A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3

Common Criteria Configuration Guide

25-January-2023

Revision: 1.0 (NDcPPv2.2e AGD)

TABLE OF CONTENTS

1. INTRODUCTION 1

1.1 Intended Audience 1
1.2 TOE Documentation 1
1.3 Evaluation Scope 1
1.3.1 TOE Models Evaluated 2
1.3.2 Elements Included in the TOE Operational Environment 3
1.3.3 Elements Excluded from the TOE via Guidance 4
1.3.4 Operational Environment Assumptions 5

2. SECURE INSTALLATION AND CONFIGURATION 6

2.1 Physical Installation 6
2.2 Initial Setup via TOE Local Console 6
2.2.1 Initial Connection and FIPS Mode Confirmation 6
2.2.2 Basic System Parameters Configuration 7
2.2.3 Establish an IPsec Tunnel for Connections in the Operational Environment 9
2.2.4 Verify and Ensure Software Version 11
2.2.5 Restrict Management Traffic to Ping/Traceroute and IPsec Tunnel 11
2.2.6 Enable Remote SSH Management Access 12

3. SECURE MANAGEMENT 13

3.1 Managing Administrators 13
3.2 Password Management 15
3.3 Session Termination 16
3.3.1 Graceful Termination 16
3.3.2 Inactivity Termination 16
3.4 Login Banners 16
3.4.1 CLI Login Banner 16
3.4.2 Web/GUI Login Banner 16
3.5 System and Network Time Configuration 17
3.5.1 System Time Configuration 17
3.5.2 Network Time (NTP) Configuration 17
3.6 Failed Authentication Lockout 17
3.7 Audit Logging 19
3.7.1 Local Logging 19
3.7.2 Remote Logging to Syslog 19
3.7.3 IPSec and X.509 Logging 20
3.8 File Servers 21

3.9 Trusted Updates 22
3.10 Remote Management 23
3.10.1 SSH Clients via IPsec 23
3.10.2 Web/GUI Clients via IPsec 23
3.11 X.509 Certificate and Key Management 25
3.11.1 Generate Private Key + Certificate Signing Request (CSR), Export CSR 26
3.11.2 Generate Certificates Signed by the CA 27
3.11.3 Import Signed Certificates 27
3.11.4 Import Root CA Certificates 27
3.11.5 Zeroization on Security-Reset 28
3.12 Certificate Revocation 29
3.12.1 CRL Revocation 29
3.12.2 OCSP Revocation 29
3.13 IPsec Tunnel Management 30
3.13.1 IPsec Supported on the TOE 30
3.13.2 Configure a VPN IKE Gateway 31
3.13.3 Configure a VPN IPsec Tunnel 33
3.13.4 ACL Rules 35
3.13.5 IPsec Tunnel Debugging 36
3.14 Boot Time Integrity Self-Tests 37

4. ACRONYMS 38

APPENDIX A. AUDIT LOG ENTRIES 40

A.1 Audit Record Entries 40
A.1.1 CLI Audit Records 40
A.1.2 Web/GUI Audit Records 40
A.2 Event Record Entries 41
A.1.2 Event Records 41
A.3 Audit Log Entry Samples 42

REVISION HISTORY 61

ABOUT A10 NETWORKS 62

DISCLAIMER

1. INTRODUCTION

This document provides customer guidance for configuring and using A10 Thunder Series appliances running A10's Advanced Core Operating System (ACOS) 5.2.1-P3 in NDcPP-evaluated Target of Evaluation (TOE) configurations.

This document includes a description of the evaluated configuration.

1.1 INTENDED AUDIENCE

This document is intended for administrators responsible for installing, configuring, and/or operating ACOS 5.2.1-P3 on A10 Thunder Series appliances. Configuration guidance information in this document is intended to support administrators deploying these appliances in environments that is consistent with the configuration evaluated as part of the product's Common Criteria (CC) testing process.

A10 Thunder Series appliances support great deal of security functions, but only those the claimed Protection Profile (PP) are addressed in this document. Any functions not described in this document or its corresponding Security Target were not evaluated and should be exercised at the customer's risk.

1.2 TOE DOCUMENTATION

The products in the evaluation scope are described in the following documents, downloadable from the A10 Networks support web site (https://support.a10networks.com). An A10 Networks support login ID and password is required to access online documentation.

- A10 Thunder Series Installation Guides (for the given Thunder model)
  - A10 Thunder Series 6435(S)/5435/4435
  - A10 Thunder Series 7440-11/5840-11
  - A10 Thunder Installation Reference Guide Series: TH7445/TH5845
  - A10 Thunder Installation Reference Guide Series: TH7655/7650

- ACOS Configuration Guides
  - ACOS 5.2.1-P3 - System Configuration and Administration Guide
  - ACOS 5.2.1-P3 - Management Access and Security Guide
  - ACOS 5.2.1-P3 - Command Line Interface Reference
  - ACOS 5.2.1-P3 - IP Security Configuration Guide

The information is largely derived from these documents, albeit summarized to describe the configuration a TOE as part of the 'evaluated configuration'.

1.3 EVALUATION SCOPE

This section describes the components included in the TOE's evaluated configuration, environmental components that support the TOE's security behaviour, or are environmental components outside the scope of evaluation for the TOE.

1.3.1 TOE Models Evaluated

The following products were evaluated against the NDcPP v2.2e protection profile.

MODELS	DESCRIPTION
TH-4435	A10 Networks Thunder TH-4435 appliance
TH-5840-11	A10 Networks Thunder TH-5840-11 appliance
TH-7445	A10 Networks Thunder TH-7445 appliance
TH-7650-11	A10 Networks Thunder TH-7650-11 appliance
TH-7655	A10 Networks Thunder TH-7655 appliance

Table 1: Evaluated TOE Models

Model specific hardware and TOE configurations are shown in Table 2.

	TH-4435	TH-5840-11	TH-7445
1/10 GE Fiber (SFP+) Ports	16	48	48
100 GE Fiber	-	4 (QSFP28)	4 (QSFP28)
Management Ports	1 x Ethernet, 1 x RJ-45 Console, 1 x Lights Out Management		
Processor	Intel E5-2680v2 (10-cores)	Intel E5-2695v4 (18-cores)	2x Intel E5-2695v4 (36-cores)
Microarchitecture	Ivy Bridge	Broadwell	Broadwell
Memory	64 GB	64 GB/128 GB	128 GB
Storage	SSD	SSD	SSD
Hardware Acceleration	FTA-3, SPE	2 x FTA-4	3 x FTA-4, SPE
Data Plane Processor	Yes	Yes	Yes
Rack Units (mountable)	1 RU	1 RU	1 RU

	TH-7650-11	TH-7655
1/10 GE Fiber (SFP+) Ports	48	-
100 GE Fiber	4 (QSFP28)	16 (QSFP28)
Management Ports	1 x Ethernet, 1 x RJ-45 Console, 1 x Lights Out Management	
Processor	2x Intel Gold 6258R (56-cores)	2x Intel Gold 6258R (56-cores)
Microarchitecture	Cascade Lake	Cascade lake
Memory	256 GB	384 GB
Storage	SSD	SSD
Hardware Acceleration	2 x FTA-5	2 x FTA-5, SPE
Data Plane Processor	Yes	Yes
Rack Units (mountable)	1.5 RU	1.5 RU

Table 2: TOE Appliances Models

1.3.2 Elements Included in the TOE Operational Environment

The following table lists elements in the TOE's operational environment tested in the evaluated configuration. These non-TOE elements are recommended or required for the operational environment.

ELEMENT	DESCRIPTION
SYSLOG (audit log) Server	The TOE communicates with SYSLOG servers via IPsec for remote storage of audit and logging events reported by the TOE management and control planes.
NTP Servers	The TOE communicates with NTP servers via IPsec to synchronize date and time.
SSH Clients	The TOE can be managed via IPsec from terminal clients on remote administrator workstations accessing the management Command Line Interface (CLI) of the TOE.
Web GUI Browser Clients	The TOE can be managed via IPsec from web browsers on remote administrator workstations accessing the management web GUI of the TOE.
File Servers	The TOE communicates with file servers via IPsec to transfer files for purposes including: • configuration backup (restoration) from (to) the TOE • updates of the TOE • exporting and copying information from the TOE • importing information, including credentials and other data, to the TOE • loading management CLI and Web GUI credentials to the TOE
Distribution Points	The TOE communicates with CRL and OCSP distribution points via HTTP to confirming the validity and revocation status of certificates.

Table 3: Non-TOE Management Elements

1.3.3 Elements Excluded from the TOE via Guidance

The following items are excluded from the TOE. To maintain compliance with the TOE CC evaluated configuration, do not configure their related services or capabilities.

1. Remote servers/services configuration
    a. External Authentication (Radius, TACACS+, LDAPS)
    b. Brightcloud Service for Web Category
    c. Webroot Service for Threat Intelligence
    d. A10 Harmony Controller Management
    e. A10 Global or Enterprise License Management (GLM, ELM)
    f. A10 Global Server Load Balancing (GSLB) Peers
    g. RESTful AXAPI Client Applications
    h. SMTP Mail Servers
    i. SNMP Remote Management
    j. HTTPS File Servers

2. IPsec/IKE configuration settings
    a. Encryption Algorithms: DES, 3DES, Null (no encryption)
    b. Hashing Algorithms: MD5, Null (no hash)
    c. Diffie-Hellman Groups: 1, 2, 15, 16, 18, 19, 20
    d. IKEv1 Key Exchange

3. Key generation and CSR settings
    a. Key size (in bits): 1024, 4098
    b. Digest type: SHA-1

4. Digital signature generation with SHA-1

5. Non-FIPS mode of operation

6. IPv6 configuration of the TOE management plane

7. Management connections using TOE data ports (e.g. only TOE management port should be used)

8. Compact Flash, GUI Image updates

9. Thunder Lights-Out Management (LOM) port

1.3.4 Operational Environment Assumptions

To ensure an A10 Thunder appliance can meet its security requirements when deployed a CC evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile.

- **Physical security:** It is necessary to install the TOE in a physically secure environment where only authorized administrators can physically access to the device, including its local (serial) console.

- **Limited functionality:** The TOE must only be used for its intended networking purpose. The TOE is a closed-system and does not support general-purpose computing capabilities. Only appliance specific interfaces are supported, including CLI (local console and remote SSH via IPsec) and GUI (via remote HTTPS/TLS via IPsec) for management of the TOE. For example, general OS Shell access is not available from the appliance.

- **No through traffic protection:** The security boundary of the CC-evaluated configuration is limited to traffic to and from the TOE management plane. The intent is for the TOE to protect secure data sourced from or directed to the TOE, including administrative and audit data. Traffic passing through the TOE's data plane to/from other network entities is not within the NDcPP scope. Protection of such data plane traffic is assumed to be covered separately by under applicable Extended Profile cPPs.

- **Trusted administration:** The TOE product does not provide mechanisms to protect against the threat of a rogue or otherwise malicious administrator. It is the responsibility of the organization to appropriate vet and train security administrators prior to granting them access to manage the TOE.

- **Regular updates:** A10 Networks provides regular product updates for A10 Thunder products. These include bug and security fixes as well as functionality enhancements. It is expected that administrators are reasonably diligent in ensuring that software updates to the TOE are applied regularly as they are made available.

- **Secure admin credentials:** The TOE protects credentials stored on the TOE and which may be used to access the TOE. Administrators of the TOE are trusted to maintain security and integrity consistent with the organization's security policy.

- **Residual information**: It is the responsibility of Security Administrators to ensure that there is no unauthorized access is possible for sensitive residual information (e.g. cryptographic keys, passwords, etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

2. SECURE INSTALLATION AND CONFIGURATION

To ensure that the TOE operates per the evaluated configuration, apply the configuration settings outlined in this chapter.

NOTE: **It is assumed that any prior configuration saved on the device from any prior used will be lost in this process.**

2.1 PHYSICAL INSTALLATION

Prepare of the physical site and install the TOE hardware by unpacking the hardware, rack mounting it, connecting the TOE's Ethernet Management for a local network, and connecting TOE's console port for access from a terminal server.

2.2 INITIAL SETUP VIA TOE LOCAL CONSOLE

Initial configuration of the TOE must be performed via the local console of the device prior to connecting to any network. At any time during this process the **`write memory`** CLI command may be issued to write all unsaved changes to the ACOS startup-config.

Note that help is available from the CLI by entering question mark (?) at a CLI prompt to show available CLI commands. In addition, typing a question mark (?) after a given CLI commands will reveal supported command options or option values selections. For example:

```
ACOS(config)# host?
  hostname  Set system's network name
ACOS(config)# hostname ?
  NAME<length:1-31>  This System's Network Name
ACOS(config)# hostname ACOS-dev
  <cr>
ACOS-dev(config)#
```

Cryptographic engine parameters are all preconfigured at the factory or are defaulted in the TOE. They should not be changed by the administrators of the TOE.

Note that when the TOE is booted it will perform various self-tests. If any of the tests fail, the TOE will enter into an error state until an Administrator reboots the TOE. If this condition persists, contact A10 Networks support (https://support.a10networks.com) to resolve the issue.

2.2.1 Initial Connection and FIPS Mode Confirmation

The FIPS mode of operation is required for the CC evaluated configuration. To ensure that the TOE is operating in FIPS mode, perform the following procedure.

1. Connect to the TOE via the local console using a terminal application.

2. Authenticate using default ACOS credentials and enter the global configuration mode.

```
login as: admin
Password: a10$pass      (for device configured in FIPS-mode)
          a10           (for device configured in Non-FIPS-mode)
```

3. Confirm FIPS mode of operation is configured. Using the **`show version`** command observe the that "fips" is as a platform feature. If "fips" is indicated, then the TOE is configured for FIPS mode. If not indicated or the "Platform Features" line are not indicated, then the TOE is configured for Non-FIPS mode. For example:

```
ACOS> show version | include fips
      Platform features: fips
```

4. Enter ACOS Privileged EXEC configuration mode.

```
ACOS> enable
ACOS# config
ACOS(config)#
```

5. If TOE is configured in Non-FIPS mode:
   a. Change the TOE to FIPS-mode using the **`system fips`**

```
ACOS(config)#system fips ?
  disable  Disable fips
  enable   Enable fips
We have to login from console to execute this command :

ACOS(config)#system fips enable
```

   b. Reboot the system using the **`reboot`** CLI command.
   c. Go back to Step #1 above.

2.2.2 Basic System Parameters Configuration

Configure basic parameters for the TOE system and as indicated below.

1. Change the TOE default password of the "admin" ACOS root administrator account using the **`admin password`** CLI command where ***`pw-string`*** is the new password string and is at least 8 characters long.

```
ACOS(config)# admin password pw-string
```

2. Set the system date/time and time zone using the **`clock`** and **`timezone`** CLI commands; respectively. For example:

```
ACOS(config)# timezone America/Los_Angeles
ACOS(config)# clock set 10:31:00 February 21 2021
```

3. Set a hostname, DNS servers, and DNS suffix for the TOE **`hostname`**, **`ip dns [primary | secondary]`**, and **`ip dns suffix`** CLI commands; respectively. For example:

```
ACOS(config)# hostname ACOS-dev
ACOS-dev(config)# ip dns primary 10.1.1.8
ACOS-dev(config)# ip dns suffix abccorp.com
```

4. Configure the CLI Login Banner using the **banner login** CLI command. This banner is displayed prior to the prompting for credentials when the ACOS CLI is accessed locally on the TOE console or remotely via SSH over IPsec. The banner can be entered in a single command or in multi-line mode where the banner content is prompted for entry by the CLI. For example:

```
ACOS-dev(config)# banner login Welcome to Login Mode
ACOS-dev(config)# banner login multi-line
Input a string to mark the end of banner text, up to 2 characters:
bb
Enter text message, end with string 'bb'.
Welcome to Login Mode.
This is the second line of the banner.
And here is yet another (third) line.
bb
ACOS-dev(config)#
```

5. Set the terminal idle timeout in minutes using the **terminal idle-timeout** CLI command, per the organization's security policy. For example:

```
ACOS-dev(config)# terminal idle-timeout 10
```

6. Use the **interface management** CLI command to configure the IPv4 address on the TOE management interface and to enable the interface as the default for use management control function on the TOE. For example:

```
ACOS-dev(config)# interface management
ACOS-dev(config-if:management)# ip address 100.1.1.38 255.255.255.0
ACOS-dev(config-if:management)# ip control-apps-use-mgmt-port
```

7. Set the password policy to strict to enable 8 characters minimum with 2 lower-case, 2 upper-case, 2 numeric, and 1 special characters at a minimum using the **system password-policy complexity Strict** CLI command For example:

```
ACOS-dev(config)# system password-policy complexity Strict
```

8. Set the failed authentication lockout policy for failure threshold count and lockout durations using the **admin-lockout** CLI command, per the organization's security policy. The lockout threshold reflects a number of attempts, while the duration and reset time are in minutes. Additional information for this feature is described in Section 3.7 below. For example:

```
ACOS-dev(config)# admin-lockout enable
ACOS-dev(config)# admin-lockout threshold   3           --- default is  5 attempts
ACOS-dev(config)# admin-lockout duration   15           --- default is 10 minutes
ACOS-dev(config)# admin-lockout reset-time 25           --- default is 10 minutes
```

9. Enable audit logging to include logging of configuration mode commands, as well as event logging. Select event logging severity levels consistent with the organizations security policy. For example to enable audit logging and event logging for information though emergency level events:

```
ACOS(config)# audit enable privilege
ACOS(config)# logging buffered information
```

10. By default, ACOS will report (display) event log entries to the local console. To disable the report (display) of these entries on the local console, configure the following:

```
ACOS(config)# logging console disable
```

2.2.3 Establish an IPsec Tunnel for Connections in the Operational Environment

To support secure access to external servers and from remote management administrators in the TOE's operational environment an IPsec tunnel needs to be set-up. Initially this tunnel must be set-up with a Pre-shared Key compatible with the remote IPsec peer of the tunnel.

