Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.2 for Japan (Release Version 17.2.1)

First Published: 2020-04-23

Last Modified: 2020-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

REVIEW DRAFT - CISCO CONFIDENTIAL

REVIEW DRAFT - CISCO CONFIDENTIAL

CHAPTER 1

Overview

Catalyst 9800 and EWC test

Cisco Catalyst 9800 and EWC test , an integral part of the enterprise wireless solution, is a program that validates various Cisco Wireless Products and Features. This is achieved by testing the latest versions of Cisco wireless products

Cisco Catalyst 9800 and EWC for Japan , in turn is an add-on testing at the solution level, where the requirements gathered are specific to Japanese usage and market. The requirements are derived based on the following:

- New features in Catalyst 9800 and EWC 17.2
- High priority scenarios and basic regression features
- Inputs from Cisco SEs/ TAC

The test execution is carried out on selected Cisco Wireless LAN products, which affect the Japanese segment that are prioritized by Cisco Japan team.

The following products are covered in the test execution:

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Virtual Elastic Wireless LAN Controller 9800
- Cisco Catalyst 9800-CL
- Cisco Embedded Wireless Controller on Catalyst Access Points
- Cisco Wireless LAN Controller 8540
- Cisco Wireless LAN Controller 5520
- Cisco Wireless LAN Controller 3504
- Cisco Mobility Express 1850
- Cisco Mobility Express 1830
- Cisco Mobility Express 1815I

- Cisco Mobility Express 2800
- Cisco Mobility Express 3800
- Cisco Mobility Express 4800
- Cisco Mobility Express 1562
- APIC-EM Controller appliance
- Connected Mobile Experiences (CMX)
- Cisco Prime Infrastructure (Physical-UCS,VM)
- ISE(VM)
- 9800 Controller
- Cisco ISR 1100
- Cisco AP c9115
- Cisco AP c9120
- Cisco AP c9130
- Autonomous AP
- Access Point 4800
- Access Point 3800
- Access Point 2800
- Access Point 3700
- Access Point 2700
- Access Point 1700
- Access Point 1570
- Access Point 1542
- Access Point 1530
- Access Point 702I
- Access Point 1850
- Access Point 1830
- Access Point 1815I
- Access Point 1815W
- Access Point 1810

Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server
AKM	Authentication Key Management
AP	Access Point
API	Application Programming Interface
APIC-EM	Application Policy Infrastructure Controller - Enterprise Module
ATF	Air-Time Fairness
AVC	Application Visibility and Control.
BGN	Bridge Group Network
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CA	Central Authentication
CAC	Call Admissions Control
CAPWAP	Control and Provisioning of Wireless Access Point
CCKM	Cisco Centralized Key Management
CCN	Channel Change Notification
CCX	Cisco Compatible Extensions
CDP	Cisco Discovery Protocol
CKIP	Cisco Key Integrity Protocol
CMX	Connected Mobile Experience
CVBF	Cisco Vector Beam Forming
CWA	Central Web Authentication
DCA	Dynamic Channel Assignment
DMZ	Demilitarized Zone
DNS	Domain Name System
DNA-C	Digital Network Architecture Center
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol

Acronym	Description
EULA	End User Licence Agreement
EWC	Embedded Wireless Controller
FLA	Flex Local Authentication
FLS	Flex Local Switching
FT	Fast Transition
FTP	File Transfer Protocol
FW	Firm Ware
HA	High Availability
H-REAP	Hybrid Remote Edge Access Point
IOS	Internetwork Operating System
ISE	Identity Service Engine
ISR	Integrated Services Router
LAG	Link Aggregation
LEAP	Lightweight Extensible Authentication Protocol
LSS	Location Specific Services
LWAPP	Lightweight Access Point Protocol
MAP	Mesh Access Point
MCS	Modulation Coding Scheme
MFP	Management Frame Protection
mDNS	multicast Domain Name System
MIC	Message Integrity Check
MSE	Mobility Service Engine
MTU	Maximum Transmission Unit
NAC	Network Admission Control
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCS	Network Control System
NGWC	Next Generation Wiring closet
NMSP	Network Mobility Services Protocol
OEAP	Office Extended Access Point
PEAP	Protected Extensible Authentication Protocol
PEM	Policy Enforcement Module

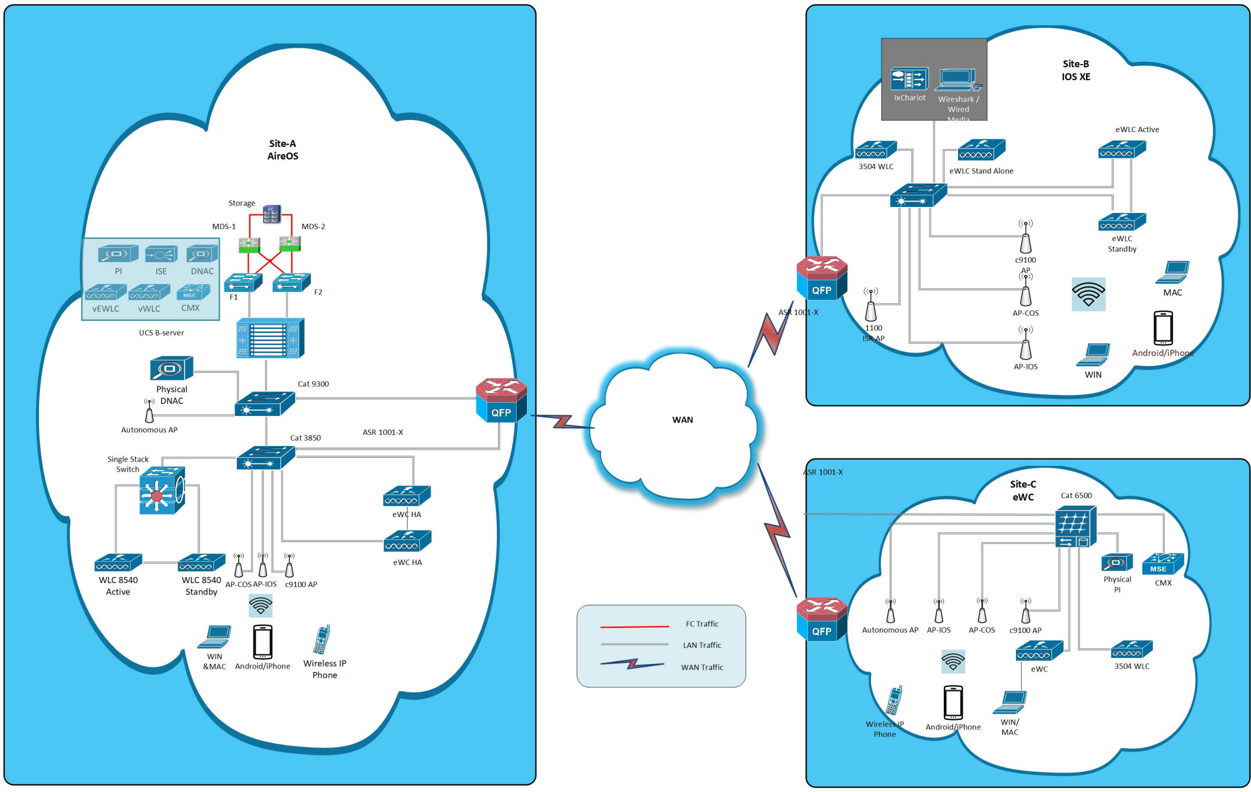
Acronym	Description
PI	Prime Infrastructure
PMF	Protected Management Frame
POI	Point of Interest
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Pre-shared Key
QOS	Quality of service
RADIUS	Remote Authentication Dial-In User Service
RAP	Root Access Point
RP	Redundancy Port
RRM	Radio Resource Management
SDN	Software Defined Networking
SOAP	Simple Object Access Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SS	Spatial Stream
SSID	Service Set Identifier
SSO	Single Sign On
SSO	Stateful Switch Over
SWIM	Software Image Management
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
vWLC	Virtual Wireless LAN Controller
VPC	Virtual port channel
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WGB	Workgroup Bridge
wIPS	Wireless Intrusion Prevention System
WLAN	Wireless LAN
WLC	Wireless LAN Controller

Acronym	Description
WPA	Wi-Fi Protected Access
WSM	Wireless Security Module

CHAPTER 2

Test Topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Cisco Catalyst 9800 Series Wireless Controller	17.2
	Cisco Catalyst 9800-CL	17.2
	Cisco Catalyst 9800-L Wireless Controller	17.2
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.2
	Wireless LAN Controller 8540	8.10.105.0
	Wireless LAN controller 5520	8.10.105.0
	Wireless LAN controller 3504	8.10.105.0
	Virtual Controller	8.10.105.0
	CME 1562/1850/1830	8.10.105.0
	CME 4800/3800/2800	8.10.105.0
Applications	Cisco DNA Center	2.1.1.0
	ISE(VM)	2.7
	CMX(Physical (3375), VM)	10.6
	Prime Infrastructure (Virtual Appliance, UCS based)	3.8
	MSE(Physical (3365), VM)	8.0.150.0
	APIC-EM Controller appliance	1.6
	Cisco Jabber for Windows, iPhone	12.6.0
	Cisco Air Provisioning App	1.4
	Cisco Wireless App	1.0.228

Category	Component	Version
Access Point	Cisco AP 9115	17.2
	Cisco AP 9120	17.2
	Cisco AP 9130	17.2
	Cisco 1100 ISR	17.2
	Cisco AP 4800	15.3
	Cisco AP 3800	15.3
	Cisco AP 2800	15.3
	Cisco AP 3700	15.3
	Cisco AP 2700	15.3
	Cisco AP 1700	15.3
	Cisco AP 1850	15.3
	Cisco AP 1830	15.3
	Cisco AP 1815	15.3
	Cisco AP 1810	15.3
	Cisco AP 1570	15.3
	Cisco AP 1562	15.3
	Cisco AP 1542	15.3
	Cisco AP 1532	15.3
	Cisco AP 702I	15.3
Switch	Cisco Cat 9300	17.2
	Cisco Cat 9200L	17.2
	Cisco Cat 9800	17.2
	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
Chipset	5300, 6300 AGN	15.40.41.5058
	7265 AC	20.120.0
	Airport Extreme	7.7.9

Category	Component	Version
Client	Operating System(JOS)	Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 10.15
	iPad Pro	iOS 13.3.1
	iPhone 6, 6S ,7 & 11 (JP Locale)	iOS 13.3.1
	Samsung Galaxy S7,S10, Nexus 6P, Sony Xperia XZ	Android 10.0
	Wireless IP Phone 8821	11.0.4-14
	End points	Windows 7 Enterprise
		Apple Mac 10.15
		Windows 8 & 8.1
		iPhone 6,6S ,7 & 11
		Windows 10
		Samsung Galaxy S4, S7,S10, Nexus 6P, Sony Xperia
	Cisco AnyConnect VPN Client	4.8.175
Module	Hyper location Module	NA
Active Directory	AD	Windows 2008R2 Enterprise
Call Control	Cisco Unified Communications Manager	12.5.0.99832-3/12.5.0.99832-3-1(JP)
Browsers	IE	11.0.180
	Mozilla Firefox	75
	Safari	13.1
	Chrome	80

What's New ?

EWC

- APSP/APDP support in WebUI for EWLC-ME
- Fabric In A Box
- ME WLAN Simplication
- WGB client support on ME

Cisco Catalyst 9800 Series Wireless Controller

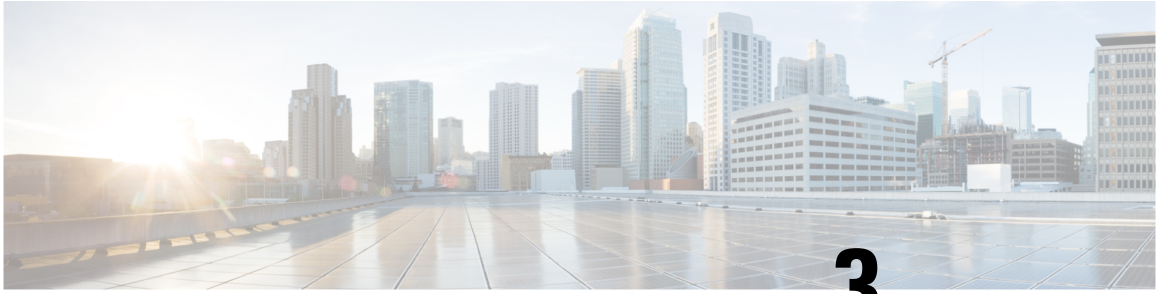
- Multi LAG and Load Balancing based on VLAN and SSO
- Client_logging
- Open Roaming
- BSSIDCounters
- QBSS Load Information Element(IE)
- Opportunistic Key Caching
- TWT_support on AP9115
- Google: DHCP Required
- Client Whitelisting
- Flex LS Client IP Context Distribution from Controller
- WPA3 Support

Open Caveats

Defect ID	Title
CSCvt03729	Without SAE AKM user able to create a WLAN with WPA3-PSK SHA256 security.
CSCvt78675	Observed a crash in Cisco Catalyst 9800-80 Wireless Controller 17.2.1 : kernel.rp_2DA Core
CSCvt62485	Transition mode wlan id is configuring as default "0"
CSCvt32458	M4 packet is missing while connecting client to WPA2+WPA3 Mixed mode WLAN in local auth flexmode
CSCvt80745	Difficult to validate BSSID and other parameters
CSCvt05220	5GHz Radio status is not Enabled via fix it now button in best practice page
CSCvt75173	Unable to add/delete whitelist user with WLAN
CSCvt34942	Device type Un-classified in both UI & CLI
CSCvt61099	Help link redirected to 404 page not found error under "Best Practice page"in eWC UI
CSCvt73441	Able to create WLAN with WPA+WPA2-PSK+CCKM AKM s.
CSCvt93222	Image Pre download happening after reactivating the APDP image from GUI

Resolved Caveats

Defect ID	Title
CSCvt75752	ATF -Optimization status showing disable in Japanese GUI
CSCvt36036	config->vlan page is keep loading when landing to this page



CHAPTER 3

New Features

WPA3 Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_WPA3_01	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE security Configuration.	Passed	
EWLCJ172S_WPA3_02	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the Client packets by connecting the windows client to WPA3 and SAE supported SSID	Passed	

EWLCJ172S_WPA3_03	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the Client packets by connecting the Android client to WPA3 and SAE supported SSID	Passed	
EWLCJ172S_WPA3_04	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the Client packets by connecting the Mac os client to WPA3 and SAE supported SSID	Failed	CSCvt03729
EWLCJ172S_WPA3_05	Verifying the WPA3 support with SAE and PSK security key.	To verify the Client packets by connecting the client to WPA3 and SAE and PSK supported SSID	Passed	
EWLCJ172S_WPA3_06	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Failed	CSCvt32458
EWLCJ172S_WPA3_07	Validating the WPA3 support with SAE and Layer 3 Splash page web redirect	To verify the WPA3 support with SAE and Layer3 Splash page web redirect	Passed	
EWLCJ172S_WPA3_08	Validating the WPA3 support with SAE and Layer 3 On Mac filter failure.	To verify the WPA3 support with SAE and Layer3 On Mac filter failure	Passed	
EWLCJ172S_WPA3_09	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ172S_WPA3_10	verifying the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	To verify the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	Passed	
EWLCJ172S_WPA3_11	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	

EWLCJ172S_WPA3_12	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security for the different clients.	Passed	
EWLCJ172S_WPA3_13	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ172S_WPA3_14	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ172S_WPA3_15	Verifying the WPA3 support and SAE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and SAE support	Passed	
EWLCJ172S_WPA3_16	Verifying the WPA3 support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Passed	
EWLCJ172S_WPA3_17	Verifying the WPA3 support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with WPA3 WLAN.	Passed	
EWLCJ172S_WPA3_18	Verifying the WPA3 support with SAE Auth key in local auth and local switching.	To verify the WPA3 support with SAE security in local auth and local switching.	Passed	

Flex LS Client IP Context Distribution from Controller

Logical ID	Title	Description	Status	Defect ID

EWLCJ172S_Flex local switching_01	IP-MAC context validation in AP	when client associates with an AP, we need to check if IP-MAC detail is shown in AP using "show ap" commands.	Passed	
EWLCJ172S_Flex local switching_02	IP-MAC context validation for MAC client in AP	when client associates with an AP, we need to check if IP-MAC detail is shown in AP using "show ap" commands.	Passed	
EWLCJ172S_Flex local switching_03	IP-MAC context validation for Android client in AP	when client associates with an AP, we need to check if IP-MAC detail is shown in AP using "show ap" commands.	Passed	
EWLCJ172S_Flex local switching_04	IP-MAC context validation for IOS client in AP	when client associates with an AP, we need to check if IP-MAC detail is shown in AP using "show ap" commands.	Passed	
EWLCJ172S_Flex local switching_05	IP-MAC context validation in multiple APs	when client associates with an AP, we need to check if IP-MAC detail is distributed by WLC to all APs.	Passed	
EWLCJ172S_Flex local switching_06	IP-MAC distribution in roaming client scenario with Central-auth configured.	When the client roams, the AP associating at that instance will receive IP-MAC context from WLC. This is checked in Central-auth config.	Passed	

EWLCJ172S_Flex local switching_07	IP-MAC distribution in roaming client scenario with Local-auth configured.	When the client roams, the AP associating at that instance will receive IP-MAC context from WLC. This is checked in Local-auth config.	Passed	
EWLCJ172S_Flex local switching_08	IP-MAC distribution upon AP movement from standalone to connected mode.	When AP moves from standalone to connected mode, all client entries will be distributed by WLC at once.	Passed	
EWLCJ172S_Flex local switching_09	IP-MAC entries deletion upon AP reboot.	IP-MAC entries will be deleted when AP reboots.	Passed	

Client Whitelisting

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_Client Whitelisting_01	Creating a Lobby Admin Account in EWLC with Japanese GUI and login with Lobby user	To check whether Lobby Admin account able to create or not in EWLC with Japanese UI	Passed	
EWLCJ172S_Client Whitelisting_02	Adding & deleting a Whitelisted User & client mac address in Japanese UI	To check whether a guest user & mac address can be added /deleted or not in EWLC Japanese UI	Failed	CSCvt75173
EWLCJ172S_Client Whitelisting_03	Associating Android client with Mac filter enabled L3-Web auth SSID & Web auth Login with Manually given password	To check that Android client got associated with Mac filter enabled L3-Web auth SSID & Login with Manually given password	Passed	

EWLCJ172S_Client Whitelisting_04	Associating iOS client with Mac filter enabled L3-Web auth SSID & Login with Auto generated password	To check that Android client got associated with Mac filter enabled L3-Web auth SSID & Login with autogenerated password	Passed	
EWLCJ172S_Client Whitelisting_05	Associating iOS client with Mac filter enabled L3-Web auth SSID & Login with expired password	To check that iOS client got associated or not with Mac filter enabled L3-Web auth SSID & Login with expired password	Passed	
EWLCJ172S_Client Whitelisting_06	Associating Window 10 client with Mac filter enabled L3-Web auth SSID & Web login with guest user	To check that Window 10 client got associated with Mac filter enabled L3-Web auth SSID & Login with guest user credentials	Passed	
EWLCJ172S_Client Whitelisting_07	Associating MacOS client with Mac filter enabled L3-Web auth SSID & Web login with guest user	To check that MacOS client got associated with Mac filter enabled L3-Web auth SSID & Login with guest user credentials	Passed	
EWLCJ172S_Client Whitelisting_08	Associating MacOS client with Mac filter enabled L3-Web auth SSID & Login with expired password	To check that MacOS client got associated or not with Mac filter enabled L3-Web auth SSID & Login with expired password	Passed	
EWLCJ172S_Client Whitelisting_09	Authenticating MacOS client with Mac filter enabled L3-Web auth SSID & without adding mac address	To check that MacOS client got authenticate or not with Mac filter enabled L3-Web auth SSID	Passed	
EWLCJ172S_Client Whitelisting_10	Backup & Restore EWLC Config after lobby Accounts config	To Check that After Restore EWLC config lobby Admin accounts config available or not	Passed	

