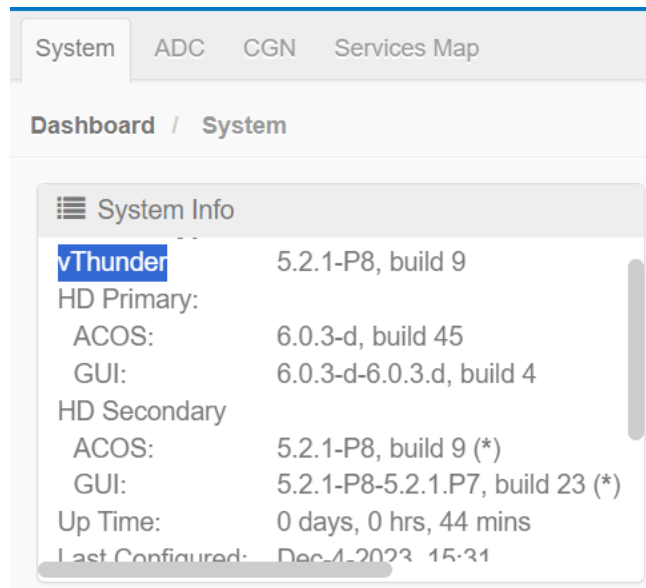
Perform [Basic Functionality Testing](#) to collect system and/or product information.

GUI Configuration

Log in to ACOS Web GUI using your credentials and perform the following checks:

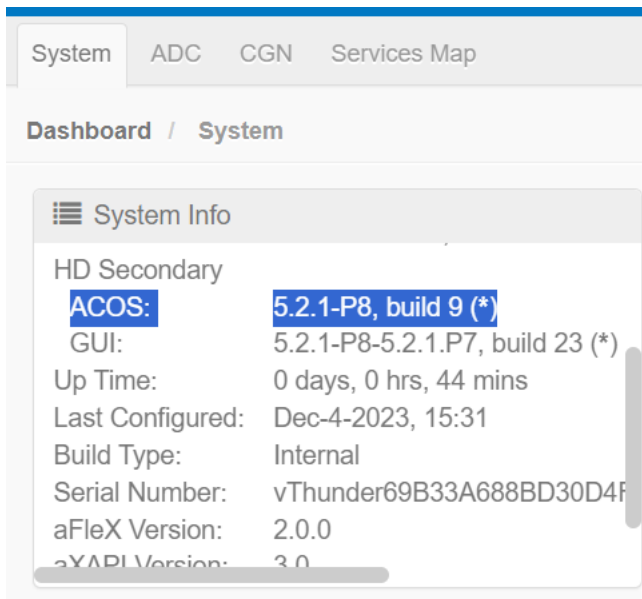
Validate the Platform Compatibility

Navigate to **Dashboard >> System >> System Info**.



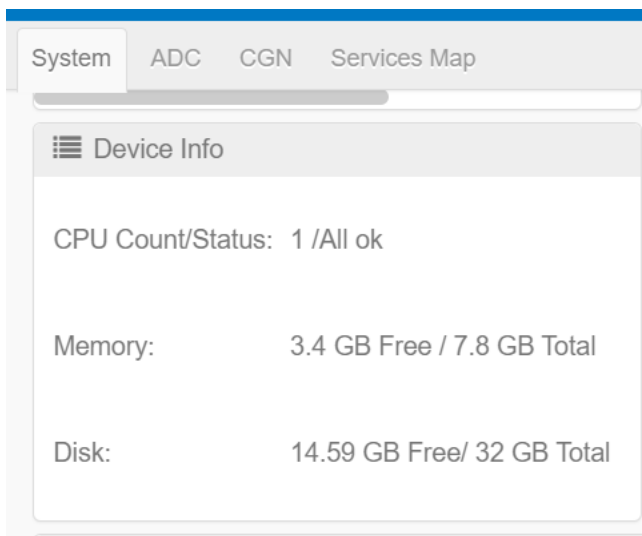
Check the Software Version

Navigate to **Dashboard >> System >> System Info**.



Check the Disk Space and Memory Usage

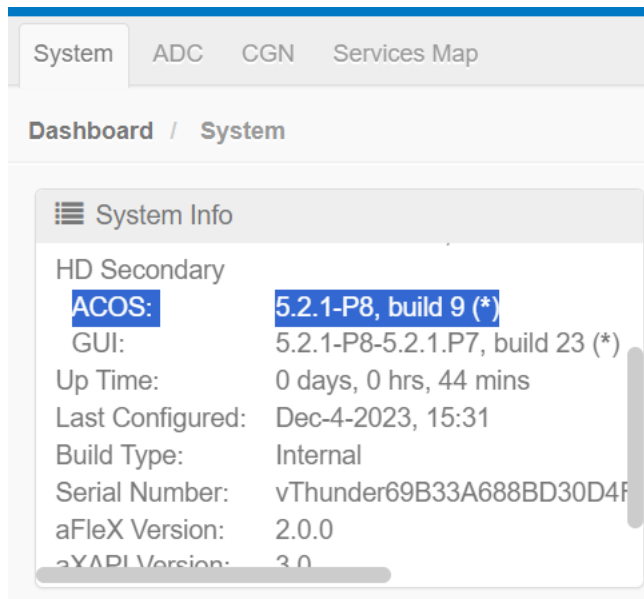
Navigate to **Dashboard >> System >> Device Info**.



Check the System Boot Order

Navigate to **Dashboard >> System >> System Info**.

The default system boot order is displayed with (*).



Perform Backup

Navigate to **System >> Maintenance >> Backup**.

See **GUI Configuration** instructions in [Perform a Backup](#).

Perform Basic Testing

Perform [Basic Functionality Testing](#) to collect system and/or product information.

See Also

- For more details on all the commands, see *Command Line Interface Reference*.
- For more details on all the GUI options, see *Online Help*.

Upgrade Instructions

This section describes the ACOS upgrade instructions using CLI and GUI. The upgrade instruction applies to FTA platforms, non-FTA platforms, and non-aVCS environments.

Before you proceed with upgrade, make sure to complete the [Pre-Upgrade Tasks](#).

You can follow one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

1. Log in to ACOS CLI using your credentials.
2. Upgrade the ACOS device to the inactive partition.

To upgrade from primary hard disk to secondary:

- On an FTA device:

```
ACOS-7-x(config)# upgrade hd sec show-percentage  
scp://admin@2.2.2.2/images/ACOS_FTA_<version>.upg
```

- On a non-FTA device:

```
ACOS-7-x(config)# upgrade hd sec show-percentage  
scp://admin@2.2.2.2/images/ACOS_non-FTA_<version>.upg
```

To upgrade from secondary hard disk to primary:

- On an FTA device:

```
ACOS-7-x(config)# upgrade hd pri show-percentage  
scp://admin@2.2.2.2/images/ACOS_FTA_<version>.upg
```

- On a non-FTA device:

```
ACOS-7-x(config)# upgrade hd pri show-percentage  
scp://admin@2.2.2.2/images/ACOS_non-FTA_<version>.upg
```

3. Enter **yes** to Save system configuration if prompted.
Allow the system to upgrade the new software image.
4. Enter **yes** to reboot the system after the upgrade.
5. (Optional) If Duo MFA is enabled on the authentication server, authenticate using Duo MFA.

When ACOS prompts for authentication, select the configured Duo MFA method:

- Direct Passcode

A 6-digit passcode is generated in the Duo mobile app. Enter this periodically refreshed passcode to authenticate and continue with the upgrade.

- Option 1: Duo Push Notification

A push notification is sent to the Duo mobile app for approval. If approved, authentication is successful, and the upgrade process continues.

- Option 2: SMS Passcode

A passcode is sent to the registered phone number via SMS. Enter the received passcode to authenticate and continue with the upgrade.

For more information, see [System Configuration and Administration Guide](#).

6. After the upgrade is complete, set the new bootimage partition.

- To set the secondary hard disk to primary boot location:

```
ACOS-5-x(config)# bootimage hd sec
```

- To set the primary hard disk to the primary boot location:

```
ACOS-5-x(config)# bootimage hd pri
```

7. Save the running configuration to the new boot location:

- To save the configuration to the secondary hard disk:

```
ACOS-5-x(config)# write memory secondary all-partitions
```

- To save the configuration to the primary hard disk:

```
ACOS-5-x(config)# write memory primary all-partitions
```

8. Run the reboot command to boot the new software image.

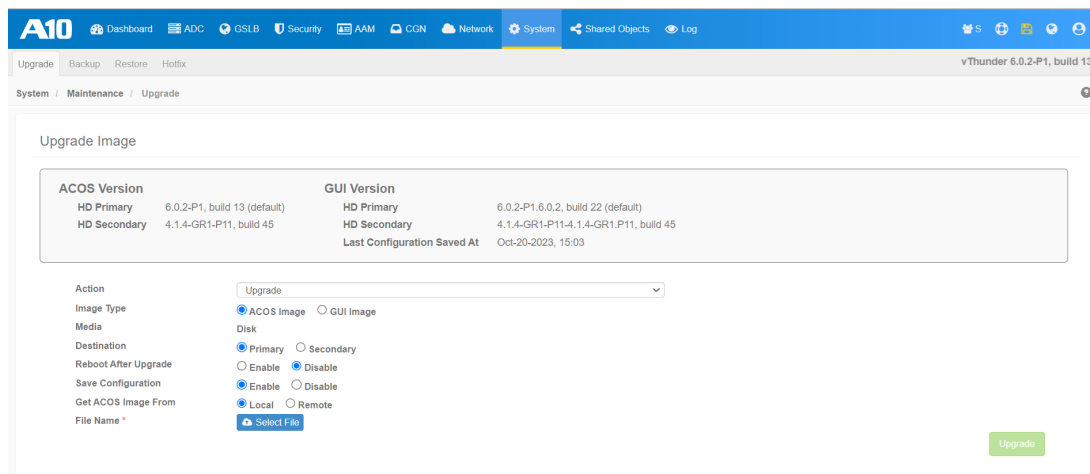
```
ACOS-5-x #reboot  
Proceed with reboot? [yes/no]:yes
```

NOTE: After rebooting in the new partition, it could take approximately 10-20 minutes to reboot and load the configuration in the new partition. The command line will show a <loading> state during the upgrade process. Allow the system to reboot completely.

The upgrade process is completed successfully.

GUI Configuration

1. Log in to ACOS Web GUI using your credentials.
2. Navigate to **System >> Maintenance >> Upgrade**.



3. On the **Upgrade** page, choose the **Upgrade** option from the **Action** field.
4. Choose the ACOS image option to upgrade the ACOS software image.
5. Upgrade the ACOS device to the inactive partition,
 - To upgrade the primary hard disk, choose the **Primary** option from **Destination** field.

OR

 - To upgrade the secondary hard disk, choose the **Secondary** option from **Destination** field.
6. Enable the **Reboot After Upgrade** option to reboot the ACOS device after upgrade.
7. Enable the **Save Configuration** option to save the configuration of all partitions.

8. Choose **Remote** to **Get ACOS Image From** the remote server.
9. Enable **Use Management Port**.
10. Enter the host and location, and the protocol used to access the host.
11. Click **Upgrade**.

NOTE: It is highly recommended to perform a cold reboot, or a power reset after upgrading from ACOS versions 4.1.x and 5.1.x to 6.x to ensure successful firmware updates.

See Also

- [Upgrading to ACOS 7.0.3 Using aVCS](#)

Post-Upgrade Tasks

After performing the upgrade, it is important to perform some basic post-upgrade checks.

You can follow one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

Log in to ACOS CLI using your credentials.