To this end, an example is given for a simple IPsec tunnel to a remote, trusted network segment outlined as follows:

TOE IP Address	10.1.1.38	(TOE connected subnet)
IPsec Peer Address 1:	10.1.1.164	(TOE connected subnet)
IPsec Peer Address 2:	10.65.25.164	(Trusted remote subnet)
Tunnel Route:	10.65.25.0/24	(Tunnel traffic for all 256 endpoints on 10.65.25.0 subnet)
Tunnel Port:	TOE management port	

This tunnel could be constrained to a single tunnel peer or additional tunnels could be configured to support more complex connectivity needs. Other algorithms could also be chosen as needed to interoperate with the IPsec Peer. Additional information configuring IPsec tunnels is provided in Section 3.13 later in this document.

First configure common settings needed to comply with the CC evaluated configuration.

1. Enable logging of IPsec and X.509 certificate validation events to the ACOS event log with the following CLI command.

```
ACOS(config)# vpn ike-logging-enable
```

   - NOTE: IPsec and X.509 related events are included in the ACOS event log as 'information' severity entries.

2. Enable enforcement of IKE SA key strength greater or equal to ESP SA strength in IPsec tunnel establishment negotiation with the following CLI command.

```
ACOS(config)# vpn ipsec-cipher-check
```

Next set-up the IKE component of the tunnel with the VPN peer with the following CLI commands, where ***ike-psk-string*** is a 1 - 127 character string.

```
vpn ike-gateway ipsec_mgmt_ike_1
   ike-version v2
   nat-traversal
   auth-method preshare-key ike-psk-string
   interface-management
   dh-group 14
   encryption aes-256 hash sha256
   local-id "10.1.1.38"
   remote-id "10.1.1.164"
   local-address ip 10.1.1.38
   remote-address ip 10.1.1.164
   lifetime 86400
```

- NOTE: The `local-id` command specifies the reference ID value of the TOE for IKE phase 1. Likewise, the `remote-id` command specifies the reference ID value of the peer IPsec peer. This example simply uses IP addresses for these values. The settings for these value should correspond, in reverse, to those values configured on the IPsec peer.
- NOTE: The `nat-traversal` command is optional, depending on whether the IPsec peer supports NAT Traversal (NAT-T).

Lastly, set-up the ESP component of the tunnel with the following CLI commands to support exchanges with all IP addresses on the trusted 10.65.25.0 network segment.

```
vpn ipsec ipsec_mgmt_esp_1
   mode tunnel
   proto esp
   dh-group 14
   encryption aes-256 hash sha256
   lifetime 28800
   lifebytes 10240
   traffic-selector ipv4 local  10.1.1.38  255.255.255.255 remote 10.65.25.0 255.255.255.0
   ike-gateway ipsec_mgmt_ike_1
```

Confirm the status of the tunnel as UP using the **`ping`** or **`traceroute`** CLI commands to an available system on the 10.65.25.0/24 trusted, remote subnetwork of this example and doing the reverse of pinging the TOE from devices on trusted, remote subnetwork.

Additional guidance and background for IPsec tunnel management on the TOE is provided in Section 3.13 later in this document.

2.2.4 Verify and Ensure Software Version

With the TOE now capable of connecting with file servers on at trusted network segment via IPsec, the next step is to ensure ACOS versions present on the TOE are support the ACOS 5.2.1-P3 release. The **show version** CLI command can again be used, now focusing on software versions installed on the primary and secondary boot images. For example:

```
ACOS>show version
Thunder Series Unified Application Service Gateway TH4435
  Copyright 2007-2021 by A10 Networks, Inc.  All A10 Networks products are
  protected by one or more of the following US patents:
  10243791, RE47296,  10230770, 10187423, 10187377, 10178165, 10158627
  * * *
  7606912, 7346695, 7287084, 6970933, 6473802, 6374300


      64-bit Advanced Core OS (ACOS) version 5.2.1-p3, build 3 (Jul-21-2021,19:30)
      Platform features: fips
      Booted from Hard Disk primary image
  * * *
      Hard Disk primary image (default) version 5.2.1-p3, build 3
      Hard Disk secondary image version 5.2.1-p3, build 3
```

Versions indicated prior to 5.2.1-P3 should be updated to the most recent update of ACOS 5.2.1-P3. Update images can be downloaded from the A10 Networks support web site (https://support.a10networks.com) to a trusted server accessible via the IPsec tunnel.

The **upgrade** CLI command can be used to update the TOE's primary and secondary images using SCP or SFTP for access to the downloaded update image. For example, the following commands can be used to update these images on the TOE from a trusted SCP server via the IPsec for ACOS version 5.2.1-P3, build 58.

```
ACOS(config)# upgrade hd pri use-mgmt-port scp://root@10.65.25.165:/updt-
files/ACOS_FTA_5_2_1-p3_58.64.upg
Password []?
  * * *
ACOS(config)# upgrade hd sec use-mgmt-port scp://root@10.65.25.165:/updt-
files/ACOS_FTA_5_2_1-p3_58.64.upg
Password []?
```

NOTE: If prompted to save modified configuration, enter "yes".

NOTE: When prompted to choose reboot after upgrade, enter "no".

NOTE: Username and password credentials are those for the administration user on the trusted SCP server.

Observe that the **upgrade** CLI command operations succeed and confirm the ACOS primary and secondary images reflect the updated versions using the **show version** command.

Next, reboot the TOE using **reboot** CLI command and login again to the TOE console as the "admin" ACOS root administrator.

2.2.5 Restrict Management Traffic to Ping/Traceroute and IPsec Tunnel

Before configuring the TOE to support access with other systems in the TOE operational environment first restrict local traffic on the management port and traffic via the IPsec tunnel, then apply the ACL to the TOE management interface.

```
ACOS(config)# access-list 100 84 remark "Default permit IPsec Peer"
ACOS(config)# access-list 100 88 permit ip 10.1.1.164 any

ACOS(config)# access-list 100 92 remark "Default deny all IPs”
ACOS(config)# access-list 100 96 deny ip any

ACOS(config)# interface management
ACOS(config-if:management)# access-list 100 in
```

To support connectivity troubleshooting and status for the TOE, permit pings and traceroute on locally on the TOE management port and via the IPsec tunnel. Continuing the example, to support this for all 256 endpoints on these subnets add the following. More complex connectivity needs and ICMP types can be applied at the administrators' discretion.

```
ACOS(config)# access-list 100 4  remark "Permit Ping/Traceroute – Local & via IPsec”
ACOS(config)# access-list 100 8  permit icmp type 0 10.65.25.0 /24 any
ACOS(config)# access-list 100 10 permit icmp type 8 10.65.25.0 /24 any
ACOS(config)# access-list 100 11 permit icmp type 0 10.1.1.0   /24 any
ACOS(config)# access-list 100 12 permit icmp type 8 10.1.1.0   /24 any
```

2.2.6 Enable Remote SSH Management Access

To support more convenient CLI access to the TOE, access from remote SSH terminal clients via the IPsec tunnel can be enabled. Continuing the example, to support SSH access from all 256 endpoints via the IPsec secured subnet add the following.

```
ACOS(config)# access-list 100 16 remark "Default SSH from IPsec subnet"
ACOS(config)# access-list 100 20 permit tcp 10.65.25.0 /24 any eq 22
```

Confirm that the TOE can be accessed from an SSH client on the subnetwork supported by the IPsec tunnel using the default "admin" ACOS root administrator account. SSH access will not be available for the locally attached subnet of the TOE's management port.

3. SECURE MANAGEMENT

This section describes TOE capabilities and provides further guidance on configuring and managing the TOE functionality when deployed in a CC evaluated configuration. It summarizes information in the ACOS Configuration Guides indicated in Section 1.2 above as pertains to the CC evaluated configuration for the TOE.

TOE administrators should refer review these ACOS Configuration Guides to establish a broad awareness of the range of functionality and capabilities in ACOS, including functions and capabilities that may be beyond the scope of the CC evaluated configuration.

3.1 MANAGING ADMINISTRATORS

The TOE supports two types of administrators (users) in the CC evaluated configuration: read-only privileged and read-write privileged.

Read-only administrators	can only use the User EXEC services of the ACOS CLI or GUI to display information and perform basic tasks such as pings and traceroutes
Read-write administrators	can, in addition to the User EXEC services, use the Privileged EXEC services of the ACOS CLI or GUI add, modify, and delete configuration of the TOE.

All read-write administrators are considered Security Administrators of the TOE.

NOTE: **For the remainder of this document, references to administrators or TOE administrators should be assumed to equate to Security Administrators of the TOE.**

The “admin” account is a permanent read-write privileged account on the TOE. Externally defined accounts through services such as Radius, TACACS+, and LDAP are not in the scope of the CC evaluated configuration.

Attributes associated with locally defined TOE administrator accounts are:

- Login-name
- Password
- Privilege
- Access Interfaces Allowed (namely local/remote CLI and and remote Web/GUI).

The login-name and password credentials are for authenticating to the TOE and determining privileges to be allowed for the management session.

Locally defined accounts on the TOE management are managed through the **`admin`** CLI command or the **‘System -> Admin -> Users’** Web/GUI page. For example, to add a Security Administrator (e.g. read-write) account:

```
ACOS(config)# admin secadmin1
ACOS(config-admin:secadmin1)# password pw-string
ACOS(config-admin:secadmin1)# access cli web axapi
ACOS(config-admin:secadmin1)# privilege write
ACOS(config-admin:secadmin1)# enable
```

NOTE: Attempts to configure values for *pw-string* values that are too-short or too long will be considered input syntax errors by the **`admin`** CLI command and not be logged as audit or event records by the TOE.

By default, newly added TOE accounts do not enable the write-privilege . To distinguish a Security Administrator for the TOE, include the write-privilege for the account as indicated in the example.

To change the password for a locally defined account on the TOE, use the **admin** CLI command to enter the **config-admin** mode where the acccount's password can be set or use the **admin** CLI command with the **password** option. For example, the following operations will reset the `secadmin1` account's password to *new-pw-string*.

```
ACOS(config)# admin secadmin1
ACOS(config-admin:secadmin1)# password new-pw-string
```

or

```
ACOS(config)# admin secadmin1 password new-pw-string
```

3.2 PASSWORD MANAGEMENT

Passwords maintained by the TOE can be composed using any combination of upper-case and lower-case letters, numbers, and special characters including the following. The password special characters supported both for CLI and Web/GUI interfaces to successfully authenticate with the TOE.

- “ ”, “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, “ ”, “"”, “'”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[”, “\”, “]”, “ ”, “`”, “{”, “|”, “}”, “~”

The password policy is configurable with strict, medium, and simple options that include various minimums for the number of lower-case, upper-case, numeric, and special characters using the **system password-policy complexity** CLI command.

```
ACOS(config)# system password-policy complexity ?
  Strict  Strict: Min length:8, Min Lower Case:2, Min Upper Case:2, Min Numbers:2, Min Special
Character:1
  Medium  Medium: Min length:6, Min Lower Case:2, Min Upper Case:2, Min Numbers:1, Min Special
Character:1
  Simple  Simple: Min length:4, Min Lower Case:1, Min Upper Case:1, Min Numbers:1, Min Special
Character:0
```

The “Strict” mode for password complexity is recommended to minimize the account compromise risk. In FIPS mode of operation the TOE enforces a minimum of 8 characters for password length, regardless of the password-policy complexity selection or if password-policy is not configured.

The password policy is configurable by TOE administrators and supports the minimum password length of 8 characters and a maximum password length of 63 characters. This minimum length can be configured by indicating a **min-pswd-len** value at the end of the **system password-policy complexity** command with a range of 8 to 63 characters. . For example, to change the minimum length for passwords configured on the TOE to 15 characters:

```
ACOS(config)# system password-policy complexity Strict min-pswd-len 15
```

With the strict setting for password policy, the TOE requires passwords to have:

- Minimum of 2 lower-case characters
- Minimum of 2 upper-case characters
- Minimum of 2 numeric characters
- Minimum of 1 special character.

Password information is never revealed during interactive administrator logins to the TOE. For logins using the CLI to the local console or remotely with SSH, input characters are simply not echoed. For the Web/GUI, ‘*’ characters are echoed.

3.3 SESSION TERMINATION

3.3.1 Graceful Termination

The TOE allows interactive sessions to exit (logout) gracefully by command (operation). Administrative sessions to the TOE CLI using the local console or remotely accessing the CLI with SSHv2 via IPsec can terminate their sessions using one or more instances of the 'exit' CLI command.

Administrative sessions to the TOE Web/GUI via IPsec can terminate their sessions using the provided 'logout' option in the user control menu at the top right corner of the browser window.

3.3.2 Inactivity Termination

Authenticated sessions to the TOE can be configured for inactivity timeouts up to 60 minutes using the **`terminal idle-timeout`** CLI command. This timeout will affect management sessions to the TOE CLI on the local console or remotely using SSHv2 via IPsec. The default for this idle-time out is 15 minutes. For example:

```
ACOS(config)# terminal idle-timeout 10
```

Separate web service timout values can be similarly configured to control inactivity timeouts for authenticated sessions to the TOE's web GUI via IPsec. These timeouts are configured by the **`web-service gui-timeout-policy idle`** CLI command. The default for this idle-time out is 10 minutes. For example:

```
ACOS(config)# web-service gui-timeout-policy idle 15
```

To maintain compliance with the TOE CC evaluated configuration, ensure that these timeout settings are configured for non-zero values.

3.4 LOGIN BANNERS

For all interactive administrative sessions to the TOE, absolutely no actions can be performed on the TOE before to successfully authenticating (logging in) to the TOE.

Before being prompted for credentials in these sessions the TOE will display advisory notice and consent warning messages per the organizations security policy. These messages (banners) can be configured for the TOE as described below.

3.4.1 CLI Login Banner

Prior to being prompted for credentials in administrative sessions to the TOE CLI using the local console or remotely accessing the CLI with SSHv2 via IPsec a banner will be displayed. This banner is configured for the TOE using the **`banner login`** CLI command. See Section 2.2.2 above for examples using this command.

3.4.2 Web/GUI Login Banner

Prior to being prompted for credentials in administrative sessions to the TOE Web/GUI via IPsec a banner well be displayed. This banner is configured for the TOE on **'System -> Settings -> Web'** Web/GUI page for the parameter **'Pre-GUI Login Message'**. The banner is displayed in a pop-up window that must be accepted by clicking an "OK" button before the TOE's standard login page is displayed prompting inputs for username and password.

