ACOS 6.0.8
Release Notes

December, 2025

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

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 6.x.x

Harmony Controller Integration Deprecated

Starting from the ACOS 6.0.8 release, integration of Harmony Controller is no longer supported.

Instead, ACOS 6.0.8 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 A10 Control Documentation and A10 Control Integration Guide.

JWT Cache Expiration Change

In the prior releases, the JSON Web Token (JWT) cache expiration was limited to a maximum value of 86400 seconds.

Starting from the ACOS 6.0.8 release, you can configure the default JWT cache expiration time up to 2592000 seconds using the `jwt-exp-default` command.

This improvement provides greater flexibility for deployments where JWTs are reused for extended periods, reducing repeated token validations and improving system performance. For more information, see *Application Access Management* and *Command Line Interface Reference*.

Scaleout Traffic-Map Change

In the prior releases, ACOS maintained separate traffic-map for IPv4 and IPv6 traffic.

Starting from the ACOS 6.0.8 release, ACOS now uses the same traffic-map for both IPv4 and IPv6 traffic. A new command `scaleout apps separate-v4-v6-traffic-map enable` has been introduced to revert to the earlier behavior and maintain separate traffic-maps for IPv4 and IPv6. For more information, see *Command Line Interface Reference*.

show web-category Command Deprecated

Starting from the ACOS 6.0.8 release, the `show web-category version` command is deprecated and you can use `show web-category license` to check the configured web category version.

The following example shows the configured web category type value is `New`

```
ACOS#show web-category license
Module Type                     : New
Module Status                   : Disabled
License Status                  : License is valid
License Type                    : show license-info for webroot type
License Expiry                  : show license-info for expiration
Remaining Period                : show license-info for expiration
Grace Period Status             : show license-info for grace period
Grace Period                    : show license-info for grace period
UUID/SN                         : TH33075E21040038
```

Webroot SDK changes

When you upgrade to Webroot SDK version 5.38, the following CLI options are no longer supported:

web-category configuration:

- **database-server**

- **port**

web-category-proxy-server configuration:

- **http-port**

- **auth-type ntlm**

TACACS+ Server Counter Changes

In the prior releases, the `show tacacs-server` command displayed TACACS+ server counters such as socket opens, closes, timeouts, errors, and packets received/sent when executed from an L3V partition.

Starting from ACOS 6.0.7 , the TACACS+ server counters are no longer displayed when running `show tacacs-server` from an L3V partition. To view TACACS+ server statistics, the same command must now be executed from the shared partition.

For more information, refer to the *Management Access and Security Guide* and *Command Line Interface Reference Guide*.

SNMP CM Subagent Deprecated

Starting from the ACOS 6.0.5 release, 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 subject to limited support. It is recommended to avoid their usage.

Local Log Buffer Changes

In the prior releases, the maximum number of messages per second that can be sent to the local log buffer, was between 1-100 messages per second, with a default of 32 messages per second.

Starting from ACOS 6.0.5 , the the maximum number of messages per second has been changed to 1-500, with a default value of 64 messages per second.

SMB and NTLM Authentication Protocols Deprecated

Starting from the ACOS 6.0.5 release, as the SMB (Server Message Block) and NTLM (NT LAN Manager) authentication protocols are insecure, and outdated, they are deprecated and removed from ACOS to eliminate potential vulnerabilities.

Updated Partition Limit Per Platform

The Application Delivery Partition (ADP) software limits per platform have been updated based on the RAM capacity. In addition, the maximum supported partition limit for FTA platforms has been capped to 255 L3V partitions.

NOTE:	A10 recommend that customers consult with the A10 Sales team when considering a partition limit more than the supported 255 L3Vs on FTA platforms to ensure optimal performance and system stability.

For more information, see Supported Number of Partitions Per Platforms.

GLM Configuration Synchronization Changes

Starting from the ACOS 6.0.4 release, the GLM configurations are no longer automatically synced from vMaster to vBlade. It allows unique GLM configurations on each device. The required configurations must be manually configured on each device.

For more information, see Global License Manager User Guide.

DNSSEC Signature Validity Check Done Everyday

Starting from ACOS 6.x release, the validity of DNSSEC signatures is now checked everyday. This ensures that if the signatures are due to expire in the next 1 or 2 days, they are duly resigned well on time.

ADC Multi-PU Deployment with VRRP-A Changes

Starting from ACOS 6.x release, the ADC with VRRP-A (traffic distribution using VRID) on the multi-PU platform is no longer supported. As a result, all related configurations will be removed after upgrading from ACOS 5.x.x to ACOS 6.x.x.

However, the ADC multi-PU deployment using IP address was introduced. This deployment utilizes the client-side and server-side (odd-even NAT) IP addresses to determine the traffic distribution to PU1 and PU2.

For more information, refer to the *Application Delivery Controller Guide*.

aVCS Multicast IP Address Change

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 IP address can be changed to 224.0.0.210 by following the steps below:

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

ACL Sequence Number

Starting from the ACOS 6.0.0 release, the ACL sequence number is explicitly displayed in the running and startup config. The sequence number remains constant after reload or reboot. The configurations will be synchronized between vMaster and vBlade.

Call Home Enabled By Default

Starting with ACOS 5.2.1-P8 and 6.0.2, the ACOS Call Home feature is now enabled by default. This feature enables all participating ACOS devices on your premises to send information securely on how A10 products are used to the A10 Product Research team. This information includes configuration and environmental data such as the ACOS device model, its form factor, deployment location (such as on-premise or public cloud), number of interfaces, L3V partitions, VLANs, and more. Additionally, it collects information on the active ACOS licenses installed on the device.

All information collected by A10 is processed in accordance with A10 Networks' Data Processing Addendum. All information received through the Call Home feature is anonymized and used purely to enhance our products and improve quality. For a complete list of the information collected by Call Home, see the **Call Home** Chapter in the *ACOS System Configuration and Administration Guide*.

A10 Next-Gen WAF Changes

Starting from ACOS 6.0.1, ACOS authenticates A10 Next-Gen WAF (NGWAF) access requests through the Global License Manager (GLM). A valid license must be acquired from the GLM to use A10 NGWAF. However, the procedure to import and configure NGWAF on ACOS is the same as the previous releases.

Web Application Firewall Changes

Starting from ACOS 6.0.0 release, the Web Application Firewall (WAF) is no longer supported. Therefore, all WAF configurations will be unsupported after upgrading from ACOS 5.x.x or ACOS 4.1.4-GR1-Px to ACOS 6.x.x. However, the A10 Next Generation Web Application Firewall (NGWAF) is introduced to provide enhanced Layer 7 protection.