Verify Upgrade Success

Verify that ACOS device is upgraded successfully using the following command:

```
ACOS>show version
```

Validate Imported License

Verify that the required license is imported successfully using the following command:

```
ACOS>show license-info
```

Verify Configuration Profiles

Verify if the saved configuration from all the partitions is loaded successfully using the following command:

```
ACOS# show startup-config [all | all-partitions | partition | profile]
```

Perform Basic Testing

Verify if all the basic functionalities are working using the [Basic Functionality Testing](#).

Configure New Features

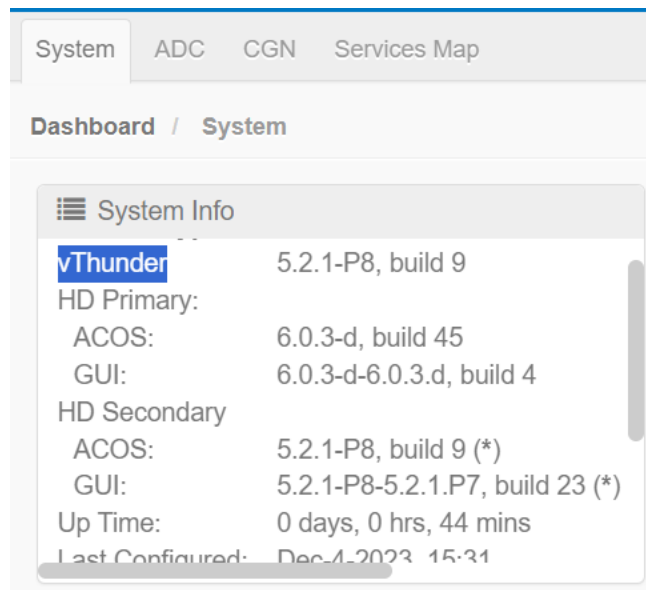
Configure the new features or settings introduced in the latest release, see *New Features and Enhancements* guide from the [Documentation Site](#).

GUI Configuration

Log in to ACOS Web GUI using your credentials.

Verify Upgrade Success

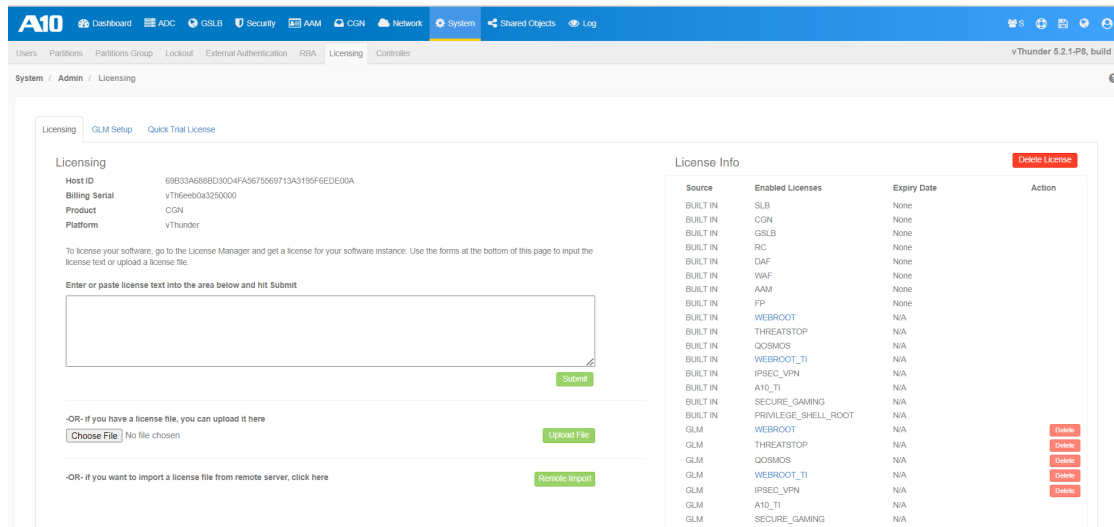
Navigate to **Dashboard >> System >> System Info**.



System Info	
vThunder	5.2.1-P8, build 9
HD Primary:	
ACOS:	6.0.3-d, build 45
GUI:	6.0.3-d-6.0.3.d, build 4
HD Secondary	
ACOS:	5.2.1-P8, build 9 (*)
GUI:	5.2.1-P8-5.2.1.P7, build 23 (*)
Up Time:	0 days, 0 hrs, 44 mins
Last Configured:	Dec 4, 2023 15:31

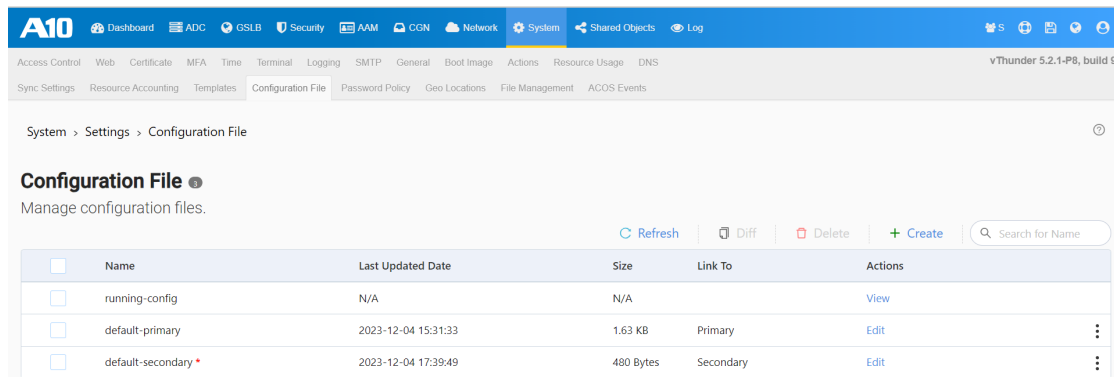
Validate Imported License

Navigate to **System >> Admin >> Licensing**.



Verify Configuration Profiles

Navigate to **System >> Configuration File**.



Perform Basic Testing

Perform the [Basic Functionality Testing](#) to collect system and/or product information.

Configure New Features

Configure the new features or settings introduced in the latest release, see *New Features and Enhancements* guide from the [Documentation Site](#).

Upgrade Rollback

The process of upgrading ACOS software is designed to be smooth and simple. In the unlikely event or unforeseen failure circumstance, a rollback plan is outlined to revert to the previous version. The rollback for ACOS device is like the upgrade process.

You can follow one of the instructions below:

- [CLI Configuration](#)
- [GUI Configuration](#)

CLI Configuration

1. Log in to the ACOS CLI and determine the current boot location.

```
ACOS-5-x(config)# show bootimage
                        (* = Default)
                        Version
-----
Hard Disk primary      5.2.1-P8.79
Hard Disk secondary    6.0.2.68 (*)
```

2. Backup the system configuration.

```
ACOS-5-x(config)# backup system
scp://exampleuser@192.168.3.3/home/users/exampleuser/backups/backupfile.tar.gz
```

3. Set the bootimage to the previous partition.

- To set the secondary hard disk to primary boot location:

```
ACOS-5-x(config)# bootimage hd sec
```

- To set the primary hard disk to the primary boot location:

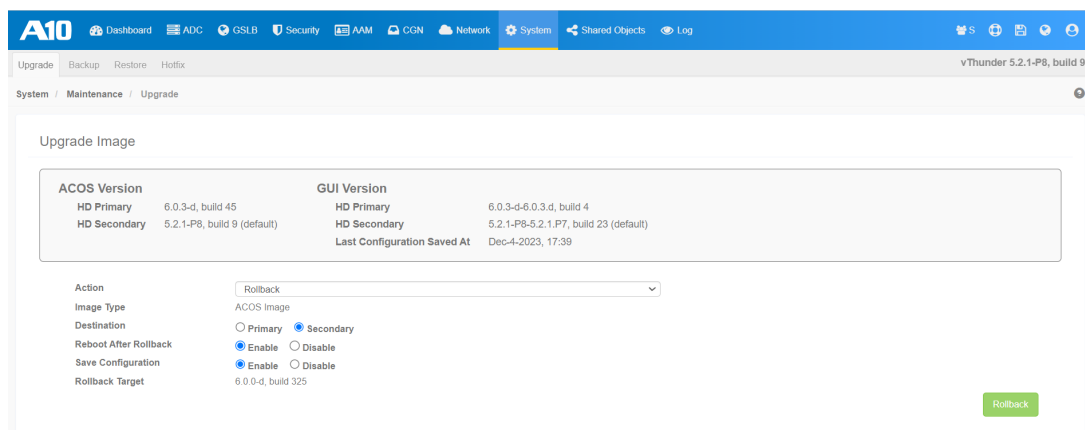
```
ACOS-5-x(config)# bootimage hd pri
```

4. Boot the previous image using the `reboot` command.

```
ACOS-5-x# reboot
Proceed with reboot? [yes/no]:yes
```

GUI Configuration

1. Log in to ACOS Web GUI using your credentials.
2. To take the system backup, navigate to **System >> Maintenance >> Backup >> System**.
3. To change the boot order, navigate to **Dashboard >> Settings >> BootImage**.
4. To roll back to the previous ACOS version, navigate to **System >> Maintenance >> Upgrade**.
5. Select the **Rollback** option from the **Action** drop-down list.



6. By default, the upgraded **Image Type** is selected.
7. Enable **Reboot After Rollback**.
8. Enable **Save Configuration**.
9. By default, the **Rollback Target** will display the previous ACOS version from where you have upgraded.
10. Click **Rollback**.

Upgrading to ACOS 7.0.3 Using aVCS

aVCS can be used to upgrade software images from 4.x and above releases. Before you begin the upgrade, it is recommended to check the [Upgrade Path](#) and [backup the system](#).

NOTE: Starting with ACOS 7.0.x, it is mandatory to install a valid RHEL Support license for all new ACOS installations and upgrades. If this license is not installed, the upgrade will fail. For more information, see [RHEL Support License Installation](#).

The following upgrade procedures are available; choose the one that best fits your deployment.

- [Full Chassis Upgrade \(with or without VRRP-A\)](#) – This procedure upgrades the software on the vMaster for full chassis upgrade deployments with or without VRRP-A. The vMaster puts the upgrade image onto each vBlade, then reboots the vBlades to activate the new software. During the reboot, service is briefly disrupted.
- [Staggered Upgrade \(with or without VRRP-A\)](#) (Recommended) – This procedure applies to staggered upgrade deployments with or without VRRP-A. A10 recommends using staggered upgrade as it avoids disruption, but has more steps to perform.

NOTE:

- Staggered Upgrade is not supported for upgrading ACOS 5.x cluster to ACOS 6.x cluster.
- Starting from the ACOS 6.0.0 release, the default aVCS multicast IP address has changed from 224.0.0.210 to 224.0.1.210. This change from 224.0.0.210 to 224.0.1.210 indicates that an intermediate switch can handle the packet differently, and aVCS communication could be interrupted. In an aVCS cluster, all devices must run the same version.

If required, the IPv4 multicast address can be changed to 224.0.0.210 by following the steps below:

```
#config
vcs multicast-ip 224.0.0.210
vcs reload
```

In the ACOS 6.0.6 release, the default aVCS multicast IP address has been changed from 224.0.1.210 to 224.0.0.211.

- [Manual Upgrade \(with VRRP-A\)](#) – This procedure applies to manually upgrade a VRRP-A ACOS device.

NOTE:

A reboot can take up to five minutes to complete. However, the actual time will differ depending on the system settings. The system does a full reset and goes offline during a reboot.

Backing Up the System

A full system backup includes the startup-config file, aFlex files, and SSL certificates and keys.

Using CLI

```
ACOS(config)#backup system scp://exampleuser@examplehost/dir1/dir2/
```

Using GUI

1. Navigate to **System >> Backup**.

2. Click **Backup**, then select **System** from the drop-down menu.
3. Select the backup host and location, and the protocol used to access the host.
4. Click **Backup**.