3.5 SYSTEM AND NETWORK TIME CONFIGURATION

A critical capability for any secure networking appliance is to is to maintain an accurate sense of time, at the minimum to ensure reliable times stamps in audit logging, monitor administrator sessions for inactivity, and administrator account lockout periods. To this end, the TOE can maintain time locally as an independent device when necessary or in synchrony with network time when NTP services are available.

3.5.1 System Time Configuration

The TOE maintains date/time based on the system clock provided by its underlying hardware. This system can be configured (set) by the administrator using the **clock** and **timezone** CLI commands, previously described in Section 2.2.2.

3.5.2 Network Time (NTP) Configuration

The TOE supports up to three (3) NTP servers to synchronize the TOE with the network date and time with communication is protected by the IPsec tunnel in the CC evaluated configuration.

Continuing the examples above, NTP servers on the IPsec secured subnet can be configured using the **ntp server** CLI command and extending ACLs to permit traffic for them through the IPsec tunnel. The **prefer** command option can be used to designate one of the servers as a default NTP source with the additional servers as backup time NTP sources.

```
ACOS(config)# ntp server 10.65.25.165
ACOS(config-ntpsvr:10.65.25.165)# prefer
ACOS(config-ntpsvr:10.65.25.165)# exit
ACOS(config)# ntp server 10.65.25.166
ACOS(config)# ntp server 10.65.25.167

ACOS(config)# access-list 100 24 remark "NTP Servers on IPsec subnet"
ACOS(config)# access-list 100 28 permit udp host 10.65.25.165 eq 123 any
ACOS(config)# access-list 100 32 permit udp host 10.65.25.166 eq 123 any
ACOS(config)# access-list 100 36 permit udp host 10.65.25.167 eq 123 any
```

Confirm connectivity to NTP servers using the **show ntp status** CLI command which should show one of the servers with a “synchronized” status and the other servers as “polling”. If connectivity to a synchronized NTP server is lost, the TOE will attempt to connect with the other configured servers to maintain synchrony with the network time domain.

The TOE does not support NTP broadcast and multicast time updates. The TOE does not support configuration of the NTP version. Only NTP Version 4 is supported.

NTP communications are secured by IPsec tunnels in the CC evaluated configuration.

3.6 FAILED AUTHENTICATION LOCKOUT

The TOE counts consecutive remote attempts to the ACOS CLI and Web/GUI interfaces for configured administrator accounts on the TOE. When this threshold is reached for a given administrator account, the TOE will lock that account and permit no successful logins for the account until either a configurable period of time has elapsed, or the account is manually unlocked by a Security Administrator.

A valid login that occurs prior to the failure counter reaching its threshold will reset the counter to zero. Also, this counter is exempted for failed logins occurring on the local console to avoid denial of service that could render the TOE inaccessible (blocked) to all administrators.

Login failure settings can be configured on a system-wide basis to control:

- Lockout attempts threshold
- Lockout duration (a value of zero (0) means permanent lockout requiring manual unlocking)
- Lockout window time (aka 'reset-time', how long the TOE will track failed authentications)

For example, to enable and configure the lockout feature.

```
ACOS(config)# admin-lockout enable
ACOS(config)# admin-lockout threshold   3         --- default is  5 attempts
ACOS(config)# admin-lockout duration   15         --- default is 10 minutes
ACOS(config)# admin-lockout reset-time 25         --- default is 10 minutes.
```

Locked administrator accounts can be manually unlocked at any time with the **`admin`** CLI command by the ACOS *admin* root-administrator from the local console of the TOE. For example:

```
ACOS(config)# admin adminuser1
ACOS(config-admin:adminuser1)# unlock
```

Locked administrators accounts are only blocked for remote CLI and Web/GUI management access via IPsec. These accounts are not blocked during lockout for administrators able to access to the local console of the TOE.

To maintain compliance with the TOE CC evaluated configuration, ensure that the lockout attempts threshold (`admin-lockout threshold`) is configured for a non-zero value.

3.7 AUDIT LOGGING

Audit logging is supported by TOE both locally on the TOE device and transmitted externally to remote Syslog servers via IPsec.

3.7.1 Local Logging

Audit entries are generated and stored in two logging stores on the TOE, one for ACOS audit category records and one for ACOS event category records. Each store supports a circular log with the oldest records overwritten when the logging store is full. These audit stores are sized as follows:

- Audit category logging store 1000 to 30,000 records (20,000 default)
- Event category logging store 10,000 to 50,000 records (30,000 default)

Audit and event logging are enabled through the **`audit enable privilege`** and **`logging buffered`** ***`log-level`*** CLI commands, with event logging configurable for a selected range of event severities. TOE administrators must enable these logging services. For example to enable command audit logging and event logging for notification to emergency events:

```
ACOS(config)# audit enable privilege
ACOS(config)# logging buffered notification
```

These locally stored logs are limited in size and circular such that oldest records are overwritten when their respective stores are full. The size of the audit and event logging stores can be changed using the **`audit size`** and **`logging buffered`** ***`max-messages`*** CLI commands; respectively. For example, to set these stores to their maximum sizes:

```
ACOS(config)# audit size 30000
ACOS(config)# logging buffered 50000
```

Audit log entries can be viewed using the **`show audit`** CLI command. Event log entries can be viewed using the **`show log`** CLI command.

All TOE administrators can view these logs. Only Security Administrators can enable/disable, clear (delete), or alter the size of these logs and no administrators can modify log contents in any way. If an administrator disables or clears a log, an audit record of this action is recorded.

Locally logged records can be deleted by using the **`clear audit`** and **`clear log`** CLI commands. Local logging for audit and event category records can be disabled by the **`no audit enable`** and **`logging buffered disable`** CLI commands. Security Administrators should not clear logs or disable logging on the TOE and should have no cause or need to do so.

3.7.2 Remote Logging to Syslog

Audit and event category entries can be logged to trusted Syslog servers via IPsec in the CC evaluated configuration. When configured for logging to one or more Syslog servers, new audit and event records are saved in the local audit and event logging stores and are immediately sent to the Syslog servers via the IPsec encrypted channel.

Multiple Syslog servers can be configured on the TOE by using the **`logging host`** CLI command once for each server and extending ACLs to permit traffic for them through the IPsec tunnel. If you use the command with the same IP address as an existing logging server, it replaces any existing configuration for that existing server. The **`use-mgmt-port`** command option must be used for the CC evaluated configuration. The port command **`option`** allows a given Syslog server to be configured for an alternate port other than the default 514.

Continuing the examples above, Syslog servers on the IPsec secured subnet can be configured using the **logging host**, **logging auditlog host**, and **logging syslog** CLI commands along with an extended ACL to permit traffic for the Syslog server through the IPsec tunnel.

```
ACOS(config)# logging host 10.65.25.165          use-mgmt-port
ACOS(config)# logging auditlog host 10.65.25.165 facility local0

ACOS(config)# logging syslog ?
  disable       Do not send log to syslog
  emergency     System unusable log messages      (severity=0)
  alert         Action must be taken immediately  (severity=1)
  critical      Critical conditions               (severity=2)
  error         Error conditions                  (severity=3)
  warning       Warning conditions                (severity=4)
  notification  Normal but significant conditions (severity=5)
  information   Informational messages            (severity=6)
  debugging     Debug level messages              (severity=7)
ACOS(config)# logging syslog notification

ACOS(config)# acos-events log-properties use-syslog-standard-header


ACOS(config)# access-list 100 40 remark "Syslog Servers on IPsec subnet"
ACOS(config)# access-list 100 44 permit udp host 10.65.25.165 eq 514 any
```

The **logging host** command identifies an external Syslog server for ACOS to direct ACOS event log entries to. The **logging syslog** indicates the event severity level, inclusive of lower numbered severities, for entries to be logged to Syslog. The **logging auditlog host** directs ACOS to report ACOS audit log events to the identified Syslog server. The `acos-events` command enables the RFC-5424 compatible format for log messages ACOS sends to configured Syslog servers.

If communications with a Syslog server are lost and becomes re-established, new logging records will be logged successfully on the server. Records locally logged while communications with a Syslog server is down will be retained in the local logs and will not be logged (re-sent) to the Syslog server.

Logging to a configured external Syslog server can be disabled by removing the configured server with the **no logging host** and **no logging auditlog** CLI commands to disable logging to syslog for event-category and audit-category records. Event-category record logging to Syslog servers can also be disabled by setting the logging severity level to "disable" with the **logging syslog disable** CLI command.

3.7.3 IPSec and X.509 Logging

As noted in Section 2.2.3 above, IPsec and X.509 related events are included in the ACOS event log as 'information' severity entries. To ensure that these events are locally logged and reported to the external Syslog audit server, alternately configure the TOE with the following CLI commands:

```
ACOS(config)# logging buffered information
ACOS(config)# logging syslog information
```

3.8 FILE SERVERS

Access to remote file servers is important for the TOE in file transfers operation underlying administrative actions such as trusted update of the TOE and configuring X.509 certificates for IPsec. These operations involve importing (exporting) files to (from) the TOE and trusted file servers via IPsec in the CC evaluated configuration.

The TOE supports import/export file transfers operation with SCP or SFTP file servers via IPsec tunnels to trusted subnetworks. To configure the TOE for such operations, it is necessary to extending ACLs to permit traffic for these servers through the IPsec tunnel.

Continuing the examples above, SCP and SFTP servers can be configured for their default SSH port 22. These ACLs can certainly use alternate TCP ports and other servers on the IPsec secured subnet can be configured by TOE Security Administrators.

```
ACOS(config)# access-list 100 52 remark "File Servers (SCP/SFTP) on IPsec subnet"
ACOS(config)# access-list 100 56 permit tcp host 10.65.25.165 eq 22 any
ACOS(config)# access-list 100 60 permit tcp host 10.65.25.166 eq 22 any
```

If the connection fails to establish or is lost during an import or export operation, the update operation will be failed, and the administrator will have to retry the operation at a later time when reliable access to the server(s) is available. In addition to general import/export operations, this consideration also applies to CSR exports and certificate imports as described in Section 3.11 below.

3.9 TRUSTED UPDATES

A10 Networks regularly publishes updates to ACOS software releases with security and bug fixes. Regularly applying these updates to the TOE is critical to maintaining security of the TOE. TOE update images are available from the A10 Networks support web site (https://support.a10networks.com). An A10 Networks support login ID and password is required to download these images.

The TOE supports two ACOS images (boot-images), primary and secondary. A trusted update operation for the TOE performs a full image upgrade of either the TOE's primary or secondary boot-images. TOE Administrators can choose to maintain either or both of these images up-to-date with updates to the ACOS 5.2.1 release.

The **show version** CLI command discussed in Section 2.2.4 above can be used to show the software versions installed on the TOE's primary and secondary boot-images. The image indicated with "**(default)**" is the boot-image currently enabled for the TOE.

To perform an update an administrator will download a TOE update image to a local, trusted file server accessible to the TOE via IPsec as described in Section 3.8 above. After downloading the TOE update image, note the MD5 signature for the image indicated on the A10 support web site and confirm the signature before proceeding with the update. The TOE update image downloaded is an ".upg" file, signed with a digital signature.

The **upgrade** CLI command can be used to update the TOEs primary and secondary images downloaded to the trusted server. The **use-mgmt-port** command option must be used for the CC evaluated configuration. For example, the following commands can be used to update these images on the TOE from a trusted SCP server via the IPsec for ACOS version 5.2.1-P3, build 3.

```
ACOS(config)# upgrade hd pri use-mgmt-port scp://admin@10.65.25.165/updt-
files/ACOS_FTA_5_2_1-p3_3.64.upg
Password []?
  * * *
ACOS(config)# upgrade hd sec use-mgmt-port scp://admin@10.65.25.165/updt-
files/ACOS_FTA_5_2_1-p3_3.64.upg
Password []?
```

If the connection fails to establish or is lost while downloading the TOE update image from the trusted server, the update operation will be failed, and the administrator will have to retry the operation at a later time when reliable access to the server(s) is available.

Before installing the TOE update image, the signature is verified against a key stored in the TOE. If the digital signature verifies successfully, an MD5 integrity check will additionally be performed for the contents of the update image. If the digital signature and MD5 integrity checks succeeds, the update will proceed to be installed on the requested TOE boot-image (primary or secondary). If any of these tests fail, the TOE update operation will be failed with visual feedback to the administrator initiating the update, along with corresponding logged failure events. All validations of the TOE update image are performed at the time of the **upgrade** operation.

If the TOE update image had just been installed for the active (running) boot-image, the administrator may choose to reboot the device immediately, as prompted by the **upgrade** CLI command or at a later time of the administrator's discretion when the update to take effect.

The **bootimage** CLI command can be used to change between primary and secondary boot-images that the TOE will boot from. The **reboot** CLI command can be used to manually reboot the TOE. The TOE must be rebooted for the update to take effect. The operating TOE system will not be affected by the TOE update operation until the reboot of the TOE device is performed.

3.10 REMOTE MANAGEMENT

The TOE supports remote management from via IPsec for:

- SSH terminal clients to the ACOS CLI
- Web browser clients to the ACOS Web/GUI

This section describes secure management procedures for these remote management capabilities.

3.10.1 SSH Clients via IPsec

Section 2.2.5 above described how to configure the TOE to support access for administrators to the TOE via SSH protected by IPsec for the initial setup of the TOE. The ACLs described in Section 2.2.5 can be extended to support the desired access policy for the organization and IPsec tunnels configured to permit access to the TOE CLI from SSH terminal clients on TCP port 22 of the TOE.

SSH clients accessing the TOE will need to be configured to support the following key settings to interoperate with the TOE.

- SSH Protocol Version: 2
- Encryption Algorithms: aes128-ctr, aes256-ctr
- Integrity Algorithms: hmac-sha1,hmac-sha2-512,hmac-sha2-256
- Key Exchange: diffie-hellman-group14-sha1
- Public Key Authentication: RSA

3.10.2 Web/GUI Clients via IPsec

To support Web/GUI access to the TOE from remote web-browser clients via the IPsec tunnels configured for the TOE additional ACLs can be configured to enable access to the TOE. Continuing the examples above, to support Web/GUI access from all 256 endpoints via the IPsec secured subnet add the following.

```
ACOS(config)# access-list 100 64 remark "Default Web/GUI from IPsec subnet"
ACOS(config)# access-list 100 68 permit tcp 10.65.25.0 /24 any eq 443
```

Confirm that the TOE Web/GUI can be accessed from a browser client on the subnetwork supported by the IPsec tunnel using the “admin” ACOS root administrator account or another administrator account added as described in Section 3.1 above. Web/GUI access will not be available for the locally attached subnet of the TOE’s management port.

Browser clients accessing the TOE will need to be configured to support the following key settings to interoperate with the TOE's Web/GUI:

- TLS Protocol: TLS 1.2
- HTTP Protocol: HTTP/1.1
- Elliptic Curves: secp256r1, secp521r1, secp384r1, secp256k1
- Ciphers:

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_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

3.11 X.509 CERTIFICATE AND KEY MANAGEMENT

The initial set-up via the TOE local console described in Section 2.2.3 above used a Pre-shared Key to secure communications for trusted channels and paths with a remote IPsec tunnel peer. The TOE also supports use of X.509 Public Key certificates and private key for IPsec authentication.

This section describes how to configure the TOE for X.509 certificates and private keys. In summary, the process will involve the following steps.

1. Generate Private Keys and Certificate Signing Requests (CSR)
2. Export the CSRs to a trusted file server
3. Use the CSRs to generate an X.509 certificates signed by a root Certificate Authority (CA) or an intermediate CA of the root CA
4. Import the signed X.509 certificates to TOE
5. Import the Root CA certificates to the TOE

The TOE supports the following key sizes for the CC evaluated configuration:

- RSA: 2048 bits
- ECDSA: 256, 384 bits

3.11.1 Generate Private Key + Certificate Signing Request (CSR), Export CSR

Use the **pki create** CLI command to generate a private key with corresponding CSR and export the CSR to a trusted server. The **use-mgmt-port** command option must be used for the CC evaluated configuration.