NGWAF is an application security monitoring system that monitors suspicious and anomalous web traffic and protects against attacks directed at applications and origin servers. It provides superior protection for applications and APIs by delivering several advantages over legacy WAF.

For more information, see the *Next Generation Web Application Firewall Configuration guide*.

SSL/TLS Management Plane Changes

ACOS management plane access through SSL/TLS will not support the following SSL/TLS ciphers when configured in FIPS mode. Only Perfect-Forward Security (PFS) ciphers will be supported.

- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_AES_128_CBC_SHA256

- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_RSA_WITH_AES_128_GCM_SHA256

- TLS_RSA_WITH_AES_256_GCM_SHA384

SSL/TLS Data Plane Changes

ACOS data plane SSL/TLS will not support the following SSL/TLS ciphers when configured in FIPS mode:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_AES_128_CBC_SHA256

- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_RSA_WITH_AES_128_GCM_SHA256

- TLS_RSA_WITH_AES_256_GCM_SHA384

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

- TLS1_DHE_RSA_CHACHA20_POLY1305_SHA256

- TLS1_ECDHE_RSA_CHACHA20_POLY1305_SHA256

- TLS1_ECDHE_ECDSA_CHACHA20_POLY1305_SHA256

- TLS1_ECDHE_SM2_WITH_SMS4_SM3

- TLS1_ECDHE_SM2_WITH_SMS4_SHA256

- TLS1_ECDHE_SM2_WITH_SMS4_GCM_SM3

ACOS data plane SSL/TLS will not support the following SSL/TLS protocols when
configured for FIPS mode of operation:

- TLS 1.1

- TLS 1.0

- SSLv2

- SSLv3

Scaleout Changes

Starting from ACOS 6.0.0, the Scaleout for Server Load Balancing (SLB) is not supported. Therefore, all SLB Scaleout configurations will be unsupported after upgrading from ACOS 5.x.x to ACOS 6.x.x.

For more information, see the *Scaleout Configuration Guide*.

Single Node Mode in Scaleout Cluster

Starting with ACOS 6.0.0, the quorum number requirement of N/2+1, where N is the total number of nodes, is not applicable anymore. The Scaleout cluster does not require a minimum of N/2+1 number of nodes to be active. In addition, the Single Node Mode is not supported in the Scaleout cluster.

BGP Peer Group Changes

Starting from ACOS 6.0.0, the following CLI options are not supported for the BGP peer-group:

- `neighbor neighbor-id capability-orf`

- `neighbor neighbor-id default-originate`

- `neighbor neighbor-id disallow-infinite-holdtime`

- `neighbor neighbor-id distribute-list`

- `neighbor neighbor-id filter-list`

- `neighbor neighbor-id next-hop-self`

- `neighbor neighbor-id prefix-list`

- `neighbor neighbor-id send-community`

- `neighbor neighbor-id unsuppress-map`

Least-Request Load-Balancing Server Selection Method Changes

Starting from ACOS 6.0.1, the least-request method does not consider the weight configured on the real server for server selection during load-balancing. Instead, it bases the server selection on the request count, which consider the HTTP/HTTPS requests that are sent to the server but have not received responses.

Default Behavior Changes Introduced in ACOS 5.x.x

ACOS Routing Protocol Support Changes

ACOS routing protocols will not support MD5 authentication when configured in FIPS mode. This affects the following protocols:

- Border Gateway Protocol (BGP)

- Open Shortest Path First Version 2 (OSPFv2) and Version 3 (OSPFv3)

- Intermediate System to Intermediate System (ISIS)

- Routing Information Protocol (RIP)/RIPv2

- Bidirectional Forwarding Detection (BFD)

For more information about the ACOS configuration commands and options of these routing protocols impacted, see the *System Configuration and Administration Guide* and the *Command Line Reference Guide*.

System Table Integrity

In the ACOS 5.2.1-P2 release, the System Table Integrity Check aXAPI and configuration have changed.

- Prior to 5.2.1-P2, the following command was used to check the table integrity for the ARP, ND6, IPv4 FIB, IPv6 FIB, and MAC tables:

```
ACOS(config)#system table-integrity-check [enable]
```

- From 5.2.1-P2, the following command is used to enable or disable the table integrity checks and auto-sync options:

```
ACOS(config)#system table-integrity all audit [enable | disable] auto-
sync [enable | disable]
```

For more information, see System Table Integrity Support under Platform in the Release Notes. Also, see 'system table-integrity' in the CLI Reference Guide.

System CPU Load Sharing Changes

In the previous releases, when a CPU receives a packet of an overloaded CPU and if no session exists for the packet, the packet is dropped by default, and the session is not established.

With the ACOS 5.2.1-P2 release, the packet is not dropped by default. Instead, the packet is sent to the overloaded CPU, where a new session is established. When a packet of the same session is received next time, the CPU processes the packet.

The following command can be used not to allow the new sessions to be created by default:

```
ACOS(config)#system cpu-load-sharing disallow-new-sessions [tcp | udp]
```

HTTP/2 Feature Changes

Previously, ACOS supported HTTP/2 traffic on HTTP virtual port by default. From ACOS 5.2.1-P2 release, the 'support-http2' command must be configured at the virtual server port level for HTTP virtual port to process HTTP/2 traffic.

Default SSL Version Changed for Client-SSL

The default SSL version of Client-SSL template is changed from Transport Layer Security (TLS) 1.3 to TLS 1.2. Hence, in case you need TLS 1.3 support, then you must update the Secure Sockets Layer (SSL) version to TLS 1.3 under the Client-SSL template using the GUI.

Certificate Command Management Changes

In ACOS 5.2.1-P2, the SSL certificate management was enhanced to include the cert, key, and chain-cert information together for forward proxy features. For more information, refer *ACOS 5.2.1-P2 New Features and Enhancements.*

Similarly, the certificate command was introduced in the previous releases for SSL offloading features to configure the cert, key, and chain-cert information together.

