

# *Preparation and Operation of Common Criteria Evaluated OmniSwitch Products (NDcPP)*

AOS Release 8.9.R11  
July 2023

## Table of Contents

1	Using this Guide.....	4
1.1	Hardware and Software Supported.....	4
1.2	Assumptions for Secure OmniSwitch Operation.....	5
1.3	Definitions and Acronyms.....	6
1.4	Flaw Reporting .....	7
2	Secure Delivery and Installation of the TOE.....	9
2.1	Secure Acceptance of TOE .....	9
2.2	Verify the TOE.....	10
2.3	Downloading Applicable Documentation and Software .....	10
2.3.1	Support contract and login credentials .....	11
2.3.2	Download AOS 8.9 R11 .....	13
2.4	Operating Modes of TOE .....	14
2.5	Configure the TOE for the Common Criteria Evaluated Configuration.....	15
2.5.1	Enable CC Mode.....	15
2.5.2	Excluded Functionalities in Common Criteria Mode .....	16
2.5.3	CLI Commands shall or must not be used in Common Criteria Mode.....	17
3	OmniSwitch Guidance related to CC SFRs.....	18
3.1	Security Audit (FAU) .....	18
3.1.1	Security Audit Data Generation (FAU_GEN) .....	18
3.1.2	Security Audit Event Storage (Extended – FAU_STG_EXT) .....	32
3.1.3	Protected Audit Trail Storage (FAU_STG.1) .....	33
3.2	Cryptographic Support (FCS_CKM, FCS_COP).....	33
3.2.1	Cryptographic Key Generation (FCS_CKM.1).....	33
3.2.2	Cryptographic Key Establishment (FCS_CKM.2) .....	34
3.2.3	Cryptographic Key Destruction (FCS_CKM.4) .....	35
3.2.4	Cryptographic Operation (FCS_COP) .....	35
3.2.5	Extended: Random bit generation (FCS_RBG_EXT.1) .....	37
3.2.6	SSH Server (FCS_SSHS_EXT.1).....	37
3.2.7	TLS Client Protocol (FCS_TLSC_EXT.2) and (FCS_TLSC_EXT.1.1) .....	40
3.3	Identification and Authentication (FIA).....	41
3.3.1	Authentication Failure Management (FIA_AFL.1) .....	41
3.3.2	Password Management (Extended – FIA_PMG_EXT) .....	42
3.3.3	User Identification and Authentication (Extended – FIA_UIA_EXT) .....	43
3.3.4	User authentication (Extended – FIA_UAU_EXT) .....	43
3.3.5	Protected authentication feedback (FIA_UAU.7) .....	43
3.3.6	Authentication using X.509 Certificates (Extended – FIA_X509_EXT) .....	44
3.4	Security Management (FMT).....	48
3.4.1	Management of functions in TSF (FMT_MOF).....	49
3.4.2	Management of TSF Data (FMT_MTD) .....	49
3.4.3	Specification of management functions (FMT_SMF) .....	50
3.4.4	Security management roles (FMT_SMR) .....	50
3.5	Protection of the TSF (FPT) .....	51
3.5.1	Protection of TSF Data (Extended – FPT_SKP_EXT) .....	51
3.5.2	Protection of Administrator Passwords (Extended – FPT_APW_EXT) .....	51
3.5.3	TSF testing (Extended – FPT_TST_EXT) .....	51

3.5.4	Trusted Update (FPT_TUD_EXT) .....	52
3.5.5	Time stamps (FPT_STM_EXT) .....	54
3.6	TOE Access (FTA) .....	55
3.6.1	TSF-initiated Session Locking and Termination (Extended – FTA_SSL_EXT, FTA_SSL).....	55
3.6.2	TOE access banners (FTA_TAB).....	55
3.7	Trusted path/channels (FTP) .....	55
3.7.1	Trusted path (FTP_TRP.1) .....	55
3.7.2	Trusted Channel (FTP_ITC.1) .....	56

**List of Tables**

Table 1 - Security Objective of Operational Environments.....	6
Table 2 - Definitions .....	6
Table 3 - Acronyms.....	7
Table 5 - Excluded Functionalities in Common Criteria Mode .....	17
Table 6 - Functionality not to be used in Common Criteria Mode.....	17
Table 7 - CLI Commands shall or must not to be used in Common Criteria Mode.....	17
Table 8 - Sample Audit Records Table .....	31
Table 9 - Supported Crypto Algorithms.....	37

## 1 Using this Guide

All OmniSwitch® products are accompanied by a documentation suite designed to guide users to correctly prepare and operate an OmniSwitch. This guide supplements the standard OmniSwitch product family documentation, providing the additional information necessary for users to prepare and operate an OmniSwitch product as evaluated by the Common Criteria evaluation team.

This document is written for Network Administrators configuring the TOE with the AOS software. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking and the protocols that the devices use in your network. This document assumes that you are a trusted individual, and that you are trained to use AOS software. It is also assumed that you are aware of various operating systems on which you are running your network and understand your network topology.

This document describes the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It highlights the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document covers all the security functional requirements specified in the Security Target (ST). It does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, such as information flow polices and access control, which should be set according to your organizational security policies.

This document is a road map for identifying appropriate locations within AOS documentation to get the specific details for configuring and maintaining OmniSwitch operations. It is recommended that you read all the instructions in this document and any references, before performing steps outlined and entering commands.

In this document, *OmniSwitch product family* refers to all valid configurations of each TOE: OS6360/6465/6465T/6560/6860E/6860N/6865/6900/9900 (Release 8.9.6.R11 Common Criteria Certified) and all associated OmniSwitch guidance, including this document and the specific document versions listed in Table 4.

### 1.1 Hardware and Software Supported

The Hardware and Software listed below is compliant with the Common Criteria Evaluation. Using hardware or software not specified invalidates the secure configuration.

- OmniSwitch 6360
- OmniSwitch 6465
- OmniSwitch 6465T
- OmniSwitch 6560
- OmniSwitch 6860E
- OmniSwitch 6860N
- OmniSwitch 6865
- OmniSwitch 6900
- OmniSwitch 9900
- **Software:** 8.9.6.R11 Common Criteria Certified (This is the CC build for 8.9 R11)

## 1.2 Assumptions for Secure OmniSwitch Operation

Section 3.2.2 of the OmniSwitch Security Target document describes the assumptions for the secure operation of the CC evaluated OmniSwitch. Trust in the OmniSwitch administrator is a critical factor for secure operation. Organizational policies must assure that the OmniSwitch administrator:

Operational Environments Security Objective	Description of the Security Objective	Administrators Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The OmniSwitch must be installed to a physically secured location that allows physical access to Administrators / Authorized personnel only.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	The administrator must ensure there is no general-purpose computing capabilities (e.g. compilers or user applications) running on the TOE, other than the software and services necessary only for the operation, administration and support of the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.	The administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE. The administrator must monitor the revocation status of all X.509 certificates in the TOE's trust store and remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must perform regular firmware/software updates to ensure that the security functionality of the TOE is maintained and is not affected by any vulnerability.

OE.ADMIN_CREDENTIALS_SECURITY	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must securely store the private keys and passwords appropriately and restrict access to credentials that are used to access the TOE.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	When the equipment is discarded or removed from the operational environment, the administrator must ensure that there is no unauthorized access possible for sensitive information like cryptographic keys, passwords etc. stored on the networking equipment.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	The administrator is responsible for configuring the TOE with traffic filtering policies as per the requirements. The pass through traffic is protected by the traffic filtering policy.

**Table 1 - Security Objective of Operational Environments**

### 1.3 Definitions and Acronyms

Term	Definition
OmniSwitch	The OmniSwitch product family, inclusive of the following products OmniSwitch 6360, 6465, 6560, 6860, 6865, 6900, 9900, (AOS 8.9.6.R11)
Syslog	Standard computer (POSIX) abstraction for log file management

**Table 2 - Definitions**

Term	Definition
AAA	Authentication, Authorization and Accounting, an OmniSwitch component
ACL	Access Control List
ASA	Authenticated Switch Access, refers to Administration domain authentication
AVLAN	Authenticated VLAN: deprecated functionality, replaced by CaptivePortal
CA	Certification Authority
CC	Common Criteria
CCE	Common Criteria Evaluation
CSR	Certificate Signing Request
CRL	Certificate Revocation List
CLI	Command line interface, used for local or remote administration

Term	Definition
CMM	Chassis Management Module. The TOE processing module which runs most TOE processes and control TOE functions.
IPSec	Internet Protocol Security, a standard for layer 3 encryption and message integrity
IPSec SA	IPSec Security Association – a configuration of IPSec parameters specific to an entity
MAC	1) Media Access Control, used in the context of a physical address; 2) Message authentication code, used in the context of message integrity
OSCP	Online Certificate Status Protocol
OS6360	Alcatel-Lucent Enterprise OmniSwitch 6360 Series with AOS Release 8.9 R11
OS6465	Alcatel-Lucent Enterprise OmniSwitch 6465 Series with AOS Release 8.9 R11
OS6560	Alcatel-Lucent Enterprise OmniSwitch 6560 Series with AOS Release 8.9 R11
OS6900	Alcatel-Lucent Enterprise OmniSwitch 6900 Series with AOS Release 8.9 R11
OS6860	Alcatel-Lucent Enterprise OmniSwitch 6860 Series with AOS Release 8.9 R11
OS6865	Alcatel-Lucent Enterprise OmniSwitch 6865 Series with AOS Release 8.9 R11
OS9900	Alcatel-Lucent Enterprise OmniSwitch 9900 with AOS Release 8.9 R11
SCP	Secure Copy Protocol
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation: The OmniSwitch, configured for CC evaluation conditions, along with all associated documentation
TSF	TOE Security Function – the set of all CC related security functionality implemented by the OmniSwitch TOE
VLAN	Virtual Local Area Network

**Table 3 - Acronyms**

## 1.4 Flaw Reporting

Product problems, including all security flaws, may be reported using the following contact information:

- Address: ALE USA Inc. 2000 Corporate Center Drive Thousand Oaks, California 91320 U.S.A.
- Telephone:
  - Toll Free Number for USA: 1-800-995-2696
  - International Toll Free Number: +800-00200100
  - FAX: 1-818-880-3505
  - Europe Union: +800 00200100 (Toll Free) or +1-650-385-2193
- Email:
  - First level support: [ebg\\_global\\_supportcenter@al-enterprise.com](mailto:ebg_global_supportcenter@al-enterprise.com)
  - End-user customer vulnerability problem reporting: [psirt@al-enterprise.com](mailto:psirt@al-enterprise.com)
- Websites:
  - Customers with service agreements are directed to use ALE’s support page at: <https://myportal.al-enterprise.com/s>

- Product Security Incident Response Team  
<https://www.al-enterprise.com/en/support/security-advisories>

Using the CLI, the **show system** command provides critical product identification and support information as shown below:

```
-> show system
```

```
System:
```

```
Description: Alcatel-Lucent Enterprise OS6860E-P24Z8 8.9.6.R11 Development, July 24, 2023.,
```

```
Object ID: 1.3.6.1.4.1.6486.801.1.1.2.1.11.1.10,
```

```
Up Time: 0 days 0 hours 3 minutes and 40 seconds,
```

```
Contact: Alcatel-Lucent Enterprise, https://www.al-enterprise.com,
```

```
Name: OS6860,
```

```
Location: Unknown,
```

```
Services: 78,
```

```
Date & Time: TUE JUL 25 2023 02:05:36 (UTC)
```

```
Flash Space:
```

```
Primary CMM:
```

```
Available (bytes): 563986432,
```

```
Comments : None
```



## 2 Secure Delivery and Installation of the TOE

OmniSwitch products are built in small lots to optimize stock on hand versus delivery time. Following manufacture, OmniSwitch products are warehoused in depot facilities until order fulfillment and shipment to the customer.

Alcatel-Lucent Enterprise orders for the Common Criteria evaluated TOE are delivered with the AOS loaded, to meet Common Criteria requirements for part numbers that will not change. The TOE is delivered with software loaded, but the software can be an old version. The user shall download the CC evaluated version from the [ALE Support website](#).

This document describes secure acceptance, installation and preparation of the delivered TOE in accordance with the *Security Target* [ST]. The Administrator must verify the TOE model number and refer to the appropriate user documentation to install the hardware, upload, and upgrade specific software for the TOE.

The *Hardware Guide* appropriate to the specific TOE, obtained as described in the next section, addresses unpacking the TOE and provides a list of expected package contents.

The OmniSwitch is typically located in a physically secure environment, accessible only by authorized personnel.

### 2.1 Secure Acceptance of TOE

The customer must perform the following checks upon receipt of an appliance to verify the integrity of the platform.

1. ALE only uses reputable couriers for shipping. Factory to depot shipping is only done with UPS, FedEx, Expeditors, Panalpina, and Kuehne+Nagel. From hub to customer the same three couriers are used for countries they have a presence. For the few countries which they do not serve, ALE uses reputable local couriers.
2. Ensure that the shipping label exactly identifies the correct customer name and address as well as the TOE.
3. Ensure that the TOE is packaged in ESD bags and sealed with an ESD warning label.
4. Inspect whether the TOE is boxed and has factory sealing tape with “Alcatel-Lucent Enterprise”

and the logo



. This tape seal would be broken or missing if the box was opened during transit.

If the customer identifies a problem during the inspection, he or she must immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

## 2.2 Verify the TOE

The TOE is shipped with the software installed, and as such, physical labeling of software distributions does not apply. However, the software version can be confirmed by the user by entering the CLI command *show microcode loaded*.

The customer can verify the exact product release for comparison to the evaluated CC Version by confirming:

- The hardware model as given on the rating label or front panel. The location of the rating label and the model identifier on the front panel are product dependent.
- The software version, using *show microcode loaded* CLI command.
- Document part and revision numbers are printed on the title page, with part number in the header of every page.