For example, to generate an RSA key with a CSR and export it to an SCP server via IPsec tunnels on a trusted subnetwork.

```
ACOS(config)#pki create csr rsa-cert1 use-mgmt-port \
                                      rsa digest-type sha256 \
                                      scp://adminusr@10.65.25.165/cert/rsa-cert1-csr
Password []?
input key bits(1024, 2048, 4096) default 1024:2048
input Common Name, 1~64:test-dut1
input Division, 0~31:abc-test-lab
input Organization, 0~63:ABC Corp
input Locality, 0~31:San Jose
input State or Province, 0~31:CA
input Country, 2 characters:US
input email address, 0~64:abc-test1@abccorp.com
```

NOTE: See Section 1.3.3 for key sizes and digest type settings that should not be selected.

NOTE: Username and password credentials are those for the administration user on the trusted SCP server.

For example, to alternately or additionally generate an ECDSA key with a CSR and export it to an SFTP server via IPsec tunnels on a trusted subnetwork.

```
ACOS(config)#pki create csr ecdsa-cert1 use-mgmt-port \
                                        ecdsa digest-type sha256 \
                                        sftp://adminusr@10.65.25.165/cert/ecdsa-cert1-csr
Password []?
input key bits(256, 384) default 256::256
input Common Name, 1~64:test-dut1
input Division, 0~31:abc-test-lab
input Organization, 0~63:ABC Corp
input Locality, 0~31:San Jose
input State or Province, 0~31:CA
input Country, 2 characters:US
input email address, 0~64:abc-test1@abccorp.com
```

NOTE: See Section 1.3.3 for key sizes and digest type settings that should not be selected.

NOTE: Username and password credentials are those for the administration user on the trusted SFTP server.

Note that when including a value for the input email address, this value will be appended to the Common Name and concatenated with “emailAddress=” such that the CSR’s CN value would be rendered as:

```
CN=test-dut1/emailAddress=abc-test1@abccorp.com
```

To restrict the Common Name to just the value input, do not enter a value for the input email address by simply entering a carriage-return <CR> for the value. This would result in the following CN value being rendered in the CSR:

```
CN=test-dut1
```

When subsequently configuring the TOE to use the keys generated in this example, the names for these keys would be:

- RSA Key: rsa-cert1
- ECDSA Key: ecdsa-cert1

Private keys and CSRs incidentally created or otherwise unused by the TOE can be immediately removed, with zeroized deletion, from the TOE using the **pki delete key** and **pki delete csr** commands; respectively.

3.11.2 Generate Certificates Signed by the CA

Using the CSRs exported to the trusted server, next generate RSA and/or ECDSA certificates for the TOE, signed by the root CA or an intermediate CA of the Root CA.

From the example above, these CSRs would be stored on the trusted server as:

- /home/adminusr/certs/rsa-cert1-csr
- /home/adminusr/certs/ecdsa-cert1-csr

For purposes of the example, let's assume that the resulting X.509 signed certificates are named as follows on the trusted server:

- /home/adminusr/certs/rsa-cert1-signed
- /home/adminusr/certs/ecdsa-cert1-signed

3.11.3 Import Signed Certificates

Next, use the **import cert** CLI command import the signed certificates to the TOE from the trusted server via IPsec. The **use-mgmt-port** command option must be used for the CC evaluated configuration.

To continue the example above, import the signed certificates from the SCP server via IPsec tunnels to the trusted subnetwork.

```
ACOS(config)#import cert rsa-cert1-signed use-mgmt-port \
                         scp://adminusr@10.65.25.165/cert/rsa-cert1-signed
ACOS(config)#import cert ecdsa-cert1-signed use-mgmt-port \
                         scp://adminusr@10.65.25.165/cert/ecdsa-cert1-signed
```

When subsequently configuring the TOE to use the keys generated in this example, the names for these keys would be:

- RSA Certificate: rsa-cert1-signed
- ECDSA Certificate: ecdsa-cert1-signed

3.11.4 Import Root CA Certificates

Lastly, use the **import ca-cert** CLI command import the root-CA certificates to the TOE from the trusted server via IPsec. The **use-mgmt-port** command option must be used for the CC evaluated configuration.

For example, import the signed certificates from the SCP server via IPsec tunnels to the trusted subnetwork.

```
ACOS(config)#import ca-cert ca-cert1 use-mgmt-port scp://adminusr@10.65.25.165/cert/ca-cert1
```

3.11.5 Zeroization on Security-Reset

When a Security Administrator chooses to zeroize the TOE, the `security-reset` CLI command should be used to destroy all encryption keys and sensitive information on the device. This command is only available via CLI access to the local console of the TOE.

After entering this command and when prompted by TOE with "`The next reboot would fail due to zeroization`", physically power off or remove power from the TOE device.

CAUTION: Performing this procedure will remove all sensitive information from the system, including that used for image integrity during bootup.

After this procedure is performed, the TOE device will not boot again.

Examples of circumstances when this procedure may be desired include:

- Disposal or decommissioning of the TOE device
- Returning the TOE to A10 Networks using the standard Return Merchandise Authorization (RMA) process.

3.12 CERTIFICATE REVOCATION

The TOE uses the Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs) during validation of peer and local certificates. When a certificate is received from an IPsec peer, the TOE processes the certificate chain path until the last certificate is reached.

Local domain communications with OCSP and CRL servers will need ACLs to permit access from the TOE to their HTTP (TCP/80) services. For example:

```
ACOS(config)# access-list 100 72 remark "OCSP Svrs and CRL DPs"
ACOS(config)# access-list 100 74 permit tcp host 10.1.1.111 eq 80 any
ACOS(config)# access-list 100 78 permit tcp host 10.1.1.112 eq 80 any
```

On occasions where the referenced OCSP servers or CRL distribution points are unavailable, the certificate being validated will be not revoked.

3.12.1 CRL Revocation

CRL validation of a certificate is done against any CRL indicated in the certificate as a CRL Distribution Point (CDP) whereby the CRL will be downloaded from the CDP and used to determine revocation status in certificate validations. A local domain CDP is indicated in the certificate in a form similar to the following:

```
URI:http://10.1.1.111/certs/crls/crl.pem
```

3.12.2 OCSP Revocation

OCSP validation of a certificate is done against any OCSP server indicated in the certificate whereby the OCSP server will be queried to determine revocation status in certificate validations. A local domain OCSP server is indicated in the certificate in a form similar to the following:

```
http://ocsp.abc-test-lab.abccorp.com
    or
http://10.1.1.112
```

3.13 IPSEC TUNNEL MANAGEMENT

IPSsec is fundamental to securing TOE communications for the ACOS CLI and Web/GUI management interfaces, as well as communications with servers in the CC evaluated configuration.

An initial configuration was recommended in Section 2.2.3 for IPsec using Pre-Shared Keys to support TOE installation and the initial stage of securely configuring the TOE. With the additional considerations described in the prior sections we can now look to the general configuration for IPsec tunnels to trusted management network segments for trusted paths and trusted channels, including the use of X.509 certificates for identification and authorization.

The general procedure for configuring IPsec on the TOE for a given IPsec peer involves the following:

1. Configure an ACOS VPN IKE Gateway
2. Configure an ACOS VPN IPsec Tunnel
3. Configure ACLs to restrict traffic through the tunnel

3.13.1 IPsec Supported on the TOE

IPsec, as implemented on the TOE, supports the following summary capabilities for the CC evaluated configuration.

- IKEv2 supported only.
- Tunnel mode is supported only. Transport mode is not supported.
- ESP is supported only. AH is not supported.
- NAT Traversal for IKEv2 is supported to encapsulate ESP traffic inside UDP packets.
- 'reference identifier' value is supported either in Subject or SAN (if present) fields of a received certificate and must contain the FQDN or IP address of the IPsec entity.

- IKEv2 support the following algorithms and Security Association (SA) lifetimes.
    - Encryption: AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256
    - Integrity: SHA-1, SHA-128, SHA-256, SHA-384
    - PRF: SHA-128, SHA-256, SHA-384
    - Authentication: RSA, ECDSA, Pre-Shared Keys (text based)
    - DH Groups: 14 (2048-bit MODP)
    - SA Lifetimes: 300 seconds - 86400 seconds (24 hours)

- ESP supports the following algorithms and Security Association (SA) lifetimes.
    - Encryption: AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256
    - Integrity: SHA-1, SHA-128, SHA-256, SHA-384
    - SA Lifetimes: 300 seconds - 28800 seconds (8 hours) and/or 10 (or unlimited) GBytes.

3.13.2 Configure a VPN IKE Gateway

ACOS VPN IKE Gateways supports configuration for IKE on the TOE for a tunnel to a given VPN peer and are configured using the **`vpn ike-gateway`** CLI command. To configure a given peer IKE Gateway, perform the following steps.

1. Create a new VPN IKE Gateway instance

```
ACOS(config)# vpn ike-gateway ipsec_mgmt_ike_1
```

2. Select the IKE version as either IKEv2 for the instance

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# ike-version v2
```

3. Set the instance to use the TOE's management port.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# interface-management
```

4. Choose the authentication method to be used for IKE Phase 1. If use of a Pre-Shared Key is selected, *`ike-psk-string`* is the 1 - 127 character string text of the key. Alternately, RSA or ECDSA methods may be chosen.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# auth-method preshare-key ike-psk-string
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# dh-group 14
```

or

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# auth-method rsa-signature
```

or

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# auth-method ecdsa-signature
```

5. (For RSA Method) If RSA method selected, add an X.509 certificate and corresponding RSA private key and enable diffie-hellman-group14 for the instance. See Section 3.11 for discussion on configuring X.509 certificates and keys.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# local-cert rsa-cert1-signed
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# key  rsa-cert1
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# dh-group 14
```

- NOTE: this example uses the RSA key and X.509 signed certificate configured from examples in Section 3.11.

6. (For ECDSA Method) If ECDSA method selected, add an X.509 certificate and corresponding ECDSA private key and enable diffie-hellman-group14 for the instance. See Section 3.11 for discussion on configuring X.509 certificates and keys.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# local-cert ecdsa-cert1-signed
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# key ecdsa-cert1
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# dh-group 14
```

   - NOTE: this example uses the ECDSA key and X.509 signed certificate configured from examples in Section 3.11.

7. Choose encryption and integrity algorithms for the instance. AES-CBC algorithms use the keyword “hash” to specify the integrity algorithm, while AES-GCM algorithms use the “prf” keyword.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# encryption aes-256 hash sha256
```

   or

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# encryption aes-gcm-256 prf sha512
```

8. Configure the local IP address of the TOE management port and address IP address of the VPN peer:

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# local-address  ip 10.1.1.38
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# remote-address ip 10.1.1.164
```

9. Configure the Remote ID configured in the VPN peer to identify itself during IKE Phase 1 and a Local ID the TOE will use to identify itself to the VPN peer for this instance as corresponding FQDNs or IP Addresses as appropriate. For example:

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# local-id  \
                                              "DC=abccorp, DC=com, CN=test-dut1"
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# remote-id \
                                              "DC=abccorp, DC=com, CN=test-vpn"
```

   or

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# remote-id "10.1.1.164"
```

   - NOTE: To configure the Local ID of the TOE to be the management IP address, simply do not include the “local-id” configuration option as this is the default for the IKE Gateway instance. In this example, not including the “local-id” option would be equivalent to having indicated ‘`local-id "10.1.1.38"`

10. Configure the lifetime for Security Association (SA) re-keying on the instance. This is the duration (in seconds) prior to which the TOE will initiate re-keying of the IKE SA.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# lifetime 86400
```

11. (Optional) Configure NAT Traversal (NAT-T) for the Security Association (SA), if supported by the IPsec peer.

```
ACOS(config-ike-gateway:ipsec_mgmt_ike_1)# nat-traversal
```

An IKEv2 session is a unique combination of the TOE's management IP address, remote peer's IP address, and a configured VPN IKE Gateway instance. The VPN IKE Gateway instance additionally determines the local and remote identifiers of the combination, all of which need to be matched along with other compatible settings for the instance, in order for the session to successfully instantiate.

For TOE initiated IKEv2 sessions, the remote IPsec peer will perform the matching based on the peer's configuration and will accept (reject) the session accordingly. For IPsec peer initiated IKEv2 sessions, the TOE will perform this matching.

Multiple VPN IKE Gateway instances can be configured on the TOE to support multiple IPsec peers in the target (deployment) environment. Such IPsec peers can be intermediate IPsec gateway devices or individual servers with IPsec supported directly on the servers.

Validation of X.509 leaf, intermediate, and root-CA certificates used for IKEv2 are performed immediately after they are imported (transferred) to the TOE. Successfully validated certificates are added to the TOE's local, trusted IKEv2 certificates store. Certificates that fail to validate are logged and left inert (unused) until they are deleted by a Security Administrator.

When establishing IPsec tunnels, the TOE validates certificates received from the IPsec peer and confirms that the IPsec peer certificate and the certificate path are valid (not revoked) as described in Section 3.12 above.

3.13.3 Configure a VPN IPsec Tunnel

ACOS VPN IPsec Gateways supports configuration for ESP on the TOE and are instantiated using the **`vpn ipsec`** CLI command.

ACOS VPN IPsec Gateways supports configuration for ESP on the TOE for a tunnel to a given VPN peer and are configured using the **`vpn ipsec`** CLI command. To configure a given IPsec Gateway, perform the following steps.

1. Create a new VPN IPsec Gateway instance

```
ACOS(config)# vpn ipsec ipsec_mgmt_esp_1
```

2. (Optional) Select the tunnel mode and ESP protocol for the instance. This is optional since these are the only settings supported and are the defaults when not configured for the instance.

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# mode tunnel
ACOS(config-ipsec:ipsec_mgmt_esp_1)# protocol esp
```

3. Enable diffie-hellman-group14 for the instance.

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# dh-group 14
```

4. Choose encryption and integrity algorithms for the instance.

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# encryption aes-256 hash sha256
```

or

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# encryption aes-gcm-256
```

- **NOTE:** If the key size of the encryption setting or the VPN IPsec Gateway instance is greater than the key size for the VPN IKE Gateway instance, the TOE will not instantiate the tunnel with the VPN peer and will log a corresponding error.

5. Configure the time-based lifetime for Security Association (SA) re-keying on the instance. This is the duration (in seconds) prior to which the TOE will initiate renegotiation of the ESP SA.

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# lifetime 28800
```

6. Configure the traffic volume lifetime for Security Association (SA) re-keying on the instance. This is the duration (in seconds) prior to which the TOE will initiate re-keying of the ESP SA.

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# lifebytes 10240
```

7. Configure the traffic selector for the IPsec tunnel which will define the reachable IP subnetwork trusted to support management access to and from the TOE.

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# traffic-selector ipv4
                                      local  10.1.1.38  255.255.255.255 \
                                      remote 10.65.25.0 255.255.255.0
```

   - **NOTE:** ACL can be further defined to further constrain access to individual servers and support remote access for administration users as described in earlier sections of this Chapter 3.

8. Lastly, configure this VPN IPsec Tunnel instance to operate over the VPN IKE Gateway instance supporting connectivity consistent with the traffic selector (e.g. the VPN IKE Gateway configured per Section 3.13.2 above)

```
ACOS(config-ipsec:ipsec_mgmt_esp_1)# ike-gateway ipsec_mgmt_ike_1
```

   - **NOTE:** Multiple VPN IPsec Tunnel instances can be configured to use the same VPN IKE Gateway for flexibility in configuring access to subnetworks segments. To share the same VPN IKE Gateway, the VPN IPsec Tunnel instances would use the same `ike-gateway` setting

     Multiple VPN IPsec Tunnel instances can be defined to steer (direct) management traffic to different subnetworks using the same VPN IKE Gateway. They can also be defined to steer (direct) to individual servers with `traffic-selector` setting using `remote` endpoints with their address masks set to 255.255.255.255.

3.13.4 ACL Rules

The administrator is expected to configure a “default deny” rule as the final ACL rule on the management interfaces to ensure that the TOE rejects traffic on the TOE management interface that is not explicitly allowed by earlier rules. This rule is described in Section 2.2.5.

To be compatible with the CC evaluated configuration, ACLs should be compatible with configured VPN IKE Gateway instances. To support one or more IPsec peers, the “permit” example rules described in Section 2.2.5 can be extended to support the IPsec peers with connectivity to the management port of the TOE.

Additionally, ACLs to support secure communications with external servers and access remote management access by administrators, as described in earlier sections of this Chapter 3, should be defined. These ACLs should “permit” traffic consistent with the `remote` parameter settings for the `traffic-selector` setting of configured VPN IPsec Tunnels.