EWLCJ172S_Client Whitelisting_11	Verifying Connected Whitelisted user in lobby account	To verify that connected whitelisted user showing in Connected/Whitelisted tab	Passed	
EWLCJ172S_Client Whitelisting_12	Verifying Connected Not Whitelisted user in lobby account	To verify that connected Not Whitelisted user showing in Connected/Not Whitelisted tab	Passed	
EWLCJ172S_Client Whitelisting_13	Verifying not Connected Whitelisted user in lobby account	To verify that not connected whitelisted user showing in Connected/Whitelisted tab	Passed	
EWLCJ172S_Client Whitelisting_14	Removing the whitelisted user	To verify that whitelisted user removing or not	Failed	CSCvt75173

DHCP Required

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_DHCP Required_01	Enabling/Disabling DHCP required checkbox with Local Auth & Central switching in Japanese UI	To verifying the DHCP required checkbox enabled/disabled with local auth & central switching in Japanese UI or not	Passed	
EWLCJ172S_DHCP Required_02	Enabling/Disabling DHCP required checkbox with Central Auth or Central switching	To verifying the DHCP required checkbox enabled/disabled with central auth & central switching in Japanese UI or not	Passed	
EWLCJ172S_DHCP Required_03	Connect IOS client with DHCP require state and local auth & local switching	To connecting the IOS client with DHCP require state and local auth & local switching	Passed	

EWLCJ172S_DHCP Required_04	Connect IOS client with DHCP require state and Central auth & local switching	To connecting the IOS client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_05	Connect IOS client with DHCP require state and central auth & central switching	To connecting the IOS client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_06	Connect S10 client with DHCP require state and local auth & local switching	To connecting the S10 client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_07	Connect S10 client with DHCP require state and central auth & central switching	To connecting the S10 client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_08	Connect MACOS client with DHCP require state and local auth & local switching	To connecting the MACOS client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_09	Connect MacOS client with DHCP require state and central auth & central switching	To connecting the MacOS client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_10	Connect Windows client with DHCP require state and local auth & local switching	To connecting the Windows client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_11	Connect Windows client with DHCP require state and central auth & central switching	To connecting the Windows client with DHCP require state and local auth & local switching	Passed	
EWLCJ172S_DHCP Required_12	Roam the iOS client which connected with CA & CS and DHCP required enabled	To roaming the iOS client which connect with CA & CS and dhcp required state enabled	Passed	

EWLCJ172S_DHCP Required_13	Roam the iOS client which connected with LA & LS and DHCP required enabled	To roaming the iOS client which connect with LA & LS and dhcp required state enabled	Passed	

TWT_support on AP9115

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_TWT_01	Configuring TWT in 9115 Ap	To check Whether 9115 Ap get TWT parameter details properly	Passed	
EWLCJ172S_TWT_02	Configuring TWT in 9120 Ap	To check Whether 9120 Ap get TWT parameter details properly	Passed	
EWLCJ172S_TWT_03	Associate 5G Hz client to 9115/9120 Ap with TWT configuration.	To verify the 5GHz client associate the 9115/9120 Ap with TWT configuration or not	Passed	
EWLCJ172S_TWT_04	Associate 2.4 GHz client to 9115/9120 Ap with TWT configuration.	To verify the 2.4 GHz client associate the 9115/9120 Ap with TWT configuration or not	Passed	
EWLCJ172S_TWT_05	Configuring TWT in 11ax Ap with flexconnect mode	To verify the 11ax ap get TWT parameter in flexconnect mode	Passed	
EWLCJ172S_TWT_06	Configuring TWT in 11ax Ap with Local mode	To verify the 11ax ap get TWT parameter in Local mode	Passed	
EWLCJ172S_TWT_07	Associate the sleeping client with 11ax Ap	To Verify sleeping client associate with 11ax Ap properly or not	Passed	
EWLCJ172S_TWT_08	Clear the TWT configuration Check the Client behaviour	To verify the client behaviour after clear the TWT configuration	Passed	

Opportunistic Key Caching

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_OKC_01	Configure and verify the OKC to the WLAN configuration.	To check whether OKC configured to WLAN or not.	Passed	
EWLCJ172S_OKC_02	Configure and verify the OKC to WPA3-SAE WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA3-SAE WLAN.	Passed	
EWLCJ172S_OKC_03	Configure and verify the OKC to WPA3-SAE WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA3-SAE WLAN.	Passed	
EWLCJ172S_OKC_04	Configure and verify the OKC to WPA2-PSK WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-PSK WLAN.	Passed	
EWLCJ172S_OKC_05	Configure and verify the OKC to WPA2-PSK WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-PSK WLAN.	Passed	
EWLCJ172S_OKC_06	Configure and verify the OKC to OPEN security WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to OPEN security WLAN.	Passed	

EWLCJ172S_OKC_07	Configure and verify the OKC to OPEN security WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to OPEN security WLAN.	Passed	
EWLCJ172S_OKC_08	Configure and verify the OKC to WPA2-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-802.1x WLAN.	Passed	
EWLCJ172S_OKC_09	Configure and verify the OKC to WPA2-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-802.1x WLAN.	Passed	
EWLCJ172S_OKC_10	Configure and verify the OKC to WPA3-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA3-802.1x WLAN.	Passed	
EWLCJ172S_OKC_11	Configure and verify the OKC to WPA3-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA3-802.1x WLAN.	Passed	
EWLCJ172S_OKC_12	Configure and verify the OKC to WPA2-Ft-PSK WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-Ft-PSK WLAN.	Passed	
EWLCJ172S_OKC_13	Configure and verify the OKC to WPA2-Ft-PSKWLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-Ft-PSK WLAN.	Passed	

EWLCJ172S_OKC_14	Configure and verify the OKC to WPA2-Ft-802.1x WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2-Ft-802.1x WLAN.	Passed	
EWLCJ172S_OKC_15	Configure and verify the OKC to WPA2-Ft-802.1x WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2-Ft-802.1x WLAN.	Passed	
EWLCJ172S_OKC_16	Configure and verify the OKC to WPA2+WPA3 mixed mode WLAN with Inter roaming.	To check whether roaming happening or not after configuring the OKC to WPA2+WPA3 mixed mode WLAN.	Passed	
EWLCJ172S_OKC_17	Configure and verify the OKC to WPA2+WPA3 mixed mode WLAN with Intra roaming.	To check whether intra roaming happening or not after configuring the OKC to WPA2+WPA3 mixed mode WLAN.	Passed	

QBSS Load Information Element(IE)

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_QBSSload_01	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as allowed with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with qbss load for policy profile.	Passed	

EWLCJ172S_QBSSload_02	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile	Passed	
EWLCJ172S_QBSSload_03	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with no qbss load for policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as allowed with no qbss load for policy profile.	Passed	
EWLCJ172S_QBSSload_04	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for local AUTH policy profile.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for Local AUTH policy profile	Passed	
EWLCJ172S_QBSSload_05	Verify the QBSS load information in Beacon and Probes fames by upload/download the configuration file from controller	To check whether QBSS load showing in Beacon and Probe frames or not by upload/download the configuration file from controller	Passed	
EWLCJ172S_QBSSload_06	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Flex mode AP.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile and Flex mode AP	Passed	

EWLCJ172S_QBSSload_07	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Bridge mode AP.	To check whether QBSS load showing in Beacon and Probe frames or not by configuring WMM as required with qbss load for policy profile and Bridge mode AP	Passed	
EWLCJ172S_QBSSload_08	Verify the AP name in Beacon and Probes fames by configuring Aironet IE.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE.	Passed	
EWLCJ172S_QBSSload_09	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with modified AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with Modified AP name.	Passed	
EWLCJ172S_QBSSload_10	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and upload/download the configuration file from controller.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and upload/download the configuration file from controller.	Passed	
EWLCJ172S_QBSSload_11	Verify the AP name in Beacon and Probes fames by configuring Aironet IE with more than 15 characters of AP name.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE with more than 15 characters of AP name.	Passed	
EWLCJ172S_QBSSload_12	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and re-join the AP's to eWLC-2 from eWLC-1.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and re-join the AP's to eWLC-2 from eWLC-1.	Passed	

EWLCJ172S_QBSSload_13	Verify the Multicast filter and MC2UC traffic to local-switching client	To verify the Multicast filter and local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ172S_QBSSload_14	Verify the Multicast filter and MC2UC traffic to Central-switching client	To verify the Multicast filter and central-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ172S_QBSSload_15	Verify the Multicast filter and Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode with multicast filter.	Passed	
EWLCJ172S_QBSSload_16	Verify the Multicast filter and MC2UC traffic to Central-switching client after Download/upload the configuration file to controller	To verify the Multicast filter client subscribed to video streaming receives MC2UC traffic after download/upload the configuration file from controller	Passed	

BSSIDCounters

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_BSSID_01	Checking the BSSID Statistics in eWLC	To check whether the BSSID showing proper in ewlc or not	Passed	
EWLCJ172S_BSSID_02	Verifying the BSSID Statistics in catalyst AP's	To verify whether the BSSID showing proper in catalyst AP's or not	Passed	
EWLCJ172S_BSSID_03	Verifying the BSSID record in FMAN/CPP.	To verify whether the BSSID record showing correct in FMAN/CPP or not	Passed	

EWLCJ172S_BSSID _04	Checking the Client object's hierarchy relationship in FMAN	To check whether FMAN showing the client object hierarchy or not	Passed	
EWLCJ172S_BSSID _05	Validating the client record in FMAN/CPP.	To validate the client record in FMAN/CPP	Passed	
EWLCJ172S_BSSID _06	Verifying BSSID with Intra client roaming	To verify whether BSSID with client roaming between AP's or not	Passed	
EWLCJ172S_BSSID _07	Verifying BSSID with inter client roaming	To check whether BSSID is appearing or not ,when clients are roaming between controllers	Passed	
EWLCJ172S_BSSID _08	Monitoring BSSID status in eWLC UI after client association	To check whether BSSID status showing or not in eWLC UI	Passed	
EWLCJ172S_BSSID _09	Monitoring the BSSID through WNCd Validation	To check the BSSID through WNCd Validation	Passed	
EWLCJ172S_BSSID _10	Capturing the BSSID & Windows client connectivity using Wireshark	To check the window client connectivity & BSSID using Wireshark	Failed	CSCvt80745
EWLCJ172S_BSSID _11	Capturing the BSSID & MAC client connectivity using Wireshark	To check the MAC client connectivity & BSSID using Wireshark	Passed	
EWLCJ172S_BSSID _12	Monitoring the BSSID & Android client connectivity using Wireshark	To check the Android client connectivity & BSSID using Wireshark	Passed	
EWLCJ172S_BSSID _13	Capturing the BSSID & iOS client connectivity using Wireshark	To check the iOS client connectivity & BSSID using Wireshark	Passed	

Client_logging

Logical ID	Title	Description	Status	Owners
EWLCJ172S_Client Logging_01	To Verify default Notice level in Always-ON logs for Windows wireless client.	Default Notice level in Always-ON logs for Windows wireless client.	Passed	
EWLCJ172S_Client Logging_02	To Verify default Notice level in Always-ON logs for MAC wireless client.	Default Notice level in Always-ON logs for MAC wireless client.	Passed	
EWLCJ172S_Client Logging_03	To Verify default Notice level in Always-ON logs for Android wireless client.	To Verify default Notice level in Always-ON logs for Android wireless client.	Passed	
EWLCJ172S_Client Logging_04	To Verify default Notice level in Always-ON logs for Apple Mobile wireless client.	To Verify default Notice level in Always-ON logs for Apple Mobile wireless client.	Passed	
EWLCJ172S_Client Logging_05	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when Windows wireless client joined successfully in chamber environment.	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when Windows wireless client joined successfully in chamber environment.	Passed	
EWLCJ172S_Client Logging_06	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when MAC wireless client joined successfully in chamber environment.	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when MAC wireless client joined successfully in chamber environment.	Passed	

EWLCJ172S_Client Logging_07	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when Android wireless client joined successfully in chamber environment.	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when Android wireless client joined successfully in chamber environment.	Passed	
EWLCJ172S_Client Logging_08	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when Apple Mobile wireless client joined successfully in chamber environment.	To Verify there should not be any error or other level logs except default notice level in Always-on logs, when Apple Mobile wireless client joined successfully in chamber environment.	Passed	
EWLCJ172S_Client Logging_09	To Verify Notice logs should print basic necessary information about a Windows client.	To Verify Notice logs should print basic necessary information about a Windows client.	Passed	
EWLCJ172S_Client Logging_10	To Verify Notice logs should print basic necessary information about a MAC client.	To Verify Notice logs should print basic necessary information about a MAC client.	Passed	
EWLCJ172S_Client Logging_11	To Verify Notice logs should print basic necessary information about a Android client.	To Verify Notice logs should print basic necessary information about a Android client.	Passed	
EWLCJ172S_Client Logging_12	To Verify Notice logs should print basic necessary information about a Apple Mobile client.	To Verify Notice logs should print basic necessary information about a Apple Mobile client.	Passed	

EWLCJ172S_Client Logging_13	To Verify number of Always-ON log lines respect to security are as as 17 for Open with Windows wireless client.	To Verify number of Always-ON log lines respect to security are as as 17 for Open with Windows wireless client.	Passed	
EWLCJ172S_Client Logging_14	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x with	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x with	Passed	
EWLCJ172S_Client Logging_15	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK .	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK .	Passed	
EWLCJ172S_Client Logging_16	To Verify number of Always-ON log lines respect to security are as 17 for Open with MAC wireless client.	To Verify number of Always-ON log lines respect to security are as 17 for Open with MAC wireless client.	Passed	
EWLCJ172S_Client Logging_17	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x .	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x .	Passed	
EWLCJ172S_Client Logging_18	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK .	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK .	Passed	
EWLCJ172S_Client Logging_19	To Verify number of Always-ON log lines respect to security are as 17 for Open with Android wireless client.	To Verify number of Always-ON log lines respect to security are as 17 for Open with Android wireless client.	Passed	

EWLCJ172S_Client Logging_20	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x .	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x .	Passed	
EWLCJ172S_Client Logging_21	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK.	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK.	Passed	
EWLCJ172S_Client Logging_22	To Verify number of Always-ON log lines respect to security are as 17 for Open with Apple Mobile wireless client.	To Verify number of Always-ON log lines respect to security are as 17 for Open with Apple Mobile wireless client.	Passed	
EWLCJ172S_Client Logging_23	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x .	To Verify number of Always-ON log lines respect to security are as 19 for WPA1/WPA2 PSK and WPA1/WPA2 dot1x .	Passed	
EWLCJ172S_Client Logging_24	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK.	To Verify number of Always-ON log lines respect to security are as 22 for MAB with PSK.	Passed	

Multi LAG and Load Balancing based on VLAN and SSO

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_Multi LAG_01	To Verify the Multi LAG and Load balancing on 9800-40 Controller.	To Verify the Multi LAG and Load balancing on 9800-40 Controller.	Passed	
EWLCJ172S_Multi LAG_02	To Verify the Multi LAG and Load balancing on 9800-80 Controller.	To Verify the Multi LAG and Load balancing on 9800-80 Controller.	Passed	

EWLCJ172S_Multi LAG_03	To Verify the Multi LAG and Load balancing on 9800-L Controller.	To Verify the Multi LAG and Load balancing on 9800-L Controller.	Passed	
EWLCJ172S_Multi LAG_04	To Verify the Multi LAG and Load balancing on 9800-40 Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-40 Controller after Switch failure	Passed	
EWLCJ172S_Multi LAG_05	To Verify the Multi LAG and Load balancing on 9800-80 Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-80 Controller after Switch failure	Passed	
EWLCJ172S_Multi LAG_06	To Verify the Multi LAG and Load balancing on 9800-L Controller after Switch failure	To Verify the Multi LAG and Load balancing on 9800-L Controller after Switch failure	Passed	

WGB client support on ME

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_WGB_1	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWCJ172S_WGB_2	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWCJ172S_WGB_3	Configuring WGB in eWC	To verify WGB configuration is successful or not in eWC	Passed	
EWCJ172S_WGB_4	Associating the WGB on open authentication with 9115 AP	To associate the WGB on open authentication and check if the WGB associates with the open WLAN or not.	Passed	

EWCJ172S_WGB_5	Associating the WGB on open authentication with flex+bridge	To associate the WGB on open authentication with 9115 AP flex+bridge AP and check if the WGB associates with the open WLAN or not.	Passed	
EWCJ172S_WGB_6	Associating the WGB on WPA 2 with PSK with flex+bridge AP	To associate the WGB on WPA 2 PSK security with 9115 AP flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWCJ172S_WGB_7	Associating the WGB on WPA 2 with 802.1x with flex+bridge AP	To associate the WGB on WPA 2 802.1x security with 9115 flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWCJ172S_WGB_8	Checking of WGB roaming from one AP to another AP in flex+bridge mode	To check the roaming of WGB from one AP to another AP when Aps are in flex+bridge mode	Passed	
EWCJ172S_WGB_9	Performing Inter controller roaming for WGB clients with OPEN security in AP flex+bridge mode	To check inter controller roaming for WGB clients with OPEN security in AP flex+bridge mode	Passed	
EWCJ172S_WGB_10	Performing Inter controller roaming for WGB clients with WPA2 PSK security in AP flex+bridge mode	To check inter controller roaming for WGB clients with WPA2 PSK security in AP flex+bridge mode	Passed	
EWCJ172S_WGB_11	Performing Inter controller roaming for WGB clients with WPA2 Dot1x security in AP flex+bridge mode	To check inter controller roaming for WGB clients with WPA2 Dot1x security in AP flex+bridge mode	Passed	

EWCJ172S_WGB_12	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWCJ172S_WGB_13	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients after session timeout	Passed	
EWCJ172S_WGB_14	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

ME WLAN Simplication

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_ME WLAN Simplication_1	Adding/editing the location in Japanese UI	To verify that location added and location name , description , Client density , native vlan edited succefully	Passed	
EWCJ172S_ME WLAN Simplication_2	Adding/editing the AAA server in Japanese UI	To verify that AAA server added and deleted succefully	Passed	
EWCJ172S_ME WLAN Simplication_3	Creating new WLAN with WPA2 Enterprise	To verify that WLAN created with WPA2 Enterprise	Passed	
EWCJ172S_ME WLAN Simplication_4	Creating new WLAN with WPA2 Personal	To verify that WLAN created with WPA2 Personal	Passed	
EWCJ172S_ME WLAN Simplication_5	Creating the Employee Network with use of Existing network	To verify that new network created with the use of existing network	Passed	
EWCJ172S_ME WLAN Simplication_6	Creating WLAN with Network type as guest	To verify that guest network created successfully	Passed	
EWCJ172S_ME WLAN Simplication_7	Deleting the network from location in Japanese UI	To verify that network deleted from location	Passed	

EWCJ172S_ME WLAN Simplication_8	Importing AP MAC address using CSV file and moved in the location	To verify that AP moved to location using CSV file	Passed	
EWCJ172S_ME WLAN Simplication_9	Moving AP in the location by providing mac address	To verify that AP moved by mac address	Passed	
EWCJ172S_ME WLAN Simplication_10	Moving AP in the location from Available AP list	To verify that AP moved from Available AP list	Passed	

OpenRoaming/HS2.0

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_Open Roaming_01	Setup DNA Spaces connector & import connector in DNA Spaces portal.	To Setup DNA Spaces connector from an ova file and import connector into DNA Spaces.	Passed	
EWLCJ172S_Open Roaming_02	Configure DNA Spaces connector as AAA.	To configure DNA Spaces connector as AAA.	Passed	
EWLCJ172S_Open Roaming_03	Set up a PassPoint based SSID	To create a WLAN with related config to Open roaming feature.	Passed	
EWLCJ172S_Open Roaming_04	Configuration related to Open roaming HS 2.0 feature	To do all the required config related to Open roaming HS 2.0	Passed	
EWLCJ172S_Open Roaming_05	Connect a client to Open roaming hotspot	To check if the client connects to the open roaming hotspot SSID	Passed	

Fabric In A Box (webUI for Embedded Wireless on 9k Switches)

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Fabric_UI_1	To Deploy Fabric configuration from webUI on 9300	To Verify Fabric UI on 9300	Passed	

EWCJ172S_Fabric_UI_2	To Deploy Fabric configuration from webUI on 9300 and Windows Client	To Verify Fabric UI on 9300 with Window Client	Passed	
EWCJ172S_Fabric_UI_3	To Deploy Fabric configuration from webUI on 9300 and Android Client	To Verify Fabric UI on 9300 with Android Client	Passed	
EWCJ172S_Fabric_UI_4	To Deploy Fabric configuration from webUI on 9300 and MAC Client	To Verify Fabric UI on 9300 with MAC Client	Passed	
EWCJ172S_Fabric_UI_5	To Deploy Fabric configuration from webUI on 9300 and Apple Mobile Client	To Verify Fabric UI on 9300 with Apple Mobile Client	Passed	
EWCJ172S_Fabric_UI_6	To Deploy Fabric configuration from webUI on 9400	To Verify Fabric UI on 9400	Passed	
EWCJ172S_Fabric_UI_7	To Deploy Fabric configuration from webUI on 9400 and Windows Client	To Verify Fabric UI on 9400 with Window Client	Passed	
EWCJ172S_Fabric_UI_8	To Deploy Fabric configuration from webUI on 9400 and Android Client	To Verify Fabric UI on 9400 with Android Client	Passed	
EWCJ172S_Fabric_UI_9	To Deploy Fabric configuration from webUI on 9400 and MAC Client	To Verify Fabric UI on 9400 with MAC Client	Passed	
EWCJ172S_Fabric_UI_10	To Deploy Fabric configuration from webUI on 9400 and Apple Mobile Client	To Verify Fabric UI on 9400 with Apple Mobile Client	Passed	
EWCJ172S_Fabric_UI_11	To Deploy Fabric configuration from webUI on 9500	To Verify Fabric UI on 9500	Passed	
EWCJ172S_Fabric_UI_12	To Deploy Fabric configuration from webUI on 9500 and Windows Client	To Verify Fabric UI on 9500 with Window Client	Passed	

EWCJ172S_Fabric_UI_13	To Deploy Fabric configuration from webUI on 9500 and Android Client	To Verify Fabric UI on 9500 with Android Client	Passed	
EWCJ172S_Fabric_UI_14	To Deploy Fabric configuration from webUI on 9500 and MAC Client	To Verify Fabric UI on 9500 with MAC Client	Passed	
EWCJ172S_Fabric_UI_15	To Deploy Fabric configuration from webUI on 9500 and Apple Mobile Client	To Verify Fabric UI on 9500 with Apple Mobile Client	Passed	

APSP/APDP support in WebUI for EWLC-ME

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_APDP WebUI support_1	Adding the APSP configuration in EWC for AP image upgrade.	To check whether the APSP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ172S_APDP WebUI support_2	Adding the APDP configuration in EWC for AP image upgrade.	To check whether the APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ172S_APDP WebUI support_3	Adding the APSP/APDP configuration in EWC for AP image upgrade using SFTP type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ172S_APDP WebUI support_4	Adding the APSP/APDP configuration in EWC for AP image upgrade using FTP type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	

EWCJ172S_APDP WebUI support_5	Adding the APSP/APDP configuration in EWC for AP image upgrade using Device type.	To check whether the APSP/APDP configuration is added successfully and AP is upgraded or not.	Passed	
EWCJ172S_APDP WebUI support_6	Verifying whether APSP/APDP is accepting a invalid file path.	To check whether APSP/APDP is accepting invalid file path or not	Passed	
EWCJ172S_APDP WebUI support_7	Verifying whether APSP/APDP is accepting a invalid ip address.	To check whether APSP/APDP is accepting invalid Ip address or not	Passed	
EWCJ172S_APDP WebUI support_8	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ172S_APDP WebUI support_9	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ172S_APDP WebUI support_10	Connecting client after upgrading AP image using APSP/APDP.	To check whether connecting clients after the ap image upgradation using APSP/APDP	Passed	

CHAPTER 4

Regression Features - Test Summary

Intelligent Capture

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_180	Packet capture for Android client using Intelligent Capture option in APgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWCJ172S_Reg_181	Packet capture for Windows JOS client using Intelligent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWCJ172S_Reg_182	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
EWCJ172S_Reg_183	Packet capture for Mac OS client using Intelligent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	
EWCJ172S_Reg_184	Packet capture of client when the client is connected to AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4 GHz in eWLC ME	Passed	

EWCJ172S_Reg_185	Packet capture of client when the client is connected to AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz in eWLC ME	Passed	
EWCJ172S_Reg_186	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in eWLC ME	Passed	
EWCJ172S_Reg_187	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in eWLC ME	Passed	
EWCJ172S_Reg_188	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in eWLC ME	Passed	
EWCJ172S_Reg_189	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-web consent	Passed	
EWCJ172S_Reg_190	Packet capture for AnyConnect client using Intelligent Capture option in APgroup page	To verify the packet capture for AnyConnect client using Intelligent capture in APgroup page	Passed	
EWCJ172S_Reg_191	Packet capture for Windows JOS client using Intelligent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWCJ172S_Reg_192	Packet capture for Android client using Intelligent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	

EWCJ172S_Reg_193	Packet capture for iOS client using Intelligent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWCJ172S_Reg_194	Packet capture for MacOS client using Intelligent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	
EWCJ172S_Reg_195	Packet capture for AnyConnect client using Intelligent Capture option in AP page	To verify the packet capture for AnyConnect client using Intelligent capture in AP page	Passed	

ME AP convert to CAPWAP via DHCP Option

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_301	Change the 1852 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ172S_Reg_302	Change the 2800 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ172S_Reg_303	Change the 1542 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ172S_Reg_304	Change the 1815i ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ172S_Reg_305	Change the AP mode after converting in to capwap	To change the AP mode after converting in to CAPWAP	Passed	
EWCJ172S_Reg_306	Connect iOS client to Capwap converted AP from ME with WPA2-PSK security	To connect the iOS client to capwap converted AP from ME with WPA2-PSK security	Passed	

EWCJ172S_Reg_307	Connect Android client to Capwap converted AP from ME with WPA2-PSK security	To connect the Android client to capwap converted AP from ME with WPA2-PSK security	Passed	
EWCJ172S_Reg_308	Config primary, secondary controller in AP and reload ME controller	To verify that ME changed to capwap and send join request to controller that configured using DHCP option 43	Passed	
EWCJ172S_Reg_309	Config two controller ip in dhcp option 43 and first should be wrong ip	To verify that AP joined to second controller if first ip is wrong in dhcp	Passed	
EWCJ172S_Reg_310	Change the 1815i ME AP type to capwap using DHCP 43 and join in to vWLC	To change the AP type to capwap using DHCP 43and join in to vWLC	Passed	
EWCJ172S_Reg_311	Make the Preferred Master one ME capable AP and reload ME Controller	To verify that ME Controller changed to capwap after make Preferred master as another another ME capable AP	Passed	

Capwap Image Conversion

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_258	Joining the AP image with less than other than eWC and checking the details	To verify whether AP join to the eWLC eWC and downloading the image or not	Passed	
EWCJ172S_Reg_259	Joining the AP after Efficient join enable/Disable state	To verify whether AP is joining & downloading image from eWC or not after efficient join enable state	Passed	

EWCJ172S_Reg_260	CAPWAP image joins to eWC	To verify whether COS AP is joining to the eWC with eWC capable or not	Passed	
EWCJ172S_Reg_261	CAPWAP image joins to eWC	To verify whether IOS AP is joining to the eWC with AP & eWC different version and not downloading the image	Passed	
EWCJ172S_Reg_262	Upgrading the eWC image and making the capwap Aps to eWC capable	To verify whether Aps converting the eWC capable or not after upgrade the eWC image	Passed	
EWCJ172S_Reg_263	Downgrading the eWC image and making the capwap Aps to eWC capable	To verify whether Aps converting the eWC capable or not after downgrade the eWC image	Passed	
EWCJ172S_Reg_264	Removing the Master AP at the time of AP downloading the image	To verify whether it is possible to remove the Master AP at the time of AP downloading the image	Passed	
EWCJ172S_Reg_265	Changing the eWC time and trying to join the AP	To verify whether AP joining to the eWC or not with AP and eWC times are different	Passed	
EWCJ172S_Reg_266	Performing the Master AP failover	To verify whether after Master Ap failover, ap is again downloading the images or not	Passed	
EWCJ172S_Reg_267	Interchanging the eWC image	To verify whether after image interchange eWC coming as changed version or not	Passed	

EWCJ172S_Reg_268	Interchanging the AP image and making as eWC Controller	To verify whether after AP interchange, AP is coming as changed image with eWC capable controller or not	Passed	

Hotspot 2.0

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_48	Configure Mesh setup and the Network type from one to another	To verify that Mesh setup configured and client connecting or not with network type changes from one to other	Passed	
EWLCJ172S_Reg_49	Enabling the Internet Access WLAN and connecting client	To verify whether Internet Access mode is enabled or not	Passed	
EWLCJ172S_Reg_50	Configuring the Network type from one to another	To verify whether client connecting or not with network type changes from one to other	Passed	
EWLCJ172S_Reg_51	Configuring the Network Authentication	To verify whether Client is connecting after Network Authentication or not	Passed	
EWLCJ172S_Reg_52	Checking with IPv4 type details	To verify whether Client connecting or not after IPv4 type changes from one to another	Passed	
EWLCJ172S_Reg_53	Creating OUI with Duplicate name	To verify whether OUI is creating with duplicate name or not	Passed	
EWLCJ172S_Reg_54	Configuring the NAI-relam and Eap-methods.	To verify whether client will connect with NAI-relam credentials or not	Passed	

EWLCJ172S_Reg_55	Adding cellular network information with duplicate name	To verify whether Cellular network information added successfully	Passed	
EWLCJ172S_Reg_56	Configuring the OSU SSID	To verify whether OSU SSID applying or not	Passed	
EWLCJ172S_Reg_57	Configuring the OSU Provider information	To verify whether OSU Provider information applying or not	Passed	
EWLCJ172S_Reg_58	Configure the WAN metrics.	To verify whether WAN status is varying or not	Passed	
EWLCJ172S_Reg_59	Varying Port configurations	To verify whether Port configurations can vary after client connect	Passed	
EWLCJ172S_Reg_60	Downgrading the AP after Hotspot configurations	To verify whether Client connected or not after downgrade with Hotspot	Passed	
EWLCJ172S_Reg_61	Upgrading the AP after Hotspot configurations	To verify whether all hotspot details are showing properly or not	Passed	
EWLCJ172S_Reg_62	Changing the AP modes after Client connect to Hotspot	To verify whether client will connect or not after modes changes in AP	Passed	
EWLCJ172S_Reg_63	Configure the Venue name and URL.	To verify whether venue name or URL applying or not.	Passed	
EWLCJ172S_Reg_64	Configure the Domain name.	To verify whether Domain name applying or not.	Passed	
EWLCJ172S_Reg_65	Checking the Roaming after roaming-oi configurations	To verify whether client will roam between hotspots or not	Passed	
EWLCJ172S_Reg_66	Configure the Operating class	To verify whether operating class configured or not.	Passed	

802.1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_345	Enabling dot1x auth for AP and ioining AP to WLC	To check whether AP joins WLC or not after dot1x authentication from Switch/ISE	Passed	
EWCJ172S_Reg_346	Associating Windows clients to AP joined via Dot1x authentication	To check whether Windows clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ172S_Reg_347	Joining COS AP to WLC through Dot1x+PEAP authentication	To check whether COS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method PEAP	Passed	
EWCJ172S_Reg_348	Joining iOS AP to WLC through Dot1x+EAP TLS authentication	To check whether iOS AP joins WLC or not after dot1x authentication from Switch/ISE via EAP method TLS	Passed	
EWCJ172S_Reg_349	Trying to join AP's through Dot1x authentication with LSC provisioning	To check whether AP's joins WLC or not through LSC provisioning & dot1x authentication	Passed	
EWCJ172S_Reg_350	Providing invalid credentials for AP authentication and checking the status of AP in console	To check whether AP throws error message or not when invalid credentials provided during dot1x authentication	Passed	
EWCJ172S_Reg_351	Disabling dot1x support in Switch and trying to associate AP via Dot1x authentication to WLC	To check whether AP joins WLC or not even dot1x is disabled in switch	Passed	

EWCJ172S_Reg_352	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
EWCJ172S_Reg_353	Checking the configuration of 802.1x authentication parameters after export/import the config file	To check whether 802.1x auth parameters restores or not after export/import the config file in WLC UI via TFTP	Passed	
EWCJ172S_Reg_354	Associating Mac OS clients to AP joined via Dot1x authentication	To check whether Mac OS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ172S_Reg_355	Associating Android clients to AP joined via Dot1x authentication	To check whether Android clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ172S_Reg_356	Associating iOS clients to AP joined via Dot1x authentication	To check whether iOS clients associated successfully or not once AP joined via dot1x authentication from Switch/ISE	Passed	
EWCJ172S_Reg_357	Trying to configure of 802.1x authentication parameters via Read-only User	To check whether Read only user can be able to configure or not the 802.1x auth parameters in WLC UI	Passed	

Master AP Failover Issues

Logical ID	Title	Description	Status	Defect ID

EWCJ172S_Reg_312	Changing the next preferred eWLC ME capable AP to Controller from UI	To verify whether Next preferred Master AP can changing the eWLC ME or not by using the UI	Passed	
EWCJ172S_Reg_313	Changing the next preferred eWLC ME capable AP to Controller from CLI	To verify whether Next preferred Master AP can changing the eWLC ME or not by using the CLI	Passed	
EWCJ172S_Reg_314	Making the More than 5 Aps to eWLC ME capable	To verify whether more than 5 Aps are changing the state to eWLC ME capable or not	Passed	
EWCJ172S_Reg_315	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
EWCJ172S_Reg_316	Configuring the Controller IP address with DHCP server	To verify whether DHCP server IP address is assign to the Controller and come up with same IP address or not	Passed	
EWCJ172S_Reg_317	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	

CMX Parity for Cisco Catalyst 9800 Series Wireless Controller ME

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_107	Adding eWC-ME to CMX & CMX to DNAC	To Check Whether the eWLC-ME gets added to CMX & CMX added to DNAC successfully or not	Passed	

EWCJ172S_Reg_108	Connecting the IOS Client to the access point on the floor and check the details of the Client.	To connect a IOS Client to the access point on the floor and check if the details of the IOS Clients are shown correctly or not.	Passed	
EWCJ172S_Reg_109	Connecting the MacOS Client to the access point on the floor and check the details of the Client.	To connect a MacOS Client to the access point on the floor and check if the details of the MacOS Clients are shown correctly or not.	Passed	
EWCJ172S_Reg_110	Connecting the Android Client to the access point on the floor and check the details of the Client.	To connect a Android Client to the access point on the floor and check if the details of the IOS Clients are shown correctly or not.	Passed	
EWCJ172S_Reg_111	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWCJ172S_Reg_112	Connecting a 2.4 ghz Client to the access point which is placed in floor and checking the client details	To connect a 2.4 ghz Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ172S_Reg_113	Connecting a 5 ghz Client to the access point which is placed in floor and checking the client details	To connect a 5 ghz Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	

EWCJ172S_Reg_114	Connecting a Dual band Client to the access point which is placed in floor and checking the client details	To connect a Dual band Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWCJ172S_Reg_115	Verify the Disconnected client details in CMX	To check whether the client is disconnected or not in CMX	Passed	
EWCJ172S_Reg_116	Verifying the Intra client roaming in CMX	To verify whether the client is roaming between AP's or not	Passed	
EWCJ172S_Reg_117	Verifying the Inter client roaming in CMX	To verify whether the clients are roaming between controllers	Passed	
EWCJ172S_Reg_118	Verifying the Wired client details in CMX	To Check whether the Wired client details are showing or not in CMX	Passed	
EWCJ172S_Reg_119	Verifying the guest LAN client details in CMX	To Check whether the Guest LAN client details are showing or not in CMX	Passed	
EWCJ172S_Reg_120	Verifying MIMO client details using Wireshark	To check Whether all the clients getting same BW & data rate or not	Passed	

Scheduled Config Download

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_90	New Config should be applied when changes in old config through schedule download configuration using FTP server	To verify New Config should be applied when changes in old config through schedule download configuration using FTP server	Passed	

EWCJ172S_Reg_91	New Config should be applied when changes in old config through schedule download configuration using SFTP server	To verify New Config should be applied when changes in old config through schedule download configuration using SFTP server	Passed	
EWCJ172S_Reg_92	New Config should not applied when old config having no changes through schedule download configuration using FTP server	To verify New Config should not applied when old config having no changes through schedule download configuration using FTP server	Passed	
EWCJ172S_Reg_93	New Config should not applied when old config having no changes through schedule download configuration using SFTP server	To verify New Config should not applied when old config having no changes through schedule download configuration using SFTP server	Passed	
EWCJ172S_Reg_94	New config should not apply to the Device using FTP transfer mode when having bad config in server	To verify the new config should not apply to the Device using FTP transfer mode when having bad config in server	Passed	
EWCJ172S_Reg_95	New config should not apply to the Device using SFTP transfer mode when having bad config in server	To verify the new config should not apply to the Device using SFTP transfer mode when having bad config in server	Passed	
EWCJ172S_Reg_96	Getting error message when passing wrong CLI commands (Wrong format of server IP address) in schedule download configuration using FTP/SFTP server	To verify Getting error message when passing wrong CLI commands (Wrong format of server IP address) in schedule download configuration using FTP/SFTP server	Passed	

EWCJ172S_Reg_97	Getting error message when passing wrong CLI commands (Wrong file path/ file name) in schedule download configuration using FTP/SFTP server	To verify Getting error message when passing wrong CLI commands (Wrong file path/file name) in schedule download configuration using FTP/SFTP server	Passed	
EWCJ172S_Reg_98	New Config should be applied when changes in old config through schedule download configuration using FTP/SFTP server when passing domain name instead of server address in CLI command	To verify New Config should be applied when changes in old config through schedule download configuration using FTP/SFTP server when passing domain name instead of server address in CLI command	Passed	
EWCJ172S_Reg_99	New Config should not apply when preferred Master AP is up after downloading config	To verify New Config should not apply when preferred Master AP is up after downloading config	Passed	
EWCJ172S_Reg_100	New config should not apply when passing file name which is not available in the server	To verify New config should not apply when passing file name which is not available in the server	Passed	
EWCJ172S_Reg_101	verify server reachable error message when FTP/SFTP sever is down	To verify server reachable error message when FTP/SFTP sever is down	Passed	
EWCJ172S_Reg_102	Verify the behaviour of schedule config download when system time is changed after setting hourly schedule download	To Verify the behaviour of schedule config download when system time is changed after setting hourly schedule download	Passed	

EWCJ172S_Reg_103	Verify EWC should be come up (after reset) after downloading new config	To Verify EWC should be come up (after reset) after downloading new config	Passed	
EWCJ172S_Reg_104	Verify Ap join and client connectivity after new config downloaded	To verify Ap join and client connectivity after new config downloaded	Passed	
EWCJ172S_Reg_105	Verify apply new config when Primary controller goes down and secondary controller is active (when both EWC on same model) after downloading config	To verify apply new config when Primary controller goes down and secondary controller is active (when both EWC on same model) after downloading config	Passed	
EWCJ172S_Reg_106	Verify not apply new config when Primary controller goes down and secondary controller is active (when both EWC on different model) after downloading config	To verify not apply new config when Primary controller goes down and secondary controller is active (when both EWC on different model) after downloading config	Passed	

BSS Coloring on AX APs

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_75	Configuring Automatic BSS colouring for 2.4 ghz AP radios	To Check whether automatic BSS colouring is applied or not in 2.4 ghz ap radio	Passed	
EWCJ172S_Reg_76	Configuring automatic BSS colour for 5ghz radio	To Check whether automatic BSS colouring is applied or not in 5 ghz ap radio	Passed	

EWCJ172S_Reg_77	Configuring auto BSS colour appearing 2.4 to 5 Ghz radio or vice versa	To verify whether different BSS colouring is occur while Changing the AP radios 2.4 to 5 viseversa	Passed	
EWCJ172S_Reg_78	Configuring Manual BSS colour configuration for 2.4/5 ghz radio	To Check whether Manual BSS colouring is applied or not in 2.4 ghz ap radio	Passed	
EWCJ172S_Reg_79	Verifying the static BSS colour assignment for the 5 ghz radio in Flex-connect mode	To Check whether Static BSS colouring is applied or not in 5 ghz ap radio	Passed	
EWCJ172S_Reg_80	Checking the manual BSS colouring while changing the AP radio from 2.4 ghz to 5 ghz	To verify whether different BSS colouring is occur while Changing the AP radios	Passed	
EWCJ172S_Reg_81	Checking the BSS colour details are retained after AP and Controller reload	To Check whether the BSS colour retained after AP & Controller reload	Passed	
EWCJ172S_Reg_82	Verifying BSS colouring with Intra client roaming by using 9115AP	To verify whether BSS colouring with client roaming between AP's or not	Passed	
EWCJ172S_Reg_83	Verifying BSS colouring with inter roaming client using different radio	To check whether BSS colouring is appearing or not , when different radio clients are roaming between controllers	Passed	
EWCJ172S_Reg_84	Verifying BSS colouring with inter roaming client using same radio	To check whether BSS colouring is appearing or not , when same radio clients are roaming between controllers	Passed	

EWCJ172S_Reg_85	Capturing the Windows client connectivity & BSS colouring using Wireshark	To check the window client connectivity & BSS colouring using Wireshark	Passed	
EWCJ172S_Reg_86	Capturing the Android client connectivity & BSS colouring using Wireshark	To check the Android client connectivity & BSS colouring using Wireshark	Passed	
EWCJ172S_Reg_87	Capturing the Mac OS client connectivity & BSS colouring using Wireshark	To check the Mac OS client connectivity & BSS colouring using Wireshark	Passed	
EWCJ172S_Reg_88	Changing 9115 AP mode from local to Flex connect & check the BSS colouring Configuration	To change the mode of AP from local mode to Flexconnect mode and check the BSS colouring configuration in 9115 Ap	Passed	
EWCJ172S_Reg_89	Changing 9115 AP mode from flex to local & check the BSS colouring Configuration	To change the mode of AP from flex mode to local mode and check the BSS colouring configuration in 9115 Ap	Passed	

EoGRE Support for ME

Logical ID	Title	Description	Status	Defect ID
EWCJ172S_Reg_17	Creating EoGRE Tunnel Gateway.	To check whether the tunnel gateway is created or not.	Passed	
EWCJ172S_Reg_18	Creating EoGRE Tunnel Domain	To check whether the tunnel Domain is created or not.	Passed	
EWCJ172S_Reg_19	Configuring the Global Parameter for the EoGRE.	To check whether the global parameters are configured or not.	Passed	

EWCJ172S_Reg_20	Configuring the tunnel Profile.	To check whether the tunnel profile is created or not.	Passed	
EWCJ172S_Reg_21	Associate the WLAN to the Wireless policy profile.	To check whether the wlan is associated with the policy profile.	Passed	
EWCJ172S_Reg_22	Adding a policy tag and site tag to AP	To check whether the policy and site tag is added to an AP.	Failed	CSCvt61099
EWCJ172S_Reg_23	Checking the client connectivity.	To check whether the client is connected or not	Passed	
EWCJ172S_Reg_24	Getting the EoGRE tunnel from PI	To check whether the tunnel is exported from PI or not	Passed	
EWCJ172S_Reg_25	Connect the ios clients and check the connectivity.	To check whether the ios clients get connected successfully.	Passed	
EWCJ172S_Reg_26	Connect the mac os clients and check the connectivity.	To check whether the mac os clients get connected successfully.	Passed	
EWCJ172S_Reg_27	Checking the traffic in the tunnel.	To check whether the traffic in the tunnel is managed or not.	Passed	

Image Predownload

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_213	eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ172S_Reg_214	Invalid eWLC Software updating via SFTP server.	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ172S_Reg_215	Software updating via tftp server	Checking the eWLC software updating or not via tftp server	Failed	CSCvt93222

EWLCJ172S_Reg_216	Invalid eWLC Software updating via tftp server	To check whether eWLC software upgrading or not via tftp server	Passed	
EWLCJ172S_Reg_217	eWLC Software upgrading through Invalid SFTP user name/password	Verifying eWLC software is upgrading or not through Invalid SFTP user name/password	Passed	
EWLCJ172S_Reg_218	eWLC software upgrading through invalid tftp file path	Checking eWLC software upgrading or not through invalid tftp file path	Passed	
EWLCJ172S_Reg_219	eWLC Software upgrading via Desktop(HTTP)	Verifying eWLC software upgrading or not via Desktop(HTTP) server	Passed	
EWLCJ172S_Reg_220	Invalid eWLC Software updating via Desktop(HTTP) mode	Verifying eWLC software upgrading or not via Desktop(HTTP) mode	Passed	
EWLCJ172S_Reg_221	ME Software upgrading via webserver	Verifying eWLC software upgrading or not via webserver	Passed	
EWLCJ172S_Reg_222	Invalid eWLC Software updating via webserver	To check whether Invalid eWLC software upgrading or not via webserver	Passed	

Best Practices WebUI

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_116	Enable/Disable the http/https for management	Verify the web UI is able to open or not through http/https after modification	Passed	
EWLCJ172S_Reg_117	Configure the NTP server	To check whether NTP server is able to configure or not for WEB UI	Passed	

EWLCJ172S_Reg_118	Configure the Client Exclusion policies[fix button is not available need to check in latest build]	To check whether Client Exclusion Policies is enabled or not	Passed	
EWLCJ172S_Reg_119	Create the WLAN with WPA2	Verify the WLAN with WPA2 after configuring via best practice	Passed	
EWLCJ172S_Reg_120	Enable the User Login Policies	Checking the User Login Policies is enabled or not	Passed	
EWLCJ172S_Reg_121	Enable the Local Profiling on one or more active WLANs	Verify the enabled Local Profile on Active WLAN	Passed	
EWLCJ172S_Reg_122	Configure the client band for all Active WLANs	To check whether client Band is applied or not for Active WLANs	Passed	
EWLCJ172S_Reg_123	Enable the 5ghz band for Active WLAN	Verify the 5ghz client band on active WLANs	Failed	CSCvt05220
EWLCJ172S_Reg_124	Enable the 2.4ghz band for Active WLAN	Checking the 2.4ghz client band on active WLANs	Passed	
EWLCJ172S_Reg_125	Configure the Best channel width	To check whether Best channel width is configured or not on both radios	Passed	
EWLCJ172S_Reg_126	Enable the Flexible Radio Assignment	To check whether Flexible Radio Assignment is enabled or not	Passed	
EWLCJ172S_Reg_127	Configure the Load balance for one or more active WLAN	Verify the Load balance enabled or not on Active WLAN	Passed	
EWLCJ172S_Reg_128	Enable the Auto Dynamic Channel Assignment	To check whether global channel is enabled or not	Passed	

Opportunistic Wireless Encryption Support

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_103	Verifying WPA3 and OWE support for the Windows client	To verify the OWE Auth key support to the WPA3 security for the Windows client.	Passed	
EWLCJ172S_Reg_104	Verifying WPA3 and OWE support for the Android client	To verify the OWE Auth key support to the WPA3 security for the Android client.	Passed	
EWLCJ172S_Reg_105	Verifying WPA3 and OWE support for the Mac os client	To verify the OWE Auth key support to the WPA3 security for the Mac os client.	Passed	
EWLCJ172S_Reg_106	Verifying WPA3 and OWE-Transition mode support for the Windows client	To verify the OWE-Transition mode support to the WPA3 security for the Windows client.	Passed	
EWLCJ172S_Reg_107	Verifying WPA3 and OWE-Transition mode support for the Android client	To verify the OWE-Transition mode support to the WPA3 security for the Android client.	Passed	
EWLCJ172S_Reg_108	Verifying WPA3 and OWE-Transition mode support for the Mac os client	To verify the OWE-Transition mode support to the WPA3 security for the Mac os client.	Passed	
EWLCJ172S_Reg_109	Checking the WPA3 and OWE support with Layer3 Splash page web redirect	To check the Client packets by connecting the client to WPA3 and OWE support SSID with Layer3 Splash page Web redirect.	Passed	
EWLCJ172S_Reg_110	Verifying theWPA3 and OWE Support with Layer3 On Mac filter failure.	To verify the WPA3 and OWE Support with OWE transition mode and Layer3On Mac filter failure.	Passed	

EWLCJ172S_Reg_111	Verifying the WPA3 support with OWE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and OWE support	Passed	
EWLCJ172S_Reg_112	Verifying the WPA3 support and OWE with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ172S_Reg_113	Verifying the WPA3 support and OWE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and OWE support	Passed	
EWLCJ172S_Reg_114	Verifying the WPA3 and OWE support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Passed	
EWLCJ172S_Reg_115	Verifying the WPA3 and OWE support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with WPA3 WLAN.	Passed	

WPA3 Support

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_86	Verifying the WPA3 support with SAE security key.	To verify the WPA3 support with SAE security Configuration.	Passed	
EWLCJ172S_Reg_87	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the Client packets by connecting the windows client to WPA3 and SAE supported SSID	Passed	

EWLCJ172S_Reg_88	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the Client packets by connecting the Android client to WPA3 and SAE supported SSID	Passed	
EWLCJ172S_Reg_89	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the Client packets by connecting the Mac os client to WPA3 and SAE supported SSID	Passed	
EWLCJ172S_Reg_90	Verifying the WPA3 support with SAE and PSK security key.	To verify the Client packets by connecting the client to WPA3 and SAE and PSK supported SSID	Passed	
EWLCJ172S_Reg_91	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Passed	
EWLCJ172S_Reg_92	Validating the WPA3 support with SAE and Layer 3 Splash page web redirect	To verify the WPA3 support with SAE and Layer3 Splash page web redirect	Passed	
EWLCJ172S_Reg_93	Validating the WPA3 support with SAE and Layer 3 On Mac filter failure.	To verify the WPA3 support with SAE and Layer3 On Mac filter failure	Passed	
EWLCJ172S_Reg_94	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ172S_Reg_95	verifying the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	To verify the WPA3 support with SAE and PSK Auth key and Layer3 Splash page web redirect.	Passed	
EWLCJ172S_Reg_96	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	

EWLCJ172S_Reg_97	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security for the different clients.	Passed	
EWLCJ172S_Reg_98	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ172S_Reg_99	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ172S_Reg_100	Verifying the WPA3 support and SAE security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with WPA3 support and SAE support	Passed	
EWLCJ172S_Reg_101	Verifying the WPA3 support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Passed	
EWLCJ172S_Reg_102	Verifying the WPA3 support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with WPA3 WLAN.	Passed	

Schedule WLAN

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_432	Configure the Calendar Profile in open security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	

EWLCJ172S_Reg_433	Configure the Calendar Profile in WPA2 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ172S_Reg_434	Configure the Calendar Profile in WPA3 security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ172S_Reg_435	Configure the Calendar Profile in Static WEP security WLAN with Start/End time.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ172S_Reg_436	Configure the Calendar Profile in Static WEP security WLAN with Start/End time with Monthly/Weekly/Daily option.	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ172S_Reg_437	Configure the Calendar Profile in Static WEP security WLAN with L3 Security Filtering and with Start/End time .	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	
EWLCJ172S_Reg_438	Observe the Client Disassociation on Calendar Profile after end time	To check whether client is disassociating after end time.	Passed	

mDNS Support

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_246	Checking mDNS services are applied to MAC OS with wlan open security	Verifying mDNS services are applied to Mac OS with open ssid	Passed	

EWLCJ172S_Reg_247	Checking mDNS services are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	
EWLCJ172S_Reg_248	Checking mDNS services are applied to Apple TV and IOS with wlan WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
EWLCJ172S_Reg_249	Checking mDNS services are applied to MacOS and IOS with wlan WPA3-SAE security	Verifying mDNS services are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWLCJ172S_Reg_250	Checking mDNS services are applied to Apple Devices with Fast transition enabled	Verifying mDNS services are applied to Apple Devices with fast transition enabled	Passed	
EWLCJ172S_Reg_251	Performing client communication between two clients connected two different vlan	Checking client communication between two clients connected to different vlan	Passed	
EWLCJ172S_Reg_252	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	
EWLCJ172S_Reg_253	Exporting config file after upgrading eWLC	Checking mDNS config after exporting config file	Passed	
EWLCJ172S_Reg_254	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	
EWLCJ172S_Reg_255	Checking mDNS services are applied to IOS with wlan Static WEP security	Verifying mDNS services are applied to IOS with Static WEP ssid	Passed	

EWCJ172S_Reg_358	Checking mDNS services are applied to MAC OS with wlan open security	Verifying mDNS services are applied to Mac OS with open ssid	Passed	
EWCJ172S_Reg_359	Checking mDNS services are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS services are applied to MacOS and IOS with WPA2 personal security	Passed	
EWCJ172S_Reg_360	Checking mDNS services are applied to Apple TV and IOS with wlan WPA2 Enterprise security and authentication server as radius	Verifying mDNS services are applied to AppleTV and IOS with WPA2 Enterprise security and radius as authentication server	Passed	
EWCJ172S_Reg_361	Checking mDNS services are applied to MacOS and IOS with wlan WPA3-SAE security	Verifying mDNS services are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWCJ172S_Reg_362	Checking mDNS services are applied to Apple Devices with Fast transition enabled	Verifying mDNS services are applied to Apple Devices with fast transition enabled	Passed	
EWCJ172S_Reg_363	Performing client communication between two clients connected two different vlan	Checking client communication between two clients connected to different vlan	Passed	
EWCJ172S_Reg_364	Performing roaming operation when mDNS is applied	Checking roaming when mDNS is applied	Passed	
EWCJ172S_Reg_365	Exporting config file after upgrading eWC	Checking mDNS config after exporting config file	Passed	
EWCJ172S_Reg_366	Creating mDNS profile by adding required services	Verifying mDNS profile is creating with required services	Passed	

EWCJ172S_Reg_367	Checking mDNS services are applied to IOS with wlan Static WEP security	Verifying mDNS services are applied to IOS with Static WEP ssid	Passed	

MC2UC (Videostreaming)

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_264	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ172S_Reg_265	MC2UC traffic to local-switching client when MC2UC is disabled	To verify the local switching client receiving MC traffic when MC2UC is disabled at the WLAN	Passed	
EWLCJ172S_Reg_266	MC2UC traffic to local-switching client when Media stream is removed at AP	To verify the local switching client receiving MC traffic when Media Stream is disabled at AP	Passed	
EWLCJ172S_Reg_267	Multiple LS clients in same vlan, same wlan, receiving MC2UC traffic	To verify whether the multiple local-switching clients receives MC2UC traffic when subscribed to video stream	Passed	
EWLCJ172S_Reg_268	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWLCJ172S_Reg_269	LS client receiving MC2UC traffic roam between radios at the AP	To verify the local-switching client receiving MC2UC traffic roaming between radios of the AP	Passed	

EWLCJ172S_Reg_270	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with same config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with same config	Passed	
EWLCJ172S_Reg_271	Flex LS client receiving MC2UC traffic when AP move from connected > SA > connected with different config	To verify whether the LS client receives continuous MC2UC traffic when AP moves from connected > SA > connected with different config	Passed	
EWLCJ172S_Reg_272	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
EWLCJ172S_Reg_273	Videstream config sync for LS WLAN in HA setup	To verify whether the video streaming config for LS WLAN has been synced between the Active and Standby in HA setup	Passed	
EWLCJ172S_Reg_274	LS client with MC2UC enabled receiving traffic after switchover in HA pair	To verify whether LS client with MC2UC enabled receives unicast traffic after switchover	Passed	

CMX Support

Logical Id	Title	Description	Status	Defect ID

EWLCJ172S_Reg_148	Adding Cisco eWLCto CMX	To add a Cisco eWLCto CMX and check if the eWLCgets added to the CMX with the eWLCstatus showing	Passed	
EWLCJ172S_Reg_149	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
EWLCJ172S_Reg_150	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including Clients connected .	Passed	
EWLCJ172S_Reg_151	Connecting the Client to the access point on the floor and check if the details of the Client.	To connect a Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	
EWLCJ172S_Reg_152	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWLCJ172S_Reg_153	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
EWLCJ172S_Reg_154	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	

EWLCJ172S_Reg_155	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWLCJ172S_Reg_156	Number of Clients visiting the building and floor in hourly and daily basis	Verifying the number of Clients visiting the building or floor on hourly and daily basis	Passed	
EWLCJ172S_Reg_157	Number of Client visits to the building and the floor	To check the number of new Clients and repeated Clients to the building or floor .	Passed	
EWCJ172S_Reg_269	Adding Cisco eWLC_ME to CMX	To add a Cisco eWLC_ME to CMX and check if the eWLC_ME gets added to the CMX with the eWLC_ME status showing	Passed	
EWCJ172S_Reg_270	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
EWCJ172S_Reg_271	Importing the maps with Access points from PI to CMX	To import the maps from prime infra to CMX with Access points and check if the access point details are shown correctly including Clients connected .	Passed	
EWCJ172S_Reg_272	Connecting the Client to the access point on the floor and check if the details of the Client.	To connect a Client to the access point on the floor and check if the details of the Clients are shown correctly or not.	Passed	

EWCJ172S_Reg_273	Connecting many Clients from different place and check the location of the Clients	To connect many Client from different place to the access points and check if the location of the Client are shown in CMX	Passed	
EWCJ172S_Reg_274	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
EWCJ172S_Reg_275	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	
EWCJ172S_Reg_276	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWCJ172S_Reg_277	Number of Clients visiting the building and floor in hourly and daily basis	Verifying the number of Clients visiting the building or floor on hourly and daily basis	Passed	
EWCJ172S_Reg_278	Number of Client visits to the building and the floor	To check the number of new Clients and repeated Clients to the building or floor .	Passed	

Aging Test Cases

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_158	Connecting a JOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect JOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	

EWLCJ172S_Reg_159	Connecting a Window client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Window client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ172S_Reg_160	Connecting a Android client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Android client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ172S_Reg_161	Connecting a IOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect IOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ172S_Reg_162	Connecting a MAC OS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect MAC OS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWLCJ172S_Reg_163	Checking the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWLCJ172S_Reg_164	Checking the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	

EWLCJ172S_Reg_165	Checking the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWLCJ172S_Reg_166	Checking the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWLCJ172S_Reg_167	Checking the Air Quality data for different AP with JOS client and check the health of the AP in a regular interval.	To check the Air quality data for different AP with JOS client and check the health of the particular AP in a regular interval	Passed	
EWCJ172S_Reg_223	Connecting a JOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect JOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ172S_Reg_224	Connecting a Window client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Window client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ172S_Reg_225	Connecting a Android client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect Android client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	

REVIEW DRAFT - CISCO CONFIDENTIAL

EWCJ172S_Reg_226	Connecting a IOS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect IOS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ172S_Reg_227	Connecting a MAC OS client to a 1815I AP and enable debug log and check RSSI value for the client for 2 to 3 hours.	To connect MAC OS client to 1815I and check the debug log for the client and check the RSSI value for 2 to 3 hours.	Passed	
EWCJ172S_Reg_228	Checking the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the JOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWCJ172S_Reg_229	Checking the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Android Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWCJ172S_Reg_230	Checking the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the Window Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	
EWCJ172S_Reg_231	Checking the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	To check the IOS Client details when the client is connected to 2802/3802 AP and check the Average rate for the client for more than 2 hours	Passed	

EWCJ172S_Reg_232	Checking the Air Quality data for different AP with JOS client and check the health of the AP in a regular interval.	To check the Air quality data for different AP with JOS client and check the health of the particular AP in a regular interval	Passed	

Software update using SFTP

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_205	Enable AAA override and connecting a JOS window 10 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 10 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ172S_Reg_206	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ172S_Reg_207	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

EWLCJ172S_Reg_208	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ172S_Reg_209	Connecting a window 10 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 10 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ172S_Reg_210	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ172S_Reg_211	Connecting a IOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ172S_Reg_212	Connecting a MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	

EWCJ172S_Reg_252	eWC Software updating via SFTP server	Verifying eWC software updating or not via SFTP server	Passed	
EWCJ172S_Reg_253	Invalid eWC Software updating via SFTP server	Verifying eWC software updating or not via SFTP server	Passed	
EWCJ172S_Reg_254	eWC .bin Software updating via SFTP server	Checking the eWC .bin software updating or not via SFTP server	Passed	
EWCJ172S_Reg_255	eWC .SSH Software updating via SFTP server	Checking the eWC .bin software updating or not via SFTP server	Passed	
EWCJ172S_Reg_256	eWC Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
EWCJ172S_Reg_257	eWC Software updating through Invalid SFTP user name/password	Verifying eWC software is upgrading or not through Invalid SFTP user name/password	Passed	

AAA Override of VLAN Name-id template

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_205	Enable AAA override and connecting a JOS window 10 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 10 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

EWLCJ172S_Reg_206	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ172S_Reg_207	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ172S_Reg_208	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWLCJ172S_Reg_209	Connecting a window 10 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 10 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	

EWLCJ172S_Reg_210	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ172S_Reg_211	Connecting a IOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWLCJ172S_Reg_212	Connecting a MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWCJ172S_Reg_215	Enable AAA override and connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a JOS window 7 client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWCJ172S_Reg_216	Enable AAA override and connecting a Android client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Android client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	

EWCJ172S_Reg_217	Enable AAA override and connecting a IOS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a IOS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWCJ172S_Reg_218	Enable AAA override and connecting a Mac OS client to the AAA override enabled WLAN with WPA 2 Personal security .	To enable AAA override and connecting a Mac OS client to the AAA override enabled with WPA 2 Personal security WLAN and check if the VLAN from AAA server is overridden to the client	Passed	
EWCJ172S_Reg_219	Connecting a JOS window 7 client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a JOS Window 7 client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWCJ172S_Reg_220	Connecting a Android client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Android client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	

EWCJ172S_Reg_221	Connecting a IOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a IOS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	
EWCJ172S_Reg_222	Connecting a MacOS client to the AAA override enabled WLAN with WPA 2 Enterprise security enabled with AAA override .	To connect a Mac OS client to AAA override enabled WLAN with WPA 2 Enterprise security and check if the Native VLAN is overridden or not.	Passed	

Bidirectional rate limit per client

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_75	Configuring rate limit for per client for JOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ172S_Reg_76	Configuring rate limit for per client for Android client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Android client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ172S_Reg_77	Configuring rate limit for per client for Mac OS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Mac OS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	

EWLCJ172S_Reg_78	Configuring rate limit for per client for IOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for IOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ172S_Reg_79	Configuring rate limit for per client with QOS as Gold for JOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a JOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWLCJ172S_Reg_80	Configuring rate limit for per client with QOS as Gold for Android client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Android client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWLCJ172S_Reg_81	Configuring rate limit for per client with QOS as Gold for IOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a IOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWLCJ172S_Reg_82	Configuring rate limit for per client with QOS as Gold for Mac OS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Mac OS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	

EWLCJ172S_Reg_83	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behaviour of the client is same or not	Passed	
EWLCJ172S_Reg_84	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Passed	
EWLCJ172S_Reg_85	Creating a AVC rule for the WLAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	
EWCJ172S_Reg_150	Configuring rate limit for per client for JOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for JOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWCJ172S_Reg_151	Configuring rate limit for per client for Android client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Android client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	

EWCJ172S_Reg_152	Configuring rate limit for per client for Mac OS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Mac OS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWCJ172S_Reg_153	Configuring rate limit for per client for IOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for IOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWCJ172S_Reg_154	Configuring rate limit for per client with QOS as Gold for JOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a JOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWCJ172S_Reg_155	Configuring rate limit for per client with QOS as Gold for Android client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Android client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWCJ172S_Reg_156	Configuring rate limit for per client with QOS as Gold for IOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a IOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	

EWCJ172S_Reg_157	Configuring rate limit for per client with QOS as Gold for Mac OS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Mac OS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWCJ172S_Reg_158	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behaviour of the client is same or not	Passed	
EWCJ172S_Reg_159	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Passed	
EWCJ172S_Reg_160	Creating a AVC rule for the WLAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	

CWA (Central Web Authentication)

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_223	Creating a CWA along with ACL Configuration in eWLc UI	To check Whether CWA along with ACL Configuration in eWLC UI created or not	Passed	

EWLCJ172S_Reg_224	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ172S_Reg_225	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ172S_Reg_226	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ172S_Reg_227	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	
EWLCJ172S_Reg_228	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to ssid redirecting to Guest portal page with invalid credentials	Passed	
EWLCJ172S_Reg_229	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	
EWLCJ172S_Reg_230	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	

EWLCJ172S_Reg_231	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
EWLCJ172S_Reg_232	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	
EWLCJ172S_Reg_233	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	
EWLCJ172S_Reg_234	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
EWLCJ172S_Reg_235	Validate whether eWLC is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
EWLCJ172S_Reg_236	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWLCJ172S_Reg_237	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	

EWLCJ172S_Reg_238	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Passed	
EWLCJ172S_Reg_239	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	
EWCJ172S_Reg_318	Creating a CWA along with ACL Configuration in eWC UI	To check Whether CWA along with ACL Configuration in eWC UI created or not	Passed	
EWCJ172S_Reg_319	Associating a Japanese Windows Client to a SSID which is mapped with ISE	To verify whether Japanese Windows Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ172S_Reg_320	Associating a iOS Client to a SSID which is mapped with ISE	To verify whether iOS Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ172S_Reg_321	Associating a Android Client to a SSID which is mapped with ISE	To verify whether Android Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ172S_Reg_322	Associating a MAC OS Client to a SSID which is mapped with ISE	To verify whether MAC Client which is mapped to ISE is redirected successfully or not	Passed	
EWCJ172S_Reg_323	Associating a different Clients to SSID which is mapped with ISE and redirecting to Guest portal page with invalid credentials	To verify whether client connected to ssid redirecting to Guest portal page with invalid credentials	Passed	

EWCJ172S_Reg_324	Associating a different Clients to a SSID which is mapped with ISE by creating AVC profile	To verify whether different Clients is redirected successfully and checking that particular application is dropped or not	Passed	
EWCJ172S_Reg_325	Associating a different Clients to a SSID which is mapped with ISE by denying the action in ACL	To verify whether Clients gets denied when it is connected to SSID which is mapped with ISE	Passed	
EWCJ172S_Reg_326	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using TCP protocol	Passed	
EWCJ172S_Reg_327	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using UDP protocol	Passed	
EWCJ172S_Reg_328	Associating a different Clients to a SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permitting the action in ACL using ICMP protocol	Passed	
EWCJ172S_Reg_329	Checking the expired Radius Guest User for proper error message	To verify whether the expired Guest user gets proper Error messages when he logging in	Passed	
EWCJ172S_Reg_330	Validate whether eWC is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	

EWCJ172S_Reg_331	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWCJ172S_Reg_332	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWCJ172S_Reg_333	Checking the configuration of CWA when the user is in Read-only	To verify whether configuration display error message or not when the user is in Read-only	Passed	
EWCJ172S_Reg_334	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	

Maximum number of clients per WLAN/radio

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_240	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting client with WPA 2 Personal security.	To configure maximum allowed client Per AP radio as 4 and connecting 5 different client with radio policy as ALL and check if the number of client that is configured alone gets connected to the WLAN	Passed	
EWLCJ172S_Reg_241	Configuring maximum Allowed Clients Per AP Radio as 3 and connecting client with WPA 2 Enterprise security .	To configure maximum allowed client Per AP radio as 3 and connecting 4 different client with radio policy as ALL and now after 3 client disconnect one client and check if other client get authenticated to the WLAN	Failed	CSCvt73441

EWLCJ172S_Reg_242	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in WLAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in WLAN and check which of the configured number of clients gets connected .	Passed	
EWLCJ172S_Reg_243	Creating WPA 2 Personal security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Failed	CSCvt62485
EWLCJ172S_Reg_244	Creating WPA 2 Enterprise security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
EWLCJ172S_Reg_245	Creating WPA 2 Personal security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Failed	CSCvt34942

EWCJ172S_Reg_368	Configuring maximum Allowed Clients Per AP Radio as 4 and connecting client with WPA 2 Personal security.	To configure maximum allowed client Per AP radio as 4 and connecting 5 different client with radio policy as ALL and check if the number of client that is configured alone gets connected to the WLAN	Passed	
EWCJ172S_Reg_369	Configuring maximum Allowed Clients Per AP Radio as 3 and connecting client with WPA 2 Enterprise security .	To configure maximum allowed client Per AP radio as 3 and connecting 4 different client with radio policy as ALL and now after 3 client disconnect one client and check if other client get authenticated to the WLAN	Passed	
EWCJ172S_Reg_370	Configuring maximum Allowed Clients Per AP Radio in RF profile as 4 and in WLAN as 3 and connecting the client	To configure maximum allowed client Per AP radio in RF profile and also setting the same in WLAN and check which of the configured number of clients gets connected .	Passed	
EWCJ172S_Reg_371	Creating WPA 2 Personal security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Personal and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

EWCJ172S_Reg_372	Creating WPA 2 Enterprise security WLAN with radio policy as 5 GHz and configuring Maximum Allowed Clients Per AP Radio	To configure maximum allowed client per AP radio setting the WLAN security with WPA 2 Enterprise and radio policy as 5 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	
EWCJ172S_Reg_373	Creating WPA 2 Personal security WLAN with radio policy as 2.4 GHz and configuring Maximum Allowed Clients Per AP Radio	To create WPA 2 Personal security WLAN configuring Maximum allowed client per AP radio with radio policy as 2.4 GHz and check if only the defined number of client alone connect to the WLAN.	Passed	

TLS Tunnel

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_138	Associating Windows JOS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Windows JOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
EWLCJ172S_Reg_139	Associating iOS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Apple iOS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	

EWLCJ172S_Reg_140	Associating MAC OS Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether MAC OS client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
EWLCJ172S_Reg_141	Associating Android Client with WPA2-dot1x using ISE server in cloud via TLS Tunnel	To verify whether Android client associated successfully or not with WPA2-dot1x via ISE server configured in cloud	Passed	
EWLCJ172S_Reg_142	Allowing the user for complete access to CME network via TACACS (ISE server configured in cloud)	To check whether user can able to read-write access the complete CME network or not via TACACS (ISE server configured in cloud)	Passed	
EWLCJ172S_Reg_143	Associating all OS clients to CME with Security MAC filtering via Cloud ISE server	To check whether all OS clients associated successfully or not to CME with Mac filtering via Cloud ISE server	Passed	
EWLCJ172S_Reg_144	Setting up the tunnel configurations in CME	To check whether tunnel status get UP or not after configuring in CME	Passed	
EWLCJ172S_Reg_145	Checking the ME association with PI after establishing TLS tunnel	To check whether ME is getting synchronized or not with PI	Passed	
EWLCJ172S_Reg_146	Checking the TLS Tunnel configurations after export/import the config file via TFTP	To check whether TLS Tunnel configurations gets retained or not while export/import the config file via TFTP	Passed	

EWLCJ172S_Reg_147	Checking the RADIUS server's reachability from CME	To check whether cloud RADIUS server is reachable or not from eWLCusing Ping functionality/username in troubleshooting tools page	Passed	

Syslogs

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_256	Adding syslog server in eWLC and checking the syslog messages in syslog server	To check whether syslog's are generating in syslog server after adding in Ewlc	Passed	
EWLCJ172S_Reg_257	Configuring multiple syslog servers in eWLC and checking the syslog messages in syslog server	To verify whether syslog's are generating in syslog server after adding multiple servers in Ewlc	Passed	
EWLCJ172S_Reg_258	Downloading the syslog's after generated in Ewlc	To check whether able to download the syslog's from Ewlc	Passed	
EWLCJ172S_Reg_259	Clearing the logs in controller after generated successfully	To verify whether user able to clear the all generated logs in Ewlc	Passed	
EWLCJ172S_Reg_260	Checking the alert messages after configured syslog server level as "alert"	To check the alert syslog's in syslog server after configured severity level as alert	Passed	
EWLCJ172S_Reg_261	Configuring syslog servers in eWLC with log level setting as critical	To verify the critical logs in syslog server after configuration in device	Passed	

EWLCJ172S_Reg_262	Checking the information messages after configured syslog server level as "information"	To check the information syslog's in syslog server after configured severity level as information	Passed	
EWLCJ172S_Reg_263	Checking the debugging messages after configured syslog server level as "debugging"	To check the debugging syslog's in syslog server after configured severity level as debugging	Passed	
EWCJ172S_Reg_285	Enabling logging for Errors in eWLC-ME	To check whether log can be generated or not for Error Message in eWLC-ME GUI	Passed	
EWCJ172S_Reg_286	Disabling logging for Errors in eWLC-ME	To check whether logging for Errors disabled or not in eWLC-ME	Passed	
EWCJ172S_Reg_287	Enabling logging for Debugging in eWLC-ME	To check whether log can be generated or not for Debug Message in eWLC-ME GUI	Passed	
EWCJ172S_Reg_288	Enabling logging server for Emergencies	To check whether log can be generated or not for Emergencies in eWLC-ME GUI	Passed	
EWCJ172S_Reg_289	Enabling logging for Alerts	To check whether log can be generated or not for alerts in eWLC-ME GUI	Passed	
EWCJ172S_Reg_290	Enabling logging for Warning	To check whether log can be generated or not for warning in eWLC-ME GUI	Passed	
EWCJ172S_Reg_291	Enabling logging for Critical	To check whether log can be generated or not for critical events in eWLC-ME GUI	Passed	

EWCJ172S_Reg_292	Enabling logging for Notification	To check whether log can be generated or not for notification in eWLC-ME GUI	Passed	
EWCJ172S_Reg_293	Enabling logging for Information message	To check whether log can be generated or not for Informational message in eWLC-ME GUI	Passed	
EWCJ172S_Reg_294	Checking the validation of syslog errors in PI	To check whether the syslog errors are displayed in PI	Passed	
EWCJ172S_Reg_295	Checking the validation of syslog information in PI	To check whether the syslog information are displayed in PI	Passed	
EWCJ172S_Reg_296	Checking the historic information about syslog in PI	To check whether the historic information about syslog in PI	Passed	
EWCJ172S_Reg_297	Validating the syslog warning message in PI	To check whether the syslog warning message in PI	Passed	
EWCJ172S_Reg_298	Validating the syslog notification in PI	To check whether syslog notification in PI	Passed	
EWCJ172S_Reg_299	Verifying the severity filtering for syslog in PI	To verify the severity filtering for syslog in PI	Passed	
EWCJ172S_Reg_300	Verifying the Device IP address filtering for syslog in PI	To verify the Device IP address filtering for syslog in PI	Passed	

Internal DHCP Server

Logical Id	Title	Description	Status	Defect ID

EWLCJ172S_Reg_200	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ172S_Reg_201	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ172S_Reg_202	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ172S_Reg_203	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWLCJ172S_Reg_204	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	
EWCJ172S_Reg_233	Mapping a Internal DHCP pool to WLAN and verifying Windows Client IP Address and vlan id	To verify whether a window client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ172S_Reg_234	Mapping a Internal DHCP pool to WLAN and verifying Android Client IP Address and vlan id	To verify whether a Android client get Ip address and vlan id from a specified DHCP pool or not	Passed	

EWCJ172S_Reg_235	Mapping a Internal DHCP pool to WLAN and verifying MAC Client IP Address and vlan id	To verify whether a MAC Os client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ172S_Reg_236	Mapping a Internal DHCP pool to WLAN and verifying iOS Client IP Address and vlan id	To verify whether a iOS client get Ip address and vlan id from a specified DHCP pool or not	Passed	
EWCJ172S_Reg_237	Checking lease period for connected Client through a DHCP pool	To verify whether DHCP release a particular IP address or not after a certain lease period for client	Passed	

Lobby Ambassador

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_67	Create and verify Lobby user account and try to login GUI with lobby credentials.	To verify the user able to login GUI with the lobby user credentials.	Passed	
EWLCJ172S_Reg_68	Create 3 lobby users and try to login GUI with all 3 lobby users with different browsers.	To verify the user able to login GUI with the all 3 lobby user credentials with different browsers.	Passed	
EWLCJ172S_Reg_69	Delete the Created lobby users and try to login GUI with lobby user credentials.	To verify the user able to login GUI with the deleted lobby user credentials .	Passed	
EWLCJ172S_Reg_70	Create the Lobby user and try to login CLI with lobby credentials.	To verify the user able to login CLI with the lobby credentials.	Passed	

EWLCJ172S_Reg_71	Create 3 lobby users and try to login CLI with all 3 lobby users with Telnet.	To verify the user able to login CLI with the all 3 lobby credentials with Telnet	Passed	
EWLCJ172S_Reg_72	Create 3 lobby users and try to login CLI with all 3 lobby users with SSh	To verify the user able to login CLI with the all 3 lobby credentials with SSH	Passed	
EWLCJ172S_Reg_73	Delete the Created lobby users and try to login CLI with lobby user credentials.	To verify the user able to login CLI with the deleted lobby user credentials .	Passed	
EWLCJ172S_Reg_74	Create and verify the lobby user in CLI	To verify the User able to login with Lobby credentials	Passed	

Mac filtering (for L2 security)

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_168	Adding Windows 10 Client mac address in eWLCand checking the connection of Clients in 1800 Series ME	To add the windows Client mac address in mac filtering in eWLC UI and checking whether Clients gets associated or not successfully	Passed	
EWLCJ172S_Reg_169	Uploading the empty CSV file in eWLC UI	To check whether an blank CSV file could be uploaded in eWLC UI	Passed	
EWLCJ172S_Reg_170	Importing the .CSV file with modifications in eWLC UI	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
EWLCJ172S_Reg_171	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	

EWLCJ172S_Reg_172	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWLCJ172S_Reg_173	Connecting the Client with WLAN as MAC Filtering+WPA Enterprise Choosing Authentication Server as AP	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as AP	Passed	
EWLCJ172S_Reg_174	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	
EWLCJ172S_Reg_175	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWLCJ172S_Reg_176	Connecting the Client and then moving it to block using MAC address	To Connect the client and then blocking it using the MAC address	Passed	
EWCJ172S_Reg_207	Adding Windows 10 Client mac address in eWC and checking the connection of Clients	To add the windows Client mac address in mac filtering in eWC and checking whether Clients gets associated or not successfully in	Passed	
EWCJ172S_Reg_208	Uploading the empty CSV file in eWC UI	To check whether an blank CSV file could be uploaded in eWC UI	Passed	

EWCJ172S_Reg_209	Importing the .CSV file with modifications in eWC	To check whether .CSV file gets imported or not after importing the updated file with some changes in it	Passed	
EWCJ172S_Reg_210	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
EWCJ172S_Reg_211	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWCJ172S_Reg_212	Connecting the Client with Wlan Security Type as WPA Enterprise enabling MAC Filtering option Choosing Authentication Server as External Radius and RADIUS Compatibility as other	To Connect the Client with MAC Filtering using WPA Enterprise as security type choosing Authentication Server as External Radius and RADIUS Compatibility as other	Passed	
EWCJ172S_Reg_213	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWCJ172S_Reg_214	Connecting the Client and then moving it to block using MAC address	To Connect the client and then blocking it using the MAC address	Passed	

TACACS

Logical Id	Title	Description	Status	Defect ID

EWLCJ172S_Reg_129	Allowing the user for complete access to eWLC network via TACACS	To check whether user can able to read-write access the complete eWLC network or not via TACACS	Passed	
EWLCJ172S_Reg_130	Providing the user for lobby admin access to the eWLC via TACACS	To check whether user can able to have lobby admin access or not to eWLC via TACACS	Passed	
EWLCJ172S_Reg_131	Providing the user for monitoring access to the eWLC via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to eWLC via TACACS	Passed	
EWLCJ172S_Reg_132	Trying to login eWLC via TACACS with invalid credentials	To check whether user can able to login or not in eWLC via TACACS with invalid credentials	Passed	
EWLCJ172S_Reg_133	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	
EWLCJ172S_Reg_134	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
EWLCJ172S_Reg_135	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	

EWLCJ172S_Reg_136	Providing the user for selected access to the eWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN", "Controller", "Wireless", "Security", "Command Line Interfaces and "Management" checkboxes.	Passed	
EWLCJ172S_Reg_137	Trying to login eWLC network via TACACS with Invalid credentials.	To verify whether user can able to login or not in eWLC via TACACS with invalid credentials	Passed	
EWCJ172S_Reg_131	Allowing the user for complete access to ME EWLC network via TACACS	To check whether user can able to read-write access the complete ME EWLC network or not via TACACS	Passed	
EWCJ172S_Reg_132	Providing the user for lobby admin access to the ME EWLC via TACACS	To check whether user can able to have lobby admin access or not to ME EWLC via TACACS	Passed	
EWCJ172S_Reg_133	Providing the user for monitoring access to the ME EWLC via TACACS	To check whether user can able to have monitoring access (which is read-only) or not to ME EWLC via TACACS	Passed	
EWCJ172S_Reg_134	Trying to login ME EWLC via TACACS with invalid credentials	To check whether user can able to login or not in ME EWLC via TACACS with invalid credentials	Passed	
EWCJ172S_Reg_135	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN" and "Controller" checkboxes.	Passed	

REVIEW DRAFT - CISCO CONFIDENTIAL

EWCJ172S_Reg_136	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Wireless" and "Security" checkboxes.	Passed	
EWCJ172S_Reg_137	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "Command" and "Management" checkboxes.	Passed	
EWCJ172S_Reg_138	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like"WLAN, Controller, Wireless, Security, Command Line Interfaces and "Management" checkboxes.	Passed	
EWCJ172S_Reg_139	Trying to login ME EWLC network via TACACS with Invalid credentials.	To verify whether user can able to login or not in ME EWLC via TACACS with invalid credentials	Passed	

Open DNS

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_389	Verifying ewlc registered with open DNS server	To Verify whether the ewlc registered in open DNS and eWLC got the device ID or not	Passed	
EWLCJ172S_Reg_390	Verifying the created profile mapped with eWLC GUI and CLI	To Verify whether the profile mapped with eWLC and reflected in eWLC GUI & CLI or not	Passed	
EWLCJ172S_Reg_391	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	

EWLCJ172S_Reg_392	Verifying the open DNS configuration for the connected Windows Client in eWLC UI/CLI	To Verify whether the open DNS configured or not when Windows JOS connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ172S_Reg_393	Verifying the open DNS configuration for the connected MAC OS Client in eWLC UI/CLI	To Verify whether the open DNS configured or not when MAC OS connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ172S_Reg_394	Verifying the open DNS configuration for the connected iOS Client in eWLC UI/CLI	To Verify whether the open DNS configured or not when iOS client connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ172S_Reg_395	Verifying the open DNS configuration for the connected Android Client in eWLC UI/CLI	To Verify whether the open DNS configured or not when Android client connected to Umbrella enabled WLAN Profile	Passed	
EWLCJ172S_Reg_396	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWLCJ172S_Reg_397	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWLCJ172S_Reg_398	Perform the roaming between two ewlc	To verify the open dns after Inter roaming	Passed	
EWCJ172S_Reg_335	verifying ewc registered with open DNS server	To Verify whether the ewc registered in open DNS and ewc got the device ID or not	Passed	

EWCJ172S_Reg_336	Verifying the created profile mapped with ewc GUI and CLI	To Verify whether the profile mapped with ewc and reflected in ewc GUI & CLI or not	Passed	
EWCJ172S_Reg_337	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWCJ172S_Reg_338	Verifying the open DNS configuration for the connected Windows Client in ewc UI/CLI	To Verify whether the open DNS configured or not when Windows JOS connected to Umbrella enabled WLAN Profile	Passed	
EWCJ172S_Reg_339	Verifying the open DNS configuration for the connected MAC OS Client in ewc UI/CLI	To Verify whether the open DNS configured or not when MAC OS connected to Umbrella enabled WLAN Profile	Passed	
EWCJ172S_Reg_340	Verifying the open DNS configuration for the connected iOS Client in ewc UI/CLI	To Verify whether the open DNS configured or not when iOS client connected to Umbrella enabled WLAN Profile	Passed	
EWCJ172S_Reg_341	Verifying the open DNS configuration for the connected Android Client in ewc UI/CLI	To Verify whether the open DNS configured or not when Android client connected to Umbrella enabled WLAN Profile	Passed	
EWCJ172S_Reg_342	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWCJ172S_Reg_343	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	

EWCJ172S_Reg_344	Perform the roaming between two ewc	To verify the open dns after Inter roaming	Passed	

EWLC Crashes(DHCP/Troubleshootings)

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_320	Creating the DHCP scope form CLI with invalid IP address and oberserve crash while configuring	To verify whether invalid IP accepting in DHCP pool or not and EWLC not crashing	Passed	
EWLCJ172S_Reg_321	Mapping the DHCP pool to interface and oberserve crash while configuring	To verify whether DHCP pool mapped to interface or not and EWLC not crashing	Passed	
EWLCJ172S_Reg_322	Changing the RRM details after client connected to WLAN	To verify whether EWLC going to Crash or not after changing the RRM details	Passed	
EWLCJ172S_Reg_323	Creating more than 10 DHCP pool in EWLC with Japanese UI	To verify whether more than 10 DHCP pools are created and EWLC not crashing	Passed	
EWLCJ172S_Reg_324	Clearing the EWLC Configurations	To verify whether Controller Configurations are clearing or not	Passed	
EWLCJ172S_Reg_325	Backup & Restore the EWLC Configurations	To verify whether Controller Configurations are Backup & Restore or not and EWLC not crashing	Failed	CSCvt78675
EWLCJ172S_Reg_326	Convert the CAPWAP to EWLC	To verify whether AP can be converted to new EWLC or not without crash	Passed	

EWLCJ172S_Reg_327	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not and EWLC not crashing	Passed	
EWLCJ172S_Reg_328	Checking the ping response	To verify whether ping response is getting without packet drop and EWLC not crashing	Passed	
EWLCJ172S_Reg_329	Checking the traceroute response	To verify whether traceroute response is getting with actual hop count and EWLC not crashing	Passed	

EWC Crashes(DHCP/Troubleshootings)

EWCJ172S_Reg_121	Creating the DHCP scope form CLI with invalid IP address and oberserve crash while configuring	To verify whether invalid IP accepting in DHCP pool or not and eWC not crashing	Passed	
EWCJ172S_Reg_122	Mapping the DHCP pool to interface and oberserve crash while configuring	To verify whether DHCP pool mapped to interrace or not and eWC not crashing	Passed	
EWCJ172S_Reg_123	Changing the RRM details after client connected to WLAN	To verify whether eWC going to Crash or not after changing the RRM details	Passed	
EWCJ172S_Reg_124	Creating more than 10 DHCP pool in eWC with Japanese UI	To verify whether more than 10 DHCP pools are created and eWC not crashing	Passed	
EWCJ172S_Reg_125	Clearing the eWC Configurations	To verify whether Controller Configurations are clearing or not	Passed	

EWCJ172S_Reg_126	Backup & Restore the eWC Configurations	To verify whether Controller Configurations are Backup & Restore or not and eWC not crashing	Passed	
EWCJ172S_Reg_127	Convert the CAPWAP to eWC	To verify whether AP can be converted to new eWC or not without crash	Passed	
EWCJ172S_Reg_128	Invalid DNS server IP address configuration	To verify whether DNS IP address field accepting the Invalid IP address or not and eWC not crashing	Passed	
EWCJ172S_Reg_129	Checking the ping response	To verify whether ping response is getting without packet drop and eWC not crashing	Passed	
EWCJ172S_Reg_130	Checking the traceroute response	To verify whether traceroute response is getting with actual hop count and eWC not crashing	Passed	

SNMP trap

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_194	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	
EWLCJ172S_Reg_195	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	

EWLCJ172S_Reg_196	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
EWLCJ172S_Reg_197	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
EWLCJ172S_Reg_198	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	
EWLCJ172S_Reg_199	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	
EWCJ172S_Reg_279	Create the SNMP trap receiver name with invalid IP address.	To check whether the SNMP trap receiver is created with invalid IP address or not in CME GUI	Passed	
EWCJ172S_Reg_280	Create the SNMP trap receiver name is the more than 31 characters in CME ui.	To check whether the SNMP trap receiver is created with more than 31 characters or not in CME GUI	Passed	
EWCJ172S_Reg_281	Checking the validation of SNMP trap receiver information.	To check whether the SNMP trap receiver is received the information or not.	Passed	
EWCJ172S_Reg_282	Verifying the severity filtering for SNMP trap receiver information.	To verify the severity filtering for SNMP trap receiver information.	Passed	
EWCJ172S_Reg_283	Verifying the Device IP address filtering for SNMP trap receiver in PI	To verify the Device IP address filtering for SNMP trap receiver in PI	Passed	

EWCJ172S_Reg_284	Create the SNMP trap receiver by using the invalid IP address in CME CLI.	To check whether the SNMP trap receiver is created or not in CME CLI	Passed	

Shedule download

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_415	New Config should be applied when changes in old config through schedule download configuration using FTP server	To verify New Config should be applied when changes in old config through schedule download configuration using FTP server	Passed	
EWLCJ172S_Reg_416	New Config should be applied when changes in old config through schedule download configuration using SFTP server	To verify New Config should be applied when changes in old config through schedule download configuration using SFTP server	Passed	
EWLCJ172S_Reg_417	New Config should not applied when old config having no changes through schedule download configuration using FTP server	To verify New Config should not applied when old config having no changes through schedule download configuration using FTP server	Passed	
EWLCJ172S_Reg_418	New Config should not applied when old config having no changes through schedule download configuration using SFTP server	To verify New Config should not applied when old config having no changes through schedule download configuration using SFTP server	Passed	

EWLCJ172S_Reg_419	New config should not apply to the Device using FTP transfer mode when having bad config in server	To verify the new config should not apply to the Device using FTP transfer mode when having bad config in server	Passed	
EWLCJ172S_Reg_420	New config should not apply to the Device using SFTP transfer mode when having bad config in server	To verify the new config should not apply to the Device using SFTP transfer mode when having bad config in server	Passed	
EWLCJ172S_Reg_421	Getting error message when passing wrong CLI commands (Wrong format of server IP address) in schedule download configuration using FTP/SFTP server	To verify Getting error message when passing wrong CLI commands (Wrong format of server IP address) in schedule download configuration using FTP/SFTP server	Passed	
EWLCJ172S_Reg_422	Getting error message when passing wrong CLI commands (Wrong file path/ file name) in schedule download configuration using FTP/SFTP server	To verify Getting error message when passing wrong CLI commands (Wrong file path/file name) in schedule download configuration using FTP/SFTP server	Passed	
EWLCJ172S_Reg_423	New Config should be applied when changes in old config through schedule download configuration using FTP/SFTP server when passing domain name instead of server address in CLI command	To verify New Config should be applied when changes in old config through schedule download configuration using FTP/SFTP server when passing domain name instead of server address in CLI command	Passed	

EWLCJ172S_Reg_424	New Config should not apply when preferred Master AP is up after downloading config	To verify New Config should not apply when preferred Master AP is up after downloading config	Passed	
EWLCJ172S_Reg_425	New config should not apply when passing file name which is not available in the server	To verify New config should not apply when passing file name which is not available in the server	Passed	
EWLCJ172S_Reg_426	verify server reachable error message when FTP/SFTP sever is down	To verify server reachable error message when FTP/SFTP sever is down	Passed	
EWLCJ172S_Reg_427	Verify the behaviour of schedule config download when system time is changed after setting hourly schedule download	To Verify the behaviour of schedule config download when system time is changed after setting hourly schedule download	Passed	
EWLCJ172S_Reg_428	Verify eWLC should be come up (after reset) after downloading new config	To Verify eWLC should be come up (after reset) after downloading new config	Passed	
EWLCJ172S_Reg_429	Verify Ap join and client connectivity after new config downloaded	To verify Ap join and client connectivity after new config downloaded	Passed	
EWLCJ172S_Reg_430	Verify apply new config when Primary controller goes down and secondary controller is active (when both eWLC on same model) after downloading config	To verify apply new config when Primary controller goes down and secondary controller is active (when both eWLC on same model) after downloading config	Passed	

EWLCJ172S_Reg_431	Verify not apply new config when Primary controller goes down and secondary controller is active (when both eWLC on different model) after downloading config	To verify not apply new config when Primary controller goes down and secondary controller is active (when both eWLC on different model) after downloading config	Passed	

ISSU

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_312	Performing Upgradation using ISSU	To check whether the upgradation is performed or not via ftp	Passed	
EWLCJ172S_Reg_313	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ172S_Reg_314	Disabling the Rollback timer during upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ172S_Reg_315	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ172S_Reg_316	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Failed	CSCvt71710
EWLCJ172S_Reg_317	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ172S_Reg_318	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Passed	

REVIEW DRAFT - CISCO CONFIDENTIAL

EWLCJ172S_Reg_319	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	

IRCM

EWLCJ172S_Reg_289	Setting UP the secure mobility tunnel between 9800 Controller & 5520 WLC	To check whether both Control & Data path gets UP or not between 9800 Controller & 5520 Controller	Passed	
EWLCJ172S_Reg_290	Checking the mobility groups configuration after upload/download the config file in 5520 WLC via TFTP	To check whether mobility groups configurations gets retained or not after upload/download the config file via TFTP in 5520 WLC	Passed	
EWLCJ172S_Reg_291	Checking the mobility groups configuration after backup/restore the config file in 9800 Controller via TFTP	To check whether mobility groups configurations gets retained or not after backup/restore the config file via TFTP in Cat 9800 Controller	Passed	
EWLCJ172S_Reg_292	Configuring the Anchor controller option in a WLAN in 5520 WLC UI	To check whether Anchor option can be configured or not in a WLAN for WLC's	Passed	
EWLCJ172S_Reg_293	Configuring the Anchor controller option in 9800 WLC UI	To check whether Anchor option can be configured or not in a 9800 Controller.	Passed	

EWLCJ172S_Reg_294	Performing Inter Controller roaming of Windows client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Windows clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ172S_Reg_295	Performing Inter Controller roaming of Android client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Android clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ172S_Reg_296	Checking Inter Controller roaming of Mac Os client between 9800 Controller and 5520 WLC	To check whether Inter Controller roaming works properly or not for Mac os clients between 5520 WLC and 9800 Controller with secure mobility tunnel config	Passed	
EWLCJ172S_Reg_297	Verifying Inter Controller roaming of different OS clients between 9800 Controller and 5520 WLC with WPA2+dot1x (PEAP)	To check whether Inter Controller roaming works properly or not for clients between 5520 WLC and 9800 Controller with security type WPA2+dot1x (PEAP)	Passed	
EWLCJ172S_Reg_298	Checking the Anchor controller functionality during the roaming of Windows Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client	Passed	

EWLCJ172S_Reg_299	Checking the Anchor controller functionality during the roaming of Android Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client	Passed	
EWLCJ172S_Reg_300	Checking the Anchor controller functionality during the roaming of IOS Client with L2 security-WEP	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client	Passed	
EWLCJ172S_Reg_301	Checking the Mobility groups configuration in Active/Standby HA WLC	To check whether mobility group configurations gets synced or not in Standby WLC during HA	Passed	
EWLCJ172S_Reg_302	Checking the Mobility groups configuration in Active/Standby HA WLC	To check whether mobility group configurations gets synced or not in Standby WLC during HA	Passed	
EWLCJ172S_Reg_303	Checking the Anchor controller functionality during the roaming of Windows Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ172S_Reg_304	Checking the Anchor controller functionality during the roaming of Android Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	

EWLCJ172S_Reg_305	Checking the Anchor controller functionality during the roaming of IOS Client with L2 security-WPA3-SAE	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	
EWLCJ172S_Reg_306	Checking Inter Controller roaming of Windows client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	
EWLCJ172S_Reg_307	Checking Inter Controller roaming of Android client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	
EWLCJ172S_Reg_308	Checking Inter Controller roaming of IOS client between 9800 Controller and 3504 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	
EWLCJ172S_Reg_309	Checking Inter Controller roaming of Windows client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Windows Client with WPA3-SAE security	Passed	

EWLCJ172S_Reg_310	Checking Inter Controller roaming of Android client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of Android Client with WPA3-SAE security	Passed	
EWLCJ172S_Reg_311	Checking Inter Controller roaming of IOS client between 9800 Controller and 8540 WLC	To check whether Anchor controller functionality works properly or not in Cat 9800 Controller during the roaming of IOS Client with WPA3-SAE security	Passed	

mDNS AP Support

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_275	Checking mDNS services are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 9115AP	To check whether the mdns services applying to Mac OS and Apple Tv clients or not after enabling the mDNS-ap to 9115AP.	Passed	
EWLCJ172S_Reg_276	Checking mDNS services are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 9120AP	To check whether the mdns services applying to Mac OS and Apple Tv clients after enabling the mDNS-ap to 9120AP	Passed	
EWLCJ172S_Reg_277	Checking mDNS services are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 4800AP	To check whether the mdns services applying to Mac OS and Apple Tv clients or not after enabling the mDNS-ap to 4800AP.	Passed	
EWLCJ172S_Reg_278	Checking mDNS services are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 3700AP	To check whether the mdns services applying to Mac OS and Apple Tv clients or not after enabling the mDNS-ap to 3700AP	Passed	

EWLCJ172S_Reg_279	Checking the mDNS Services and mDNS AP configuration.	To check whether mDNS Services and mDNS AP support configurations able to configure or not.	Passed	
EWLCJ172S_Reg_280	Verifying the mDNS services and mDNS AP support configurations after changing the AP mode to Monitor from Local	To check whether mDNS Services and mDNS AP support configurations after changing the AP mode to Monitor from Local.	Passed	
EWLCJ172S_Reg_281	Checking mDNS services are applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns AP to 9115AP	To check whether the mdns services applying to Apple iPad and iPhone, Apple Tv clients or not after enabling the mDNS-ap to 9115AP.	Passed	
EWLCJ172S_Reg_282	Checking mDNS services are applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns AP to 4800AP	To check whether the mdns services applying to Apple iPad and iPhone, Apple Tv clients or not after enabling the mDNS-ap to 4800AP.	Passed	
EWLCJ172S_Reg_283	Checking mDNS services are applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns AP to 9120AP	To check whether the mdns services applying to Apple iPad and iPhone, Apple Tv clients or not after enabling the mDNS-ap to 9120AP.	Passed	
EWLCJ172S_Reg_284	Checking mDNS services are applying to Apple iPad and IPhone and Apple Tv clients after enabling the mdns AP to 3700AP	To check whether the mdns services applying to Apple iPad and iPhone, Apple Tv clients or not after enabling the mDNS-ap to 3700AP.	Passed	
EWLCJ172S_Reg_285	Checking the mDNS Services and mDNS AP configuration after export and importing the Configuration file.	To check the mDNS Services and mDNS AP support configurations after export and importing the Configuration file.	Passed	

EWLCJ172S_Reg_286	Checking mDNS services are applying to Apple iPad and Mac os and Apple Chromecast clients with WPA2-PSK security after enabling the mdns AP to 9115/4800/9120/3700AP	To check whether the mdns services applying to Apple iPad and Mac os and Apple Chromecast clients with WPA2-PSK security or not after enabling the mDNS-ap to 9115/4800/9120/3700AP.	Passed	
EWLCJ172S_Reg_287	Checking mDNS services are applying to Apple iPad and Mac os and Apple Chromecast clients with WPA3-SAE security after enabling the mdns AP to 9115/4800/9120/3700AP's	To check whether the mdns services applying to Apple iPad and Mac os and Apple Chromecast clients with WPA2-SAE security or not after enabling the mDNS-ap to 9115/4800/9120/3700AP's.	Passed	
EWLCJ172S_Reg_288	Checking mDNS services are applying to Apple iPad and Mac os and Apple Chromecast clients with Static WEP security after enabling the mdns AP to9115/4800/9120/3700AP's	To check whether the mdns services applying to Apple iPad and Mac os and Apple Chromecast clients with Static WEP security or not after enabling the mDNS-ap to9115/4800/9120/3700AP's.	Passed	

Nat Support

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_338	Perform the roaming scenario and NAT with Windows client.	To Verify the roaming scenario and NAT with Windows client.	Passed	
EWLCJ172S_Reg_339	Perform the roaming scenario and NAT with MAC client.	To Verify the roaming scenario and NAT with MAC client.	Passed	
EWLCJ172S_Reg_340	Perform the roaming scenario and NAT with Android client.	To Verify the roaming scenario and NAT with Android client.	Passed	

EWLCJ172S_Reg_341	Perform the roaming scenario and NAT with Apple client.	To Verify the roaming scenario and NAT with Apple client.	Passed	

IPSK

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_399	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ172S_Reg_400	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ172S_Reg_401	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ172S_Reg_402	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ172S_Reg_403	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ172S_Reg_404	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWLCJ172S_Reg_405	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ172S_Reg_406	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	

EWLCJ172S_Reg_407	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWLCJ172S_Reg_408	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ172S_Reg_409	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ172S_Reg_410	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ172S_Reg_411	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ172S_Reg_412	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ172S_Reg_413	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ172S_Reg_414	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ172S_Reg_28	Verifying the iPSK tag generation for the Connected Window JOS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWCJ172S_Reg_29	Verifying the iPSK tag generation for the Connected MAC OS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	

EWCJ172S_Reg_30	Verifying the iPSK tag generation for the Connected iOS Client in EWC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWCJ172S_Reg_31	Verifying the iPSK tag generation for the Connected Android Client in EWC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	
EWCJ172S_Reg_32	Verifying peer to peer communication of Windows JOS clients while sharing same iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ172S_Reg_33	Verifying peer to peer communication of MAC clients while sharing same iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ172S_Reg_34	Verifying peer to peer communication of iOS clients while sharing same iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ172S_Reg_35	Verifying peer to peer communication of Android clients while sharing same iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the same iPSK tag	Passed	
EWCJ172S_Reg_36	Verifying peer to peer communication of Windows JOS clients while sharing different iPSK tag	To verify whether windows JOS clients are able to ping each other or not when they share the different iPSK tag	Passed	

EWCJ172S_Reg_37	Verifying peer to peer communication of MAC clients while sharing different iPSK tag	To verify whether MAC OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ172S_Reg_38	Verifying peer to peer communication of iOS clients while sharing different iPSK tag	To verify whether iOS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ172S_Reg_39	Verifying peer to peer communication of Android clients while sharing different iPSK tag	To verify whether windows Android OS clients are able to ping each other or not when they share the different iPSK tag	Passed	
EWCJ172S_Reg_40	Verifying peer to peer communication of different OS clients when clients share same iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWCJ172S_Reg_41	Verifying peer to peer communication of different OS clients when clients share different iPSK Tag	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag	Passed	
EWCJ172S_Reg_42	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	

EWCJ172S_Reg_43	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWCJ172S_Reg_44	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	
EWCJ172S_Reg_45	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWCJ172S_Reg_46	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in EWC CLI	Passed	
EWCJ172S_Reg_47	Verifying the wlan configuration with iPSK tag Configuration through EWC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the EWC Web	Passed	
EWCJ172S_Reg_48	Verifying the wlan generation with iPSK tag Configuration through EWC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the EWC CLI	Passed	
EWCJ172S_Reg_49	Verifying iPSK tag for the for different OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	

EWCJ172S_Reg_50	Verifying clients connectivity with iPSK tag while radius fallback is enabled	To verify whether clients iPSK is being generated from secondary AAA server or not	Passed	
EWCJ172S_Reg_51	Verifying generation of iPSK tag with FT-PSK for different OS clients	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK	Passed	
EWCJ172S_Reg_52	Verifying connectivity among the clients when clients are connected to different WLAN	To verify whether the different platform OS clients can ping each other or not based on the iPSK tag	Passed	
EWCJ172S_Reg_53	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWCJ172S_Reg_54	Verifying peer to peer action of connected clients with same iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with central Switching	Passed	
EWCJ172S_Reg_55	Verifying peer to peer action of connected clients with same iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the same iPSK tag with local switching	Passed	
EWCJ172S_Reg_56	Verifying peer to peer action of connected clients with different iPSK tag in case of central switching mode	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with central Switching	Passed	

EWCJ172S_Reg_57	Verifying peer to peer action of connected clients with different iPSK tag in case of local switching	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag with local switching	Passed	
EWCJ172S_Reg_58	Verifying iPSK tag for the for Same OS clients with Flex+Bridge Mode	To verify whether iPSK tag is generated or not for the connected clients	Passed	
EWCJ172S_Reg_59	Verifying generation of iPSK tag with FT-PSK for same OS clients.	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK for same OS Clients.	Passed	
EWCJ172S_Reg_60	Verifying peer to peer action of same OS clients with different iPSK tag in case of local switching with FT-PSK.	To verify whether the same platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK.	Passed	
EWCJ172S_Reg_61	Verifying peer to peer action of different OS clients with different iPSK tag in case of local switching with FT-PSK	To verify whether the different platform OS clients can ping each other or not when they share the different iPSK tag in case of local switching with FT-PSK for the	Passed	
EWCJ172S_Reg_62	Verifying the iPSK tag generation for the Connected AnyConnect Client in EWC UI/CLI	To verify whether iPSK tag generated or not When AnyConnect client connected to iPSK enabled WLAN Profile	Passed	
EWCJ172S_Reg_63	Verifying the iPSK tag generation for the same password with different groups.	To verify whether iPSK tag generated or not for the same password with different groups	Passed	

EWCJ172S_Reg_64	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	
EWCJ172S_Reg_65	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Central Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of central switching.	Passed	
EWCJ172S_Reg_66	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network groups in case of central switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of central switching.	Passed	
EWCJ172S_Reg_67	Verifying the peer to peer communication of different clients connected to different SSIDs in same network group in case of Local Switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in same network group in case of local switching.	Passed	
EWCJ172S_Reg_68	Verifying the peer to peer communication of different clients connected to different SSIDs in Different network group in case of local switching.	To Verify the peer to peer communication of different clients connected to different SSIDs in different network group in case of local switching.	Passed	

EWCJ172S_Reg_69	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWCJ172S_Reg_70	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with same group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with same group	Passed	
EWCJ172S_Reg_71	Verifying iPSK tag and peer to peer communication for the for Same OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for Same OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWCJ172S_Reg_72	Verifying iPSK tag and peer to peer communication for the for different OS clients with Flex+Bridge Mode in case of local switching with different group	To verify whether iPSK tag and peer to peer communication for different OS clients with Flex+Bridge Mode in case of local switching with different group	Passed	
EWCJ172S_Reg_73	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ172S_Reg_74	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

Psk Multi Auth

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_399	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ172S_Reg_400	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ172S_Reg_401	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ172S_Reg_402	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ172S_Reg_403	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ172S_Reg_404	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWLCJ172S_Reg_405	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ172S_Reg_406	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWLCJ172S_Reg_407	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	

EWLCJ172S_Reg_408	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ172S_Reg_409	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ172S_Reg_410	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ172S_Reg_411	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ172S_Reg_412	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ172S_Reg_413	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ172S_Reg_414	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ172S_Reg_01	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWCJ172S_Reg_02	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ172S_Reg_03	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWCJ172S_Reg_04	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	

EWCJ172S_Reg_05	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ172S_Reg_06	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWCJ172S_Reg_07	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ172S_Reg_08	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ172S_Reg_09	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ172S_Reg_10	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ172S_Reg_11	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ172S_Reg_12	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ172S_Reg_13	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWCJ172S_Reg_14	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	

EWCJ172S_Reg_15	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ172S_Reg_16	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

mDNS_Support for wired guest

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_330	Create the Guest Lan with mDNS Mode Bridging Gateway and Verify with Apple TV	Verify able to create the Guest Lan with mDNS Mode Bridging with Apple TV	Passed	
EWLCJ172S_Reg_331	Create the Guest Lan with mDNS Mode Bridging.	Verify able to create the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ172S_Reg_332	Edit the Guest Lan with mDNS Mode Bridging.	Verify able to edit the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ172S_Reg_333	Delete the Guest Lan with mDNS Mode Bridging.	Verify able to Delete the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ172S_Reg_334	Create the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to create with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ172S_Reg_335	Delete the Guest Lan with mDNS Mode Bridging with Guest LAN Map Configuration.	Verify able to Delete with the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ172S_Reg_336	Create the Guest Lan with mDNS Mode Gateway: .	Verify able to Create the Guest Lan with mDNS Mode Bridging Gateway: .	Passed	

EWLCJ172S_Reg_337	Create the Guest Lan with mDNS Mode Bridging Drop.	verify able to Create the Guest Lan with mDNS Mode Drop.	Passed	

WGB_Support_for_9115AP

EWLCJ172S_Reg_28	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWLCJ172S_Reg_29	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWLCJ172S_Reg_30	Configuring WGB in eWLC	To verify WGB configuration is successful or not in eWLC	Passed	
EWLCJ172S_Reg_31	Associating the WGB on open authentication with 9115 AP	To associate the WGB on open authentication and check if the WGB associates with the open WLAN or not.	Passed	
EWLCJ172S_Reg_32	Associating the WGB on WPA 2 with PSK with 9115 bridge AP	To associate the WGB on WPA 2 PSK security with 9115 bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ172S_Reg_33	Associating the WGB on WPA 2 with 802.1x with 9115 AP	To associate the WGB on WPA 2 802.1x security when AP in local mode and check if the WGB associates with the WLAN or not.	Passed	

EWLCJ172S_Reg_34	Associating the WGB on open authentication with flex+bridge	To associate the WGB on open authentication with 9115 AP flex+bridge AP and check if the WGB associates with the open WLAN or not.	Passed	
EWLCJ172S_Reg_35	Associating the WGB on WPA 2 with PSK with flex+bridge AP	To associate the WGB on WPA 2 PSK security with 9115 AP flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ172S_Reg_36	Associating the WGB on WPA 2 with 802.1x with flex+bridge AP	To associate the WGB on WPA 2 802.1x security with 9115 flex+bridge AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ172S_Reg_37	Checking of WGB roaming from one AP to another AP in bridge mode	To check the roaming of WGB from one AP to another AP when the AP is in bridge mode .	Passed	
EWLCJ172S_Reg_38	Checking of WGB roaming from one AP to another AP in flex+bridge mode	To check the roaming of WGB from one AP to another AP when Aps are in flex+bridge mode	Passed	
EWLCJ172S_Reg_39	Performing Inter controller roaming for WGB clients with OPEN security in AP flex+bridge mode	To check inter controller roaming for WGB clients with OPEN security in AP flex+bridge mode	Passed	
EWLCJ172S_Reg_40	Performing Inter controller roaming for WGB clients with WPA2 PSK security in AP flex+bridge mode	To check inter controller roaming for WGB clients with WPA2 PSK security in AP flex+bridge mode	Passed	

EWLCJ172S_Reg_41	Performing Inter controller roaming for WGB clients with WPA2 Dot1x security in AP flex+bridge mode	To check inter controller roaming for WGB clients with WPA2 Dot1x security in AP flex+bridge mode	Passed	
EWLCJ172S_Reg_42	Performing Inter controller roaming for WGB clients with OPEN security in AP bridge mode	To check inter controller roaming for WGB clients with OPEN security in AP bridge mode	Passed	
EWLCJ172S_Reg_43	Performing Inter controller roaming for WGB clients with WPA2 PSK security in AP bridge mode	To check inter controller roaming for WGB clients with WPA2 PSK security in AP bridge mode	Passed	
EWLCJ172S_Reg_44	Performing Inter controller roaming for WGB clients with WPA2 Dot1x security in AP bridge mode	To check inter controller roaming for WGB clients with WPA2 Dot1x security in AP bridge mode	Passed	
EWLCJ172S_Reg_45	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWLCJ172S_Reg_46	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients after session timeout	Passed	
EWLCJ172S_Reg_47	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

Mesh Support on all 11ac

Logical Id	Title	Description	Status	Defect ID
EWLCJ172S_Reg_01	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	

EWLCJ172S_Reg_02	Check the Joining of 3800AP in to eWLC with Mesh /Bridge Mode	To check the Mesh/Bridge support of 3800 AP after joining in to eWLC	Passed	
EWLCJ172S_Reg_03	Check the Joining of 3800AP in to eWLC with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 3800 AP in to eWLC	Passed	
EWLCJ172S_Reg_04	Check the Joining of 4800AP in to eWLC with Mesh/Bridge Mode	To check the Mesh/Bridge support of 4800 AP after joining in to eWLC	Passed	
EWLCJ172S_Reg_05	Check the Joining of 4800AP in to eWLC with Flex+Bridge Mode	To check the Flex+Bridge Mode support of 4800 AP in to eWLC	Passed	
EWLCJ172S_Reg_06	Verify the Windows clients connection for bridge mode AP's with WEP security	To check whether the windows client is connected or not to bridge mode AP's	Passed	
EWLCJ172S_Reg_07	Verify the Android clients connection for bridge mode AP's with WEP security	To check whether the Android client is connected or not to bridge mode AP's	Passed	
EWLCJ172S_Reg_08	Verify the IOS clients connection for bridge mode AP's with WEP security	To check whether the IOS client is connected or not to bridge mode AP's	Passed	
EWLCJ172S_Reg_09	Verify the Windows clients connection for Flex+bridge mode AP's with WEP security	To check whether the windows client is connected or not to Flex+bridge mode AP's	Passed	
EWLCJ172S_Reg_10	Verify the Android clients connection for Flex+bridge mode AP's with WEP security	To check whether the Android client is connected or not to Flex+bridge mode AP's	Passed	

EWLCJ172S_Reg_11	Verify the IOS clients connection for Flex+bridge mode AP's with WEP security	To check whether the IOS client is connected or not to Flex+bridge mode AP's	Passed	
EWLCJ172S_Reg_12	Verify the Windows clients connection for bridge mode AP's with WPA2-PSk security	To check whether the windows client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ172S_Reg_13	Verify the Android clients connection for bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ172S_Reg_14	Verify the IOS clients connection for bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ172S_Reg_15	Verify the Windows clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the windows client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ172S_Reg_16	Verify the Android clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the Android client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ172S_Reg_17	Verify the IOS clients connection for Flex+bridge mode AP's with WPA2-PSK security	To check whether the IOS client is connected or not to Flex+bridge mode AP's with WPA2-PSK security	Passed	
EWLCJ172S_Reg_18	Verify the Windows clients connection for bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	

EWLCJ172S_Reg_19	Verify the Android clients connection for bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ172S_Reg_20	Verify the IOS clients connection for bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ172S_Reg_21	Verify the Windows clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the windows client is connected or not to Flex+bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ172S_Reg_22	Verify the Android clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the Android client is connected or not to Flex+bridge mode AP's with WPA3-SAEsecurity	Passed	
EWLCJ172S_Reg_23	Verify the IOS clients connection for Flex+bridge mode AP's with WPA3-SAE security	To check whether the IOS client is connected or not to Flex+bridge mode AP's with WPA3-SAE security	Passed	
EWLCJ172S_Reg_24	Check and verify the AP mode changes by changing From bridge mode to local	To check whether AP mode changing or not from bridge to local	Passed	
EWLCJ172S_Reg_25	Check and verify the AP mode changes by changing From Flex+bridge mode to Flex connect.	To check whether AP mode changing or not from Flex+bridge to Flex connect.	Passed	
EWLCJ172S_Reg_26	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	

EWLCJ172S_Reg_27	Check and verify the intra roaming with Flex+bridge mode AP	To check whether intra roaming happening or not with Flex+bridge mode Ap's	Passed	

SR Cases

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_SR_01	Checking the rendering issue while navigating to mobility tab.	To verify whether the rendering issue is not found while navigating to mobility tab in latest internet explorer browser	Passed	
EWLCJ172S_SR_02	Capture the Console logs in EWLC Dashboard page via Firefox	To verify console logs are captured or not through Firefox	Passed	
EWLCJ172S_SR_03	Checking the ip address of catalyst AP after joining to the controller.	To check whether the Catalyst AP getting IP or not after joined to the controller	Passed	
EWLCJ172S_SR_04	Checking the ip address of 9130 AP after client connectivity and controller reload	To check whether the 9130 AP getting IP or not after client connectivity and controller reload.	Passed	
EWLCJ172S_SR_05	configuring mode of access as switch port in catalyst ap	To check whether the AP getting IP or not after configuring mode of access as switch port	Passed	
EWLCJ172S_SR_06	Checking the error message in CMX for different clients connected to different AP.	To check whether any error message is coming or not while connecting different client to different AP	Passed	

EWLCJ172S_SR_07	Verifying the clients details in CMX for different clients keeping the client ideal for some time .	To verify different client details in CMX keeping the client ideal for some time and check any error message appear or not.	Passed	
EWLCJ172S_SR_08	Verify the Client devices are reporting health.	To verify whether Client device are reporting health or not.	Passed	
EWLCJ172S_SR_09	Check the number of Client visits to the building and the floor and devices are reporting health.	To check the number of new Clients and repeated Clients to the building or floor	Passed	
EWLCJ172S_SR_10	Checking the AP crash issue while upgrade/downgrade the latest software image in eWLC	To verify whether AP crashes occur or not while upgrade/downgrade the latest software image in eWLC	Passed	
EWLCJ172S_SR_11	Checking the AP Crash issue while Change the AP radios in eWLC	To verify whetherAP Crash issue occur while Changing the AP radios in eWLC	Passed	
EWLCJ172S_SR_12	Checking any crash issue while Joining of 9130 AP in to eWLC with Mesh /Bridge Mode	To check whether any crash issue occur while joining 9130 AP with mesh/bridge mode	Passed	
EWLCJ172S_SR_13	Checking mesh setup by configuring RAP downlink with 2.4GhZ/5 Ghz	To check whether the mesh setup is proper or not by setting RAP downlink to 2.4GhZ/5 Ghz	Passed	
EWLCJ172S_SR_14	Changing continuously policy tag for 9120 AP & checking the AP and client behaviour in eWLC	To check Whether the AP & client details are proper while changing the Policy tag	Passed	

EWLCJ172S_SR_15	Changing the 9115 AP Country code and checking the AP behaviour	To Check whether any crash occur while changing the 9115 AP country code	Passed	
EWLCJ172S_SR_16	Verify the 4800/2800AP with multicast traffic.	To verify whether 4800/2800AP crashing or not with multicast traffic.	Passed	
EWLCJ172S_SR_17	Verify the 4800/2800 Bridge mode AP with multicast traffic.	To verify whether 4800/2800 Bridge mode AP crashing or not with multicast traffic.	Passed	
EWLCJ172S_SR_18	Verify the 4800/2800AP by passing the multicast traffic to 5 clients.	To verify whether 4800/2800AP crashing or not by passing the multicast traffic to 5clients.	Passed	
EWLCJ172S_SR_19	Checking the c9130 AP connectivity after joined MU-MIMO clients	To check the c9130 is not reloading after joined MU-MIMO clients to 9130 AP	Passed	
EWLCJ172S_SR_20	Checking the c9115/c9120 AP connectivity after joined MU-MIMO clients	To check the c9115/c9120 is not reloading after joined MU-MIMO clients to 9130 AP	Passed	
EWLCJ172S_SR_21	Checking the ap crash in 4800 AP	To check the 4800 AP crash logs that using in network	Passed	
EWLCJ172S_SR_22	Checking the ap crash in 9115 AP	To check the 9115 AP crash logs that using in network	Passed	
EWLCJ172S_SR_23	Resetting 9130 AP radios multiple times (10 times)	To check that radio is up after every reset	Passed	
EWLCJ172S_SR_24	Resetting 4800 AP radios multiple times (10 times)	To check that radio is up after every reset	Passed	
EWLCJ172S_SR_25	Checking the memory increasing rapidly in 9130 AP	To check memory increased rapidly in 9130 AP	Passed	

EWLCJ172S_SR_26	Checking the memory increasing rapidly in 9115 AP	To check memory increased rapidly in 9115 AP	Passed	
EWLCJ172S_SR_27	Moving COS AP from connected to standalone and vice versa	To move the COS AP from connected to standalone & vice versa and observe crash if any	Passed	
EWLCJ172S_SR_28	Moving EWC internal AP from connected to standalone and vice versa	To move the EWC internal AP from connected to standalone & vice versa and observe crash if any	Passed	
EWLCJ172S_SR_29	Observing 'ThreadSafeQueue: overflow' message while reloading catalyst Aps	To observe 'ThreadSafeQueue: overflow' message while reloading AP	Passed	
EWLCJ172S_SR_30	Observing 'ThreadSafeQueue: overflow' message while reloading catalyst Aps	To observe 'ThreadSafeQueue: overflow' message while reloading AP	Passed	
EWLCJ172S_SR_31	Checking inventory of Catalyst AP and make sure that it has correct domain wrt part id	To check the inventory of Catalyst AP and make sure that it has correct domain wrt part id or not	Passed	
EWLCJ172S_SR_32	Connecting 5 clients to c9115 AP and verify that beacon stuck due to high cca load or not	To verify the beacon stuck due to high cca load or not while serving 4 to 5 clients	Passed	
EWLCJ172S_SR_33	Connecting 5 clients to c9130 AP and verify that beacon stuck due to high cca load or not	To verify the beacon stuck due to high cca load or not while serving 4 to 5 clients	Passed	
EWLCJ172S_SR_34	CMX 10.6.1 : password expiry and change password	To check if password change gets implemented after the user gets password expiry message and if new password is set.	Passed	

EWLCJ172S_SR_35	CMX 10.6.2 : password expiry and change password	To check if password change gets implemented after the user gets password expiry message and if new password is set.	Passed	
EWLCJ172S_SR_36	CMX 10.6.2 : Check password expiry configuration & lifetime effect through CLI	To check if password change expiry & lifetime is configured through CLI and taken effect	Passed	
EWLCJ172S_SR_37	CMX 10.6.2 : Check password expiry & lifetime configuration effect through UI	To check if password change expiry & lifetime is configured through UI and taken effect	Passed	
EWLCJ172S_SR_38	CMX 10.6.2 : Check password expiry & lifetime configuration effect after cmx restart	To check if password change expiry & lifetime is configured through UI and taken effect after cmx agent restart	Passed	
EWLCJ172S_SR_39	Redirection flow on guest/BYOD portal is broken with untrusted certificate on ISE portal in other browsers	To verify chrome issue is replicated in Firefox browser	Passed	
EWLCJ172S_SR_40	Redirection flow on guest/BYOD portal is broken with untrusted certificate on ISE portal in other browsers	To verify chrome issue is replicated in IE/Edge browser	Passed	
EWLCJ172S_SR_41	Redirection flow on guest/BYOD portal is broken with untrusted certificate on ISE portal in other browsers & devices	To verify chrome issue in other devices and in different mobile browsers	Passed	
EWLCJ172S_SR_42	Stale ARP entry because of Static IP client scenario	To check ARP entry issue with Win 10 client	Passed	

EWLCJ172S_SR_43	Stale ARP entry because of Static IP client scenario	To check ARP entry issue with mobile client	Passed	
EWLCJ172S_SR_44	Stale ARP entry because of Static IP client scenario	To check ARP entry issue with different AP models	Passed	
EWLCJ172S_SR_45	Stale ARP entry because of Static IP client scenario	To check ARP entry issue with different security method configured	Passed	
EWLCJ172S_SR_46	Check AP info upon AP unplug & connect to switch	To check if AP joins eWLC automatically upon after initial connect & unplug with switch	Passed	
EWLCJ172S_SR_47	Check AP info upon AP unplug & connect to switch	To check if different models of AP join eWLC automatically upon after initial connect & unplug with switch	Passed	
EWLCJ172S_SR_48	Check AP info upon AP factory reset, unplug & connect to switch	To check if AP joins eWLC automatically upon after initial connect, factory reset & unplug with switch	Passed	
EWLCJ172S_SR_49	3702 AP 5GHz radio with controller and client traffic scenario	To check If AP is functional with 5GHz radio enabled and client traffic is enabled without memory loss	Passed	
EWLCJ172S_SR_50	3702 AP 2.4GHz radio with controller and client traffic scenario	To check If AP is functional with 2.4GHz radio enabled and client traffic is enabled without memory loss	Passed	
EWLCJ172S_SR_51	Different models of AP 5GHz radio with controller and client traffic scenario	To check If AP is functional with 5GHz radio enabled and client traffic is enabled without memory loss	Passed	

REVIEW DRAFT - CISCO CONFIDENTIAL

EWLCJ172S_SR_52	Different models of AP 2.4GHz radio with controller and client traffic scenario	To check If AP is functional with 2.4GHz radio enabled and client traffic is enabled without memory loss	Passed	
EWLCJ172S_SR_53	Unified to autonomous conversion 2600 AP	To check if we're able to convert 2600 AP from unified to autonomous mode.	Passed	
EWLCJ172S_SR_54	Autonomous to unified conversion using 2600 AP	To check if we're able to convert 2600 AP from autonomous to unified mode.	Passed	
EWLCJ172S_SR_55	Unified to autonomous conversion 3700 AP	To check if we're able to convert 3700 AP from unified to autonomous mode.	Passed	
EWLCJ172S_SR_56	Autonomous to unified conversion using 3700 AP	To check if we're able to convert 3700 AP from autonomous to unified mode.	Passed	
EWLCJ172S_SR_57	Monitor client connectivity upon association with an AP over a period of time.	To check client connectivity upon AP association over a period of time we use different models of AP(2800,3800)	Passed	
EWLCJ172S_SR_58	Monitor client connectivity upon association with an AP over a period of time.	To check client connectivity upon 4800 AP association over a period of time.	Passed	
EWLCJ172S_SR_59	Monitor client connectivity upon association with an AP over a period of time.	To check client connectivity upon 9120 AP association over a period of time.	Passed	
EWLCJ172S_SR_60	To check ACL feature using connected client	To check if ACL is enforced onto the connected client and communication is permitted/denied based on ACL.	Passed	

EWLCJ172S_SR_61	To check ACL feature using two windows client and enable/disable traffic between them	To check if ACL is enforced onto the connected clients and if communication is permitted/denied based on ACL.	Passed	
EWLCJ172S_SR_62	Checking the 1700 series AP console logs while changing the Ap radios(2.4 GHz /5GHz)	To Check whether AP crashed or not while changing the radios(2.4 & 5GHz)	Passed	
EWLCJ172S_SR_63	Checking the 1700 series AP console logs after Ap Reset.	To Check whether AP crashed or not after Ap reload.	Passed	
EWLCJ172S_SR_64	Checking the Ap console logs while disabling the MFP configuration	To Check whether ap crashed or not after disabling MFP	Passed	
EWLCJ172S_SR_65	Checking the Time zones name for the COS AP in EWC	To check whether time zones can be modified for the COS AP's	Passed	
EWLCJ172S_SR_66	Checking the Time zones name for the COS AP in EWC after reload	To check whether time zones can be modified for the COS AP's after reload	Passed	
EWLCJ172S_SR_67	Checking the accessibility of the CMX UI.	To verify whether Logging to CMX UI is allowed or not.	Passed	
EWLCJ172S_SR_68	Checking the accessibility of the CMX UI by connecting Android clients.	To verify whether Android clients can be logged to CMX UI is allowed or not.	Passed	
EWLCJ172S_SR_69	Verifying the status and version of CMX via CLI.	To verify the CMX status by logging into the CMX CLI .	Passed	
EWLCJ172S_SR_70	Checking the RTS packet during the connectivity of the client	To verify the RTS packets value during the connectivity of the client.	Passed	

EWLCJ172S_SR_71	Checking the RTS of the client when connecting it to the Probing client.	To verify the RTS packets value during the connectivity of the probing client.	Passed	
EWLCJ172S_SR_72	Checking the RTS of the client during the client roaming	To verify the RTS packets during the client roaming	Passed	
EWLCJ172S_SR_73	Checking the ICMP reply messages on Cisco 9115 AP's	To verify whether the ICMP reply messages from AP	Passed	
EWLCJ172S_SR_74	Checking the ICMP reply messages between the client and the AP	To verify whether the ICMP reply messages are proper between AP and controller	Passed	
EWLCJ172S_SR_75	Checking the ICMP reply messages on Cisco 9130 AP's	To verify whether the ICMP reply messages from AP	Passed	
EWLCJ172S_SR_76	Checking the status of PWRINJ5 connected to AP	To verify the status of PWRINJ5 when connected to AP	Passed	
EWLCJ172S_SR_77	Checking the client status when PWRINJ5 is very low power.	To verify the status of the client when the PWRINJ5 is very low power.	Passed	
EWLCJ172S_SR_78	Checking the status of PWRINJ5 connected to AP	To verify the status of the client when the PWRINJ5 is very low power.	Passed	
EWLCJ172S_SR_79	Verifying the CMX GUI.	To check whether the CMX GUI displaying the proper client count	Passed	
EWLCJ172S_SR_80	Verifying the CMX GUI and checking the response of it.	To check whether the CMX GUI displaying the client count after disconnecting the clients	Passed	
EWLCJ172S_SR_81	Verifying the Location service in CMX.	To check the health of the location service.	Passed	

EWLCJ172S_SR_82	Verifying the status of the client in location page of the CMX using DNAc.	To check the health of the client after deploying it from DNAc	Passed	
EWLCJ172S_SR_83	Verifying the status of the client in location page of the CMX using PI.	To check the health of the client after deploying it from PI	Passed	
EWLCJ172S_SR_84	Checking the AP crash issue while client Roaming between different controllers	To verify whether the clients are roaming between different controllers or not without any Crash.	Passed	
EWLCJ172S_SR_85	Checking the AP crash issue while client Roaming between AP's	To verify whether the clients are roaming between AP's or not without any Crash.	Passed	
EWLCJ172S_SR_86	Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues	To verify the NMSP statistics showing properly or not after changing the NMSP settings	Passed	
EWLCJ172S_SR_87	Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues	To verify the NMSP statistics showing properly or not after changing the NMSP settings	Passed	
EWLCJ172S_SR_88	Configuring Air level license	To verify the license status showing properly or not during the N+1 upgrade	Passed	
EWLCJ172S_SR_89	Perform HA and checking the license status	To verify the license status showing properly or not on HA	Passed	
EWLCJ172S_SR_90	Configuring SSID & assign the Vlan	To verify the SSID created via GUI or not without any error	Passed	
EWLCJ172S_SR_91	Perform the reload via Ap UI	To verify the ap behaviour after giving the reload via GUI	Passed	

EWLCJ172S_SR_92	Resetting the radios of AP in ewlc	To check the ap crash happened or not while resetting the ap radios	Passed	
EWLCJ172S_SR_93	Verifying the internal AP's Association	To check whether the internal AP properly associate with the EWC	Passed	
EWLCJ172S_SR_94	Verifying the internal AP's Association after the EWC reload	To check whether the internal AP properly associate with the EWC after reload	Passed	
EWLCJ172S_SR_95	To Verify the Internal error at setup wizard and setup loop	To Verify the Internal error at setup wizard and setup loop	Passed	
EWLCJ172S_SR_96	Verify Day 0 configuration in 9800- L	Verify Day 0 configuration in 9800- L	Passed	
EWLCJ172S_SR_97	Verify Day 0 configuration in 9800- 80	Verify Day 0 configuration in 9800- 80	Passed	
EWLCJ172S_SR_98	To Verify the Internal error at setup wizard and setup loop with Chrome	To Verify the Internal error at setup wizard and setup loop	Passed	
EWLCJ172S_SR_99	To Verify the Internal error at setup wizard and setup loop with IE	To Verify the Internal error at setup wizard and setup loop with IE	Passed	
EWLCJ172S_SR_100	To Verify the Internal error at setup wizard and setup loop with Safari	To Verify the Internal error at setup wizard and setup loop with Safari	Passed	
EWLCJ172S_SR_101	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients Windows	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients Windows	Passed	

EWLCJ172S_SR_102	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients MAC	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients MAC	Passed	
EWLCJ172S_SR_103	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients Android	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients Android	Passed	
EWLCJ172S_SR_104	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients Apple Mobile	Verify 3800 Cisco Wave 2 APs for reloads unexpectedly by adding different clients Apple Mobile	Passed	
EWLCJ172S_SR_105	Verify Apple Client Joining fine with SSID on 9120 Ap's	Verify Apple Client Joining fine with SSID on 9120 Ap's	Passed	
EWLCJ172S_SR_106	Verify Apple Client Joining fine with SSID on 9130 Ap's	Verify Apple Client Joining fine with SSID on 9130 Ap's	Passed	
EWLCJ172S_SR_107	Verify the Client username details in API's with Window Client	Verify the Client username details in API's with Window Client	Passed	
EWLCJ172S_SR_108	Verify the Client username details in API's with MAC Client	Verify the Client username details in API's with MAC Client	Passed	
EWLCJ172S_SR_109	Verify the Client username details in API's with Android Client	Verify the Client username details in API's with Android Client	Passed	
EWLCJ172S_SR_110	Verify the Client username details in API's with Apple Mobile Client	Verify the Client username details in API's with Apple Mobile Client	Passed	
EWLCJ172S_SR_111	Verify eWLC is able to create the mgmt user successfully and able to login with it 9800-40	Verify eWLC is able to create the mgmt user successfully and able to login with it 9800-40	Passed	

EWLCJ172S_SR_112	Verify eWLC is able to create the mgmt user successfully and able to login with it 9800-80	Verify eWLC is able to create the mgmt user successfully and able to login with it 9800-80	Passed	
EWLCJ172S_SR_113	Verify eWLC is able to create the mgmt user successfully and able to login with it 9800-L	Verify eWLC is able to create the mgmt user successfully and able to login with it 9800-L	Passed	
EWLCJ172S_SR_114	Verify eWLC is able to create the mgmt user successfully and able to login with it ME1852	Verify eWLC is able to create the mgmt user successfully and able to login with it ME1852	Passed	
EWLCJ172S_SR_115	Verify eWLC is able to create the mgmt user successfully and able to login with it ME1832	Verify eWLC is able to create the mgmt user successfully and able to login with it ME1832	Passed	
EWLCJ172S_SR_116	Verify the logs are getting clean up after the upgrade of MSE	Verify the logs are getting clean up after the upgrade of MSE	Passed	
EWLCJ172S_SR_117	Verify the logs are getting clean up after the upgrade by connecting the Windows clients to it and sync	Verify the logs are getting clean up after the upgrade by connecting the different clients to it and sync	Passed	
EWLCJ172S_SR_118	Verify the logs are getting clean up after the upgrade by connecting the MAC clients to it and sync	Verify the logs are getting clean up after the upgrade by connecting the MAC clients to it and sync	Passed	
EWLCJ172S_SR_119	Verify the logs are getting clean up after the upgrade by connecting the Android clients to it and sync	Verify the logs are getting clean up after the upgrade by connecting the Android clients to it and sync	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
EWLCJ172S_config_1	Trustsec SGT Mapping deleted when configured with Multicast Address	To configure the multicast address in ewlc	Failed	CSCvt76816
EWLCJ172S_config_2	Unable to change consent with email to webconsent type in edit web auth parameter page	To verify web auth parameter after changing the consent with email to webconsent	Failed	CSCvt11264
EWCJ172S_config_2	DHCP pools - 'Reserved Only' Toggle button not working in Japanese UI	To verify Toggle button working in Japanese UI	Failed	CSCvt27577

CHAPTER 5

Related Documentation

Related Documentation

CME 8.10 Rlease Notes

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/810/release_notes/b_ME_RN_810.html

WLC 8.10 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810.html

CMX 10.6 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/getting_started_with_cisco_cmx.html

PI 3.8 User Guide

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure-3-8/model.html

ISE 2.7 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/release_notes/b_ise_27_RN.html

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.2 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/config-guide/b_wl_17_2_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.2 Release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/release-notes/rn-17-2-9800.html#id_133139