Currently, the following certificate-specific commands are available under the client-SSL template:

- **certificate** <cert-name> **key** <key-name> [**pass-phrase** <pass-phrase-str>]
  [**chain-cert** <chain-cert-name>] [**partition** <shared>]

- **forward-proxy-ca-certificate** <cert-name> **key** <key-name> [**pass-phrase**
  <pass-phrase>] [**chain-cert** <chain-cert-name>] [**partition** <shared>]

- **forward-proxy-alt-sign cert** <cert-name> **key** <key-name> [**pass-phrase**
  <pass-phrase>] [**chain-cert** <chain-cert-name>] [**partition** <shared>]

- s**erver-name cert** <cert-name> [**chain** <chain-name> | **key** <key-name> [**pass-phrase** <string> | **alternate** | **partition** <shared>]

Hence, all the previously configured old certificate commands (mentioned below) available in the startup profile shall be converted and mapped to the new certificate commands during upgrade/migration.

Client-SSL Template:

- cert
- cert-alternate
- chain-cert
- key
- key-alternate

- forward-proxy-ca-cert

- forward-proxy-ca-key

Server-SSL Template:

- cert

- key

NOTE:	The old cert or key commands are not supported in aXAPI.

Starting with ACOS 6.0.0, if the old chain-cert command is configured and the partition option matches, the forward-proxy-alt-sign cert and server-name commands shall be migrated, and the chain-cert shall be added.

Additionally, you must make sure to check and verify if all the old certificate commands (mentioned in the above list) have the matching partition option before upgrading/migrating to the latest ACOS version. This will ensure that all the previously configured certificate commands are converted and mapped to the new certificate commands effortlessly and efficiently.

NOTE:	Make sure to back up the ACOS 4.1.4.x startup profile. This ensures that if you downgrade from ACOS 5.2.1 or later release to ACOS 4.1.4.x, you can rollback the ACOS 4.1.4.x startup profile with the old certificate configuration.

CAUTION:	If you downgrade without taking the backup, then the new certificate command will not revert back to the old certificate commands, and it becomes invalid for ACOS 4.1.4.x and older releases. Also, SSL templates will not bind to virtual ports.

aXAPI Changes for VRRP-A Ethernet Interface VLAN Options

The aXAPI to retrieve or manipulate the VLAN options of the VRRP-A ethernet interface command has changed from 5.1.x release.

For the following CLI command:

```
ACOS(config)#vrrp-a interface ethernet 1
ACOS(config-ethernet:1)#vlan 2
```

```
ACOS(config-ethernet:1)#vlan 3
```

The aXAPI GET will display the following results for 5.1.0 and above releases:

```
/axapi/v3/vrrp-a/interface/ethernet/
{
"ethernet-list": [
{
"ethernet-val":1,
"vlan-cfg": [
{
"vlan":2
},
{
"vlan":3
}
],
"no-heartbeat":0,
"uuid":"df157986-cf17-11eb-8e95-e6fca04a9b02",
"a10-url":"/axapi/v3/vrrp-a/interface/ethernet/1"
}
]
}
```

The aXAPI GET will display the following results for prior 5.1.0 releases:

```
/axapi/v3/vrrp-a/interface/ethernet/
{
"ethernet-list": [
{
"ethernet-val":1,
"vlan": [
2,
3
],
"no-heartbeat":0,
"uuid":"df157986-cf17-11eb-8e95-e6fca04a9b02",
"a10-url":"/axapi/v3/vrrp-a/interface/ethernet/1"
}
]
}
```

Upgraded SHA1 Hash Algorithm to SHA256

With this release, the enable password HASH algorithm is upgraded from SHA1 to SHA256. Consider the following points:

- After upgrading to the latest version, the existing SHA1 encrypted enable password is verified to ensure it works as expected.

- After configuring SHA256 encrypted enable password in the latest version, if you downgrade to the earlier release, the enable password is set to the default empty password. An enable password error log may appear in some of the older versions. In this case, you have to set the enable password again.

SLB Virtual Server ACL Changes

The aXAPI to create an SLB virtual server with a specific payload that configures access-lists under the virtual-port objects has changed from the 5.2.1-P2 release. The aXAPI changes are as follows:

```
{
"port": {
"protocol": "tcp",
"port-number": 10,
"acl-list": [
{
"acl-id-shared": "1",
"v-shared-partition-pool-id": 1,
"v-acl-id-src-nat-pool-shared":"test"
},
{
"acl-name-shared":"test",
"v-shared-partition-pool-name": 1,
"v-acl-name-src-nat-pool-shared":"test"
}
]
}
}
```

IPsec Changes

From the ACOS 5.2.1-P3 release, IPsec is supported on the ACOS management plane and the data plane.

IPsec is included in the scope for FIPS Level 2 certification and both planes. From the ACOS 5.2.1-P5 release, when ACOS is configured in FIPS mode, IPsec will not support the following capabilities:

- Internet Key Exchange Version 1 (IKEv1)

- EAP-Radius or EAP-TLS authentication

- Message Digest Algorithm 5 (MD5) or Null hashes

- Diffie-Hellman (DH) Groups 0, 1, 2, and 5

- Data Encryption Standard (DES), 3DES, or Null encryption

- Pre-shared keys (PSK) strings less than 8 characters in length

Interface Order Changes

In release prior to 5.2.0, the interface order is mgmt, sriov/pci-passthrough, virtio/netvsc/vmxnet3. This order has been changed to mgmt, virtio/netvsc/vmxnet3, sriov/pci-passthrough. You will observe the following:

- On fresh install of vThunder, the interfaces will be detected in new order.

- On an upgrade from releases before 5.2.0 to 5.2.0-P1, the old interface order will be changed to new order.

WAF Template Configuration Changes

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 WAF template configuration does not work as expected.

To upgrade the WAF template configuration, follow the below mentioned steps:

1. Login to https://support.a10networks.com/support/axseries using your GLM credentials.

2. On the **Software Downloads and Documentation** page, jump to section **Tools**, expand the **Other Tools and Updates**, and click **Download Zip File** next to **WAF Configuration Migration Script for ACOS 5.x**.

   The script to upgrade the WAF template configuration (`waf_migrate_conf.pl`) will be downloaded to your machine.

3. Copy this script to a remote machine.

NOTE:	The remote machine must be capable of executing Perl scripts.

4. Copy the 4.x configuration (old-config) from the A10 device to the remote machine. Execute the following command on the A10 device (in `config` mode).

