REVIEW DRAFT - CISCO CONFIDENTIAL

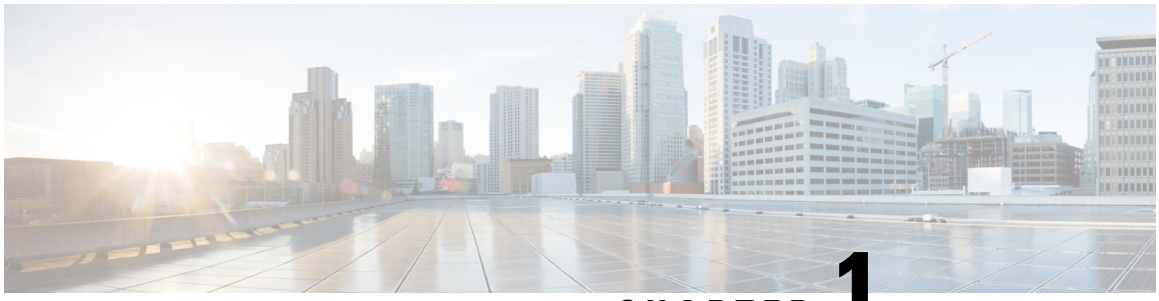
Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.3.2 for Japan (Release Version 17.3.2)

First Published: 2020-07-23

Last Modified: 2020-07-24

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



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 17.3
- 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

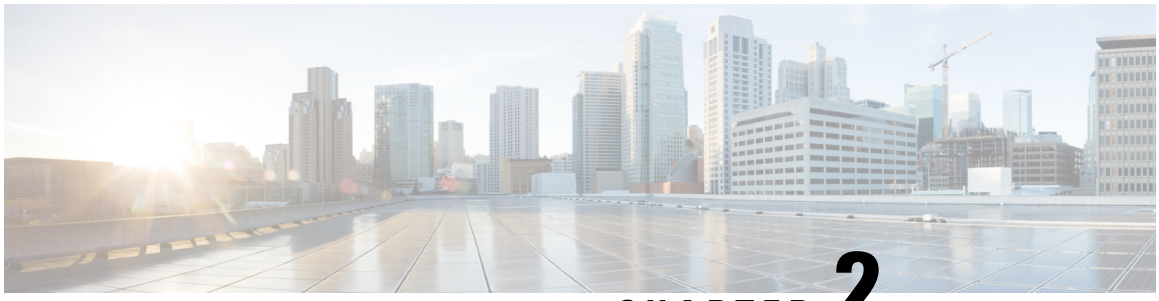
Acronyms

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 Center	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

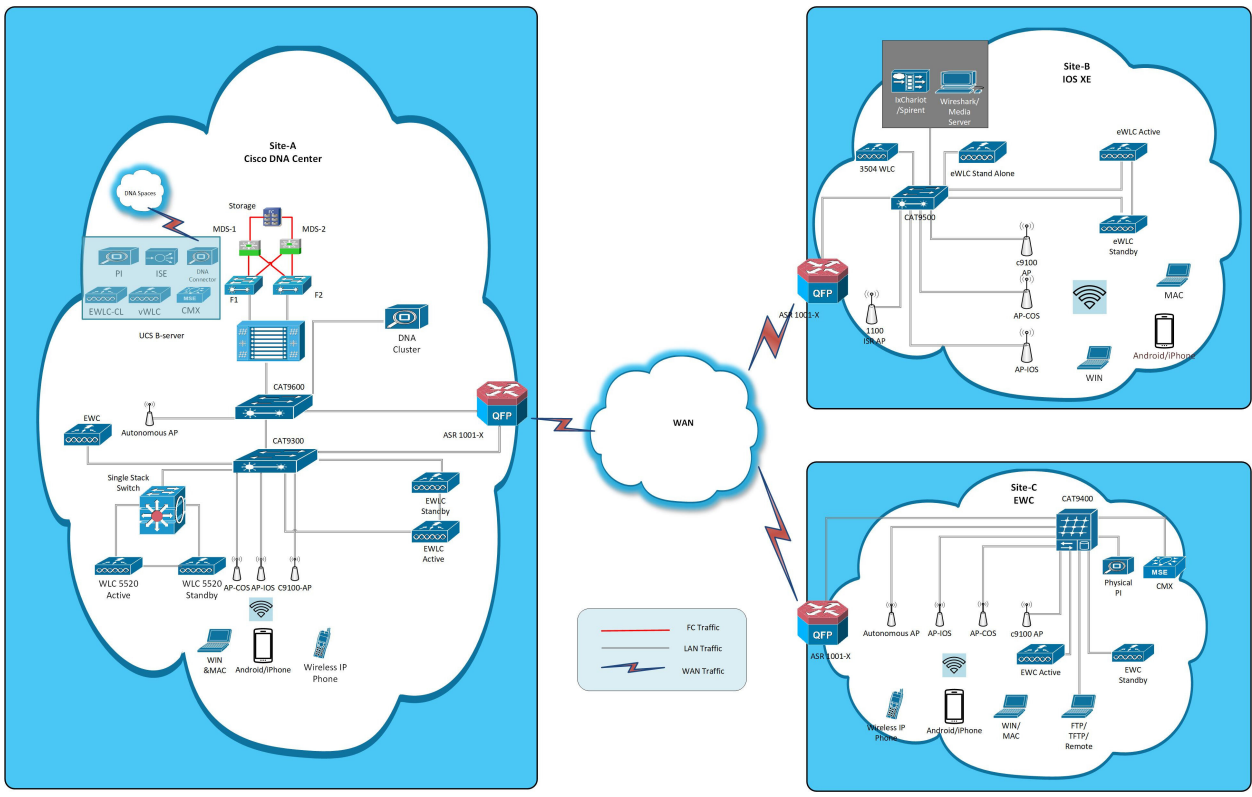
Acronym	Description
WPA	Wi-Fi Protected Access
WSM	Wireless Security Module



CHAPTER 2

Test Topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Cisco Elastic Wireless LAN Controller 9800	17.3
	Cisco Virtual Elastic Wireless LAN Controller 9800	17.3
	Cisco Catalyst 9800-L Wireless Controller	17.3
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.3
	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	2.1.2
	DNA Spaces	Cloud(June 2020)
	DNA spaces connector	2.2.295
	ISE(VM)	2.7
	CMX(Physical (3375), VM)	10.6
	Prime Infrastructure (Virtual Appliance, UCS based)	3.8.0.0.284
	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	17.3
	Cisco AP 9120	17.3
	Cisco AP 9130	17.3
	Cisco 1100 ISR	17.3
	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	17.3
	Cisco Cat 9200L	17.3
	Cisco Cat 9600	17.3
	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	7.9.1

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 13.5.1
	iPhone 6, 6S ,7 & 11 (JP Locale)	iOS 13.5.1
	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	78.0
	Safari	2.1.13
	Chrome	83.0

What's New ?

Cisco Catalyst 9800 Series Wireless Controller

- Tracking of appliance temperature in the System Information dashlet
- Software Upgrade page enhancement
- EWLC Better certificate management through UI
- HA SSO RMI
- Wireless Trap Control

- Client roaming across policy profile
- Rogue Enhancement
- Out of band access to standby
- OFDMA in Cisco Catalyst 9130 APs
- Client assoc/disassoc/reassoc syslogs
- Stand by Monitoring
- Dark Mode option

EWC

- Client Tracking with Locally Administered MAC Address
- Retain Client for 10sec after delete
- EWC Upgrade path
- 200 Country Code Support
- Intelligent Capture Support for C9130
- mDNS gateway support for flex/Mobility Express

Open Caveats

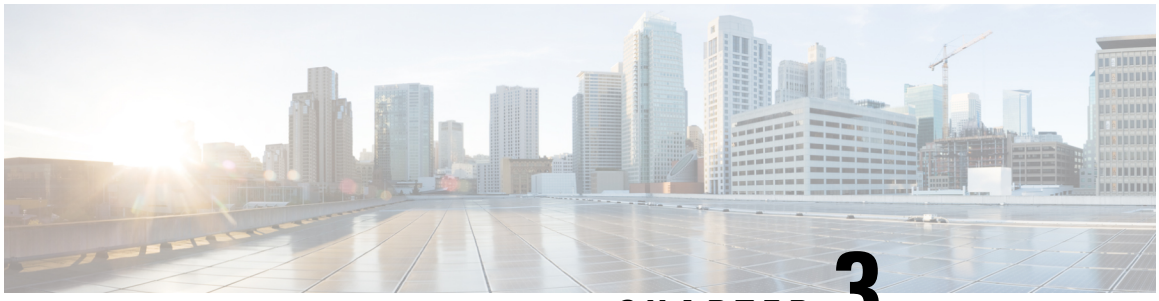
Defect ID	Title
CSCvu68395	Selecting the configuration file via HTTP, the cancel (X) mark not in proper line
CSCvu49340	Wpa3 security wlan able to has aes cipher but not used and client joining like open SSID
CSCvu49400	DNS server IP shown as invalid
CSCvu06348	WebUI: FTP/SFTP upgrade fails if the username/password contains special characters
CSCvu70630	Rogue rule created is overridden with with latest Priority
CSCvv04519	Show Password icon ovelaps password string
CSCvv06147	Cookie timeout: Automation Scripts fail due to session timeout more than an hour in EWC and EWLC
CSCvu80115	Tunnel interface '0' showing two times in EWLC CLI
CSCvu84821	Observed continues syslog message PLATFORM_SCC-1-AUTHENTICATION_FAIL Chassis authentication failed
CSCvu87707	Active CLI session for deleted local user - Aireos parity gap behaviour
CSCvu37780	Remove inactive files option is failing in 9800 eWLC UI but works in CLI
CSCvu61995	ISSU fails without proper error message

CSCvu99674	In eWLC,No close/exit option for guided assistance
CSCvu79875	Difficult to validate active client information
CSCvu95071	Able to configure more number of clients in coverage hole detection via CLI
CSCvu48139	17.3 Build allowing WLAN with WPA3-PSK security without WPA2. (Waiting on CSCvu49340)
CSCvv04861	Ap9120 Software page Middle container is over flowing outside
CSCvu17458	EWC upgrade via TFTP issue
CSCvu16286	9130 upgrade fails from 17.2.2 to 17.3 and error message is too generic
CSCvv01477	EWC - HTTP upgrade syslog popup issue
CSCvu64854	FTP download fails if the username/password contains special characters in EWLC
CSCvu59065	EWC Core dump generated due to core-pubd
CSCvu92121	EWCAP 9130 - Dual radio mode is enabled even when tri-radio is disabled
CSCvu78699	AP 9130 - Dual radio mode configuration is accepted without any error when tri-radio is disabled
CSCvv04385	Typo error in japanese local for WLANs option in Menu
CSCvv04773	Observed Kernel panic assert crash!"N_ENAB(wlc->pub)[CHSPEC_ISLE20(chanspec)]"failedfile"wlcc4121"
CSCvu87040	Driver Crash in 9120 AP after controller upgrade
CSCvu92874	Module Product ID shown empty for few AP
CSCvu27719	AP shown "UNKNOWN" tag until user explicitly writing tag is base line behavior

Resolved Caveats

Defect ID	Title
CSCvu96324	In eWLC, WLAN Count gets added for each update
CSCvu64857	Add WLAN popup - UI scrollbar issue
CSCvu89928	Editing the trustpoint attribute from other TP value to"none"could see the old attribute value in UI
CSCvu33143	After changing the trustpoint attribute to "none" in LocalEAP could see junk value in UI in JA

CSCvu51223	ISSU Auto-abort - MCL errror with No information on console during Downgrade
CSCvu76954	Client connected via 11ac or 11n, even when dot11 options are disabled
CSCvu22495	Temperature Tool tip is not working
CSCvu49452	eWLC UI not loading after enabling dark mode
CSCvu98293	9800 - Search results not accessible in collapsed menu panel
CSCvu48921	Not able to Configure VLAN configuration in EWC
CSCvv01262	EWC - Upgrade not working & shows empty dropdown for Japanese locale



CHAPTER 3

New Features

Tracking of appliance temperature in the System Information dashlet

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Temperature_01	Verify the Temperature details shows up under Device type on the "System Information" dashlet	To verify the Temperature details shows up under Device type on the "System Information" dashlet	Passed	

EWLCJ173S_Temperature_02	Verify Threshold information popup is shows when click on the Temperature info icon	To verify Threshold information pop up is shows when click on the Temperature info icon	Passed	
EWLCJ173S_Temperature_03	Verify Threshold information shows details of Minor,Major,Critical, shutdown	To verify Threshold information shows details of Minor,Major,Critical, shutdown	Passed	
EWLCJ173S_Temperature_04	Verify Temperature details shows in CLI and match in UI	To verify Temperature details shows in CLI and match in UI	Passed	
EWLCJ173S_Temperature_05	Verify Temperature details shows after image upgrade	To verify Temperature details shows after image upgrade	Passed	
EWLCJ173S_Temperature_06	Verify Temperature details shows after image downgrade	To verify Temperature details shows after image downgrade	Passed	
EWLCJ173S_Temperature_07	Verify Temperature details shows after multiple times controller reload	To verify Temperature details shows after multiple times controller reload	Passed	
EWLCJ173S_Temperature_08	Verify Temperature details shows after more than 5 devices Client connected to device	To verify Temperature details shows after more than 5 devices Client connected to device	Passed	
EWLCJ173S_Temperature_09	Verify Temperature details should not shows for Virtual device	To verify Temperature details should not shows for Virtual device	Passed	
EWLCJ173S_Temperature_10	Verify Temperature details shows after HA setup	To verify Temperature details shows after HA setup	Passed	

Software Upgrade page enhancement

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Upgrade_page_01	Verifying "My Desktop" option is default when loading software upgrade page	To verify "My Desktop" option is default when loading software upgrade page	Passed	
EWLCJ173S_Upgrade_page_02	Verifying the recommended Transport type order as "My Desktop, SFTP, FTP, TFTP, Device".	To verify the recommended Transport type order as "My Desktop, SFTP, FTP, TFTP, Device".	Passed	
EWLCJ173S_Upgrade_page_03	Verify user is able to upgrade using default option "My Desktop"	To Verify user is able to upgrade using default option "My Desktop"	Passed	
EWLCJ173S_Upgrade_page_04	Verify user is able to upgrade using option "SFTP"	To Verify user is able to upgrade using option "SFTP"	Passed	
EWLCJ173S_Upgrade_page_05	Verify user is able to upgrade using option "FTP"	To Verify user is able to upgrade using option "FTP"	Passed	
EWLCJ173S_Upgrade_page_06	Verify user is able to upgrade using option "TFTP"	To Verify user is able to upgrade using option "TFTP"	Passed	
EWLCJ173S_Upgrade_page_07	Verify user is able to upgrade using option "Device"	To Verify user is able to upgrade using option "Device"	Passed	
EWLCJ173S_Upgrade_page_08	Verify Image download should fail via TFTP when TFTP server stopped service while downloading	To verify Image download should fail via TFTP when TFTP server stopped service while downloading	Passed	

EWLCJ173S_Upgrade_page_09	Verify EWLC Image upgrade from DNAC	To verify EWLC Image upgrade from DNAC	Passed	
EWLCJ173S_Upgrade_page_10	Verify ISSU Upgrade (HA Upgrade) via default transport type	To verify ISSU Upgrade (HA Upgrade) via default transport type	Passed	
EWLCJ173S_Upgrade_page_11	Verify Enable hitless upgrade via FTP transport type	To verify Enable hitless upgrade via FTP transport type	Passed	

EWLC Better certificate management through UI

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Certificate_01	To configure the trust point certificate in Local EAP Page	To check weather trust point is added in Local EAP	Passed	
EWLCJ173S_Certificate_02	To configure the trust point certificate in Web Auth Page	To check weather trust point is added in Web Auth Page	Passed	
EWLCJ173S_Certificate_03	To configure the trust point certificate in Wireless Management Interface Page	To check weather trust point is added in Wireless Management Interface Page	Passed	
EWLCJ173S_Certificate_04	To configure the trust point certificate in Web admin Page	To check weather trust point is added in Web admin Page	Passed	
EWLCJ173S_Certificate_05	To Edit the trust point certificate in Local EAP Page	To check weather trust point can be editable in Local EAP Page	Passed	
EWLCJ173S_Certificate_06	To Edit the trust point certificate in Web Auth Page	To check weather trust point can be editable in Web Auth Page	Passed	

