Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6

CC Configuration Guide

Version: 0.8
Date: February 10, 2023

Table of Contents

Document Introduction

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides Guidance to IT personnel for the TOE, Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6. This Guidance document includes instructions to successfully install the TOE in the Operational Environment, instructions to manage the security of the TSF, and instructions to provide a protected administrative capability.

Revision History

Version	Date	Change
0.1	July 15, 2020	Initial Version
0.2	February 11, 2021	Initial Updates
0.3	August 9, 2021	Update to 17.6.1
0.4	February 24, 2022	Updates to address ORs
0.5	September 7, 2022	Updates to finalize AGD
0.6	November 8, 2022	Updates to address CBOR3
0.7	January 12, 2023	Updates to address ATE CBOR4
0.8	February 10, 2023	Updates to address final ORs

Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Wireless LAN TOE, as it was certified under Common Criteria. The Wireless LAN may be referenced below by the related acronym e.g. WLAN or simply the TOE.

Audience

This document is written for administrators installing and configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining Wireless LAN operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

Document References

This section lists the Cisco Systems documentation that is also a portion of the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 1. Throughout this document, the guides will be referred to by the "#", such as [1].

Table 1 Cisco Documentation

#	Title	Link
1	Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L.html
2	Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40.html
3	Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-80/installation-guide/b-wlc-ig-9800-80.html
4	Cisco Catalyst 9800-CL Private Cloud Wireless Controller Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-cloud/installation/b-c9800-cl-install-guide.html
5	Cisco Catalyst C9800-CL Wireless Controller Virtual Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_virtual_dg.html
6	Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg.html
7	Cisco Catalyst 9800 Wireless Controller Series Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_cisco_catalyst_9800_wireless_controller_series_dg.html

#	Title	Link
8	Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide	https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-4/deployment-guide/c9800-webui-dg.pdf
9	Understanding Catalyst 9800 Wireless Controllers Configuration Model	https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html
10	Understand FlexConnect on Catalyst 9800 Wireless Controller	https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html
11	C9800 Radio Resource Management Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_C9800_rrm_dg.html
12	Security Configuration Guide, Cisco IOS XE Gibraltar 17.4.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-4/configuration_guide/sec/b_174_sec_9500_cg.html
13	Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/cmd-ref/b_wl_17_6_cr.html
14	Cisco Catalyst 9130AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9130ax/quick/guide/ap9130ax-getstart.html
15	Cisco Catalyst 9120AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9120ax/quick/guide/ap9120ax-getstart.html
16	Cisco Catalyst 9115AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9115ax/quick/guide/ap9115ax-getstart.html
17	Cisco Catalyst 9105AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9105ax/quick/guide/ap9105axi-getstart.html
18	Cisco Catalyst IW6300 Heavy Duty Series Access Point Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw6300/hardware/install/guide/b_iw6300_hig.html
19	Cisco ESW6300 Embedded Services Access Point	https://www.cisco.com/c/en/us/products/collateral/wireless/6300-series-embedded-services-access-points/guide-c07-742909.html
20	Cisco Aironet 1560 Series Outdoor Access Point Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1560/installation/guide/1560hig.html
21	Getting Started Guide - Cisco Aironet 2800 Series Access Points	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/2800/quick/guide/ap2800iegetstart.html
22	Getting Started Guide - Cisco Aironet 3800 Series Access Points	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/3800/quick/guide/ap3800iepgetstart.html
23	Cisco Aironet Series 2800/3800 Access Point Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_aironet_series_2800_3800_access_point_deployment_guide.html
24	Cisco Aironet 4800 Series Access Points Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/4800/quick/guide/ap4800getstart.html

#	Title	Link
25	Cisco Aironet Series 4800 Access Point Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_cisco_aironet_series_4800_acces_point_deployment_guide.html
26	Cisco Catalyst 9130 Series Access Point Deployment Guide	https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-3/deployment-guide/c9130-ap-dg.pdf
27	Security for VPNs with IPsec Configuration Guide, Cisco IOS XE 17	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-17/sec-sec-for-vpns-w-ipsec-xe-17-book.html
28	Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/release-notes/rn-17-6-9800.html

TOE Overview

The TOE combines Wireless LAN Controllers and Access Points to create a WLAN Access System. The Wireless LAN Controller manages the Access Points which provide users secure over-the-air access to an organization's network.

Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

Table 2. Operational Environment Components

Component	Usage/Purpose Description
Wireless Client	Allows users to establish wireless communications with an organization's private network through the TOE.
EST Server	The EST Server[1] authenticates EST Clients and determines if the EST Client is authorized to receive the certificate it has requested.
Certificate Authority	The Certification Authority is used to provide the TOE, Authentication Server, and Wireless clients with valid certificates. The CA also provides the TOE with a method to check the revocation status of peer certificates the TOE communicates with on the wired network.
RADIUS Authentication Server	The purpose of the RADIUS Authentication Server is to authenticate wireless clients using EAP-TLS. FreeRADIUS 3.0.x or higher is required in the IT environment to support RADIUS over TLS (RADsec).
Management Workstation	This includes any IT Environment Management workstation with a TLS web browser client or SSH client installed that is used by the Security Administrator for remote administration over TLS or SSH trusted paths.

[1] Refer to RFC 7030 for additional information on EST Server

Local Console	This is an IT Environment Console that is directly connected to the Wireless LAN Controller TOE component via the Serial Console Port or Auxiliary Port and is used by the Security Administrator for local TOE administration.
Syslog Server	This includes any syslog server to which the TOE would transmit syslog messages over a trusted channel.
Cisco UCS C-Series M5 Rack Servers (applies only to the Cisco Catalyst 9800-CL Wireless Controller for Private Cloud - vSphere)	Provides the Virtualisation System (VS) including the hypervisor, physical chassis, and supporting software.
DHCP Server (Optional)	Use of a DHCP server allows the AP to automatically discover the IP address of the controller to which it joins.

Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

Table 3. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 and CC mode of operation	The TOE includes FIPS and CC modes of operation. The FIPS modes allows the TOE to use only approved cryptography and CC mode removes the ability to use PFS ciphersuites for DTLS. FIPS and CC modes of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
WPA and WPA2 with TKIP encryption	Only WPA2-Enterprise along with 802.1X with AES encryption will meet the requirements of the WLAN AS EP.
Cisco Catalyst 9800-CL for public cloud	The Cisco Catalyst 9800-CL for public cloud is an Infrastructure-as-a-Service (IaaS) solution available on the Amazon Web Services (AWS) and Google Cloud Platform (GCP) Marketplace. The Cisco Catalyst 9800-CL for public cloud solution is excluded from the evaluation.
Cisco CleanAir	Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum.

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2 or the WLAN Access System Extended Package v1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

Evaluated Configuration

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 TOE is distributed. Deployment of the TOE in its evaluated configuration consists of at least one Wireless LAN Controller (WLC) model and at least one Access Point (AP) model specified in table 3 of the Security Target. Extra instances of a WLC or AP TOE component are permitted in the evaluated configuration. If the Security Administrator installs an extra instance of a WLC or AP TOE component the respective sections of this AGD must be applied.

TOE Acceptance

The administrator should perform the following actions to ensure the TOE is correct and that it has not been tampered with during delivery.

1. Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

2. Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

3. Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

4. Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

5. Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

6. Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Installation

Wireless LAN Controller

If you are installing the hardware Wireless Controllers (Cisco Catalyst 9800-L, Cisco Catalyst 9800-40, or Cisco Catalyst 9800-80) refer to the instructions in the chapters listed below from the Hardware Installation Guide for your model [**1**], [**2**], or [**3].**

- Overview
- Supported Hardware Components
- Preparing Your Site for Installation
- Installing the Controller

If you are installing the virtual Wireless Controllers (Cisco Catalyst 9800-CL) refer to the instructions in the chapters listed below from the Cisco Catalyst 9800-CL Private Cloud Wireless Controller Installation Guide in [**4**]**.**

- Overview
- Installing Controller in VMware Environment

Additionally refer to the instructions for the virtual Wireless Controllers including preparing for VMware networking in the Wireless Controller Virtual Deployment Guide, [**5**].

Note: For virtual Wireless Controller (Cisco Catalyst 9800-CL) deployments the CC evaluated configuration requires there must be only one vND instance for each physical UCS C220-M5SX platform and there must be no other guest VMs on the UCS C220-M5SX platform providing non-network device functionality.

Wireless Access Points

The Administrator must read and follow the Getting Started Guide and/or Hardware Installation Guides for your AP model. Before proceeding the administrator must read and understand the Regulatory Information, Safety Guidelines, and Warnings contained in each guide.

Warning: The administrator needs to verify that the AP model is approved for use in the country. To verify approval and to identify the regulatory domain that corresponds to a particular country, visit http://www.cisco.com/go/aironet/compliance

Site Survey

Before installing wireless access points, the administrator should perform a site survey to determine the optimum use of networking components and to maximize range, coverage, and network performance.

Site surveys reveals problems that can be resolved before the network is operational. Because 802.11a/b/g/n operates in an unlicensed spectrum, there may be sources of interference from other 802.11a wireless devices (especially in multi-tenant buildings) that could degrade your 802.11 signals. A site survey can determine if such interference exists at the time of deployment.

A proper site survey involves temporarily setting up mesh links and taking measurements to determine whether your antenna calculations are accurate. Determine the correct locations and antenna types before you drill holes and route cables and mounting equipment.

Consider the following operating and environmental conditions when performing a site survey:

1. Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
2. Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary, because the extra height also increases potential interference from other unlicensed radio systems and decreases the wireless coverage from the ground.
3. Physical environment—Clear or open areas provide better radio range than closed or filled areas.
4. Obstructions—Physical obstructions such as buildings, trees, or hills can hinder performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.

5. How far is your wireless link?
6. Has a previous site survey been conducted?
7. Do you have a clear Fresnel zone between the access points or radio line of sight?
8. What is the minimum acceptable data rate within the link?
9. Do you have the correct antenna (if more than one antenna is being offered?)
10. Do you have access to both of the mesh site locations?
11. Do you have the proper permits, if required?
12. Are you following the proper safety procedures and practices?
13. Have you configured the access points before you go onsite? It is always easier to resolve configurations or device problems first.
14. Do you have the proper tools and equipment to complete your survey?

Procedures and Operational Guidance for IT Environment

To operate in its evaluated configuration, the TOE requires:

- FreeRADIUS 3.0.x or higher is required to support RADsec over TLS and centralized authentication of wireless clients using EAP-TLS. Install FreeRADIUS and configure to support RADsec over TLS as per FreeRADIUS documentation. The contents below is complementary to the FreeRADIUS documentation. It provides a minimum configuration needed to support RADsec and EAP-TLS.

    a. RADsec configuration: Below is a sample tls virtual server located in the /etc/freeradius/3.0/sites-available directory. At a minimum ensure the contents of private_key_password, private_key_file, certificate_file, ca_file, and IP addresses are configured for your environment.

```
server {
       listen {
              ipaddr = *
              port = 2083
              type = auth
              proto = tcp
              clients = radsec

              limit {
              max_connections = 16
              lifetime = 0
              idle_timeout = 30
              }

              tls {
                     #private_key_password = whatever
                     private_key_file = /etc/freera-
                     dius/3.0/certs/radsec_server_key.pem
                     certificate_file = /etc/freeradius/3.0/certs/radsec_server.pem
                     ca_file = /etc/freeradius/3.0/certs/ca-certs.pem
                     dh_file = ${certdir}/dh
                     random_file = /dev/urandom
                     fragment_size = 8192
                     ca_path = ${cadir}
                     cipher_list = "HIGH"
                     cipher_server_preference = no

                     cache {
                     enable = no
                     lifetime = 24 # hours
                     }
                     require_client_cert = yes
              }
       }
       authorize {
              preprocess
              eap {
                     ok = return
              }
              expiration
              logintime
       }
       authenticate {
              eap
```

```
        }
        preacct {
                preprocess
                acct_unique
                suffix
                files
        }
        accounting {
                detail
                # unix
                radutmp
                # exec
                attr_filter.accounting_response
                }
        session {
                radutmp
         }
        post-auth {
                # exec
                Post-Auth-Type REJECT {
                        attr_filter.access_reject
                        }
         }
        pre-proxy {

         }
        post-proxy {
        eap
         }
}

clients radsec {
        client C9800 {
                ipaddr = <C9800 WLC IP Address>
                secret = radius/dtls
                nastype = "other"
                require_message_authenticator = no
                proto = tls

        }
}

home_server myradsec {
        ipaddr = <FreeRADIUS/RADsec IP Address>
        port = 2083
        type = auth
        secret = radius/dtls
        proto = tcp
        status_check = none

        tls {
                #private_key_password = whatever
                private_key_file = /etc/freeradius/3.0/certs/radsec_server_key.pem
                certificate_file = /etc/freeradius/3.0/certs/radsec_server.pem
```

```
                ca_file = /etc/freeradius/3.0/certs/ca-certs.pem
                dh_file = ${certdir}/dh
                random_file = /dev/urandom
                fragment_size = 8192
                ca_path = ${cadir}
                cipher_list = "HIGH"
        }

}

home_server_pool mypool {
                type = fail-over
                home_server = myradsec
}

realm tls {
       auth_pool = mypool
}
```

b. EAP-TLS: Below is a sample eap module that supports eap-tls only. The eap module located in the /etc/freeradius/3.0/mods-enabled directory. At a minimum ensure the contents of private_key_password, private_key_file, certificate_file, and ca_file are configured for your environment.

```
        eap {
                default_eap_type = tls
                timer_expire     = 60
                ignore_unknown_eap_types = no
                cisco_accounting_username_bug = no
                max_sessions = ${max_requests}

                tls-config tls-common {
                        private_key_password = whatever
                        private_key_file = ${certdir}/eap_server_key.pem
                        certificate_file = ${certdir}/eap-server.crt
                        ca_file = ${cadir}/ca-certs.pem
                        dh_file = ${certdir}/dh
                        ca_path = ${cadir}
                        cipher_list = "HIGH"
                        cipher_server_preference = no
                        ecdh_curve = "prime256v1"

                        cache {
                                enable = no
                                lifetime = 24 # hours
                                name = "EAP-TLS"
                                persist_dir = "${logdir}/tlscache"
                        }
                        verify {
                                tmpdir = /tmp/radiusd
                                client = "/usr/bin/openssl verify -CAfile /etc/freera-
        dius/3.0/certs/ca-certs.pem %{TLS-Client-Cert-Filename}"
                        }

                        ocsp {
                                enable = no
```

```
                override_cert_url = yes
                url = "http://127.0.0.1/ocsp/"
        }
    }

    tls {
        tls = tls-common
    }
}
```

c. Clients.conf: Below is the contents of a sample clients.conf located in the /etc/freeradius/3.0 directory:

```
client  C9800 {
    ipaddr = <IP Address of C9800 WLC>
    secret = radius/dtls
    nastype = "other"
    require_message_authenticator = yes
}
```

d. Additional FreeRADIUS configuration:

i. Create /tmp/radiusd

```
# cd tmp

# mkdir radiusd
```

ii. Change owner of /tmp/radius to freerad:

```
# chown -hR freerad /tmp/radiusd
```

iii. Change directory to: /etc/freeradius/3.0/sites-enabled/

```
# cd /etc/freeradius/3.0/sites-enabled/
```

iv. Remove all default servers in /etc/freeradius/3.0/sites-enabled/. If you need any of the default servers in the future make a backup copy before deleting.

```
# rm *
```

v. Create a symbolic link to the tls virtual server that is located in site-available:

```
# ln -s ../sites-available/tls ./tls
```

vi. Start FreeRADIUS in debug mode: service freeradius debug-threaded

```
# service freeradius debug-threaded
```

vii. Review for errors and correct until it says “Ready to process requests”

viii. To stop FreeRADIUS

```
# service freeradius stop
```

ix. To start FreeRADIUS without debug output

```
# service freeradius start
```

- Syslog Server. Any syslog server that can be accessed over IPsec may be used. Install the syslog server per installation instructions provided with the syslog server software. Configure the host operating system to restrict access to syslog data to authorized personnel only. Configure the system to accept inbound syslog over a IPsec from each WLAN Controller.

- Certificate Authority and Server that supports EST. An EST capable Certificate Authority and EST Server is required to support automated certificate enrollment. Third-party Certificate Authorities that support EST include CertAgent from Information Security Corporation and EJBCA Enterprise from PrimeKey.

Preparative Procedures and Operational Guidance for the TOE

Controller — Power Up

Warning: IMPORTANT SAFETY INSTRUCTIONS

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

1. If you are powering up the hardware Controller, move the chassis power switch to the ON position. Listen for the fans; you should immediately hear them operating. Ensure that the power supply LED OK is green and the FAIL LED is not illuminated. The front-panel indicator LEDs provide power, activity, and status information useful during bootup. For more detailed information about the LEDs, see the LEDs section in the Hardware Installation Guide.

2. Observe the initialization process. When the system boot is complete (the process takes a few seconds), the controller begins to initialize.

   ```
   Loading from ROMMON with a System Image in Bootflash
   ```

3. When initialization has completed, the following will be displayed:

   ```
   Press RETURN to get started!
   ```

Virtual Controller — Power Up

1. If you have the virtual controller select the VM within VMware vSphere and click Power On. The VM starts the launch process. After the VM is launched, the controller starts the boot process.

Virtual Controller — Initial Configuration

1. The administrator will be prompted to enter the initial configuration dialog. Enter no and confirm you would like to terminate auto install. The CC Configuration will use manual steps to provide the initial configuration.

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]:yes

Press RETURN to get started!
```

2. Enter privilege EXEC mode

```
WLC> enable
```

3. Enter configure terminal

```
WLC# configure terminal
```

4. Configure a hostname

```
WLC(config)# hostname myWLC
```

5. Configure the Enable Secret Password using Type 8 or Type 9

    a. Configure the Enable Secret Password using Type 8:

```
WLC(config)# enable algorithm-type sha256 secret <the unencrypted (cleartext)
'enable' secret>
```

    b. Configure the Enable Secret Password using Type 9:

```
WLC(config)# enable algorithm-type scrypt secret <the unencrypted (cleartext)
'enable' secret>
```

Note: Compose a password with a length between 8 and 16 using any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)

6. Provide an initial configuration for the Out-of-Band Management Interface:

Note: When deploying the virtual Controller using the OVA template, the VM will bootstrap with three interfaces: The G1 interface is for out of band management, G2 is for wireless management (usually mapped to a trunk interface on the switch side) and the third one, G3, is for HA to connect to the SSO peer.

    a. Configure the Gigabit Ethernet 1 interface for Out-of-Band Management:

```
WLC(config)# interface GigabitEthernet1

WLC(config-if)# ip address <IP address> <mask>

WLC(config-if)# no shutdown

WLC(config-if)# exit
```

    b. Configure a default route to reach the Controller. Verify that you can ping the out-of-band management interface from the network where you will manage the Controller

```
WLC(config)# ip route <prefix> <mask> <ip-address>
```

7. Provide an initial configuration for the Wireless Management Interface:

Note: The Cisco Catalyst 9800-CL Wireless Controller provides a ‘Day 0’ Express Setup for first time out of box installation and configuration. This CC Configuration Guide will not use the ‘Day 0’ Express Setup.

Note: The VLAN ID you use in this section needs to be consistent.

a. Configure the VLAN for Wireless Management Interface

```
WLC(config)# vlan <VLAN ID 1-4094>
WLC(config-vlan)# name wireless_management
WLC(config-vlan)# exit
```

b. Configure the SVI for Wireless Management Interface

```
WLC(config)# interface vlan <VLAN ID 1-4094>
WLC(config-if)# ip address <IP address> <mask>
WLC(config-if)# no shutdown
WLC(config-if)# exit
```

c. Specify the SVI for the wireless management interface

```
WLC(config)# wireless management interface <vlan ID>
```

d. Configure the Gigabit Ethernet 2 interface as trunk

```
WLC(config)# interface GigabitEthernet2
WLC(config-if)# switchport mode trunk
WLC(config-if)# switchport trunk allowed <VLAN ID 1-4094>
WLC(config-if)# shutdown
WLC(config-if)# no shutdown
```

e. Configure a default route to reach the Controller. Verify that you can ping the wireless management interface from the network where APs and network services are deployed.

```
WLC(config)# ip route <prefix> <mask> <ip-address>
```

f. Disable the radios

```
WLC(config)# ap dot11 5ghz shutdown
WLC(config)# ap dot11 24ghz shutdown
```

g. Configure the AP country domain. For example, ap country US

```
WLC(config)# ap country <country code>
```

Note: Ensure the Country Code is capitalized

h. Enable the radios

```
WLC(config)# no ap dot11 5ghz shutdown
WLC(config)# no ap dot11 24ghz shutdown
```

8. Save the initial configuration to nvram by executing “wr mem” or “copy system:running-config nvram:startup-config” command.

Physical Controller — Initial Configuration

1. The administrator will be prompted to enter the initial configuration dialog. Enter no and confirm you would like to terminate autoinstall. The CC Configuration will use manual steps to provide the initial configuration.

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]:yes

Press RETURN to get started!
```

2. Enter privilege EXEC mode

```
WLC> enable
```

3. Enter configure terminal

```
WLC# configure terminal
```

4. Configure a hostname

```
WLC(config)# hostname myWLC
```

5. Configure the Enable Secret Password using Type 8 or Type 9

    a. Configure the Enable Secret Password Using Type 8:

```
WLC(config)# enable algorithm-type sha256 secret <the unencrypted (cleartext)
'enable' secret>
```

    b. Configure the Enable Secret Password Using Type 9:

```
WLC(config)# enable algorithm-type scrypt secret <the unencrypted (cleartext)
'enable' secret>
```

Note: Compose a password with a length between 8 and 16 using any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)

6. Provide an initial configuration for the Out-of-Band Management Interface:

```
WLC(config)# interface GigabitEthernet1

WLC(config-if)# ip address <IP address> <mask>

WLC(config-if)# no shutdown

WLC(config-if)# exit
```

7. Configure a default route to reach the Controller. Verify that you can ping the out-of-band management interface from the network where you will manage the Controller

```
WLC(config)# ip route <prefix> <mask> <ip-address>
```

8. Provide an initial configuration for the Wireless Management Interface:

Note: The Cisco Catalyst 9800 Wireless Controller provides a ‘Day 0’ Express Setup for first time out of box installation and configuration. This CC Configuration Guide will not use the ‘Day 0’ Express Setup.

Note: The VLAN ID you use in this section needs to be consistent.

i. Configure the VLAN for Wireless Management Interface

```
WLC(config)# vlan <VLAN ID 1-4094>
```

```
WLC(config-vlan)# name wireless_management
WLC(config-vlan)# exit
```

j. Configure the SVI for Wireless Management Interface

```
WLC(config)# interface vlan <VLAN ID 1-4094>
WLC(config-if)# ip address <IP address> <mask>
WLC(config-if)# no shutdown
WLC(config-if)# exit
```

k. Specify the SVI for the wireless management interface

```
WLC(config)# wireless management interface <vlan ID>
```

l. Configure a Gigabit Ethernet interface (with connectivity to Access Points) as trunk

```
WLC(config)# interface TwoGigabitEthernet0/0/0
WLC(config-if)# switchport mode trunk
WLC(config-if)# switchport trunk allowed <VLAN ID 1-4094>
WLC(config-if)# shutdown
WLC(config-if)# no shutdown
```

m. Configure a default route to reach the Controller. Verify that you can ping the wireless management interface from the network where APs and network services are deployed.

```
WLC(config)# ip route <prefix> <mask> <ip-address>
```

n. Disable the radios

```
WLC(config)# ap dot11 5ghz shutdown
WLC(config)# ap dot11 24ghz shutdown
```

o. Configure the AP country domain. For example, ap country US

```
WLC(config)# ap country <country code>
```

Note: Ensure the Country Code is capitalized

p. Enable the radios

```
WLC(config)# no ap dot11 5ghz shutdown
WLC(config)# no ap dot11 24ghz shutdown
```

9. Save the initial configuration to nvram by executing “wr mem” or “copy system:running-config nvram:startup-config” command.

Configure Time and Date

Note: The remainder of this document applies to both physical and virtual controllers.

Perform the following to configure time and date.

1. Enter enable and then enter configuration mode.

```
WLC> enable

WLC# configure terminal
```

2. Configure the time zone. The zone argument is the name of the time zone (typically a standard acronym). The hours-offset argument is the number of hours the time zone is different from UTC. The minutes-offset argument is the number of minutes the time zone is different from UTC. For example clock timezone EST -5

```
WLC(config)# clock timezone zone-hours-offset [minutes-offset]
```

3. Configure daylight savings time in areas where it starts and ends on a particular day of the week each year. The offset argument is used to indicate the number of minutes to add to the clock during summer time. For example clock summer-time PST recurring 1 monday january 12:12 4 Tuesday december 12:12 120

```
WLC(config)# clock summer-time zone recurring [week day month hh : mm week day month hh :
mm [offset]]
```

4. Configure a specific summer time start and end date. The offset argument is used to indicate the number of minutes to add to the clock during summer time. For example clock summer-time PST date 1 january 1999 12:12 4 december 2001 12:12 120

```
WLC(config)# clock summer-time zone date month year hh:mm date month year hh : mm
[offset]1:5
```

5. Configure Calendar time authoritative.

```
WLC(config)# clock calendar-valid
```

6. Return to privileged EXEC mode.

```
WLC(config)# end
```

7. Set the clock using the clock set command. For example clock set 12:12:12 1 january 2011

```
WLC# clock set hh : mm : ss date month year
```

Enable Configuration Change Notification and Logging

The Configuration Change Notification and Logging feature tracks changes made to the Cisco software running configuration. Perform the following steps to ensure all required audit events are logged.

1. Ensure logging is enabled

```
WLC(config)#logging on
```

2. Enter archive config mode

```
WLC(config)# archive
```

3. Enter logging config sub-mode

```
WLC(config-archive)# log config
```

4. Enable the config logger

```
WLC(config-archive-log-cfg)# logging enable
```

5. Suppress password when displaying logged commands

```
WLC(config-archive-log-cfg)# hidekeys
```

6. Enter the number of entries to be retained. The range is from 1 to 1000; the default is 100

```
WLC(config-archive-log-cfg)# logging size <1-1000>
```

7. Enable sending of logged commands to remote syslog server

```
WLC(config-archive-log-cfg)# notify syslog
```

8. Exit configuration mode and return to privileged EXEC mode

```
WLC(config-archive-log-cfg)# end
```

Configure Embedded Event Manager (EEM)

To capture audit events for Common Criteria the following Cisco Embedded Event Manager script should be used. Enter it at the CLI as follows:

```
WLC(config)# event manager applet ca_cert_check

WLC(config-applet)# event syslog pattern "CRYPTO_PKI: status = 65535: failed to insert CA
cert"

WLC(config-applet)# action 1.0 syslog msg "CRYPTO_PKI: status = 65535: failed to insert CA
cert.  It is not a CA certificate."

WLC(config-applet)# exit

WLC(config)# end

WLC#

WLC# config t

WLC(config)#event manager applet cli_log

WLC(config-applet)#event cli pattern "clear log" mode "exec" enter

WLC(config-applet)#action 0010 syslog msg "User:$_cli_username administratively cleared
message log"

WLC(config-applet)#exit

WLC(config)#end

WLC#set platform software trace all verbose

WLC#config t

WLC(config)# event manager applet tlss_log

WLC(config-applet)# event timer watchdog time 60

WLC(config-applet)# action 0010 cli command "enable"

WLC(config-applet)# action 0020 cli command "show logging process nginx internal start
last 90 seconds level verbose | in while SSL handshaking"
```

```
WLC(config-applet)# action 0030 regexp ".*(SSL_do_handshake).*" "$_cli_result"
WLC(config-applet)# action 0040 if $_regexp_result eq 1
WLC(config-applet)# action 0050 syslog msg $_cli_result
WLC(config-applet)# action 0060 end
WLC(config-applet)#exit
WLC(config)#end
```

Configure Local Logging Buffer Size

Configure the size of the local logging buffer. The local logging buffer size can be configured in a range of 4096 (default) to 2,148,483,647bytes. **Note:** It is recommended to not make the buffer size too large because the TOE could run out of memory for other tasks. It is recommended to set it to at least 150000000

```
WLC(config)# logging buffer 150000000
```

If the local storage space for audit data is full the TOE will overwrite the oldest audit record to make room for the new audit record.

Generate Logs on Failed Login Attempts

To generate logs for failed login attempts enter

```
WLC(config)# login on-failure log
```

Include Date on Audit Records

To include the year with the time stamp on all audit records in the message log enter:

```
WLC(config)# service timestamps log datetime year
```

Generate Logs on Successful Login Attempts

To generate logs for successful login attempts enter

```
WLC(config)# login on-success log
```

Set Syslog Server Logging Level

Set syslog server logging level to debug

```
WLC(config)# logging trap debugging
```

Generate PKI Validation Logs

1. To generate logs for PKI validation enter

   ```
   WLC# debug crypto pki validation
   ```

2. To generate logs for PKI transactions enter

   ```
   WLC# debug crypto pki transactions
   ```

Configure Local Authentication

1. To enable the authentication, authorization, and accounting (AAA) access control model, issue the aaa new-model command in global configuration mode.

   ```
   WLC(config)# aaa new-model
   ```

2. To set the default authentication at login to use local authentication use the aaa authentication login command

   ```
   WLC(config)# aaa authentication login default local
   ```

3. To set the default authorization method to use local credentials use the aaa authorization exec command

   ```
   WLC(config)# aaa authorization exec default local
   ```

4. To set the credential for AP authorization list enter

   ```
   WLC(config)# aaa authorization credential-download default local
   ```

5. To set the default authentication for the WebGUI use the ip http authentication aaa command

   ```
   WLC(config)# ip http authentication aaa
   ```

Configure Authentication Failure

To block brute-force attack attempts, the Controller needs to be configured for authentication failure. The administrator needs to define the maximum number of failed login attempts within a time period. In addition, the administrator needs to define the time period to ban an offending account.

1. Specify the value for maximum number of failed attempts within a time period (seconds), and the time period (seconds) to ban an offending account.

   ```
   WLC(config)# aaa authentication rejected <1-25> in <1-65535> ban <1-65535>
   ```

   For example, to block accounts for 10 minutes after 5 failed login attempts within one 1 hour, enter:

   ```
   aaa authentication rejected 5 in 3600 ban 600
   ```

2. Exit configuration mode and return to privileged EXEC mode

   ```
   WLC(config)# end
   ```

Define Password Policy

Administrators must define a “aaa common-criteria policy” and apply the policy to each local account. This ensures password changes will prompt for your old password before allowing a new password and will also ensure passwords contain a minimum of 8 characters.

1. Create the AAA security password policy and enter common criteria configuration policy mode.

   ```
   WLC(config)# aaa common-criteria policy <policy name>
   ```

2. Set the minimum length for passwords

   ```
   WLC(config-cc-policy)# min-length <8-16>
   ```

3. Set a password lifetime appropriate for your organization. If you do not specify a password lifetime, the WebGUI will remind you to set one each time upon login. To set a password lifetime of 90 days enter:

   ```
   WLC(config-cc-policy)# lifetime day 90
   ```

   When the password expires the user will prompted to perform a password change.

4. Type exit to return to the main configuration mode.

```
WLC(config-cc-policy)# exit
```

5. To verify the Common Criteria password policy enter

```
WLC(config)# show aaa common-criteria policy <policy name>
```

Add Administrator Account

The administrator should create and use a new account that has the Common Criteria Password Policy applied. To add an administrative account use the username command in configuration mode. You will need to specify the Common Criteria Password Policy.

```
WLC(config)# username <user> privilege 15 common-criteria-policy <policy name> algorithm-type <sha256 | scrypt> secret password <the unencrypted (cleartext) password for the user>
```

Passwords may be composed of any combination of upper and lower case letters, numbers, and the following special characters:

Table 4. Password Special Characters

Special Character	Name
!	Exclamation
@	At sign
#	Number sign (hash)
$	Dollar sign
%	Percent
^	Caret
&	Ampersand
*	Asterisk
(	Left parenthesis
)	Right parenthesis
	Space
;	Semicolon
:	Colon
"	Double Quote
‘	Single Quote
|	Vertical Bar
+	Plus
-	Minus
=	Equal Sign

.	Period
,	Comma
/	Slash
\	Backslash
<	Less Than
>	Greater Than
_	Underscore
`	Grave accent (backtick)
~	Tilde
{	Left Brace
}	Right Brace

Increase Privilege Level

The TOE requires all Admin users to have full level 15 privileges. If an organization wishes to create Admin users without level 15 privileges, the Security Administrator will need to run the following command:

```
WLC(config)# privilege exec level 15 show tech-support unprivilege wireless
```

This will address an issue with the "show tech-support unprivilege wireless" command that provides users without level 15 access additional configuration privileges.

Session Termination

All sessions at the local console and auxiliary port must terminate after an Administrator specified time interval of session inactivity has elapsed. **Note:** The auxiliary port is not available on the Catalyst 9800-CL (vSphere).

Use the steps below to configure the time interval.

1. Enter the line configuration mode for console.

```
WLC(config)# line console 0
```

2. Specify the timeout value in minutes. The range is from 0 to 35791.

```
WLC(config-line)# exec-timeout <time in minutes>
```

3. Enter the line configuration mode for aux port:

```
WLC(config-line)# line aux 0
```

4. Specify the timeout value in minutes. The range is from 0 to 35791.

```
WLC(config-line)# exec-timeout <time in minutes>
```

Access Banner

The administrator should configure an initial banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the Controller. The banner will display on the CLI, SSH, and HTTPS interface prior to allowing any administrative access.

To configure an access banner, follow the steps below

1. In privilege EXEC mode, enter configure terminal

   ```
   WLC# config terminal
   ```

2. Enter the banner text using 'banner login delimiter message delimiter' format. Do not use " or % as a delimiting character. White space characters will not work.

   ```
   WLC(config)# banner login z <message text> z
   ```

   Message text. The text is alphanumeric, case sensitive, and can contain special characters. It cannot contain the delimiter character you have chosen. The text has a maximum length of 80 characters and a maximum of 40 lines.

   To clear a login banner use "no login banner"

Verify TOE Software

The TOE ships with the correct software image pre-installed however this may not be the CC validated version. Follow the steps below to verify if you have the CC validated version.

1. Enter show version and verify the version is 17.6

   ```
   WLC# show version | include Software
   ```

2. If the version is not 17.6 you will need to obtain the 17.6 software image. Navigate to Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account and download the 17.6 image for your Controller platform.

Table 5. Evaluated Software Images

Platform	Image
Cisco Catalyst 9800-L	C9800-L-universalk9_wlc.17.06.01.SPA.bin
Cisco Catalyst 9800-40	C9800-40-universalk9_wlc.17.06.01.SPA.bin
Cisco Catalyst 9800-80	C9800-80-universalk9_wlc.17.06.01.SPA.bin
Cisco Catalyst 9800 Wireless Controller for Private Cloud - VMware ESXi	C9800-CL-universalk9.17.06.01.ova

The AP software images v17.6.01 are embedded in each WLC v17.06.01 image and are not separately downloaded and installed.

Upgrade TOE Software

1. Place the downloaded image on a TFTP, FTP, or SFTP server that is reachable by the WLC.

2. At the WLC console enter: `install add file [tftp | ftp | sftp://<IP Address of TFTP/FTP/SFTP server>] <image name.bin> activate commit`

Note: Upon installation, the WLC extracts sub-packages from the image file that was installed (.bin) and the WLC boots using a package provisioning file, packages.conf. This provisioning file manages the bootup of each individual sub-package.

For additional information refer to the "Upgrading the Software" section of [**4**].

Remote Administration Protocols

To provide a protected remote administrative capability, the administrator needs to configure the Controller for SSH and HTTPS.

SSH

SSH is used to securely access the CLI from a remote workstation. The steps below provide instructions to configure SSH Server for the CC evaluated configuration. For additional information on SSH refer to the "Configuring Secure Shell" Chapter of [**12**].

1. In privileged EXEC mode, enter configure terminal

```
WLC# configure terminal
```

2. Specify the host domain name applicable to the Controller

```
WLC(config)# ip domain name cisco.com
```

3. Generate a crypto key for SSH. Assign a label such as SSH-KEY

```
WLC(config)# crypto key generate rsa label SSH-KEY modulus [2048 | 3072]
```

4. Assign the key pair to SSH

```
WLC(config)# ip ssh rsa keypair-name SSH-KEY
```

5. Enable SSHv2. This will also deny use of SSHv1

```
WLC(config)# ip ssh version 2
```

6. Configure the SSH Server Key Exchange

```
WLC(config)# ip ssh server algorithm kex ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-
nistp521
```

7. Specify the allowed encryption algorithms and the order they are to be supported

```
WLC(config)# ip ssh server algorithm encryption aes256-cbc aes128-cbc
```

8. Specify the allowed Message Authentication Code (MAC) algorithms and the order they are to be supported

```
WLC(config)# ip ssh server algorithm mac hmac-sha2-512 hmac-sha2-256
```

9. The administrator needs to configure the Controller for SSH public key authentication. This is necessary to avoid a potential situation where password failures by remote Administrators lead to no Administrator access for a temporary period of time. During the defined lockout period, the Controller provides the ability for the Administrator account to login remotely using SSH public key authentication.

   Before proceeding, please have the SSH public key ready for use. The public key is generated from your SSH client on the Management workstation.

   a. Configure Host Key Algorithms for SSH public-key based authentication

```
WLC(config)# ip ssh server algorithm hostkey rsa-sha2-256 rsa-sha2-512
```

   b. Enter public-key configuration mode

```
WLC(config)# ip ssh pubkey-chain
```

   c. Specify the admin user account to configure for SSH public key authentication

```
WLC(conf-ssh-pubkey-user)# username admin
```

d. Enter public-key data configuration mode

```
WLC(conf-ssh-pubkey-user)# key-string
```

e. Paste the data portion of the public key generated from the SSH client. **Note:** If necessary you may split the key into multiple lines.

```
WLC(conf-ssh-pubkey-data)# <paste your public key>
```

f. Return to configuration mode by entering exit 3 times:

```
WLC(conf-ssh-pubkey-data)# exit

WLC(conf-ssh-pubkey-user)# exit

WLC(conf-ssh-pubkey)# exit
```

10. Disable keyboard-interactive based authentication

```
WLC(config)# no ip ssh server authenticate user keyboard
```

11. SSH connections with the same session keys cannot be used longer than one hour, and with no more than one gigabyte of transmitted data. In the steps below configure a time-based and volume-based (in kilobytes) rekey values. **Note:** Values can be configured to be lower if desired. The minimum time value is 10 minutes. The minimum volume value is 100 kilobytes.

```
WLC(config)# ip ssh rekey time 60

WLC(config)# ip ssh rekey volume 1000000
```

12. Display SSH configuration information

```
WLC(config)# do show ip ssh
```

13. Confirm the SSH configuration includes the following settings. Your choice for encryption and MAC algorithms may be a subset of this list.

- SSH Enabled - version 2.0
- Authentication methods: publickey or password
- Hostkey Algorithms: rsa-sha2-256, rsa-sha2-512
- Encryption Algorithms: aes128-cbc, aes256-cbc
- MAC Algorithms: hmac-sha2-512, hmac-sha2-256
- KEX Algorithms: ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

14. Enter line configuration mode to configure the virtual terminal line settings 0 4

```
WLC(config)# line vty 0 4
```

15. Specify vty lines 0-4 to use only SSH

```
WLC(config-line)# transport input ssh
```

16. Specify a timeout value for vty lines 0-4

```
WLC(config-line)# exec-timeout <time in minutes>
```

17. Type Exit

```
WLC(config-line)# exit
```

18. Enter line configuration mode to configure the virtual terminal lines 5-15

```
WLC(config)# line vty 5 15
```

19. Specify the vty lines to use only SSH

```
WLC(config-line)# transport input ssh
```

20. Specify a timeout value for vty lines 5-15

```
WLC(config-line)# exec-timeout <time in minutes>
```

21. Exit configuration mode and return to privileged EXEC mode

```
WLC(config)# end
```

22. Enter "show running-config" and verify all vty lines include "transport input SSH" and have a configured timeout value

```
WLC# show running-config
```

Before proceeding to the next section, logout out of your local console CLI session by entering either "exit or "logout"

```
WLC# logout
```

From your remote management workstation, initiate a connect using SSH and supply either your public key or password credentials. Upon successful login you will be presented with privilege administrator access denoted by the 'hashtag' symbol:

```
WLC#
```

The remaining preparative procedures can be performed using the local console or remotely over SSH.

HTTPS

HTTPS is used by the Administrator to securely access the WebGUI from a remote workstation. The steps below provide instructions to configure HTTPS. For additional information on HTTPS refer to the "Configuring Secure Socket Layer HTTP" Chapter of [**12**].

Caution: Before proceeding, the administrator should determine the TLS 1.2 ciphersuites to use for HTTPS on your Cisco 9800 Controller. The table below lists the configuration option and its associated Non-Suite B CipherSuite Support:

Table 6. Non-Suite B HTTPS ciphersuites

Configuration Option	Ciphersuite Support
rsa-aes-cbc-sha2	RSA_WITH_AES_128_CBC_SHA256 RSA_WITH_AES_256_CBC_SHA256
ecdhe-rsa-aes-cbc-sha2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ecdhe-rsa-aes-gcm-sha2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
rsa-aes-gcm-sha2	TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384

aes-128-cbc-sha	TLS_RSA_WITH_AES_128_CBC_SHA
aes-256-cbc-sha	TLS_RSA_WITH_AES_256_CBC_SHA

The table below lists the configuration option and Suite B CipherSuite Support:

Table 7. Suite B HTTPS ciphersuites

Configuration Option	Ciphersuite Support
ecdhe-ecdsa-aes-gcm-sha2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

If you selected the Suite B Ciphersuite option (tls_ecdhe_ecdsa_aes_gcm_sha2) you must generate an elliptic curve key for ECDSA and not a RSA key.

Note: If you selected any of the following configuration options:

- **ecdhe_ecdsa_aes_gcm_sha2 (Suite B Ciphersuite)**
- **ecdhe_rsa_aes_cbc_sha2**
- **ecdhe_rsa_aes_gcm_sha2**

You have the ability to set the NIST elliptic curve. The choices are secp256r1 and secp384r1. If you do not provide one, the default NIST elliptic curve of secp256r1 will be used.

Generate a Crypto Key Pair for HTTPS

1. In privileged EXEC mode, enter configure terminal

```
WLC# configure terminal
```

2. If you chose the Suite B ciphersuite you must generate an elliptic curve key. Assign a label such as HTTPS-KEY

```
WLC(config)# crypto key generate ec keysize [256 | 384] exportable label HTTPS-KEY
```

Else if you want to use any of the non-Suite B ciphersuites you must generate a rsa key. Assign a label such as HTTPS-KEY

```
WLC(config)# crypto key generate rsa general modulus 2048 label HTTPS-KEY
```

Configure HTTPS Server and TLS 1.2

The HTTPS server must be configured to use X.509v3 certificates supporting a minimum path length of three (root CA -> intermediate CA -> end-entity). Therefore, you will need to create two trustpoints. The section below provides steps to create a root CA and a subordinate CA using CA certificates from your organization's PKI. Before proceeding, please have the root CA and subordinate CA certificates ready for import from your CA administrator.

1. Create, configure, and authenticate the root trustpoint

```
WLC(config)# crypto pki trustpoint <root trustpoint name>
WLC(ca-trustpoint)# enrollment terminal pem
WLC(ca-trustpoint)# chain-validation stop
WLC(ca-trustpoint)# revocation-check none
```

```
WLC(ca-trustpoint)# crypto pki authenticate <root trustpoint name>
```

Enter your base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

2. Create, configure, and authenticate the subordinate trustpoint:

```
WLC(config)# crypto pki trustpoint < subordinate trustpoint name>

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# revocation-check none

WLC(ca-trustpoint)# subject-name C=<two letter country code>, ST=<two letter state code>,
L=<locality>, O=<organization>, OU=<organizational unit>, CN=wlc
```

In the next step you will need to provide the key pair selected and the label

a. If you generated an elliptic curve key for the Suite B ciphersuite option enter

```
WLC(ca-trustpoint)# eckeypair HTTPS-KEY
```

b. If you generated a rsa key for all other ciphersuites enter

```
WLC(ca-trustpoint)# rsakeypair HTTPS-KEY
```

Authenticate the trustpoint

```
WLC(ca-trustpoint)# crypto pki authenticate <subordinate trustpoint name>
```

Enter your base 64 encoded subordinate CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

3. Generate a certificate signing request for the Controller

```
WLC(config)# crypto pki enroll <subordinate trustpoint name>
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

4. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

5. Save the contents in a file and distribute it to your PKI administrator for signing by the subordinate CA. Once signed, your PKI administrator will need to provide the certificate in PEM format.

6. Import the signed certificate to the intermediate trustpoint

```
WLC(config)# crypto pki import <subordinate trustpoint name> certificate
```

7. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The Controller should respond with:

"% Router Certificate successfully imported"

8. Enable HTTP secure server

```
WLC(config)# ip http secure-server
```

9. Allow TLS v1.2 and deny TLS 1.1 and all lower versions

```
WLC(config)# ip http tls-version TLSv1.2
```

10. Configure HTTPS for the ciphersuite configuration option

    a. If you selected the Suite B ciphersuite enter:

    ```
    WLC(config)# ip http secure-ciphersuite ecdhe-ecdsa-aes-gcm-sha2
    ```

    b. If not using the Suite B ciphersuite, you can choose any or all of the following configuration options for non-Suite B ciphersuites:

    ```
    WLC(config)# ip http secure-ciphersuite ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2
    rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 aes-128-cbc-sha aes-256-cbc-sha
    ```

    Refer to the HTTPS ciphersuite tables in this section for each configuration option and the supported ciphersuites.

11. If you would like to set the NIST elliptic curve use the following command. The choices are secp256r1 or secp384r1 and only one can be chosen. If you do not provide one the default NIST elliptic curve of secp256r1 will be used. **Note:** NIST elliptic curve does not apply to dhe-aes-cbc-sha2, dhe-aes-gcm-sha2, rsa-aes-cbc-sha2, rsa-aes-gcm-sha2.

```
WLC(config)# ip http secure-ecdhe-curve <secp256r1 | secp384r1>
```

12. Display HTTPS configuration information

```
WLC(config)# do show ip http server secure status
```

13. Confirm the HTTPS configuration at a minimum includes TLSv1.2, ciphersuites as selected from the list above and, if applicable, the ECDHE curve.

14. Set the http secure server certificate trustpoint

```
WLC(config)# ip http secure-trustpoint <subordinate trustpoint name>
```

HTTPS Session Inactivity Timeout

All HTTPS sessions must terminate after an Administrator-configurable time interval of session inactivity has elapsed. Specify the timeout value in seconds. The range is from 180 to 1200.

```
WLC(config)# ip http session-idle-timeout <180-1200>
```

Remove HTTP

Ensure HTTP is removed by entering the command below.

```
WLC(config)# no ip http server
```

Apply Changes

To apply changes to HTTPS you must reload the Controller.

Note: The TOE uses X.509v3 certificates to support authentication for TLS connections. The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate.

The TOE ensures the extendedKeyUsage field includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) for server certificates used in TLS. OCSP is not supported; therefore the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) is trivially satisfied by the TOE.

IPsec

IPsec is a framework of open standards developed by the IETF. It provides security for the transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec device(s). In the CC evaluated configuration IPsec is required to provide protected transmission of audit events to remote syslog server. This protection can be provided in one of two methods:

1. With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection.
2. With a syslog server is not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.

The Administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec recognizes a sensitive packet, the Controller sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per the ESP security protocol.

The administrator defines the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence and the Controller attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged, IPsec is triggered. If there is no SA that IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Controller. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the Controller needs protected by IPsec. Inbound traffic is processed against crypto map entries. if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Note: The evaluated configuration allows authentication of the peer using pre-shared key or X.509 certificates. If you are only using pre-shared keys and not X.509 certificates you can skip the next two sections and proceed directly to the IKE section.

Generate a Crypto Key Pair for IPsec

Caution: Before proceeding, the administrator should determine the Diffie-Hellman Groups to use for IKE/IPsec on your Cisco 9800 Controller. The Common Criteria evaluated configuration supports the following Suite B algorithms for IKE/IPsec

- DH Group 19 (256-bit Random ECP)
- DH Group 20 (384-bit Random ECP)

1. In privileged EXEC mode, enter configure terminal

```
WLC# configure terminal
```

2. Generate an elliptic curve key. Assign a label such as IPSEC-KEY

```
WLC(config)# crypto key generate ec keysize [256 | 384] exportable label IPSEC-KEY
```

Create Trustpoints for IPsec

IPsec must be configured to use X.509v3 certificates supporting a minimum path length of three (root CA -> intermediate CA -> end-entity). Therefore, you will need to create two trustpoints. The section below provides steps to create a root CA and a subordinate CA using CA certificates from your organization's PKI. Before proceeding, please have the root CA and subordinate CA certificates ready for import from your CA administrator.

Note: You will set up the CRL certificate revocation mechanism used to ensure that the certificate of the IPsec peer has not been revoked. If the TOE is unable to obtain a CRL, the TOE will reject the peer's certificate.

1. Create, configure, and authenticate a root trustpoint for IPsec

```
WLC(config)# crypto pki trustpoint <root trustpoint name>

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# chain-validation stop

WLC(ca-trustpoint)# crypto pki authenticate <root trustpoint name>
```

Enter your base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

2. Create, configure, and authenticate the subordinate trustpoint:

```
WLC(config)# crypto pki trustpoint <subordinate trustpoint name>

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# chain-validation continue <root trustpoint name>

WLC(ca-trustpoint)# subject-name C=<two letter country code>, ST=<two letter state code>,
L=<locality>, O=<organization>, OU=<organizational unit>, CN=wlc
```

In the next step you will need to provide the key pair selected and the label

a. If you generated an elliptic curve key for the Suite B enter

```
WLC(ca-trustpoint)# eckeypair IPSEC-KEY
```

b. If you generated a rsa key for non-Suite B enter

```
WLC(ca-trustpoint)# rsakeypair IPSEC-KEY
```

Authenticate the trustpoint

```
WLC(ca-trustpoint)# crypto pki authenticate <subordinate trustpoint name>
```

Enter your base 64 encoded subordinate CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

3. Generate a certificate signing request for the Controller

```
WLC(config)# crypto pki enroll <subordinate trustpoint name>
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

4. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

5. Save the contents in a file and securely distribute it to your PKI administrator for signing by the subordinate CA. Once signed, your PKI administrator will need to provide the certificate in PEM format.

6. Import the signed certificate to the subordinate trustpoint

```
WLC(config)# crypto pki import <subordinate trustpoint name> certificate
```

7. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The Controller should respond with:

"% Router Certificate successfully imported"

8. Configure the trustpoints to perform revocation checking using CRL

```
WLC(config)# crypto pki trustpoint <root trustpoint name>
WLC(ca-trustpoint)# revocation-check CRL
WLC(ca-trustpoint)# match key-usage cRLSign
WLC(ca-trustpoint)# exit
WLC(config)# crypto pki trustpoint <subordinate trustpoint name>
WLC(ca-trustpoint)# revocation-check CRL
WLC(ca-trustpoint)# match key-usage cRLSign
WLC(ca-trustpoint)# exit
```

IKEv2

This section discusses IKEv2 which requires configuring an IKEv2 Proposal, Policy, Keyring, and Profile.

1. Configure the IKEv2 Proposal. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation, and it contains selections that are not valid for the TOE. Thus the following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE:

    a. In privileged EXEC mode, enter configure terminal.

    ```
    WLC# configure terminal
    ```

    b. Specify the IKEv2 proposal. The IKEv2 proposal MUST either have a set of an encryption algorithm other than aes-gcm, an integrity algorithm and a DH group configured or encryption algorithm aes-gcm, a prf algorithm and a DH group configured.

    ```
    WLC(config)# crypto ikev2 proposal <name>
    ```

    c. Set the encryption algorithm(s) for the proposal.

```
WLC(config-ikev2-proposal)# encryption < aes-gcm-128 | aes-gcm-256>
```

d. Set the PRF algorithm(s) for the proposal.

```
WLC(config-ikev2-proposal)# prf <sha1 | sha256  sha384 | sha512>
```

e. Set the Diffie-Hellman group(s)

```
WLC(config-ikev2-proposal)# group <19 | 20>
```

f. Enter exit to return to the main configuration mode.

```
WLC(config-isakmp)# exit
```

2. Configure the IKEv2 Policy

a. Define the IKEv2 policy name.

```
WLC(config)# crypto ikev2 policy <Name of IKEv2 policy>
```

b. Specify the proposal created in the previous section

```
WLC(config-ikev2-policy)# proposal <name>
```

c. Enter exit to return to the main configuration mode

```
WLC(config-ikev2-policy)# exit
```

3. Configure the IKEv2 Keyring. If you chose pre-shared key as the authentication method you must complete these steps.

a. Define the IKEv2 keyring.

```
WLC(config)# crypto ikev2 keyring <Name of IKEv2 Keyring>
```

b. Define the peer block

```
WLC(config-ikev2-keyring)# peer <Name of the peer block>
```

c. In peer sub mode specify the IPv4/IPv6 address of peer

```
WLC(config-ikev2-keyring-peer)# address <IPv4 Address | IPv6 Address/prefix>
```

d. Specify the IKEv2 peer through an identity address

```
WLC(config-ikev2-keyring-peer)# identity address <IPv4 Address | IPv6
Address/prefix>
```

e. Specify a pre-shared key.

To specify a text-based pre-shared key:

```
WLC(config-ikev2-keyring-peer)# pre-shared-key 0 <pre-shared key>
```

Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

To specify a bit-based pre-shared key:

```
WLC(config-ikev2-keyring-peer)# pre-shared-key hex <pre-shared key in hex>
```

d. Enter exit twice to return to the main configuration mode

```
WLC(config-ikev2-keyring-peer)# exit

WLC(config-ikev2-keyring)# exit
```

4. Configure the IKEv2 Profile. An IKEv2 profile is a repository of nonnegotiable parameters of the IKE SA (such as local/remote identities and authentication methods) and the services available to the authenticated peers that match the profile. An IKEv2 profile must be configured and must be attached to either a crypto map or an IPsec profile on both the IKEv2 initiator and responder.

a. Define the IKEv2 Profile.

```
WLC(config)# crypto ikev2 profile <name of IKEv2 profile>
```

b. Set the local authentication method.

```
WLC(config-ikev2-profile)# authentication local <ecdsa-sig> <rsa-sig> <pre-share>
```

c. Set the remote authentication method.

```
WLC(config-ikev2-profile)# authentication remote <ecdsa-sig> <rsa-sig> <pre-share>
```

d. Specify the local IKE FQDN identity to use.

```
WLC(config-ikev2-profile)# identity local fqdn <fully qualified domain name string>
```

e. If you are using pre-shared keys specify the key ring created in the previous section

```
WLC(config-ikev2-profile)# keyring local <key ring name>
```

f. Set the IKE SA lifetime in seconds.

```
WLC(config-ikev2-profile)# lifetime <120-86400>
```

g. Enter exit to return to the main configuration mode

```
WLC(config-ikev2-profile)# exit
```

IPsec Transform Sets and SA Lifetimes

Regardless of the IKE version selected, the Controller must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

The Administrator can specify multiple transform sets and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry's access list.

During IPsec security association negotiations with IKE, peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both peers' IPsec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

1. Define the allowed transform sets.

```
WLC(config)# crypto ipsec transform-set <transform set tag> esp-gcm
```

2. Define the IPsec mode which is either tunnel mode or transport mode.

```
WLC(cfg-crypto-trans)# mode <transport | tunnel>
```

3. Type exit to return to the main configuration mode.

```
WLC(cfg-crypto-trans)# exit
```

4. Define the IPsec security association lifetime. The lifetime can be chosen based on time (hours) or can be volume based. A time-based lifetime must be entered in seconds where 1 hour=3600 seconds and 8 hours=28800 seconds.

```
WLC(config)# crypto ipsec security-association lifetime <seconds < 120-28800>> | <kilobytes
<2560-4294967295>>
```

IPsec Crypto Map and Access Control List

The administrator can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface).

```
WLC(config)# access-list <IP access-list number> permit ip 192.168.3.0 0.0.0.255
10.3.2.0 0.0.0.255
```

For example, if your syslog host is 10.83.84.76 you could define an access list 102 as:

```
WLC(config)# access-list 102 permit ip any host 10.83.84.76

WLC(config)# access-list 102 permit ip host 10.83.84.76 any
```

When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. For example:

```
WLC(config)# crypto map <crypto map tag> <sequence number> ipsec-isakmp
```

The match address command specifies to use access list number order to determine which traffic is relevant.

```
WLC(config-crypto-map)# match address <IP access-list number>
```

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow. Use the set transform-set command specifies the transform set tag.

```
WLC(config-crypto-map)# set transform-set <proposal tag>
```

The set peer command specifies the ip address of the peer

```
WLC(config-crypto-map)# set peer <IP address of peer>
```

If using IKEv2 the set ikev2-profile command specifies the profile to use

```
WLC(config-crypto-map)# set ikev2-profile <name of the ikev2 profile>
```

You will need to apply the crypto map to an interface. The VLAN ID created earlier in the initial configuration section may be used.

```
WLC(config)# vlan <VLAN ID 1-4094>

WLC(config-if)# crypto map <crypto map tag>

WLC(config-if)# end
```

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered.

If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Controller. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the Controller needs protected by IPsec. Inbound traffic is processed against crypto map entries. if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Security Policy Database (SPD)

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet).

The traffic matching permit ACL would then flow through the IPsec tunnel and be classified as “PROTECTED”.

Traffic that does not match a permit crypto map ACL and does not match a non-crypto permit ACL on the interface would be DISCARDED.

Traffic that does not match a permit ACL in the crypto map, but does match a non-crypto permit ACL would be allowed to BYPASS the tunnel. For example, a non-crypto permit ACL for icmp would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic.

Configure Reference Identifier

If you are using X.509 certificates for IKE peer authentication this section describes configuration of the peer reference identifier through use of a certificate map. Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. IKEv2 profiles can bind themselves to certificate maps, and the Controller will determine if they are valid during IKE authentication.

1. Start certificate-map mode

```
WLC(config)# crypto pki certificate map <attribute map tag> | <sequence-number>
```

2. Specify one or more certificate fields together with their matching criteria and the value to match. In the evaluated configuration, the field name must specify the SAN (alt-subject-name) field of the peer’s certificate. Match criteria should be “eq” for equal.

   For example:

```
WLC(ca-certificate-map)# alt-subject-name eq <peer.cisco.com>
```

3. Type exit to return to the main configuration mode.

```
WLC(ca-certificate-map)# exit
```

4. Associate the certificate map to the IKE v2 profile

```
WLC(config)# crypto ikev2 profile <profile name>
```

```
WLC(config-ikev2-profile)# match certificate <attribute map tag>

WLC(config-ikev2-profile)# end
```

Match Identity

If you are not using X.509 certificates and are using pre-shared key for IKE peer authentication, add a match identity statement to your IKE profile created earlier. Enter:

```
WLC(config)# crypto ikev2 profile <profile name>

WLC(config-ikev2-profile)# match identity remote address <IP address of peer>
```

Enable IKE and IPsec Logging

To generate the required audit events for IKE and IPsec perform the following steps

```
WLC# debug crypto ipsec
```

In addition to generate the required audit events for IKE you will need to enter:

```
WLC# debug crypto ikev2
```

IPsec Session Interruption and Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken and the Administrator will find a connection time out error message in the audit log. The administrator can use the show command below to confirm the connection is broken:

```
WLC# show crypto ipsec sa
```

When a connection is broken no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

Enable Remote Syslog Server

Once IPsec has been setup and configured to protect the transmission of audit events to the remote syslog server, use the logging host command below to enable the WLC to transmit audit data. When an audit event is generated, is it simultaneously sent to the external server and the local store.

To configure a remote syslog server enter the following command:

```
WLC(config)# logging host <ip address>
```

IPsec References

For Cisco IPsec documentation references, see [**27**]

Note: The TOE uses X.509v3 certificates to support authentication for IPsec connections. The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. OCSP is not supported; therefore the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) is trivially satisfied by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer.

Note: When operating in FIPS mode, the WLC expects incoming IKEv2 AUTH payload signatures to use SHA256 as the hash function when RSA certificates are used.

TLS — RADsec

RADIUS over TLS (RADsec) is used by the Controller to securely access the RADIUS server. The steps below provide instructions to configure RADIUS over TLS. Since TLS mutual authentication is required, you will need to generate a private key and enroll the intermediate trustpoint for a certificate. Radius TLS supports the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite.

Generate a Crypto Key Pair for RADIUS over TLS

1. In privileged EXEC mode, enter configure terminal

```
WLC# configure terminal
```

2. Generate a RSA key for RADsec. Assign a label such as TLS-RADSEC-KEY

```
WLC(config)# crypto key generate rsa general modulus [2048 | 3072] label TLS-RADSEC-KEY
```

Configure TLS Client

TLS must be configured to use X.509v3 certificates supporting a minimum path length of three (root CA -> intermediate CA -> end-entity). Therefore, you will need to create two trustpoints. The section below provides steps to create a root CA and a subordinate CA using CA certificates from your organization's PKI. Before proceeding, please have the root CA and subordinate CA certificates ready for import from your CA administrator.

Note: The TOE may be configured to perform identity verification using either an IP address or DNS Name in the SAN extension of the X.509 certificate. This is covered in step 14 in the section below. The Administrator is advised to follow the security policies and procedures of their organization if using an IP address to verify RADsec server identity.

1. Create, configure, and authenticate a root trustpoint

```
WLC(config)# crypto pki trustpoint <root trustpoint name>

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# chain-validation stop

WLC(ca-trustpoint)# exit

WLC(config)# crypto pki authenticate <root trustpoint name>
```

Enter your base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

2. Create, configure, and authenticate the subordinate trustpoint:

```
WLC(config)# crypto pki trustpoint <subordinate trustpoint name>

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# chain-validation continue <root trustpoint name>

WLC(ca-trustpoint)# eku request client-auth

WLC(ca-trustpoint)# match eku server-auth

WLC(ca-trustpoint)# fqdn <WLC fully-qualified domain name>

WLC(ca-trustpoint)# subject-name C=<two letter country code>, ST=<two letter state code>,
L=<locality>, O=<organization>, OU=<organizational unit>, CN=wlc
```

In the next step you will need to provide the RSA key pair and the label

```
WLC(ca-trustpoint)# rsakeypair TLS-RADSEC-KEY

WLC(ca-trustpoint)# exit
```

Authenticate the trustpoint

```
WLC(config)# crypto pki authenticate <subordinate trustpoint name>
```

Enter your base 64 encoded subordinate CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

3. Generate a certificate signing request for the Controller

```
WLC(config)# crypto pki enroll <subordinate trustpoint name>
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

4. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

5. Save the contents in a file and securely distribute it to your PKI administrator for signing by the subordinate CA. Once signed, your PKI administrator will need to provide the certificate in PEM format.

6. Import the signed certificate to the subordinate trustpoint

```
WLC(config)# crypto pki import <subordinate trustpoint name> certificate
```

7. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The Controller should respond with:

"% Router Certificate successfully imported"

8. Create a Certificate Map. This will configure the reference identifier of the RADsec Server.

```
WLC(config)# crypto pki certificate map <attribute map tag> | <sequence-number>
```

For example: `crypto pki certificate map radsec 1`

9. Specify the SAN (alt-subject-name) field together with the matching criteria of equal and the value to match. In this example the value to match is radsec.cisco.com.

```
WLC(ca-certificate-map)# alt-subject-name eq radsec.cisco.com
```

10. Exit to main config mode

```
WLC(ca-certificate-map)# exit
```

11. Configure the trustpoints to perform revocation checking using CRL

```
WLC(config)# crypto pki trustpoint <root trustpoint name>

WLC(ca-trustpoint)# revocation-check CRL
```

```
WLC(ca-trustpoint)# match key-usage cRLSign

WLC(ca-trustpoint)# exit

WLC(config)# crypto pki trustpoint <subordinate trustpoint name>

WLC(ca-trustpoint)# revocation-check CRL

WLC(ca-trustpoint)# match key-usage cRLSign

WLC(ca-trustpoint)# match certificate <attribute map tag>
```

For example: `match certificate radsec`

```
WLC(ca-trustpoint)# exit
```

12. Specify the RADIUS Server Name

```
WLC(config)# radius server <name for the radius server configuration>
```

13. Specify the RADIUS Server Address

```
WLC(config-radius-server)# address ipv4 | ipv6 <IPv4 Address> <IPv6 Address>
```

14. Specify the RADIUS shared secret

```
WLC(config-radius-server)# key <0 | 6> radius/dtls
```

Note: The shared secret must be: radius/dtls

15. Specify the RADIUS port

```
WLC(config-radius-server)# tls port <port number>
```

16. Specify the trustpoint for client

```
WLC(config-radius-server)# tls trustpoint client <subordinate trustpoint name>
```

17. Specify the trustpoint for server

```
WLC(config-radius-server)# tls trustpoint server <subordinate trustpoint name>
```

18. Specify the Reference Identifier for the Peer using DNS name or IP address.

```
WLC(config-radius-server)# tls match-server-identity hostname <DNS Name>

WLC(config-radius-server)# tls match-server-identity ip-address <IP Address>
```

19. Type exit to return to the main configuration mode.

```
WLC(config-radius-server)# exit
```

20. Configure AAA for RADIUS

    a. Configure Group Server Name

    ```
    WLC(config)# aaa group server radius <radius server-group name>
    ```

    b. Specify RADIUS Server Name

    ```
    WLC(config-sg-radius)# server name <radius server name>
    ```

    c. Type exit to return to the main configuration mode

    ```
    WLC(config-sg-radius)# exit
    ```

21. Set authentication list for IEEE 802.1X

```
WLC(config)# aaa authentication dot1x default group <radius server-group name>
```

Note The TOE uses X.509v3 certificates to support authentication for TLS connections to a RADsec server. The WLC determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. The WLC will also verify the extendedKeyUsage field of the TLS peer certificate contains the Server Authentication purpose. OCSP is not supported; therefore the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) is trivially satisfied by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer.

DTLS — CAPWAP

CAPWAP is an open standard developed by the IETF for the management of wireless access points which uses DTLS to provide for secure communication between the Controller and Access Points. In this section you will configure DTLS for use by CAPWAP in order to enroll to obtain certificates for the Controller and Access Points.

First Time AP Join

The first time an Access Point joins the Controller it must use either a manufactured-installed certificate (MIC) or a self-signed certificate (SSC). MICs and SSCs are only for the very first time the AP joins a Controller. For all subsequent joins, the AP will use Locally Significant Certificates (LSC). Locally Significant Certificates (LSCs) are obtained via Enrollment over Secure Transport (EST) and requires the organization has its own PKI and a Certificate Authority (CA) that support EST.

All controller models can use the SSC method. Hardware-based Controllers (C9800-80, C9800-40, C9800-L) can use the MIC method. The C9800-CL cannot use the MIC method and must use SSC.

SSC

The SSC method must be used when the Controller is a 9800-CL. SSC may be optionally used on the C9800-80, C9800-40, and C9800-L Controllers as an alternative to the MIC method.

Note: The steps below must be followed exactly in order for SSC to be enabled.

1. Configure IOS CA Server

    a. Generate a RSA key

    ```
    WLC(config)# crypto key generate rsa general-keys modulus 2048 label ca
    ```

    b. Define an IOS certificate server

    ```
    WLC(config)# crypto pki server ca
    ```

    c. Enter the issuer-name. **Note:** For SSC use only the below organization and CN values

    ```
    WLC(cs-server)# issuer-name O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC
    ```

    d. Automatically grant the enrollment requests

    ```
    WLC(cs-server)# grant auto
    ```

    e. Define a hash

    ```
    WLC(cs-server)# hash sha256
    ```

    f. Define the CA certificate lifetime

```
WLC(cs-server)# lifetime ca-certificate <lifetime in days>
```

g. Define the certificate lifetime

```
WLC(cs-server)# lifetime certificate <lifetime in days>
```

h. Backup Certificate Server Signing Certificate and Keys

```
WLC(cs-server)# database archive pkcs12 password 0 <password>
```

i. Enable the IOS certificate server

```
WLC(cs-server)# no shutdown
```

2. Configure Trustpoint

a. Generate a RSA key

```
WLC(config)# crypto key generate rsa general-keys modulus 2048 label ewlc-tp1
```

b. Create ewlc-tp1 Trustpoint.

```
WLC(config)# crypto pki trustpoint ewlc-tp1

WLC(ca-trustpoint)# rsakeypair ewlc-tp1

WLC(ca-trustpoint)# subject-name O=Cisco Virtual Wireless LAN Controller,
CN=DEVICE-vWLC

WLC(ca-trustpoint)# revocation-check none

WLC(ca-trustpoint)# hash sha256

WLC(ca-trustpoint)# serial-number

WLC(ca-trustpoint)# eku request server-auth client-auth

WLC(ca-trustpoint)# password 0 <password>

WLC(ca-trustpoint)# enrollment url <management-IPv4>
```

Replace `<management-IPv4>` with management vlan interface IP of the Controller where CA server is configured.

```
WLC(ca-trustpoint)# exit
```

c. Authenticate trustpoint with CA

```
WLC(config)# crypto pki authenticate ewlc-tp1
```

The Controller should respond with

Certificate has the following attributes:

Fingerprint MD5: 64C5FC9A C581D827 C25FC3CF 1A7F42AC

Fingerprint SHA1: 6FAFF812 7C552783 6A8FB566 52D95849 CC2FC050

% Do you accept this certificate? [yes/no]: `yes`

Trustpoint CA certificate accepted

d. Enroll Controller with CA

```
WLC(config)# crypto pki enroll ewlc-tp1
```

The Controller should respond with

% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes

f. Verify trustpoint status

```
WLC(config)# do show crypto pki trustpoint ewlc-tp1 status
```

The Controller should respond with

State:
Keys generated ..... Yes (General Purpose, exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes

3. Set the wireless management trustpoint

```
WLC(config)# wireless management trustpoint ewlc-tp1
```

MIC

If you have a C9800-80, C9800-40, or C9800-L Controller you may use the MIC method:

1. Verify wireless management interface configured during initial installation:

```
WLC# sh run | s wireless management interface
```

The output should include:

```
wireless management interface <vlan ID>
```

Access Point Deployment

The Access Points must be discovered by a Controller before they can become an active part of the network. Access Points support the following controller discovery methods:

- Locally stored controller IP address discovery. If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IPv4 or IPv6 addresses on an access point for later deployment is called priming the access point. To prime an access point for first time use follow the steps below.

  1. Connect to the console port and power-up the AP.
  2. Login using Cisco/Cisco credentials and enter privilege EXEC mode by entering enable followed by Cisco.
  3. Provide the primary controller name and IP address. The primary controller name is the host name and the IP address are the address of the management interface.

     ```
     # capwap ap primary-base <controller name> <ip address of management
     interface>
     ```

  4. If you are not using DHCP provide the AP an IP address

     ```
     # capwap ap ip <ip address> <subnet mask> <default gateway>
     ```

  5. Power-off the AP. The configuration will be saved automatically

- DHCP server discovery. This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the Configuring DHCP Option 43 of [**15**].

- DNS discovery. The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.
- Layer 3 CAPWAP Discovery. After the AP gets an IP address from the DHCP server, the AP begins this discovery process. The LAP broadcasts a Layer 3 discovery message on the local IP subnet. Any WLC that is connected to the same local subnet receives the Layer 3 discovery message. Each of the WLCs that receives the discovery message replies with a unicast discovery response message to the AP.

Regardless of the controller discovery methods you are using, if this is the first time you are connecting the AP to the Controller, it is recommended to connect to the console port and power-up the AP to observe the boot-up sequence and discovery process. Once FIPS mode is enabled local login access to the AP is disabled automatically.

On the Controller enter the show ap config general command to confirm the AP has joined using SSC. The output should say the AP certificate type is Self Signed Certificate.

```
WLC# show ap config general
```

Note: Record the AP serial number if you do not have this information. The AP serial number is needed in the FIPS mode section below.

FIPS Mode

The administrator needs to configure the Controller for FIPS mode of operation. This action will also configure the APs for FIPS mode. To configure FIPS mode, follow the steps below:

1. Authorize Access Points. The Common Criteria evaluated configuration requires the Administrator to Authorize the Access Points that are allowed to join. Follow the steps below:

   a. First enable the authorization of APs using serial number:

   ```
   WLC(config)# ap auth-list authorize-serialNum
   ```

   b. Add the serial numbers of the APs you are enabling to join. The serial number can be obtain from running the command “show ap config general” as described in the preceding section. In configuration mode at the CLI enter username <AP serial number> serial-number. For example:

   ```
   WLC(config)# username FDW2025A314 serial-number
   ```

2. In privilege EXEC mode, enter configure terminal

   ```
   WLC# config terminal
   ```

3. Enter a FIPS authorization key. **Note:** The key length should be 32 characters. **Note:** If you have High Availability enabled ensure both active and standby controllers have the same FIPS authorization key.

   ```
   WLC(config)# fips authorization-key 12345678901234567890123456789012
   ```

4. Exit configuration mode and return to privileged EXEC mode

   ```
   WLC(config)# end
   ```

5. You must now reboot the controller to enable FIPS mode. After the controller is rebooted, the APs, as soon as they rejoin the controller, also reboot.

Verify FIPS Mode

To verify FIPS mode:

1. Enter the following

```
WLC# show fips status
```

The status of FIPS mode on the device will be displayed

For additional information, refer to the FIPS Chapter of [**6**].

CC Mode

The administrator needs to configure the Controller for CC mode of operation. To configure CC mode, follow the steps below:

1. In privilege EXEC mode, enter configure terminal

```
WLC# config terminal
```

2. Enter wireless wlancc

```
WLC(config)# wireless wlancc
```

3. Exit configuration mode and return to privileged EXEC mode

```
WLC(config)# end
```

4. You must now reboot the controller to enable CC mode. After the controller is rebooted, the APs, as soon as they rejoin the controller, also reboot.

Configure Locally Significant Certificates (LSC) Using EST – RSA Certificates

When obtaining a certificate for the AP to use for DTLS, the Controller must establish a mutually authenticated TLS trusted channel to the EST server. Those certificates on each side are generated by a manual out-of-band method. Once the TLS channel has been successfully established, the Controller will submit a certificate request on behalf of an Access Point to use for DTLS. The Cisco 9800 Wireless LAN Controller TOE refers to these X.509 certificates as Locally Significant Certificates (LSC).

Note: The TOE may be configured to perform identity verification using either an IP address or DNS Name in the SAN extension of the X.509 certificate. This is covered in step 21 in the section below. The Administrator is advised to follow the security policies and procedures of their organization if using an IP address to verify EST server identity.

This section describes the configuration necessary for:

- The Controller to obtain certificates to establish a TLS 1.2 mutually-authenticated client connection to an EST Server supporting the following ciphersuites:
    a. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    b. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    d. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
    e. TLS_RSA_WITH_AES_256_GCM_SHA384
    f. TLS_RSA_WITH_AES_256_CBC_SHA256
    g. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    h. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
    i. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

j. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

k. TLS_RSA_WITH_AES_128_GCM_SHA256

l. TLS_RSA_WITH_AES_128_CBC_SHA256

- The Controller and Access Point to obtain certificates to establish a DTLS 1.2 mutually-authenticated connection supporting the following ciphersuites:

  a. TLS_DHE_RSA_WITH_AES_128_CBC_SHA

  b. TLS_DHE_RSA_WITH_AES_256_CBC_SHA

  c. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

Refer to the table below for certificate type, CA Name, Trustpoint Name, and associated purpose. The names are used as examples in the instructions that follow.

Certificate Type	CA Name	IOS-XE Trustpoint Name	Purpose
RSA	myrootESTCA	myrootESTCA	Trustpoint for RSA Certificates used to generate intermediate CA (mysubESTCA)
		estclient	Trustpoint for RSA Certificates obtained using EST for internal components of a distributed TOE to communicate over DTLS 1.2
	mysubESTCA	mysubESTCA	Trustpoint for RSA Certificates used to communicate to EST Sever over TLS 1.2.

1. In privileged EXEC mode, enter configure terminal

```
WLC# configure terminal
```

2. Create a Certificate Map. This will configure the reference identifier of the EST Server.

```
WLC(config)# crypto pki certificate map <attribute map tag> | <sequence-number>
```

3. Specify the SAN (alt-subject-name) field together with the matching criteria of equal and the value to match. In this example the value to match is estserver.cisco.com.

```
WLC(ca-certificate-map)# alt-subject-name eq estserver.cisco.com
```

4. Exit to main config mode

```
WLC(ca-certificate-map)# exit
```

5. Generate a 2048-bit key and provide an associated label

```
WLC(config)# crypto key generate rsa general modulus 2048 label TLS-EST-RSA
```

6. Create, configure, and authenticate the root trustpoint

```
WLC(config)# crypto pki trustpoint myrootESTCA

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# chain-validation stop

WLC(ca-trustpoint)# exit

WLC(ca-trustpoint)# crypto pki authenticate myrootESTCA
```

Enter the base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The C9800 should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

7. Create, configure, and authenticate the intermediate trustpoint:

```
WLC(config)# crypto pki trustpoint mysubESTCA

WLC(ca-trustpoint)# enrollment terminal pem

WLC(ca-trustpoint)# chain-validation continue myrootESTCA

WLC(ca-trustpoint)# match certificate est

WLC(ca-trustpoint)# subject-name C=<two letter country code>, ST=<two letter state code>,
L=<locality>, O=<organization>, OU=<organizational unit>, CN=<Common Name>
```

For example: `subject-name C=US, ST=MA, L=Boxborough, O=STO, OU=GCT, CN=C9800`

8. Provide the key pair and label:

```
WLC(ca-trustpoint)# rsakeypair TLS-EST-RSA

WLC(ca-trustpoint)# exit
```

9. Authenticate the trustpoint

```
WLC(config)# crypto pki authenticate mysubESTCA
```

Enter the base 64 encoded intermediate CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

10. Generate a certificate signing request for the C9800

```
WLC(config)# crypto pki enroll mysubESTCA
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

11. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

Save the contents in a file and distribute it to the EST Server for signing by the intermediate CA.

12. On the C9800, import the signed certificate to the subordinate trustpoint

```
WLC(config)# crypto pki import mysubESTCA certificate
```

13. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The C9800 should respond with:

"% Router Certificate successfully imported"

14. Configure the trustpoints to perform revocation checking using CRL

```
WLC(config)# crypto pki trustpoint myrootESTCA
WLC(ca-trustpoint)# revocation-check CRL
WLC(ca-trustpoint)# match key-usage cRLSign
WLC(ca-trustpoint)# exit
WLC(config)# crypto pki trustpoint mysubESTCA
WLC(ca-trustpoint)# revocation-check CRL
WLC(ca-trustpoint)# match key-usage cRLSign
WLC(ca-trustpoint)# exit
```

Manually Obtain RSA Certificates for CAPWAP/DTLS

In the section below, you will manually enroll the WLC to obtain an X.509 certificate for CAPWAP/DTLS

15. Create and authenticate the root trustpoint. This will be the same root CA certificate imported for myrootESTCA

```
WLC(config)# crypto pki trustpoint estclient
WLC(ca-trustpoint)# enrollment terminal pem
WLC(ca-trustpoint)# subject-name C=US, ST=MA, L=Boxborough, O=STO, OU=GCT, CN=C9800
WLC(ca-trustpoint)# exit

WLC(config)# crypto pki authenticate estclient
```

Enter the base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The WLC should respond with:

“Trustpoint CA certificate accepted.”

“% Certificate successfully imported”

16. On the WLC, enter the following to enroll for device certificate:

```
WLC(ca-trustpoint)# crypto pki enroll estclient
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

17. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

18. Save the contents in a file on the EST Server for signing by the root CA. The CA Administrator will need to manually generate the signed certificate.

19. On the WLC, import the signed certificate to the estclient trustpoint

```
WLC(config)# crypto pki import estclient certificate
```

20. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The WLC should respond with:

    "% Router Certificate successfully imported"

21. On the WLC, view the certificates

```
show crypto pki certificate verbose estclient
```

    Ensure there is a certificate and CA certificate in the output. For example:

```
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 1001
  Certificate Usage: General Purpose
  Issuer:
    e=tac@cisco.com
    cn=myrootESTCA
    ou=GCT
    o=STO
    l=Boxborough
    st=MA
    c=US
  Subject:
    Name: C9800
    st=MA
    cn= C9800
    ou=GCT
    o=STO
    c=US
  Validity Date:
    start date: 11:17:21 EST Apr 23 2021
    end   date: 11:17:21 EST Apr 23 2023
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 9A99FD2A E23D16DE 9574620E B310424A
  Fingerprint SHA1: BB02F1E2 6C1ED786 870CA899 F4EF7865 CFC82BA8
  X509v3 extensions:
    X509v3 Key Usage: B8000000
      Digital Signature
      Key Encipherment
      Data Encipherment
      Key Agreement
    X509v3 Subject Key ID: 9DA7FB8C B4954287 65842706 CC00356F 5B513466
    X509v3 Basic Constraints:
        CA: FALSE
    X509v3 Authority Key ID: 661469F6 9EEA304D E631FE78 B4A85781 6CC2DE56
    Authority Info Access:
    Extended Key Usage:
        Client Auth
        Server Auth
Cert install time: 15:09:00 EST Apr 28 2021
  Associated Trustpoints: estclient
  Storage: nvram:tacciscocom#1001.cer
  Key Label: LSC-EST-RSA
  Key storage device: private config
```

```
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 6DB1FC6EA470B5708012B1FA1D56BE6C7FE95ACE
  Certificate Usage: Signature
  Issuer:
    e=tac@cisco.com
    cn=myrootESTCA
    ou=GCT
    o=STO
    l=Boxborough
    st=MA
    c=US
  Subject:
    e=tac@cisco.com
    cn=myrootESTCA
    ou=GCT
    o=STO
    l=Boxborough
    st=MA
    c=US
  Validity Date:
    start date: 10:51:48 EST Apr 23 2021
    end   date: 10:51:48 EST Apr 23 2023
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: F98401F3 24DBEC0E 778E8A0E 8B66F416
  Fingerprint SHA1: 34B81902 C884D1B2 8B3A9188 E238DFE4 F881BB1A
  X509v3 extensions:
    X509v3 Key Usage: 6000000
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 661469F6 9EEA304D E631FE78 B4A85781 6CC2DE56
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
Cert install time: 15:09:00 EST Apr 28 2021
  Associated Trustpoints: estclient myrootESTCA
  Storage: nvram:tacciscocom#5ACECA.cer
```

22. On the C9800, create a PKI enrollment profile. You will need to provide the host name or IP address of the EST server

```
WLC(config)# crypto pki profile enrollment myEST

WLC(ca-profile-enroll)# method-est

WLC(ca-profile-enroll)# enrollment url <url>
```

For example: `enrollment url https://estserver.cisco.com:8085`

```
WLC(ca-profile-enroll)# enrollment credential mysubESTCA

WLC(ca-profile-enroll)# exit
```

23. On the C9800, update the trustpoint for the EST client to use the enrollment profile

```
WLC(config)# crypto pki trustpoint estclient

WLC(ca-trustpoint)# usage ssl-client

WLC(ca-trustpoint)# no enrollment terminal pem

WLC(ca-trustpoint)# enrollment profile myEST

WLC(ca-trustpoint)# match eku server-auth

WLC(ca-trustpoint)# subject-name C=US, ST=MA, L=Boxborough, O=STO, OU=GCT, CN=C9800
```

Note: The CN needs to match the CN supplied in Step 6

```
WLC(ca-trustpoint)# revocation-check none

WLC(ca-trustpoint)# rsakeypair TLS-EST-RSA
```

Configure Locally Significant Certificates (LSC) Using EST – ECC Certificates

When obtaining a certificate for the AP to use for DTLS, the Controller must establish a mutually authenticated TLS trusted channel to the EST server. Those certificates on each side are generated by a manual out-of-band method. Once the TLS channel has been successfully established, the Controller will submit a certificate request on behalf of an Access Point to use for DTLS. The Cisco 9800 Wireless LAN Controller TOE refers to these X.509 certificates as Locally Significant Certificates (LSC).

Note: The TOE may be configured to perform identity verification using either an IP address or DNS Name in the SAN extension of the X.509 certificate. This is covered in step 21 in the section below. The Administrator is advised to follow the security policies and procedures of their organization if using an IP address to verify EST server identity

This section describes the configuration necessary for:

- The Controller to establish a TLS 1.2 mutually-authenticated client connection to an EST Server supporting the following ciphersuites:
    a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    b. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- The Controller and Access Point to establish a DTLS 1.2 mutually-authenticated connection supporting the following ciphersuites:
    c. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    d. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Refer to the table below for certificate type, CA Name, Trustpoint Name, and associated purpose. The names are used as examples in the instructions that follow.

Certificate Type	CA Name	IOS-XE Trustpoint Name	Purpose
EC	myrootESTCA-ecc	myrootESTCA-ecc	Trustpoint for EC Certificates used to generate intermediate CA (mysubESTCA-ecc)
		EC-estclient	Trustpoint for EC Certificates obtained using EST for internal components of a distributed TOE to communicate over DTLS 1.2.
	mysubESTCA-ecc	mysubESTCA-ecc	Trustpoint for EC Certificates used to communicate to EST Sever over TLS 1.2.

22. In privileged EXEC mode, enter configure terminal

```
WLC# configure terminal
```

Note: Change the hostname be different than the one used for RSA certificates. For example, wlc-ecc

```
WLC# hostname WLC-ecc
```

Note: Steps 2-4 below are only necessary if you did not create a certificate map in the section above for RSA certificates

23. Create a Certificate Map. This will configure the reference identifier of the EST Server.

```
WLC-ecc(config)# crypto pki certificate map <attribute map tag> | <sequence-number>
```

24. Specify the SAN (alt-subject-name) field together with the matching criteria of equal and the value to match. In this example the value to match is estserver.cisco.com.

```
WLC-ecc(ca-certificate-map)# alt-subject-name eq estserver.cisco.com
```

25. Exit to main config mode

```
WLC-ecc(ca-certificate-map)# exit
```

26. Generate a 256-bit key and provide an associated label

```
WLC-ecc(config)# crypto key generate ec keysize 256 exportable label LSC-SUB-ECC
```

27. Create, configure, and authenticate the root trustpoint

```
WLC-ecc(config)# crypto pki trustpoint myrootESTCA-ecc

WLC-ecc(ca-trustpoint)# enrollment terminal pem

WLC-ecc(ca-trustpoint)# chain-validation stop

WLC-ecc(ca-trustpoint)# exit

WLC-ecc(config)# crypto pki authenticate myrootESTCA-ecc
```

Enter the base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The C9800 should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

28. Create, configure, and authenticate the intermediate trustpoint:

```
WLC-ecc(config)# crypto pki trustpoint mysubESTCA-ecc

WLC-ecc(ca-trustpoint)# enrollment terminal pem

WLC-ecc(ca-trustpoint)# chain-validation continue myrootESTCA-ecc

WLC-ecc(ca-trustpoint)# match certificate est

WLC-ecc(ca-trustpoint)# subject-name C=<two letter country code>, ST=<two letter state
code>, L=<locality>, O=<organization>, OU=<organizational unit>, CN=<Common Name>
```

Note: The Common Name needs to be different than the one created for RSA certificates and needs to match the hostname.

For example: `subject-name C=US, ST=MA, L=Boxborough, O=STO, OU=GCT, CN=C9800-ecc`

29. Provide the key pair and label:

```
WLC-ecc(ca-trustpoint)# eckeypair LSC-SUB-ECC

WLC-ecc(ca-trustpoint)# exit
```

30. Authenticate the trustpoint

```
WLC-ecc(config)# crypto pki authenticate mysubESTCA-ecc
```

Enter the base 64 encoded intermediate CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

31. Generate a certificate signing request for the C9800

```
WLC-ecc(config)# crypto pki enroll mysubESTCA-ecc
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

32. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

Save the contents in a file and distribute it to the EST Server for signing by the intermediate CA. The CA Administrator should provide the signed certificate.

33. On the C9800, import the signed certificate to the subordinate trustpoint

```
WLC-ecc(config)# crypto pki import mysubESTCA-ecc certificate
```

34. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The C9800 should respond with:

"% Router Certificate successfully imported"

35. Configure the trustpoints to perform revocation checking using CRL

```
WLC(config)# crypto pki trustpoint myrootESTCA-ecc

WLC(ca-trustpoint)# revocation-check CRL

WLC(ca-trustpoint)# match key-usage cRLSign

WLC(ca-trustpoint)# exit

WLC(config)# crypto pki trustpoint mysubESTCA-ecc

WLC(ca-trustpoint)# revocation-check CRL

WLC(ca-trustpoint)# match key-usage cRLSign

WLC(ca-trustpoint)# exit
```

Manually Obtain ECC Certificates for CAPWAP/DTLS

In the section below, you will manually enroll the WLC to obtain an X.509 certificate for CAPWAP/DTLS

36. Create and authenticate the root trustpoint. This will be the same root CA certificate imported for myrootESTCA-ecc

```
WLC-ecc(config)# crypto pki trustpoint EC-estclient
```

Note: For ECC the name of the trustpoint must be preceded by "EC-". This example uses EC-estclient

```
WLC-ecc(ca-trustpoint)# enrollment terminal pem

WLC-ecc(ca-trustpoint)# subject-name C=US, ST=MA, L=Boxborough, O=STO, OU=GCT, CN=C9800-ecc

WLC-ecc(ca-trustpoint)# exit

WLC-ecc(config)# crypto pki authenticate EC-estclient
```

Enter the base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The WLC should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

37. On the WLC, enter the following to enroll for device certificate:

```
WLC-ecc(ca-trustpoint)# crypto pki enroll EC-estclient
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

38. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

39. Save the contents in a file on the EST Server for signing by the root CA. The CA Administrator will need to manually generate the signed certificate.

40. On the WLC, import the signed certificate to the estclient trustpoint

```
WLC-ecc(config)# crypto pki import EC-estclient certificate
```

41. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The WLC should respond with:

"% Router Certificate successfully imported"

42. On the WLC, view the certificates

```
show crypto pki certificate verbose EC-estclient
```

Ensure there is a certificate and CA certificate in the output. For example:

```
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 1005
  Certificate Usage: General Purpose
  Issuer:
```

```
    e=tac@cisco.com
    cn=myrootESTCA-ecc
    ou=GCT
    o=STO
    l=Boxborough
    st=MA
    c=US
  Subject:
    Name: C9800-ecc
    st=MA
    cn= C9800-ecc
    ou=GCT
    o=STO
    c=US
  Validity Date:
    start date: 16:03:25 EST May 5 2021
    end   date: 16:03:25 EST May 5 2023
  Subject Key Info:
    Public Key Algorithm: ecEncryption
    EC Public Key:  (384 bit)
  Signature Algorithm: SHA256 with ECDSA
  Fingerprint MD5: 57B14395 3FEB4B32 B400068D 5F4DB0F1
  Fingerprint SHA1: 9356039B 356C97BE 83F5B9F9 B1878CFB 53A0867B
  X509v3 extensions:
    X509v3 Key Usage: B8000000
      Digital Signature
      Key Encipherment
      Data Encipherment
      Key Agreement
    X509v3 Subject Key ID: 6755D26F 3824E528 9E50BAC1 C567E305 98BEA59F
    X509v3 Basic Constraints:
        CA: FALSE
    X509v3 Authority Key ID: 56488B34 4BD99239 7DE67D44 1A77521E 9E3E8DD3
    Authority Info Access:
    Extended Key Usage:
        Server Auth
        Client Auth
Cert install time: 17:48:45 EST May 5 2021
  Associated Trustpoints: EC-estclient
  Storage: nvram:tacciscocom#1005.cer

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 477ACF1C60616F773F84B9728B650DC26DC1DF65
  Certificate Usage: Signature
  Issuer:
    e=tac@cisco.com
    cn=myrootESTCA-ecc
    ou=GCT
    o=STO
    l=Boxborough
    st=MA
    c=US
  Subject:
    e=tac@cisco.com
    cn=myrootESTCA-ecc
    ou=GCT
```

```
    o=STO
    l=Boxborough
    st=MA
    c=US
  Validity Date:
    start date: 14:59:40 EST May 5 2021
    end   date: 14:59:40 EST May 5 2023
  Subject Key Info:
    Public Key Algorithm: ecEncryption
    EC Public Key:  (256 bit)
  Signature Algorithm: SHA256 with ECDSA
  Fingerprint MD5: AECC4B93 C6D2D5DC 53C928AE 29B2C75A
  Fingerprint SHA1: 80FECD22 2F73ABAF E668D90F CBA212E1 51D05172
  X509v3 extensions:
    X509v3 Key Usage: 6000000
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 56488B34 4BD99239 7DE67D44 1A77521E 9E3E8DD3
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
Cert install time: 17:48:45 EST May 5 2021
  Associated Trustpoints: EC-estclient myrootESTCA-ecc
  Storage: nvram:tacciscocom#DF65CA.cer
```

43. On the C9800, create a PKI enrollment profile. You will need to provide the host name or IP address of the EST server

```
WLC-ecc(config)# crypto pki profile enrollment myEST-ecc

WLC-ecc(ca-profile-enroll)# method-est

WLC-ecc(ca-profile-enroll)# enrollment url <url>
```

For example: `enrollment url https://estserver.cisco.com:8086`

```
WLC-ecc(ca-profile-enroll)# enrollment credential mysubESTCA-ecc

WLC-ecc(ca-profile-enroll)# exit
```

44. On the C9800, update the PKI trustpoint for the EST client

```
WLC-ecc(config)# crypto pki trustpoint EC-estclient

WLC-ecc(ca-trustpoint)# usage ssl-client

WLC-ecc(ca-trustpoint)# no enrollment terminal pem

WLC-ecc(ca-trustpoint)# match eku server-auth

WLC-ecc(ca-trustpoint)# enrollment profile myEST-ecc

WLC-ecc(ca-trustpoint)# subject-name C=US, ST=MA, L=Boxborough, O=STO, OU=GCT, CN=C9800-
ecc
```

Note: The CN needs to match the CN supplied in Step 6

```
WLC-ecc(ca-trustpoint)# revocation-check none

WLC-ecc(ca-trustpoint)# eckeypair LSC-SUB-ECC
```

Enable LSC Provisioning for AP

Perform the following steps on the Controller to configure LSC provisioning:

1. The Administrator should determine which type certificates the WLC and AP should use and then specify a ciphersuite priority. For example, if the Administrator wants to support RSA certificates, the following priority list can be specified:

```
(config)# ap dtls-ciphersuite priority 0 ECDHE-RSA-AES128-GCM-SHA256

(config)# ap dtls-ciphersuite priority 1 DHE-RSA-AES256-SHA256

(config)# ap dtls-ciphersuite priority 2 DHE-RSA-AES256-SHA

(config)# ap dtls-ciphersuite priority 3 DHE-RSA-AES128-SHA
```

   In the above example, ECDHE-RSA-AES128-GCM-SHA256 has the highest priority

   If the Administrator wants to support ECC certificates, the following priority list can be specified:

```
(config)# ap dtls-ciphersuite priority 0 ECDHE-ECDSA-AES128-GCM-SHA256

(config)# ap dtls-ciphersuite priority 1 ECDHE-ECDSA-AES256-GCM-SHA384
```

   In the above example, ECDHE-ECDSA-AES128-GCM-SHA256 has the highest priority

2. Disable fallback if AP is unable to join using LSC

```
(config)# ap lsc-provision join-attempt 0
```

3. Configure Subject-Name Parameters in LSC Certificate

```
(config)# ap lsc-provision subject-name country US state MA city Boxborough domain GCT org
STO email-address tac@cisco.com
```

   Note: Configuration of the Common Name parameter is not required for the AP. The CN field in the certificate request is auto filled with the AP's product ID and its unique hardware serial number.

4. Configure LSC Key Size

```
(config)# ap lsc-provision key-size 2048
```

5. Set the Trustpoint for LSC provisioning. In the examples used in this document, the choices are either estclient or EC-estclient

```
(config)# ap lsc-provision trustpoint <estclient | EC-estclient>
```

6. Enable LSC provisioning for Access Points.

```
(config)# ap lsc-provision

        In Non-WLANCC mode APs will be provisioning with RSA certificates with specified
        key-size configuration. In WLANCC mode APs will be provisioning with EC
        certificates with a 384 bit key.

        Are you sure you want to continue? (y/n): y
```

   The Controller will establish a TLS 1.2 mutually-authenticated connection to the EST Server and enroll the AP for a certificate.

7. The Access Points will immediately reboot. As the Access points are rebooting, set the Wireless Management Trustpoint. In the examples used in this document, the choices are either estclient or EC-estclient.

```
(config)# wireless management trustpoint <estclient | EC-estclient>
```

8. Verify Wireless Management Trustpoint status and ensure it says FIPS Suitable. For example:

```
(config)#do show wireless management trustpoint
Trustpoint Name  : EC-estclient
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9356039b356c97be83f5b9f9b1878cfb53a0867b
Private key Info : Available
FIPS suitability : Suitable
```

If it does not say FIPS Suitable, check the hostname matches the CN in the WLC's certificate.

9. To confirm the AP has joined using LSC, enter the "show ap config general" command. The output should say the AP certificate type is "Locally Significant Certificate"

```
# show ap config general | include Cert|Cisco AP Name
```

10. To confirm the DTLS ciphersuite that was successfully negotiated, enter the "show wireless dtls connections" command.

```
# show wireless dtls connections
```

Note: The TOE uses X.509v3 certificates to support authentication for DTLS connections. X.509v3 certificate validation is performed when the AP attempts to join the WLC. The AP will only be able to join the WLC and form a distributed TOE if the WLC determines the X.509v3 certificate of the AP is valid and the subject Distinguished Name field, which contains the AP's hardware serial number, matches an entry in the AP authorization list defined and maintained by the Security Administrator. The WLC will also verify the extendedKeyUsage field of the AP certificate contains the Client Authentication purpose. OCSP is not supported; therefore the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) is trivially satisfied by the TOE.

Note The TOE uses X.509v3 certificates to support authentication for TLS connections to the EST Server. The WLC determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. The WLC will also verify the extendedKeyUsage field of the TLS peer certificate contains the Server Authentication purpose. OCSP is not supported; therefore the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) is trivially satisfied by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer.

Operational Guidance for the TOE

Access Remote Administrative Interfaces

Note: The WLC provides all the capabilities necessary to centrally manage all TOE components. There is no remote trusted path administrative interface available directly on the Access Points. In addition, the TOE prohibits direct Access Point administration on the local console.

Access CLI Over SSH

From your remote management workstation, initiate a connect using SSH and supply either your public key or password credentials. Upon successful login you will be presented with privilege administrator access denoted by the 'hashtag' symbol:

```
WLC#
```

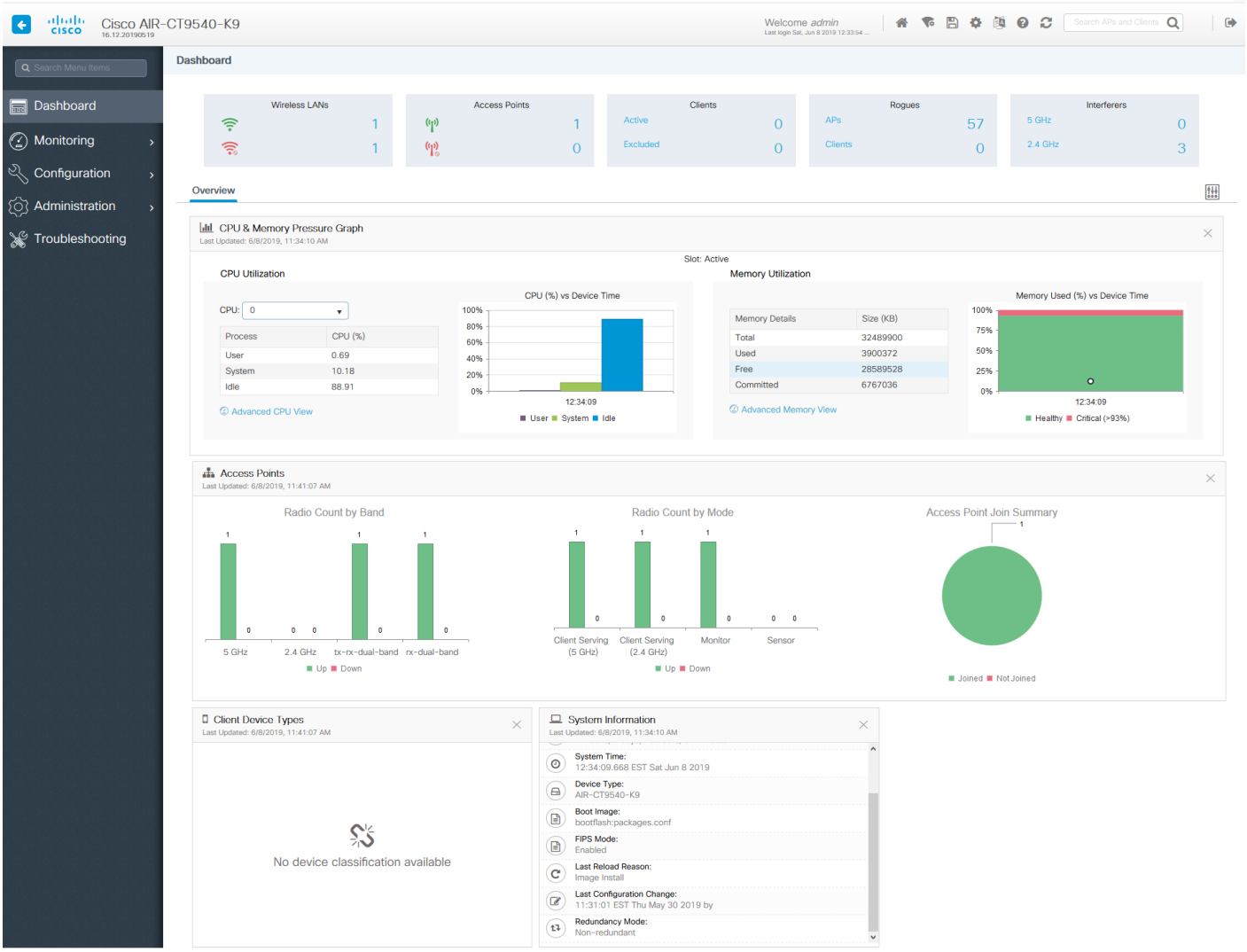
To logout of your session enter either "exit or "logout"

```
WLC# logout
```

Access Web GUI over HTTPS

From the Management workstation open a web browser to the IP address or fully-qualified domain name of the Controller. To login use the username and password credentials as for CLI/SSH.

Upon successful login you will be presented with the Dashboard page. The Dashboard displays a snapshot of the overall status and statistics for your controller.



The time stamp associated with each section indicates how recent the device status information and statistics are.

To logout click the exit icon in the top right corner:

Configure WLANs

Before configuring WLANs, it is recommended that the Administrator refer to the “Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide” [**8**] and “Understand Catalyst 9800 Wireless Controllers Configuration Model document” [**9**] before continuing with this section.

Workflows

The WLC has two built-in workflows that will enable the Administrator to create and deploy the polices for a new wireless LAN. The basic wireless setup allows you to segment the APs function with minimal effort. The advanced wireless setup allows you to segment the APs functions with more detail. The basic setup wizard can be found by navigating to Configuration -> Wireless Setup -> Basic. Refer to the

"Wireless Basic Workflow" section of [**8]** for more information. The advanced setup is under Configuration -> Wireless Setup -> Advanced. Refer to the "Wireless Advanced Workflow" section of [**8**].

During the Workflow process, when you create a new WLAN, ensure the following is set:

- Layer 2 Security Mode: WPA + WPA2
- WPA2 Encryption: Choose from the list below:
  - AES(CCMP128)
  - CCCM256
  - GCMP128
  - GCMP256
- Auth Key Mgmt: Ensure 802.1x is checked.

The configuration settings above can be found in the Security tab and Layer 2 subtab of the WLAN profile.

Manual Configuration

You can also manually configure the polices and required profiles and tags by modifying the default ones or creating custom ones. At a minimum you will need a AP Join Policy, a WLAN, a Policy Profile, and a Policy Tag.

Navigate to Configuration -> Tags and Profiles -> Policy. Double-click on the default-policy-profile. In the General tab ensure the policy is enabled by clicking the Status button to green.

In the Access Policies tab, enter the correct VLAN for your wireless clients. You may have multiple SSIDs and multiple VLANs, in which case you would need to create a custom Policy Profile for each WLAN and assign the appropriate VLAN under the Access Policies tab.

Navigate to Configuration -> Tags and Profiles -> WLANs. Click the Add button to create a new WLAN. In the General tab provide the required information and make sure to enable the WLAN by clicking the Status button to green.

In the Security tab, ensure the following is set:

- Layer 2 Security Mode: WPA + WPA2
- WPA2 Encryption: Choose from the list below:
  - AES(CCMP128)
  - CCCM256
  - GCMP128
  - GCMP256
- Auth Key Mgmt: Ensure 802.1x is checked.

Navigate to Configuration -> Tags and Profiles -> Tags. Select default-policy-tag. If you are using custom policies, this is where you would need to tie the profile components with a Policy Tag.

It is recommended the Administrator ensure the radios were re-enabled. Navigate to Configuration -> Radio Configurations -> Network. Ensure the check box next to 5GHz Network Status is checked. Tab over to 2.4 Ghz and ensure the check box next to 2.4 GHz Network Status is checked.

Enable Data DTLS

1. Navigate to Configuration -> Tags and Profiles -> AP Join.

2. Click Add to create a new AP Join Profile or click an existing profile to edit it.
3. Click CAPWAP > Advanced
4. Check Enable Data Encryption check box to enable Datagram Transport Layer Security (DTLS) data encryption.
5. Click Update & Apply to Device.

For more information on Data DTLS, refer to the "Data DTLS" chapter of [**6**].

FlexConnect

FlexConnect refers to the capability of an Access Point (AP) to decide whether the traffic from the wireless clients is put directly on the network at the AP level (Local switching) or if the traffic is centralized to the 9800 controller (Central Switching). By default, the TOE operates with Central Switching enabled. For more information on the FlexConnect feature and configuration on the Cisco 9800 Wireless Controller TOE, refer to Understand FlexConnect on Catalyst 9800 Wireless Controller [**10**].

Change Date and Time

To change the Date and/or Time, login to the Web GUI and navigate to Administration -> Time. Make necessary changes to the local time.

View Audit Events

Audit events may be viewed the WebGUI by navigating to Troubleshooting -> Logs

Alternatively audit events may be viewed at the CLI by entering:

```
WLC# show logging
```

View RADsec Server Statistics

To view up/down status and statistics of the RADsec server enter:

```
WLC# show aaa servers
```

Unblock Locked-Out Account

To unblock an account that has been prevented from logging in due to successive login failures enter the following:

```
WLC# clear aaa local user blocked username <username>
```

Adding New APs

Adding new APs to the controller depends on the method used to first join the AP to the Controller. Refer to the subsections below:

MIC

If you have a C9800-80, C9800-40, or C9800-L Controller and the MIC method was used to first join existing APs, remove the wireless management trustpoint:

```
(config)# no wireless management trustpoint <estclient | EC-estclient>
```

SSC

If you have the C9800-CL Controller set the wireless management trustpoint back to ewlc-tp1:

```
(config)# wireless management trustpoint ewlc-tp1
```

Add Serial Numbers

Add the serial numbers of the APs you are enabling to join. The serial number can also be obtained from the output of show version command on the AP.

Note: Ensure you are using the Top Assembly Serial Number for the serial number. For example:

```
(config)# username FDW2025A314 serial-number
```

Deploy New APs

Deploy the new AP and leave LSC provisioning enabled on the WLC. The AP will reboot several times to enable FIPS mode and to obtain a LSC certificate using EST. Once an LSC certificate is obtained, set the wireless management trustpoint back to estclient or EC-estclient.

```
(config)# wireless management trustpoint <estclient> | <EC-estclient>
```

Enable/Disable APs

At any point the Administrator may enable or disable APs from joining. In the Web GUI, Navigate to Configuration -> Security -> AAA. Click on AAA Advanced - Device Authentication. Click the Serial Number tab and add the AP Serial Number. To remove an AP click the checkbox next to the AP and then click the Delete button.

Cryptographic Self-Tests

All TOE components (WLC and AP) run a suite of self-tests during initial start-up to verify correct operation of cryptographic modules. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the local console. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If any of the tests fail, a message is displayed to the local console and the TOE component will automatically reboot. If the Administrator observes a cryptographic self-test failure, they should contact Cisco Technical Support. Refer to the Contact Cisco section of this document.

If the Administrator needs to execute cryptographic self-tests for the WLC after the image is loaded enter the following command:

```
WLC# test crypto self-test
```

Zeroize Private Keys

Should the Administrator need to zeroize a private key generated as instructed in the SSH, HTTPS, TLS, or DTLS sections of this document and stored in NVRAM, the following command may be used in configuration mode:

```
WLC(config)# crypto key zeroize ec | rsa <key pair label>
```

The keys are zeroized immediately after use.

Other keys stored in SDRAM are zeroized when no longer in use, zeroized with a new value of the key, or zeroized on power-cycle.

Deny Wireless Sessions

The Administrator can deny establishment of wireless client sessions based on SSID, time, day attributes. To deny based on time or day attributes, the Administrator defines “calendar profile” and tags that to the “wireless profile policy”. The wireless clients where the Administrator has applied the “wireless profile policy” are denied access to WLAN during the configured day and/or time.

For example, if the Administrator wanted to deny clients on

Thursday (during 9pm to 10pm)

Sunday (complete day)

The following steps would be followed:

wireless profile calender-profile name sun_calendar_profile

day sunday

recurrence weekly

start 00:00:01 end 23:59:59

wireless profile calender-profile name thursday_calendar_profile

day thursday

recurrance weekly

start 21:00:00 end 22:00:00

wireless profile policy default-policy-profile

calender-profile name sun_calendar_profile

action deny-client

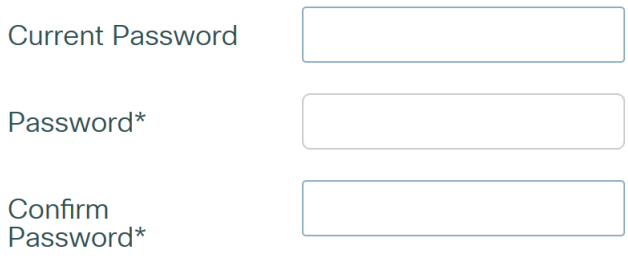
calender-profile name thursday_calendar_profile

action deny-client

For additional information refer to the "Deny Wireless Client Session Establishment Using Calendar Profiles" section of [**6**].

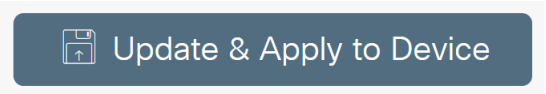
Change Password

1. To change the administrator's own password, login to the Web GUI and navigate to Administration -> User Administration and double-click on your account. You will be required to provide your current password.



Passwords may be composed of any combination of upper and lower case letters, numbers, and the special characters listed in table 4 of the document.

2. When entered, press the Update and Apply to Device button.



Add Administrative Account

To add a new administrative account login to the Web GUI and navigate to Administration -> User Administration and click Add. In the Policy drop-down box, you will need to specify the Common Criteria Password Policy. In the privilege drop-down box, select Admin. When done click Save and Apply to Device.

Delete Administrative Account

To remove an administrative account that is no longer in use, login to the Web GUI and navigate to Administration -> User Administration and click the checkbox to the left of account name to be removed. Confirm there is a checkmark then click the Delete button.

Modify Access Banner

To modify the TOE Access Banner login to the Web GUI and navigate to Administration -> Device

Enter the Banner message and click Apply.

HTTPS Session Inactivity Timeout

To modify the inactivity timeout period for HTTPS sessions, login to the Web GUI and navigate to Administration -> Management -> HTTP/HTTPS. Under Timeout Policy Configuration modify the value for Session Idle Timeout. Valid values can range from 180 to 1200 seconds. Click Apply to Device. The web server will need to restart.

IPsec Session Interruption and Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken and the Administrator will find a connection time out error message in the audit log. The administrator can use the show command below to confirm the connection is broken:

```
WLC# show crypto ipsec sa
```

When a connection is broken no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

DTLS Session Interruption and Recovery

If the DTLS connection used by the TOE for internal communication as specified in FPT_ITT.1. is unintentionally broken, the Security Administrator may find the AP is no longer listed in the Web GUI in the Monitoring Dashboard (Monitoring -> Wireless -> AP Statistics).

If this condition occurs the AP will restart the DTLS connection and attempt to re-join the WLC automatically. No Security Administrator intervention is required for the AP to recover from an interrupted DTLS session.

RADsec Session Interruption and Recovery

If a RADsec connection is unexpectedly interrupted, the TLS client connection will be broken and the Administrator will find a the state listed as DOWN in the output of show aaa servers command.

If this condition occurs no administrative interaction is required. The RADsec session will be reestablished and a new TLS client session setup once the peer is back online.

EST Server Session Interruption and Recovery

If an EST Server connection is unexpectedly interrupted during certificate enrollment, the TLS client connection will be broken and the Administrator will find the LSC provisioning for Access Points has failed. Specifically, the Access Point will not automatically reboot.

If this condition occurs the administrator will need to re-perform steps 6 - 10 in the "Enable LSC Provisioning for AP" section of this document once the EST server peer is back online.

Update WLC and AP Software

Using CLI

Using the CLI, the Administrator may install new image files in one stage (all at once) or may choose to perform stage separately.

1. Follow the steps below to update the TOE Software in one stage (all at once) using the CLI.

   a. You will need to obtain an updated 17.6 software image. Navigate to Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account and download the image for your Controller platform.

   b. Place the image on a TFTP, FTP, or SFTP server that is reachable by the WLC.

   c. At the WLC console enter: `install add file [tftp | ftp | sftp://<IP Address of TFTP/FTP/SFTP server>] <image name.bin> activate commit`

      The image installation process will begin.

   d. The WLC console will respond with "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

      Before responding 'y' to reboot, the administrator may pre-download the AP Image to the Access Points To pre-download the image for all Access Points, enter the following at the CLI:

      ```
      WLC# ap image predownload
      ```

      To verify the download status of the image to the AP enter

      ```
      WLC# show ap image
      ```

      Once the image has successfully downloaded, the Predownload Status will change to "Complete"

   e. The Administrator can query the currently installed but not yet active WLC software version by entering the following command at the CLI:

      ```
      WLC#show active install
      ```

      For the APs Administrator can query the currently installed but not yet active AP image version by entering the following command at the CLI before pre-downloading the AP image:

      ```
      WLC#show ap image
      ```

   f. To Activate the new image, return to the WLC console and respond "y" to the prompt "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

   g. The WLC will commit the new image, save the configuration, and reload. All APs that are joined to the WLC will automatically reboot when the WLC reboots.

All TOE components (WLC and AP) will automatically verify the integrity of the stored image when loaded for execution.

The WLC uses a Cisco public key to validate the digital signature to obtain an embedded SHA512 hash that was generated prior to the image being distributed from Cisco. The WLC then computes its own hash of the image using the same SHA512 algorithm. The WLC

verifies the computed hash against the embedded hash. If they match the image is authenticated and has not been modified or tampered. If they do not match the image will not boot or execute.

All hardware WLC appliances will display at bootup a message that the image was successfully validated:

`"RSA Signed RELEASE Image Signature Verification Successful."`

After boot, the authorized administrator can also manually verify the digital signature by executing on the WLC:

`verify bootflash:<image or package name>`

The AP will perform a digital signature verification check on its stored image. When successfully validated the AP will display at bootup:

`"Image signing verification success, continue to run…"`

If integrity of the stored image is not successfully verified the image will not boot or execute.

2. Follow the steps below to update the TOE Software in separate stages:

   a. You will need to obtain an updated 17.6 software image. Navigate to Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account and download the image for your Controller platform.

   b. Place the image on a TFTP, FTP, or SFTP server that is reachable by the WLC.

   c. At the WLC console enter: `WLC# copy tftp bootflash:`

      The WLC will prompt for address or name of remote host. Enter the IP address of your TFTP Sever. Once the image has successfully downloaded, the Predownload Status will change to "Complete"

      The WLC will prompt for Source filename. Enter the name of the C9800-CL bin image file.

      The WLC will begin loading the image via TFTP to bootflash:

   d. At the WLC console enter: `install add file bootflash:<C9800-CL bin file>`

      The WLC will begin installing the image file. It should respond that the image was successfully added and will display the version.

   e. If you are ready to perform the upgrade, enter: `install activate`

      The WLC should respond with "`System configuration has been modified`"

      Press Yes(y) to save the configuration and proceed.

   f. The WLC console will respond with "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

      Before responding 'y' to reboot, the administrator may pre-download the AP Image to the Access Points To pre-download the image for all Access Points, enter the following at the CLI:

      `WLC# ap image predownload`

      To verify the download status of the image to the AP enter

      `WLC# show ap image`

      Once the image has successfully downloaded, the Predownload Status will change to "Complete"

   h. The Administrator can query the currently installed but not yet active WLC software version by entering the following command at the CLI:

      `WLC#show active install`

For the APs Administrator can query the currently installed but not yet active AP image version by entering the following command at the CLI before pre-downloading the AP image:

```
WLC#show ap image
```

g. To Activate the new image, return to the WLC console and respond "y" to the prompt "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

The WLC will begin activating the image package and should respond with a list of the packages that it activated. The WLC console will then respond with a message stating the Activate stage finished and that it will now reload.

h. After the WLC has reloaded, access the CLI console and enter the following to commit the image:

```
WLC# install commit
```

The WLC should respond that it successful committed the package.

3. The administrator can verify the image is install and activated on the WLC by entering:

```
WLC# show install summary
```

The image Filename/Version should say "C" for activated and committed.

Note: At installation, the WLC extracts sub-packages from the image file that was installed (.bin) and the WLC boots using a package provisioning file, packages.conf. This provisioning file manages the bootup of each individual sub-package.

If desired, the authorized administrator can manually verify the digital signature on each individual sub-package by executing verify bootflash:<package name> on the WLC. For example:

```
WLC# verify bootflash: C9800-L-rpboot.17.06.01.SPA.pkg

WLC# verify bootflash: C9800-L-mono-universalk9_wlc.17.06.01.SPA.pkg
```

All TOE components (WLC and AP) will automatically verify the integrity of the stored image when loaded for execution.

The WLC uses a Cisco public key to validate the digital signature to obtain an embedded SHA512 hash that was generated prior to the image being distributed from Cisco. The WLC then computes its own hash of the image using the same SHA512 algorithm. The WLC verifies the computed hash against the embedded hash. If they match the image is authenticated and has not been modified or tampered. If they do not match the image will not boot or execute.

All hardware WLC appliances will display at bootup a message that the image was successfully validated:

`"RSA Signed RELEASE Image Signature Verification Successful."`

After boot, the authorized administrator can also manually verify the digital signature by executing on the WLC:

`verify bootflash:<image or package name>`

The AP will perform a digital signature verification check on its stored image. When successfully validated the AP will display at bootup:

`"Image signing verification success, continue to run…"`

If integrity of the stored image is not successfully verified the image will not boot or execute.

Using WebGUI

Follow the steps below to update the TOE Software in one stage (all at once) using the WebGUI.

1. You will need to obtain an updated 17.6 software image. Navigate to Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account and download the image for your Controller platform. You can place this image onto the Management Workstation where the Administrator accesses the WebGUI using HTTPS

2. In the WebGUI, Navigate to Administration -> Software Management

3. Select Transport Type. If using the Management Workstation select Desktop (HTTPS).
4. In Source File Path select the file where the Administrator downloaded the image onto the Management Workstation.
5. Click "Download and Install Button"
6. Once the image/package has downloaded, the status will change to Installing.
7. Once the image is installed, the Administrator may pre-download the image to the Access Point. Navigate to Configuration > Wireless > Access Points. In the Access Points page, expand the All Access Points section and click the name of the AP to edit. In the Edit AP page, click the Advanced tab and from the AP Image Management section, click Predownload.
8. In the WebGUI, under Administration -> Software Management, click the “Save Configuration & Reload” button.

Auditing

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.

The WLC, which is the component that stores audit data locally, will also transmit all audit messages in real-time to a specified external syslog server. The AP maintains its audit data in a transmission buffer and continues to do so until the AP has transferred its contents to the WLC where it is stored locally.

Table 8. Sample Audit Events

SFR	Auditable Event	Sample Audit Event Data
FAU_GEN.1.1a	Startup and Shutdown of Audit Function	<Date Time> %SYS-5-LOGGING_START: Logging enabled - CLI initiated <Date Time> %SYS-5-LOGGING_STOP: Logging disabled - CLI initiated
FAU_GEN.1.1.c	Administrative login and logout	**Web GUI Login** <Date Time> %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host <ip address> by user <admin name> using crypto cipher <cipher> **Web GUI Logout** <Date Time> %WEBSERVER-5-SESS_LOGOUT: Chassis 1 R0/0: nginx: Successfully logged out from host <ip address> by user <admin name> using crypto cipher <cipher> **SSH Login** <Date Time> %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: <admin name>] [Source: <remote ip address>] [localport: 22] at <Time Date> **SSH Logout** <Date Time> %SYS-6-LOGOUT: User <admin user> has exited tty session <session number><ip address> **Console Login** <Date Time> %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: <admin user>] [Source: LOCAL] [localport: 0] at <Time Date> **Console Logout** <Date Time> %SYS-6-LOGOUT: User <admin user> has exited tty session 0

FAU_GEN.1.1.c	Changes to TSF data related to configuration changes	See Table 8 in the next section
FAU_GEN.1.1.c	Generating/import of, changing, or deleting of cryptographic keys.	<Date Time> %CRYPTO_ENGINE-5-KEY_ADDITION: A key named <label> has been generated or imported by crypto-engine <Date Time> %CRYPTO_ENGINE-5-KEY_DELETED: A key named <label> has been removed from key storage <Date Time> Generating an EC private key <Date Time> Done delete object status 1/TAM_SUCCESS!
FAU_GEN.1.1.c	Resetting passwords	<Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:username <admin user> privilege 15 password * <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:!config: USER TABLE MODIFIED
FAU_GEN.1.1.c	Starting and stopping services	**Web Server** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<Admin User> logged command: ip http server <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<Admin User> logged command:no ip http server **SSH** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<Admin User> logged command: ip ssh version 2 <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<Admin User> logged command:no ip ssh version 2 **IPsec** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<Admin User> logged command:crypto map <crypto map tag> <Date Time> %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<Admin User> logged command:no crypto map <Date Time> %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	<Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:username <serial number> serial-number <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:no username <serial number> serial-number

FCS_IPSEC_EXT.1	Protocol failures. Establishment/Termination of an IPsec SA.	**Establishment** <Date Time> IPSEC:(SESSION ID)(create_sa) sa created <Date Time> IKEv2:(SA ID = <ID>):[IPsec -> IKEv2] Creation of IPsec SA into IPsec database PASSED **Termination** <Date Time> IPSEC:(SESSION ID = 1) (delete_sa) deleting SA **Protocol Failures** <Date Time> IKEv2-ERROR:(SESSION ID = <ID>,SA ID = <ID>):Initial exchange failed: Initial exchange failed <Date Time> IKEv2-ERROR:(SESSION ID = <ID>,SA ID = <ID>):: Received no proposal chosen notify
FCS_DTLSS_EXT.1	Failure to establish a DTLS session Detected replay attacks	**Failure to Establish DTLS Session** <Date Time> %CAPWAPAC_SMGR_TRACE_MESSAGE-3-EWLC_GEN_ERR: Chassis 1 R0/0: wncd: Error in Session-IP:<IP Address>[5272] CAPWAP DTLS session closed for AP, cause: DTLS handshake error **Detected Replay** <Date Time>: %DTLS_AUDIT_MESSAGE-6-FIPS_AUDIT_FCS_DTLSS_EXT_2_DTLS_REPLAY_ATTACK_DETECTED: Chassis 1 R0/0: wncd: User ID: 003a.7dd9.e09c - DTLS Replay Attack detected for Source IP <ip address>[5264] and Dest IP <ip address>[5246] <Date Time> %IOSXE-3-PLATFORM: Chassis 1 R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00000004339858625462 %DTLS-3-REPLAY_ERROR_DTLS: DTLS anti-replay error, src_addr <ip address>, src_port 52347, dest_addr <ip address>, dst_port 5247
FCS_DTLSS_EXT.2	Failure to authenticate the client	<Date Time> {wncd_x_R0-0}{1}: [errmsg] [18046]: (info): %DTLS_AUDIT_MESSAGE-6-FIPS_AUDIT_FPT_ITT_1_DTLS_SESSION_HANDSHAKE_FAILURE: User ID: 4c77.6d9e.6252 - Failed to complete DTLS handshake with peer, reason: certificate verify failed
FCS_DTLSC_EXT.1	Failure to establish a DTLS session	<Date Time> dtls_verify_server_cert: X509 verify cert error rc: 1 error:0 <Date Time> dtls_verify_server_cert: Controller Discovery Name does not match certificate CN
FCS_DTLSC_EXT.2	Detected replay attacks	<Date Time> dtls_log_replay: dtls_log_replay replay detected <Date Time> dtls_log_replay: dtls_log_replay: DTLS Replay Attack detected for Source IP <IP Address[port]> and Destination IP <IP Address[port]>

FCS_SSHS_EXT.1	Failure to establish an SSH session; Reason for failure	`<Date Time> %SSH-3-NO_MATCH: No matching cipher found: <invalid cipher>`
		
		`<Date Time> %SSH-3-NO_MATCH: No matching mac found: <invalid mac>`
		
		`<Date Time> %SSH-3-NO_MATCH: No matching kex algorithm found: <invalid key algorithm>`

FCS_HTTPS_EXT.1 FCS_TLSS_EXT.1	Failure to establish a HTTPS Session; Reason for failure Failure to establish a TLS Session; Reason for failure	`<Date Time> %WEBSERVER-5 CONNECTION_FAILED: Chassis 1 R0/0: nginx: connection failed from host <IP address> - Cipher Mismatch/No shared cipher`
FCS_TLSC_EXT.2	Failure to establish a TLS session; Reason for failure	`<Date Time> %RADSEC_AUDIT_MESSAGE User ID: <IP Address> Failure to establish a TLS session with RadSec server, reason: Handshake failed, other errors while in handshake phase`
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g, disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	`<Date Time> %AAA-5-LOCAL_USER_BLOCKED: User <user> blocked for login till <Time Date>`

FIA_UIA_EXT.1 FIA_UAU_EXT.2	All use of the authentication mechanism.	**WebGUI Authentication Success** <Date Time> %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host <ip address> by user <admin name> using crypto cipher <cipher> **WebGUI Authentication Failure** <Date Time> %WEBSERVER-5-LOGIN_FAILED: Chassis 1 R0/0: nginx: Login Un-Successful from host <ip address> by user <admin user> using crypto cipher <cipher> **SSH Authentication Success** <Date Time> %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: <admin user>] [Source: <source ip>] [localport: 22] at <Time Date> **SSH Authentication Failure** <Date Time> %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: <admin user>] [Source: <source ip>] [localport: 22] [Reason: Login Authentication Failed] at <Time Date> **Console Authentication Success** <Date Time> %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: <admin user>] [Source: LOCAL] [localport: 0] at <Time Date> **Console Authentication Failure** <Date Time> %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: <admin user>] [Source: <LOCAL] [localport: 0] [Reason: Login Authentication Failed] at <Time Date>
FIA_UAU.6	Attempts to re-authenticate; Origin of the attempt	<Date Time> %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: <admin user>] [Source: <source ip>] [localport: 80] at <Time Date>

FIA_8021X_EXT.1	Attempts to access to the 802.1X controlled port prior to successful completion of the authentication exchange.	<Date Time> %SESSION_MGR-5-FAIL: Chassis 1 R0/0: wncd: Authorization failed or unapplied for client <MAC Address> on Interface capwap_90000004 AuditSessionID 4554530A000000464FC95A8D. Failure reason: Authc fail. Authc failure reason: Cred Fail. <Date Time> %DOT1X-5-FAIL: Chassis 1 R0/0: wncd: Authentication failed for client (MAC Address) with reason (Timeout) on Interface capwap_90000004 AuditSessionID 4554530A00000010E0366187 Username: <CN Name> <Date Time> %DOT1X-5-FAIL: Chassis 1 R0/0: wncd: Authentication failed for client (MAC Address) with reason (Timeout) on Interface capwap_90000004 AuditSessionID 4554530A00000010E0366187 Username: <CN Name> <Date Time> %SESSION_MGR-5-FAIL: Chassis 1 R0/0: wncd: Authorization failed or unapplied for client (MAC Address) on Interface capwap_90000004 AuditSessionID 4554530A00000010E0366187. Failure reason: Authc fail. Authc failure reason: Timeout. <Date Time> %CLIENT_EXCLUSION_AUDIT_MESSAGE-3-FIPS_AUDIT_FTA_TSE_1_CLIENT_ASSOCIATION_REJECTED: Chassis 1 R0/0:wncd: Client (MAC Address) association rejected and blacklisted, reason: 802.1X authentication timeout

FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	**Expired Certificate** <Date Time> %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: 09) has expired. Validity period ended on <Date Time> **Absent or invalid basicConstraint flag** <Date Time> CRYPTO_PKI: status = 65535: failed to insert CA cert. It is not a CA certificate. **Revoked Certificate** <Date Time> %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 1F) is revoked **CRL Incorrectly Signed** <Date Time> CRYPTO_PKI: CRL verify has failed <Date Time> %PKI-3-CRL_INSERT_FAIL: CRL download for trustpoint <trustpoint name> has been discarded. Reason : failed to verify CRL signature **Untrusted Certificate** <Date Time> CRYPTO_PKI: (A6267) No suitable trustpoints found **Invalid Certificate** <Date Time> CRYPTO_PKI: (A28AF) Certificate validation failed **Signature Validation Failure** <Date Time> ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature
	Any addition, replacement or removal of trust anchors in the TOE's trust store	**Addition of Trust Anchors** <Date Time> CRYPTO_PKI: Creating trustpoint <trustpoint name> <Date Time> CRYPTO_PKI: trustpoint <trustpoint name> authentication status = 0 <trustpoint name> A CA certificate has been installed Issuer-name : e=,cn=,ou=,o=,l=,st=,c= Subject-name : e=,cn=,ou=,o=,l=,st=,c= Serial-number: <serial number> End-date : <date> **Removal of Trust Anchors** <Date Time> CRYPTO_PKI: Deleting trustpoint <trustpoint name>

FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate	**Expired Certificate** <Date Time> %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: 09) has expired. Validity period ended on <Date Time> **Absent or invalid basicConstraint flag** <Date Time> CRYPTO_PKI: status = 65535: failed to insert CA cert. It is not a CA certificate. **Invalid Certificate** <Date Time> %DTLS_TRACE_MSG-3-EWLC_DTLS_ERR: Chassis 1 R0/0: wncd: DTLS Error, session:<IP Address>[port], Certificate validation failed <Date Time> dtls_verify_server_cert: Controller Discovery Name does not match certificate CN **Signature Validation Failure** <Date Time> ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature
	Any addition, replacement or removal of trust anchors in the TOE's trust store	**Addition of Trust Anchors** <Date Time> CRYPTO_PKI: Creating trustpoint <trustpoint name> <Date Time> LSC_ENABLE: saving ROOT_CERT **Removal of Trust Anchors** <Date Time> CRYPTO_PKI: Deleting trustpoint <trustpoint name> <Date Time> Done delete object status 1/TAM_SUCCESS!
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	<Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:!exec: enable install_add_activate_commit: START <Date Time>

FMT_SMF.1	All management activities of TSF data.	**Unblock Locked Account** <Date Time> %AAA-5-USER_RESET: User <admin user> failed attempts reset by <admin user> on console | vty <number> (ip address) **Importing certificates into the TOE's trust store** <Date Time> CRYPTO_PKI: make trustedCerts list for <trustpoint name> **Designating X509.v3 certificates as trust anchors** <Date Time> CRYPTO_PKI: Creating trustpoint <trustpoint name> <Date Time> CRYPTO_PKI: Deleting trustpoint <trustpoint name> **Setting the Time** <Date Time> %SYS-6-CLOCKUPDATE: System clock has been updated from <Time> <Date> to <Time> <Date>, configured from console by <Admin User> on console | vty <number> **Manage the cryptographic keys** <Date Time> %CRYPTO_ENGINE-5-KEY_ADDITION: A key named <label> has been generated or imported by crypto-engine <Date Time> %CRYPTO_ENGINE-5-KEY_DELETED: A key named <label> has been removed from key storage **Unblock Locked Account** <Date Time> %AAA-5-USER_RESET: User <admin user> failed attempts reset by <admin user> on console | vty <number> (ip address) **SSH Rekeying Thresholds** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:ip ssh rekey time <time> <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:ip ssh rekey volume <volume> **Configure Audit Behavior** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:logging buffered 150000000 <Date Time> %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host <IP Address> port 514 started - CLI initiated **Configure the lifetime for IPsec SAs** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:crypto ipsec security-association lifetime seconds <seconds> **Configure the reference identifier** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:tls match-server-identity hostname <radsec server fqdn>

		<Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:tls match-server-identity ip-address <radsec server ip address> <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:alt-subject-name eq <ipsec peer fqdn> **Configure the interaction between TOE components** <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:username <serial number> serial-number <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:no username <serial number> serial-number **Start and Stop Services** See audit event for FAU_GEN.1.1.c **Local Message Log Cleared** <Date Time> <Admin User> administratively cleared message log
FPT_FLS.1	Failure of the TSF and the type of failure that occurred.	**WLC** <Date Time> %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed <algorithm> encryption/decryption <Date Time> %PMAN-3-PROCFAIL: R0/0: The process keyman has failed (rc 1) <Date Time> %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger **AP** <Date Time> <Algorithm> encryption/decryption…Failed!

FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**Initiation** <Date Time> %DTLS_AUDIT_MESSAGE-6-FIPS_AUDIT_FPT_ITT_1_DTLS_SESSION_ESTABLISHED: Chassis 1 R0/0: wncd: User ID: <AP Name> - DTLS connection established with peer, cipher DHE-RSA-AES256-SHA256 <Date Time> Sending Join request to <IP Address> through port <port> **Termination** <Date Time> %DTLS_AUDIT_MESSAGE-6-FIPS_AUDIT_FPT_ITT_1_DTLS_SESSION_CLOSED: Chassis 1 R0/0: wncd: User ID: <AP Name> - DTLS peer has closed the connection, cipher DHE-RSA-AES256-SHA256 <Date Time> %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/0: wncd: AP Event: AP Name: <AP Name> MAC: <MAC Address> Disjoined <Date Time> CAPWAP State: DTLS Teardown **Failure** <Date Time> %CAPWAPAC_SMGR_TRACE_MESSAGE-3-EWLC_GEN_ERR: Chassis 1 R0/0: wncd: Error in Session-IP:<IP Address>[5272] CAPWAP DTLS session closed for AP, cause: DTLS handshake error <Date Time> Dropping dtls packet since session is not established. Peer <IP Address-5246, Local <IP Address>-<Port> conn (nil)
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	<Date Time> %SYS-6-CLOCKUPDATE: System clock has been updated from <Time> <Date> to <Time> <Date>, configured from console by <Admin User> on console | vty <number>
FPT_TST_EXT.1	Execution of this set of TSF-self-tests. Detected integrity violations.	**WLC – Self-Test Admin Executed** <Date Time> %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test activated by <Admin Name> on console | vty <number> (<IP Address>)) **WLC – Detected integrity Violation** <Date Time> %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file bootflash:<Image Name> <Date Time> %INSTALL-3-OPERATION_ERROR_MESSAGE: Error: File bootflash:<Image Name> is corrupt or is not a valid package. **Access Points – Self-Test Execution** "Image signing verification success, continue to run..." Console Message **Access Points – Detected integrity Violation** "Image signing verification failure(-3), not allowed to run…" Console Message

FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	**WLC – Initiation** <Date Time> %INSTALL-5-INSTALL_START_INFO: Chassis 1 R0/0: install_engine: Started install one-shot bootflash:<image name> SUCCESS: install_add_activate_commit <Date Time> **WLC – Success** SUCCESS: install_add_activate_commit <Date Time> Console Message **WLC – Failed** May 16 14:44:09.020: %INSTALL-3-OPERATION_ERROR_MESSAGE: Chassis 1 R0/0: install_engine: Failed to install_add package bootflash: <image name>, Error: install_add : bootflash: <image name> is not valid file or cannot be handled by install CLI. **AP – Initiation** <Date Time> %UPGRADE-5-AP_SW_UPDATE_LOG_MSG: Chassis 1 R0/0: wncmgrd: AP SW update predownload is in progress **AP – Success** <Date Time> %UPGRADE-5-AP_SW_UPDATE_LOG_MSG: Chassis 1 R0/0: wncmgrd: AP SW update Predownload is successful <Date Time> %APMGR_AUDIT_MESSAGE-6-FIPS_AUDIT_FCS_COP_1_DataEncryption: Chassis 1 R0/0: wncd: AP <AP Name> User ID: Admin AP_IMAGE_INTEGRITY_CHECK INVALID_KEY_TYPE Success **AP – Failed** <Date Time> %APMGR_AUDIT_MESSAGE-6-FIPS_AUDIT_FCS_COP_1_DataEncryption: Chassis 1 R0/0: wncd: AP <AP Name> User ID: Admin AP_IMAGE_INTEGRITY_CHECK INVALID_KEY_TYPE FAILED
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	<Date Time> %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user <admin user>
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	**SSH** <Date Time> %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty <number> <(ip address)>, user <admin user> **Web GUI** <Date Time> %WEBSERVER-5-SESS_LOGOUT: Chassis 1 R0/0: nginx: Successfully logged out from host <ip address> by user <admin name> using crypto cipher <cipher>

FTA_SSL.4	The termination of an interactive session.	**Web GUI Logout** <Date Time> %WEBSERVER-5-SESS_LOGOUT: Chassis 1 R0/0: nginx: Successfully logged out from host <ip address> by user <admin name> using crypto cipher <cipher> **SSH Logout** <Date Time> %SYS-6-LOGOUT: User <admin user> has exited tty session <session number><ip address> **Console Logout** <Date Time> %SYS-6-LOGOUT: User <admin user> has exited tty session 0
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	<Date Time> %CLIENT_ORCH_AUDIT_MESSAGE-3-FIPS_AUDIT_FCS_DENY_CLIENT_ACCESS: Chassis 1 R0/0: wncd: User ID: <MAC Address>- - Client association rejected as it is not in Active Hours slot
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions (including IEEE 802.11). Detection of modification of channel data.	**TLS – Initiation** <Date Time> RADIUS_RADSEC_CLIENT_HS_START: TLS handshake in progress...<IP Address/2083> **TLS – Termination** <Date Time>: RADIUS_RADSEC_IDLE_TIMER_HDLR: No RADSEC activity since last idle timeoout, server <IP address>/2083 - Closing RADSEC connection now **TLS – Failure** <Date Time> %RADSEC_AUDIT_MESSAGE User ID: <IP Address> Failure to establish a TLS session with RadSec server, reason: Handshake failed, other errors while in handshake phase **IEEE 802.11 - Failure** <Date Time> %CLIENT_EXCLUSION_AUDIT_MESSAGE-3-FIPS_AUDIT_FTA_TSE_1_CLIENT_ASSOCIATION_REJECTED: Chassis 1 R0/0:wncd: Client <MAC Address> association rejected and blacklisted, reason: 802.11 association failure **Detection of modification of channel data** <Date Time> %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/0: wncd: AP Event: AP Name: <AP Name> Mac: <AP Mac Address> Session-IP: <IP Address[<port>]> <IP Address[<port>]> Disjoined Heart beat timer expiry For IPsec Refer to the audit messages under FCS_IPSEC_EXT.1

FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	**WebGUI Initiation** <Date Time> %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host <ip address> by user <admin name> using crypto cipher <cipher> **SSH Initiation** <Date Time> %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: <admin user>] [Source: <source ip>] [localport: 22] at <Time Date> **WebGUI Termination** <Date Time> %WEBSERVER-5-SESS_LOGOUT: Chassis 1 R0/0: nginx: Successfully logged out from host <ip address> by user <admin name> using crypto cipher <cipher> **SSH Termination** <Date Time> %SYS-6-LOGOUT: User <admin user> has exited tty session <session number><ip address> **WebGUI Failure** <Date Time> %WEBSERVER-5 CONNECTION_FAILED: Chassis 1 R0/0: nginx: connection failed from host <IP address> - Cipher Mismatch/No shared cipher **SSH Failure** <Date Time> %SSH-3-NO_MATCH: No matching cipher found: <invalid cipher> <Date Time> %SSH-3-NO_MATCH: No matching mac found: <invalid mac> <Date Time> %SSH-3-NO_MATCH: No matching kex algorithm found: <invalid key algorithm>

For administrative actions related to TSF data related to configuration changes, refer to the table below

Table 9. Admin Actions Related to TSF Data Related Configuration Changes

Action	Command	Sample Audit Event Data

Resetting Passwords	Navigate to Administration -> User Administration and double-click on your account. You will be required to provide your current password. When password has been entered press the Update and Apply to Device button.	<Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:username <admin user> privilege 15 password * <Date Time> %PARSER-5-CFGLOG_LOGGEDCMD: User:<admin user> logged command:!config: USER TABLE MODIFIED
Importing certificates into the TOE's trust store	WLC(config)# crypto pki import <trustpoint name> certificate	<Date Time> CRYPTO_PKI: make trustedCerts list for <trustpoint name>
Designating X509.v3 certificates as trust anchors	WLC(config)# crypto pki authenticate trustpoint name>	<Date Time> CRYPTO_PKI: Creating trustpoint <trustpoint name> <Date Time> CRYPTO_PKI: Deleting trustpoint <trustpoint name>
Setting the Time	Navigate to Administration -> Time -or – WLC# clock set hh : mm : ss date month year	<Date Time> %SYS-6-CLOCKUPDATE: System clock has been updated from <Time> <Date> to <Time> <Date>, configured from console by <Admin User> on console | vty <number>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.