   ```
   ACOS(config)# copy [running-config| startup-config] [use-mgmt-port]
   scp://[user@]host/old-config
   ```

5. Generate the new Web Application Firewall (WAF) template configuration (new-config) by executing the following command on the remote machine,

   ```
   ./waf_migrate_conf.pl old-config > new-config
   ```

6. Upgrade the system to 5.x.

7. Copy the newly generated configuration (new-config) from the remote machine to the A10 device. Execute the following command on the A10 device (in `config` mode),

   ```
   ACOS(config)# copy [use-mgmt-port] scp://[user@]host/new-config
   [running-config| startup-config]
   ```

The newly generated Web Application Firewall (WAF) template configuration will work seamlessly on 5.x. The old configuration (old-config) remains unchanged. The script does not modify the old configuration.

IPsec VPN License Changes

The Convergent Firewall (CFW) platforms no longer enable IPsec functionality by default. The changes are applicable from ACOS versions 4.1.4-GR1-P2 and 5.1.0-P3

Feedback

and above.

The IPsec perpetual license must be obtained from GLM and installed on the device for IPsec functionality to work.

For more information, refer to the *Global License Manager User Guide*.

Platforms Support Information

This section summarizes the platforms support information:

The following topics are covered:

Platforms Compatibility Matrix

For the latest updates on the supported platforms, see Platform Compatibility Matrix.

Splitter Cable Support

The Quad Small Form-factor Pluggable (QSFP) port can be configured to serve a dual purpose. A 40-Gigabit Ethernet port can be configured as one 40 Gigabit port or four 10-Gigabit ports.

NOTE: For your specific hardware model *Installation Guide* for more information on configuration, see **Splitter Cable Support for QSFP 40G Ports**.

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.

Feedback

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

Hardware Product Licenses

The following topics are covered:

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

 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

Feedback

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 6655(S)	✔	6.0.4
Thunder 6440		

Table 5 : Modular Licenses Support Matrix

Thunder Devices	Modular Licensing Support	Minimum Release
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 6.0.8

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 *Installation Guide* for Thunder Physical Appliance.
- For instruction on installing vThunder, see *Installation Guide* for Thunder Virtual Appliance.
- For instructions on installing cThunder, see *Installation Guide* for Thunder Container.
- For instructions on installing ACOS on Bare Metal, see *Installation Guide* for 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

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 3rd Generation Hardware Platforms cannot be upgraded to ACOS 6.x version. For more information, see Platforms Compatibility Matrix.

- 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.	Platforms Compatibility Matrix
Check the availability of SKUs or product licenses.	Hardware Product Licenses
Review the ACOS Upgrade path.	Upgrade path
Check the storage 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
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.

Revisit the Platforms Compatibility Matrix table to check which software version is compatible with your hardware model.

Table 7 : ACOS Upgrade Path

Existing Version	First Hop	Second Hop
4.1.x	4.1.x to 5.x	5.x to 6.x
5.1.x	5.1.x to 5.2.x	5.2.x to 6.x
5.2.x	5.2.x to 6.x	

NOTE:	If you are upgrading from ACOS 2.7.x, then the first hop is migrating to 4.1.x version. For detailed instructions, see *ACOS 2.7x to 4.x Migration Guide*.

Upgrade Requirements

The system requirements for ACOS software are as follows:

vThunder	vCPUs	Memory	Storage
Small_4 vCPUs	4	8 GB	40 GB
Small_8 vCPUs	8	16 GB	60 GB
Medium	16	32 GB	80 GB
Large	32	64 GB	100 GB

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

Feedback

Table 8 : Write Memory Command Usage

Command	Descriptions
`<profile-name>`	the current partition.
`write memory <profile-name> all-partitions`	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**.
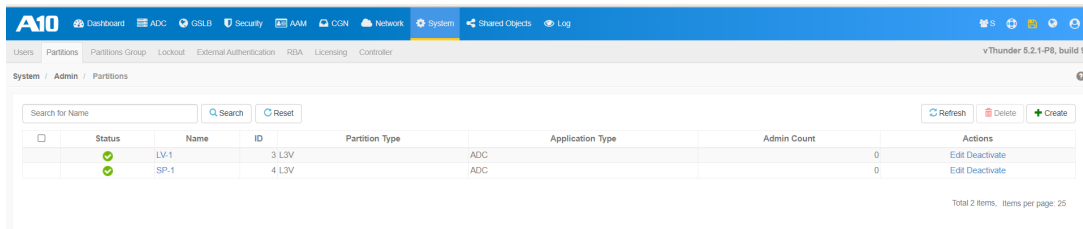
3. To view the configuration profiles of the partitions, navigate to **System >> Settings >> Configuration File**.
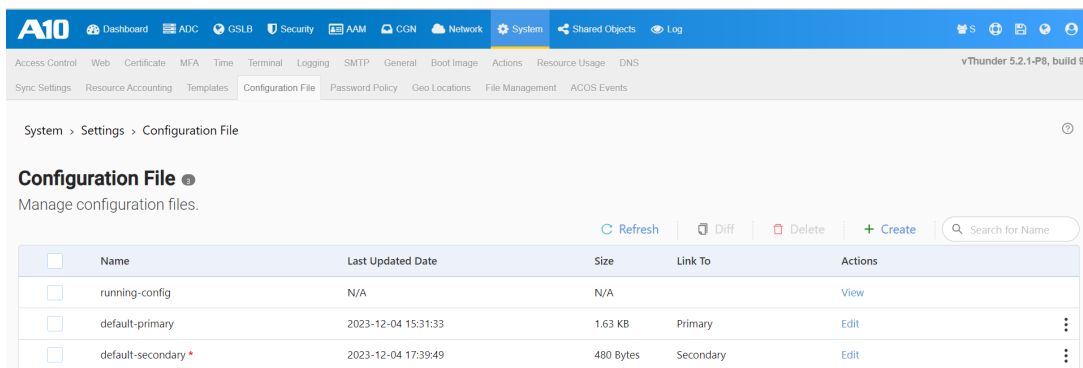
4. To save the partition configuration, navigate to **System >> Settings >> Action**.
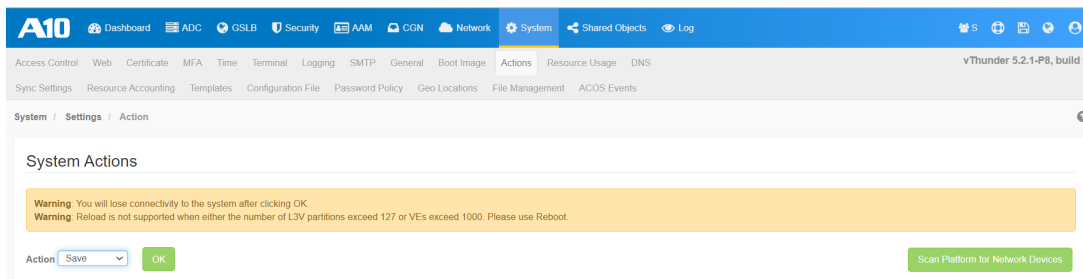
5. Select the **Save** option from the **Action** drop-down list.