EWLCJ173S_Certificate_07	To Edit the trust point certificate in Wireless Management interface Page	To check weather trust point can be editable in Wireless management interface Page	Passed	
EWLCJ173S_Certificate_08	To Edit the trust point certificate in Web Admin Page	To check weather trust point can be editable in web admin Page	Passed	
EWLCJ173S_Certificate_09	Create the certificate from CLI and verify in GUI	To check able to create the certificate from CLI	Passed	
EWLCJ173S_Certificate_10	Create the certificate from GUI and verify in CLI	To check able to create the certificate from CLI	Passed	
EWLCJ173S_Certificate_11	Delete the generated certificate from GUI and CLI	To check able to delete the certificate	Passed	

HA SSO RMI

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_RMI_01	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	
EWLCJ173S_RMI_02	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ173S_RMI_03	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ173S_RMI_04	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ173S_RMI_05	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ173S_RMI_06	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	

EWLCJ173S_RMI_07	Enable gateway failover, verify output details and monitor devices for switchover.	To enable gateway failover, verify output details & monitor devices for switchover.	Passed	
EWLCJ173S_RMI_08	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	
EWLCJ173S_RMI_09	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ173S_RMI_10	Verify HA setup details in Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ173S_RMI_11	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ173S_RMI_12	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ173S_RMI_13	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	

Wireless_Trap_Control

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Trap_01	Verifying if the Wireless Trap option is shown in all the eWLC	To verify if the Wireless trap option is shown in all the flavours of the 9800 eWLC	Passed	
EWLCJ173S_Trap_02	Enabling the Wireless Trap option in eWLC UI and verifying the same in CLI	To enable the Wireless trap option in eWLC UI and verify the same in CLI	Passed	
EWLCJ173S_Trap_03	Enabling the Wireless Trap option in eWLC CLI and verifying the same in UI	To enable the Wireless trap option in eWLC CLI and verify the same in UI	Passed	

EWLCJ173S_Trap_04	Check if the Wireless traps enabled in eWLC UI remains the same after reloading the controller	To check if the Wireless trap are enabled in eWLC UI after reloading the controller .	Passed	
EWLCJ173S_Trap_05	Check if the Wireless traps enabled in eWLC UI remains the same after Upgrading the controller	To Upgrade the eWLC and check if the Wireless trap are enabled in eWLC UI are same as before upgrading	Passed	
EWLCJ173S_Trap_06	Backup and restore confi file and check if the Wireless trap option configured are same before and after backup restore	To restore the backup config file in which Wireless trap is enabled in UI and check if the restored config file has the same confi as before	Passed	
EWLCJ173S_Trap_07	Enabling Wireless Trap related to AP and validating the same if traps are shown .	To enable Wireless trap related to AP in eWLC UI and validating the trap message in trap receiver	Passed	
EWLCJ173S_Trap_08	Configuring Wireless Trap related to Wireless Client and validating the same if traps are shown .	To configure Wireless trap related to Wireless Clients in eWLC UI and validating the trap message in trap receiver	Passed	
EWLCJ173S_Trap_09	Enabling Wireless Trap related to RF and validating the same if traps in are shown in trap receiver.	To enable Wireless trap related to RF in eWLC UI and validating the trap message in trap receiver	Passed	
EWLCJ173S_Trap_10	Configuring Wireless Trap related to Security and validating the same if traps are shown .	To enable Wireless trap related to Security in eWLC UI and validating the trap message in trap receiver	Passed	

EWLCJ173S_Trap_11	Configuring Wireless Trap related to Rogue and validating the same if traps are shown .	To enable Wireless trap related to Rogue in eWLC UI and validating the trap message in trap receiver	Passed	
EWLCJ173S_Trap_12	Configuring Wireless Trap related to general Controller and validating the same if traps are shown .	To enable Wireless trap related to general Controller in eWLC UI and validating the trap message in trap receiver	Passed	

Client Roaming Across Policy Profile

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Roam_policy_01	Perform roaming with same vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_02	Perform roaming with different vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_03	Roams the client to aaa override vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_04	Roams the client from aaa override vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_05	Perform roaming for wpa2 client with different vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_06	Perform roaming for wpa3 client with different vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	

EWLCJ173S_Roam_policy_07	Perform roaming for open authentication client with different vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_08	Perform roaming for dot1x+FT client with different vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_09	Roam the client with different vlan flex central	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_10	Roam the client with aaa override vlan to vlan flex central	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_11	Roam the client with multiple Vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_12	Roam the client between flex to local mode vlan	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_13	Roam the client with central association	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	
EWLCJ173S_Roam_policy_14	Roam the client with central authentication	Verifying the vlan details after roaming vlan v1 will applied or not	Passed	

Rogue Enhancement

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Rogue_Enhance_01	Enabling Rogue detection on eWLC	To enable rogue detection on eWLC and check if the rogue detection is enabled on eWLC	Passed	

EWLCJ173S_Rogue_Enhance_02	Check if the rogue detection works on the 9115 AP connected in eWLC	To check if the rogue AP and clients are detected by 9115 AP connected in eWLC	Passed	
EWLCJ173S_Rogue_Enhance_03	Check if the rogue detection works on the 9120 AP connected in eWLC	To check if the rogue AP and clients are detected by 9120 AP connected in eWLC	Passed	
EWLCJ173S_Rogue_Enhance_04	Check if the rogue detection works on the 9130 AP connected in eWLC	To check if the rogue AP and clients are detected by 9130AP connected in eWLC	Passed	
EWLCJ173S_Rogue_Enhance_05	Check if the rogue detection works on the 4800 AP connected in eWLC	To check if the rogue AP and clients are detected by 4800 AP connected in eWLC	Passed	
EWLCJ173S_Rogue_Enhance_06	Detection of the rogue using 9115 in Local mode	To detect the rogue using 9115 in local mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_07	Detection of the rogue using 9115 in Flex mode	To detect the rogue using 9115 in Flex mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_08	Detection of the rogue using 9120 in Local mode	To detect the rogue using 9120 in local mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_09	Detection of the rogue using 9120 in Flex mode	To detect the rogue using 9120 in Flex mode and check the details of the rogue	Passed	

EWLCJ173S_Rogue_Enhance_10	Detection of the rogue using 9130 in Local mode	To detect the rogue using 9130 in local mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_11	Detection of the rogue using 9130 in Flex mode	To detect the rogue using 9130 in Flex mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_12	Detection of the rogue using 4800 in Local mode	To detect the rogue using 4800 in local mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_13	Detection of the rogue using 4800 in Flex mode	To detect the rogue using 4800 in Flex mode and check the details of the rogue	Passed	
EWLCJ173S_Rogue_Enhance_14	Configuring Rogue Detection Security Level to low and classifying the rogue detected	To configure rogue detection security level to low to detect the rogue and check if the rogue can be manually classified	Failed	CSCvu49400
EWLCJ173S_Rogue_Enhance_15	Configuring Rogue Detection Security Level to High and classifying the rogue detected	To configure rogue detection security level to high to detect the rogue and check if the rogue can be manually classified	Passed	
EWLCJ173S_Rogue_Enhance_16	Configuring Rogue Detection Security Level to critical and classifying the rogue detected	To configure rogue detection security level to critical to detect the rogue and check if the rogue can be manually classified	Passed	

EWLCJ173S_Rogue_Enhance_17	Detecting rogue using Global MFP with rogue detection security	To detect the rogue using Global MFP with rogue detection security	Passed	
EWLCJ173S_Rogue_Enhance_18	Manual containment of the rogue using AP in Local mode	To manually contain the rogue using the AP in Local mode	Passed	
EWLCJ173S_Rogue_Enhance_19	Manual containment of the rogue using AP in Flex mode	To manually contain the rogue using the AP in Flex mode	Passed	
EWLCJ173S_Rogue_Enhance_20	Manual containment of the rogue using AP in Monitor mode	To manually contain the rogue using the AP in Monitor mode	Passed	
EWLCJ173S_Rogue_Enhance_21	Auto contain of rogue using custom rogue security with Catalyst AP	To auto contain rogue using the custom rogue security with Catalyst AP	Passed	
EWLCJ173S_Rogue_Enhance_22	Auto contain of rogue using custom rogue security with COS AP	To auto contain rogue using the custom rogue security with COS AP	Passed	
EWLCJ173S_Rogue_Enhance_23	Creating a rouge AP policies to classify the rogue	To create a rogue Ap policies to classify the rogues bases on the type configured	Failed	CSCvu70630
EWLCJ173S_Rogue_Enhance_24	Enabling RLDP and scheduling RLDP	To enable RLDP and scheduling RLDP and check if the RLDP works as per scheduling	Passed	

Out of band access to standby

Logical ID	Title	Description	Status	Defect ID

EWLCJ173S_Out_of_band_1	Configure HA SSO RMI & validate Standby Environmental Comments	To validate Standby Environmental Comments	Passed	
EWLCJ173S_Out_of_band_2	Configure HA SSO RMI & validate Standby process Comments	To validate Standby process Comments	Passed	
EWLCJ173S_Out_of_band_3	Configure HA SSO RMI & validate Standby debugging Comments	To validate Standby debugging Comments	Passed	
EWLCJ173S_Out_of_band_4	Configure HA SSO RMI & validate Standby memory Comments	To validate Standby memory Comments	Passed	
EWLCJ173S_Out_of_band_5	Configure HA SSO RMI & validate Standby File System Comments	To validate Standby File System Comments	Passed	
EWLCJ173S_Out_of_band_6	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	
EWLCJ173S_Out_of_band_7	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ173S_Out_of_band_8	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ173S_Out_of_band_9	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ173S_Out_of_band_10	Check process usage details in standby console	To check process usage details in standby console	Passed	

OFDMA in Cisco Catalyst 9130 APs

Logical ID	Title	Description	Status	Defect ID

EWLCJ173S_OFDMA_SUPPORT_1	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ173S_OFDMA_SUPPORT_2	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWLCJ173S_OFDMA_SUPPORT_3	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ173S_OFDMA_SUPPORT_4	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ173S_OFDMA_SUPPORT_5	Verifying details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ173S_OFDMA_SUPPORT_6	Verifying details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ173S_OFDMA_SUPPORT_7	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ173S_OFDMA_SUPPORT_8	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	

EWLCJ173S_OFDMA_SUPPORT_9	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	
EWLCJ173S_OFDMA_SUPPORT_10	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWLCJ173S_OFDMA_SUPPORT_11	Check OFDMA support for AP configured in Flex+Mesh mode.	To check OFDMA support for AP configured in Flex+Mesh mode.	Passed	
EWLCJ173S_OFDMA_SUPPORT_12	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ173S_OFDMA_SUPPORT_13	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ173S_OFDMA_SUPPORT_14	Connect up to 8 clients and monitor DL/UL OFDMA statistics	To connect up to 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ173S_OFDMA_SUPPORT_15	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	

EWLCJ173S_OFDMA_SUPPORT_16	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWLCJ173S_OFDMA_SUPPORT_17	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWLCJ173S_OFDMA_SUPPORT_18	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWLCJ173S_OFDMA_SUPPORT_19	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWLCJ173S_OFDMA_SUPPORT_20	Modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	To modify MCS data rates & monitor OFDMA stats with 11ax Android client connected.	Passed	
EWLCJ173S_OFDMA_SUPPORT_21	Check OFDMA stats with roaming client scenario	Check OFDMA stats with roaming client scenario	Passed	

Client assoc/disassoc/reassoc syslogs

Logical ID	Title	Description	Status	Defect ID

EWLCJ173S_Client_Syslog_01	Observing Syslog for open authentication client association	Validating the syslog observed or not after client moved to run state while it associate with open authentication	Passed	
EWLCJ173S_Client_Syslog_02	Observing Syslog for dot1x client association	Validating the syslog observed or not after client moved to run state while it associate with dot1x security	Passed	
EWLCJ173S_Client_Syslog_03	Observing Syslog for Wpa2 client association	Validating the syslog after client moved to run state while it associate with WPA2 security	Passed	
EWLCJ173S_Client_Syslog_04	Observing Syslog for WPA3 client association	Validating the syslog after client moved to run state while it associate with WPA3 security	Passed	
EWLCJ173S_Client_Syslog_05	Observing Syslog for open authentication client deletion	Validating the syslog after client deauthentication	Failed	CSCvu84821
EWLCJ173S_Client_Syslog_06	Observing Syslog for dot1x client deletion	Validating the syslog after client deauthentication	Passed	
EWLCJ173S_Client_Syslog_07	Observing Syslog for WPA2 client deletion	Validating the syslog after client deauthentication	Passed	
EWLCJ173S_Client_Syslog_08	Observing Syslog for WPA3 client deletion	Validating the syslog after client deauthentication	Passed	
EWLCJ173S_Client_Syslog_09	Observing Syslog for client reassociation	Validating the syslog while client re-association	Passed	
EWLCJ173S_Client_Syslog_10	Get client syslog for assoc & deauth & reassoc	Validating the syslog and verifying the details	Passed	

EWLCJ173S_Client_Syslog_11	Observe syslog while client getting ip	Validate the syslog for client getting ip from controller or not	Passed	
EWLCJ173S_Client_Syslog_12	Get syslog after performing reload	Verifying the syslog while controller reload	Passed	
EWLCJ173S_Client_Syslog_13	Get Syslog for Rouge client	Validated the syslog for rouge client	Passed	
EWLCJ173S_Client_Syslog_14	Get Syslog for sleeping client	Validated the syslog for Sleeping client	Passed	
EWLCJ173S_Client_Syslog_15	Verifying the syslog details shown in syslog server	Check the syslog details are shown in syslog server or not	Passed	
EWLCJ173S_Client_Syslog_16	Observing syslog for inter roaming	Validating the syslog while client roam between two controllers	Passed	
EWLCJ173S_Client_Syslog_17	Observing syslog for intra roaming	Validating the syslog while client roam between two Ap's connected in same controller	Passed	
EWLCJ173S_Client_Syslog_18	Observing syslog for IRCM client	Validated the syslog for Sleeping client	Passed	
EWLCJ173S_Client_Syslog_19	Observing syslog for Mab client	Validated the syslog for MAB client	Passed	
EWLCJ173S_Client_Syslog_20	Verifying the syslog details after disabling the syslog	Validating the syslog shown or not after disabling the command	Passed	

Stand by Monitoring

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Monitor_01	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	

EWLCJ173S_Monitor_02	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ173S_Monitor_03	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ173S_Monitor_04	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ173S_Monitor_05	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ173S_Monitor_06	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ173S_Monitor_07	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	

Dark Mode option

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Dark_Mode_01	Enabling dark mode in eWLC and validating the dashboard Page	To enable dark mode in eWLC UI and check if the dark mode applied in dashboard page	Passed	
EWLCJ173S_Dark_Mode_02	Validating dark mode in eWLC Monitor > General Page	To check if the dark mode is shown in the Monitor > General page	Passed	
EWLCJ173S_Dark_Mode_03	Checking the dark mode in Monitor > Security Page	To check if the dark mode is shown in the Monitor > General page	Passed	

EWLCJ173S_Dark_Mode_04	Checking the dark mode in Monitor > Services Page	To check if the dark mode is shown in the Monitor > Services page	Passed	
EWLCJ173S_Dark_Mode_05	Checking the dark mode in Monitor > Wireless Page	To check if the dark mode is shown in the Monitor > Wireless page	Passed	
EWLCJ173S_Dark_Mode_06	Validating dark mode in eWLC Configuration > Interface Page	To check if the dark mode is shown in the Configuration > Interface Page	Passed	
EWLCJ173S_Dark_Mode_07	Checking dark mode in eWLC Configuration > Layer 2	To check if the dark mode is shown in the Configuration > Layer 2 Page	Passed	
EWLCJ173S_Dark_Mode_08	Checking dark mode in eWLC Configuration > Radio Configuration	To check if the dark mode is shown in the Configuration > Radio Configuration	Passed	
EWLCJ173S_Dark_Mode_09	Checking dark mode in eWLC Configuration > Routing Protocols	To check if the dark mode is shown in the Configuration > Routing protocols	Passed	
EWLCJ173S_Dark_Mode_10	Checking dark mode in eWLC Configuration > Security	To check if the dark mode is shown in the Configuration > Security	Passed	
EWLCJ173S_Dark_Mode_11	Checking dark mode in eWLC Configuration > Services	To check if the dark mode is shown in the Configuration > Services	Passed	
EWLCJ173S_Dark_Mode_12	Checking dark mode in eWLC Configuration > Tags and profiles	To check if the dark mode is shown in the Configuration > tags and profiles	Passed	