ACLs that allow traffic other than via IPsec peers are effectively rules that “bypass” secure communications in the CC evaluated configuration. Other than rules recommended for ICMP in Section 2.2.5 to support ping and traceroute for network availability detection on the locally connected network, such bypass rules should not be configured on the TOE.

The third parameter of an ACL is a sequence number to indicate the precedence of evaluation of an ACL relative to others. ACLs with lower valued sequence numbers are evaluated first. The first ACL with a matching rule during an evaluation will apply its indicated action for the packet being evaluated.

3.13.5 IPsec Tunnel Debugging

ACOS supports a separate logging capability local to the TOE to support debugging of IPsec tunnel establishment, X.509 certificate validation matters, and interworking with peer IPsec entities. This capability is particularly useful in resolving interworking issues with external IPsec peer entities in establishing and maintaining IPsec tunnels.

This log is disabled by default and is enabled with the CLI `debug vpn` command where the selected logging levels are for:

- 1 - Basic Tunnel/Packet Negotiation
- 2 - Problem Diagnosis
- 3 - Raw Binary Listings

With the `vpn ike-logging-enable` configuration described in Section 2.2.3 above, the level 1 events are included in the ACOS event log and external Syslog when enabled for the 'information' severity level. For level 2 and higher, in the local debugging log, use the `debug vpn` configuration for levels 2 and higher.

This local debug log can be displayed with the `show vpn log` CLI command.

3.14 BOOT TIME INTEGRITY SELF-TESTS

During boot-up from either a power-on or a reboot, the TOE will perform integrity checks on the TOE software and TOE cryptographic capabilities. If any of these tests fail the TOE is put into FIPS failure mode (A10 ACOS specific state). In this mode, the TOE will operate with nominal management services available from the TOE console only. Remote management to the TOE (trusted paths), connections to external servers (trusted channels), and TOE data-plane services will also not be available or operational.

The FIPS failure mode is indicated by general lack of availability of the TOE in the network infrastructure and the following prompt when logging into the local console of the TOE:

```
ACOS(FIPS FAIL MODE)#
```

Failure of the TOE's software integrity check can be confirmed by observing the following outputs.

```
ACOS(FIPS FAIL MODE)#show varlog | inc check failed
Sep 21 02:07:49 localhost a10mon: Image verification check failed
Sep 21 02:07:49 localhost a10mon: FIPS Power On Self Test failed. Enter FIPS faiil mode
```

Alternately, failure of the TOE's cryptographic capabilities can be confirmed by observing the following outputs.

```
ACOS(FIPS FAIL MODE)# show varlog | inc library power
Sep 21 20:53:36 localhost a10mon: FIPS library power on self test failed
Sep 21 20:53:36 localhost a10mon: FIPS Power On Self Test failed. Enter FIPS faiil mode
```

If this condition occurs, the following actions should be taken:

- Power-cycle and restart the TOE to perform these tests again and determine if normal operation can be resumed
- If this condition persists, contact A10 Networks support (https://support.a10networks.com) to troubleshoot the issue and coordinate replacement of the hardware, if needed.

4. ACRONYMS

ACRONYM/ABBREVIATIONS	MEANING
ACL	Access Control List
ACOS	Advanced Core Operating System
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AH	Authentication Header
AXAPI	A10 AX Application Programming Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CFW	Convergent Firewall
CGN	Carrier-Grade NAT
CLI	Command-line interface
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CSR	Certificate Signing Requests
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
LDAPS	Lightweight Directory Access Protocol Secure
MD5	Message-Digest algorithm 5
NAT	Network Address Translation

NDcPP	Network Device collaborative Protection Profile
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OCSP	Online Certificate Status Protocol
PP	Protection Profile
PKI	Public Key Infrastructure
PRF	Pseudo Random Function
PSK	Pre-Shared Key
QSFP	Quad (4-channel) Small Form-factor Pluggable
QSFP28	Quad (4-channel) Small Form-factor Pluggable 28 GB data
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest Shamir Adleman Algorithm
SA	Security Associations (IPSec)
SCP	Secure Copy Protocol
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SSD	Solid State Disk
SSH	Secure Shell
SSLi	SSL Intercept
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
UDP	User Datagram Protocol
VPN	Virtual Private Network

APPENDIX A. AUDIT LOG ENTRIES

As described in Section 3.7 above, audit entries are generated and stored in two logging stores on the TOE, one for ACOS audit category records and one for ACOS event category records. The information in these records includes the date and time of the event, the type of event, the subject identity of the event, the source of the event, and additional information relevant to the event.

A.1 AUDIT RECORD ENTRIES

The "Sample Record" column in Table 5 includes samples for each audit-category event for which the TOE needs to produce a record. Audit category records are generated by TOE configuration operations either via the CLI or Web/GUI management interfaces to the TOE. Audit-category records of management operations implicitly convey success, unless otherwise ensued by an event-category record indicating that the operation failed.

- NOTE: Syntax errors on input to the CLI are not logged

Audit records are logged to Syslog at the "information" level (severity=6).

A.1.1 CLI Audit Records

CLI management operations are distinguished between local console and remote management in logged entries by the indicated IP address and TCP port information, with:

- Local Console Operations Loopback IP Address (e.g. 127.0.0.1)
- Remote Management Operations Peer IP Address and TCP Port (e.g. 10.65.25.166:53288)

The following is an example of an ACOS CLI audit-category record, including descriptions if it's content.

May 25 2021 01:09:29 [admin] cli: [10.65.25.166:53288] banner login "SSH–Test Pre-Login Message"

- *May 25 2021 01:09:29* - Date and time the operation occurred
- *[admin]* - ID of Administrator performing the operation
- *cli:* - Indicates operation is via CLI
- *[10.65.25.166:53288]* - Source IP address/port of the administration client (e.g. 10.65.25.166:53288) (NOTE: 127.0.0.0 IP address with no TCP/UDP port indicates local console)
- *banner login "SSH–Test Pre-Login Message"* - Message indicating the type of operation and any other information relevant to the operation.

A.1.2 Web/GUI Audit Records

Web/GUI management operations are always remote and will indicate the IP address and TCP port of the remote management client. These operations may include newline (\n) characters and hence appear on multiple lines of displayed output.

The following is an example of an ACOS Web/GUI audit-category record, including descriptions if it's content.

May 25 2021 01:54:28 [admin] web: [361:10.65.25.166:13166] payload section 1
{"web-service": {"axapi-idle": 10, "axapi-session-limit": 30, "gui-idle": 15, "gui-session-limit": 30, "port": 80, "secure-port": 443, "login-message": "GUI-Test Post-Login Message", "pre-login-message": "GUI-Test Pre-Login Message."}}

- *May 25 2021 01:54:28* - Date and time the operation occurred

- *[admin]* - ID of Administrator performing the operation
- *web:* - Indicates operation is via Web/GUI
- *[361:* - ACOS Session ID of the administration client session
- *10.65.25.166:13166]* - Source IP address/port of the administration client
- *payload section 1*
  {"web-service": {"axapi-idle": 10, "axapi-session-limit": 30, "gui-idle": 15, "gui-session-limit": 30, "port": 80, "secure-port": 443, "login-message": "GUI-Test Post-Login Message", "pre-login-message": "GUI-Test Pre-Login Message."}}
  - Message indicating the type of operation and any other information relevant to the operation

A.2 EVENT RECORD ENTRIES

The "Sample Record" column in Table 5 also includes samples for each event-category event for which the TOE needs to produce a record. Event-category records are generated to indicate failure of management operations and other events of the system which by the nature and description may be informational, indicate success, or indicate failure.

A.1.2 Event Records

Event-category records differ slightly from audit-category record notably by including an event level and related component, while including success/failure/information factor by the nature of the logged messages.

The following is an example of an ACOS event-category record, including descriptions if it's content.

Mar 08 2021 03:41:45 Notice [SYSTEM]:A web session for user "niap-user1" from 10.1.1.165 has been opened. Session ID assigned is 64.

- *Mar 08 2021 03:41:45* Date and time the operation occurred
- *Notice* Event severity level
- *[SYSTEM]:* TOE software component/sub-system reporting
- *A web session for user "niap-user1" from 10.1.1.165 has been opened. Session ID assigned is 64*
  - Message indicating the type of operation and other information relevant to the event (including IP address(es)where relevant to the event).

The indicated Event severity levels in these event records correspond to the Syslog severities described in Section 3.7.2 above as shown in Table 4.

EVENT RECORD SEVERITY	LOGGING SYSLOG SEVERITY	DESCRIPTION	SYSLOG SEVERITY
Emergency	emergency	System unusable log messages	severity=0
Alert	alert	Action must be taken immediately	severity=1
Critical	critical	Critical conditions	severity=2
Error	error	Error conditions	severity=3
Warning	warning	Warning conditions	severity=4
Notice	notification	Normal but significant conditions	severity=5
Info	information	Informational messages	severity=6
Debug	debugging	Debug level messages	severity=7

Table 4: Event Log Severities

A.3 AUDIT LOG ENTRY SAMPLES

The following tables lists some of the notable log entries supported by the TOE.

AUDITABLE EVENT	SAMPLE RECORD
Start-up and shut-down of the audit functions **(FAU_GEN.1)**	**Startup Audit Services** Mar 30 2021 04:16:03 Info [CFGMGR]:Server thread is running. Mar 30 2021 04:16:02 Notice [CFGMGR]:Platform resource file is ready. Mar 30 2021 04:16:02 Notice [CFGMGR]:Platform resource file not ready... Mar 30 2021 04:16:02 Info [CFGMGR]:a10cfgmgr daemon start running May 05 2021 12:43:53 [admin] cli: [10.65.25.165:46876] audit enable May 06 2021 16:38:12 [admin] web: [362:10.65.25.165:9940] RESP HTTP status 200 OK May 06 2021 16:38:12 [admin] web: [362:10.65.25.165:9940] payload section 1 {"audit": {"enable": 1, "privilege": 1}} May 06 2021 16:37:32 [admin] web: [362:10.65.25.165:9792] POST: /axapi/v3/audit **Shutdown Audit Services** May 06 2021 16:09:52 [admin] cli: [10.1.1.164:1766] no audit enable May 06 2021 16:38:31 [admin] web: [362:10.65.25.165:9988] POST: /axapi/v3/audit
Administrative login and logout **(FAU_GEN.1)** Ability to administer the TOE locally and remotely **(FMT_SMF.1)**	**Add Administrator Account** Sep 03 2021 15:48:02 [admin] cli: [127.0.0.1] privilege write Sep 03 2021 15:47:54 [admin] cli: [127.0.0.1] admin acos-rw password ****** Sep 03 2021 16:20:19 [admin] web: [8:10.65.25.165:16122] payload section 1 {"admin": {"user": "GUI-ro", "password-key": 1, "passwd-string": "*" , "action": "enable", "privilege-global": "read", "access": {"access-type": "cli,web,axapi"}}} Sep 03 2021 16:20:19 [admin] web: [8:10.65.25.165:16122] POST: /axapi/v3/admin **Delete Administrator Account** Sep 03 2021 15:50:48 Info [SYSTEM]:User acos-rw delete ssh-pubkey (index: 0) succeed Sep 03 2021 15:50:46 [admin] cli: [127.0.0.1] no admin acos-rw Sep 03 2021 16:29:12 [admin] web: [8:10.65.25.165:17786] DELETE: /axapi/v3/admin/GUI-ro **Console Login** Mar 08 2021 03:07:08 [niap-user1] cli: [127.0.0.1] configure Mar 08 2021 03:07:07 [niap-user1] cli: [127.0.0.1] enable Mar 08 2021 03:07:06 Notice [SYSTEM]:A cli session for user "niap-user1" from 127.0.0.1 has been opened. Session ID assigned is 55. Mar 08 2021 03:07:04 Info [SYSTEM]:Local authentication successful (user: niap-user1). **Remote SSH Login** Mar 08 2021 03:28:59 [niap-user1] cli: [10.1.1.165:47440] configure Mar 08 2021 03:28:57 [niap-user1] cli: [10.1.1.165:47440] enable

AUDITABLE EVENT	SAMPLE RECORD
	Mar 08 2021 03:28:56 Notice [SYSTEM]:A cli session for user "niap-user1" from 10.1.1.165 has been opened. Session ID assigned is 60. Mar 08 2021 03:28:54 Info [SYSTEM]:Local authentication successful (user: niap-user1). **Remote GUI Login** Mar 08 2021 03:41:45 Notice [SYSTEM]:A web session for user "niap-user1" from 10.1.1.165 has been opened. Session ID assigned is 64. Mar 08 2021 03:41:45 Info [SYSTEM]:Local authentication successful (user: niap-user1). Mar 08 2021 03:41:45 [niap-user1] web: [64:10.1.1.165:9348] RESP HTTP status 200 OK Mar 08 2021 03:41:45 [niap-user1] web: [64:10.1.1.165:9348] POST: /axapi/v3/auth Mar 08 2021 03:41:45 A web session[64] opened, username: niap-user1, remote host: 10.1.1.165 **Console Logout** May 25 2021 23:45:34 Notice [SYSTEM]:Session ID 17 is now closed. May 25 2021 23:45:34 Session[17] closed May 25 2021 23:45:32 [niap-user1] cli: [127.0.0.1] exit **Remote SSH Logout** May 25 2021 23:24:27 Notice [SYSTEM]:Session ID 14 is now closed. May 25 2021 23:24:27 Session[14] closed May 25 2021 23:24:25 [niap-user1] cli: [10.65.25.166:58654] exit **Remote GUI Logout** May 25 2021 23:30:04 Notice [SYSTEM]:Session ID 15 is now closed. May 25 2021 23:30:04 [niap-user1] web: [15:10.65.25.166:8104] RESP HTTP status 200 OK May 25 2021 23:30:04 Session[15] closed May 25 2021 23:30:04 [niap-user1] web: [15:10.65.25.166:8104] POST: /axapi/v3/logoff
Security related configuration changes **(FAU_GEN.1)** Configure the access banner **(FMT_SMF.1)**	**CLI Configured Login Banners** May 25 2021 01:09:29 Info [SYSTEM]:ACOS Login banner is set. May 25 2021 01:09:29 [admin] cli: [10.65.25.166:53288] banner login "SSH–Test Pre-Login Message" May 25 2021 01:37:48 Info [SYSTEM]:ACOS EXEC banner is set. May 25 2021 01:37:48 [admin] cli: [10.65.25.166:40114] banner exec "SSH–Test Post-Login Message" **GUI Configured Login Banners** May 25 2021 01:54:28 [admin] web: [361:10.65.25.166:13166] payload section 1 {"web-service": {"axapi-idle": 10, "axapi-session-limit": 30, "gui-idle": 15, "gui-session-limit": 30, "port": 80, "secure-port": 443, "login-message": "GUI-Test Post-Login Message", "pre-login-message": "GUI-Test Pre-Login Message."}} May 25 2021 01:54:28 [admin] web: [361:10.65.25.166:13166] PUT: /axapi/v3/web-service
Generating/import of, changing, or deleting of cryptographic keys **(FAU_GEN.1)**	**CSR - Generate CSR+Key Pair, Export CSR- CLI** May 14 2021 18:07:50 Info [SYSTEM]:Exported file niap to root :10.65.25.165 /root/myca/intermediate/certs/niap.csr using scp May 14 2021 18:07:50 [admin] cli: [10.65.25.165:55496] export csr niap use-mgmt-port scp://root:******@10.65.25.165/root/myca/intermediate/certs/niap.csr