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

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 **(*)**.
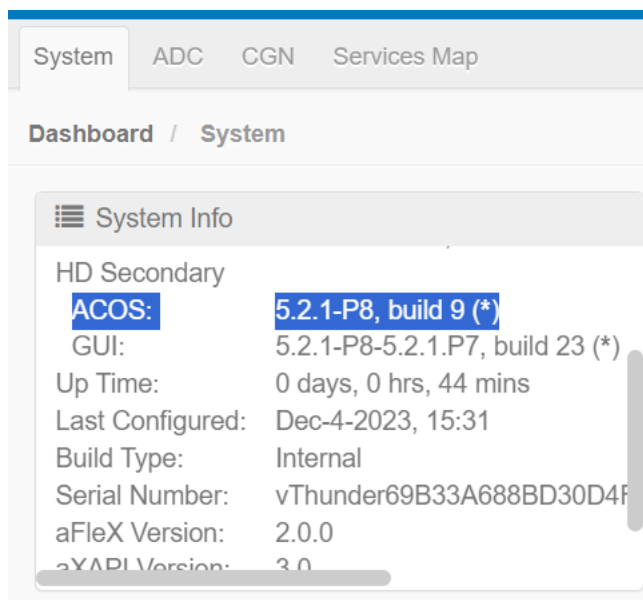
3. To change the boot order, navigate to **Dashboard >> Settings >> Boot Image**.
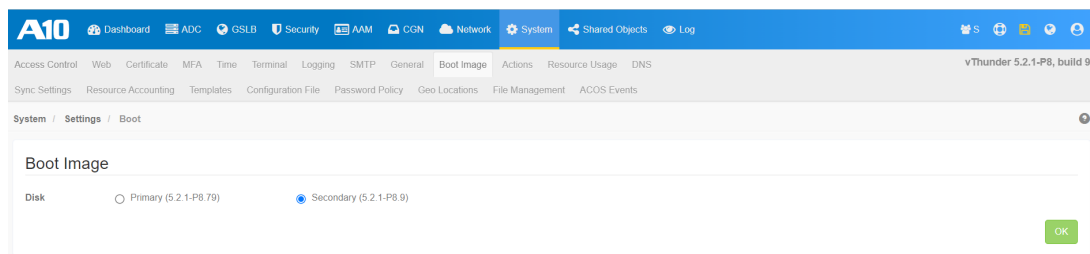
4. Choose the boot order and click **OK**.

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*.

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 uses 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**.
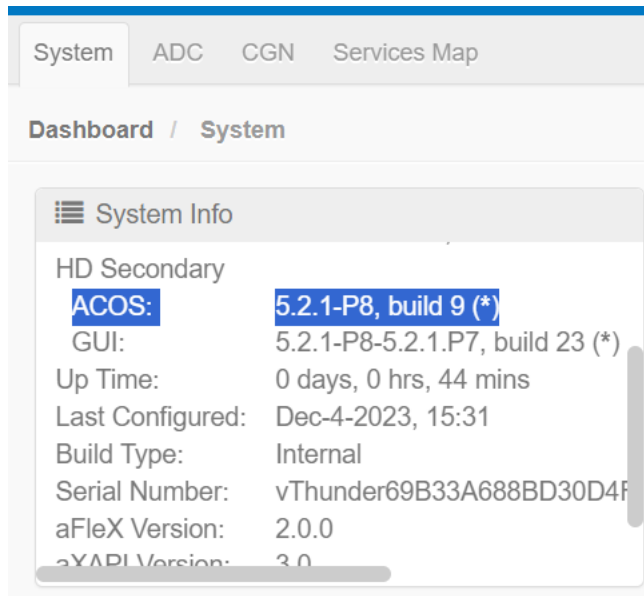
Download the Software Image

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>ONEIMG.upg`

   ○ For non-FTA enabled platforms (including vThunder), use the image with the file name: `ACOS_non_FTA_<version>ONEIMG.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:

Feedback

- [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/backupfi
le.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/backuplo
g.tar.gz
```

GUI Configuration

1. Log in to ACOS Web GUI using your credentials.

2. Navigate to **System >> Maintenance >> Backup**.
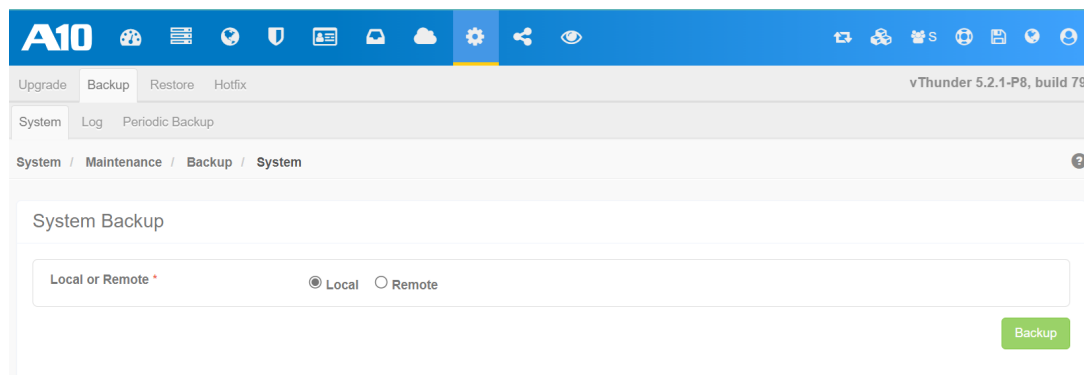
3. Select one of the following tabs:

Feedback

- *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**.
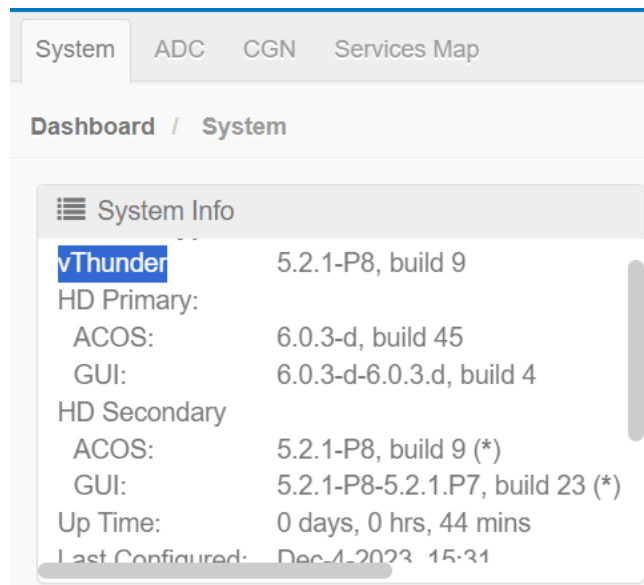
Check the Software Version

Navigate to **Dashboard >> System >> System Info**.
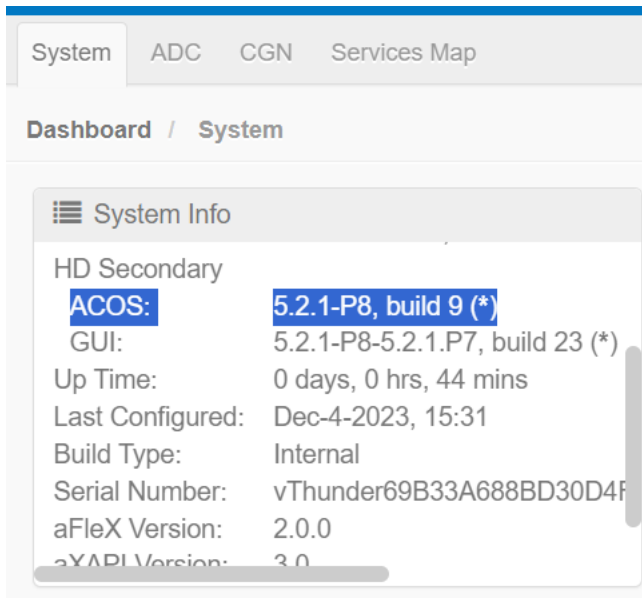
Check the Disk Space and Memory Usage

Navigate to **Dashboard >> System >> Device Info**.
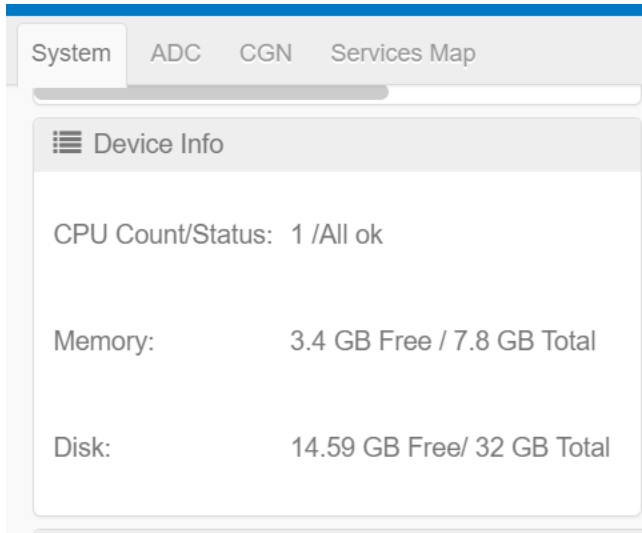
Check the System Boot Order

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

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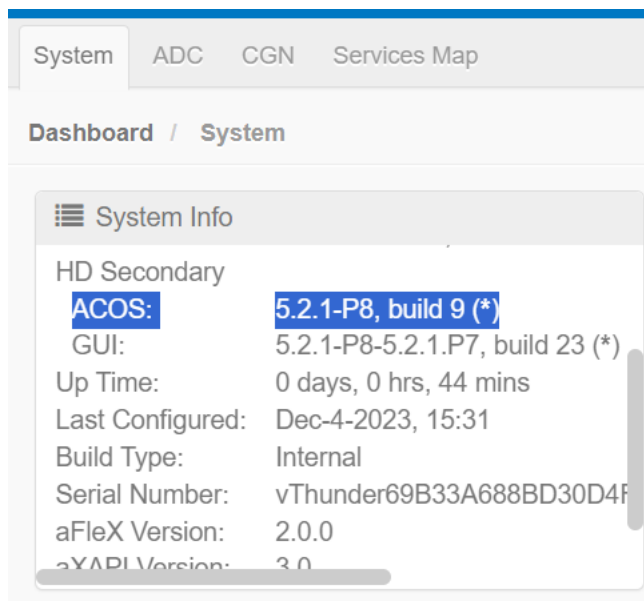
Perform Backup

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-5-x(config)# upgrade hd sec show-percentage
   scp://admin@2.2.2.2/images/ACOS_FTA_<version>ONEIMG.upg
   ```

   - On a non-FTA device:

   ```
   ACOS-5-x(config)# upgrade hd sec show-percentage
   scp://admin@2.2.2.2/images/ACOS_non-FTA_<version>ONEIMG.upg
   ```

   To upgrade from secondary hard disk to primary:

   - On an FTA device:

   ```
   ACOS-5-x(config)# upgrade hd pri show-percentage
   scp://admin@2.2.2.2/images/ACOS_FTA_<version>ONEIMG.upg
   ```

   - On a non-FTA device:

   ```
   ACOS-5-x(config)# upgrade hd pri show-percentage
   scp://admin@2.2.2.2/images/ACOS_non-FTA_<version>ONEIMG.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**.
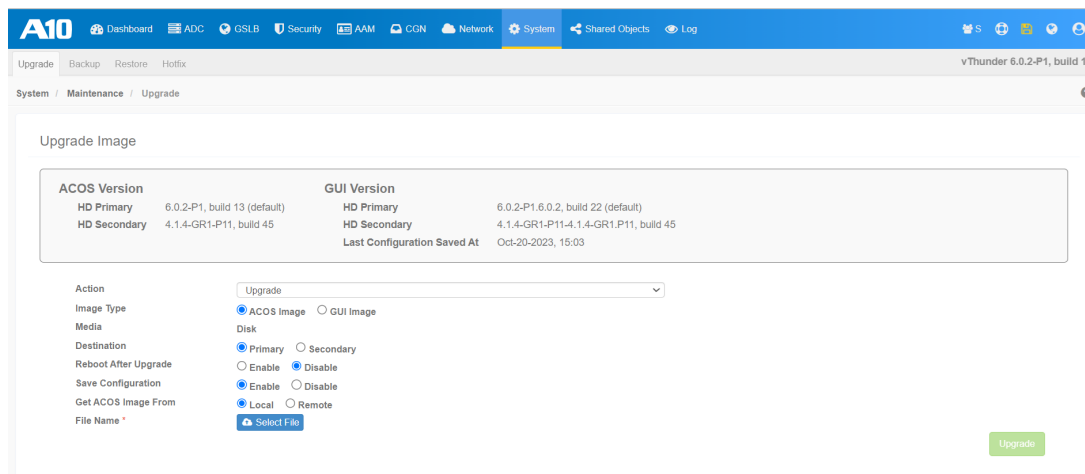
3. On the **Upgrade** page, choose the **Upgrade** option from the **Action** field.

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 6.0.7-P2 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	ADC	CGN	Services Map

Dashboard / System

☰ 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
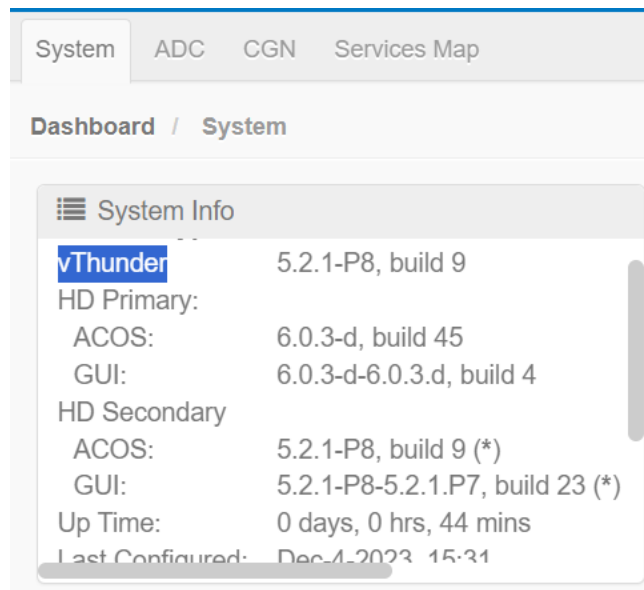
Validate Imported License

Navigate to **System >> Admin >> Licensing**.
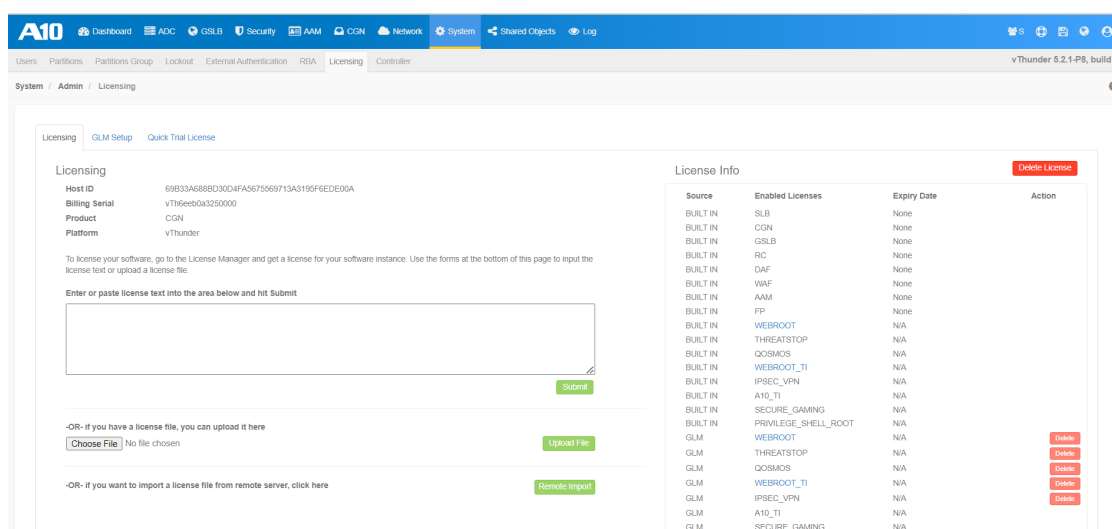
Verify Configuration Profiles

Navigate to **System >> Configuration File**.
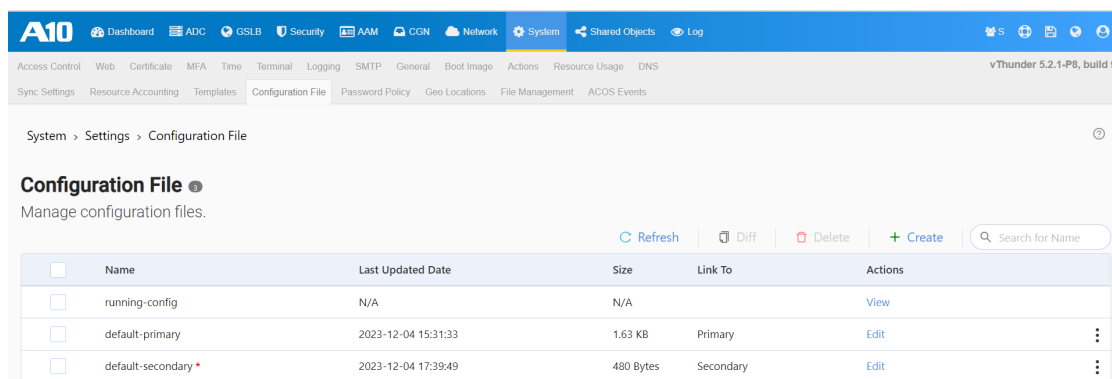
Perform Basic Testing

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/backupfi
   le.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
   ```

Feedback

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.
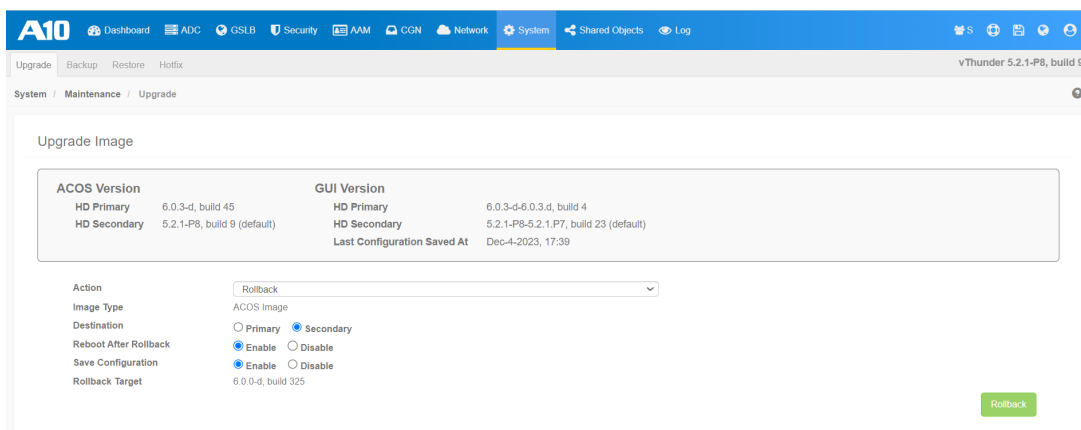
6. By default, the upgraded **Image Type** is selected.

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 6.0.7-P2 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 backup the system.

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

- Full Chassis Upgrade (with VRRP-A) – This procedure upgrades the software on the vMaster for full chassis upgrade deployments with 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 VRRP-A) (Recommended) – This procedure applies to staggered upgrade deployments with 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 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 VRRP-A)

This section describes the staggered upgrade procedure with 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-P2

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

Software and Hardware Limitations

This section lists the software and hardware limitations in ACOS.

The following topics are covered:

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

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
```

```
vrrp-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 axedebug/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 VPPR-A Deployments

If vThunder (Virtual Thunder) is deployed with VRRP-A l3-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.

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

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 media`CLI is currently not supported on Thunder 3350 series.

Thunder 7650 Feature 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 Feature 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 Feature 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.

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.

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:

ACOS 6.0.8 Release Notes

Schema Changes Impacting Backward Compatibility

Feedback

/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

``
"key":{
        "type":"object",
        "properties":{
            "key-name":{
                "type":"string",
                "format":"string",
                "minLength":1,
                "maxLength":64,
``
	``
	"key":{
	        "type": "string",
	        "format": "string",
	        "minLength": 1,
	        "maxLength": 255,
	        "description": "Private
	Key",
	        "optional": true
	``

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_ounter":{
        "type": "number",
        "format": "counter",
        "size": "8",
        "oid": "16",
        "description": "Reverse NAT TCP",
        "optional": true
},
"reverse_nat_udp_ounter":{
        "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_donn":{
        "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-connectionss	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
| ```
{
  "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,

...
``` | ```
{
"port": {
"stats" : {
"curr_conn":126,
"total_l4_conn":13128,
"total_l7_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,
...
``` |

/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
```"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"` `}` `]```	```"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"` `}` `]```

/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
```"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"] }, ```	```"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" } } } ```

Table 14 : Isis Revisions

4.0 Suppress-List	4.1.4 Suppress-Cfg

`"optional": true`
`}`
`}]`
`}`	

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 `system-reset` 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
```
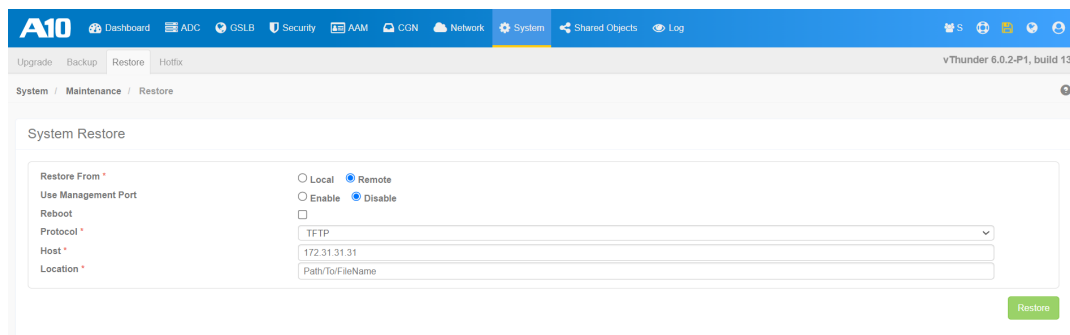
```
!Configuration last updated at 05:38:18 UTC Fri Mar 17 2017
!Configuration last saved at 05:38:19 UTC Fri Mar 17 2017
!64-bit Advanced Core OS (ACOS) version 4.1.1-P2, build 112 (Mar-13-
2017,15:41)
!
interface management
  ip address 192.168.210.24 255.255.255.0
  ip default-gateway 192.168.210.1
!#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**.

3. On the **Restore** page, choose the appropriate options.

4. Click the **Help** icon to open the Online Help for more details.

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.	`show version`
	
	OR
	
	`show version | inc ACOS`
		Navigate to **Dashboard >> System >> System Info**.

Verify the boot image area from where the ACOS software image is loaded.	`show bootimage`	Navigate to **Dashboard >> System >> System Info**.

Check the ACOS hardware information.	`show hardware`
	
	OR
	
	`show hardware | inc Storage`
		Navigate to **Dashboard >> System >> System Info**.

	`show cpu`
	
	OR
	
	`show cpu history`
		Navigate to **Dashboard >> System >> Device Info**.
		
		OR
		
		Navigate to **Dashboard >> System >> Control CPU**.

Feedback

Table 17 : Basic Testing & Troubleshooting

Testing Guidelines	CLI Commands	GUI Menu

	`show memory`
	
	OR
	
	`show memory system`
		Navigate to **Dashboard >> System >> Device Info**.
		
		OR
		
		Navigate to **Dashboard >> System >> Realtime Memory Usage**.

	`show disk`	Navigate to **Dashboard >> System >> Device Info**.
Check the system and A10 resource usage information.	`show system resource-usage`	Navigate to **System >> Settings >> Resource Usage**.
	`show resource-accounting`	Navigate to **System >> Settings >> Resource Accounting**.
Check and verify the interface and networking information.	`show interfaces brief`	Navigate to **Network >> Interface >> LAN**. Click **Statistics**.
	`show trunk`	Navigate to **Network >> Interface >> Trunks**.
	`show lacp trunk summary`	Navigate to **Network >> Interface >> Trunks**. Click **Statistics**.

	`show ip interfaces`
	
	OR
	
	`show ipv6 interfaces`
		Navigate to **Network >> Interface**.

	`show interfaces media`	

Feedback

Table 17 : Basic Testing & Troubleshooting

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

Table 17 : Basic Testing & Troubleshooting

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

Feedback

Table 17 : Basic Testing & Troubleshooting

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

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*.