## 2.3 Downloading Applicable Documentation and Software

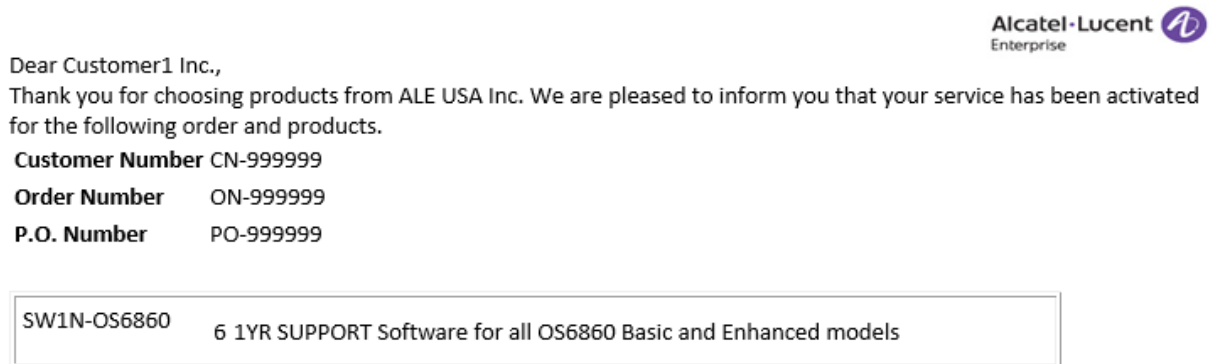
All TOE software and documentation are downloaded from the Alcatel-Lucent Enterprise Service and Support website. The Service and Support website enables download of all applicable documentation, the Common Criteria validated AOS release and any optional purchased software or upgrades. The AOS 8.9.6.R11 Common Criteria Certified is the CC evaluated version for OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900, OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 9900.

### 2.3.1 Support contract and login credentials

To get the common criteria version the user must have a support contract in place.

The steps for setting up a support account are as follows:

1. When you order for **OmniSwitch**, you will get a welcome email with support address as shown below.



The image shows a sample customer support email. In the top right corner, there is the Alcatel-Lucent Enterprise logo. The main body of the email starts with "Dear Customer1 Inc.," followed by a thank you message: "Thank you for choosing products from ALE USA Inc. We are pleased to inform you that your service has been activated for the following order and products." Below this, there are three lines of order details: "Customer Number CN-999999", "Order Number ON-999999", and "P.O. Number PO-999999". A table with a border contains the following information: "SW1N-OS6860" in the first column and "6 1YR SUPPORT Software for all OS6860 Basic and Enhanced models" in the second column. At the bottom of the email, there is a paragraph of text providing a website link (<https://www.al-enterprise.com/en/support>), a toll-free phone number (1-800-995-2696), an email address ([ebg\\_global\\_supportcenter@al-enterprise.com](mailto:ebg_global_supportcenter@al-enterprise.com)), and another website link (<https://www.al-enterprise.com/en>).

Please refer to the following web site for any questions you may have.

<https://www.al-enterprise.com/en/support>

To obtain technical assistance, please contact the ALE USA Inc. Technical Assistance Center at: 1-800-995-2696(Toll free)

Email: [ebg\\_global\\_supportcenter@al-enterprise.com](mailto:ebg_global_supportcenter@al-enterprise.com)

For additional information about ALE USA Inc. products and services, please contact your ALE USA Inc. Sales Representative or visit our Web site at <https://www.al-enterprise.com/en>

#### Figure 2-1 – Sample Customer Support email

2. To create a new support account, go to the support site <https://myportal.al-enterprise.com/s>
3. Click on **Create new account. User Management Portal** page is displayed.
4. Follow the **User Registration** process displayed in the screen.

- When the user account is created, you will get an email with user credentials and password from ALE Support team.

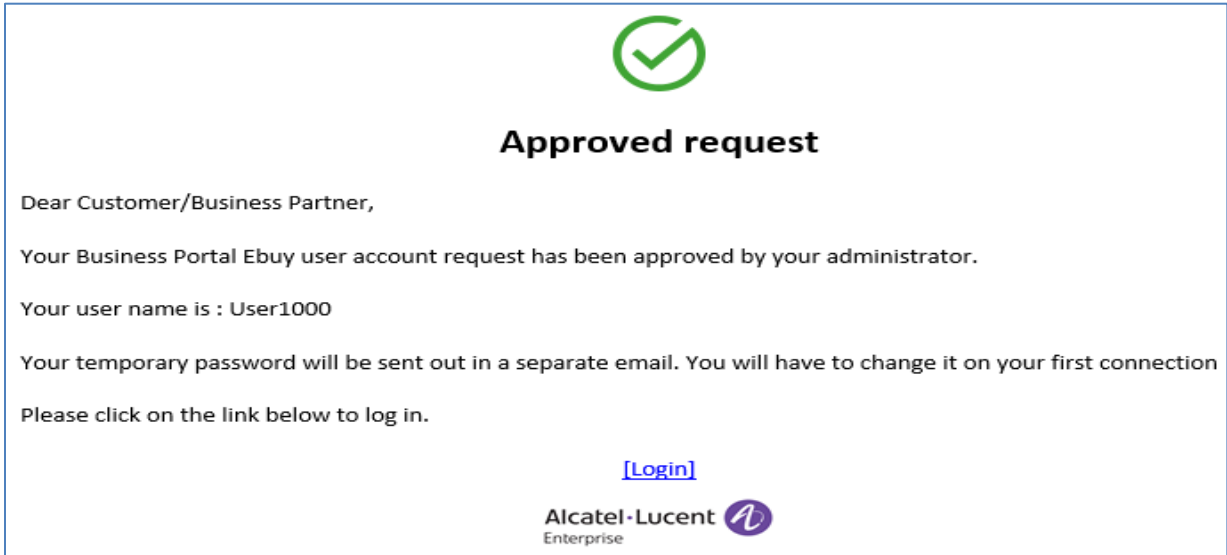


Figure 2-2 – Approved Account Request

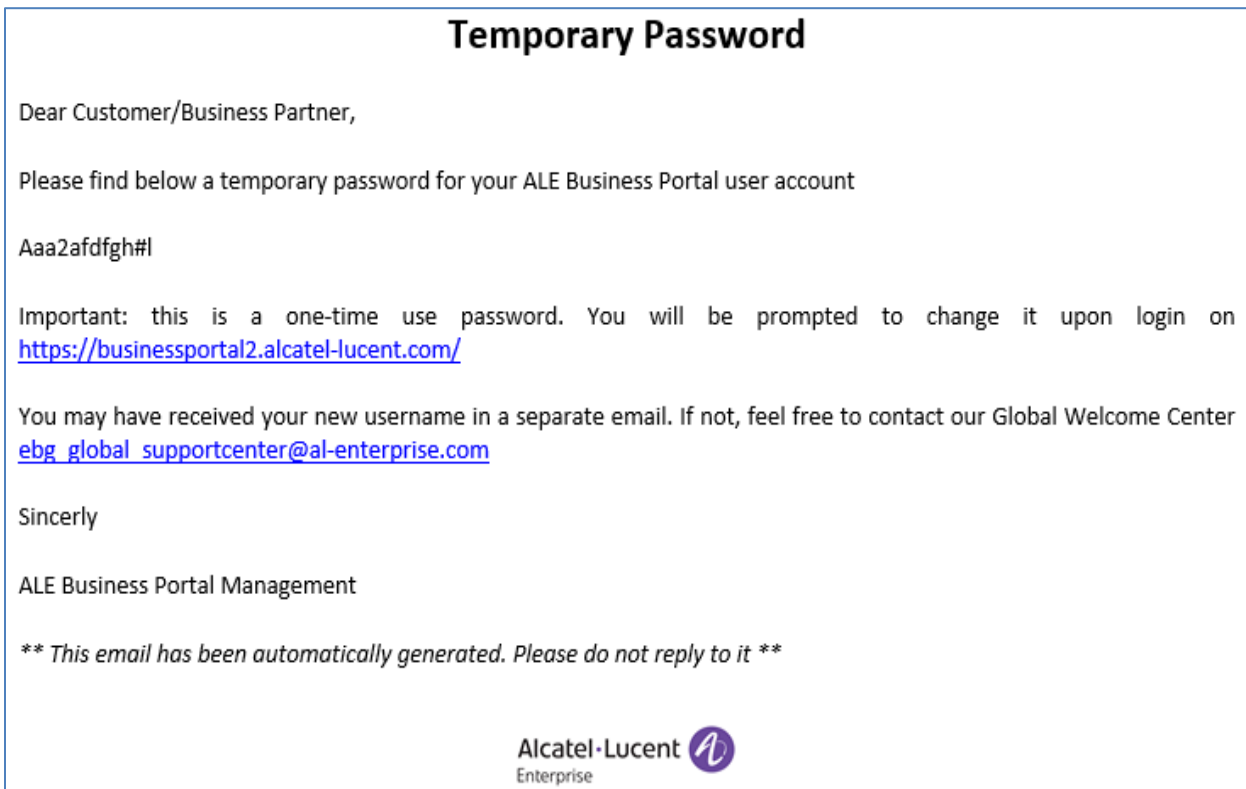


Figure 2-3 – Temporary Password Mail

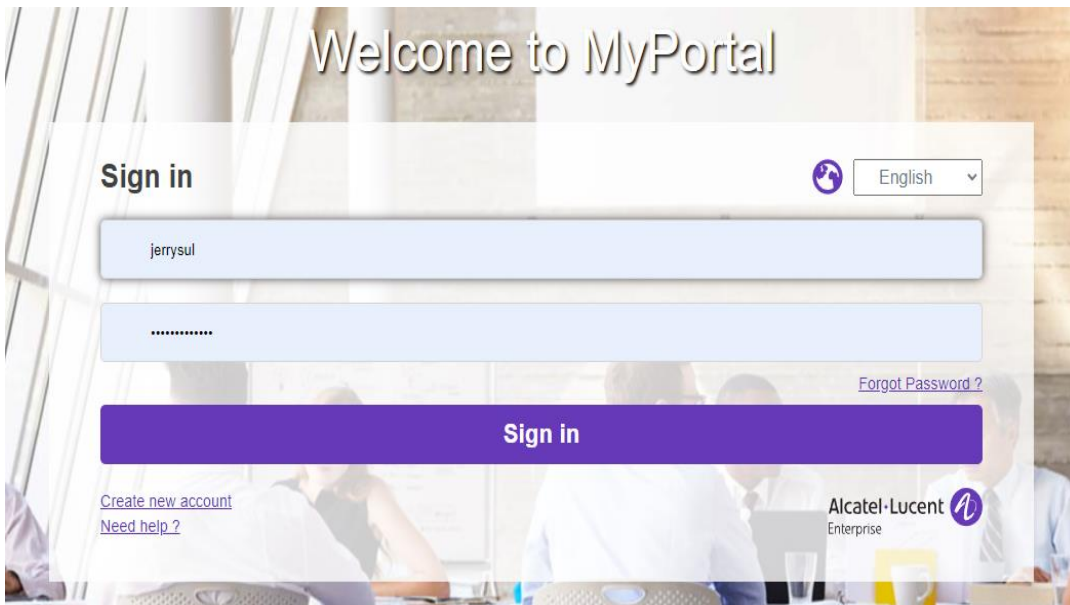
- You have successfully created a support user account.

If any clarification is required on creating a support account, contact Alcatel-Lucent Enterprise through the contacts mentioned in [Flaw Reporting](#).

### 2.3.2 Download AOS 8.9 R11

After logging into the ALE support website, perform the following steps to download the **AOS 8.9.R11 Common Criteria Certified** image. Instructions are provided in a later section of this document to install AOS and to perform all configurations.

1. Go to support website <https://myportal.al-enterprise.com/s> Log in with your username/password.



**Figure 2-4 - Service and Support Login page**

2. Upon successful login, the Support page is shown. Click on **Support -> Software Download->Network Products->Switches Select a Product.**

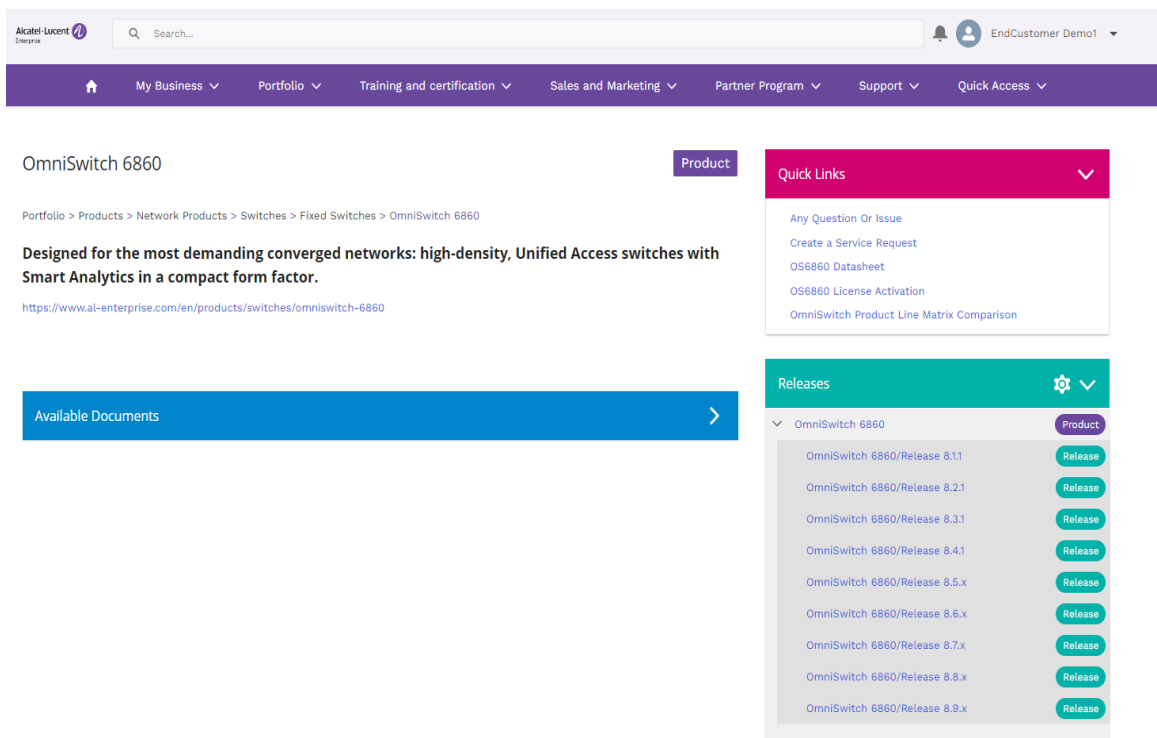


Figure 2-5 - Product Page, Product Selection

- Expand the **Software** tab and select the appropriate file(s). Add to the cart and download the files.