AUDITABLE EVENT	SAMPLE RECORD
	May 14 2021 18:06:49 [admin] cli: [10.65.25.165:55496] pki create csr niap **CSR - Generate CSR+Key Pair, Export CSR - GUI** May 14 2021 20:35:06 [admin] web: [255:10.65.25.165:9762] payload section 1 {"ssl-key": {"file": "niap1", "file-handle": "/a10data/key/niap1", "secured": 0, "action": "create"}} May 14 2021 20:35:06 [admin] web: [255:10.65.25.165:9762] POST: /axapi/v3/file/ssl-key May 14 2021 20:35:06 [admin] web: [255:10.65.25.165:9760] RESP HTTP status 204 No Content : No content. May 14 2021 20:35:06 [admin] web: [255:10.65.25.165:9760] payload section 1 {"create-oper": {"filename": "niap1", "bits": "2048", "common-name": "niap1", "valid-days": 730, "country": "US", "cert-type": "rsa", "digest": "sha256", "v3-request": 1}} May 14 2021 20:35:05 [admin] web: [255:10.65.25.165:9760] POST: /axapi/v3/pki/create-oper **CSR - Import --- N/A** **CSR – Delete - CLI** May 14 2021 20:26:14 Info [MGMT]:CSR 'niap' was deleted May 14 2021 20:26:14 [admin] cli: [10.65.25.165:46312] pki delete csr niap Jul 09 2021 19:30:29 Info [MGMT]:Private key 'del_pkey' was deleted Jul 09 2021 19:30:29 [admin] cli: [127.0.0.1] pki delete private-key del_pkey **CSR – Delete - GUI** May 14 2021 21:06:27 Info [MGMT]:Private key 'niap2' was deleted May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15990] RESP HTTP status 204 No Content : No content. May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15990] payload section 1 {"delete": {"private-key": "niap2"}} May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15990] POST: /axapi/v3/pki/delete May 14 2021 21:06:27 Info [MGMT]:CSR 'niap2' was deleted May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15994] payload section 1 {"delete": {"csr": "niap2"}} May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15994] POST: /axapi/v3/pki/delete **CSR - Change/Modify --- N/A**
Resetting Passwords **(FAU_GEN.1)**	Mar 29 2021 23:11:42 Info [SYSTEM]:change user(niap-user3) password successfully Mar 29 2021 23:11:42 [admin] cli: [10.1.1.165:41422] admin niap-user3 password ****** May 24 2021 01:10:44 Info [SYSTEM]:change user(niap-user1) password successfully May 24 2021 01:10:44 [admin] cli: [10.65.25.166:56652] password ****** May 24 2021 01:10:32 [admin] cli: [10.65.25.166:56652] admin niap-user1 Sep 03 2021 16:25:27 [admin] web: [8:10.65.25.165:17098] payload section 1 {"admin": {"user": "GUI-ro", "password-key": 1, "passwd-string": "*" , "action": "enable", "access": {"access-type": "cli,web,axapi"}}} Sep 03 2021 16:25:27 [admin] web: [8:10.65.25.165:17098] PUT: /axapi/v3/admin/GUI-ro

AUDITABLE EVENT	SAMPLE RECORD
Configure the session inactivity time before session termination or locking; **(FMT_SMF.1)**	**Set Session termination due to CLI inactivity** May 12 2021 17:44:20 [admin] cli: [127.0.0.1] terminal idle-timeout 5 Sep 03 2021 17:04:27 [admin] web: [14:10.65.25.165:3276] payload section 1 {"terminal": {"auto-size": 1, "editing": 1, "history-cfg": {"enable": 1, "size": 256}, "idle-timeout": 15, "prompt-cfg": {"prompt": 0}}} Sep 03 2021 17:04:27 [admin] web: [14:10.65.25.165:3276] PUT: /axapi/v3/terminal **Set Session termination due to GUI inactivity** May 12 2021 17:45:53 [admin] cli: [127.0.0.1] web-service gui-timeout-policy idle 5 Sep 03 2021 17:07:02 [admin] web: [14:10.65.25.165:3772] payload section 1 {"web-service": {"axapi-idle": 10, "axapi-session-limit": 30, "gui-idle": 20, "gui-session-limit": 30, "port": 80, "secure-port": 443}} Sep 03 2021 17:07:02 [admin] web: [14:10.65.25.165:3772] PUT: /axapi/v3/web-service **CLI Local Console - Inactivity Timeout** Mar 05 2021 04:01:15 Notice [SYSTEM]:Session ID 80 is now closed. Mar 05 2021 04:01:15 Notice [SYSTEM]:Session ID 80 for user "niap-user1" from 127.0.0.1 has timed out. * * * Mar 05 2021 03:56:08 Notice [SYSTEM]:A cli session for user "niap-user1" from 127.0.0.1 has been opened. Session ID assigned is 80. **CLI SSH Remote - Inactivity Timeout** Mar 05 2021 04:26:12 Notice [SYSTEM]:Session ID 87 is now closed. Mar 05 2021 04:26:12 Notice [SYSTEM]:Session ID 87 for user "niap-user1" from 10.1.1.165 has timed out. * * * Mar 05 2021 04:23:06 Notice [SYSTEM]:A cli session for user "niap-user1" from 10.1.1.165 has been opened. Session ID assigned is 87. **GUI - Inactivity Timeout** Mar 05 2021 04:44:56 Info [SYSTEM]:Session timed out Mar 05 2021 04:44:56 Notice [SYSTEM]:Session ID 92 for user "niap-user1" from 10.1.1.165 has timed out. * * * Mar 05 2021 04:41:50 Notice [SYSTEM]:A web session for user "niap-user1" from 10.1.1.165 has been opened. Session ID assigned is 92.
Update the TOE **(FMT_SMF.1)**	**Update Initiation (primary/secondary) via CLI** Sep 08 2021 02:00:25 Info [SYSTEM]:upgrade: user=root;host=10.65.25.165;filepath=/root/images/re_test_images/ACOS_FTA_5_2_1-p3_41.64.upg;service=scp;primary=1 Sep 08 2021 02:00:13 [niap-user1] cli: [10.65.25.166:41938] upgrade hd pri use-mgmt-port scp://root@10.65.25.165/root/images/re_test_images/ACOS_FTA_5_2_1-p3_41.64.upg

AUDITABLE EVENT	SAMPLE RECORD
	Sep 08 2021 02:26:21 Info [SYSTEM]:upgrade: user=root;host=10.65.25.165;filepath=/root/images/re_test_images/ACOS_FTA_5_2_1-p3_41.64.upg;service=scp;primary=0 Sep 08 2021 02:26:16 [niap-user1] cli: [10.65.25.166:55222] upgrade hd sec use-mgmt-port scp://root@10.65.25.165/root/images/re_test_images/ACOS_FTA_5_2_1-p3_41.64.upg **Update Initiation (primary/secondary) via GUI** Sep 07 2021 13:52:52 Info [SYSTEM]:upgrade: user=user;host=10.65.25.165;filepath=/home/user/ACOS_FTA_5_2_1-p3_43.64.upg;service=scp;primary=1 Sep 07 2021 13:52:52 [admin] web: [69:10.65.25.166:33204] RESP HTTP status 202 Accepted : The upgrade request has been received. Sep 07 2021 13:52:52 [admin] web: [69:10.65.25.166:33204] POST: /axapi/v3/upgrade/hd Sep 07 2021 14:00:59 Info [SYSTEM]:upgrade: user=user;host=10.65.25.165;filepath=/home/user/ACOS_FTA_5_2_1-p3_43.64.upg;service=scp;primary=0 Sep 07 2021 14:00:59 [admin] web: [69:10.65.25.166:43012] RESP HTTP status 202 Accepted : The upgrade request has been received. Sep 07 2021 14:00:59 [admin] web: [69:10.65.25.166:43012] POST: /axapi/v3/upgrade/hd **Update Success (primary/secondary)** Sep 08 2021 02:03:51 Info [SYSTEM]:Upgraded Hard Disk Primary image of ACOS from root@10.65.25.165:/root/images/re_test_images/ACOS_FTA_5_2_1-p3_41.64.upg. Sep 08 2021 02:30:07 Info [SYSTEM]:Upgraded Hard Disk Secondary image of ACOS from root@10.65.25.165:/root/images/re_test_images/ACOS_FTA_5_2_1-p3_41.64.upg.. **Update Failure** Jun 24 2021 02:41:31 Error [SYSTEM]:file is invalid: image integrity test failed Jun 24 2021 02:54:05 Error [SYSTEM]:Upgrade image file is invalid.
Configure the Authentication Failure Parameters **(FMT_SMF.1)**	**Configure Auth Failure Lockout** May 25 2021 23:20:35 [admin] cli: [10.65.25.166:50928] admin-lockout threshold 10 May 25 2021 23:20:15 [admin] cli: [10.65.25.166:50928] admin-lockout duration 15 May 25 2021 23:19:52 [admin] cli: [10.65.25.166:50928] admin-lockout enable "Sep 03 2021 17:11:48 [admin] web: [15:10.65.25.165:4394] payload section 1 {""admin-lockout"": {""duration"": 15, ""enable"": 1, ""reset-time"": 25, ""threshold"": 3}} Sep 03 2021 17:11:48 [admin] web: [15:10.65.25.165:4394] PUT: /axapi/v3/admin-lockout" **Configure Auth Failure Lockout** Mar 29 2021 22:04:41 [admin] cli: [10.1.1.165:33850] system password-policy complexity Simple min-pswd-len 15 **CLI Lockout**

AUDITABLE EVENT	SAMPLE RECORD
	May 25 2021 23:48:27 Error [SYSTEM]:The user, niap-user1, from the remote host, 10.65.25.166, failed in the cli authentication. May 25 2021 23:48:27 Info [SYSTEM]:Local authentication failed(user: niap-user1): Admin user is disabled. **Web/GUI Lockout** Mar 29 2021 00:40:06 Error [SYSTEM]:The user, niap-user1, from the remote host, 10.1.1.165, failed in the web authentication. Mar 29 2021 00:40:06 Info [SYSTEM]:Local authentication failed(user: niap-user1): Admin user is disabled.
Configure Audit Behaviour **(FMT_SMF.1)**	**Audit-Category Logging - Enable** May 05 2021 12:43:58 [admin] cli: [10.65.25.165:46876] audit size 1000 May 05 2021 12:43:53 [admin] cli: [10.65.25.165:46876] audit enable May 06 2021 16:38:12 [admin] web: [362:10.65.25.165:9940] payload section 1 {"audit": {"enable": 1, "privilege": 1}} May 06 2021 16:37:32 [admin] web: [362:10.65.25.165:9792] POST: /axapi/v3/audit **Audit-Category Logging - Disable** May 06 2021 16:09:52 [admin] cli: [10.1.1.164:1766] no audit enable May 06 2021 16:38:31 [admin] web: [362:10.65.25.165:9988] POST: /axapi/v3/audit **Audit-Category Logging – Enable Syslog** May 05 2021 12:44:27 [admin] cli: [10.65.25.165:46876] logging auditlog host 1.1.1.1 facility local1 May 06 2021 16:48:27 [admin] web: [362:10.65.25.165:12298] payload section 1 {"auditlog": {"host4": "1.1.1.1", "audit-facility": "local0", "port": 514}} May 06 2021 16:48:27 [admin] web: [362:10.65.25.165:12298] POST: /axapi/v3/logging/auditlog **Audit-Category Logging – Disable Syslog** May 05 2021 12:47:20 [admin] cli: [10.65.25.165:46876] no logging auditlog host 1.1.1.1 May 06 2021 16:48:49 [admin] web: [362:10.65.25.165:12420] DELETE: /axapi/v3/logging/auditlog **Event-Category Logging – Enable** May 05 2021 12:44:37 [admin] cli: [10.65.25.165:46876] logging buffered debugging May 05 2021 12:44:33 [admin] cli: [10.65.25.165:46876] logging buffered 50000 May 05 2021 13:02:38 [admin] web: [234:10.65.25.165:3710] payload section 1 {"buffered": {"buffersize": 50000, "levelname": "debugging"}} May 05 2021 13:02:38 [admin] web: [234:10.65.25.165:3710] PUT: /axapi/v3/logging/buffered **Event-Category Logging – Disable** May 06 2021 16:07:06 [admin] cli: [10.1.1.164:1766] logging buffered disable May 06 2021 16:42:39 [admin] web: [362:10.65.25.165:11046] payload section 1

AUDITABLE EVENT	SAMPLE RECORD
	{"buffered": {"buffersize": 50000, "levelname": "disable"}} May 06 2021 16:42:39 [admin] web: [362:10.65.25.165:11046] PUT: /axapi/v3/logging/buffered **Event-Category Logging – Enable Syslog and Server** May 06 2021 16:10:54 [admin] cli: [10.1.1.164:1766] logging host 2.2.2.2 May 05 2021 12:46:21 [admin] cli: [10.65.25.165:46876] logging syslog notification May 06 2021 16:46:28 [admin] web: [362:10.65.25.165:11876] payload section 1 {"ipv4addr": {"host-ipv4": "1.1.1.1", "port": 514}} May 06 2021 16:46:28 [admin] web: [362:10.65.25.165:11876] POST: /axapi/v3/logging/host/ipv4addr May 05 2021 13:02:38 [admin] web: [234:10.65.25.165:3714] payload section 1 {"syslog": {"syslog-levelname": "notification"}} May 05 2021 13:02:38 [admin] web: [234:10.65.25.165:3714] PUT: /axapi/v3/logging/syslog **Event-Category Logging – Disable Syslog** May 06 2021 16:06:23 [admin] cli: [10.1.1.164:1766] logging syslog disable May 06 2021 16:42:39 [admin] web: [362:10.65.25.165:11050] payload section 1 {"syslog": {"syslog-levelname": "disable"}} May 06 2021 16:42:39 [admin] web: [362:10.65.25.165:11050] PUT: /axapi/v3/logging/syslog **Event-Category Logging – Disable Syslog Server** May 06 2021 16:11:14 [admin] cli: [10.1.1.164:1766] no logging host 2.2.2.2 May 06 2021 16:46:42 [admin] web: [362:10.65.25.165:11928] DELETE: /axapi/v3/logging/host/ipv4addr/1.1.1.1 **Clear Audit and Event Logs** May 06 2021 16:05:35 [admin] cli: [10.1.1.164:1766] clear logging May 06 2021 16:05:31 [admin] cli: [10.1.1.164:1766] clear audit May 05 2021 14:09:30 [admin] web: [241:10.65.25.165:13594] DELETE: /axapi/v3/syslog/oper May 05 2021 14:06:31 [admin] web: [241:10.65.25.165:13002] DELETE: /axapi/v3/sys-audit-log/oper **Disable Event Logging Display to TOE Console** Jul 09 2021 15:32:51 [admin] cli: [127.0.0.1] logging console disable **Enable VPN Log to Event Log** Jul 09 2021 15:33:23 [admin] cli: [127.0.0.1] vpn ike-logging-enable
Manage the Cryptographic Keys **(FMT_SMF.1)**	*See "Generating/import of, changing, or deleting of cryptographic keys (FAU_GEN.1)".*
Configure the Cryptographic Functionality **(FMT_SMF.1)**	**Enable IPsec IKE SA Key Strength Checking** Jul 09 2021 15:33:16 [admin] cli: [127.0.0.1] vpn ipsec-cipher-check **Configure VPN IKE Gateway** Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] nat-traversal

AUDITABLE EVENT	SAMPLE RECORD
	Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] lifetime 86400 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] remote-address ip 10.1.1.164 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] local-address ip 10.1.1.39 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] dh-group 14 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] encryption aes-256 hash sha256 priority 5 Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] remote-id "C=US, ST=CA, O=a10app, CN=ocsp" Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] local-id "C=US, ST=CA, O=a10app, OU=a10app, CN=ACOS" Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] local-cert test-rsa Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] key test-rsa ****** Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] interface-management Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] auth-method rsa-signature Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] ike-version v2 Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] vpn ike-gateway ipsec_to_mgmt39 "Sep 03 2021 19:00:08 [admin] web: [32:10.1.1.167:7364] payload section 1 {""ike-gateway"": {""auth-method"": ""preshare-key"", ""ike-version"": ""v2"", ""dh-group"": ""14"", ""enc-cfg"": [{""encryption"": ""aes-256"", ""hash"": ""sha256"", ""priority"": 5}], ""name"": ""ipsec_to_mgmt39"", ""local-address"": {""local-ip"": ""10.1.1.39""}, ""local-cert"": {""local-cert-name"": null}, ""local-id"": ""ST=CA, O=a10app, OU=a10app, CN=ACOS"", ""remote-address"": {""remote-ip"": ""10.1.1.164""}, ""remote-id"": ""C=US, ST=CA, O=a10app, CN=ocsp"", ""lifetime"": 86400, ""nat-traversal"": ""1"", ""dpd"": {""interval"": 10, ""retry"": 3}, ""preshare-key-value"": ""*"" , ""interface-management"": ""1""}} Sep 03 2021 19:00:06 [admin] web: [32:10.1.1.167:7364] POST: /axapi/v3/vpn/i" **Configure VPN IPsec Tunnel** Jul 09 2021 15:35:07 [admin] cli: [127.0.0.1] ike-gateway ipsec_to_mgmt39 Jul 09 2021 15:35:07 [admin] cli: [127.0.0.1] traffic-selector ipv4 local 10.1.1.39 255.255.255.255 remote 10.65.25.67 255.255.255.255 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] lifebytes 10240 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] lifetime 28800 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] encryption aes-256 hash sha256 priority 5 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] dh-group 14 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] proto esp Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] mode tunnel Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] vpn ipsec ipsec_to_mgmt39 "Sep 03 2021 19:07:33 [admin] web: [32:10.1.1.167:8778] payload section 1 {""ipsec"": {""name"": ""ipsec_to_mgmt39_1"", ""ipsec-gateway"": {""ike-gateway"": ""ipsec_to_mgmt39""}, ""dh-group"": ""14"", ""enc-cfg"": [{""encryption"": ""aes-256"", ""hash"": ""sha256"", ""priority"": ""5""}], ""lifetime"": 28800, ""lifebytes"": 0, ""anti-replay-window"": ""0"", ""mode"": ""tunnel"", ""proto"": ""esp"", ""traffic-selector"": {""ipv4"": {""local"": ""10.1.1.39"", ""local_netmask"": ""255.255.255.255"", ""remote-ip"": ""10.65.25.165"", ""remote_netmask"": ""255.255.255.255"", ""protocol"": null}}, ""dscp"": null, ""sequence-number-disable"": 0}} Sep 03 2021 19:07:26 [admin] web: [32:10.1.1.167:8778] POST: /axapi/v3/vpn/ipsec/"