EWLCJ173S_Dark_Mode_13	Checking dark mode in eWLC Configuration > Wireless	To check if the dark mode is shown in the Configuration > Wireless	Passed	
EWLCJ173S_Dark_Mode_14	Checking dark mode in eWLC Configuration > Wireless Setup	To check if the dark mode is shown in the Configuration > Wireless Setup	Passed	
EWLCJ173S_Dark_Mode_15	Checking dark mode in eWLC Administration > Best practices	To check if the dark mode is shown in the Administration > Best practices	Passed	
EWLCJ173S_Dark_Mode_16	Checking dark mode in eWLC Administration > Command Line Interface	To check if the dark mode is shown in the Administration > Command Line Interface	Passed	
EWLCJ173S_Dark_Mode_17	Checking dark mode in eWLC Administration > device	To check if the dark mode is shown in the Administration > Device	Passed	
EWLCJ173S_Dark_Mode_18	Checking dark mode in eWLC Administration > DHCP Pools	To check if the dark mode is shown in the Administration > DHCP pools	Passed	
EWLCJ173S_Dark_Mode_19	Checking dark mode in eWLC Administration > DNS	To check if the dark mode is shown in the Administration > DNS	Passed	
EWLCJ173S_Dark_Mode_20	Checking dark mode in eWLC Administration > Management	To check if the dark mode is shown in the Administration > Management	Passed	
EWLCJ173S_Dark_Mode_21	Checking dark mode in eWLC Administration > Reload	To check if the dark mode is shown in the Administration > Reload	Passed	

EWLCJ173S_Dark_Mode_22	Checking dark mode in eWLC Administration > Smart Call Home	To check if the dark mode is shown in the Administration > Smart Call Home	Passed	
EWLCJ173S_Dark_Mode_23	Checking dark mode in eWLC Administration > Software Management	To check if the dark mode is shown in the Administration > Software management	Passed	
EWLCJ173S_Dark_Mode_24	Checking dark mode in eWLC Administration > Time	To check if the dark mode is shown in the Administration > Time	Passed	
EWLCJ173S_Dark_Mode_25	Checking dark mode in eWLC Administration > User Administration	To check if the dark mode is shown in the Administration > User Administration	Passed	
EWLCJ173S_Dark_Mode_26	Enabling dark mode in eWLC and validating the Licence Page	To enable dark mode in eWLC UI and check if the dark mode applied in Licence page	Passed	
EWLCJ173S_Dark_Mode_27	Validating dark mode in eWLC Troubleshooting > Logs Page	To validate if the dark mode is shown in the Troubleshooting > Logs Page	Passed	
EWLCJ173S_Dark_Mode_28	Validating dark mode in eWLC Troubleshooting > Core Dump and System Report page	To validate if the dark mode is shown in the Troubleshooting > Core Dump and System Report Page	Passed	
EWLCJ173S_Dark_Mode_29	Validating dark mode in eWLC Troubleshooting > Debug Bundle Page	To validate if the dark mode is shown in the Troubleshooting > Debug Bundle Page	Passed	

EWLCJ173S_Dark_Mode_30	Validating dark mode in eWLC Troubleshooting > Packet Capture Page	To validate if the dark mode is shown in the Troubleshooting > Packet Capture Page	Passed	
EWLCJ173S_Dark_Mode_31	Validating dark mode in eWLC Troubleshooting > Ping and Traceroute Page	To validate if the dark mode is shown in the Troubleshooting > Ping and Traceroute Page	Passed	
EWLCJ173S_Dark_Mode_32	Validating dark mode in eWLC Troubleshooting > AP Packet Capture Page	To validate if the dark mode is shown in the Troubleshooting > AP Packet Capture Page	Passed	
EWLCJ173S_Dark_Mode_33	Validating dark mode in eWLC Troubleshooting > Radioactive Trace Page	To validate if the dark mode is shown in the Troubleshooting > Radioactive Trace Page	Passed	

Intelligent Capture Support for C9130

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_ICAP for C9130_01	Packet capture of client when the client is connected to 9130 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 EWC	Failed	CSCvu93108
EWCJ173S_ICAP for C9130_02	Packet capture of client when the client is connected to 9130 AP with 5 GHz	To capture the Packet of the client when the client is connected to AP with radio as 5 GHz in EWC	Failed	CSCvu93108
EWCJ173S_ICAP for C9130_03	Packet capture for Android client using Intelligent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Failed	CSCvu93108

mDNS gateway support for flex/Mobility Express

Logical Id	Title	Description	Status	Defect ID
EWCJ173S_mDNS Gateway_01	Checking the mDNS Ap with Flex connect group configuration.	To check whether mDNS AP with Flex connect group configurations are able to configure or not.	Passed	
EWCJ173S_mDNS Gateway_02	Creating mDNS profile by adding required services	To verify whether mDNS profile is created with required services	Passed	
EWCJ173S_mDNS Gateway_03	Checking mDNS gateway are applying to Apple Tv clients after enabling the mdns AP to 9115AP	To check whether the mdns gateway applying to Apple Tv clients or not after enabling the mDNS-ap to 9115AP.	Passed	
EWCJ173S_mDNS Gateway_04	Checking mDNS gateway are applying to Mac OS clients after enabling the mdns AP to 9120AP	To check whether the mdns gateway applying to Mac OS and Apple Tv clients after enabling the mDNS-ap to 9120AP	Passed	
EWCJ173S_mDNS Gateway_05	Checking mDNS gateway are applied to Apple TV and authentication server as radius in ME	To verify mDNS gateway are applied to Apple TV and authentication server as radius in ME.	Passed	
EWCJ173S_mDNS Gateway_06	Checking mDNS gateway are applying to Mac OS and Apple Tv clients after enabling the mdns AP to 4800AP	To check whether the mdns gateway applying to Mac OS and Apple Tv clients or not after enabling the mDNS-ap to 4800AP.	Passed	
EWCJ173S_mDNS Gateway_07	Verifying the mDNS gateway configurations after changing the AP mode to monitor from flex	To check whether mDNS gateway configurations after changing the AP mode to Monitor from flex	Passed	
EWCJ173S_mDNS Gateway_08	Checking mDNS gateway are applying to Apple iPad and Apple chrome cast clients with Static WEP security after enabling the mdns AP to 9130/9115/4800/9120/3700AP's	To check whether the mdns gateway are applying to Apple iPad and Apple chrome cast clients with Static WEP security or not after enabling the mDNS-ap to9130/9115/4800/9120/3700AP's.	Passed	

EWCJ173S_mDNS Gateway_09	Checking mDNS gateway are applied to MAC OS with wlan open security	Verifying mDNS gateway are applied to Mac OS with open ssid	Passed	
EWCJ173S_mDNS Gateway_10	Checking mDNS gateway are applied to MacOS and IOS with wlan WPA2 personal security	Verifying mDNS gateway are applied to MacOS and IOS with WPA2 personal security	Passed	
EWCJ173S_mDNS Gateway_11	Checking mDNS gateway are applied to MacOS and IOS with wlan WPA3-SAE security	To Check mDNS gateway are applied to MacOS and IOS with WPA3-SAE security	Passed	
EWCJ173S_mDNS Gateway_12	Checking mDNS gateway are applied to Apple Devices with Fast transition enabled	To Check mDNS gateway are applied to Apple Devices with fast transition enabled	Passed	
EWCJ173S_mDNS Gateway_13	Performing client communication between two clients connected two different vlan	To Check whether client communicate between two clients connected to different vlan	Passed	
EWCJ173S_mDNS Gateway_14	Performing roaming operation when mDNS is applied	To Check the roaming operation when mDNS is applied	Passed	
EWCJ173S_mDNS Gateway_15	Checking mDNS config after exporting config file	To check whether the mDNS config is same after exporting config file	Passed	
EWCJ173S_mDNS Gateway_16	Checking mDNS gateway are applied to IOS with wlan Static WEP security	To verify whether mDNS gateway are applied to IOS with Static WEP SSID	Passed	
EWCJ173S_mDNS Gateway_17	Verifying the mDNS configuration in DNAC	To Verify the mDNS gateway configuration in DNAC	Passed	
EWCJ173S_mDNS Gateway_18	Verifying mDNS configuration Via EWC CLI	To verify the mDNS configuration through EWC CLI	Passed	

Client Tracking with Locally Administered MAC Address

Logical Id	Title	Description	Status	Defect ID

EWCJ173ST_Client Tracking_01	Creating local policy for Android clients and tracking the client mac type	To verify the mac address type for Android clients	Passed	
EWCJ173ST_Client Tracking_02	Creating local policy for Mac clients and tracking the client mac type	To verify the mac address type for Mac clients	Passed	
EWCJ173ST_Client Tracking_03	Creating local policy for IOS clients and tracking the client mac type	To verify the mac address type for IOS clients	Passed	
EWCJ173ST_Client Tracking_04	Creating local policy for Apple clients and tracking the client mac type	To Verify the mac address type for Apple client	Failed	CSCvu87040
EWCJ173ST_Client Tracking_05	Tracking the client mac address with different AP modes	To validate the client mac type for different AP modes	Passed	
EWCJ173ST_Client Tracking_06	Creating the local policy for sleeping client & Validate the Mac type	To validate the client mac type for sleeping client	Passed	
EWCJ173ST_Client Tracking_07	Creating the local policy for rogue client & Validate the Mac type	To check the mac type for Rogue clients	Passed	
EWCJ173ST_Client Tracking_08	Tracking the client mac type for roaming clients	To Check the mac type for roaming clients	Passed	
EWCJ173ST_Client Tracking_09	Creating local policy -device type as Android & try to connect IOS client	To Check whether the IOS client able to connect or not	Passed	
EWCJ173ST_Client Tracking_10	Creating Local policy-mac address not-eq to Android client	To Check whether the Android client able to connect or not	Passed	
EWCJ173ST_Client Tracking_11	Creating Local policy-mac address eq to Apple client	To Check whether the Apple client able to connect or not	Passed	
EWCJ173ST_Client Tracking_12	Creating local policy -device type as not equal to intel device	To Check whether the intel client able to connect or not	Failed	CSCvu95071

EWCJ173ST_Client Tracking_13	Tracking the client mac type in syslog server	To verify whether the client mac type showing in Syslog server or not	Passed	
EWCJ173ST_Client Tracking_14	Tracking the client mac type after AP reboot	To validate the client mac type after Ap reboot	Passed	
EWCJ173ST_Client Tracking_15	Creating local policy for Samsung S10 with sensor mode AP & Tracking the client mac type	To check the mac address type for S10	Passed	
EWCJ173ST_Client Tracking_16	Tracking client mac address type when client mac not Mapping any local polices in WLAN	To Track the client mac type when client mac not mapping any local polices in WLAN	Passed	

Retain Client for 10sec after delete

Logical ID	Title	Description	Status	Defect ID
EWCJ173ST_Retain Client_01	Creating WLAN with different security & Checking the retain client status for each security	To verify the retain Client status for each security	Passed	
EWCJ173ST_Retain Client_02	Checking the retain clients status for different type of clients	To verify the retaining client status for different clients	Passed	
EWCJ173ST_Retain Client_03	Verifying the retain client status by editing the WLAN	To verify whether retaining client status showing for 10 sec after editing WLAN	Failed	CSCvv04773
EWCJ173ST_Retain Client_04	Checking the retain client status for 2.4/5 Ghz or both radio	To check whether the retaining client status showing for 2.4/5 Ghz or both radio	Passed	
EWCJ173ST_Retain Client_05	Verifying the retain client status for different AP models	To Verify the retain client status for different AP models	Passed	

EWCJ173ST_Retain Client_06	Checking the client status after disjoin the AP	To check the retaining client status showing for 10 sec after disjoin the AP	Failed	CSCvu79875
EWCJ173ST_Retain Client_07	Verifying the retain client status by deleting the BSSID	To Verify the retaining client status showing for 10 sec after Deleting BSSID	Passed	
EWCJ173ST_Retain Client_08	Checking the retain client status by changing the AP Modes	To Check the retain client status by changing AP modes	Passed	
EWCJ173ST_Retain Client_09	Verifying the retain client status for intra roaming client	To Verify the retain client status after client roaming between AP's	Passed	
EWCJ173ST_Retain Client_10	Checking the retain client status for inter roaming client	To Verify the retain client status after client roaming between controllers	Passed	
EWCJ173ST_Retain Client_11	Verifying the retain client status for sleeping client	To verify the retain client status for Sleeping client	Passed	
EWCJ173ST_Retain Client_12	Verifying the Retain client status shown in syslog server	To Check the Retain client status shown in syslog server or not	Passed	
EWCJ173ST_Retain Client_13	Creating WLAN with WPA3+WPA2 security & Checking the retain client status	To Check the retain client status for Mixed mode security	Passed	
EWCJ173ST_Retain Client_14	Verifying the retain client status by changing the policy profile	To validate the retain client status after changing the policy profile	Failed	CSCvu64854
EWCJ173ST_Retain Client_15	Verifying the retain client status after deleting the client	To verify the retain client status for deleted client	Passed	
EWCJ173ST_Retain Client_16	Validating the Retain client status for Rouge client	Validated the retain client details for rouge client	Passed	

EWCJ173ST_Retain Client_17	Verifying the retain client status by changing the security type	To check the retain client status after changing the security type	Passed	
EWCJ173ST_Retain Client_18	Verifying the retain client status after 2.4/5 ghz radio down	To verify the retain client status after 2.4/5 ghz radio down	Passed	
EWCJ173ST_Retain Client_19	Verifying the retain client status by changing the AP ip Address	To validate the retain client status by changing the AP ip Address	Passed	
EWCJ173ST_Retain Client_20	Verifying the retain client status by changing the Channel Throughput	To verify the retain client status while changing the channel width	Passed	
EWCJ173ST_Retain Client_21	Verifying the retain client status by upgrading the AP Using MFG image	To validate the retain client status by upgrading the AP using MFG image	Passed	
EWCJ173ST_Retain Client_22	Validating the Retain client status for Virtual EWLC	To validate the retain client status for vEWLC	Passed	

EWC Upgrade path

Logical ID	Title	Description	Status	Defect ID
EWCJ173ST_Upgrade Patch_01	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the CCO option in UI with 9120 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the CCO option in UI with 9120 AP.	Passed	
EWCJ173ST_Upgrade Patch_02	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the command line interface option with 9120 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the command line interface option with 9120 AP.	Passed	

EWCJ173ST_UpgradePatch_03	upgrading path from 17.1 Desktop(Local) > 17.2 CCO and then 17.3 Latest Images by using the Desktop(Local) option in UI with 9120 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the Desktop(Local) option in UI with 9120 AP.	Passed	
EWCJ173ST_UpgradePatch_04	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9120 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9120 AP.	Passed	
EWCJ173ST_UpgradePatch_05	upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Latest Images by using the CCO option in UI.	To Verify the upgrading path from 17.3 Latest > 17.2 CCO and then 17.1 CCO Latest Images by using the CCO option in UI.	Passed	
EWCJ173ST_UpgradePatch_06	upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the command line interface option with 9120 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the command line interface option with 9120 AP.	Passed	
EWCJ173ST_UpgradePatch_07	upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with 9120 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with 9120 AP.	Passed	