Full Chassis Upgrade (with or without VRRP-A)

This section describes the full chassis upgrade procedure on the vMaster.

NOTE: Each ACOS device in the virtual chassis must be rebooted. In this situation, the vMaster sends the new image to all vBlades and reboots all virtual chassis devices, including itself. This may take several minutes, during which time the service will be unavailable.

Using CLI

1. Save the startup-config to a new configuration profile:

```
ACOS(config)#write memory all-partitions
```

2. Upload the new image onto the vMaster and reboot. For example:

```
ACOS(config)#upgrade hd pri  
scp://exampleuser@examplehost/dir1/dir2/upgrade_file.upg
```

The CLI prompts you whether or not to reboot. Enter yes if you want to reboot now, or no if you want to reboot later. Only after a reboot does the new image take effect.

3. To verify the upgrade after the ACOS device reboots, use the `show version` command.

Using GUI

1. Navigate to **System >> Maintenance >> Upgrade**.
2. Make sure **Disable** is selected in the **Staggered Upgrade Mode** field, and complete the other fields on this screen as needed to specify the location of the upgrade file. Refer to the online help for detailed information about all the fields on the screen.
3. Click **Upgrade**.

4. After the upgrade file is successfully loaded, reboot your device.

Staggered Upgrade (with or without VRRP-A)

This section describes the staggered upgrade procedure with or without VRRP-A.

In case of VRRP-A environment, it is assumed that the vMaster is also the active VRRP-A device for all VRIDs. The vBlades are upgraded first, followed by the vMaster.

Using CLI

NOTE: If VRRP-A is not actively configured and running in the staggered environment, then skip [step 4](#) and [step b](#).

Perform the following step on Current vMaster (ACOS1)

1. On the vMaster, verify the currently running software version and the image area currently in use.

```
ACOS1-Active-vMaster[1/1]#show bootimage
(* = Default)
Version
-----
Hard Disk primary      4.0.3.25 (*)
Hard Disk secondary    2.6.1-GR1-P7.51
Compact Flash primary  2.6.1-GR1-P7.51 (*)
ACOS1-Active-vMaster[1/1]#show version
AX Series Advanced Traffic Manager AX5100
Copyright 2007-2015 by A10 Networks, Inc.
All A10 Networks products are protected by one or more of the
following US patents:
826372, 8813180
8918857, 8914871, 8904512, 8897154, 8868765, 8849938, 8
8782751, 8782221, 8595819, 8595791, 8595383, 8584199, 8464333,
8423676
8387128, 8332925, 8312507, 8291487, 8266235, 8151322, 8079077,
7979585
7804956, 7716378, 7665138, 7647635, 7627672, 7596695, 7577833,
7552126
```

```

7392241, 7236491, 7139267, 6748084, 6658114, 6535516, 6363075,
6324286
5931914, RE44701, 8392563, 8103770, 7831712, 7606912, 7346695,
7287084
6970933, 6473802, 6374300
64-bit Advanced Core OS (ACOS) version 4.0.3, build 25 (Oct-25-
2015,21:22) Booted from Hard Disk primary image
Serial Number: AX51051110360007 Firmware version: 0.26
aFlex version: 2.0.0
aXAPI version: 3.0
Hard Disk primary image (default) version 4.0.3, build 25 Hard Disk
secondary image version 2.6.1-GR1-P7, build 51
Compact Flash primary image (default) version 2.6.1-GR1-P7, build 51
Last configuration saved at Oct-26-2015, 05:58
Build Type: Internal
Hardware: 16 CPUs(Stepping 5), Single 62G Hard disk Memory 24685
Mbyte, Free Memory 9878 Mbyte
Hardware Manufacturing Code: 103600 Current time is Oct-30-2015,
16:13
The system has been up 4 days, 10 hours, 14 minutes

```

All devices in the virtual chassis use the same image area (primary or secondary). For example, if the software running on the vMaster is in the primary image area, all the vBlades also are running their software from the primary image areas on those devices.

2. Save the configuration. Be sure to use the all-partitions option if you have RBA or L3V partitions configured.

```

ACOS1-Active-vMaster[1/1]#write memory all-partitions
Building configuration...
Write configuration to primary default startup-config
[OK]

```

3. Upgrade the vBlade, by loading the new software image into the image area currently used by the vBlade:

```

ACOS1-Active-vMaster[1/1](config)#upgrade hd pri
scp://exampleuser@examplehost/dir1/ dir2/upgrade_file.upg staggered-
upgrade-mode Device 2

```

This step reboots the vBlade. The vMaster continues to operate.

4. For each VRID that is active on the device, force failover from the vMaster to the vBlade by setting the priority to 255. For example:

```
ACOS1-Active-vMaster[1/1](config)#vrrp-a vrid 2
ACOS1-Active-vMaster[1/1](config-vrid:2)# blade-parameters
ACOS1-Active-vMaster[1/1](config:2-vrid:2-blade-parameters)#priority
255
```

NOTE: Do not use the vrrp-a force-self-standby command.

5. Validate that the load-balanced services are working. (The show commands or other techniques depend on your deployment. The show slb virtual-server command is useful in almost any deployment.)

Perform the following step on the vBlade (ACOS2)

6. On the vBlade that is running the new software image, enter the `vcs vmaster-take-over` command to force the vBlade to take over the vMaster role:

```
ACOS2-Active-vBlade[1/2]#vcs vmaster-take-over 255
During failover, the vBlade becomes the vMaster, and the vMaster
becomes a vBlade. The new vMaster will detect that the vBlade device
is running old software, and it will upgrade the vBlade. As part of
this upgrade, the vMaster will reboot the vBlade.
```

Optional: Perform the following step on the original vMaster (ACOS1)

7. Optionally, force failover back to the original vMaster. Perform the following step on the new vBlade (former vMaster) to resume the vMaster role and again become the active device for the VRID:
 - a. At the Privileged EXEC level, use the `vcs vmaster-take-over` command to take over the vMaster role:

```
ACOS1-Active-vBlade[1/1]#vcs vmaster-take-over 255
```

- b. For each VRID, use the following commands to reset the VRRP-A priority to its previous value. For example:

```
ACOS1-Active-vMaster[1/1](config)#vrrp-a vrid 2
```

```
ACOS1-Active-vNaster[1/1] (config-vrid:2) # blade-parameters
ACOS-Active-vMaster[1/1] (config-vrid:2-blade-parameters) #priority
100
```

Using GUI

NOTE: If VRRP-A is not actively configured and running in the staggered environment, then skip [step 7](#) and [step 11](#).

1. Navigate to **System >> Maintenance >> Upgrade**.
2. Make sure **Enable** is selected in the **Staggered Upgrade Mode** field.
3. Specify the ID of the device you want to upgrade.
4. Complete the other fields on this screen as needed to specify the location of the upgrade file. Refer to the online help for detailed information about all the fields on the screen.

NOTE: All devices in the virtual chassis use the same image area (primary or secondary). For example, if the software running on the vMaster is in the primary image area, all the vBlades also are running their software from their own primary image areas.

5. Click **Upgrade**.
6. After the upgrade file is successfully loaded, reboot your device.
7. After the device reboots, set the priority value of each VRID on the device to a lower value than on the backup ACOS device:

NOTE: Do not use the **Force Self Standby** option.

- a. Navigate to **System >> VRRP-A**.
- b. Click **Settings**, then select **VRID** from the drop-down list.
- c. Click **Edit** in the **Actions** column for a VRID.
- d. Verify that **Enable** is selected in the **Preempt Mode** field.
- e. Open the **Blade Parameters** section, then edit the value in the **Priority** field to a value that is lower than the priority value(s) for the VRIDs on the

backup ACOS device.

- f. Click **Update**.
8. Go to the vBlade device and force failover in order to take over the vMaster role:
 - a. Navigate to **System >> aVCS >> Settings**.
 - b. Open the **Actions** section, then enter 255 in the **vMaster Take Over** field.
 - c. Click **OK**.

NOTE: During failover, the vBlade becomes the vMaster and vMaster becomes a vBlade device. The new vMaster will detect that the vBlade device is running old software, and it will upgrade the vBlade. As part of the upgrade, the vMaster will reboot the vBlade.

9. Optionally, force failover back to the original vMaster.
10. Take over the vMaster role:
 - a. Navigate to **System >> aVCS >> Settings**.
 - b. Open the **Actions** section, then enter 255 in the vMaster Take Over field.
 - c. Click **OK**.
11. For each VRID, repeat [step 7](#) to reset the VRRP-A priority to its previous value.

Manual Upgrade (with VRRP-A)

This section discusses how to upgrade aVCS manually from a previous 4.x release to the current release. The steps stay the same if you are upgrading from a 2.7.2.x or 2.8.2.x release, although the CLI commands and prompt may slightly differ.

In this example, the virtual chassis contains two devices:

- Current VRRP-A active device and vMaster “ACOS1”
- Current VRRP-A standby and vBlade device “ACOS2”

Manual Upgrade General Workflow

1. Save and backup your configuration on both devices.

2. Disable aVCS on ACOS2.
3. Force VRRP-A to fail over from ACOS1 to ACOS2.
4. Upgrade and reboot ACOS1.
5. Force VRRP-A fail over from ACOS2 back to ACOS1.
6. Without saving the configuration on ACOS2, upgrade and reboot ACOS2.

Your original configuration will be loaded after the reboot. ACOS2 will rejoin the aVCS chassis and become the VRRP-A standby device. The manual forced failover induced by modifying the VRID priority has no effect on your VRRP-A configuration.

Manual Upgrade Instructions

1. Obtain the appropriate upgrade package.
2. On all devices in the virtual chassis, save the startup configuration to a new profile.
3. Use the all-partitions option if you have L3V partitions configured.

Do not link the profile; this profile will serve as the local backup of the current release configuration. For example, on the current vMaster “ACOS1:”

```
ACOS1-vMaster[8/1](config)# write memory backup_profile all-
partitions
Building configuration...
Write configuration to profile "backup_profile"
Do you want to link "backup_profile" to startup-config profile?
(y/n): n
[OK]
```

4. Backup your system to a remote device. For example:

```
ACOS1-vMaster[8/1](config)# backup system
scp://exampleuser@examplehost/dir1/dir2/
```

5. On the vBlade device “ACOS2,” disable aVCS.

```
ACOS2-vBlade[8/1](config:2)# vcs disable
ACOS2-vBlade[8/1](config:2)#Mar 21 2016 16:14:41 B3 a10logd: [VCS]<3>
dcs thread
peer closed connection prematurely
```

```
Mar 21 2016 16:14:41 B3 a10logd: [CLI]<3> rimacli: socket select
operation failed
Mar 21 2016 16:14:41 B3 a10logd: [CLI]<3> rimacli: terminted because
received SIGTERM
signal

ACOS2# show vcs summary
VCS is not active.
ACOS2#
```

6. On “ACOS2:”

- a. Access the configuration level for the VRRP-A VRID in the shared partition and each L3V partition. For example:

```
ACOS2# configure
ACOS2(config)# vrrp-a vrid 1
ACOS2(config-vrid:1)#
```

- b. Change the VRID priority to a value that is higher than the priority on the vMaster. For example, if the VRID priority on the vMaster is 100, we can change the priority to 105:

```
ACOS2(config-vrid:1)# blade-parameters
ACOS2(config-vrid:1-blade-parameters)# priority 105
ACOS2(config-vrid:1-blade-parameters)# exit
ACOS2(config-vrid:1)# exit
ACOS2(config)#
```

- c. This will cause VRRP-A to fail over so that ACOS2, now with the higher priority, becomes the new active device.

7. Install the software build image that you want to upgrade on ACOS1 and reboot the device for the change to take effect.