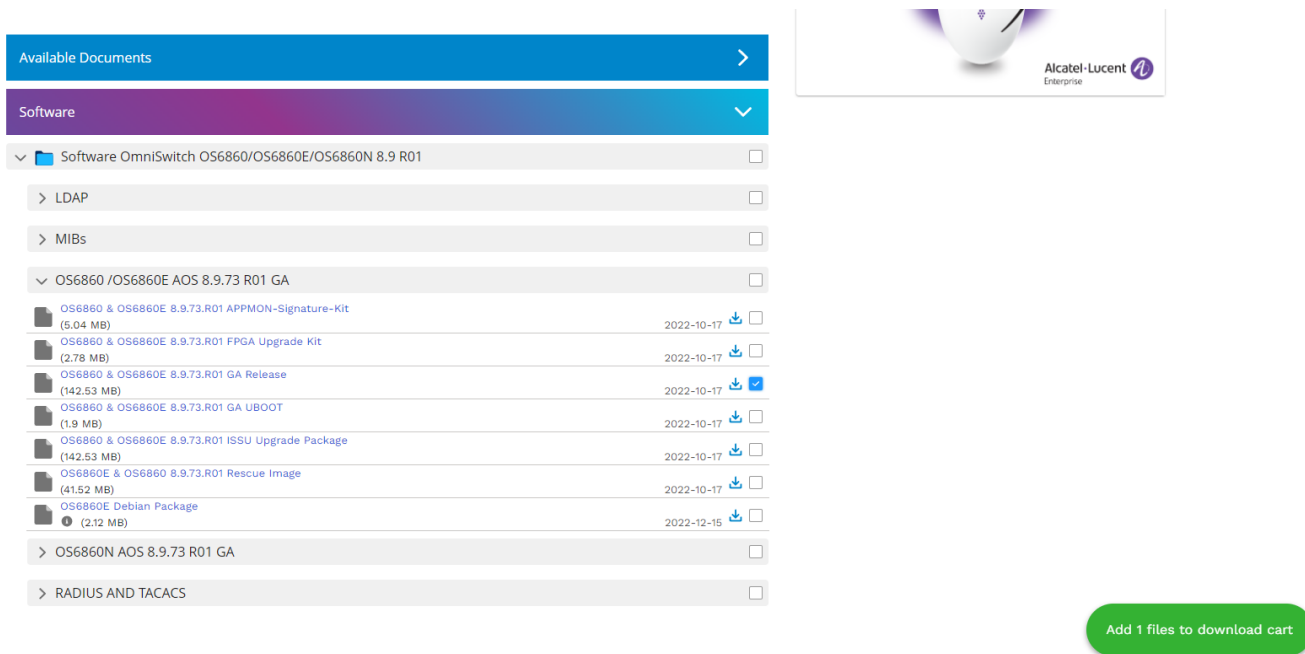


Figure 2-6 – Example, product specific download page

## 2.4 Operating Modes of TOE

AOS switch has several modes of operation; OmniSwitch can be operated in the following modes:

- **Booting** - While booting, the switch drops all network traffic until the switch image and configuration is loaded. This mode of operation automatically progresses into the Normal mode of operation. During the booting process, a user may press any key on a console connection to enter the Rescue mode of operation. If the Switch does not find a valid operating system image it will enter Rescue mode by default therefore protecting the switch from booting into an insecure state.
- **Normal** - The AOS switch image and configuration is loaded and the switch is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all switch based security functions are operating. Once the switch is in normal operating mode and fully configured, there is little interaction between the switch and the administrator. However, the configuration of the switch can have a detrimental effect on security; therefore, adherence to the guidelines in this document should be followed. Incorrect configuration of the switch could result in the unprotected network having access to the internal/protected network.
- **Rescue** - This mode of operation is a maintenance, debugging and disaster recovery mode. While the switch is in this mode, no network traffic is routed between the network interfaces. In this state, the switch may be configured to upload a new boot image from a USB flash drive and run various debugging commands.

**Note:** If NVRAM is empty and a *reload* is done, AOS will try to boot automatically from an image that is in the */flash/certified* directory. Make sure the valid AOS image is loaded in the */flash/certified* directory in flash.

It should be noted that while no administrator password is required to enter Rescue mode, physical access to the switch is required, therefore the switch should be stored in a physically secure location to avoid unauthorized access which may lead to the switch being placed in an insecure state.

## 2.5 Configure the TOE for the Common Criteria Evaluated Configuration

This section describes guidance for enabling Common Criteria mode for features within the scope of the CC Evaluation. Other Alcatel-Lucent Enterprise documents corresponding to features outside of CC scope are not relevant to the CC Evaluation.

### 2.5.1 Enable CC Mode

For Common Criteria, the OmniSwitch runs in the Common Criteria mode under which it will have all the Common Criteria functions enabled. Common Criteria can be enabled/disabled via the CLI command *aaa common-criteria admin-state*. The configuration is applied only after reloading.

Use the *aaa common-criteria admin-state enable* command to enable the Common Criteria mode.

```
-> aaa common-criteria admin-state enable
WARNING: Common Criteria configuration is applied only after reload.

-> show aaa common-criteria config
Admin State: Enabled,
Operational State: Disabled
-> write memory
```

```
-> reload from working no rollback-timeout
Confirm Activate (Y/N) : Y
```

After the switch boot up in common criteria mode, during log on to the switch the user will be prompted to change the password if the password doesn't satisfy the common criteria password policy. This is applicable for the default "admin" user as well created during initial installation of the TOE.

It should be noted that the default "admin" user is considered the privileged administrator and has full administrative privileges for all commands on the TOE. Hence, the default "admin" user must be used only to perform installation and initial configuration of the TOE. The general switch administration or management must be performed by the users with appropriate administrative privileges (created by the "admin" user), but not by the default "admin" user.

The Common Criteria mode will only allow console and SSH access to the OmniSwitch.

CCE requires each administrative user to be successfully identified and authenticated before allowing any other TSF mediated actions on behalf of that administrative user.

In Common Criteria mode, TOE can be accessed locally through serial console and remotely through SSH. SSH communication supports both password based and public-key based authentication.

During local/remote access, authentication is done through local switch database.

In Common Criteria mode the cryptographic algorithms for TLS and SSH are limited to only evaluated encryption algorithms, key exchanges, public key algorithms and data integrity MAC algorithms.

## 2.5.2 Excluded Functionalities in Common Criteria Mode

The following features interfere with the TOE security functionality claims and are disabled by default in the common criteria evaluated configuration:

Service or Protocol	Description
FTP access to the switch	FTP traffic is not secured so the FTP service is disabled for security reasons in the CC evaluated configuration.
Telnet access to the switch	Telnet traffic is not secured so the Telnet service is disabled for security reasons in the CC evaluated configuration. Telnet passes authentication credentials in clear text. This feature is disabled by default and cannot be configured for use in the evaluated configuration. SSHv2 secured connection is to be used instead of telnet.
Webview access to the switch	This web-based interface used for switch management is disabled for security reasons in the CC evaluated configuration.
Hypertext Transfer Protocol (HTTP)	HTTP and HTTPs is disabled in the CC evaluated configuration. HTTP Server for web user interface management sends authentication data in the clear and does not enforce the required privilege levels. This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.
RADIUS, LDAP and SNMP	RADIUS, LDAP and SNMP are not supported in CC evaluated configuration.



**Table 4 - Excluded Functionalities in Common Criteria Mode**

The following features interfere with the TOE security functionality claims and must not be configured for use in the evaluated configuration:

Service or Protocol	Description
Captive Portal	This feature allows web-based authentication of end-users. This feature is disabled by default and should not be configured for use in the CC evaluated configuration.
Terminal Access Controller Access-Control System Plus (TACACS+)	Authentication using an external TACACS+ server is not allowed in the CC evaluated configuration. This feature is disabled by default and should not be configured for use in the CC evaluated configuration.
Port Mobility Rules	Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic.  This feature is superseded by User Network Profiles and has been kept in the product for backwards compatibility reasons.  Port Mobility Rules is disabled by default and should not be configured for use in the CC evaluated configuration.
Cryptographic algorithms	The MD5 algorithm must not be used. MD5 algorithms should not be configured for use in the CC evaluated configuration.
NTP	The use of NTP to synchronize the time with an external time source must be disabled in the CC evaluated configuration. NTP is disabled by default and should not be configured for use in the CC evaluated configuration.

**Table 5 - Functionality not to be used in Common Criteria Mode**

### 2.5.3 CLI Commands shall or must not be used in Common Criteria Mode

The following table describes the CLI commands must not be used on the TOE, while in Common Criteria mode.

CLI Command	Description
<code>-&gt;swlog disable</code>	This command will disable switch logging due to which history of various switch activities cannot be viewed.
<code>-&gt;swlog appid all subapp all level &lt;logging level below info&gt;</code>	Audit events are logged in swlog with logging level as 'INFO'. If the logging level is configured to be below INFO, then audit events will not be captured in swlog.
<code>-&gt; ssh admin-state disable</code>	This command will administratively disable secure shell in switch. If disabled remote access to OmniSwitch will not be possible.
<code>-&gt; ip service ssh admin-state disable</code>	This command will disable SSH service in the switch thereby disabling remote access to OmniSwitch.

**Table 6 - CLI Commands shall or must not to be used in Common Criteria Mode**

### 3 OmniSwitch Guidance related to CC SFRs

This section reviews OmniSwitch features related to the SFR references and provides references to the applicable preparation and operational guidance documentation.

#### 3.1 Security Audit (FAU)

The OmniSwitch product family Switch Logging features provide the functionality necessary to meet CC Security Audit requirements.

The FPT\_STM\_EXT.1 requirement for reliable time stamping is met by the OmniSwitch internal system clock. Setting system date and time is covered in section below (3.5.5). No further guidance documentation is applicable.

##### 3.1.1 Security Audit Data Generation (FAU\_GEN)

AOS 8.x platforms maintain logs in multiple locations: Local storage of generated audit records and simultaneous offload of those events to the External Syslog Server. For the most complete view of audited events, across all devices and to view the auditable events as defined in Security Target, administrators should review these Audit Records on a regular basis.

Using the AOS Command Line Interface (CLI) provisioned, administrators can review audited events. The information provided in the audit records includes date and time of the event, subject identity (as applicable), outcome of the event and additional information relevant to respective events. To review the locally stored audit records, provide the command "*show log swlog*" through CLI.

In detail, any swlog message contains date, time-stamp, device identifier, process, facility, log level and message in specified order. Following information defines the basic information and format that is incorporated in an audit/log record.

- Element - Description or a log message briefing an event with prefix "EVENT-AUDIT".
- Date/ Timestamp - Date and time of the message or event. This information appears as the first field in the log record and the format date & time can be depicted as "YYYY MMM DD" followed by "HH:MM: SS" respectively.
- Device identifier - This field refers to the hostname configured on the device. In a centralized logging infrastructure; the significance of this field is to identify the source from which respective audit records were generated
- Process – This field is significant in determining the process from which the record is generated.
- Facility - Facility refers to the application or module in which the event has occurred resulting in audit record generation (for example, AAA, SES, and so on). The supported lists of facilities are as applicable.
- Log Level - This field is significant in determining severity of the message. The list of supported severity levels is WARNING, OFF, INFO, ERROR, DEBUG3, DEBUG2, DEBUG1, ALERT and ALARM.

The individual AOS modules have SWLog APIs for each of these events.