EWCJ173ST_Upgrade Patch_08	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9120 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9120 AP.	Failed	CSCvu17458
EWCJ173ST_Upgrade Patch_09	upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Mozilla Firefox Browser with 9120 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Mozilla Firefox Browser with 9120 AP.	Passed	
EWCJ173ST_Upgrade Patch_10	Upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Chrome Browser with 9120 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Chrome Browser with 9120 AP.	Passed	
EWCJ173ST_Upgrade Patch_11	Upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with IE Browser with 9120 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with IE Browser with 9120 AP.	Passed	

EWCJ173ST_Upgrade Patch_12	Upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the CCO option in UI with 9130 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the CCO option in UI with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_13	Upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the command line interface option with 9130 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the command line interface option with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_14	Upgrading path from 17.1 Desktop(Local) > 17.2 CCO and then 17.3 Latest Images by using the Desktop(Local) option in UI with 9130 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the Desktop(Local) option in UI with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_15	Upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9130 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_16	Downgrading with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Latest Images by using the CCO option in UI.	To Verify the upgrading path from 17.3 Latest > 17.2 CCO and then 17.1 CCO Latest Images by using the CCO option in UI.	Failed	CSCvv01477

EWCJ173ST_Upgrade Patch_17	Downgrading with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the command line interface option with 9130 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the command line interface option with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_18	Downgrading with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with 9130 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_19	Upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9130 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9130 AP.	Passed	
EWCJ173ST_Upgrade Patch_20	Upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Mozilla Firefox Browser with 9130 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Mozilla Firefox Browser with 9130 AP.	Passed	

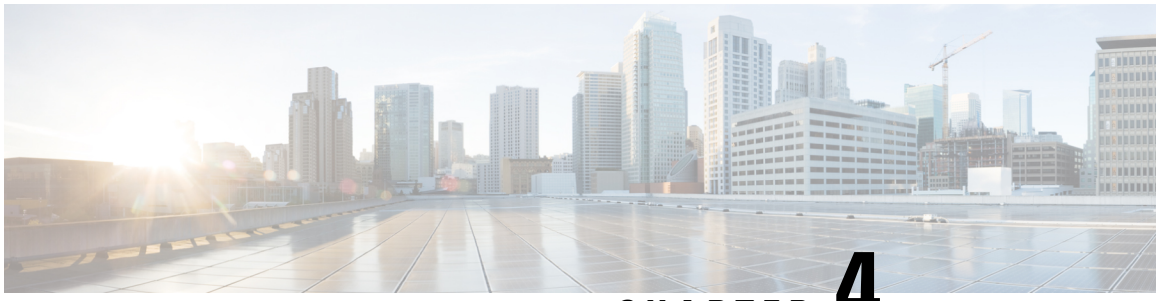
EWCJ173ST_UpgradePatch_21	Upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Chrome Browser with 9130 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with Chrome Browser with 9130 AP.	Passed	
EWCJ173ST_UpgradePatch_22	Upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with IE Browser with 9130 AP.	To Verify the upgrading path with downgrading the images from Latest 17.3 build > 17.2 CCO and then 17.1 Images by using the Desktop(Local) option in UI with IE Browser with 9130 AP.	Passed	
EWCJ173St_UpgradePatch_23	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the CCO option in UI with 9115 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the CCO option in UI with 9115 AP.	Passed	
EWCJ173ST_UpgradePatch_24	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the command line interface option with 9115 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the command line interface option with 9115 AP.	Passed	
EWCJ173ST_UpgradePatch_25	upgrading path from 17.1 Desktop(Local) > 17.2 CCO and then 17.3 Latest Images by using the Desktop(Local) option in UI with 9115 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the Desktop(Local) option in UI with 9115 AP.	Passed	

EWCJ173ST_Upgrade Patch_26	upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9115 AP.	To Verify the upgrading path from 17.1 CCO > 17.2 CCO and then 17.3 Latest Images by using the TFTP option in UI with 9115 AP.	Passed	

200 Country Code Support

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_200 country Code_01	Verifying by Configuring the country code in EWC GUI.	To Check whether the country code is Configured Properly or not in GUI	Passed	
EWCJ173S_200 country Code_02	Verifying the country code by connecting Mac OS clients.	To Check whether Mac OS clients are connected successfully after a change in the country code.	Passed	
EWCJ173S_200 country Code_03	Verifying by Configuring the Country code and upgrading the controller.	To Check whether the country code is Configured Properly after the upgradation process.	Passed	
EWCJ173S_200 country Code_04	Verifying by Configuring the Country code and downgrading the controller.	To Check whether the country code is Configured Properly after the down gradation process.	Passed	
EWCJ173S_200 country Code_05	Verifying the Configuration of the country code during day 0 Configuration.	To Check whether the country code is configured during day 0 Configuration.	Passed	
EWCJ173S_200 country Code_06	Verifying the country code by connecting Android clients.	To Check whether android clients are connected successfully after a change in the country code.	Passed	

EWCJ173S_200 country Code_07	Verifying whether the country code is configured without disabling the radio's	To verify whether the country code is configured without disabling the radio's	Passed	
EWCJ173S_200 country Code_08	Verifying the country code by connecting Windows clients.	To Check whether Windows clients are connected successfully after a change in the country code.	Passed	



CHAPTER 4

Regression Features - Test Summary

Multi LAG and Load Balance

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_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	
EWLCJ173S_Reg_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	
EWLCJ173S_Reg_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	
EWLCJ173S_Reg_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	
EWLCJ173S_Reg_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	

EWLCJ173S_Reg_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	

Client logging

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_430	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	
EWLCJ173S_Reg_431	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	
EWLCJ173S_Reg_432	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	
EWLCJ173S_Reg_433	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	
EWLCJ173S_Reg_434	To Verify default Notice level in TAC level logs for Windows wireless client.	Default Notice level in TAC level logs for Windows wireless client.	Passed	
EWLCJ173S_Reg_435	To Verify default Notice level in TAC level logs for MAC wireless client.	Default Notice level in TAC level logs for MAC wireless client.	Passed	
EWLCJ173S_Reg_436	To Verify default Notice level in TAC level logs for Android wireless client.	To Verify default Notice level in TAC level logs for Android wireless client.	Passed	

EWLCJ173S_Reg_437	To Verify default Notice level in TAC level logs for Apple Mobile wireless client.	To Verify default Notice level in TAC level logs for Apple Mobile wireless client.	Passed	

BSSID Counters

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_07	Checking the BSSID Statistics in eWLC	To check whether the BSSID showing proper in ewlc or not	Passed	
EWLCJ173S_Reg_08	Verifying the BSSID Statistics in catalyst AP's	To verify whether the BSSID showing proper in catalyst AP's or not	Passed	
EWLCJ173S_Reg_09	Verifying the BSSID record in FMAN/CPP.	To verify whether the BSSID record showing correct in FMAN/CPP or not	Passed	
EWLCJ173S_Reg_10	Checking the Client object's hierarchy relationship in FMAN	To check whether FMAN showing the client object hierarchy or not	Passed	
EWLCJ173S_Reg_11	Validating the client record in FMAN/CPP.	To validate the client record in FMAN/CPP	Passed	
EWLCJ173S_Reg_12	Verifying BSSID with Intra client roaming	To verify whether BSSID with client roaming between AP's or not	Passed	
EWLCJ173S_Reg_13	Verifying BSSID with inter client roming	To check whether BSSID is appearing or not ,when clients are roaming between controllers	Passed	
EWLCJ173S_Reg_14	Monitoring BSSID status in eWLC UI after client association	To check whether BSSID status showing or not in eWLC UI	Passed	
EWLCJ173S_Reg_15	Monitoring the BSSID through WNCd Validation	To check the BSSID through WNCd Validation	Passed	

EWLCJ173S_Reg_16	Capturing the BSSID & Windows client connectivity using Wireshark	To check the window client connectivity & BSSID using Wireshark	Passed	
EWLCJ173S_Reg_17	Capturing the BSSID & MAC client connectivity using Wireshark	To check the MAC client connectivity & BSSID using Wireshark	Passed	
EWLCJ173S_Reg_18	Monitoring the BSSID & Android client connectivity using Wireshark	To check the Android client connectivity & BSSID using Wireshark	Passed	
EWLCJ173S_Reg_19	Capturing the BSSID & iOS client connectivity using Wireshark	To check the iOS client connectivity & BSSID using Wireshark	Passed	

AdvAP QBSS MCAST

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_20	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	
EWLCJ173S_Reg_21	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	
EWLCJ173S_Reg_22	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	

EWLCJ173S_Reg_23	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	
EWLCJ173S_Reg_24	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	
EWLCJ173S_Reg_25	Verify the QBSS load information in Beacon and Probes fames by configuring WMM as Required with qbss load for policy profile and Flexmode 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 Flexmode AP	Passed	
EWLCJ173S_Reg_26	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	
EWLCJ173S_Reg_27	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	
EWLCJ173S_Reg_28	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	

EWLCJ173S_Reg_29	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	
EWLCJ173S_Reg_30	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	
EWLCJ173S_Reg_31	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	
EWLCJ173S_Reg_32	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	
EWLCJ173S_Reg_33	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	
EWLCJ173S_Reg_34	Verify the Multicast filter and Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client associates and receives MC2UC traffic when flex AP is rebooted in connected mode with multicast filter.	Passed	

EWLCJ173S_Reg_35	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	

Opportunistic Key Caching

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_36	Configure and verify the OKC to the WLAN configuration.	To check whether OKC configured to WLAN or not.	Passed	
EWLCJ173S_Reg_37	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	
EWLCJ173S_Reg_38	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	
EWLCJ173S_Reg_39	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	
EWLCJ173S_Reg_40	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	

EWLCJ173S_Reg_41	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	
EWLCJ173S_Reg_42	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	
EWLCJ173S_Reg_43	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	
EWLCJ173S_Reg_44	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	
EWLCJ173S_Reg_45	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	
EWLCJ173S_Reg_46	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	
EWLCJ173S_Reg_47	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	

EWLCJ173S_Reg_48	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	
EWLCJ173S_Reg_49	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	
EWLCJ173S_Reg_50	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	
EWLCJ173S_Reg_51	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	
EWLCJ173S_Reg_52	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	

TWT support on Axel AP

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_53	Configuring TWT in 9115 Ap	To check Whether 9115 Ap get TWT parameter details properly	Passed	

EWLCJ173S_Reg_54	Configuring TWT in 9120 Ap	To check Whether 9120 Ap get TWT parameter details properly	Passed	
EWLCJ173S_Reg_55	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	
EWLCJ173S_Reg_56	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	
EWLCJ173S_Reg_57	Configuring TWT in 11ax Ap with flex connect mode	To verify the 11ax ap get TWT parameter in flex connect mode	Passed	
EWLCJ173S_Reg_58	Configuring TWT in 11ax Ap with Local mode	To verify the 11ax ap get TWT parameter in Local mode	Passed	
EWLCJ173S_Reg_59	Associate the sleeping client with 11ax Ap	To Verify sleeping client associate with 11ax Ap properly or not	Passed	
EWLCJ173S_Reg_60	Clear the TWT configuration Check the Client behaviour	To verify the client behaviour after clear the TWT configuration	Passed	

Google: DHCP Required

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_61	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	

EWLCJ173S_Reg_62	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	
EWLCJ173S_Reg_63	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	
EWLCJ173S_Reg_64	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	
EWLCJ173S_Reg_65	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	
EWLCJ173S_Reg_66	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	
EWLCJ173S_Reg_67	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	
EWLCJ173S_Reg_68	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	
EWLCJ173S_Reg_69	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	
EWLCJ173S_Reg_70	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	

EWLCJ173S_Reg_71	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	
EWLCJ173S_Reg_72	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	
EWLCJ173S_Reg_73	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	

Client Whitelisting

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_74	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	
EWLCJ173S_Reg_75	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	Passed	
EWLCJ173S_Reg_76	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	
EWLCJ173S_Reg_77	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	

EWLCJ173S_Reg_78	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	
EWLCJ173S_Reg_79	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	
EWLCJ173S_Reg_80	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	
EWLCJ173S_Reg_81	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	
EWLCJ173S_Reg_82	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	
EWLCJ173S_Reg_83	Backup & Restore EWLC Config after lobby Accounts config	To Check that After Restore EWLC config lobby Admin accounts config available or not	Passed	
EWLCJ173S_Reg_84	Verifying Connected Whitelisted user in lobby account	To verify that connected whitelisted user showing in Connected/Whitelisted tab	Passed	

EWLCJ173S_Reg_85	Verifying Connected Not Whitelisted user in lobby account	To verify that connected Not Whitelisted user showing in Connected/Not Whitelisted tab	Passed	
EWLCJ173S_Reg_86	Verifying not Connected Whitelisted user in lobby account	To verify that not connected whitelisted user showing in Connected/Whitelisted tab	Passed	
EWLCJ173S_Reg_87	Removing the whitelisted user	To verify that whitelisted user removing or not	Passed	

Flex LS Client IP Context Distribution from Controller

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_88	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	
EWLCJ173S_Reg_89	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	
EWLCJ173S_Reg_90	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	

EWLCJ173S_Reg_91	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	
EWLCJ173S_Reg_92	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	
EWLCJ173S_Reg_93	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	
EWLCJ173S_Reg_94	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	
EWLCJ173S_Reg_95	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	
EWLCJ173S_Reg_96	IP-MAC entries deletion upon AP reboot.	IP-MAC entries will be deleted when AP reboots.	Passed	

WPA3 Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_97	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE security Configuration.	Passed	

EWLCJ173S_Reg_98	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	
EWLCJ173S_Reg_99	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	
EWLCJ173S_Reg_100	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	
EWLCJ173S_Reg_101	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	
EWLCJ173S_Reg_102	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Passed	
EWLCJ173S_Reg_103	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	
EWLCJ173S_Reg_104	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	
EWLCJ173S_Reg_105	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ173S_Reg_106	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	

EWLCJ173S_Reg_107	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	
EWLCJ173S_Reg_108	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	
EWLCJ173S_Reg_109	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ173S_Reg_110	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using WPA3 support with 9115AP	Passed	
EWLCJ173S_Reg_111	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	
EWLCJ173S_Reg_112	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	
EWLCJ173S_Reg_113	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	
EWLCJ173S_Reg_114	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	

Mesh & (Flex + Mesh) support on all 11ac Wave 2 Indoor Aps

Logical ID	Title	Description	Status	Defect ID

EWLCJ173S_Reg_115	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	
EWLCJ173S_Reg_116	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	
EWLCJ173S_Reg_117	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	Failed	CSCvv07740
EWLCJ173S_Reg_118	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	
EWLCJ173S_Reg_119	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	
EWLCJ173S_Reg_120	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	
EWLCJ173S_Reg_121	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	
EWLCJ173S_Reg_122	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	
EWLCJ173S_Reg_123	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	

EWLCJ173S_Reg_124	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	
EWLCJ173S_Reg_125	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	
EWLCJ173S_Reg_126	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	
EWLCJ173S_Reg_127	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	
EWLCJ173S_Reg_128	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	
EWLCJ173S_Reg_129	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	
EWLCJ173S_Reg_130	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	
EWLCJ173S_Reg_131	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	

EWLCJ173S_Reg_132	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	
EWLCJ173S_Reg_133	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	
EWLCJ173S_Reg_134	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	
EWLCJ173S_Reg_135	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	
EWLCJ173S_Reg_136	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	
EWLCJ173S_Reg_137	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	
EWLCJ173S_Reg_138	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	

EWLCJ173S_Reg_139	Check and verify the AP mode changes by changing From Flex+bridge mode to Flexconnect.	To check whether AP mode changing or not from Flex+bridge to Flexconnect.	Passed	
EWLCJ173S_Reg_140	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	
EWLCJ173S_Reg_141	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	

WGB Support for C9115 AXI AP

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_142	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWLCJ173S_Reg_143	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWLCJ173S_Reg_144	Configuring WGB in eWLC	To verify WGB configuration is successful or not in eWLC	Passed	
EWLCJ173S_Reg_145	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	

EWLCJ173S_Reg_146	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	
EWLCJ173S_Reg_147	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	
EWLCJ173S_Reg_148	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	
EWLCJ173S_Reg_149	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	
EWLCJ173S_Reg_150	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	
EWLCJ173S_Reg_151	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	

EWLCJ173S_Reg_152	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	
EWLCJ173S_Reg_153	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	
EWLCJ173S_Reg_154	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	
EWLCJ173S_Reg_155	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	
EWLCJ173S_Reg_156	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	
EWLCJ173S_Reg_157	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	
EWLCJ173S_Reg_158	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	
EWLCJ173S_Reg_159	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	

EWLCJ173S_Reg_160	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients after session timeout	Passed	
EWLCJ173S_Reg_161	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

mDNS Support for Wired Guest Access and Ap support

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_342	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	
EWLCJ173S_Reg_343	Create the Guest Lan with mDNS Mode Bridging.	Verify able to create the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ173S_Reg_344	Edit the Guest Lan with mDNS Mode Bridging.	Verify able to edit the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ173S_Reg_345	Delete the Guest Lan with mDNS Mode Bridging.	Verify able to Delete the Guest Lan with mDNS Mode Bridging.	Passed	
EWLCJ173S_Reg_346	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	
EWLCJ173S_Reg_347	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	
EWLCJ173S_Reg_348	Create the Guest Lan with mDNS Mode Gateway: .	Verify able to Create the Guest Lan with mDNS Mode Bridging Gateway: .	Passed	

EWLCJ173S_Reg_349	Create the Guest Lan with mDNS Mode Bridging Drop.	verify able to Create the Guest Lan with mDNS Mode Drop.	Passed	

PSK + Multi Auth Support for Guest

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_407	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Failed	CSCvv04519
EWLCJ173S_Reg_408	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ173S_Reg_409	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ173S_Reg_410	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ173S_Reg_411	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ173S_Reg_412	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	
EWLCJ173S_Reg_413	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ173S_Reg_414	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	

EWLCJ173S_Reg_415	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWLCJ173S_Reg_416	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ173S_Reg_417	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ173S_Reg_418	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ173S_Reg_419	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ173S_Reg_420	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ173S_Reg_421	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ173S_Reg_422	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ173S_Reg_50	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWCJ173S_Reg_51	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ173S_Reg_52	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	

EWCJ173S_Reg_53	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWCJ173S_Reg_54	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ173S_Reg_55	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	
EWCJ173S_Reg_56	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ173S_Reg_57	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ173S_Reg_58	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ173S_Reg_59	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ173S_Reg_60	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ173S_Reg_61	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ173S_Reg_62	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	

EWCJ173S_Reg_63	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWCJ173S_Reg_64	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ173S_Reg_65	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

iPSK Peer to Peer Blocking

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_350	Verifying the iPSK tag generation for the Connected Window JOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ173S_Reg_351	Verifying the iPSK tag generation for the Connected MAC OS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ173S_Reg_352	Verifying the iPSK tag generation for the Connected iOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ173S_Reg_353	Verifying the iPSK tag generation for the Connected Android Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	

EWLCJ173S_Reg_354	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	
EWLCJ173S_Reg_355	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	
EWLCJ173S_Reg_356	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	
EWLCJ173S_Reg_357	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	
EWLCJ173S_Reg_358	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	
EWLCJ173S_Reg_359	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	
EWLCJ173S_Reg_360	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	

EWLCJ173S_Reg_361	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	
EWLCJ173S_Reg_362	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	
EWLCJ173S_Reg_363	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	
EWLCJ173S_Reg_364	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	
EWLCJ173S_Reg_365	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	
EWLCJ173S_Reg_366	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	

EWLCJ173S_Reg_367	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	
EWLCJ173S_Reg_368	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in eWLC CLI	Passed	
EWLCJ173S_Reg_369	Verifying the wlan configuration with iPSK tag Configuration through eWLC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC Web	Passed	
EWLCJ173S_Reg_370	Verifying the wlan generation with iPSK tag Configuration through eWLC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC CLI	Passed	
EWLCJ173S_Reg_371	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	
EWLCJ173S_Reg_372	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	
EWLCJ173S_Reg_373	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	

EWLCJ173S_Reg_374	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	
EWLCJ173S_Reg_375	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	
EWLCJ173S_Reg_376	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	
EWLCJ173S_Reg_377	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	
EWLCJ173S_Reg_378	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	
EWLCJ173S_Reg_379	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	
EWLCJ173S_Reg_380	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	

EWLCJ173S_Reg_381	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	
EWLCJ173S_Reg_382	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	
EWLCJ173S_Reg_383	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	
EWLCJ173S_Reg_384	Verifying the iPSK tag generation for the Connected AnyConnect Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When AnyConnect client connected to iPSK enabled WLAN Profile	Passed	
EWLCJ173S_Reg_385	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	
EWLCJ173S_Reg_386	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	

EWLCJ173S_Reg_387	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	
EWLCJ173S_Reg_388	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	
EWLCJ173S_Reg_389	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	
EWLCJ173S_Reg_390	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	
EWLCJ173S_Reg_391	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	

EWLCJ173S_Reg_392	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	
EWLCJ173S_Reg_393	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	
EWLCJ173S_Reg_394	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	
EWLCJ173S_Reg_395	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ173S_Reg_396	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ173S_Reg_77	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	
EWCJ173S_Reg_78	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	

EWCJ173S_Reg_79	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	
EWCJ173S_Reg_80	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	
EWCJ173S_Reg_81	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	
EWCJ173S_Reg_82	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	
EWCJ173S_Reg_83	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	
EWCJ173S_Reg_84	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	
EWCJ173S_Reg_85	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	

EWCJ173S_Reg_86	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	
EWCJ173S_Reg_87	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	
EWCJ173S_Reg_88	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	
EWCJ173S_Reg_89	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	
EWCJ173S_Reg_90	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	
EWCJ173S_Reg_91	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	

EWCJ173S_Reg_92	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	
EWCJ173S_Reg_93	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	
EWCJ173S_Reg_94	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	
EWCJ173S_Reg_95	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	
EWCJ173S_Reg_96	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	
EWCJ173S_Reg_97	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	
EWCJ173S_Reg_98	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	

EWCJ173S_Reg_99	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	
EWCJ173S_Reg_100	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	
EWCJ173S_Reg_101	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	
EWCJ173S_Reg_102	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	
EWCJ173S_Reg_103	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	
EWCJ173S_Reg_104	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	
EWCJ173S_Reg_105	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	

EWCJ173S_Reg_106	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	
EWCJ173S_Reg_107	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	
EWCJ173S_Reg_108	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	
EWCJ173S_Reg_109	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	
EWCJ173S_Reg_110	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	
EWCJ173S_Reg_111	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	
EWCJ173S_Reg_112	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	

EWCJ173S_Reg_113	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	
EWCJ173S_Reg_114	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	
EWCJ173S_Reg_115	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	
EWCJ173S_Reg_116	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	
EWCJ173S_Reg_117	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	

EWCJ173S_Reg_118	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	
EWCJ173S_Reg_119	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	
EWCJ173S_Reg_120	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	
EWCJ173S_Reg_121	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	
EWCJ173S_Reg_122	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ173S_Reg_123	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

Inter-Release Controller Mobility

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_311	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	Failed	CSCvu80115
EWLCJ173S_Reg_312	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	
EWLCJ173S_Reg_313	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	
EWLCJ173S_Reg_314	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	
EWLCJ173S_Reg_315	Configuring the Anchor controller option in 9800 WLC UI	To check whether Anchor option can be configured or not in a 9800 Controller.	Passed	
EWLCJ173S_Reg_316	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	

EWLCJ173S_Reg_317	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	
EWLCJ173S_Reg_318	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	
EWLCJ173S_Reg_319	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	
EWLCJ173S_Reg_320	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	
EWLCJ173S_Reg_321	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	

EWLCJ173S_Reg_322	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	
EWLCJ173S_Reg_323	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	
EWLCJ173S_Reg_324	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	
EWLCJ173S_Reg_325	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	
EWLCJ173S_Reg_326	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	
EWLCJ173S_Reg_327	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	

EWLCJ173S_Reg_328	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	
EWLCJ173S_Reg_329	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	
EWLCJ173S_Reg_330	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	
EWLCJ173S_Reg_331	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	
EWLCJ173S_Reg_332	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	

EWLCJ173S_Reg_333	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	

ISSU Enhancement(Zero downtime for Wireless N/W)

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_334	Performing Upgradation using ISSU	To check whether the upgradation is performed or not via ftp	Failed	CSCvu37780
EWLCJ173S_Reg_335	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ173S_Reg_336	Disabling the Rollback timer during upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Failed	CSCvu68395
EWLCJ173S_Reg_337	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ173S_Reg_338	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	
EWLCJ173S_Reg_339	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ173S_Reg_340	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Failed	CSCvu61995

EWLCJ173S_Reg_341	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	

Open DNS Support for Flex

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_397	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	
EWLCJ173S_Reg_398	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	
EWLCJ173S_Reg_399	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWLCJ173S_Reg_400	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	
EWLCJ173S_Reg_401	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	
EWLCJ173S_Reg_402	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	

EWLCJ173S_Reg_403	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	
EWLCJ173S_Reg_404	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWLCJ173S_Reg_405	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWLCJ173S_Reg_406	Perform the roaming between two ewlc	To verify the open dns after Inter roaming	Passed	
EWCJ173S_Reg_212	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	
EWCJ173S_Reg_213	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	
EWCJ173S_Reg_214	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWCJ173S_Reg_215	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	
EWCJ173S_Reg_216	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	

EWCJ173S_Reg_217	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	
EWCJ173S_Reg_218	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	
EWCJ173S_Reg_219	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWCJ173S_Reg_220	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWCJ173S_Reg_221	Perform the roaming between two ewc	To verify the open dns after Inter roaming	Passed	

TACACS

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_397	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	
EWLCJ173S_Reg_398	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	
EWLCJ173S_Reg_399	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	

EWLCJ173S_Reg_400	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	
EWLCJ173S_Reg_401	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	
EWLCJ173S_Reg_402	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	
EWLCJ173S_Reg_403	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	
EWLCJ173S_Reg_404	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWLCJ173S_Reg_405	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWLCJ173S_Reg_406	Perform the roaming between two ewlc	To verify the open dns after Inter roaming	Passed	
EWCJ173S_Reg_190	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	

EWCJ173S_Reg_191	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	
EWCJ173S_Reg_192	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	
EWCJ173S_Reg_193	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	
EWCJ173S_Reg_194	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	
EWCJ173S_Reg_195	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	
EWCJ173S_Reg_196	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	
EWCJ173S_Reg_197	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", "Command Line Interfaces and "Management" checkboxes.	Passed	

EWCJ173S_Reg_198	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	

Mac filtering (for L2 security)

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_226	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	
EWLCJ173S_Reg_227	Uploading the empty CSV file in eWLC UI	To check whether an blank CSV file could be uploaded in eWLC UI	Passed	
EWLCJ173S_Reg_228	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	
EWLCJ173S_Reg_229	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
EWLCJ173S_Reg_230	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWLCJ173S_Reg_231	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	

EWLCJ173S_Reg_232	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	
EWLCJ173S_Reg_233	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWLCJ173S_Reg_234	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	
EWCJ173S_Reg_199	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	
EWCJ173S_Reg_200	Uploading the empty CSV file in eWC UI	To check whether an blank CSV file could be uploaded in eWC UI	Passed	
EWCJ173S_Reg_201	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	
EWCJ173S_Reg_202	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	

EWCJ173S_Reg_203	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWCJ173S_Reg_204	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	
EWCJ173S_Reg_205	Connecting the client after client identity account expired in ISE	To Connect the Client after client identity account expired in ISE	Passed	
EWCJ173S_Reg_206	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	

Lobby Ambassador

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_162	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	
EWLCJ173S_Reg_163	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	
EWLCJ173S_Reg_164	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	

EWLCJ173S_Reg_165	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	
EWLCJ173S_Reg_166	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	
EWLCJ173S_Reg_167	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	
EWLCJ173S_Reg_168	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	
EWLCJ173S_Reg_169	Create and verify the lobby user in CLI	To verify the User able to login with Lobby credentials	Passed	

Syslogs

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_292	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	
EWLCJ173S_Reg_293	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	
EWLCJ173S_Reg_294	Downloading the syslog's after generated in Ewlc	To check whether able to download the syslog's from Ewlc	Passed	
EWLCJ173S_Reg_295	Clearing the logs in controller after generated successfully	To verify whether user able to clear the all generated logs in Ewlc	Passed	

EWLCJ173S_Reg_296	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	
EWLCJ173S_Reg_297	Configuring syslog servers in eWLC with log level setting as critical	To verify the critical logs in syslog server after configuration in device	Passed	
EWLCJ173S_Reg_298	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	
EWLCJ173S_Reg_299	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	

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_252	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	
EWLCJ173S_Reg_253	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	
EWLCJ173S_Reg_254	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	

EWLCJ173S_Reg_255	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	
EWLCJ173S_Reg_256	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	
EWCJ173S_Reg_207	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	
EWCJ173S_Reg_208	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	
EWCJ173S_Reg_209	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	
EWCJ173S_Reg_210	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	
EWCJ173S_Reg_211	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	

CWA

Logical ID	Title	Description	Status	Defect ID

EWLCJ173S_Reg_275	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	
EWLCJ173S_Reg_276	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	
EWLCJ173S_Reg_277	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	
EWLCJ173S_Reg_278	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	
EWLCJ173S_Reg_279	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	
EWLCJ173S_Reg_280	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	
EWLCJ173S_Reg_281	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	

EWLCJ173S_Reg_282	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	
EWLCJ173S_Reg_283	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	Failed	CSCvv06147
EWLCJ173S_Reg_284	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	
EWLCJ173S_Reg_285	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	
EWLCJ173S_Reg_286	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	
EWLCJ173S_Reg_287	Validate whether eWLC is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	
EWLCJ173S_Reg_288	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	

EWLCJ173S_Reg_289	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWLCJ173S_Reg_290	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	
EWLCJ173S_Reg_291	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	
EWCJ173S_Reg_228	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	
EWCJ173S_Reg_229	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	
EWCJ173S_Reg_230	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	
EWCJ173S_Reg_231	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	
EWCJ173S_Reg_232	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	
EWCJ173S_Reg_233	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	

EWCJ173S_Reg_234	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	
EWCJ173S_Reg_235	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	
EWCJ173S_Reg_236	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	
EWCJ173S_Reg_237	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	
EWCJ173S_Reg_238	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	
EWCJ173S_Reg_239	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	
EWCJ173S_Reg_240	Validate whether eWC is switch between configured Radius servers	To verify whether AAA authentication is occurring when one radius server goes down	Passed	

EWCJ173S_Reg_241	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWCJ173S_Reg_242	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWCJ173S_Reg_243	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	
EWCJ173S_Reg_244	Exporting/Importing configuration of CWA	To verify whether export and import is done successfully	Passed	

Bidirectional rate limit per client

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_170	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	
EWLCJ173S_Reg_171	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	
EWLCJ173S_Reg_172	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	

EWLCJ173S_Reg_173	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	
EWLCJ173S_Reg_174	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	
EWLCJ173S_Reg_175	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	
EWLCJ173S_Reg_176	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	
EWLCJ173S_Reg_177	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	

EWLCJ173S_Reg_178	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	
EWLCJ173S_Reg_179	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	
EWLCJ173S_Reg_180	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	

AAA Override of VLAN Name-id template

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_257	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	

EWLCJ173S_Reg_258	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	
EWLCJ173S_Reg_259	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	
EWLCJ173S_Reg_260	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	
EWLCJ173S_Reg_261	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	

EWLCJ173S_Reg_262	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	
EWLCJ173S_Reg_263	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	
EWLCJ173S_Reg_264	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	

Software update using SFTP with SFTP Domain Name support

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_246	eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ173S_Reg_247	Invalid eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ173S_Reg_248	eWLC .bin Software updating via SFTP server	Checking the eWLC .bin software updating or not via SFTP server	Passed	
EWLCJ173S_Reg_249	eWLC .SSH Software updating via SFTP server	Checking the eWLC .bin software updating or not via SFTP server	Passed	

EWLCJ173S_Reg_250	eWLC Software updating through Invalid SFTP IP	To check whether software is upgrading or not through Invalid SFTP IP	Passed	
EWLCJ173S_Reg_251	eWLC Software updating through Invalid SFTP user name/password	Verifying eWLC software is upgrading or not through Invalid SFTP user name/password	Passed	

CMX Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_216	Adding Cisco eWLCto CMX	To add a Cisco eWLCto CMX and check if the eWLCgets added to the CMX with the eWLCstatus showing	Passed	
EWLCJ173S_Reg_217	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	
EWLCJ173S_Reg_218	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	
EWLCJ173S_Reg_219	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	

EWLCJ173S_Reg_220	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	
EWLCJ173S_Reg_221	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
EWLCJ173S_Reg_222	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	
EWLCJ173S_Reg_223	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWLCJ173S_Reg_224	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	
EWLCJ173S_Reg_225	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	
EWCJ173S_Reg_280	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	
EWCJ173S_Reg_281	Importing maps from prime infrastructure	To import maps from prime infrastructure and check if the maps gets imported to the cmx .	Passed	

EWCJ173S_Reg_282	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	
EWCJ173S_Reg_283	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	
EWCJ173S_Reg_284	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	
EWCJ173S_Reg_285	Using MAC address the Client devices are searched	To check whether Client device can be searched by specifying its MAC address or not	Passed	
EWCJ173S_Reg_286	Using IP address the Client devices are searched	To check whether Client device can be searched by specifying its IP address or not	Passed	
EWCJ173S_Reg_287	Using SSID the Client devices are searched	To verify whether Client device can be searched by specifying the SSID or not	Passed	
EWCJ173S_Reg_288	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	
EWCJ173S_Reg_289	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	

MC2UC (Video streaming)

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_300	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWLCJ173S_Reg_301	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	
EWLCJ173S_Reg_302	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	
EWLCJ173S_Reg_303	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	
EWLCJ173S_Reg_304	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWLCJ173S_Reg_305	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	
EWLCJ173S_Reg_306	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	

EWLCJ173S_Reg_307	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	
EWLCJ173S_Reg_308	Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client associates and receives MC2UC traffic when flex AP is rebooted in connected mode.	Passed	
EWLCJ173S_Reg_309	Vide stream 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	
EWLCJ173S_Reg_310	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	
EWCJ173S_Reg_290	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to video streaming receives MC2UC traffic	Passed	
EWCJ173S_Reg_291	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	
EWCJ173S_Reg_292	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	

EWCJ173S_Reg_293	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	
EWCJ173S_Reg_294	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWCJ173S_Reg_295	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	
EWCJ173S_Reg_296	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	
EWCJ173S_Reg_297	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	
EWCJ173S_Reg_298	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	
EWCJ173S_Reg_299	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	

EWCJ173S_Reg_300	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	

Scheduled WLAN Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_423	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	
EWLCJ173S_Reg_424	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	
EWLCJ173S_Reg_425	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	
EWLCJ173S_Reg_426	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	
EWLCJ173S_Reg_427	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	
EWLCJ173S_Reg_428	Configure the Calendar Profile in Static WEP security WLAN with L3 Security,MAC Flittering and with Start/End time .	To check whether WLAN is broadcasting or not on configured Start/End time	Passed	

EWLCJ173S_Reg_429	Observe the Client Disassociation on Calendar Profile after end time	To check whether client is disassociating after end time.	Passed	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_235	Configuring optimized roaming with 2.4 GHz band and roam Android client	To verify that optimized roaming with 2.4 GHz band gets configured or not and check association of Android client	Passed	
EWLCJ173S_Reg_236	Configuring optimized roaming with 5 GHz band and roam Android client	To verify that optimized roaming with 5 GHz band and check association of Android client	Passed	
EWLCJ173S_Reg_237	Configuring optimized roaming with 5 GHz band , 6 MBPS Threshold and roam Android client	To verify that optimized roaming with 5 GHz band , 6 MBPS Threshold configured and check association of Android client	Passed	
EWLCJ173S_Reg_238	Configuring optimized roaming with 2.4 GHz band ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,9 MBPS Threshold configured and check association of iOS client	Passed	
EWLCJ173S_Reg_239	Configuring optimized roaming with 5 GHz band and roam iOS client	To verify that optimized roaming with 5 GHz band &customized interval(40 Sec) configured successfully and check association of iOS client	Passed	

EWLCJ173S_Reg_240	Moving the Android client from AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from AP	Passed	
EWLCJ173S_Reg_241	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassociated when signal is poor while moving from AP	Passed	
EWLCJ173S_Reg_242	Moving the Android client from AP after enable optimized roaming with interference availability	To verify that client got disassociated when signal is poor while moving from AP with interference availability	Passed	
EWLCJ173S_Reg_243	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
EWLCJ173S_Reg_244	Restarting the EWLC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWLCJ173S_Reg_245	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	
EWCJ173S_Reg_301	Configuring optimized roaming with 2.4 GHz band and roam Android client	To verify that optimized roaming with 2.4 GHz band gets configured or not and check association of Android client	Passed	

EWCJ173S_Reg_302	Configuring optimized roaming with 2.4 GHz band ,1 MBPS Thresholds and roam Android client	To verify that optimized roaming with 2.4 GHz band,1 MBPS Thresholds gets configured or not and check association of Android client	Passed	
EWCJ173S_Reg_303	Configuring optimized roaming with 5 GHz band and roam Android client	To verify that optimized roaming with 5 GHz band and check association of Android client	Passed	
EWCJ173S_Reg_304	Configuring optimized roaming with 5 GHz band , 6 MBPS Threshold and roam Android client	To verify that optimized roaming with 5 GHz band , 6 MBPS Threshold configured and check association of Android client	Passed	
EWCJ173S_Reg_305	Configuring optimized roaming with 2.4 GHz band ,5.5 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,5.5 MBPS Threshold configured successfully and check association of iOS client	Passed	
EWCJ173S_Reg_306	Configuring optimized roaming with 2.4 GHz band ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,9 MBPS Threshold configured and check association of iOS client	Passed	
EWCJ173S_Reg_307	Configuring optimized roaming with 5 GHz band and roam iOS client	To verify that optimized roaming with 5 GHz band &customized interval(40 Sec) configured successfully and check association of iOS client	Passed	

EWCJ173S_Reg_308	Configuring optimized roaming with 5 GHz band , 12 MBPS Threshold and roam iOS client	To verify that optimized roaming with 5 GHz band , 12 MBPS Threshold configured successfully and check association of iOS client	Passed	
EWCJ173S_Reg_309	Moving the Android client from AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from AP	Passed	
EWCJ173S_Reg_310	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassociated when signal is poor while moving from AP	Passed	
EWCJ173S_Reg_311	Moving the Android client from AP after enable optimized roaming in ME with interference availability	To verify that client got disassociated when signal is poor while moving from 2700 AP with interference availability	Passed	
EWCJ173S_Reg_312	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
EWCJ173S_Reg_313	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWCJ173S_Reg_314	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	

OWE Support

Logical ID	Title	Description	Status	Defect ID

EWLCJ173S_Reg_181	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	
EWLCJ173S_Reg_182	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	
EWLCJ173S_Reg_183	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	
EWLCJ173S_Reg_184	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	
EWLCJ173S_Reg_185	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	
EWLCJ173S_Reg_186	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	
EWLCJ173S_Reg_187	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	
EWLCJ173S_Reg_188	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	
EWLCJ173S_Reg_189	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	

EWLCJ173S_Reg_190	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	
EWLCJ173S_Reg_191	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	
EWLCJ173S_Reg_192	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	
EWLCJ173S_Reg_193	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	

Best Practices WebUI

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_194	Enable/Disable the http/https for management	Verify the web UI is able to open or not through http/https after modification	Passed	
EWLCJ173S_Reg_195	Configure the NTP server	To check whether NTP server is able to configure or not for WEB UI	Passed	
EWLCJ173S_Reg_196	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	
EWLCJ173S_Reg_197	Create the WLAN with WPA2	Verify the WLAN with WPA2 after configuring via best practice	Passed	

EWLCJ173S_Reg_198	Enable the User Login Policies	Checking the User Login Policies is enabled or not	Passed	
EWLCJ173S_Reg_199	Enable the Local Profiling on one or more active WLANs	Verify the enabled Local Profile on Active WLAN	Passed	
EWLCJ173S_Reg_200	Configure the client band for all Active WLANs	To check whether client Band is applied or not for Active WLANs	Passed	
EWLCJ173S_Reg_201	Enable the 5ghz band for Active WLAN	Verify the 5ghz client band on active WLANs	Passed	
EWLCJ173S_Reg_202	Enable the 2.4ghz band for Active WLAN	Checking the 2.4ghz client band on active WLANs	Passed	
EWLCJ173S_Reg_203	Configure the Best channel width	To check whether Best channel width is configured or not on both radios	Passed	
EWLCJ173S_Reg_204	Enable the Flexible Radio Assignment	To check whether Flexible Radio Assignment is enabled or not	Passed	
EWLCJ173S_Reg_205	Configure the Load balance for one or more active WLAN	Verify the Load balance enabled or not on Active WLAN	Passed	
EWLCJ173S_Reg_206	Enable the Auto Dynamic Channel Assignment	To check whether global channel is enabled or not	Passed	

Image Pre download

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_Reg_265	eWLC Software updating via SFTP server	Verifying eWLC software updating or not via SFTP server	Passed	
EWLCJ173S_Reg_266	Invalid eWLC Software updating via SFTP server.	Verifying eWLC software updating or not via SFTP server	Passed	

EWLCJ173S_Reg_267	Software updating via tftp server	Checking the eWLC software updating or not via tftp server	Passed	
EWLCJ173S_Reg_268	Invalid eWLC Software updating via tftp server	To check whether eWLC software upgrading or not via tftp server	Passed	
EWLCJ173S_Reg_269	eWLC Software upgrading through Invalid SFTP user name/password	Verifying eWLC software is upgrading or not through Invalid SFTP user name/password	Passed	
EWLCJ173S_Reg_270	eWLC software upgrading through invalid tftp file path	Checking eWLC software upgrading or not through invalid tftp file path	Passed	
EWLCJ173S_Reg_271	eWLC Software upgrading via Desktop(HTTP)	Verifying eWLC software upgrading or not via Desktop(HTTP) server	Passed	
EWLCJ173S_Reg_272	Invalid eWLC Software updating via Desktop(HTTP) mode	Verifying eWLC software upgrading or not via Desktop(HTTP) mode	Passed	
EWLCJ173S_Reg_273	ME Software upgrading via webserver	Verifying eWLC software upgrading or not via webserver	Passed	
EWLCJ173S_Reg_274	Invalid eWLC Software updating via webserver	To check whether Invalid eWLC software upgrading or not via webserver	Passed	

APSP/APDP support in WebUI for EWLC-ME

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_01	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	

EWCJ173S_Reg_02	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	
EWCJ173S_Reg_03	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	
EWCJ173S_Reg_04	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	
EWCJ173S_Reg_05	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	
EWCJ173S_Reg_06	Verifying whether APSP/APDP is accepting a invalid file path.	To check whether APSP/APDP is accepting invalid file path or not	Passed	
EWCJ173S_Reg_07	Verifying whether APSP/APDP is accepting a invalid ip address.	To check whether APSP/APDP is accepting invalid Ip address or not	Passed	
EWCJ173S_Reg_08	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ173S_Reg_09	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ173S_Reg_10	Connecting client after upgrading AP image using APSP/APDP.	To check whether connecting clients after the ap image upgradation using APSP/APDP	Passed	

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

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_11	To Deploy Fabric configuration from webUI on 9300	To Verify Fabric UI on 9300	Passed	
EWCJ173S_Reg_12	To Deploy Fabric configuration from webUI on 9300 and Windows Client	To Verify Fabric UI on 9300 with Window Client	Passed	
EWCJ173S_Reg_13	To Deploy Fabric configuration from webUI on 9300 and Android Client	To Verify Fabric UI on 9300 with Android Client	Passed	
EWCJ173S_Reg_14	To Deploy Fabric configuration from webUI on 9300 and MAC Client	To Verify Fabric UI on 9300 with MAC Client	Passed	
EWCJ173S_Reg_15	To Deploy Fabric configuration from webUI on 9300 and Apple Mobile Client	To Verify Fabric UI on 9300 with Apple Mobile Client	Passed	
EWCJ173S_Reg_16	To Deploy Fabric configuration from webUI on 9400	To Verify Fabric UI on 9400	Passed	
EWCJ173S_Reg_17	To Deploy Fabric configuration from webUI on 9400 and Windows Client	To Verify Fabric UI on 9400 with Window Client	Passed	
EWCJ173S_Reg_18	To Deploy Fabric configuration from webUI on 9400 and Android Client	To Verify Fabric UI on 9400 with Android Client	Passed	
EWCJ173S_Reg_19	To Deploy Fabric configuration from webUI on 9400 and MAC Client	To Verify Fabric UI on 9400 with MAC Client	Passed	
EWCJ173S_Reg_20	To Deploy Fabric configuration from webUI on 9400 and Apple Mobile Client	To Verify Fabric UI on 9400 with Apple Mobile Client	Passed	

EWCJ173S_Reg_21	To Deploy Fabric configuration from webUI on 9500	To Verify Fabric UI on 9500	Passed	
EWCJ173S_Reg_22	To Deploy Fabric configuration from webUI on 9500 and Windows Client	To Verify Fabric UI on 9500 with Window Client	Passed	
EWCJ173S_Reg_23	To Deploy Fabric configuration from webUI on 9500 and Android Client	To Verify Fabric UI on 9500 with Android Client	Passed	
EWCJ173S_Reg_24	To Deploy Fabric configuration from webUI on 9500 and MAC Client	To Verify Fabric UI on 9500 with MAC Client	Passed	
EWCJ173S_Reg_25	To Deploy Fabric configuration from webUI on 9500 and Apple Mobile Client	To Verify Fabric UI on 9500 with Apple Mobile Client	Passed	

ME WLAN Simplication

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_26	Adding/editing the location in Japanese UI	To verify that location added and location name , description , Client density , native vlan edited usefully	Passed	
EWCJ173S_Reg_27	Adding/editing the AAA server in Japanese UI	To verify that AAA server added and deleted succefully	Passed	
EWCJ173S_Reg_28	Creating new WLAN with WPA2 Enterprise	To verify that WLAN created with WPA2 Enterprise	Passed	
EWCJ173S_Reg_29	Creating new WLAN with WPA2 Personal	To verify that WLAN created with WPA2 Personal	Passed	
EWCJ173S_Reg_30	Creating the Employee Network with use of Existing network	To verify that new network created with the use of existing network	Passed	

EWCJ173S_Reg_31	Creating WLAN with Network type as guest	To verify that guest network created successfully	Passed	
EWCJ173S_Reg_32	Deleting the network from location in Japanese UI	To verify that network deleted from location	Passed	
EWCJ173S_Reg_33	Importing AP MAC address using CSV file and moved in the location	To verify that AP moved to location using CSV file	Passed	
EWCJ173S_Reg_34	Moving AP in the location by providing mac address	To verify that AP moved by mac address	Passed	
EWCJ173S_Reg_35	Moving AP in the location from Available AP list	To verify that AP moved from Available AP list	Passed	

WGB client support on ME

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_36	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWCJ173S_Reg_37	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWCJ173S_Reg_38	Configuring WGB in eWC	To verify WGB configuration is successful or not in eWC	Passed	
EWCJ173S_Reg_39	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	

EWCJ173S_Reg_40	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	
EWCJ173S_Reg_41	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	
EWCJ173S_Reg_42	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	
EWCJ173S_Reg_43	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	
EWCJ173S_Reg_44	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	
EWCJ173S_Reg_45	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	
EWCJ173S_Reg_46	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	

EWCJ173S_Reg_47	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWCJ173S_Reg_48	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients after session timeout	Passed	
EWCJ173S_Reg_49	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

EoGRE Support for ME

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_66	Creating EoGRE Tunnel Gateway.	To check whether the tunnel gateway is created or not.	Passed	
EWCJ173S_Reg_67	Creating EoGRE Tunnel Domain	To check whether the tunnel Domain is created or not.	Passed	
EWCJ173S_Reg_68	Configuring the Global Parameter for the EoGRE.	To check whether the global parameters are configured or not.	Passed	
EWCJ173S_Reg_69	Configuring the tunnel Profile.	To check whether the tunnel profile is created or not.	Passed	
EWCJ173S_Reg_70	Associate the WLAN to the Wireless policy profile.	To check whether the wlan is associated with the policy profile.	Passed	
EWCJ173S_Reg_71	Adding a policy tag and site tag to AP	To check whether the policy and site tag is added to an AP.	Passed	
EWCJ173S_Reg_72	Checking the client connectivity.	To check whether the client is connected or not	Passed	

EWCJ173S_Reg_73	Getting the EoGRE tunnel from PI	To check whether the tunnel is exported from PI or not	Passed	
EWCJ173S_Reg_74	Connect the ios clients and check the connectivity.	To check whether the ios clients get connected successfully.	Passed	
EWCJ173S_Reg_75	Connect the mac os clients and check the connectivity.	To check whether the mac os clients get connected successfully.	Passed	
EWCJ173S_Reg_76	Checking the traffic in the tunnel.	To check whether the traffic in the tunnel is managed or not.	Passed	

BSS Coloring on AX APs

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_124	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	
EWCJ173S_Reg_125	Configuring automatic BSS colour for 5ghz radio	To Check whether automatic BSS colouring is applied or not in 5 ghz ap radio	Passed	
EWCJ173S_Reg_126	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	
EWCJ173S_Reg_127	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	

EWCJ173S_Reg_128	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	
EWCJ173S_Reg_129	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	
EWCJ173S_Reg_130	Checking the BSS colour details are retained after AP and Controller reload	To Check whether the BSS colour retained after AP & Controller reload	Passed	
EWCJ173S_Reg_131	Verifying BSS colouring with Intra client roaming by using 9115AP	To verify whether BSS colouring with client roaming between AP's or not	Passed	
EWCJ173S_Reg_132	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	
EWCJ173S_Reg_133	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	
EWCJ173S_Reg_134	Capturing the Windows client connectivity & BSS colouring using Wireshark	To check the window client connectivity & BSS colouring using Wireshark	Passed	
EWCJ173S_Reg_135	Capturing the Android client connectivity & BSS colouring using Wireshark	To check the Android client connectivity & BSS colouring using Wireshark	Passed	
EWCJ173S_Reg_136	Capturing the Mac OS client connectivity & BSS colouring using Wireshark	To check the Mac OS client connectivity & BSS colouring using Wireshark	Passed	

EWCJ173S_Reg_137	Changing 9115 AP mode from local to Flex connect & check the BSS colouring Configuration	To change the mode of AP from local mode to Flex connect mode and check the BSS colouring configuration in 9115 Ap	Passed	
EWCJ173S_Reg_138	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	

CMX Parity for eWLC ME

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_139	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	
EWCJ173S_Reg_140	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	
EWCJ173S_Reg_141	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	

EWCJ173S_Reg_142	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	
EWCJ173S_Reg_143	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	
EWCJ173S_Reg_144	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	
EWCJ173S_Reg_145	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	
EWCJ173S_Reg_146	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	
EWCJ173S_Reg_147	Verify the Disconnected client details in CMX	To check whether the client is disconnected or not in CMX	Passed	
EWCJ173S_Reg_148	Verifying the Intra client roaming in CMX	To verify whether the client is roaming between AP's or not	Passed	
EWCJ173S_Reg_149	Verifying the Inter client roaming in CMX	To verify whether the clients are roaming between controllers	Passed	

EWCJ173S_Reg_150	Verifying the Wired client details in CMX	To Check whether the Wired client details are showing or not in CMX	Passed	
EWCJ173S_Reg_151	Verifying the guest LAN client details in CMX	To Check whether the Guest LAN client details are showing or not in CMX	Passed	
EWCJ173S_Reg_152	Verifying MIMO client details using Wireshark	To check Whether all the clients getting same BW & data rate or not	Passed	

Mesh on EWC

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_153	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	
EWCJ173S_Reg_154	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	
EWCJ173S_Reg_155	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	
EWCJ173S_Reg_156	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	
EWCJ173S_Reg_157	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	
EWCJ173S_Reg_158	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	

EWCJ173S_Reg_159	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	
EWCJ173S_Reg_160	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	
EWCJ173S_Reg_161	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	
EWCJ173S_Reg_162	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	
EWCJ173S_Reg_163	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	
EWCJ173S_Reg_164	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	
EWCJ173S_Reg_165	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	
EWCJ173S_Reg_166	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	

EWCJ173S_Reg_167	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	
EWCJ173S_Reg_168	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	
EWCJ173S_Reg_169	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	
EWCJ173S_Reg_170	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	
EWCJ173S_Reg_171	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	
EWCJ173S_Reg_172	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	
EWCJ173S_Reg_173	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	

EWCJ173S_Reg_174	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	
EWCJ173S_Reg_175	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	
EWCJ173S_Reg_176	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	
EWCJ173S_Reg_177	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	
EWCJ173S_Reg_178	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	
EWCJ173S_Reg_179	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	

EWC Day0 Elimination

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_180	Provisioning the eWLC_ME in day0 via PnP profile	Verify that user is able to Provisioned the eWLC_ME in day0 via PnP profile or not	Passed	

EWCJ173S_Reg_181	Manually adding single device Pnp details and Provisioning the 9115AX eWLC_ME in day0	Verify that user is able to Provisioned the eWLC_ME in day0 after adding Pnp Details manually	Passed	
EWCJ173S_Reg_182	Adding the device details in PnP with importing the .csv file in Bulk devices option	Verify that user is able to Provisioned the 1815eWLC_ME in day0 after adding Pnp Details with importing .csv file	Passed	
EWCJ173S_Reg_183	Checking the image version after Provisioning Ewlc_ME with PnP	Verifying the image version after Provisioning Ewlc_ME with PnP	Passed	
EWCJ173S_Reg_184	Checking the AP details after Provisioning Ewlc_ME with PnP	Verifying the AP details after Provisioning Ewlc_ME with PnP	Failed	CSCvu92121
EWCJ173S_Reg_185	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Failed	CSCvu78699
EWCJ173S_Reg_186	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	
EWCJ173S_Reg_187	Configuring wrong DNAC IP address in switch and trying for the provisioning	To verify whether user is able to Provisioned the eWLC_ME with providing wrong DNAC IP in Switch	Passed	
EWCJ173S_Reg_188	Configuring wrong details for PnP while claiming the device	To verify whether user is able to Provisioned the eWLC_ME with providing wrong PnP configuration in DNAC	Passed	
EWCJ173S_Reg_189	Checking the eWLC_ME after configuring factory reset with save config	Verifying whether user able to bring device to day0 or not with save config as yes	Passed	

Master AP Failover Issues

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_222	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	
EWCJ173S_Reg_223	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	
EWCJ173S_Reg_224	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	
EWCJ173S_Reg_225	Deleting the Master Prepared AP from CLI	To verify whether Master preferred AP is deleting from CLI or not	Passed	
EWCJ173S_Reg_226	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	
EWCJ173S_Reg_227	Assigning the Global AP Configurations	To verify whether Global AP Configurations authenticate to the AP or not	Passed	

802.1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_245	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	

EWCJ173S_Reg_246	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	
EWCJ173S_Reg_247	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	
EWCJ173S_Reg_248	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	
EWCJ173S_Reg_249	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	
EWCJ173S_Reg_250	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	
EWCJ173S_Reg_251	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	
EWCJ173S_Reg_252	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	

EWCJ173S_Reg_253	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	
EWCJ173S_Reg_254	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	
EWCJ173S_Reg_255	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	
EWCJ173S_Reg_256	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	
EWCJ173S_Reg_257	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	

Capwap Image Conversion

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_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	

EWCJ173S_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	
EWCJ173S_Reg_260	CAPWAP image joins to eWC	To verify whether COS AP is joining to the eWC with eWC capable or not	Passed	
EWCJ173S_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	
EWCJ173S_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	
EWCJ173S_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	
EWCJ173S_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	
EWCJ173S_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	
EWCJ173S_Reg_266	Performing the Master AP failover	To verify whether after Master Ap failover, ap is again downloading the images or not	Passed	

EWCJ173S_Reg_267	Interchanging the eWC image	To verify whether after image interchange eWC coming as changed version or not	Passed	
EWCJ173S_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	

ME AP convert to CAPWAP via DHCP Option

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_269	Change the 1852 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ173S_Reg_270	Change the 2800 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ173S_Reg_271	Change the 1542 ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ173S_Reg_272	Change the 1815i ME AP type to capwap using DHCP 43	To change the AP type to capwap using DHCP 43	Passed	
EWCJ173S_Reg_273	Change the AP mode after converting in to capwap	To change the AP mode after converting in to CAPWAP	Passed	
EWCJ173S_Reg_274	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	

EWCJ173S_Reg_275	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	
EWCJ173S_Reg_276	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	
EWCJ173S_Reg_277	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	
EWCJ173S_Reg_278	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	
EWCJ173S_Reg_279	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 ME capable AP	Passed	

Intelligent Capture

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_315	Packet capture for Android client using Intelligent Capture option in APgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Failed	CSCvu93108
EWCJ173S_Reg_316	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	Failed	CSCvu93108

EWCJ173S_Reg_317	Packet capture for IOS client using Intelligent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Failed	CSCvu93108
EWCJ173S_Reg_318	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	Failed	CSCvu93108

Efficient AP join

Logical ID	Title	Description	Status	Defect ID
EWCJ173S_Reg_331	Enable efficient join with slave and master AP 2800 of same model	To verify whether slave AP downloading image from master AP	Passed	
EWCJ173S_Reg_332	Enable efficient join with slave and master AP 2800/1542 of different model using TFTP	To verify whether slave AP downloading image from TFTP	Passed	
EWCJ173S_Reg_333	Perform client connectivity after enabling efficient join for same model and same version	To verify whether client gets connected after enabling efficient join and joining as CAPWAP	Passed	
EWCJ173S_Reg_334	Perform client connectivity after enabling efficient join for same model with different version using TFTP	To verify whether client gets connected after enabling efficient join and joining as ME CAPABLE	Passed	
EWCJ173S_Reg_335	Join 4 AP's to controller and check pre downloading status for efficient join	To verify whether predownloading status is showing proper for efficient join	Passed	
EWCJ173S_Reg_336	Removal of AP bundle for particular AP and perform TFTP	To verify whether TFTP aborted successfully after removal of AP bundle	Passed	

EWCJ173S_Reg_337	Perform efficient join for same model of 1542 AP	To verify whether efficient AP join enabled and image downloaded from master AP	Passed	
EWCJ173S_Reg_338	Enable efficient join with slave and master AP 1850/1542 of different model and same version using TFTP	To verify whether slave AP downloading image from TFTP and joining as ME CAPABLE	Passed	
EWCJ173S_Reg_339	Enable efficient join with slave and master AP 2800/1815 of different model and different version using TFTP	To verify whether slave AP downloading image from TFTP and joining as ME CAPABLE	Passed	
EWCJ173S_Reg_340	Disable efficient join with slave and master AP 1850 of same model using TFTP	To verify whether slave AP downloading image from TFTP	Passed	
EWCJ173S_Reg_341	Disable efficient join with slave and master AP 1850/2800 of different model using TFTP	To verify whether slave AP downloading image from TFTP	Passed	
EWCJ173S_Reg_342	Perform efficient join for different model of 1542/3800 AP using SFTP	To verify whether slave AP downloading image from SFTP	Passed	
EWCJ173S_Reg_343	Enable efficient join with slave and master AP 1542/1850 of different model through CLI using SFTP	To verify whether efficient AP join enabled and image downloaded from SFTP	Passed	
EWCJ173S_Reg_344	Perform efficient join for different model and same version of 1815/3800 AP using SFTP	To verify whether slave AP downloading image from SFTP and joining as ME CAPABLE	Passed	

EWCJ173S_Reg_345	Disable efficient join with slave and master AP 3800 of same model using SFTP	To verify whether slave AP downloading image from SFTP	Passed	
EWCJ173S_Reg_346	Disable efficient join with slave and master AP 3800/1850 of different model using SFTP	To verify whether slave AP downloading image from SFTP	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_config_1	In eWLC,No close/exit option for guided assistance	To click on guided assistance and validate the options	Failed	CSCvu99674
EWLCJ173S_config_2	Wpa3 security wlan able to has aes cipher but not used and client joining like open SSID	To associate the client with WPa3 security	Failed	CSCvu49340
EWLCJ173S_config_3	WebUI: FTP/SFTP upgrade fails if the username/password contains special characters	To upgrade the image via FTP/SFTP	Failed	CSCvu06348
EWLCJ173S_config_6	Active CLI session for deleted local user - Aireos parity gap behaviour	To activate CLI session and validate the local user	Failed	CSCvu87707
EWLCJ173S_config_7	9800 - Search results not accessible in collapsed menu panel	To search any elemnts and validate the results showing properly or not	Passed	
EWCJ173S_config_2	17.3 Build allowing WLAN with WPA3-PSK security without WPA2.	To create WLAn with WPA3-PSK security	Failed	CSCvu48139
EWCJ173S_config_3	Ap9120 Software page Middle container is over flowing outside	To validate the 9120 AP details in GUI Software page	Failed	CSCvv04861

EWCJ173S_config_4	AP shown "UNKNOWN" tag until user explicitly writing tag is base line behavior	To validate the AP details in GUI	Failed	CSCvu27719
EWCJ173S_config_5	upgrade fails from 17.2.2 to 17.3 and error message is too generic	Upgrade the image to 17.3 from 17.2.2 image	Failed	CSCvu16286
EWCJ173S_config_6	Typo error in japanese local for WLANs option in Menu	To create the WLAN and validate the details in japanese GUI	Failed	CSCvv04385
EWCJ173S_config_7	EWC Core dump generated due to core-pubd	Loginto CLI checking the crash file generated or not	Failed	CSCvu59065
EWCJ173S_config_8	Module Product ID shown empty for few AP	To validate the AP details in GUI	Failed	CSCvu92874

SR Cases

Logical ID	Title	Description	Status	Defect ID
EWLCJ173S_SR_01	Configuring MTU value to the eWLC port which connects to the switch	To configure MTU value to the eWLC ports which connects to the switch and check if the MTU value is changed also check the behaviour of the port	Passed	
EWLCJ173S_SR_02	Changing the access VLAN configuration in eWLC UI and check the behaviour of the eWLC	To change the access VLAN configuration in eWLC UI and check the behaviour of the eWLC	Passed	

EWLCJ173S_SR_03	Connecting a client to Wave 2 AP Joined in eWLC with WLAN security as dot1x security	To connect a client to Wave 2 AP Joined in eWLC with WLAN security as dot1x and check the Wireless packet of client .	Passed	
EWLCJ173S_SR_04	Connecting a client to 9115 AP Joined in eWLC with WLAN security as dot1x security and capturing wireless packet	To connect a client to 9115 AP Joined in eWLC with WLAN security as dot1x and capturing wireless packet to validate the full client authentication	Passed	
EWLCJ173S_SR_05	Connecting a client to 9115 AP Joined in eWLC with WLAN security as PSK security and capturing wireless packet	To connect a client to 9115 AP Joined in eWLC with WLAN security as PSK and capturing wireless packet to validate the full client authentication	Passed	
EWLCJ173S_SR_06	Connect a client to 9120 11ax AP with WPA3 security and check the HE Capabilities Parameters	To connect a client to 9120 11ax AP and verify if the packet capture	Passed	
EWLCJ173S_SR_07	Connect a client to 9130 11ax AP in HA eWLC with WPA3 security and check the HE Capabilities Parameters	To connect a client to 9130 11ax AP and verify if the packet capture	Passed	
EWLCJ173S_SR_08	Connect a client to 11ax AP in flex mode connected to eWLC in HA and to check the client and AP detail	To connect a client to 11 ax AP in flex mode and check the client and AP details	Passed	
EWLCJ173S_SR_09	HA Primary failover scenario with 11ax AP and a client connected to it	To check the details of the client connected to 11ax AP after HA primary failover	Passed	

EWLCJ173S_SR_10	Upgrading PI 3.8 to 3.9	To upgrade the PI from 3.8 to 3.9 and check if the upgrade is successful or not	Passed	
EWLCJ173S_SR_11	Upgrading PI to latest version using RPM method	To upgrade the PI to latest version and check if the upgrade is successful or not	Passed	
EWLCJ173S_SR_12	Enabling Wireless Trap related to AP and validating the same if traps are shown while eWLC is in HA	To enable Wireless trap related to AP in eWLC UI and validating the trap message in trap receiver	Passed	
EWLCJ173S_SR_13	Enabling Wireless Trap related to RF and validating the same if traps in are shown in trap receiver.	To enable Wireless trap related to RF in eWLC UI and validating the trap message in trap receiver	Passed	
EWLCJ173S_SR_14	Upgrading the software image into existing group of AP	To check whether the software image is upgraded into existing AP group	Passed	
EWLCJ173S_SR_15	ReSync trigger to Controller from DNAC after upgrade the software image in controller.	To check whether Controller is reloaded when triggering from DNAC after upgrade the software image in controller.	Passed	
EWLCJ173S_SR_16	Checking the WPA3 client connection with 9130 flex AP	To verify whether client connecting to flex connect AP with WPA3 security or not	Passed	
EWLCJ173S_SR_17	Upgrade/downgrade the eWLC and check for the client authentication	To check the connected client authentication after the device upgrade/downgrade	Passed	
EWLCJ173S_SR_18	Reload the Flex AP and check for the client association using Wireshark	To Verify whether client connected to radius server successfully after AP reloaded	Passed	

EWLCJ173S_SR_19	Check the client connectivity & WLAN Configuration after master failover	To verify the client connectivity & WLAN configuration after master failover	Passed	
EWLCJ173S_SR_20	Configuring Traffic Shaping for different WLAN & checking the Client connectivity	To verify whether the configuration applied or not	Passed	
EWLCJ173S_SR_21	Checking the CDP Neighbour configuration for 9800 controllers	To verify whether CDP neighbour config are showing or not in 9800 controller	Passed	
EWLCJ173S_SR_22	Checking the CDP neighbour configuration for different model AP	To Check the CDP neighbour config for different AP mode	Passed	
EWLCJ173S_SR_23	Validate the CDP neighbour configuration after AP reboot	To Validate the CDP neighbour config after AP reboot	Passed	
EWLCJ173S_SR_24	Checking the client ARP entry by changing the security type	To check the client ARP after changing the security type	Passed	
EWLCJ173S_SR_25	Verifying the client ARP entry after 2.4/5 ghz radio down	To verify the client ARP status after 2.4/5 ghz radio down	Passed	
EWLCJ173S_SR_26	Validate the Client ARP entry by changing the AP ip Address	To validate the client ARP by changing the AP ip Address	Passed	
EWLCJ173S_SR_27	Reloading the AP multiple times and checking for the configuration details	To verify the AP configuration details after AP reloaded multiple time	Passed	
EWLCJ173S_SR_28	Performing the eWLC reload after downloading the config file and verify the behaviour.	To check whether Factory reset happening or not after downloading the config file and performing the eWLC reload	Passed	

EWLCJ173S_SR_29	Checking the AID for Catalyst AP's	To check the AID for Catalyst AP's	Passed	
EWLCJ173S_SR_30	Associate the multiple clients to COS AP & Checking the Association ID	To associate multiple client to COS AP & Check the AID	Passed	
EWLCJ173S_SR_31	Perform HA and checking the client association	To verify the client association in HA	Passed	
EWLCJ173S_SR_32	Perform HA and checking the client association with same security type	To verify the client association in HA	Passed	
EWLCJ173S_SR_33	Associate the client with local switching	To verify the client association in local switching	Passed	
EWLCJ173S_SR_34	Validate the client ip address with flex connect with same vlan tag	To verify the client getting ip or not in flex connect	Passed	
EWLCJ173S_SR_35	Uploading new image via GUI for HA controller	To verify any crash occur during image upgradation	Passed	
EWLCJ173S_SR_36	Uploading new image via CLI for HA controller	To verify any crash occur during image upgradation	Passed	
EWLCJ173S_SR_37	Checking the username/ password after image upgradation	To check the username /password working fine after image upgradation	Passed	
EWLCJ173S_SR_38	Checking the username/ password after controller reload	To check whether the internal AP properly associate with the EWC	Passed	
EWLCJ173S_SR_39	configuring credential in day0	To check whether the internal AP properly associate with the EWC after reload	Passed	
EWLCJ173S_SR_40	Perform continuous intra roaming	To check any sxpd watchdog observed or not while performing continuous roaming	Passed	

EWLCJ173S_SR_41	Perform continuous inter roaming	To check any sxpd watchdog observed or not while performing continuous roaming	Passed	
EWLCJ173S_SR_42	Perform continuous reload	To check any sxpd watchdog observed or not while performing continuous roaming	Passed	
EWLCJ173S_SR_43	Verify user is able to enable/disable SNMP mode	To verify whether user is able to enable/disable SNMP mode	Passed	
EWLCJ173S_SR_44	Verify user is able to create SNMP community	To verify user is able to create SNMP community	Passed	
EWLCJ173S_SR_45	Verify DNAC able to join controller using SNMP community	To verify DNAC able to join controller using SNMP community	Passed	
EWLCJ173S_SR_46	Verify user is able to create V3 Users	To verify user is able to create V3 Users	Passed	
EWLCJ173S_SR_47	Verify user is able to create Hosts	To verify user is able to create Hosts	Passed	
EWLCJ173S_SR_48	Verify user is able to change password policy	To verify user is able to change password policy	Passed	
EWLCJ173S_SR_49	Verify user is able to enable all password policy	to verify user is able to enable all password policy	Passed	
EWLCJ173S_SR_50	Verify user is able to disable all password policy	to verify user is able to disable all password policy	Passed	
EWLCJ173S_SR_51	Verify eWLC Image upgraded through HTTP method without failed	To verify eWLC Image upgraded through HTTP method without fail	Passed	
EWLCJ173S_SR_52	Check the report is available after 7 days after save	To verify whether the DNAC report is not viable after 7 days	Passed	

EWLCJ173S_SR_53	Check the report is available after 7 days after save	To verify whether the PI report is avail after 7 days after data clean-up	Passed	
EWLCJ173S_SR_54	C9300 series Chassis View support in PI 3.6	To check weather we can able to add cat9600/9300 series devices to PI	Passed	
EWLCJ173S_SR_55	C9300 series Chassis View support in IN DNAC	To check weather we can able to add cat9600/9300 series devices to DNAC	Passed	
EWLCJ173S_SR_56	PI 3.7 default database variables for serial & model numbers broken due to incorrect values	To verify weather the Db variable are sending the accurate data to UI	Passed	
EWLCJ173S_SR_57	C9300-48P+8 Chassis View not displayed correctly in Device Details Summary	To verify weather you are able to get the chassis view of cat9k devices in Device details summary in PI	Passed	
EWLCJ173S_SR_58	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	
EWLCJ173S_SR_59	eWLC Lobby Admin with external Radius Authentication	To check eWLC Lobby Admin with external Radius Authentication	Passed	
EWLCJ173S_SR_60	eWLC Lobby Admin with external Radius Authentication	To check eWLC Lobby Admin with external Radius Authentication	Passed	
EWLCJ173S_SR_61	Check entitlement tag status in 9800-40 eWLC after smart license registration.	To check entitlement tag status in 9800-40 eWLC after smart license registration.	Passed	
EWLCJ173S_SR_62	Check entitlement tag status in 9800-L eWLC after smart license registration.	To check entitlement tag status in 9800-L eWLC after smart license registration.	Passed	

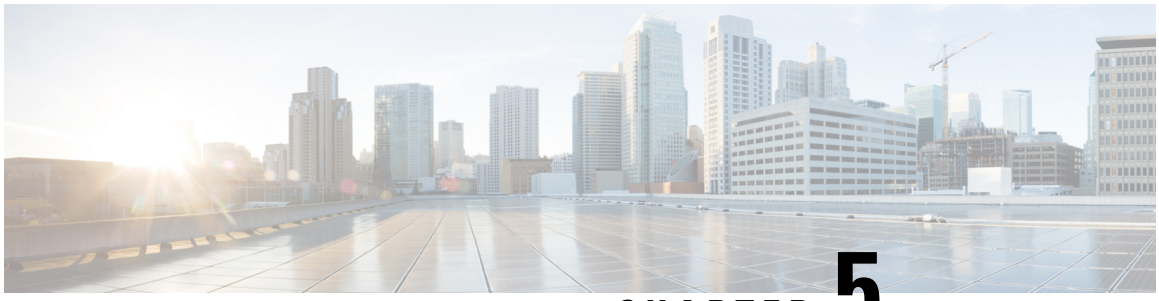
EWLCJ173S_SR_63	Check entitlement tag status in 9800-80 HA eWLC after smart license registration.	To check entitlement tag status in 9800-80 HA eWLC after smart license registration.	Passed	
EWLCJ173S_SR_64	Check entitlement tag status in 9800-CL eWLC after smart license registration.	To Check entitlement tag status in 9800-CL eWLC after smart license registration.	Passed	
EWLCJ173S_SR_65	Check advipservices status in license summary	Check advipservices status in license summary	Passed	
EWLCJ173S_SR_66	Check advipservices status in license summary after upgrade	To check advipservices status in license summary after upgrade	Passed	
EWLCJ173S_SR_67	To check advipservices status in license summary after downgrade	To check advipservices status in license summary after downgrade	Passed	
EWLCJ173S_SR_68	Check TACACS+ server connectivity from PI 3.7MR	To check TACACS+ server connectivity from PI 3.7MR	Passed	
EWLCJ173S_SR_69	Check TACACS+ server connectivity from PI 3.8	To check TACACS+ server connectivity from PI 3.8	Passed	
EWLCJ173S_SR_70	Check smart licensing in HA setup.	To check smart licensing in HA setup.	Passed	
EWLCJ173S_SR_71	Check license info after multiple reload in HA setup.	To check license info after multiple reload in HA setup.	Passed	
EWLCJ173S_SR_72	Check license info after multiple switchover in HA setup.	To check license info after multiple switchover in HA setup.	Passed	
EWLCJ173S_SR_73	Check license info after issu upgrade in HA setup.	To check license info after issu upgrade in HA setup.	Passed	

EWLCJ173S_SR_74	Check license info after issu downgrade in HA setup.	To check license info after issu downgrade in HA setup.	Passed	
EWLCJ173S_SR_75	Verify Deauthentication Reason Code's on 9120 Ap logs.	To Verify Deauthentication Reason Code's on 9120 Ap logs.	Passed	
EWLCJ173S_SR_76	Verify Deauthentication Reason Code's on 9130 Ap logs.	To Verify Deauthentication Reason Code's on 9130 Ap logs.	Passed	
EWLCJ173S_SR_77	Use the Apple mobile and verify the client delay on SSID connectivity.	To check Apple mobile and verify the client delay on SSID connectivity.	Passed	
EWLCJ173S_SR_78	Use the Apple MAC Book and verify the client delay on SSID connectivity.	To check MAC Book and verify the client delay on SSID connectivity.	Passed	
EWLCJ173S_SR_79	Use the Apple mobile and verify the client delay on SSID connectivity with different Ap Modes	Use the Apple mobile and verify the client delay on SSID connectivity with different Ap Modes	Passed	
EWLCJ173S_SR_80	Use the Apple MAC Book and verify the client delay on SSID connectivity with different Ap Modes	To check MAC Book and verify the client delay on SSID connectivity with different Ap Modes	Passed	
EWLCJ173S_SR_81	Configuration can be pushed from PI to the CMX and maps are synchronized in PI	To check the sync and reachability check with cmx and PI	Passed	
EWLCJ173S_SR_82	Configuration can be pushed from PI to the CMX and maps are synchronized in DNAC	To check the sync and reachability check with cmx and DNAC	Passed	
EWLCJ173S_SR_83	verify the data pruning in PI	To verify the data pruning in PI	Passed	
EWLCJ173S_SR_84	verify the data pruning in DNAC	To verify the data pruning in DNAC	Passed	

EWLCJ173S_SR_85	Observe AP crashed on WCPD mode on 9120	To Verify AP crashed on WCPD mode on 9120	Passed	
EWLCJ173S_SR_86	Observe AP crashed on WCPD mode on 9130	To Verify AP crashed on WCPD mode on 9130	Passed	
EWLCJ173S_SR_87	Observe AP crashed on WCPD mode on 9115	To Verify AP crashed on WCPD mode on 9115	Passed	
EWLCJ173S_SR_88	verify the stop process all comment in CMX	To verify the stop process all comment in CMX	Passed	
EWLCJ173S_SR_89	verify the stop process all comment in DNAC	To verify the stop process all comment in DNAC	Passed	
EWLCJ173S_SR_90	verify the stop process all comment in PI	To verify the stop process all comment in PI	Passed	
EWLCJ173S_SR_91	verify all the basic connectivity protocol's in AP9115	To verify all the basic connectivity protocol's in AP9115	Passed	
EWLCJ173S_SR_92	verify all the basic connectivity protocol's in AP9120	To verify all the basic connectivity protocol's in AP9120	Passed	
EWLCJ173S_SR_93	verify all the basic connectivity protocol's in AP9130	To verify all the basic connectivity protocol's in AP9130	Passed	
EWLCJ173S_SR_94	verify the Ap crash file and process memory in 9115	To verify the Ap crash file and process memory in 9115	Passed	
EWLCJ173S_SR_95	verify the Ap crash file and process memory in 9120	To verify the Ap crash file and process memory in 9120	Passed	
EWLCJ173S_SR_96	verify the Ap crash file and process memory in 9130	To verify the Ap crash file and process memory in 9130	Passed	

EWLCJ173S_SR_97	verify the Ap logs for Channel ERRORS and 3 Way hand shake issues in AP 9115	To verify the Ap logs for Channel ERRORS and 3 Way hand shake issues in AP 9115	Passed	
EWLCJ173S_SR_98	verify the Ap logs for Channel ERRORS and 3 Way hand shake issues in AP 9120	To verify the Ap logs for Channel ERRORS and 3 Way hand shake issues in AP 9120	Passed	
EWLCJ173S_SR_99	verify the Ap logs for Channel ERRORS and 3 Way hand shake issues in AP 9130	To verify the Ap logs for Channel ERRORS and 3 Way hand shake issues in AP 9130	Passed	
EWLCJ173S_SR_100	verify the Ap 9115 adding to PI with out Partial Collection failure and few basic details.	To verify the Ap 9115 adding to PI with out Partial Collection failure and few basic details.	Passed	
EWLCJ173S_SR_101	verify the Ap 9120 adding to PI with out Partial Collection failure and few basic details.	To verify the Ap 9120 adding to PI with out Partial Collection failure and few basic details.	Passed	
EWLCJ173S_SR_102	verify the Ap 9130 adding to PI with out Partial Collection failure and few basic details.	To verify the Ap 9130 adding to PI with out Partial Collection failure and few basic details.	Passed	
EWLCJ173S_SR_103	verify the Ap 9120 adding to DNAC with out Partial Collection failure and few basic details.	To verify the Ap 9120 adding to DNAC with out Partial Collection failure and few basic details.	Passed	
EWLCJ173S_SR_104	verify the Ap 9115 adding to DNAC with out Partial Collection failure and few basic details.	To verify the Ap 9115 adding to DNAC with out Partial Collection failure and few basic details.	Passed	

EWLCJ173S_SR_105	verify the Ap 9130 adding to DNAC with out Partial Collection failure and few basic details.	To verify the Ap 9130 adding to DNAC with out Partial Collection failure and few basic details.	Passed	



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

Release Notes for Cisco Digital Network Architecture Spaces

https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/release-notes/cisco-dnaspaces-june20.html

Release Notes Cisco Digital Network Architecture Center

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-3-0/release_notes/b_cisco_dna_center_rn_1_3_3_0.html

Cisco Catalyst 9600 Series Switches 17.2 Release Notes

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-2/release_notes/ol-17-2-9600.html