AUDITABLE EVENT	SAMPLE RECORD
Configure the Lifetime for IPsec SAs; **(FMT_SMF.1)**	**Configure VPN IKE Gateway - SA Lifetime** Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] lifetime 86400 Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] vpn ike-gateway ipsec_to_mgmt39 *See "Configure the Cryptographic Functionality (FMT_SMF.1)" for GUI equivalent sample log entry(s).* **Configure VPN IPsec Tunnel - SA Lifetime** Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] lifebytes 10240 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] lifetime 28800 Jul 09 2021 15:35:03 [admin] cli: [127.0.0.1] vpn ipsec ipsec_to_mgmt39 *See "Configure the Cryptographic Functionality (FMT_SMF.1)" for GUI equivalent sample log entry(s).*
Re-enable an Administrator Account **(FMT_SMF.1)**	**Unlock Admin Account Locked due to Auth Lockout** Mar 29 2021 02:10:07 [admin] cli: [127.0.0.1] unlock Mar 29 2021 02:10:02 [admin] cli: [127.0.0.1] admin inap-user1
Set the Time Which is Used for Time-stamps **(FMT_SMF.1)**	**Local Clock Time Change** Sep 03 2021 10:10:10 Notice [TM]:Time has been changed, current: Fri Sep 03 10:10:10 PDT 2021, previous: Fri Sep 03 23:36:51 PDT 2021 Sep 03 2021 23:36:51 [admin] cli: [127.0.0.1] clock set 10:10:10 September 3 2021 Sep 03 2021 23:36:35 [admin] cli: [127.0.0.1] timezone America/Los_Angeles
Configure NTP **(FMT_SMF.1)**	**Configure NTP Sources** Sep 03 2021 10:00:34 [admin] cli: [127.0.0.1] ntp server 10.65.25.67 Sep 03 2021 10:00:27 [admin] cli: [127.0.0.1] ntp server 10.65.25.166 Sep 03 2021 10:00:20 [admin] cli: [127.0.0.1] ntp server 10.65.25.165 Sep 03 2021 18:26:32 [admin] web: [29:10.65.25.165:18516] payload section 1 {"hostname": {"host-servername": "10.65.25.67", "key": null, "action": "enable"}} Sep 03 2021 18:26:32 [admin] web: [29:10.65.25.165:18516] POST: /axapi/v3/ntp/server/hostname Sep 03 2021 18:26:24 [admin] web: [29:10.65.25.165:18474] payload section 1 {"hostname": {"host-servername": "10.65.25.166", "key": null, "action": "enable"}} Sep 03 2021 18:26:24 [admin] web: [29:10.65.25.165:18474] POST: /axapi/v3/ntp/server/hostname Sep 03 2021 18:25:40 [admin] web: [29:10.65.25.165:18308] payload section 1 {"hostname": {"host-servername": "10.65.25.165", "key": null, "action": "enable"}} Sep 03 2021 18:25:40 [admin] web: [29:10.65.25.165:18308] POST: /axapi/v3/ntp/server/hostname **Remove NTP Sources** Sep 03 2021 18:24:02 Info [SYSTEM]:No NTP server defined. Setting time source to hardware calendar Jun 22 2021 19:10:38 [admin] cli: [10.65.25.165:50546] no ntp server 10.65.25.167 Jun 22 2021 19:10:33 [admin] cli: [10.65.25.165:50546] no ntp server 10.65.25.166 Jun 22 2021 19:10:26 [admin] cli: [10.65.25.165:50546] no ntp server 10.65.25.165

AUDITABLE EVENT	SAMPLE RECORD
	Sep 03 2021 18:23:38 [admin] web: [29:10.65.25.165:17930] DELETE: /axapi/v3/ntp/server/hostname/10.65.25.67 Sep 03 2021 18:23:35 [admin] web: [29:10.65.25.165:17918] DELETE: /axapi/v3/ntp/server/hostname/10.65.25.166 Sep 03 2021 18:23:29 [admin] web: [29:10.65.25.165:17888] DELETE: /axapi/v3/ntp/server/hostname/10.65.25.165 **NTP Discontinuous Time Change** Sep 03 2021 22:55:05 Notice [TM]:Time has been changed, current: Fri Sep 03 22:55:05 PDT 2021, previous: Fri Sep 03 10:20:17 PDT 2021 Sep 03 2021 22:55:04 Info [SYSTEM]:NTP server 10.65.25.67 is in polling state Sep 03 2021 22:55:04 Info [SYSTEM]:NTP server 10.65.25.166 is in polling state Sep 03 2021 22:55:04 Info [SYSTEM]:NTP server 10.65.25.165 is in polling state
Configure the Reference Identifier for the Peer **(FMT_SMF.1)**	**Configure Reference IDs for VPN IKE Gateway** Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] remote-id "C=US, ST=CA, O=a10app, CN=ocsp" Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] local-id "C=US, ST=CA, O=a10app, OU=a10app, CN=ACOS" Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] vpn ike-gateway ipsec_to_mgmt39 *See "Configure the Cryptographic Functionality (FMT_SMF.1)" for GUI equivalent sample log entry(s).*
Manage the TOE's Trust Store and Designate X509.v3 certificates as Trust Anchors; **(FMT_SMF.1)**	**Signed Device or Intermediate Cert - Generate ---N/A** **Signed Device or Intermediate Cert - Import** May 14 2021 18:17:48 Info [MGMT]:Certificate 'niap' was imported May 14 2021 18:17:48 [admin] cli: [10.65.25.165:55496] import cert niap use-mgmt-port scp://root:******@10.65.25.165/root/myca/intermediate/certs/niap.crt May 14 2021 21:04:19 Info [MGMT]:Certificate 'niap2' was imported May 14 2021 21:04:19 [admin] web: [257:10.65.25.165:15532] payload section 1 {"ssl-cert": {"file": "niap2", "file-handle": "/a10data/var/tmp/axgui/niap2_1621051458.9639745_429", "certificate-type": "pem", "pfx-password": "a10$pass", "action": "import"}} May 14 2021 21:04:19 [admin] web: [257:10.65.25.165:15532] POST: /axapi/v3/file/ssl-cert **Signed Device or Intermediate Cert - Delete** May 14 2021 20:29:02 Info [MGMT]:Certificate 'niap' was deleted May 14 2021 20:29:02 [admin] cli: [10.65.25.165:46312] pki delete certificate niap May 14 2021 21:06:27 Info [MGMT]:Certificate 'niap2' was deleted May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15988] payload section 1 {"delete": {"cert-name": "niap2"}} May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15988] POST: /axapi/v3/pki/delete **Signed Device or Intermediate Cert - Change/Modify --- N/A**

AUDITABLE EVENT	SAMPLE RECORD
	Root CA Cert - Generate ---N/A **Root CA Cert - Import** May 14 2021 20:23:32 Info [MGMT]:CA Certificate 'ca-cert' was imported May 14 2021 20:23:32 [admin] cli: [10.65.25.165:46312] import ca-cert ca-cert use-mgmt-port scp://root:******@10.65.25.165/root/myca/cacert.pem May 14 2021 21:05:44 [admin] web: [257:10.65.25.165:15840] payload section 1 {"ca-cert": {"file": "ca-cert-niap2", "file-handle": "/a10data/var/tmp/axgui/ca-cert-niap2_1621051544.5291243_99", "certificate-type": "pem", "pfx-password": "a10$pass", "action": "import"}} May 14 2021 21:05:44 [admin] web: [257:10.65.25.165:15840] POST: /axapi/v3/file/ca-cert **Root CA Cert - Delete** May 14 2021 20:28:53 Info [MGMT]:CA 'cacert.pem' was deleted May 14 2021 20:28:53 [admin] cli: [10.65.25.165:46312] pki delete certificate ca cacert.pem May 14 2021 21:06:27 Info [MGMT]:CA 'ca-cert-niap2' was deleted May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15992] payload section 1 {"delete": {"ca": "ca-cert-niap2"}} May 14 2021 21:06:27 [admin] web: [257:10.65.25.165:15992] POST: /axapi/v3/pki/delete **Root CA Cert- Change/Modify --- N/A** **Configure IPsec VPN IKE Gateway For Device Certificate/Key** Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] local-cert test-rsa Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] key test-rsa ****** Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] auth-method rsa-signature Jul 09 2021 15:34:59 [admin] cli: [127.0.0.1] vpn ike-gateway ipsec_to_mgmt39 *See "Configure the Cryptographic Functionality (FMT_SMF.1)" for GUI equivalent sample log entry(s).* **Configure IPsec VPN IKE Gateway For Device Preshared Key** Jul 09 2021 18:26:56 [admin] cli: [127.0.0.1] auth-method preshare-key ****** Jul 09 2021 18:26:50 [admin] cli: [127.0.0.1] vpn ike-gateway ipsec_to_mgmt39 *See "Configure the Cryptographic Functionality (FMT_SMF.1)" for GUI equivalent sample log entry(s).* **Invalid Peer Certificate - Broken Trust Chain** May 10 2021 14:38:59 Info [VPN]:26[CFG] <ipsec_mgmt|5> no issuer certificate found for "C=US, ST=CA, O=a10app, CN=intermediateca" **Invalid Peer Certificate - Expired**

AUDITABLE EVENT	SAMPLE RECORD
	May 10 2021 14:54:35 Info [VPN]:36[IKE] <ipsec_mgmt|21> no trusted RSA public key found for 'C=US, ST=CA, O=a10app, CN=test2-ax' May 10 2021 14:54:35 Info [VPN]:36[CFG] <ipsec_mgmt|21> subject certificate invalid (valid from Mar 31 07:44:26 2021 to Apr 01 07:44:26 2021) **Invalid Peer Certificate – CRL Revoked** May 11 2021 02:48:49 Info [VPN]:32[CFG] <ipsec_mgmt|637> certificate was revoked on Apr 01 01:46:59 UTC 2021, reason: unspecified May 11 2021 02:48:49 Info [VPN]:32[CFG] <ipsec_mgmt|637> fetching crl from 'http://10.65.25.165/myca.crl' … May 11 2021 02:48:49 Info [VPN]:32[CFG] <ipsec_mgmt|637> checking certificate status of "C=US, ST=CA, O=a10app, CN=test3" **Invalid Peer Certificate – OCSP Revoked** May 11 2021 05:19:08 Info [VPN]:70[CFG] <ipsec_mgmt|769> certificate was revoked on Apr 01 01:46:59 UTC 2021, reason: unspecified May 11 2021 05:19:08 Info [VPN]:70[CFG] <ipsec_mgmt|769> requesting ocsp status from 'http://10.65.25.165:8181' ... May 11 2021 05:19:08 Info [VPN]:70[CFG] <ipsec_mgmt|769> checking certificate status of "C=US, ST=CA, O=a10app, CN=test3" **Invalid Peer Certificate – Corrupt or Malformed Certificate** May 11 2021 06:14:45 Info [VPN]:34[LIB] <ipsec_mgmt|8> OpenSSL X.509 parsing failed May 11 2021 06:14:45 Info [VPN]:34[ASN] <ipsec_mgmt|8> L0 - x509: length of ASN.1 object invalid or too large **Invalid Peer Certificate – Explicit EC** May 06 2021 05:21:52 Info [VPN]:73[CFG] <ipsec_mgmt|48> untrusted issuer certificate "C=US, ST=CA, O=a10, CN=interca2-ecdsa" uses explicit EC parameters **Invalid Local Certificate – Explicit EC** May 11 2021 13:52:07 Info [VPN]:17[CFG] failed to load ca certificate from '/a10data/ca/interca2-ec', it is using explicit EC parameters **Invalid Local Certificate – Corrupt or Malformed CA Certificate** May 11 2021 14:38:52 Info [VPN]:17[CFG] failed to load ca certificate from '/a10data/ca/interca2', it is not ca certificate
Trusted Channel (Initiation, Termination, Failure)	**IPsec Initiation (from TOE)** Apr 29 2021 17:06:07 Info [VPN]:72[IKE] <ipsec_to_mgmt39|39> CHILD_SA ipsec_to_mgmt39_1{2} established with SPIs c52a706d_i 2f82c6ea_o and TS 10.1.1.39/32 === 10.65.25.165/32 Apr 29 2021 17:06:07 Info [VPN]:72[IKE] <ipsec_to_mgmt39|39> IKE_SA ipsec_to_mgmt39[39] established between 10.1.1.39[C=US, ST=CA, O=a10app, OU=a10app, CN=ACOS]...10.1.1.164[C=US, ST=CA, O=a10app, CN=ocsp] Apr 29 2021 17:04:38 Info [VPN]:86[IKE] <ipsec_to_mgmt39|39> 10.1.1.39[500]->10.1.1.164[500]: [SA KE No N(NATD_S_IP) N(NATD_D_IP)]

AUDITABLE EVENT	SAMPLE RECORD
	Apr 29 2021 17:04:38 Info [VPN]:86[ENC] <ipsec_to_mgmt39|39> generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP)] **IPsec Initiation (from Peer)** Jul 09 2021 16:35:58 Info [VPN]:68[IKE] <ipsec_to_mgmt39|5> CHILD_SA ipsec_to_mgmt39_2{3} established with SPIs cf396353_i 4995779f_o and TS 10.1.1.39/32 === 10.65.25.166/32 Jul 09 2021 16:35:58 Info [VPN]:68[IKE] <ipsec_to_mgmt39|5> IKE_SA ipsec_to_mgmt39[5] established between 10.1.1.39[C=US, ST=CA, O=a10app, OU=a10app, CN=ACOS]...10.1.1.164[C=US, ST=CA, O=a10app, CN=ocsp] Jul 09 2021 16:35:58 Info [VPN]:67[IKE] <5> 10.1.1.164[500]->10.1.1.39[500]: [SA KE No N(NATD_S_IP) N(NATD_D_IP)] Jul 09 2021 16:35:58 Info [VPN]:67[ENC] <5> parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP)] **IPsec Termination (from TOE)** May 06 2021 12:06:18 Info [VPN]:17[IKE] <ipsec_mgmt|375> sending DELETE for IKE_SA ipsec_mgmt[375] May 06 2021 12:06:18 Info [VPN]:17[IKE] <ipsec_mgmt|375> deleting IKE_SA ipsec_mgmt[375] between 10.1.1.38[C=CN, ST=BJ, O=A10, OU=QA, CN=ax1]...10.1.1.164[C=CN, ST=BJ, O=A10, OU=QA, CN=ax2] **IPsec Termination (from Peer)** Jul 09 2021 15:07:56 Info [VPN]:121[IKE] <ipsec_to_mgmt39|3> deleting IKE_SA ipsec_to_mgmt39[3] between 10.1.1.39[C=US, ST=CA, O=a10app, OU=a10app, CN=ACOS]...10.1.1.164[C=US, ST=CA, O=a10app, CN=ocsp] Jul 09 2021 15:07:56 Info [VPN]:121[IKE] <ipsec_to_mgmt39|3> received DELETE for IKE_SA ipsec_to_mgmt39[3] **IPsec Termination (due to communication outage)** Apr 29 2021 17:04:38 Info [VPN]:86[IKE] <ipsec_to_mgmt39|39> initiating IKE_SA ipsec_to_mgmt39[39] to 10.1.1.164 Apr 29 2021 17:04:38 Info [VPN]:85[IKE] <ipsec_to_mgmt39|38> giving up after 5 retransmits Apr 29 2021 17:04:37 Info [VPN]:08[KNL] creating delete job for ESP CHILD_SA with SPI c4f443b7 and reqid {3} **IPsec Failure - TOE Rejecting IKE Session with Peer (Authentication/Cert-Validation Failure)** May 18 2021 10:35:01 Info [VPN]:105[IKE] <4762> 10.1.1.38[500]->10.1.1.164[500]: [N(AUTH_FAILED)] May 18 2021 10:35:01 Info [VPN]:105[ENC] <4762> generating IKE_AUTH response 1 [N(AUTH_FAILED)] **IPsec Failure - Peer Rejecting IKE Session with TOE** Jun 04 2021 07:15:26 Info [VPN]:50[IKE] <ipsec_to_mgmt|614> 10.1.1.38[500]->10.1.1.164[500]: [N(AUTH_FAILED)] Jun 04 2021 07:15:26 Info [VPN]:50[ENC] <ipsec_to_mgmt|614> parsed IKE_AUTH response 1 [N(AUTH_FAILED)]