To distinguish audit logs with other swlog, the audit swlog is appended with special string "EVENT-AUDIT" at the beginning of each swlog. Use the CLI command *show log swlog | grep EVENT-AUDIT* to display the audit logs. The audit is logged only when Common Criteria is enabled and the same logs are transferred to the external syslog server like any other swlog (if external logging is enabled).

```
-> show log swlog | grep EVENT-AUDIT
```

Below is a sample of audit records for various required auditable events; note that these records are samples and not meant as an exact record for event(s). In addition, for rekeying scenarios producing an audit record would require extensive data transfers, time and connection stability; therefore, snippets of source code are provided to illustrate what would be displayed in an audit record. TSF self-test completion and success be indicated by reaching a log-in prompt following a boot-up. If TSF self-test did not complete successfully, a failure message would be displayed to indicate an error occurred.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FAU_GEN.1	Starting and stopping of audit functions	None	<p>Start or stop of audit function is controlled by default based on the operating mode of device and those events are recorded as:</p> <pre>2016 Sep 16 13:22:44 OS6860 swlogd: ChassisSupervisor CS Main info(5) EVENT-AUDIT: Logging Started!</pre> <pre>2017 Jan 1 17:23:50 OS6860 swlogd: ChassisSupervisor bootMgr info(5) EVENT-AUDIT: Logging Stopped</pre> <p><b>Administrative action:</b></p> <pre>2016 Nov 4 20:18:48 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: &lt;Command Text&gt;, result: SUCCESS</pre>
	Administrative login and logout	None	See FIA_UIA_EXT.1 for sample records
	Security related configuration changes & Resetting passwords	None	See FMT_MTD.1 /CoreData for sample records
	Generating or import of, changing, or deleting of Cryptographic keys	None	See FMT_MTD.1 /CryptoKeys for sample records
FAU_GEN.2	Identity of the user that caused the event	None	See FIA_UIA_EXT.1 for sample records

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FAU_STG_EXT.3/Loc Space	Warning at 90% utilization of local storage space. Overwriting previous audit records when local storage space is full.	None	<p><b>Local Storage:</b></p> <p>Utilization and management of local storage space are recorded as:</p> <pre>2017 Jan 2 19:48:20 OS6860 swlogd: SSAPP main info(5) EVENT-AUDIT: Switch log file reached 90%, Backup files before overwritten  2017 Jan 2 20:52:20 OS6860 EVENT- AUDIT: Switch log file reached 100%, overwritten !!!  2016 Sep 20 13:34:06 OS6860 ssapp: EVENT-AUDIT: Swlog cleared</pre>
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Provided user identity, origin of the attempt (only for SSHv2 connections)	<p><b>For Console:</b></p> <pre>2016 Sep 16 14:23:28 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin, failure, CONSOLE  2016 Sep 16 13:26:15 OS6860 swlogd: SES AAA info(5) EVENT-AUDIT Login by admin through Console Success [in LoginAaaSession::handleLoginResult()]  2016 Sep 16 13:26:53 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin, login, CONSOLE</pre> <p><b>User Auth:</b></p> <p><b>Sample</b></p> <pre>2016 Oct 17 16:57:37 OS6860 swlogd: SES AAA info(5) EVENT-AUDIT Login by cctesterfrom 10.145.59.99 through SSH Failed [in LoginAaaSession::handleLoginResult()]  2016 Nov 4 20:19:31 OS6860 sshd[25866]: EVENT-AUDIT: event euid 0 user aravind event 2 (AUTH_SUCCESS)</pre> <p><b>Administrator action:</b></p> <p>Command to check common-criteria configuration is recorded as</p>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>2016 Sep 16 13:27:52 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: <b>show aaa common-criteria config</b>, result: SUCCESS</p> <p><b>For SSH:</b></p> <p>2016 Sep 16 16:49:54 OS6860 swlogd: SES AAA info(5) EVENT-AUDIT Login by adminfrom 10.145.59.99 through SSH Failed [in LoginAaaSession::handleLoginResult()]</p> <p>2016 Sep 16 16:49:54 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin, failure, SSH</p> <p>2016 Sep 16 16:50:01 OS6860 swlogd: SES AAA info(5) EVENT-AUDIT Login by admin from 10.145.59.99 through SSH Success [in LoginAaaSession::handleLoginResult()]</p> <p>2023 Jan 11 03:44:44.993 os6360 sshd[PID#] EVENT-AUDIT: event euid 0 user &lt;username&gt; event 6 (AUTH_FAIL_PUBKEY)</p> <p>2016 Sep 16 16:50:01 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin, login, SSH</p> <p>2016 Sep 16 16:50:26 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin, logout, SSH</p> <p><b>Administrator action:</b> Command to check AAA configurations will be recorded as</p>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			2016 Sep 16 16:50:07 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (10.145.59.99), cmd: <b>show configuration snapshot aaa</b> , result: SUCCESS
FIA_UAU_EXT.2	All use of the identification and authentication mechanism	Origin of the attempt (only for SSHv2 connections).	See FIA_UIA_EXT.1 for sample records
FIA_X509_EXT.1/REV	Unsuccessful attempt to validate a certificate	Reason for failure	See FTP_TRP.1 for sample records
FMT_MOF.1/Manual Update	Any attempt to initiate a manual update	None	See FPT_TUD_EXT.1 for sample records
FMT_MTD.1 /CoreData	All management activities of TSF data	None	<p><b>Management Actions:</b> Management activities include changing into CC mode, creating user account, changing passwords and privileges, modifying log file size, file transfers, etc., are as recorded below:</p> <pre>2016 Sep 16 13:18:35 OS6860 swlogd: AAA Switch-Access info(5) EVENT- AUDIT: Common Criteria configuration: Enabled</pre> <pre>2016 Sep 16 13:26:52 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT password change Success</pre> <pre>2016 Sep 16 13:26:53 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT Password for User admin modified by admin.</pre>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>2016 Sep 16 17:39:00 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT User 8x_CCE_Tester_1 created by admin</p> <p>2016 Sep 16 17:39:00 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT User 8x_CCE_Tester_1 Privileges modified</p> <p>2016 Sep 16 17:39:00 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: <b>user "8x_CCE_Tester_1" password *****</b> read-write all, result: SUCCESS</p> <p>2016 Sep 20 19:24:06 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: <b>swlog output flash-file-size 85</b>, result: ERROR: Invalid File Size(85 Kbytes).</p> <p>2016 Sep 21 10:12:24 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: <b>swlog output flash-file-size 125</b>, result: SUCCESS</p>
FMT_SMF.1	All management activities of TSF data.	AOS application ID	<p>Administer the TOE locally and remotely is recorded as below:</p> <p><b>For console session:</b></p> <p>2021 Mar 5 11:54:03.732 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: aaa authentication console local, result: SUCCESS</p> <p>2016 Sep 16 13:26:53 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,login,CONSOLE</p> <p><b>For SSH session:</b></p> <p>2021 Mar 5 11:54:10.857 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: aaa authentication ssh local, result: SUCCESS</p>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>2016 Sep 16 16:50:01 OS6860 swlogd: SES AAA info(5) EVENT-AUDIT Login by admin from 10.145.59.99 through SSH Success [in LoginAaaSession::handleLoginResult() ]</p> <p>2016 Sep 16 16:50:01 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,login,SSH</p> <p><b>Configuring the access banner is recorded as below:</b></p> <p>2021 Mar 5 11:58:06.913 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: session cli banner /flash/banner.txt, result: SUCCESS</p> <p><b>Configuring the session inactivity time before session termination or Locking is recorded as below:</b></p> <p>2021 Mar 5 11:59:42.528 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: session cli timeout 100, result: SUCCESS</p> <p><b>Updating the TOE and verifying the updates using hash comparison capability prior to installing those updates are recorded as below:</b></p> <p>2021 Mar 5 12:06:37.343 OS6900-X72_VC swlogd ChassisSupervisor vcReloadMgr INFO: EVENT-AUDIT: starting reload sequence for image working</p> <p>2021 Mar 5 12:06:42.729 OS6900-X72_VC swlogd flashManager Main INFO: EVENT-AUDIT: Verifying image directory working on CMM flash</p> <p>2021 Mar 5 12:07:40.087 OS6900-X72_VC swlogd flashManager Main INFO: EVENT-AUDIT: Verifying image</p>



Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>Integrity on directory working on CMM flash</p> <pre>2021 Mar 5 12:02:02.335 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: image integrity get-key /flash/working, result: SUCCESS</pre> <pre>2021 Mar 5 12:02:52.507 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: image integrity check working key-file /flash/working/imgsha256sum, result: SUCCESS</pre> <p><b>Configuring the authentication failure parameters for FIA_AFL.1 is recorded as below:</b></p> <pre>2021 Mar 5 12:16:33.540 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: user lockout-window 99, result: SUCCESS</pre> <pre>2021 Mar 5 12:16:44.966 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: user lockout-threshold 10, result: SUCCESS</pre> <pre>2021 Mar 5 12:17:19.079 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: user lockout-duration 100, result: SUCCESS</pre> <p><b>Configuring audit behavior, see FMT_MOF.1 /Functions for sample records.</b></p> <p><b>Manage the cryptographic keys, see FMT_MTD.1 / CryptoKeys for sample records.</b></p> <p><b>Re-enable an Administrator account is recorded as below:</b></p>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>2021 Mar 5 12:25:28.421 OS6900-X72_VC swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: user test unlock, result: SUCCESS</p> <p><b>Setting the time which is used for time-stamps is recorded as:</b></p> <p>2019 Dec 1 14:25:33.016 L2-DUT2 swlogd ssapp library(SysServices) INFO: EVENT-AUDIT System Date changed from 10/29/2019 to 12/01/2019</p> <p>2019 Dec 1 14:25:33.038 L2-DUT2 swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: system date 12/01/2019, result: SUCCESS</p> <p>2019 Dec 1 03:09:00.031 L2-DUT2 swlogd ssapp library(SysServices) INFO: EVENT-AUDIT System Time changed from 14:29:50 (UTC) to 03:09:00 (UTC)</p> <p>2019 Dec 1 03:09:00.047 L2-DUT2 swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: system time 03:09:00, result: SUCCESS</p> <p><b>Importing X.509v3 certificates to the TOE's trust store are recorded as:</b></p> <p>2016 Nov 2 16:04:18 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: aaa certificate update-ca-certificate ca_and_crl.pem, result: SUCCESS</p>
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	No additional information	For a successful system update, no error messages must be witnessed; system update sequence recorded as:

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>2016 Nov 2 16:19:14 OS6860 swlogd: ChassisSupervisor vcReloadMgr info(5) EVENT-AUDIT: starting reload sequence for image working</p> <p>2016 Nov 2 16:19:37 OS6860 swlogd: flashManager FlashMgr Main info(5) EVENT-AUDIT: Verifying image Integrity on directory working on CMM flash</p> <p><b>Image Integrity Failure:</b> Verification test failure is recorded as:</p> <p>2017 Jan 1 17:08:03 OS6860 swlogd: ChassisSupervisor reloadMgr info(5) EVENT-AUDIT: Verify of reload image failed - terminating Reload request</p>
FPT_STM_EXT.1	Changes to the time	Old and new time values	<p><b>Failures:</b>2016 Sep 20 12:25:58 OS6860 swlogd: SSAPP main info(5) EVENT-AUDIT Invalid system date 20/09/2016.</p> <p><b>For Console Date/Time Change:</b></p> <p>2019 Dec 1 03:09:00.031 L2-DUT2 swlogd ssapp library(SysServices) INFO: EVENT-AUDIT System Time changed from 14:29:50 (UTC) to 03:09:00 (UTC)</p> <p>2019 Dec 1 03:09:00.047 L2-DUT2 swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (console), cmd: system time 03:09:00, result: SUCCESS</p> <p><b>For SSH Date/Time Change:</b>2019 Dec 1 04:09:00.031 L2-DUT2 swlogd ssapp library(SysServices) INFO: EVENT-AUDIT System Time changed from 14:35:14 (UTC) to 04:09:00 (UTC)</p> <p>2019 Dec 1 04:09:00.047 L2-DUT2 swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: admin (192.168.144.253), cmd: system time 04:09:00, result: SUCCESS</p>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FTA_SSL_EXT.1	Termination of a local interactive session	None	Termination of an interactive session are recorded as:  2016 Sep 16 18:33:43 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,logout,CONSOLE
FTA_SSL.3	Termination of a remote interactive session	None	Termination of an interactive session are recorded as:  2016 Sep 16 18:33:43 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,logout,SSH  2016 Nov 4 20:20:01 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,logout,SSH
FTA_SSL.4	The termination of an interactive session	None	Termination of an interactive session are recorded as:  2016 Sep 16 18:33:43 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,logout,CONSOLE  2016 Nov 4 20:20:01 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,logout,SSH
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	See FTP_TRP.1 for sample records
FTP_TRP.1	Initiation of the trusted path.	Identification of the claimed user identity	<b>Connection Establishment/ Termination:</b>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	<p>Termination of the trusted path.</p> <p>Failure of the trusted path functions</p>		<p>Secure connection establishment and terminations (TLS and SSH) are recorded as:</p> <pre>2016 Oct 17 21:08:10 OS6860 OS6860 syslog-ng[18521]: EVENT-AUDIT: Syslog TLS handshake done successfully. Session established;</pre> <pre>2023 Jun 28 17:23:31 os6360 os6360 syslog-ng[7908]: EVENT-AUDIT: Syslog TLS session terminated;2016 Nov 4 20:20:01 OS6860 swlogd: AAA Switch- Access info(5) EVENT-AUDIT aravind,logout,SSH</pre> <pre>2016 Sep 16 18:33:43 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT admin,logout,CONSOLE</pre> <p><b>Validation/ Connection Failures for SSH:</b></p> <pre>2023 Jan 4 23:03:50.142 os6360 sshd[PID#] Unable to negotiate with &lt;IP Address&gt; port &lt;#&gt;: no matching &lt;feature&gt;. Their offer: &lt;key type&gt;</pre> <pre>2023 Jan 4 23:03:50.142 os6360 sshd[PID#] Unable to negotiate with &lt;IP Address&gt; port &lt;#&gt;: no matching &lt;feature&gt;. Their offer: &lt;MAC type&gt;</pre> <pre>2023 Jan 4 23:03:50.142 os6360 sshd[PID#] Unable to negotiate with &lt;IP Address&gt; port &lt;#&gt;: no matching &lt;feature&gt;. Their offer: &lt;kex type&gt;</pre> <pre>2023 Jan 10 02:43:20.674 os6360 sshd[PID#] Bad packet length &lt;size in bytes&gt;.</pre> <pre>2023 Jan 5 00:37:34.578 os6360 sshd[PID#] EVENT-AUDIT: key setup successfully remote host: &lt;IP Address&gt;</pre>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p><b>Validation/ Connection Failures for TLS:</b></p> <p>Certificate validation failures and resulting connection failures are reported as:</p> <pre>2016 Sep 13 18:33:43 OS6860 syslog-ng[PID#]: EVENT-AUDIT: Syslog certificate validation failed; subject=&lt;SUBJECT NAME&gt;', issuer='&lt;ISSUER NAME&gt;', error='&lt;ERROR&gt;'  2016 Sep 13 18:33:43 OS6860 syslog-ng[PID#]: EVENT-AUDIT: Syslog certificate valid, but extended Key Usage is not set to serverauth, rejecting;  2023 Jan 13 02:12:53 os6360 os6360 syslog-ng[PID#]: EVENT-AUDIT: Syslog TLS session failure because of error while writing stream; tls_error=&lt;error&gt;</pre>
FMT_MTD.1 / CryptoKeys	Modification, deletion, generation/import of cryptographic keys	None	<p><b>Cryptographic key handling:</b></p> <p>Administrative operations involving crypto key/ certificate generation, deletion, etc., are recorded as:</p> <pre>2016 Nov 2 15:52:34 OS6860 swlogd: AAA Switch-Access info(5) EVENT-AUDIT: Generated RSA key file: /flash/switch/cert.d/mykey.key.  2023 Jul 12 04:15:58.654 os6465 swlogd SES CMD INFO: EVENT-AUDIT CLI log, user: gssadmin (console), cmd: aaa certificate generate-csr rsa.csr key rsa.key cn os6360.example.com ON GSS ou Lab 1 Catonsville st Maryland c US, result: SUCCESS  2016 Nov 2 16:01:38 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: aaa certificate delete myss.pem, result: SUCCESS</pre>

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<p>2016 Nov 2 16:04:18 OS6860 swlogd: SES CMD info(5) EVENT-AUDIT CLI log, user: admin (console), cmd: aaa certificate update-ca-certificate ca_and_crl.pem, result: SUCCESS</p> <p><b>Remove CA Bundle</b></p> <p>2016 Nov 2 19:17:55.723 OS6860 bash INFO: EVENT-AUDIT User gssadmin enters command "rm -r /flash/switch/ca.d/certs.pem"</p>
FCS_SSHS_EXT.1	Failure to establish an SSH session. Successful SSH rekey.	Reason for failure Non-TOE endpoint of connection (IP Address)	See FTP_TRP.1
FCS_TLSC_EXT.2	Failure to establish an TLS Session	Reason for failure	See FTP_TRP.1 for sample records
FIA_AFL.1	When unsuccessful login attempt is met or exceeded	swlog message captures the number of unsuccessful login attempts reached including the origin of the login attempt (source IP address)	2021 Feb 4 10:56:07.764 L2-DUT2 swlogd AAA Switch-Access INFO: EVENT-AUDIT: User thainguyen from 10.120.0.1 locked due to 5 times unsuccessful login attempts

**Table 7 - Sample Audit Records Table**

### 3.1.2 Security Audit Event Storage (Extended – FAU\_STG\_EXT)

OmniSwitch provides an option to configure external syslog server for transmitting the audit events to an external audit server. Audit server can be configured in the switch using the *swlog output socket <domain\_name> tls* command. OmniSwitch establishes a secure connection over TLS connection with the configured audit server. The audit logs for various events are stored locally in the OmniSwitch; simultaneously the logs are transmitted over the secure TLS connection to the configured audit server.

The logs are transmitted as meta-data with respective sequence number and timestamp correction.

**Log Server:** *Oct 17 14:41:42 192.168.20.1 192 <13>1 2016-10-17T14:40:07+05:30 OS6860 2016 - - [meta sequenceId="18"] Oct 17 14:40:06 OS6860 OS6860 syslog-ng[8008]: EVENT-AUDIT: Syslog TLS handshake done successfully. Session established;*

**OmniSwitch:** *2016 Oct 17 21:08:10 OS6860 OS6860 syslog-ng[18521]: EVENT-AUDIT: Syslog TLS handshake done successfully. Session established;*

Possible configuration option is to remove external syslog server using *no swlog output socket <domain\_name>* CLI command. Upon successful removal of External Syslog server configuration from OmniSwitch, TLS connection to Syslog server will not be further established. Also, existing TLS connections between OmniSwitch and Syslog server will be terminated. In both cases, no swlog messages will further be transmitted to External Syslog server but will be stored locally.

The audit data of all events is captured in SWLOG file. The amount of the audit data that can be captured depends on the size of the SWLOG files. The size (in kilobytes) of the SWLOG file for storing the audit data locally can be configured using the CLI command *swlog output flash-file-size <kilobytes>*. The allowed values for the maximum size of the audit log files are 125 to 12500 Kilobytes. By default, the switch logging file size is set to 1250 kilobytes.

```
-> swlog output flash-file-size 10000
```

Space available in the flash memory can be found out by the command *show hardware-info*, which shows available free memory.

For stack based products like OS6900/OS6860/OS6865/OS6465/OS6560 the audit logs are captured in total eight *swlog\_chassis<chas id>*, *swlog\_chassis<chas id>.0* till *swlog\_chassis<chas id>.6* files in the /flash directory., the SWLOG file size specified in the above command is for an individual “swlog\_\*” file. The total audit storage capacity would be eight times the SWLOG size configured through the above command. The default total audit storage capacity is 8\*1250 Kilobytes.

For chassis based product OS9900 for the CMM component the audit logs are captured in eight files *swlog\_chassis<chas id>\_CMM<CMM slot>*, *swlog\_chassis<chas id>\_CMM<CMM slot>.0* till *swlog\_chassis<chas id>\_CMM<CMM slot>.6* in the /flash directory. For the NI component, the audit logs are captured in eight files *swlog\_NI<slot no>\_chassis<chas id>\_CMM<CMM slot>*, *swlog\_NI<slot no>\_chassis<chas id>\_CMM<CMM slot>.0* till *swlog\_NI<slot no>\_chassis<chas id>\_CMM<CMM slot>.6* in the /flash directory. The SWLOG file size specified in the above command is for an individual “swlog\_\*” file. The total audit storage capacity would be eight times the SWLOG size configured through the above command. The default total audit storage capacity is 8\*1250 Kilobytes for each CMM/NI component.



For chassis based product OS9000 for the Host component the audit logs are captured in eight files *swlog\_CMM<CMM slot>\_host*, *swlog\_CMM<CMM slot>\_host.0* till *swlog\_CMM<CMM slot>\_host.6* stored in the /flash directory. For the CMM component the audit logs are captured in eight files *swlog\_chassis<chas id>\_CMM<CMM slot>*, *swlog\_chassis<chas id>\_CMM<CMM slot>.0* till *swlog\_chassis<chas id>\_CMM<CMM slot>.6* in the /flash directory. For the NI component, the audit logs are captured in eight files *swlog\_NI<slot no>\_chassis<chas id>\_CMM<CMM slot>*, *swlog\_NI<slot no>\_chassis<chas id>\_CMM<CMM slot>.0* till *swlog\_NI<slot no>\_chassis<chas id>\_CMM<CMM slot>.6* in the /flash directory. The SWLOG file size specified in the above command is for an individual “swlog\_\*” file. The total audit storage capacity would be eight times the SWLOG size configured through the above command. The default total audit storage capacity is 8\*1250 Kilobytes for each CMM/NI component.

**Note:** The *chas id* is the Chassis Id configured on the switch, *CMM slot* is the CMM slot A or B on which the CMM card is inserted and *slot no* is the slot number on which the NI card is inserted.

There is a mechanism to display a warning to the user if the storage capacity has reached a configurable threshold limit on the configured size of the SWLOG files. The warning message is appended to audit log file. The location of the audit log file has been described in above paragraph.

A sample warning message is displayed as follows:

```
2016 Jan 2 19:48:20 OS6860 swlogd: SSAPP main info(5) EVENT-AUDIT: Switch log file reached 90%, Backup files before overwritten.
```

The default threshold limit before a warning message is generated by the OmniSwitch is 90%. This Threshold limit of the storage space value can be changed using the CLI command “*swlog size-trap-threshold <threshold>*”.

### 3.1.3 Protected Audit Trail Storage (FAU\_STG.1)

The audit files are protected from deletion and modification. Only the Security Administrator can clear the audit files. The audit files can be cleared using the CLI command “*swlog clear all*”.

Sample message is as follows:

```
2016 Jan 2 19:48:20 OS6860 swlogd: SSAPP main info(5) EVENT-AUDIT: Switch log file reached 90%, Backup files before overwritten
```

```
2016 Jan 2 20:52:20 OS6860 EVENT-AUDIT: Switch log file reached 100%, overwritten !!!
```

```
2016 Sep 20 13:34:06 OS6860 ssapp: EVENT-AUDIT: Swlog cleared
```

The swlog files can also be cleared by logging into the “su” and removing the swlog files in /flash using command “*rm -rf /flash/swlog\_\**” .

## 3.2 Cryptographic Support (FCS\_CKM, FCS\_COP)

### 3.2.1 Cryptographic Key Generation (FCS\_CKM.1)

The OmniSwitch generates keys for use with a CSR, for use as an SSH hostkey, and as part of TLS and SSH session negotiations.

With CC mode enabled, the TOE supports the following cryptographic key generation algorithms.

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” P-256, P-384, P-521 that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' and RFC3526.

The OmniSwitch product family implements TLS to provide a secure channel for interaction with server communications. The OmniSwitch does not provide a self-signed certificate in the default configuration. Follow the instructions in section 3.3.6 to create RSA or ECDSA certificate signing request (CSR). The administrator uses the CSR to obtain a certificate from a trusted Certificate Authority. The administrator must then import the certificate into the OmniSwitch (using SCP) to be used in TLS negotiations with external entities (e.g., a syslog server).

The OmniSwitch product family implements SSH to provide a secure trusted path for administrators. SSH uses RSA-SHA2-256, RSA-SHA2-512, ECDSA SHA2 NISTP256, ECDSA SHA2 NISTP384 and ECDSA SHA2 NISTP521 keys for session establishment. In OmniSwitch SSH hostkey generation is carried out automatically during reload with RSA (sizes of 2048-bit or greater) and ECDSA SHA2 NISTP256 algorithms using the `ssh-keygen` command. If there are no valid key present under `/flash/system` directory and if the user would like to use a different RSA key or ECDSA SHA2 NIST256 keys, the user can generate the keys on the OmniSwitch (using `ssh-keygen` command) and copy the files to the `/flash/system` directory on the switch. The new keys take effect after the OmniSwitch is rebooted.

### 3.2.2 Cryptographic Key Establishment (FCS\_CKM.2)

With CC mode enabled, the TOE supports the below cryptographic key establishment methods:

- RSA-based key establishment schemes that meet the following:  
RSAES-PKCS1-v1\_5 as specified in Section 7.2 of [RFC8017]#, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1";
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' and groups listed in RFC 3526.

Session negotiation includes an exchange of asymmetric public keys and derivation of symmetric session keys, implemented for both SSH and TLS secure channel.

Once the session is initialized and functioning, all traffic between endpoints is communicated over a secure channel, using the negotiated encryption algorithm and key size.

For both SSH and TLS there are no specific user configuration for selecting the key establishment, it is based on negotiation during session establishment.

### 3.2.3 Cryptographic Key Destruction (FCS\_CKM.4)

Cryptographic key destruction is carried out by the internal operation of the OmniSwitch software according to the type of storage and user operation is not involved. The TOE is not subject to any delays in cryptographic key destruction.

### 3.2.4 Cryptographic Operation (FCS\_COP)

With CC mode enabled, the following table mentions the cryptographic algorithms used in OmniSwitch software and its usage to enforce the following SFRs FCS\_COP.1/DataEncryption, FCS\_COP.1/SigGen, FCS\_COP.1/Hash and FCS\_COP.1/KeyedHash.

Crypto	Supported algorithms	Usage
Key Generation	RSA 2048-bit and 3072-bit keys	TLSv1.2 SSHv2
	ECDSA P-256, P-384, P-521 keys, RSA-SHA2-256, RSA-SHA2-512	SSHv2
	ECDSA P-256, P-384 and P-521 ephemeral keys	TLSv1.2 SSHv2
	Diffie-Hellman 2048-bit and 3072-bit keys	TLSv1.2
Key Establishment	RSA-based, 2048-bit, 3072-bit keys RSA-SHA2-256, RSA-SHA2-512	TLSv1.2 SSHv2
	ECDSA-based, P-256, P-384 and P-521 keys	TLSv1.2 SSHv2
Data Encryption/Decryption	AES (CBC mode) with 128-bit and 256- bit keys	TLSv1.2 SSHv2
	AES (CTR mode) with 128-bit and 256- bit keys	SSHv2
	AES (GCM mode) with 128-bit and 256- bit keys	TLSv1.2SSH SSHv2

Signature Generation/Verification	RSA PKCS#1 v1.5 with SHA-1, SHA-256, SHA-384 and SHA-512, using 2048-bit and 3072-bit keys  ECDSA with SHA-256, SHA-384 and SHA-512 using NIST P-256, P-384, and P-521 curves	TLSv1.2 SSHv2
Hash Algorithm	SHA-1	Signature Generation and Verification Keyed Hashing Pseudorandom Function
	SHA-256	Signature Generation and Verification Keyed Hashing Password storage Trusted Update Pseudorandom Function
	SHA-384	Pseudorandom Function
	SHA-512	Keyed Hashing Pseudorandom Function
Keyed Hash Algorithm	HMAC-SHA-1 with 160-bit key	TLSv1.2 SSHv2
	HMAC-SHA-256 with 256-bit key	TLSv1.2 SSHv2
	HMAC-SHA-512 with 512-bit key	SSHv2
	HMAC-SHA-384 with 384-bit key	TLSv1.2

DRBG	Hash_DRBG (default), CTR_DRBG, HMAC_DRBG	Asymmetric key generation Session key generation
------	--	---

**Table 8 - Supported Crypto Algorithms**

The 3DES algorithms should not be configured for use in the CC evaluated configuration.

The signature algorithms used by an SSHv2 or TLSv1.2 session is determined by the negotiated cryptographic parameters and authentication methods. With CC mode enabled, the TOE only supports signature generation and verification as shown in Table 8 above.

There is no specific configuration for selection of key sizes offered by the TOE. Enabling CC mode automatically limits the key sizes offered to those allowed in an evaluated configuration. The key size used for a specific session is selected based on the negotiation during SSH session establishment.

There is no user specific configuration for all the crypto algorithms offered by the TOE during SSH and TLS connection establishment. Enabling CC mode automatically limits the key sizes offered to those allowed in an evaluated configuration. The cryptographic algorithms used for a specific SSH or TLS session are selected based on the negotiation during SSH/TLS connection establishment.

### 3.2.5 Extended: Random bit generation (FCS\_RBG\_EXT.1)

The TSF shall perform all deterministic random bit generation (DRBG) services in accordance with ISO/IEC 18031:2011. It uses HASH\_DRBG, CTR\_DRBG and HMAC\_DRBG of the openssl package for providing randomness to the cryptographic operation. This is an internal operation of OmniSwitch software and no user operation is involved.

### 3.2.6 SSH Server (FCS\_SSHS\_EXT.1)

The TOE implements SSH as the trusted path. It enforces FTP\_TRP.1, providing assured identification of the peer end point and logically distinct communication channels between the TOE and authorized remote administrators, and protecting data communicated over the channel from modification or disclosure. The SSH implements a strong cryptographic authentication mechanism to assure identification of each end point when the channel is initiated.

The TOE implements SSH, used in conjunction with the CLI command sets for secure remote administration. SSH is an industry standard mechanism used for strong authentication, negotiation of symmetric session keys and session parameters, and confidential communications. SSH is used by the TOE as a secure communication channel running over a network interface, for secure remote administration of the TOE using the CLI command set.

For the supported encryption, key exchange, public key algorithm, and data integrity MAC algorithms refer [ST]. There is no specific user configuration for selecting the encryption, key exchange, public key algorithm and data integrity MAC algorithms; they are selected by default in the CC evaluated configuration. Other SSH parameters can be configured through CLI `ssh`, “[vrf name] ssh {port [default | service\_port] | admin-state [enable | disable] | ip\_address}”.

The SSH public key generation is carried out automatically during reload with RSA (sizes of 2048-bit or greater) keys (stored in **/flash/system/ssh\_host\_rsa\_key** and **/flash/system/ssh\_host\_rsa\_key.pub**) and ECDSA (SHA2 NISTP256, SHA2 NISTP384 , SHA2 NISTP521) keys (stored in **/flash/system/ssh\_host\_ecdsa\_key** and **/flash/system/ssh\_host\_ecdsa\_key.pub**)

If there are no valid key present under **/flash/system** directory and if the user would like to use a different RSA (sizes of 2048-bit or greater) key or ECDSA (SHA2 NISTP256, SHA2 NISTP384 , SHA2 NISTP521) keys, the user can use the Secure Shell tools available on your Unix or Windows system to generate the keys externally and SSH the files to the **/flash/system** directory on the switch. The new keys take effect after the OmniSwitch is rebooted.

## Using Secure Shell Public Key Authentication (PKA)

### Generating and Copying Keys

The following procedure shows how to set up Secure Shell PKA between an OmniSwitch and a client device. The steps below use a userid of “new\_ssh\_user” on the OmniSwitch as an example:

Step 1: Use the ssh-keygen utility of the OpenSSH software suite to generate a private and public key pair as shown below:

```
[User1@Ubuntu-20.04 ~]$ ssh-keygen -t ecdsa -C admin@10.10.0.12
```

Generating public/private ecdsa key pair.

Enter file in which to save the key (/home/ User1/.ssh/id\_ecdsa):

/home/ User1/.ssh/id\_ecdsa already exists.

Overwrite (y/n)? y

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/ User1/.ssh/id\_ecdsa

Your public key has been saved in /home/ User1/.ssh/id\_ecdsa.pub

The key fingerprint is:

SHA256:yOy7Sra6XBaednG4IsYBUmNZyinzBiyO4oFU2DT++HCM User1@ubuntu

The key's randomart image is:

```
+---[ECDSA 256]---+
```

```
| +++o      |
| =.o=o.    |
|+ ++.oo    |
|=.+.+.+ +  |
|o+..E X S  |
|o. o * B   |
| + X *     |
| o B + .   |
| +oo.o.    |
```

+----[SHA256]-----+

Step 2: Copy the public key to the switch in the preferred directory. Including the user id as part of the filename can help identify the different keys:

```
#scp ~/.ssh/new_ssh_user_rsa.pub admin@12.18.2.1:/flash/system
```

For example:

```
[User1@Ubuntu-20.04 ~]$ scp ~/.ssh/id_ecdsa.pub admin@10.10.0.12:/flash/system
```

Password:

```
id_ecdsa.pub                100% 179  64.6KB/s  00:00
```

4 Verify that the userid that will use SSH is a valid username on the OmniSwitch. If the username does not exist on the switch create the username with the appropriate privileges.

5 Install the public key on the OmniSwitch for the specified user.

```
-> installsshkey new_ssh_user /flash/system/new_ssh_user_rsa.pub
```

For example:

```
-> installsshkey admin /flash/system/id_ecdsa.pub
```

Updated existing SSH key.

6 Connect to the OmniSwitch using SSH with PKA.

```
#ssh -o PreferredAuthentications=publickey new_ssh_user@12.18.2.1 -v
```

For example:

```
[User1@Ubuntu-20.04 ~]$ ssh -o PreferredAuthentications=publickey admin@10.10.0.12
```

```
-> whoami
```

Session number = 4

User name = admin,

Access type = ssh,

Access port = Ethernet,

IP address = 10.10.0.1,

Read-only domains = None,

Read-only families = ,

Read-Write domains = All ,

Read-Write families = ,

Revoking a Key

The following procedure can be used to revoke a key:

```
->revokesshkey new_ssh_user remote\_ssh\_user@12.18.10.1
```

For example:

```
-> revokesshkey admin admin@10.10.0.12
```

Revoked SSH key for that remote user.

The TOE limits the size of SSHv2 packets to 256 Kb, packets greater than this size in an SSH transport connection are dropped.

Within SSH connections the same session keys are used for a threshold of no longer than one hour (3600s), and no more than 2<sup>30</sup> bytes of transmitted data. After either of the thresholds are reached a rekey needs to be performed. These are the default rekey values that cannot be modified by the administrator.

When there is an unintentional interruption of the SSH connection, the connection will be terminated automatically, and the administrator needs to manually retry to re-establish the connection.

### 3.2.7 TLS Client Protocol (FCS\_TLSC\_EXT.2) and (FCS\_TLSC\_EXT.1.1)

OmniSwitch implements trusted channels through TLS. OmniSwitch enforce FTP\_ITC.1, providing assured identification of the peer end point and logically distinct communication channels between OmniSwitch and other trusted IT products, and protecting data communicated over the channel from modification or disclosure.

The TOE implements TLS, an industry standard mechanism used for strong authentication, negotiation of symmetric session keys and session parameters, and confidential communications.

The Syslog client can establish connection to the respective servers through TLS channel by default. Additionally, an option is available to specify the cipher suite to use for the connection.

In the CC evaluated configuration, by default the TOE use TLSv1.2 no other TLS version is allowed.

The administrator can configure custom cipher suites using the *ssl cipher* command.

**Example:** Create a file with the .cipher extension (e.x. supported\_tls.cipher) containing the following cipher suite list:

```

ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:AES128-SHA256:AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-AES128-
SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:AES128-SHA:AES256-SHA

```

And execute the following command, the configured cipher suite is applied after the user does “write memory” and reload the switch.

- *ssl cipher custom file supported\_tls.cipher*

The following table shows the TLS 1.2 ciphersuites and their equivalent OpenSSL cipher names which are used to create the cipher list for the above command. These are the only ciphers that are allowed in an evaluated configuration.

TLS 1.2 ciphersuite	OpenSSL cipher name
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256



TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384

**Table 10 – TLS 1.2 Ciphersuites to OpenSSL Cipher Names Mapping**

The TOE can generate RSA and ECDSA keys to be used for X509 certs. For generation of X509v3 certificates refer section [Mutual Authentication](#).

The TOE implements the Supported Elliptic Curves *Extension* according to [RFC4492] with NIST curves secp256r1, secp384r1, and secp521r1. This behavior is performed by default and there is no security management function to disable it.

The configured server Hostname for Syslog is being used as a reference identifier for validating the TLS certificate.

OmniSwitch supports CN (Common Name) and SAN (Subject Alternative Name). However, it does not support constructing reference identifiers (domain name) using wildcards in certificates.

*Note: The TOE can accept Domain Name (Hostname) as reference identifier for validating the TLS certificate.*

Refer to Security Audit Event Storage (Extended – FAU\_STG\_EXT) section where instructions are provided to cause the TOE to transmit the generated audit data to an external entity using TLS. While the TOE is capable of being configured to accept an IP address or IPv6 address to identify the external entity for a TLS connection, that form of reference identifier was not part of the evaluated configuration. The TOE requires the FQDN be configured as the external entity reference identifier to allow matching of the CN or SAN within the certificate presented by the external entity during TLS negotiation against the FQDN configured on the TOE.

### 3.3 Identification and Authentication (FIA)

Network administrator accounts provide access to OmniSwitch management functions and are controlled through functional privilege settings. End-user accounts are associated with end-user profiles. An account may not be configured for both network administration and end-user access.

All OmniSwitch products are configured with a default administrative account with permissions to configure all OmniSwitch accounts and settings. In addition, the OmniSwitch product family supports the use of the default user account, which cannot be used to log into the switch but is used to store default values for new accounts.

The OmniSwitch factory default configuration enables only the default network administration user over the CLI interface on the local console. All other management interfaces that require authentication must be unlocked with the `aaa authentication {console | telnet | ftp | http | snmp | ssh | default} server1 [server2...] [local]` CLI command.

#### 3.3.1 Authentication Failure Management (FIA\_AFL.1)

The OmniSwitch will detect and track any unsuccessful login attempts.

The duration for which the failed login attempts must be counted can be configured by *user lockout-window <minutes>* command. Allowed range for *<minutes>* is 0 to 99999 minutes.

The number of failed login attempts for the configured user lockout window can also be set by *user lockout-threshold <number>* command. Allowed range for *<number>* is 0 to 999.

The duration for which the unsuccessful login attempt user must be locked can also be set by *user lockout-duration <minutes>* command. Allowed range for *<minutes>* is 0 to 99999 minutes.

When the user exceeds the defined number of unsuccessful authentication attempts, the user's account is locked out. That user account is unlocked either by executing the *user <username> unlock* command or by waiting till the lock out duration time has passed.

The admin user authentication protection.

- The default “admin” user is considered the privileged administrator and has full administrative privileges for all commands on the TOE.
- It is strongly recommended that the primary admin user (i.e., admin) have access to the local console as this user is the only admin user able to login locally if otherwise locked out.
- If password expiration is configured for the admin user or configured globally through the user password-expiration command, when the admin user's password expires, the admin user will have access only through the console port.
- The *user lockout-window <minutes>* command is only available to the admin user because the admin user account is the only account protected from any type of lockout attempt.

### 3.3.2 Password Management (Extended – FIA\_PMG\_EXT)

See the *Security Management* section for user account and password policy references and session timeout and session-login timeout references. The following are the requirements for CCE for password management capabilities for user passwords:

Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: "@", "#", "\$", "%", "^", "&", "\*", "(", ")", "~", ";", "[", "]", ":", ":", ":", "|", "\_", "/", ".", "<" and ">".

*Note: Special character “!” is not allowed in user passwords.*

In CC enabled mode minimum password length is settable by the Security Administrator.

Some of the requirements of the Password length support:

In CC mode, the minimum password length shall be configurable between 1 (the minimum password length in default switch operation) and 30 (the maximum password length in default switch operation).

SHA256 encryption is used to store user passwords.

The administrator can define the password setting for the composition of strong password by configuring the global password policy settings in the switch.

### 3.3.3 User Identification and Authentication (Extended – FIA\_UIA\_EXT)

The OmniSwitch ensures each administrative user is successfully identified and authenticated before allowing any administrative actions on behalf of that user. This is supported by identifying/authenticating each user through local user database.

For successful authentication, the user must be configured on the local user database using CLI *user username {password password | password-prompt}* command prior to authentication is attempted.

### 3.3.4 User authentication (Extended – FIA\_UAU\_EXT)

The OmniSwitch provides a local password-based authentication mechanism to perform administrative user authentication. By default, the login is prompted on accessing the switch. By default, OmniSwitch provides only obscured feedback to the administrative user while the authentication is in progress at the local console.

```
OS6860 login: admin
Password:
Welcome to the Alcatel-Lucent Enterprise OS6860E-P24Z8 8.9.6.R11 Development, July 24, 2023.
```

```
Copyright (c) 1994-2014 Alcatel-Lucent. All Rights Reserved.
Copyright (c) ALE USA Inc., 2014-2022. All Rights Reserved.
```

```
OmniSwitch(tm) is a trademark of Alcatel-Lucent,
registered in the United States Patent and Trademark Office.
```

```
->
```

```
ssh admin
admin's password:
```

```
ssh user
Warning: Permanently added 'user' (RSA) to the list of known hosts.
user's password:
X11 forwarding request failed on channel 0
```

### 3.3.5 Protected authentication feedback (FIA\_UAU.7)

OmniSwitch shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console. When the user provides the password, the password is not displayed on the local console until the authentication is successful or failed.

```
login: admin
Password:
```

### 3.3.6 Authentication using X.509 Certificates (Extended – FIA\_X509\_EXT)

#### **X.509v3 Certificate pre-requisites:**

During TLS handshake, the Syslog server will send a certificate to the OmniSwitch client. The following sections cover the pre-requisites for establishing mutually authenticated TLS connection to the Syslog server.

- a) DNS must be configured. Refer Section 3.3.6.1 below.
- b) Accurate time must be configured (See section entitled Time stamps)
- c) TLS ciphers must be configured (See section entitled TLS Client Protocol)
- d) Setup the Trust Anchors in the CA Bundle (See section entitled Loading CA Bundle)
- e) Install TOE Certificates (See section entitled Mutual Authentication)
- f) Specify syslog server connection (See section entitled Security Audit Event Storage)

#### **3.3.6.1 Enabling the DNS Resolver**

A Domain Name System (DNS) resolver that translates host names into IP addresses needs to be configured in the TOE to resolve domain names.

Below steps need to be followed to enable the DNS resolver service.

Set the default domain name for DNS lookups with the *ip domain-name* CLI command.

```
-> ip domain-name mycompany1.com
```

Use the *ip domain-lookup* CLI command to enable the DNS resolver service.

```
-> ip domain-lookup
```

Specify the IP addresses of the servers with the *ip name-server* CLI command. These servers will be queried when a host lookup is requested.

```
-> ip name-server 189.202.191.14 189.202.191.15 189.255.19.1
```

#### **3.3.6.2 Certificate Validation**

The OmniSwitch validates X.509 certificate when they are imported into the TOE as well as when they are received during TLS session negotiation.

The validation of a certificate involves checking many fields within the certificate. All such checks must be successful in order for the certificate to be considered valid. OmniSwitch performs the following checks on a certificate to determine its validity.

- Verify that the certificate has a correct format and has not expired
- Verify that the chain of trust from the certificate up to the CA root certificate is maintained
- Verify that the CA root certificate is trusted
- Verify that the basicConstraints extension exists and the CA flag is set to TRUE for all CA certificates in the path
- Verify that the certificate has not been revoked

- Verify that the extendedKeyUsage field in the certificate corresponds to the use of the certificate "Server Authentication" for a certificate from a syslog server connection
- Verify the subject name of the configured server matches the Subject name within the X.509 certificate presented by the server during TLS negotiations.

These checks are performed when the administrator manually uses the CLI command: `aaa certificate verify` described in the following section. These checks are also performed when the OmniSwitch establishes a TLS session with a configured syslog server. The validation of the "Subject" name occurs during TLS session establishment.

The OmniSwitch uses the OCSP protocol as the primary method for checking the revocation status of the certificates. OmniSwitch TLS client applications obtain the OCSP Server URLs from within the certificates presented during TLS negotiation and verification the revocation status of those certificates by contacting the OCSP responder identified by the certificate AIA information. No configuration is necessary to ensure this behavior.

The OmniSwitch will treat an OCSP response indicating status is Unknown the same as a status of Revoked. Only when OmniSwitch can positively verify a certificate's revocation status with its OCSP Responder is the certificate treated as valid.

### 3.3.6.3 Loading the CA Bundle

The OmniSwitch ensures that all certificate accepted during a TLS negotiation must chain to a root certificate that an administrator has identified as trustworthy. In order for an administrator to identify a certificate as trustworthy, they must perform the following steps.

- 1) Upload a root certificate belonging to the Certificate Authority to be trusted.
- 2) Insert the certificate into the CA bundle file (**certs.pem**)
- 3) Manually verify the certificate using the CLI command `aaa certificate verify`
- 4) If the verification fails remove the certificate from the CA bundle file
- 5) If the verification succeeds update the list of CA certificate using the `aaa certificate update-ca-certificate` command.

These steps result in trustworthy root CA certificates being stored in the OmniSwitch CA bundle.

Certificate may be uploaded by sending a certificate to the OmniSwitch via SCP from an external SSH client, or by writing the base64 encoded value of the certificate into a file on the OmniSwitch (e.g., *file-with-root-ca-cert.pem*) within the `/flash/switch/cert.d` directory.

The file **certs.pem** is the CA bundle and is available in `/flash/switch/ca.d` directory. This file will have all the root CA certificates that are considered as trusted.

To manually verify a CA certificate the administrator must first insert the certificate into the **certs.pem** file, then perform the CLI command:

```
aaa certificate verify ca-certificate /flash/switch/ca.d/certs.pem certificate <file-with-root-ca-cert.pem>
```

If the verification fails, remove the cert that was added to the **certs.pem** file using an editor.

If the verification is successful, execute the CLI command:

```
aaa certificate update-ca-certificate <ca_file>
```

to commit the certificate to the CA bundle.

Updates to the CA bundle certificates must be done before the corresponding server configurations are done on the switch. If the update is done post server configuration (i.e., post step ‘f’ defined above), then a switch reboot needs to be done for the changes to take effect.

Once the update-ca-certificate command completes successfully, the import of the new CA certificate is complete.

#### **3.3.6.4 Mutual Authentication**

For OmniSwitch to be able to use mutually authenticated TLS communication with an external syslog server, it is necessary for the OmniSwitch to obtain a Mutual Authentication Client certificate to identify itself to the syslog server.

The OmniSwitch Mutual Authentication Client certificate is shared with a server during the TLS negotiation. Therefore, the OmniSwitch must have a certificate to share. The certificate can be obtained either via generation of the keys and CSR within the TOE, or generation of the keys and certificate by an external Certificate Authority.

The act of generating a certificate signing request (CSR) on the OmniSwitch causes a cryptographic key-pair (one public and one private key) to be created and stored securely within the OmniSwitch. The CSR contains the public key, and the private key is saved within the OmniSwitch and never transmitted over a network connection.

While it is possible to have a CA generate a key-pair and create the Mutual Authentication Client certificate without a CSR, this method requires the private key to be transmitted over a network and thus has potential exposure. Both methods are described in the following sections.

##### **3.3.6.4.1 Obtaining a Certificate using a CSR**

The process to obtain a certificate that is compliant with the Common Criteria evaluation is summarized as follows:

- Generate a certificate signing request (CSR) on the OmniSwitch
- Use the CSR to obtain a certificate from a Certificate Authority (CA)
- Import and Validate the certificate into the OmniSwitch

###### **3.3.6.4.1.1 Generate a certificate signing request**

The TOE implements FIA\_X509\_EXT.3.1, OmniSwitch can generate a CSR. Creating the CSR is a two-step process. Private Key needs to be generated followed by generation of the CSR. OmniSwitch provides a framework to support the creation of a Certificate Signing Request (CSR). To generate a X.509 CSR, a network administrator must specify the “Subject” to be used by the certificate. This “Subject” is composed of several possible values which include the following information:

- Common name
- Organization Name
- Organization Unit
- Locality
- State

- Country

These values are optional and should be assigned based upon customer and CA policies. If not provided default values are used to ensure that the Subject is not empty.

### 3.3.6.4.1.1.1 RSA based CSR (Certificate Signing Request) Generation for TLS Connection:

In order to generate a CSR that uses RSA keys first generate the RSA key pair, then use those keys to generate a CSR.

```
-> aaa certificate generate-rsa-key key-file <myCliPrivate.key>
```

This generates an RSA (sizes of 2048-bit or greater) key pair in **/flash/switch/cert.d** with name as provided by the command (i.e., myCliPrivate.key).

```
-> aaa certificate generate-csr <domain_name>.csr key <myCliPrivate.key> dn <domain_name>
[CN common_name] [ON org_name] [OU org_unit] [L locality] [ST state] C[country]
```

This generates the base64 encoded CSR in the file <domain\_name>.csr within the **/flash/switch/cert.d** directory.

### 3.3.6.4.1.1.2 ECDSA based CSR (Certificate Signing Request) Generation for TLS Connection:

In order to generate a CSR that uses ECDSA keys first generate the ECDSA key pair, then use those keys to generate a CSR. The “-name” field in the following command must identify the NIST curve to be used to generate the ECDSA keypair. Allowed values for “-name” are secp256r1, secp384r1 or secp521r1.

```
-> openssl ecparam -name secp256r1 -genkey -out /flash/switch/cert.d/myCliPrivate.key
```

NOTE: Execution of the above command requires ‘root’ permission.

This command generate an ECDSA (using NIST curve P256) key pair in **/flash/switch/cert.d** with name as input **myCliPrivate.key**.

```
-> aaa certificate generate-csr myCliCert.pem key myCliPrivate.key cn client.ale.com on
ALE ou ESD l BAN st KAR c V
```

This generates the CSR into the file **myCliCert.pem** within the **/flash/switch/cert.d** directory.

### 3.3.6.4.1.2 Obtaining a Certificate from a Certificate Authority

The CSR is generated by OmniSwitch as a base64 encoded text file which can readily be copied from the OmniSwitch to an external Certificate Authority. The CSR can be provided to an external Certificate Authority to have that CA issue a certificate as described by the CSR. The certificate issued by the external CA should contain the “Client Authentication” Extended Key Usage.

The steps to cause the external Certificate Authority to issue the certificate are outside the scope of this document and depend upon the CA issuing the certificate. However once issued, the certificate must be imported and validated by the OmniSwitch.

### 3.3.6.4.1.3 Import and Verify the certificate

The process to import and validate a certificate within OmniSwitch involves copying the base64 encoded certificate into the OmniSwitch using SSH or SCP from an administrative workstation. The certificate should be stored in the **/flash/switch/cert.d** directory using a descriptive name (e.g., **cert\_file.pem**).

The administrator must next validate this certificate using CLI command

```
aaa certificate verify ca-certificate /flash/switch/ca.d/certs.pem certificate <cert_file.pem>
```

If this *verify* command returns an indication that the validation failed, the file containing this certificate must be deleted from the OmniSwitch immediately.

If this *verify* command indicates the validation was successful, the administrator must copy the **cert\_file.pem** file to **/flash/switch/cert.d/myCliCert.pem**

At this point the Mutual Authentication Client certificate import is complete.

### 3.3.6.4.2 Obtaining a Certificate and Key from a Certificate Authority

The alternative to using a CSR to generate certificates is to allow an external Certificate Authority to generate the public and private keys as it is creating the Mutual Authentication Client certificate. The steps to cause the external Certificate Authority to create the keys and issue the certificate are outside the scope of this document and depend upon the CA issuing the certificate. However once issued, the certificate and keys can be imported into the OmniSwitch.

To import the Client Certificate and private key – The certificate and private key must be stored in a base64 encoded format and must be transferred into the OmniSwitch from a remote administrator’s workstation. This can be achieved using SCP or a simple SSH connection. The certificate and private keys files must be stored in the **/flash/switch/cert.d** directory. The Certificate must be given the name “**myCliCert.pem**” while the private key file must be named “**myCliPrivate.key**”.

### Commands for viewing/deleting of client certificate file used for mutual authentication

The user can view the contents of the X509v3 certificates using CLI command *aaa certificate view <cert-file-name>*. The certificate files must be stored in **/flash/switch/cert.d** directory before executing this CLI command.

```
-> aaa certificate view <client_cert_file_name>
```

The user can delete the X509v3 certificates from TOE using CLI command *aaa certificate delete <cert-file-name>*. The certificate files must be stored in **/flash/switch/cert.d** directory before executing this CLI command.

```
-> aaa certificate delete <client_cert_file_name>
```

## 3.4 Security Management (FMT)

Each ST reference to a management functions for use by the authorized administrator for secure preparation and operation are listed below, with references to Alcatel–Lucent Enterprise documentation for the appropriate guidance information.

The OmniSwitch has both privileged and semi-privileged administrator roles for administrative access. These privileged and semi-privileged users are configured using the *user <username> [read-only / read-write [families... / domains...]/ all / none / all-except [families / domains...]]* CLI command. The privileges for the users are configured using the read-only or read-write keywords for the different command families or command domains exist in the OmniSwitch.

The privileged administrator role has read-write permission for all command families or command domains whereas the semi-privileged administrator role has read-write permission for specific command families or command domains and read-only permission for the other command families or command domains.



It must be noted that read-only permission means the user can only view the configuration but cannot modify or delete the configuration for those command families or command domains.

It should be noted that the default “admin” user is considered the privileged administrator and has full administrator privileges for all commands on the TOE. Hence the default “admin” user must be used only to perform installation and initial configuration of the TOE. The general switch administration or management must be performed by the users with appropriate administrative privileges (created by the “admin” user), but not by the default “admin” user.

### 3.4.1 Management of functions in TSF (FMT\_MOF)

The update of images must be done with prior authentication as security administrator using a legitimate update image. The security administrator must have administrator privileges to update the images. On an OmniSwitch the software images can be updated only by users having administrator (both read+write) privileges for the system family. Configure with the CLI command *user <username> read-write*.

```
-> user cc_user read-write system
```

The security administrators having the admin privilege would be able to configure the audit server for secure transmission and has the privilege to modify the security functions.

The audit files can be cleared using the CLI command “*swlog clear all*”.

The swlog files can also be cleared by logging into the “su” and removing the swlog files in /flash using command “*rm -rf /flash/swlog\_\**”.

### 3.4.2 Management of TSF Data (FMT\_MTD)

The ability to update/manage switch data is permitted only for administrator or any user having the desired privileges. Administrator privilege can be controlled by modifying privileges (RW/RO) assigned to a user for specific families/domains using the CLI command *user <username> read-write*.

```
-> user cc_user read-write all
```

The ability to delete, modify, import and generate cryptographic keys is also permitted only for admin user or any user having the desired privilege. Below table lists the keys the administrator can manage.

Key/Certificate	Location	Purpose
SSH host RSA public key	/flash/system/ssh_host_rsa_key.pub	Key Establishment
SSH host RSA private key	/flash/system/ssh_host_rsa_key	Key Establishment
SSH host ECDSA public key	/flash/system/ssh_host_ecdsa_key.pub	Key Establishment
SSH host ECDSA private key	/flash/system/ssh_host_ecdsa_key	Key Establishment

SSH user public key	/flash/system/<username>_rsa.pub	Public Key authentication
TOE client certificate (public and private keys)	/flash/switch/cert.d/myCliCert.pem (or .crt) /flash/switch/cert.d/myCliPrivate.key	TOE authentication (TOE acting as client)

**Table 11 - List of keys managed by administrator.**

### 3.4.3 Specification of management functions (FMT\_SMF)

The administrator can administer the TOE locally and remotely. The TOE can be administered through console access and SSH respectively.

The administrator must have ability to configure the pre-banner. A notice can be displayed prior to logging in by updating a file name with the name **pre\_banner.txt** file in the **/flash/switch** directory. This will display the banner before logging in.

The **pre\_banner.txt** can be configured and updated to display customized notice using “vi editor” in the TOE.

The administrator can configure the session inactivity time before session termination or locking. This is achieved through the CLI *session cli timeout <num>* command.

```
-> session cli timeout 5
```

By default, the session inactive time is set to 4 minutes.

The administrator can configure the audit behavior. The audits are part of existing switch log, is achieved through the *swlog {enable | disable | preamble | hash-time-limit seconds | duplicate-detect | console level num }* configurations.

The ability to configure the above management functions is permitted only for administrator or any user having the desired privileges. Administrator privilege can be controlled by modifying privileges (RW/RO) assigned to a user for specific families/domains with the *user <username> [read-only | read-write [families... | domains...| all | none | all-except [families | domains....]]* command.

### 3.4.4 Security management roles (FMT\_SMR)

The administrator must maintain roles, associate users with roles and be able to access the TOE locally and remotely. The OmniSwitch has an **admin** user by default. The **admin** user has all the privileges to manage the switch both remotely and locally. The admin user can create different users in the switch and specific privileges can be assigned to the users (R/W for specific modules) using the *user <username> [read-only | read-write [families... | domains...| all | none | all-except [families | domains....]]* command.

```
-> user cc_user_role read-write domain-system domain-service
```

The OmniSwitch can be administered locally and remotely. The administration is performed using the authenticated switch access. For local authentication use the *aaa authentication console local* command. For remote authentication use the *aaa authentication ssh server1 [server2...]* command.

## 3.5 Protection of the TSF (FPT)

### 3.5.1 Protection of TSF Data (Extended – FPT\_SKP\_EXT)

OmniSwitch prevents reading of all pre-shared keys, symmetric keys and private keys in the CLI prompt. Accessing these files is blocked for all configured administrative users from the CLI prompt.

The usage of “su” command is required to upload and update the CA certs and TOE certificates. However, the usage of “su” prompt is limited only for debugging purpose.

It should be noted that the default “admin” user is considered the privileged administrator and has full administrator privileges for all commands on the TOE. Hence the default “admin” user must be used only to perform installation and initial configuration of the TOE. The general switch administration or management must be performed by the users with appropriate administrative privileges (created by the “admin” user), but not by the default “admin” user.

### 3.5.2 Protection of Administrator Passwords (Extended – FPT\_APW\_EXT)

OmniSwitch supports storing of user password in encrypted form and there by prevent the user reading plain text passwords. In CC evaluated configuration the user passwords are stored using SHA256 algorithm which prevents users from reading the plain text passwords.

### 3.5.3 TSF testing (Extended – FPT\_TST\_EXT)

The TOE runs the individual crypto applications in FIPS mode to achieve the self-test for cryptographic functionality during initial startup (on power on). The individual crypto applications like SSH, and perform the FIPS power on self-test during initialization.

The TOE provides self-tests consistent with the FIPS 140-2 requirements. These self-tests for the cryptographic functions in the TOE are run automatically during power-on as part of the POST.

These self-tests include the following:

- Integrity verification of the shared libraries that comprise the cryptographic module;
- Known Answer Test (KAT) for symmetric encryption and decryption algorithms;
- KAT for the DRBG;
- KAT for MAC and message digest algorithms;
- KAT for RSA signature generation and verification algorithms;
- KAT for the Elliptic Curve Diffie-Hellman algorithm;
- Pair-wise Consistency Tests (PCT) for ECDSA asymmetric algorithms (consisting of performing signature generation and verification for a known ECDSA key).

OpenSSL also performs the following conditional tests during the execution of services:

- PCT on each generation of an RSA key pair, consisting of performing signature generation and verification of a predefined message using the generated RSA key pair, as well as public key encryption and private key decryption of a predefined message using the generated RSA key pair.

- PCT on each generation of an ECDSA key pair, consisting of performing signature generation and verification of a predefined message using the generated ECDSA key pair.

During the system boot up process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component. Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms. In the event of a power-on self-test failure, the cryptographic application will force the TOE (OmniSwitch) to reload and reinitialize the operating system and cryptographic application. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful.

The FIPS self-test does not stop on encountering a failure. It proceeds until all cryptographic functions are tested. The names of failed tests are logged.

For example, assume RSA Signature test and SHA256 hash-based DRBG test fail; the following logs are displayed on the console.

```
Signature RSA test Failed Incorrectly!!
DRBG SHA256 test Failed Incorrectly!!
```

When the power on self-test fail, the following error messages are displayed on the console and the TOE automatically reloads to re-initialize the operating system and cryptographic applications.

```
3062469840:error:2D06B06F:FIPS routines:FIPS_check_incore_fingerprint:fingerprint does not
match:fips.c:232:
3062469840:error:2D079089:FIPS routines:fips_pkey_signature_test:test
failure:fips_post.c:340:Type=SHA1 Digest
3062469840:error:2D079089:FIPS routines:fips_pkey_signature_test:test
failure:fips_post.c:340:Type=SHA1 Digest
3062469840:error:2D079089:FIPS routines:fips_pkey_signature_test:test
failure:fips_post.c:340:Type=SHA1 Digest
3062469840:error:2D080086:FIPS routines:FIPS_selftest_aes:selftest
failed:fips_aes_selftest.c:98:
3062469840:error:2D079089:FIPS routines:fips_pkey_signature_test:test
failure:fips_post.c:340:Type=RSA SHA256 PSS
3062469840:error:2D079089:FIPS routines:fips_pkey_signature_test:test
failure:fips_post.c:340:Type=ECDSA P-224
3062469840:error:2D079089:FIPS routines:fips_pkey_signature_test:test
failure:fips_post.c:340:Type=DSA SHA384
FIPS_mode_set(): failed to enter FIPS mode!
In main, LDAP client enable fips mode failed
Tue Aug 5 15:18:23 : ChassisSupervisor appMgr alert message:
+++ appMgrClientTerminated: restarting task
In main, LDAP client enable fips mode failed
```

### 3.5.4 Trusted Update (FPT\_TUD\_EXT)

OmniSwitch provides the ability to query the currently executing version of the TOE firmware/software as well as the most recently installed version of the TOE firmware/software. This is provided using the various show commands *show microcode [working | certified | loaded | issu | image\_dir]* that display the firmware/software version running on the system.

```
-> show microcode loaded
/flash/working
Package          Release          Size          Description
-----+-----+-----+-----
```

Uos.img 8.9.6.R11 149464428 Alcatel-Lucent OS

OmniSwitch provides the ability to manually initiate and authenticate firmware/software updates to the TOE using a published hash prior to installing those updates.

The software images along with hash file (imgsha256sum) needs to be transferred to OmniSwitch securely using SSH for firmware or software updates. Refer section Download AOS 8.9 R11 (section 2.3.2 above) for downloading software update procedure.

After downloading the hash file (imgsha256sum) the administrator needs to compare the hash value of the file against the hash value published on the support website <https://myportal.al-enterprise.com/s>.

And then use the *image integrity check <image\_dir> key-file <filename>* command to check the integrity of the image files in working or certified directory. This command verifies the SHA256 checksum of the image files against the SHA256 checksum of the image files stored in a file (**imgsha256sum**). The **imgsha256sum** can be downloaded from the Tech Support website: <https://businessportal2.alcatel-lucent.com> along with the images.

```
-> image integrity check working key-file /flash/working/imgsha256sum
This operation may take several minutes...
```

```
SUCCESS: Key matched.
```

The above command verifies the integrity of the images against the published hash. If the verification fails administrator must remove the invalid update from the system. If the verification indicates “Key matched” the update will be applied.

The **imgsha256sum** file must be placed in the same location where the images are stored. During reload the SHA256 checksum of the image files is computed and checked against the SHA256 checksum stored on the file.

```
-> reload from working no rollback-timeout
Confirm Activate (Y/N)
This operation will verify and copy images before reloading.
It may take several minutes to complete....
```

The reload will be successful only when the SHA256 checksum is matched otherwise the reload will be cancelled with an audit message in the swlog.

A sample audit message is as follows:

For a successful system update, no error messages must be witnessed; system update sequence recorded as:

```
2016 Nov 2 16:19:14 OS6860 swlogd: ChassisSupervisor vcReloadMgr info(5) EVENT-AUDIT:
starting reload sequence for image working
```

```
2016 Nov 2 16:19:37 OS6860 swlogd: flashManager FlashMgr Main info(5) EVENT-AUDIT: Verifying
image Integrity on directory working on CMM flash
```

### Image Integrity Failure:

Verification test failure is recorded as:

```
2017 Jan 1 17:08:03 OS6860 swlogd: ChassisSupervisor reloadMgr info(5) EVENT-AUDIT: Verify
of reload image failed - terminating Reload request
```

Below table lists the image types for which validation will be done:

Platform	Image Name	File Format
OS6860N	Uosn.img	imgsha256sum
OS6900-V72/C32	Yos.img	imgsha256sum
OS6860, OS6865	Uos.img	imgsha256sum
OS9900	Mos.img Meni.img Mhost.img	imgsha256sum
OS6465, OS6465T	Nos.img	imgsha256sum
OS6560	Nos.img	imgsha256sum
OS6360	Nosa.img	imgsha256sum

### 3.5.5 Time stamps (FPT\_STM\_EXT)

OmniSwitch must be able to provide reliable time stamps. This is achieved using the *system date <mm/dd/yyyy>*, *system time <hh:mm:ss>*, *system timezone [timezone\_abbrev]*, and *system daylight-savings-time [enable / disable]* commands.

```
-> system date 04/15/2016
-> system time 08:00:00
```

The reliable time stamps set by the administrator is used in the below TOE security functions:

1. All OmniSwitch applications that generate audit events use the time utility to log the time stamp for audit events.
2. Verification of expiration of the certificate in X.509 certificate validation.
3. Calculate the inactivity period of an interactive session to evaluate the termination of local and remote sessions.

## 3.6 TOE Access (FTA)

### 3.6.1 TSF-initiated Session Locking and Termination (Extended – FTA\_SSL\_EXT, FTA\_SSL)

OmniSwitch support ability to lock local and remote interactive sessions by terminating the session after configurable time interval of session inactivity. This is achieved using the *session cli timeout <num>* command; the active session gets terminated after the configured timeout interval is reached.

```
-> session cli timeout 5
```

However, by default the inactivity time for TOE is set at 55 seconds.

OmniSwitch allows the administrator to terminate it's own session upon initiated by the administrator. This is achieved using the CLI *exit* command. The local or remote sessions gets terminated upon the administrator's request.

```
-> exit
```

### 3.6.2 TOE access banners (FTA\_TAB)

Before establishing an administrative user session, OmniSwitch displays an advisory notice and consent warning message regarding use of the TOE on login. This is achieved using the default banner shown on the console with some additional content on the user defined welcome banner configured through CLI *session cli banner <file\_name>* command.

```
-> session cli banner /flash/switch/session_banner.txt
```

Additionally, a notice can be displayed prior to logging in by updating a file name with the name **pre\_banner.txt** file in the **/flash/switch** directory. This will display the banner before logging in.

The **pre\_banner.txt** can be configured and updated to display customized notice using “vi editor” in the TOE.

## 3.7 Trusted path/channels (FTP)

### 3.7.1 Trusted path (FTP\_TRP.1)

OmniSwitch can use SSH to provide a communication path between itself and authorized remote administrator users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

OmniSwitch permits remote users and administrators to initiate communication through the trusted path. Configure through CLI *ssh {port [default / service\_port] / admin-state [enable / disable] / ip\_address}* command.

```
-> ssh port 20000 admin-state enable
```

### 3.7.2 Trusted Channel (FTP\_ITC.1)

OmniSwitch is capable of using TLS to provide a trusted communication channel between itself and another trusted IT product authorized IT entities supporting the audit server that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure and detection of modification of the channel data.

OmniSwitch shall initiate communication via the trusted channel for sending audit records to the external syslog server. Configure through CLI *swlog output socket <domain\_name> tls* command.

```
-> swlog output socket opendaylight.com tls
```

For a successful TLS connection establishment, following pre-requisites must be fulfilled and ensured.

- 1) OmniSwitch must be configured for Common Criteria mode
  - Command “**aaa common-criteria admin-state enable|disable**” will enable/disable CC mode as required, followed by a device/stack reboot to activate respective mode(s).
- 2) Generation of client certificate and private key, perform the following **060859-00\_8 9 R11\_OS\_Family\_CC\_Preparation\_and\_Operational\_Guidance** documentation, sections **3.3.6**
- 3) Client certificates must be generated and placed under **/flash/switch/cert.d** directory (if not available already)
  - Client Certificate be placed as **/flash/switch/cert.d/myCliCert.pem** and Client Private Key file be placed as **/flash/switch/cert.d/myCliPrivate.key**.
- 4) CA bundle must be updated with CA certificate under **/flash/switch/ca.d** directory (if not available already)
  - Command “**aaa certificate update-ca-certificate <CA\_CERT\_FILE>**” to update CA certificate into the OmniSwitch’s CA bundle

Also, TLS connection will be established only upon successful certificate validation. This x509 certificate validation involves CA certificates as well. Any valid CA certificate must follow below pre-requisites:

- 1) CA certificate must contain CA flag set to “**TRUE**” in the basic constraints extension for the certificate.
- 2) CA certificate must contain basic constraints extension and be set to “**critical**”.

OmniSwitch TLS clients establish secure connection over TLS with the Syslog servers. When the TLS connection is broken, syslog client application will try to re-establish the connection with the external server at regular time intervals. Audit data generated during the time when connection is down will be stored only locally and not sent to the audit server.