8. On ACOS2:

- a. Access the configuration level for the VRRP-A VRID in the shared partition and each L3V partition. For example:

```
ACOS2(config)# vrrp-a vrid 1
ACOS2(config-vrid:1)#
```

- b. In the shared partition and all L3V partitions, change the VRID priority back to its original value, or any value that is lower than the value on ACOS1. For example, if the VRID priority on ACOS1 is 100, you can change the priority to 99 on ACOS2:

```
ACOS2 (config-vrid:1) # blade-parameters
ACOS2 (config-vrid:1-blade-parameters) # priority 99
ACOS2 (config-vrid:1-blade-parameters) # exit
ACOS2 (config-vrid:1) # exit
ACOS2 (config) #
```

This will cause VRRP-A to fail over so that the ACOS1 will once again become the active device.

9. Without saving the configuration, install the software build image of the upgrade version on ACOS2 and reboot the device for the change to take effect.

Your original configuration (saved in [step 2](#)) will be loaded after ACOS2 is rebooted, and ACOS2 will rejoin the virtual chassis.

Upgrading Scaleout Cluster from ACOS 5.2.1-Px to 6.x.x

The Scaleout cluster configuration of the ACOS 5.2.1-Px version differs from the ACOS 6.x.x version. A 5.2.1-Px cluster cannot communicate or interoperate with a 6.0.x cluster. Hence, it is necessary to migrate the ACOS 5.2.1-Px Scaleout cluster to ACOS 6.0.x.

For a detailed step-by-step procedure, see the "Upgrading Scaleout Cluster from ACOS 5.2.1-Px to ACOS 6.0.x and Later Releases" section in the *Scaleout Configuration Guide*.

The steps describe the procedure for removing devices from a 5.2.1-Px cluster and adding them to a new 6.0.x cluster, while minimizing traffic loss. The procedure may be duly adapted to a larger or smaller cluster.

NOTE: Two Python scripts are available to ease the configuration migration from 5.2.1-Px to 6.0.x for all Scaleout-related configurations.

See Also:

- [Scaleout Configuration Guide](#)

Upgrading Scaleout/aVCS Cluster from ACOS 6.0.x to 6.0.7

In ACOS 6.0.6, the VCS default multicast IP address is changed from 224.0.1.210 to 224.0.0.211. Hence, while upgrading the Scaleout-VCS cluster from ACOS 6.0.x to ACOS 6.0.6 or later, you must perform a few additional steps.

For the detailed steps, see the "Upgrading Scaleout/aVCS Cluster from pre-ACOS 6.0.x to ACOS 6.0.6 and Later Releases" section in the *Scaleout Configuration Guide*.

The steps describe the procedure to upgrade the Scaleout and Virtual Chassis Systems (VCS) cluster under different scenarios for the Multi-PU and Non-Multi-PU platforms.

See Also:

- [Scaleout Configuration Guide](#)

Migrating Existing Thunder Platforms to Thunder Modular Platforms

In ACOS 7.0.1, the Thunder modular platforms are introduced such as TH7460S. Due to architectural differences between the older Thunder platforms and the Thunder modular platform, certain manual steps are required to ensure a successful migration of both configuration and modular license.

The following topics are covered:

Migrating from Thunder Device (ACOS 6.0.x) to Thunder Modular Device (ACOS 7.0.x)	62
Migrating Configuration Between Thunder Modular Devices (ACOS 7.0.x)	65

Migrating from Thunder Device (ACOS 6.0.x) to Thunder Modular Device (ACOS 7.0.x)

This section provides step-by-step instructions to back up configuration from a Thunder device running ACOS 6.0.x and restore it on a Thunder modular device running ACOS 7.0.1 and above.

NOTE: A10 recommends performing these steps in the maintenance window.

1. [Preserve encrypted password](#), if configured.

This step is applicable only if your Thunder device is running on ACOS 6.0.7 patch release.

```
ACOS(config)# system update-passphrase
```

NOTE: If you are running versions prior to ACOS 6.0.7, then upgrade to 6.0.7 patch. Execute this command and then take the backup. Otherwise, the older version will lose the configuration when upgraded to 7.0.1.

2. [Backup the configuration of ACOS 6.0.x.](#)

```
ACOS(config)# backup system use-mgmt-port <url>/backupfile.tar.gz
```

3. [Prepare the Thunder modular Device.](#)

4. Confirm that Thunder modular device is running on ACOS 7.0.1 or above software image.

```
ACOS> show version
```

5. Check if modular and RHEL licenses are preinstalled.

```
ACOS(config)# show license-info
```

6. [Import and apply modular license](#), if not preinstalled.

```
ACOS(config)# import license use-mgmt-port <url>/modular.txt
```

7. [Import and apply RHEL license](#), if not preinstalled.

```
ACOS(config)# import license use-mgmt-port <url>/rhel.txt
```

8. Verify the license information.

```
ACOS (config)# show license-info
```

9. Reboot the device to activate the licenses.

```
ACOS# reboot  
Proceed with reboot? [yes/no]:yes
```

10. [Restore the ACOS 6.0.x backup](#) on the Thunder modular device.

```
ACOS(config)# restore use-mgmt-port <url>/backupfile.tar.gz
```

11. When the system prompts to reboot, enter `no`.

NOTE: If you reboot after restore, then you will lose all the configuration in the backup. Also, you will encounter "License mismatch" warning message. This occurs because the UUID embedded in the backup file does not match the target device's UUID. This is an expected warning. Hence, **do not reboot at this point and continue with the next steps.**

12. Reapply modular license.

```
ACOS(config)# import license use-mgmt-port <url>
```

13. Verify the license is imported successfully.

```
ACOS (config)# show license-info
```

14. The system will prompt to save the configuration, enter **no**.
15. The system should trigger a reboot. If the system does not automatically reboot, manually reboot without saving the configuration.

```
ACOS# reboot  
Proceed with reboot? [yes/no]:yes
```

After the reboot, the device will load the restored backup.

16. Verify the restored configuration.

```
ACOS(config)# show running-config
```

By default, the system will boot with two [Control CPUs](#).

17. In case a higher number of control CPUs are needed, reconfigure the required number of Control CPUs.

```
ACOS(config)# multi-ctrl-cpu <x>
```

18. The system will prompt to reboot, enter **y**.
19. The system will prompt to save the configuration, enter **yes**.
20. Verify the restored configuration.

```
ACOS(config)# show running-config
```

21. Verify the modular license information.

```
ACOS(config)# show license-info
```

The restored backup along with the modular license should be loaded on Thunder modular device.

Migrating Configuration Between Thunder Modular Devices (ACOS 7.0.x)

This section provides step-by-step instructions to migrate configuration from a Thunder modular device (Source) to another Thunder modular device (Target) - both running ACOS 7.0.1 or above version.

NOTE: A10 recommends performing these steps in the maintenance window.

1. [Backup the configuration of source device ACOS 7.0.x.](#)

```
ACOS(config)# backup system use-mgmt-port <url>/backupfile.tar.gz
```

2. [Prepare the target Thunder modular device.](#)

3. Confirm that the target Thunder modular is running ACOS 7.0.x software image.

```
ACOS> show version
```

4. Check if modular and RHEL licenses are preinstalled.

```
ACOS(config)# show license-info
```

5. [Import and apply modular license](#) if not preinstalled.

```
ACOS(config)# import license use-mgmt-port <url>/modular.txt
```

6. [Import and apply RHEL license](#) if not preinstalled.

```
ACOS(config)# import license use-mgmt-port <url>/rhel.txt
```

7. Verify the license information.

```
ACOS (config)# show license-info
```

8. Reboot the device to activate the licenses.

```
ACOS# reboot
Proceed with reboot? [yes/no]:yes
```

9. By default, the system will boot with two [Control CPUs](#). In case a higher number of control CPUs are needed, reconfigure the required number of Control CPUs.

```
ACOS(config)# multi-ctrl-cpu <x>
```

10. The system will prompt to reboot, enter `y`.
11. The system will prompt to save the configuration, enter `yes`.
12. [Restore the backup from the source device](#) on the Thunder modular device.

```
ACOS(config)# restore use-mgmt-port <url>/backupfile.tar.gz
```

13. When the system prompts to reboot, enter `no`.

NOTE: If you reboot after restore, then you will lose all the configuration in the backup. Also, you will encounter "License mismatch" warning message. This occurs because the UUID embedded in the backup file does not match the target device's UUID. This is an expected warning. Hence, **do not reboot at this point and continue with the next steps.**

14. Reapply modular license.

```
ACOS(config)# import license use-mgmt-port <url>
```

15. The system will prompt to save the configuration, enter `no`.
16. The system should trigger a reboot. If the system does not automatically reboot, manually reboot without saving the configuration.

```
ACOS# reboot  
Proceed with reboot? [yes/no]:yes
```

After the reboot, the device will load the restored backup.

17. Verify the restored configuration.

```
ACOS(config)# show running-config
```

18. Verify the modular license information.

```
ACOS(config)# show license-info
```

The restored backup from the source device along with the modular license should be loaded on target device.

Software and Hardware Limitations

This section lists the software and hardware limitations in ACOS.

The following topics are covered:

Software Limitations	68
Hardware Limitations	80

Software Limitations

This section explains the limitations related to ACOS Release 4.x and above series (specific release limitations are so noted in the descriptions):

The following topics are covered:

Downgrading a Scaleout Cluster from ACOS 5.2.x to 4.1.4-GR1-Px	69
SSL Handshake Cannot Happen with Low DH-Param Value	69
Active FTP on vThunder (Virtual Thunder) for Azure	70
Active VM Limitation for Recovering floating-ip	70
aFlex Limitations	70
Application Access Management aFlex Limitations	70
Application Access Management Limitations	71
aXAPI Functionality Limitations	71
Delayed IP Migration on Azure Cloud	71
Form-based Relay Pages Limitations	71
Health Monitor is Displayed Twice in Startup Configuration	72
Incoming Axdebug/Debug Packets Are Not Captured on Azure	73
IPsec VPN Restrictions and Limitations	73
Known GUI Limitations	73
L3V Interface Disabled After Upgrading	74
Local Lagging	74
NAT Pool Statistics Limitation	74
Passive FTP on vThunder for AWS and Azure Does Not Work	74
Server-SSL Template Binding	75
SSLi Single Partition with Explicit Proxy Source NAT	76
VCS on vThunder for AWS and Azure Does Not Work	76
VCS and GSLB Limitations	76
VPN Tunnel Cannot Be Up with SLB Virtual Server Enabled on Azure	77
VRRP-A Configuration Sync Limitation	77

[vThunder Cannot Ping Standby Interface in VPPR-A Deployments](#)77

[WAF Template Configuration Missing After Upgrading to 5.x](#) 77

[Web-category License Corrupt After Upgrading to 4.x](#)77

[Encrypted Password Configuration Missing After Upgrading to ACOS 7.0.x](#) 78

Downgrading a Scaleout Cluster from ACOS 5.2.x to 4.1.4-GR1-Px

You can upgrade a Scaleout cluster from ACOS 4.1.4-GR1-Px to 5.2.x version in a staggered manner. However, you cannot perform a staggered downgrade of a Scaleout cluster from 5.2.1-P1 to 4.1.4-GR1-Px.

To downgrade a Scaleout cluster from 5.2.1-P1 to 4.1.4-GR1-Px, perform the following:

1. Disable the Scaleout cluster and save the configurations.
2. Downgrade each node individually to ACOS 4.1.4-GR1-Px version and reboot them.
3. Make sure all the nodes are running successfully.
4. Re-enable the cluster.

SSL Handshake Cannot Happen with Low DH-Param Value

Starting 4.1.4.x release, the SSL Library was upgraded so that the DH-param (Diffie-Hellman) value less than 128 bytes is considered as a weak cipher. This behavior occurs when upgrading from 2.7.2.x releases and when the DHE ciphers is selected for server-side SSL connection. This may cause 'SSL connect error' and result in SSL handshake failure.

So, before upgrading 2.7.2.x to 4.1.4.x and above releases, ensure that the DH-param value is equal to or greater than 128 bytes in the backend server.

NOTE: This limitation only applies to SSL library used for health-check and not for SSL SLB traffic on data plane.

Active FTP on vThunder (Virtual Thunder) for Azure

Active FTP mode is not supported in Azure with kdemux drivers (**A10 Tracking ID: 367223**).

Active VM Limitation for Recovering floating-ip

On Azure cloud, the user found that the Active VM does not recover `floating-ip` after power-off and power-on.

aFlex Limitations

This limitation is applicable for all 4.x releases. Tcl allows backslash-newline in its scripts but aFlex currently does not support it. For example, you can continue a long line in Tcl with a backslash character (`\`):

```
set totalLength [expr [string length $one] + \  
                  [string length $two]]
```

However, aFlex will experience a compilation error if you use backslash-newline.

The recommendation is to write the long line without the backslash character:

```
set totalLength [expr [string length $one] + [string length $two]]
```

The `RESOLVE::lookup` command does not support `CLIENT_ACCEPTED` and `CLIENT_DATA` events if the virtual port is HTTP or HTTPS type.

Application Access Management aFlex Limitations

The following limitations are applicable for all 4.x releases:

- When using a RADIUS server as the authorization server with SAML authentication and WS-Federation relay, Application Access Management aFlex will not retrieve user passwords from HTTP requests. Application Access Management aFlex authorizations against the RADIUS server will fail due to failing to provide user password for the RADIUS server.

- With WS-Federation relay, the Active Directory Federation Services (ADFS) may return attribute names in lower case or in upper case, while **AAM aFlex** **AAM::attribute** commands are case-sensitive. Make sure Application Access Management aFlex is configured with the correct attribute names for the values retrieved from ADFS.

Application Access Management Limitations

ACOS 4.x does not support Application Access Management configuration in any CGNv6 partitions.

aXAPI Functionality Limitations

The following limitations are applicable for all 4.x releases:

- The implementation of the aXAPI in the 4.x releases is not backwards compatible with any 2.7.x or 2.8.x aXAPI implementations.
- The ACOS software does not provide support for the configuration of Health Monitors, VRRP-A, or deletion of an interface that is part of a trunk using aXAPIs. Use the CLI for these operations.
- Issuing a block of configuration using the `cli.deploy` aXAPI method will cause the control CPU to experience a spike to 100% while this operation is in progress. As soon as the configuration change has been applied, the Control CPU will revert to normal behavior.

Delayed IP Migration on Azure Cloud

The user found that there is a delay on Azure cloud for the IP address migration of the API call (which are **Delete** and **Add**), which is taking approximately three minutes on average. As a result of this, the completion of vThunder (Virtual Thunder) failover also taking as long as three minutes on an average.

Form-based Relay Pages Limitations

Currently, the following two scenarios are not supported by the back-end server:

Some form-based pages will require a user to provide a dynamic variable in response.

Some pages may not contain a “Content-Length” header or the “Content-Length” header may be too short.

Health Monitor is Displayed Twice in Startup Configuration

Startup configuration intentionally displays the health monitor twice. Providing the initial listing of health monitor names with their exit-modules allows the declaration of references those health monitors before other object configurations are listed. This ensures object configurations that depend on a particular health monitor can refer to the earlier reference to verify the health monitor is properly configured.

This is a limitation for 4.x series releases, but it is also applicable to 5.x series releases as well.

The following commands are applicable to this limitation.

```
-----  
#show version | inc OS  
      64-bit Advanced Core OS (ACOS) version 5.1.0, build 90 (Dec-21-  
2019,16:08)  
  
#show start | sec health  
health monitor test  
  exit-module  
health monitor test  
  interval 100  
  exit-module  
  
#show start | sec object  
object-group network test fw v4  
  exit-module  
object-group network test fw v4  
  1.1.1.1/32  
  exit-module  
  
#show start | sec vrid  
vrrp-a vrid 10  
  exit-module
```

```
vrp-a vrid 10
floating-ip 2.2.2.2
exit-module
-----
```

The health monitor is displayed twice in the startup configuration (**A10 Tracking ID: 342736**).

Incoming Axdebug/Debug Packets Are Not Captured on Azure

vThunder (Virtual Thunder) on Azure does not allow for incoming axedebg/debug packets (**A10 Tracking ID: 365147**).

IPsec VPN Restrictions and Limitations

The following are of the limitations of the current release:

- To disable perfect forward secrecy (PFS), do not configure a Diffie Helman (DH) group in IPsec configuration.
- IPsec packet round robin may cause packet reordering.
- Disable anti-reply if IPsec packet round robin is enabled.
- In a single tunnel without IPsec round robin may cause CPU load sharing to trigger, thus forcing packet round robin. To avoid this, disable CPU load sharing.
- NAT-traversal flow affinity is A10 proprietary and may not inter-operate with other vendors.
- SNMP GET request of ifInOctets/ifOutOctets counters do not match the received/transmitted bytes for the CLI equivalent of `show interfaces tunnel <no>` beyond a certain number of bytes.

Known GUI Limitations

The following limitations are known in the GUI for release 4.0.1:

- To view global session information, hover over **CGN** in the menu bar and select **Session**. This item will be moved to a more appropriate location in future releases.

- When switching aVCS device-context from the vMaster to a vBlade, configuration of the vBlade is allowed as expected, but only statistical information from the vMaster is visible.
- Importing compressed files is not supported, except for SSL certificates.

L3V Interface Disabled After Upgrading

The status of the interfaces in L3V become disabled after upgrading from ACOS 2.7.2 to 4.1.4-Px.

However, the status of the interfaces in the shared partition were maintained after upgrading (**A10 Tracking ID: 437707**).

Local Lagging

The use of local logging is not recommended with large traffic. It will create high CPU utilization condition.

NAT Pool Statistics Limitation

The “NAT Pool Unusable” statistics in the `show cgnv6 nat64 statistics` and `show cgnv6 ds-lite statistics` output does not get incremented as the NAT pool can be used by multiple technologies.

This field works properly for LSN configurations, where there is outside-to-inside communication (full-cone session).

Passive FTP on vThunder for AWS and Azure Does Not Work

If you need to use FTP on vThunder (Virtual Thunder) for Azure or vThunder (Virtual Thunder) for AWS in pvgrub mode, use active FTP; passive FTP does not work reliably.

Server-SSL Template Binding

Starting from the ACOS 6.0.6 release, the following scenarios or limitations are supported for binding Server-SSL templates:

- A single real port can be used with multiple Server-SSL templates.
- A single service group can only be used with one Server-SSL template.

For example, if an ACOS system is configured with two virtual-servers, `SSL_Internet_vip_001` and `SSL_Internet_vip_003`. And, each of these virtual servers are configured with an HTTP virtual port, `port 8080 http`.

Same SSL-template and service group is applied to each virtual port.

The SSL-template, `SSL_Internet_vip_001_server_ssl`, and the service group, `sg2`, are applied to `port 8080 http` on `SSL_Internet_vip_001`.

```
slb virtual-server SSL_Internet_vip_001 0.0.0.0 acl 1
  user-tag Security
  port 8080 http
    service-group sg1
    use-rcv-hop-for-resp
    template server-ssl SSL_Internet_vip_001_server_ssl
    no-dest-nat port-translation
slb virtual-server SSL_Internet_vip_003 0.0.0.0 acl 3
  user-tag Security
  port 8080 http
    service-group sg2
    use-rcv-hop-for-resp
    template server-ssl SSL_Internet_vip_003_server_ssl
    no-dest-nat port-translation
```

The following example demonstrates the supported behavior where each virtual port with a server-SSL template is associated with a different service group. Here, a single real server is shared between multiple service groups, with each service group associated with a different Server-SSL template.

```
slb server rs1 192.168.1.10
  port 80 tcp

slb service-group sg1 tcp
  member rs1 80

slb service-group sg2 tcp
  member rs1 80

slb virtual-server SSL_Internet_vip_001 0.0.0.0 acl 1
  port 8080 http
  service-group sg1
  template server-ssl SSL_Internet_vip_001_server_ssl

slb virtual-server SSL_Internet_vip_003 0.0.0.0 acl 3
  port 8081 http
  service-group sg2
  template server-ssl SSL_Internet_vip_003_server_ssl
```

SSLi Single Partition with Explicit Proxy Source NAT

If Secure Sockets Layer Insight (SSLi) is configured for use in a single partition, source NAT for explicit proxy is not supported. This is illustrated here with the CLI command and highlighted parameter, configured as an action in a forward-policy under an slb policy template:

```
forward-to-proxy service-group snat snat-pool (A10 Tracking ID: 366406)
```

VCS on vThunder for AWS and Azure Does Not Work

VCS support on vThunder (Virtual Thunder) for AWS and Azure is not available. Hence, the aVCS commands are not available on vThunders instances running in Azure or AWS environments.

VCS and GSLB Limitations

A10 Networks does not recommend VCS and GSLB to work together.

VPN Tunnel Cannot Be Up with SLB Virtual Server Enabled on Azure

vThunder (Virtual Thunder) on Azure does not currently allow for VPN tunnels with a slb virtual server enabled (**A10 Tracking ID: 366599**).

VRRP-A Configuration Sync Limitation

In VRRP-A config sync environments, file type class lists that are configured from the CLI (and not imported) must be saved with the `write memory` command in order for the class list configuration to be synchronized to the vBlades.

vThunder Cannot Ping Standby Interface in VRRP-A Deployments

If vThunder (Virtual Thunder) is deployed with VRRP-A I3-inline-mode, the IP of the local interface (ethernet, VE, and trunk) for the backup ACOS device is unreachable using a standard ICMP ping.

WAF Template Configuration Missing After Upgrading to 5.x

The syntax of Web Application Firewall (WAF) template commands has changed in 5.x. Therefore, after upgrading the system from 4.x to 5.x., the Web Application Firewall (WAF) template configuration does not work as expected.

To fix this issue, see [WAF Template Configuration Changes](#).

Web-category License Corrupt After Upgrading to 4.x

If you are upgrading to 4.1.4 and have a web-category license, the web-category license corruption may occur from an upgrade. This could be because the web-category license has not enabled after the upgrade. To resolve this issue, enable your web-category license:*

```
ACOS#config  
ACOS# (config) #web-category
```

```
ACOS# (config-web-category) #enable
```

This procedure will check for and fix a web-category license corruption that might occur from an upgrade.

*Ensure your ACOS appliance is already configured with an established connection to the Global Licensing Manager (GLM). Configuration for GLM can be done at the global configuration level using the `glm` command.

Encrypted Password Configuration Missing After Upgrading to ACOS 7.0.x

After upgrading from ACOS 6.0.7 to ACOS 7.x, configurations involving encrypted passwords—such as TACACS server credentials, BGP neighbor passwords, and others, may disappear if the system passphrase is not properly set beforehand.

NOTE: The following procedure applies only while upgrading from ACOS 6.0.7 to ACOS 7.x. For versions prior to ACOS 6.0.7, you must first upgrade to ACOS 6.0.7 and then follow the steps below.

To preserve the encrypted password configuration during upgrade:

1. On ACOS 6.0.7, before upgrading, execute 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):XXXXXXXXXXXX
System passphrase update successfully.
Building configuration...
Write configuration to default primary startup-config
[OK]
```

NOTE:

- The passphrase (AES) is device specific. For example, to configure VCS, you need to use the same passphrase among devices. To run the backup system in device A, and restore it in device B, you need to use the same passphrase in device A and B.
 - After running the `system-reset` command in ACOS 7.0.x, the passphrase is reset to default AES passphrase . In ACOS 6.0.7, the passphrase is reset to the default DES passphrase. DES encryption is deprecated in ACOS 7.0.1.
-

2. Save the configuration by executing the following command:

```
ACOS(config)# write memory
```

3. Upgrade to ACOS 7.0.x.

For the upgrade instructions, see [Upgrading to ACOS 7.0.3](#).

Additionally, to downgrade from ACOS 7.0.x to ACOS 6.0.7 (or later), make sure you run the `system update-passphrase` command beforehand. To verify if you configured passphrase previously, you can run the command again.

```
ACOS(config)# system update-passphrase
The passphrase has been configured. Do you want to continue to update a
new passphrase? [yes/no]:no
```

Hardware Limitations

This section explains the hardware limitations applicable to all the releases of ACOS 4.x and above series:

The following topics are covered:

Auto-Negotiation Limitations	80
Combo Console/LOM Interface Requires Splitter Cable	80
Show Interface Media Return "ERROR"	81
Thunder 7650 Limitations	81
Thunder 14045 Limitations	82
Thunder 940/1040 Limitations	83
Thunder 5960 Limitations	83
Transceivers Not Purchased From A10 Networks May Show Error Message ...	84
Thunder 7460S, 7460S-MAX, and 7465 Platforms Limitation	84

Auto-Negotiation Limitations

Auto-negotiation is not supported on 1G SFP on 10G ports. Also, speed and duplexity cannot be changed on any ports that use transceivers, such as SFP/SFP+.

Combo Console/LOM Interface Requires Splitter Cable

The following devices feature a dual IOIO (Console) and Lights Out Management (LOM) interface with a splitter cable:

- Thunder 7440(S)
- Thunder 6440(S)
- Thunder 5840(S)
- Thunder 5440(S)
- Thunder 4440(S)

Plugging a cable directly into this interface does not work; you must use the splitter cable to have either console or LOM functionality.

Show Interface Media Return “ERROR”

The `sh int mediaCLI` is currently not supported on Thunder 3350 series.

Thunder 7650 Limitations

The Thunder 7650 model has the following limitations:

- GTP Firewall is not supported on Thunder 7650.
- Virtual Chassis System (VCS) is not supported on Thunder 7650.
- TCP Logging and the associated commands are not supported on Thunder 7650. The options to configure a TCP log server and service-group are also not supported.
- NPTv6 and the associated commands are not supported on Thunder 7650.
- ADHOC tunneling is not supported on Thunder 7650.
- SCTP and the associated commands are not supported on Thunder 7650.
- Static NAT for SCTP is disabled on Thunder 7650 and the packets are L3-forwarded.

Thunder 7650 device displays warning messages for Static NAT and range lists when there is a mismatch in the source and NAT IPs.

Refer to the following examples:

```
7650-G9-Active(config)# cgnv6 nat inside source static 5.5.5.5 6.6.6.6
Invalid binding. Please match even source IP to even NAT IP and odd
source IP to odd NAT IP.<cr>
7650-G9-Active(config)# cgnv6 nat range-list r1 4.4.4.2 /24 5.5.5.7 /24
count 35
Invalid binding. Please match even source IP to even NAT IP and odd
source IP to odd NAT IP.<cr>
```

- Configuring NAT Inside and NAT Outside on the same interface (one-armed mode)

is not supported on Thunder 7650. To implement one-armed mode on a Thunder 7650, you must configure two ve Interfaces. One ve interface must be configured as NAT inside and the other must be configured as NAT outside.

- One-to-One NAT is not supported on Thunder 7650. The One-to-One NAT pool must have at least two IP addresses on this platform. If there are less than two NAT IPs, a warning message is displayed.
- While setting the application type, the `chassis-application-type` must be configured to "adc" before configuring any other command.
- Full Packet Distribution - One of the following two methods may be used:
 - For ESP and UDP 4500 to 4500 IPsec traffic, SPI value can be used for full packet distribution.
 - The “traffic-distribution-mode blade” can be configured under interface.
- Secure Sockets Layer Insight (SSLi) and related technologies are supported only on the Processing Unit 1.

Thunder 14045 Limitations

The following is a list of Thunder 14045 model limitations:

- GTP Firewall is not supported on TH14045.
- Virtual Chassis System (VCS) is not supported on Thunder 14045.
- TCP Logging is not supported on the Thunder 14045 and associated command is not available on the 14045 CLI. User cannot access the option to configure a TCP log server and service-group.
- NPTv6 is not supported on Thunder 14045. The `nptv6` command is not available on the 14045 CLI.
- SCTP is not supported on Thunder 14045; associated commands are not available in the CLI.
- Static NAT for SCTP is disabled on Thunder 14045 and packets are L3 forwarded.

Thunder 14045 device displays warning messages for Static NAT and range lists when there is a mismatch in the source and NAT IPs.

The following are examples:

```
14045-G9-Active(config)# cgnv6 nat inside source static 5.5.5.5 6.6.6.6
Invalid binding. Please match even source IP to even NAT IP and odd
source IP to odd NAT IP. <cr>
14045-G9-Active(config)# cgnv6 nat range-list r1 4.4.4.2 /24 5.5.5.7 /24
count 35
Invalid binding. Please match even source IP to even NAT IP and odd
source IP to odd NAT IP. <cr>
```

- Configuring NAT Inside and NAT Outside on the same interface (one-armed mode) is not supported on Thunder 14045. To implement one armed mode on a Thunder 14045, configure two ve interfaces. One ve interface must be configured as NAT inside and the other must be configured as NAT outside.
- One-to-One NAT is not supported on Thunder 14045. The One-to-One NAT pool must have at least two IP addresses on this Platforms. If there are less than two NAT IPs, a warning message is displayed.
- Application Delivery Controller features are not supported on the Thunder 14045.

Thunder 940/1040 Limitations

When using a 1G Fiber SFP on the 10G ports of a TH940 or TH1040, the following symptoms may occasionally occur: The port may not transition to UP state, it may take an unusually long time to do so, or the port LEDs may blink randomly.

As a workaround, try disabling and re-enabling the port through the command-line interface. This process may need to be repeated several times before the port comes up.

Thunder 5960 Limitations

Due to firmware limitations, customers are advised NOT to hot-swap the DC Power Supply Unit (PSU) on the Thunder 5960-0D10-H DC model. Doing so may cause the system to reboot or power down unexpectedly.

If PSU needs to be replaced, always power-down the unit completely, replace the PSU, and then power it back on.

Transceivers Not Purchased From A10 Networks May Show Error Message

If you purchase a third-party transceiver, the `show int media` output may return a “Media Unknown” error message.

Thunder 7460S, 7460S-MAX, and 7465 Platforms Limitation

The Thunder 7460S, 7460S-MAX, and 7465 platforms do not power up QSFP transceivers that consume more than 5 watts. When a high-power module is inserted, the system holds the LPMODE signal high, preventing the transceiver from initializing and causing the interface to remain down.

Schema Changes Impacting Backward Compatibility

This section describes the schema changes that have been made in versions 4.1.4.x and above, which might affect backward compatibility.

The following topics are covered:

/axapi/v3/cgnv6	86
/axapi/v3/vpn/ike-gateway	86
/axapi/v3/vpn/ike-gateway	87
/axapi/v3/vpn/ike-gateway	87
/axapi/v3/system/session/stats	88
/axapi/v3/slb and /axapi/v3/slb/template	90
/axapi/v3/file and /axapi/v3/import	90
/axapi/v3/interface	91
/axapi/v3/web-category	91
/axapi/v3/slb	92
/axapi/v3/glid	93
/axapi/v3/system/glid	94
/axapi/v3/router	97
/axapi/v3/router/isis	98
Various Schema Changes	99

/axapi/v3/cgnv6

The `tunnel-endpoint-address` has been removed from these objects in favor of `use-binding-table` for multiple tunnel support.

- /axapi/v3/cgnv6
- /axapi/v3/cgnv6/lw-4o6
- /axapi/v3/cgnv6/lw-4o6/global

Revise any existing calls to remove these from POST and PUT payloads from existing scripts before upgrading.

```
"tunnel-endpoint-address":{
    "type": "string",
    "format": "ipv6-address",
    "description": "Configure LW-4over6 IPIP Tunnel Endpoint Address (LW-4over6 Tunnel Endpoint Address)"
}
```

/axapi/v3/vpn/ike-gateway

The following properties are revised in this object so that the password of a key shall be reset to null when typing the `key keyname` command. See the *Command Line Interface Reference* for further information.

Table 11 : VPN IKE Gateway Key Revision

4.0 Key	4.1.4 Key
<pre>"key":{ "type":"object", "properties":{ "key-name":{ "type":"string", "format":"string", "minLength":1, "maxLength":64,</pre>	<pre>"key":{ "type": "string", "format": "string", "minLength": 1, "maxLength": 255, "description": "Private Key", "optional": true</pre>

Table 11 : VPN IKE Gateway Key Revision

4.0 Key	4.1.4 Key
<pre> "description": "Private Key File Name" }, "key-passphrase": { "type": "string", "format": "string", "minLength": 1, "maxLength": 127, "description": "Private Key Pass Phrase" } } } </pre>	<pre> }, "key-passphrase": { "type": "string", "format": "password", "minLength": 1, "maxLength": 127, "description": "Private Key Pass Phrase", "optional": true }, }, </pre>

/axapi/v3/vpn/ike-gateway

The following properties have been removed from this object so that `vrid default` is now `vrid 0` in VPN IKE-Gateway configurations, with the range revised from beginning with 1 to <0-31> (and <0-7> in partitions). If you were previously using `vrid default`, revise it after upgrading.

```

"default": {
    "type": "number",
    "format": "flag",
    "default": 0,
    "not": "vrid-num",
    "description": "Default VRRP-A vrid"
}

```

/axapi/v3/vpn/ike-gateway

The following properties in blue have been added to this object so that the CLI and GUI formats display the same.

```

"properties": {

```

```
"inside-ipv4-address": {
  "type": "string",
  "format": "ipv4-address"
},
"inside-ipv6-address": {
  "type": "string",
  "format": "ipv6-address"
}
}
```

/axapi/v3/system/session/stats

The following properties, which are not session specific, have been removed from this object so that the GUI will know which stats to leverage going forward.

```
"reverse_nat_tcp_ouner":{
  "type": "number",
  "format": "counter",
  "size": "8",
  "oid": "16",
  "description": "Reverse NAT TCP",
  "optional": true
},
"reverse_nat_udp_ouner":{
  "type": "number",
  "format": "counter",
  "size": "8",
  "oid": "17",
  "description": "Reverse NAT UDP",
  "optional": true
},
"ssl_failed_total":{
  "type":"number",
  "format":"counter",
  "size":"8",
  "oid":"28",
  "description":"Total SSL Failures",
  "optional":true
},
```

```
"ssl_failed_ca_verification":{
  "type":"number",
  "format":"counter",
  "size":"8",
  "oid":"29",
  "description":"SSL Cert Auth Verification Errors",
  "optional":true
},
"ssl_server_cert_error":{
  "type":"number",
  "format":"counter",
  "size":"8",
  "oid":"30",
  "description":"SSL Server Cert Errors",
  "optional":true
},
"ssl_client_cert_auth_fail":{
  "type":"number",
  "format":"counter",
  "size":"8",
  "oid":"31",
  "description":"SSL Client Cert Auth Failures",
  "optional":true
},
"total_ip_nat_conn":{
  "type":"number",
  "format":"counter",
  "size":"8",
  "oid":"32",
  "description":"Total IP Nat Conn",
  "optional":true
},
"client_ssl_ctx_malloc_failure":{
  "type": "number",
  "format": "counter",
  "size": "8",
  "oid": "34",
  "description": "Client SSL Ctx malloc Failures",
  "optional": true
},
```

/axapi/v3/slb and /axapi/v3/slb/template

The following proxy chaining properties have been removed from use with `/policy/{name}/forward-policy/action/{name}` actions of `forward-to-service-group` and `forward-to-internet` in favor of using with `forward-to-proxy` instead. If proxy-chaining was configured in 4.1.0 with `forward-to-service-group` and `forward-to-internet`, it will remain, but is not available with these in 4.1.4.

```
"proxy-chaining":{
  "type": "number",
  "format": "flag",
  "default": 0,
  "description": "Enable proxy chaining feature",
  "optional": true
}
```

/axapi/v3/file and /axapi/v3/import

The `csr-generate` has been removed from various places throughout these objects because CSR Generate should only appear for a local file name.

- `/axapi/v3/file`
- `/axapi/v3/file-ca-cert`
- `/axapi/v3/file-ssl-key`
- `/axapi/v3/import`
- `/axapi/v3/import-periodic`
- `/axapi/v3/import-periodic-ssl-cert`
- `/axapi/v3/import-periodic-ssl-crl`
- `/axapi/v3/import-periodic-ssl-key`

Revise any existing calls to remove these properties from POST and PUT payloads before upgrading.

```
"csr-generate":{
  "type": "number",
  "format": "flag",

```

```
"default": 0,  
"description": "Generate CSR file",  
"optional": true  
}
```

/axapi/v3/interface

DHCP has been removed from the following objects because DHCP was not supported, even if it was configured.

- /axapi/v3/interface
- /axapi/v3/interface-tunnel
- /axapi/v3/interface-tunnel-ip

After the upgrade, the dhcp configuration will be removed automatically. If an IP address is needed on tunnel interface, static addresses are supported.

```
"dhcp": {  
  "type": "number",  
  "format": "flag",  
  "default": 0,  
  "description": "Use DHCP to configure IP address"  
}
```

/axapi/v3/web-category

The server-timeout default parameter has been revised to 15 seconds.

```
"server-timeout": {  
  "type": "number",  
  "format": "number",  
  "minimum": 1,  
  "maximum": 300,  
  "default": 15,  
  "partition-visibility": "shared",  
  "description": "BrightCloud Servers Timeout in seconds (default: 15s)",  
  "optional": true  
}
```

/axapi/v3/slb

A variety of counter names have been revised in the following statistics:

- slb-server-port-stats
- slb-server-stats
- slb-service-group-member-stats
- slb-service-group-stats
- slb-template-cache-stats
- slb-virtual-server-port-stats
- slb-virtual-server-port-stats-cache

You will see the following type of example CLI output differences when `sampling-enable` is used:

```
ACOS (config) # slb perf sampling-enable
```

Table 12 : Server Load Balancing (SLB) Sampling Enable Statistic Name Revisions

4.0 Sampling Enable Stat Names	4.1.4 Sampling Enable Stat Names
all	all
total-throughput-bits-per-sec	total-throughput-bits-per-sec
l4-connection-rate	l4-conns-per-sec
l7-connection-rate	l7-conns-per-sec
l7-trans-per-sec	l7-trans-per-sec
ssl-connection-rate	ssl-conns-per-sec
ip-nat-connection-rate	ip-nat-conns-per-sec
total-new-connection-rate	total-new-conns-per-sec
total-current-connections	total-curr-conns
l4-bandwidth	l4-bandwidth
l7-bandwidth	l7-bandwidth

You will also see the following type of example responses in your GET requests:

```
curl -k GET https://10.10.10.10/axapi/v3/slb/virtual-
server/vs/port/80+tcp/stats \
-H "Content-Type:application/json" \
-H "Authorization: A10 c223169c3ab18f9e3826b9df215c2b"
```

Table 13 : Server Load Balancing (SLB) Virtual Port Statistic Name Revisions

4.0 Virtual Port Stat Names	4.1.4 Virtual Port Stat Names
<pre>{ "port": { "stats" : { "current-conns":0, "total-l4-conns":0, "total-l7-conns":7985, "total-tcp-conns":7985, "total-conns":7985, "total-fwd-bytes":2693024, "total-fwd-packets":35929, "total-rev-bytes":2104590, "total-rev-packets":16062, "total-dns-pkts":0, "total-mf-dns-packets":0, "es-total-failure-actions":0, "compression-bytes-before":0, "compression-bytes-after":0, "compression-hit":0, "compression-miss":0, "compression-miss-no-client":0, ... } } }</pre>	<pre>{ "port": { "stats" : { "curr_conn":126, "total_14_conn":13128, "total_17_conn":0, "total_tcp_conn":13128, "total_conn":13128, "total_fwd_bytes":6433228, "total_fwd_pkts":91901, "total_rev_bytes":6892903, "total_rev_pkts":52519, "total_dns_pkts":0, "total mf_dns_pkts":0, "es_total_failure_actions":0, "compression_bytes_before":0, "compression_bytes_after":0, "compression_hit":0, "compression_miss":0, "compression_miss_no_client":0, ... } } }</pre>

/axapi/v3/glid

ACOS 6.x and later releases include the following change in the glid schema.

- `num` is changed to `name`.
- `over-limit-action` and `action-value` are moved under `over-limit-cfg`.

The following **blue** properties are revised.

6.0.0 Key	Earlier Release Key
<pre>"glid-list": [{ "name": "1", "dns": { "action": "cache-disable" }, "dns64": { "disable": 0, "exclusive-answer": 0 }, "over-limit-cfg": { "over-limit-action": 1, "action-value": "drop" }, "uuid": "f3333540-181b-11ed-95dd- cd8833ee754b", "a10-url": "/axapi/v3/glid/1" }]</pre>	<pre>"glid-list": [{ "num": 1, "over-limit-action": 1, "action-value": "drop", "dns": { "action": "cache-disable" }, "dns64": { "disable": 0, "exclusive-answer": 0 }, "uuid": "f3333540-181b-11ed-95dd- cd8833ee754b", "a10-url": "/axapi/v3/glid/1" }]</pre>

/axapi/v3/system/glid

ACOS 6.x and later releases include the system glid as an object. The following **blue** properties are revised. The change is to ensure that this configuration is not lost during startup-config.

```
{
  "glid": {
    "glid-id": "10",
    "non-shared": 0,
    "uuid": "2fa309c6-63d3-11ed-8038-000c29f400ab",
    "a10-url": "/axapi/v3/system/glid"
  }
}
```

The following displays the complete schema details:



```
{
  "id": "/axapi/v3/system/glid",
  "type": "object",
  "node-type": "scalar",
  "title": "glid",
  "partition-visibility": "shared",
  "description": "Apply global limiter to the whole system",
  "properties": {
    "glid-id": {
      "type": "string",
      "format": "string-rlx",
      "minLength": 1,
      "maxLength": 1023,
      "partition-visibility": "shared",
      "$ref": "/axapi/v3/glid",
      "description": "Apply limits to the whole system",
      "optional": true
    },
    "non-shared": {
      "type": "number",
      "format": "flag",
      "default": 0,
      "partition-visibility": "shared",
      "description": "Apply global limit ID to the whole system at
per data cpu level (default disabled)",
      "optional": true
    },
    "uuid": {
      "type": "string",
      "format": "string",
      "minLength": 1,
      "maxLength": 64,
      "partition-visibility": "shared",
      "modify-not-allowed": 1,
      "description": "uuid of the object",
      "optional": true
    }
  }
}
```

```
}
```

/axapi/v3/router

The `ha-standby-extra-cost` has been revised in various places throughout these objects to support extra cost per VRID, rather than only for the default VRID.

- /axapi/v3/router
- /axapi/v3/router-ipv6
- /axapi/v3/router-ipv6-ospf
- /axapi/v3/router-isis
- /axapi/v3/router-ospf

The following properties in blue are new. After the upgrade, move existing default VRID costs to an array.

```
"ha-standby-extra-cost": {
  "type": "array",
  "minItems": 1,
  "items": {
    "type": "object"
  },
  "uniqueItems": true,
  "array": [{
    "properties": {
      "extra-cost": {
        "type": "number",
        "format": "number",
        "minimum": 1,
        "maximum": 65535,
        "description": "The extra cost value"
      },
      "group": {
        "type": "number",
        "format": "number",
        "minimum": 0,
        "maximum": 31,
        "description": "Group (Group ID)"
      }
    }
  ]
}
```

```

        },
        "optional": true
    }
}
}

```

/axapi/v3/router/isis

The multi field block used for the `set-overload-bit suppress` command was creating multiple instances for the `set-overload-bit` such that PUT operations would fail. The following properties in [blue](#) are revised.

Table 14 : Isis Revisions

4.0 Suppress-List	4.1.4 Suppress-Cfg
<pre> "suppress-list":{ "type": "array", "minItems": 1, "items": { "type": "object" }, "uniqueItems": true, "array": [{ "properties": { "suppress": { "type": "string", "format": "enum", "description": "'external': If overload-bit set, don't advertise IP prefixes learned from other protocols; 'interlevel': If overload-bit set, don't advertise IP prefixes learned from another ISIS level; ", "enum": ["external", "interlevel"] } }, "optional": true } }, </pre>	<pre> "suppress-cfg":{ "type": "object", "properties": { "external": { "type": "number", "format": "flag", "default": 0, "description": "If overload-bit set, don't advertise IP prefixes learned from other protocols" }, "interlevel": { "type": "number", "format": "flag", "default": 0, "description": "If overload-bit set, don't advertise IP prefixes learned from another ISIS level" } } } </pre>

Table 14 : Isis Revisions

4.0 Suppress-List	4.1.4 Suppress-Cfg
<pre>"optional": true } }] }</pre>	

Various Schema Changes

- The parameter `server hostname` is hidden in the CLI, but it can still be configured. Since the log-server's configured FQDN is unable to resolve, the changes related to this issue have been implemented in the 'setup/cm/schema/evtlog.sch' file.
- To match GUI/SNMP memory usage values with the CLI memory usage values, a set of memory usage data has been removed from the 'setup/cm/schema/system.sch' file. This change was made due to discrepancies between the memory usage values found in SNMP and the CLI.
- The `aaa-policy` has been removed from the output of `show amm` due to the `auth-failure-bypass` being displayed even when it is not configured. This change has been implemented in the 'setup/cm/schema/show/aam.sch' file.

Platform Migration

The process of upgrading ACOS software is designed to be smooth and simple. In the unlikely event or unforeseen failure circumstance, a rollback plan is outlined to revert to the previous version. The rollback for ACOS device is similar to the upgrade process.

Table 15 : Platform Migration Task

Tasks	Refer
Carefully review the restoring the system backup information.	Key Considerations
Download your current version ACOS software image.	Download Software Image
Review the boot order and change the boot order, if required.	Review Boot Order
Perform the upgrade instructions.	Upgrade Instructions
Restore the backed up configurations.	Restore Example
Perform the post-upgrade tasks.	Post-Upgrade Tasks

Restore from a Backup

You can use a saved backup to restore your current system, for example, when upgrading the devices in your network to the newer A10 Thunder Series devices.

Key Considerations

System Memory

If the current device has insufficient memory compared to the backup device (for example, 16 GB on the current device compared to 32 GB on the previous device), this can adversely affect system performance.

FTA versus Non-FTA

When restoring from an FTA device to a non-FTA device, some commands may become unavailable after the restore operation. These commands are lost and cannot be restored.

For example, the `cpu-process` command will be missing post-restore.

L3V Partitions

L3v partitions and their configurations are restored. However, if you are restoring to a device that supports a fewer number of partitions (for example, 32) than you had configured from the backup device (for example, 64) any partitions and corresponding configuration beyond 32 will be lost.

Port Splitting

If you are restoring between devices with different 40 GB port splitting configurations, see [Table 16](#).

Table 16 : Restore Behavior for Port Splitting Combinations

Backup Device	Current Device	Behavior During the Restore Operation
Port splitting disabled or enabled.	Port splitting disabled or enabled.	Allow user to perform port mapping (See Port Mapping .)
Port splitting enabled.	Port splitting disabled.	Ask the user if they want to perform port mapping. If yes, enable port splitting, reboot the device, and then perform the restore operation again, where port mapping will be enabled.
Port splitting disabled.	Port splitting enabled.	Exit the restore operation. The user will have to perform a <code>system-reset</code> or disable port splitting, reboot the system, and then perform the restore operation again.

Port Mapping

When restoring from a device that has a different number of ports, or even the

same number of ports, you can map the port number from the previous configuration to a new port number (or same port number) in the new configuration.

In cases where the original number of ports is greater than the number of ports on the new system, some configurations may be lost.

If you choose to skip port mapping (see the example below), then the original port numbers and configurations are preserved. If the original device had ports 1-10 configured, and the new device only has ports 1-8, and you skip port mapping, then ports 9 and 10 are lost. If you choose port mapping, you can decide which 8 out of the original 10 ports you want to preserve during the port mapping process.

Restore Example

This section provides an example of a restore operation:

- The backup is restored from version 4.1.1-P1 to 4.1.1-P2.
- The system memory on the original device is 8 GB but is 16GB on the new device.
- The number of interfaces on the original device is 10, but the new device has 12.

CLI Configuration

See the highlighted lines in the following example output along with the corresponding comments that are marked with “<--” characters:

```
ACOS(config)# restore use-mgmt-port
scp://root@192.168.2.2/root/user1/backup1
Password []?
```

A10 Product:

Object	Backup device	Current device
Device	TH1030	TH3030
Image version	4.1.1-P1	4.1.1-P2
System memory:		
Object	Backup device	Current device
Memory (MB)	8174	16384

```

Checking memory: OK.
Ethernet Interfaces:
      Object                Backup device        Current device
-----
      Total                10                  12
      1 Gig                1-10                1-12
Do you want to skip port map?(Answer no if you want port mapping
manually.)
[yes/no]: no

Please specify the Current device to Backup device port mapping
1-10 : a valid port number in backup device.
0    : to skip a port
-1   : to restart port mapping.

Current Port:      Backup device port
Port 1  :          2 <-- port 2 on the backup device is re-numbered
to 1
Port 2  :          1 <-- port 1 on the backup device is re-numbered
to 2
Port 3  :          0
Port 4  :          0
Port 5  :          0
Port 6  :          0
Port 7  :          0
Port 8  :          0
Port 9  :          0
Port 10 :          0

The current startup-configuration will be replaced with the new
configuration that was imported.
Do you wish to see the diff between the updated startup-config and the
original backup configuration?
[yes/no]: yes

Modified configuration begin with "!#"

!Current configuration: 277 bytes

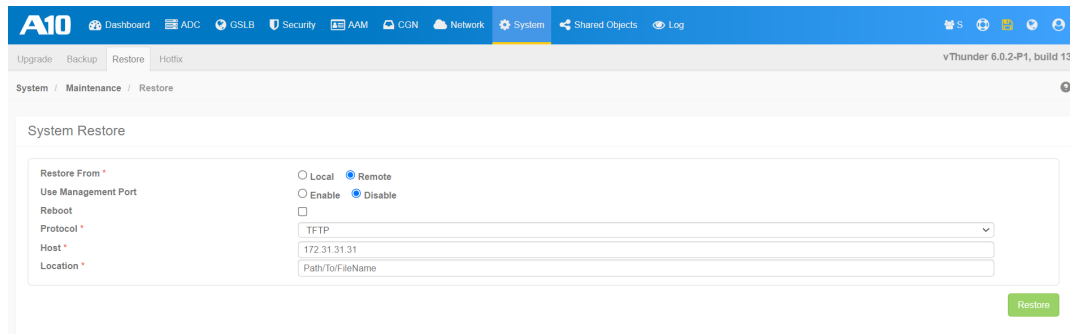
```

```
!Configuration last updated at 05:38:18 UTC Fri Mar 17 2017
!Configuration last saved at 05:38:19 UTC Fri Mar 17 2017
!64-bit Advanced Core OS (ACOS) version 4.1.1-P2, build 112 (Mar-13-
2017,15:41)
!
interface management
  ip address 192.168.210.24 255.255.255.0
  ip default-gateway 192.168.210.1
!#interface management
!# ip address 192.168.210.24 255.255.255.0
!# ip default-gateway 192.168.210.1
!# exit-module
!
interface ethernet 2
!#interface ethernet 1 <-- original port 1 is now port 2
  exit-module
!
interface ethernet 1
!#interface ethernet 2 <-- original port 2 is now port 1
  exit-module
!
!#interface ethernet 3
!# exit-module
!
!#interface ethernet 4
!# exit-module
!
!#interface ethernet 5
!# exit-module
!
!#interface ethernet 6
!# exit-module
!
!#interface ethernet 7
!# exit-module
!
!#interface ethernet 8
!# exit-module
```

```
!  
!  
end  
Complete the restore process?  
[yes/no]: yes  
  
Please wait restore to complete: .  
Restore successful. Please reboot to take effect.
```

GUI Configuration

1. Log in to ACOS Web GUI using your credentials.
2. Navigate to **System >> Maintenance >> Restore**.



The screenshot shows the ACOS Web GUI interface. The top navigation bar includes 'A10' and various system modules like Dashboard, ADC, OSLB, Security, AAM, CGN, Network, System, Shared Objects, and Log. The breadcrumb trail is 'System / Maintenance / Restore'. The main content area is titled 'System Restore' and contains the following configuration options:

- Restore From *
 - Local
 - Remote
- Use Management Port
 - Enable
 - Disable
- Reboot
 -
- Protocol *
 - TFTP
- Host *
 - 172.31.31.31
- Location *
 - Path/To/FileName

A green 'Restore' button is located at the bottom right of the form.

3. On the **Restore** page, choose the appropriate options.
4. Click the **Help** icon to open the Online Help for more details.

A10 Networks Security Advisories

The A10's Product Security Incident Response Team (PSIRT) is dedicated for responding to A10's product security incidents. Independent researchers or third parties that are experiencing product security are strongly encouraged to contact PSIRT. To contact PSIRT, provide detailed information about the vulnerability and send an email to psirt@a10networks.com.

For information on A10 Networks Security Advisories that specifically address how CVE issues affect our products, go to:

<https://support.a10networks.com/support/security-advisories>

APPENDIX Basic Functionality Testing

This section lists ([Table 17](#)) the fundamental functionality testing and troubleshooting guidelines that you can perform before and after the upgrade.

NOTE: This is not a complete list for testing all the ACOS functionalities. The testing may differ from system to system and depending on the features or modules in your environment. Refer to the respective product documentation.

Table 17 : Basic Testing & Troubleshooting

Testing Guidelines	CLI Commands	GUI Menu
System Basic Checks (All Products)		
Verify the ACOS version.	<pre>show version</pre> <p>OR</p> <pre>show version inc ACOS</pre>	Navigate to Dashboard >> System >> System Info.
Verify the boot image area from where the ACOS software image is loaded.	<pre>show bootimage</pre>	Navigate to Dashboard >> System >> System Info.
Check the ACOS hardware information.	<pre>show hardware</pre> <p>OR</p> <pre>show hardware inc Storage</pre>	Navigate to Dashboard >> System >> System Info.
	<pre>show cpu</pre> <p>OR</p> <pre>show cpu history</pre>	Navigate to Dashboard >> System >> Device Info. OR Navigate to Dashboard >> System >> Control CPU.

Table 17 : Basic Testing & Troubleshooting

Testing Guidelines	CLI Commands	GUI Menu
	<code>show memory</code> OR <code>show memory system</code>	Navigate to Dashboard >> System >> Device Info. OR Navigate to Dashboard >> System >> Realtime Memory Usage.
	<code>show disk</code>	Navigate to Dashboard >> System >> Device Info.
Check the system and A10 resource usage information.	<code>show system resource-usage</code>	Navigate to System >> Settings >> Resource Usage.
	<code>show resource-accounting</code>	Navigate to System >> Settings >> Resource Accounting.
Check and verify the interface and networking information.	<code>show interfaces brief</code>	Navigate to Network >> Interface >> LAN. Click Statistics.
	<code>show trunk</code>	Navigate to Network >> Interface >> Trunks.
	<code>show lacp trunk summary</code>	Navigate to Network >> Interface >> Trunks. Click Statistics.
	<code>show ip interfaces</code> OR <code>show ipv6 interfaces</code>	Navigate to Network >> Interface.
	<code>show interfaces media</code>	

Table 17 : Basic Testing & Troubleshooting

Testing Guidelines	CLI Commands	GUI Menu
	<code>show ip route</code>	Navigate to Network >> Routes .
	<code>show run interface ethernet <interface number></code>	Navigate to Network >> Interfaces >> LAN .
Verify the VRRP-A information.	<code>show vrrp-a detail</code>	Navigate to System >> VRRP-A >> Global Stats . OR Navigate to System >> VRRP-A >> VRID Stats .
Verify the common configurations.	<code>show running-config</code>	Navigate to System >> Settings >> Configuration File .
	<code>show startup-config</code>	Navigate to System >> Settings >> Configuration File .
	<code>show run health</code>	Navigate to ADC >> Health Monitors >> Statistics >> Health Stats .
View the history and system logs.	<code>show history</code>	Navigate to Dashboard >> System >> System Audit Log . Click GUI, CLI, or aXAPI .
	<code>show audit</code>	Navigate to Dashboard >> System >> System Audit Log .
	<code>show log</code> OR <code>show log begin <date></code>	Navigate to Dashboard >> System >> System Log .

Table 17 : Basic Testing & Troubleshooting

Testing Guidelines	CLI Commands	GUI Menu
	<code>show varlog</code> OR <code>show varlog tail</code> <code>20</code>	NA
ADC and SSLi Basic Checks		
View the server and virtual server information.	<code>show slb virtual-server</code>	Navigate to ADC >> SLB >> Virtual Servers . Click Statistics .
	<code>show slb service-group</code>	Navigate to ADC >> SLB >> Service Groups . Click Statistics .
	<code>show slb server</code>	Navigate to ADC >> SLB >> Service Groups . Click Statistics Details .
	<code>show slb resource-usage</code>	Navigate to System >> Settings >> Resource Usage >> SLB Resource Usage .
	<code>show session</code>	Navigate to ADC >> SLB >> Session .
View the server health and statistics.	<code>show health monitor</code>	Navigate to ADC >> Health Monitors >> Statistics .
	<code>show health stat</code>	
View the SSL certificate information.	<code>show pki cert</code>	Navigate to ADC >> L7 >> Statistics >> SSL >> PKI .
	<code>show pki ca-cert</code>	
View the SSL statistics.	<code>show slb ssl error</code>	Navigate to ADC >> L7 >> Statistics >> SSL >> SSL Stats .
	<code>show slb ssl stats</code>	Navigate to ADC >> L7 >> Statistics >> SSL >> SSL Stats .

Table 17 : Basic Testing & Troubleshooting

Testing Guidelines	CLI Commands	GUI Menu
	<code>show slb ssl-counters</code>	Navigate to ADC >> L7 >> Statistics >> SSL >> SSL Counters .
CGNAT Basic Checks		
View the CGNAT server information or statistics of DNS and syslog servers.	<code>show cgnv6 server</code>	Navigate to CGN >> Services >> Servers . Click Statistics .
View the CGNAT template logging configuration.	<code>show run cgnv6 template logging</code>	Navigate to CGN >> Templates >> Logging .
View the CGNAT statistics.	<code>show cgnv6 nat pool statistics</code>	Navigate to CGN >> Stats .
	<code>show cgn lsn statistics</code>	
	<code>show cgnv6 nat pool statistics top 10 users</code>	
	<code>show cgnv6 nat64 statistics</code>	

See Also

- For details on all the commands, see *Command Line Interface Reference*.
- For details on all the GUI menu or options, see *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/.