AUDITABLE EVENT	SAMPLE RECORD
	IPSec Failure - TOE Rejecting ESP Session Proposal with Peer May 18 2021 12:51:55 Info [VPN]:30[IKE] <ipsec_mgmt|4880> 10.1.1.38[500]->10.1.1.164[500]: [N(NO_PROP)] May 18 2021 12:51:55 Info [VPN]:30[ENC] <ipsec_mgmt|4880> generating CREATE_CHILD_SA response 2 [N(NO_PROP)] May 18 2021 12:51:54 Info [VPN]:26[IKE] <ipsec_mgmt|4880> failed to establish CHILD_SA, keeping IKE_SA **IPSec Failure - Peer Rejecting IKE Session Proposal with TOE** May 29 2021 10:09:37 Info [VPN]:50[IKE] <ipsec_mgmt|7346> received NO_PROPOSAL_CHOSEN notify error May 29 2021 10:09:37 Info [VPN]:50[IKE] <ipsec_mgmt|7346> 10.1.1.164[500]->10.1.1.38[500]: [N(NO_PROP)] May 29 2021 10:09:37 Info [VPN]:50[ENC] <ipsec_mgmt|7346> parsed IKE_SA_INIT response 0 [N(NO_PROP)] **IPSec Failure - TOE Rejecting ESP Session Proposal with Peer (ESP Key Strength Greater than IKE)** May 08 2021 11:45:40 Info [VPN]:84[IKE] <ipsec_mgmt|67> sending DELETE for ESP CHILD_SA with SPI c76281a0 May 08 2021 11:45:40 Info [VPN]:84[IKE] <ipsec_mgmt|67> Notify peer to delete child_sa because of verify error. May 08 2021 11:45:40 Info [VPN]:84[IKE] <ipsec_mgmt|67> failed to establish CHILD_SA, keeping IKE_SA May 08 2021 11:45:40 Info [VPN]:84[IKE] <ipsec_mgmt|67> Proposal for IKE SA [IKE:AES_CBC_192/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_2048] is weaker then proposal for IPsec SA [ESP:AES_CBC_192/HMAC_SHA2_512_256/NO_EXT_SEQ], IPsec established failed! **IPsec Failure - TOE Rejecting IKE Session with Peer (Unacceptable Proposal)** May 18 2021 12:45:57 Info [VPN]:92[IKE] <4873> 10.1.1.38[500]->10.1.1.164[500]: [N(NO_PROP)] May 18 2021 12:45:57 Info [VPN]:92[ENC] <4873> generating IKE_SA_INIT response 0 [N(NO_PROP)] May 18 2021 12:45:57 Info [VPN]:92[IKE] <4873> received proposals inacceptable May 18 2021 12:45:57 Info [VPN]:92[CFG] <4873> configured proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048 May 18 2021 12:45:57 Info [VPN]:92[CFG] <4873> received proposals: IKE:AES_CBC_128/HMAC_MD5_96/PRF_HMAC_MD5/MODP_2048 **IPsec Failure - TOE Rejecting ESP Session with Peer (Unacceptable Proposal)** May 18 2021 12:49:12 Info [VPN]:78[IKE] <ipsec_mgmt|4878> 10.1.1.38[500]->10.1.1.164[500]: [N(NO_PROP)] May 18 2021 12:49:12 Info [VPN]:78[ENC] <ipsec_mgmt|4878> generating CREATE_CHILD_SA response 2 [N(NO_PROP)] May 18 2021 12:49:11 Info [VPN]:84[IKE] <ipsec_mgmt|4878> no acceptable proposal found

AUDITABLE EVENT	SAMPLE RECORD
	May 18 2021 12:49:11 Info [VPN]:84[CFG] <ipsec_mgmt|4878> configured proposals: ESP:AES_CBC_256/HMAC_SHA2_256_128/MODP_2048/NO_EXT_SEQ May 18 2021 12:49:11 Info [VPN]:84[CFG] <ipsec_mgmt|4878> received proposals: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ **IPsec Failure - TOE Rejecting IKE Session with Peer (No Reference ID Match)** May 18 2021 10:35:01 Info [VPN]:105[IKE] <4762> 10.1.1.38[500]->10.1.1.164[500]: [N(AUTH_FAILED)] May 18 2021 10:35:01 Info [VPN]:105[ENC] <4762> generating IKE_AUTH response 1 [N(AUTH_FAILED)] May 18 2021 10:35:01 Info [VPN]:105[ENC] <4762> header could not be parsed May 18 2021 10:35:01 Info [VPN]:105[CFG] <4762> no matching peer config found May 18 2021 10:35:01 Info [VPN]:105[CFG] <4762> looking for peer configs matching 10.1.1.38[C=CN, ST=BJ, O=A10, OU=QA, CN=ax1]...10.1.1.164[ax2-new] **SCP/SFTP File Transfer via IPsec** Jun 16 2021 14:11:49 Info [SYSTEM]:Exported file aflex-02 to user :10.65.25.165 /tmp/aflex-0202.bak using scp Jun 16 2021 14:11:48 [admin] cli: [127.0.0.1] export aflex aflex-02 use-mgmt-port scp://user@10.65.25.165/tmp/aflex-0202.bak Jun 16 2021 14:11:24 [admin] cli: [127.0.0.1] import aflex aflex-02 use-mgmt-port scp://user@10.65.25.165/tmp/aflex-02 Sep 07 2021 13:26:38 [admin] web: [63:10.65.25.166:1150] RESP HTTP status 204 No Content : No content. Sep 07 2021 13:26:38 [admin] web: [63:10.65.25.166:1150] POST: /axapi/v3/import **SCP/SFTP File Transfer via IPsec - Failure connection** Jun 16 2021 12:03:34 Error [SYSTEM]:ssh: connect to host 10.65.25.165 port 22: Connection timed outCouldn't read packet: Connection reset by peer. Jun 16 2021 12:03:29 [admin] cli: [127.0.0.1] export aflex aflex-02 use-mgmt-port sftp://user@10.65.25.165/tmp/aflex-0203.bak Jun 16 2021 12:03:11 Error [SYSTEM]:ssh: connect to host 10.65.25.165 port 22: Connection timed outCouldn't read packet: Connection reset by peer. Jun 16 2021 12:03:06 [admin] cli: [127.0.0.1] import aflex aflex-0203 use-mgmt-port sftp://user@10.65.25.165/tmp/aflex-02 Jun 16 2021 12:02:50 Error [SYSTEM]:ssh: connect to host 10.65.25.165 port 22: Connection timed outlost connection. Jun 16 2021 12:02:44 [admin] cli: [127.0.0.1] export aflex aflex-02 use-mgmt-port scp://user@10.65.25.165/tmp/aflex-0202.bak Jun 16 2021 12:02:28 Error [SYSTEM]:ssh: connect to host 10.65.25.165 port 22: Connection timed out. Jun 16 2021 12:02:23 [admin] cli: [127.0.0.1] import aflex aflex-0202 use-mgmt-port scp://user@10.65.25.165/tmp/aflex-02 **SCP/SFTP File Transfer via IPsec - Filename Failure**

AUDITABLE EVENT	SAMPLE RECORD
	Jun 16 2021 13:30:33 Error [SYSTEM]:sftp: No such file or Permission denied. Jun 16 2021 13:30:33 [admin] cli: [127.0.0.1] export aflex aflex-bad-filename use-mgmt-port sftp://user@10.65.25.165/tmp/aflex-bad-filename.bak Jun 16 2021 13:30:14 Error [SYSTEM]:user@10.65.25.165's password: Authenticated to 10.65.25.165 ([10.65.25.165]:22).Connected to 10.65.25.165.No entry for terminal type "dumb";using dumb terminal settings.No entry for terminal type "dumb";using dumb terminal settings.sftp> get /tmp/aflex-bad-filename /a10data/tmp/su.import.9986.0 File "/tmp/aflex-bad-filename" not found.sftp> . Jun 16 2021 13:30:14 [admin] cli: [127.0.0.1] import aflex aflex-bad-filename use-mgmt-port sftp://user@10.65.25.165/tmp/aflex-bad-filename Jun 16 2021 13:29:56 Error [SYSTEM]:user@10.65.25.165's password: Authenticated to 10.65.25.165 ([10.65.25.165]:22)./a10data/aflex/aflex-filename.arl: No such file or directoryKilled by signal 1.. Jun 16 2021 13:29:56 [admin] cli: [127.0.0.1] export aflex aflex-filename use-mgmt-port scp://user@10.65.25.165/tmp/aflex-filename.bak Jun 16 2021 13:29:36 Error [SYSTEM]:user@10.65.25.165's password: Authenticated to 10.65.25.165 ([10.65.25.165]:22).scp: /tmp/aflex-filename: No such file or directoryTransferred: sent 1040, received 3088 bytes, in 0.5 secondsBytes per second: sent 2260.8, received 6712.8. Jun 16 2021 13:29:35 [admin] cli: [127.0.0.1] import aflex aflex-filename use-mgmt-port scp://user@10.65.25.165/tmp/aflex-filename **SCP/SFTP File Transfer via IPsec - Remote Authentication Failure** Jun 16 2021 13:38:57 Error [SYSTEM]:sftp: password error. Jun 16 2021 13:38:54 [admin] cli: [127.0.0.1] export aflex aflex-02 use-mgmt-port sftp://user_name@10.65.25.165/tmp/aflex-user-name.bak Jun 16 2021 13:38:40 Error [SYSTEM]:sftp: password error. Jun 16 2021 13:38:38 [admin] cli: [127.0.0.1] import aflex aflex-user-name use-mgmt-port sftp://user_name@10.65.25.165/tmp/aflex-02 Jun 16 2021 13:38:20 Error [SYSTEM]:scp: password error. Jun 16 2021 13:38:18 [admin] cli: [127.0.0.1] export aflex aflex-02 use-mgmt-port scp://user_name@10.65.25.165/tmp/aflex-user-name.bak Jun 16 2021 13:37:59 Error [SYSTEM]:scp: password error. Jun 16 2021 13:37:57 [admin] cli: [127.0.0.1] import aflex aflex-user-name use-mgmt-port scp://user_name@10.65.25.165/tmp/aflex-02 **NTP via IPsec - Initiation** Jun 22 2021 19:43:19 Info [SYSTEM]:NTP server 10.65.25.166 is in sync with system Jun 22 2021 19:16:15 Info [SYSTEM]:NTP server 10.65.25.166 is in polling state Jun 22 2021 19:15:15 [admin] cli: [10.65.25.165:50546] ntp server 10.65.25.166 Sep 03 2021 18:26:24 [admin] web: [29:10.65.25.165:18474] payload section 1 {"hostname": {"host-servername": "10.65.25.166", "key": null, "action": "enable"}} Sep 03 2021 18:26:24 [admin] web: [29:10.65.25.165:18474] POST: /axapi/v3/ntp/server/hostname **NTP via IPsec - Termination** Jun 22 2021 19:50:35 [admin] cli: [10.65.25.165:50546] no ntp server 10.65.25.166

AUDITABLE EVENT	SAMPLE RECORD
	Sep 03 2021 18:23:35 [admin] web: [29:10.65.25.165:17918] DELETE: /axapi/v3/ntp/server/hostname/10.65.25.166 **NTP via IPsec - Failure** Apr 29 2021 18:36:37 Info [SYSTEM]:NTP server 10.65.25.165 is in polling state
Trusted Path (Initiation, Termination, Failure)	**IPsec Initiation, Termination, Failure** *See "Trusted Channel (Initiation, Termination, Failure)" for IPsec Peer initiated tunnel establishment and termination.* **CLI SSH Remote via IPsec - Login** May 25 2021 23:24:19 Notice [SYSTEM]:A cli session for user "niap-user1" from 10.65.25.166 has been opened. Session ID assigned is 14. May 25 2021 23:24:16 Info [SYSTEM]:Local authentication successful (user: niap-user1). **Web/GUI via IPsec - Login** May 25 2021 23:29:53 [niap-user1] web: [15:10.65.25.166:7966] RESP HTTP status 200 OK May 25 2021 23:29:53 [niap-user1] web: [15:10.65.25.166:7966] POST: /axapi/v3/auth May 25 2021 23:29:53 A web session[15] opened, username: niap-user1, remote host: 10.65.25.166 May 25 2021 23:29:53 Notice [SYSTEM]:A web session for user "niap-user1" from 10.65.25.166 has been opened. Session ID assigned is 15. May 25 2021 23:29:53 Info [SYSTEM]:Local authentication successful (user: niap-user1). **CLI SSH Remote via IPsec - Logoff** May 25 2021 23:24:27 Notice [SYSTEM]:Session ID 14 is now closed. May 25 2021 23:24:27 Session[14] closed May 25 2021 23:24:25 [niap-user1] cli: [10.65.25.166:58654] exit **Web/GUI via IPsec - Logoff** May 25 2021 23:30:04 Notice [SYSTEM]:Session ID 15 is now closed. May 25 2021 23:30:04 [niap-user1] web: [15:10.65.25.166:8104] RESP HTTP status 200 OK May 25 2021 23:30:04 Session[15] closed May 25 2021 23:30:04 [niap-user1] web: [15:10.65.25.166:8104] POST: /axapi/v3/logoff **CLI SSH Remote via IPsec - Login Error** May 27 2021 21:24:40 Error [SYSTEM]:The user, niap-user1, from the remote host, 10.65.25.166, failed in the cli authentication. May 27 2021 21:24:40 Info [SYSTEM]:Local authentication failed(user: niap-user1): Admin password error. May 25 2021 03:24:38 Error [SYSTEM]:The user, niap-userBAD1, from the remote host, 10.65.25.166, failed in the cli authentication. May 25 2021 03:24:38 Info [SYSTEM]:Local authentication failed(user: niap-userBAD1): Specified admin does not exist.. **Web/GUI via IPsec - Login Error** May 25 2021 04:18:09 Error [SYSTEM]:The user, niap-user1, from the remote host, 10.65.25.166, failed in the web authentication.

AUDITABLE EVENT	SAMPLE RECORD
	May 25 2021 04:18:09 Info [SYSTEM]:Local authentication failed(user: niap-user1): Admin password error. May 25 2021 04:14:15 Error [SYSTEM]:The user, niapiuserBAD, from the remote host, 10.65.25.166, failed in the web authentication. May 25 2021 04:14:15 Info [SYSTEM]:Local authentication failed(user: niapiuserBAD): Specified admin does not exist..

Table 5: Sample Audit Entries

REVISION HISTORY

REVISION	DATE	AUTHOR	DESCRIPTION
1.0	January 25, 2023	A10 Cert Team	Initial publication.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide.

For more information, visit: a10networks.com and @a10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact