Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.5 for Japan (Release Version 17.5)

First Published: 2021-06-24

Last Modified: 2021-06-25

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 17.5

- 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 DNA Space

- Cisco DNA Connector

- Connected Mobile Experiences (CMX)

- ISE(VM)

- Cisco ISR 1100

- Cisco AP c9115

- Cisco AP c9120

- Cisco AP c9130

- Cisco AP c9105

- Access Point 4800

- Access Point 3800

- Access Point 2800

- 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

Acronym	Description
CCKM	Cisco Centralized Key Management
CCN	Channel Change Notification
CCX	Cisco Compatible Extensions
CDP	Cisco Discovery Protocol
CKIP	Cisco Key Integrity Protocol
CMX	Connected Mobile Experience
CVBF	Cisco Vector Beam Forming
CWA	Central Web Authentication
DCA	Dynamic Channel Assignment
DMZ	Demilitarized Zone
DNS	Domain Name System
DNA-C	Digital Network Architecture Center
DTIM	Delivery Traffic Indication Map
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
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

Acronym	Description
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
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

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

Test topology and Environment Matrix

Test Topology
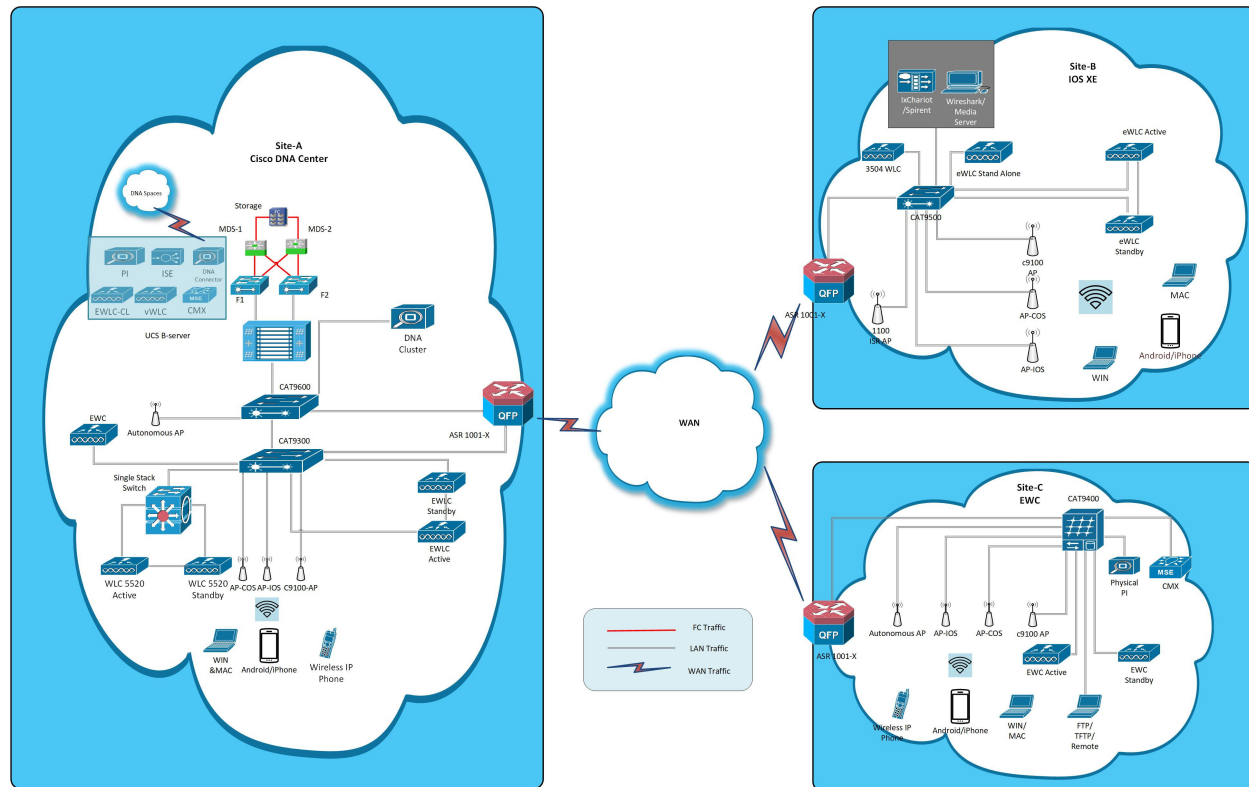
Component Matrix

Category	Component	Version
Controller	Cisco Elastic Wireless LAN Controller 9800	17.5
	Cisco Virtual Elastic Wireless LAN Controller 9800	17.5
	Cisco Catalyst 9800-L Wireless Controller	17.5
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.5
	Virtual Controller	8.10.121.0
Applications	DNAC	2.2.2
	DNA Spaces	Cloud (Dec 2020)
	DNA Spaces Connector	2.2.295
	Prime Infrastructure (Virtual Appliance, UCS based)	3.9.0.0
	ISE(VM)	3.0.0.393
	CMX(Physical (3375), VM)	10.6.2
	MSE(Physical (3365), VM)	8.0.150.0
	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	17.5
	Cisco AP 9120	17.5
	Cisco AP 9130	17.5
	Cisco AP 9105	17.5
	Cisco 1100 ISR	17.5
	Cisco AP 4800	15.3
	Cisco AP 3800	15.3
	Cisco AP 2800	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	17.5
	Cisco Cat 9200L	17.5
	Cisco Cat 9800	17.5
	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	21.40.2
	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 11.2.1
	iPad Pro	iOS 14.4
	iPhone 6, 6S ,7 & 11 (JP Locale)	iOS 14.3
	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	4.9.01095
	MS surface GO	Windows 10
Module	Hyper location Module	NA
Active Directory	AD	Windows server 2019
Call Control	Cisco Unified Communications Manager	12.5.0.99832-3/12.5.0.99832-3-1(JP)
Browsers	IE	11.0
	Mozilla Firefox	84.0.2
	Safari	14.0.2
	Chrome	88.0.4324.96

What's New ?

Cisco Catalyst 9800 Series Wireless Controller

- AdapativeLoad EDCA Parameter(Giga School)

- Umbrella Enhancements

- 11ax BSS Coloring(OBSS PD) on 9105/9115/9120 APs

- EasyPSK:WLAN Client Onboarding w/o registration

- ApplicationExperience Support on IOS-XEWireless Platforms

- EnablingPacket trace and conditional debug in eWLC 9800-CL

- Client DebugBundle for EWLC

- ICAP Support forC9130 fo 8 users

- Capabilityto enable/disable 11axfeatures per SSID

- HA ManagementEnhancements

- Standby MonitoringEnhancements

- ISSU DataModel Support

- Rejectionof Wrong WLAN ID

- Error Propagationfor Exec Commands

EWC

- Image UpgradeData Models for Controller

- 11ax Advanced traffic basedscheduler for scheduling SU, OFDMA and MU traffic on 9105/9115/9120

- 11ax OFDMA Support forEWC (8Users UL, 16Users DL) on 9105/9115/9120

- Called StationID with AP Ethernet MAC

- RRM assurancefor granular reasons for power and channel change

Open Caveats

Defect ID	Title
CSCvx06924	Yang/SNMP validation to be in parity with CLI for high throughput configuration
CSCvw39897	Password is visible for user accounts in Edge Browser
CSCvw55858	In ISE Endpoint Details Called Station ID is displayed as SSID
CSCvw60007	9800 Ap: debug all crashed multiple crash files with crash loop eg, nginx_pman
CSCvx02724	Able to configure ethernet vlan-tag for internal APs in CLI
CSCvx02719	Able to configure ethernet vlan-tag for internal APs in UI (W on CSCvx02724)

CSCvw87776	PSK and CCKM should not configure at the same time for WLAN
CSCvw49202	9800 Best practice UI Validation on Secure HTTP not handled properly
CSCvw63135	Not able to upload the core files on Cisco Catalyst 9800-L Wireless Controller
CSCvw84280	Client is getting connected without enabling aes/tkip cipher for WPA security
CSCvw67337	Time Zone is not updating in EWC platforms

Resolved Caveats

Defect ID	Title
CSCvw89218	Web UI validation for dot11 options in high throughput page needs to be implemented with CLI behavior
CSCvw33112	Unable to configure default easy psk wlan in Japanese
CSCvw56501	Umbrella: Getting an error message while deleting Registration Token
CSCvw39891	No option to enable Easy-PSK in Auth Key Management
CSCvw48905	Webpage loading issue in Threat Defense page
CSCvw34169	Unable to disable Best Channel Width in Best Practices
CSCvw98445	Webui - Threshold information is not showing in Temperature Tooltip
CSCvw82747	Database Memory Leak detected after enabling Umbrella Registration Token
CSCvw47728	Unable to see Auth Key Management parameters in WPA3
CSCvw93332	In LLDP neighbors page on Clicking "click here" option in to enable LLDP, it redirects to dashboard
CSCvw90384	Flex NAT/PAT should enable only after enabling Local Switching
CSCvx05194	Kendo upgrade : Checkboxstatus for WLAN PSK incorrect
CSCvw49781	Authentication Key Details data not found in Administration->Time
CSCvw51771	EWLC - UI issues observed in SNMP page

CSCvw36834	Button overlap observed in country code page - Japanese locale
CSCvw49046	9800 - Access points page details are hidden and cannot be viewed completely
CSCvw37154	Unable to configure wlan in Chrome and Edge Browser
CSCvw54792	Webpage loading issue observed in Policy Page
CSCvw52922	WLAN Easy-PSK Layer 3 profile creation gets failed in Japanese
CSCvw66688	When updating Packet capture name, new packet capture gets created instead of updating existing name
CSCvw74976	Unable to map layer2 security parameter in policy page
CSCvw97402	404 Not Found Error showing most of the links in Online help content
CSCvx02828	Not able to apply Client Exclusion Policies properly
CSCvx03669	MESH PSK: Cancel/Apply button to edit changes in Keys Configuration hidden behind scroll
CSCvw29281	Username is showing as 'webui' by default at the time of logging in
CSCvw82663	When trying to update radio setting in GUI , an error message is pop's up
CSCvw96999	In Switch/eWC/eWLC DHCP Configured in CLI are not reflecting properly in WebUI
CSCvw87235	In AAA Wizard Advanced, only Basic settings can be seen - EWC platforms
CSCvw69154	Preferred Active cannot be configured in EWC
CSCvw38909	Alignment issue in controller Japanese in chrome and edge browser
CSCvw34873	Dark Mode - Footer background issue in Licensing page
CSCvw29269	Controller is logging off automatically after deleting any user account from User Admin in JA
CSCvw60065	Easy-PSK option should be hide in EWC platforms
CSCvw47601	Unable to Enable Lobby admin access in WLAN
CSCvw29392	Username is predefined in eWLC after upgrading to 17.5
CSCvw53503	Lobby admin access check boxis disabled automatically in wlan profile page even after enabling it

CSCvw97495	Client is connecting via 11ac protocol even when it is disabled
CSCvw38916	Does not show SUCCESS/FAILURE when fixing in Disable Management over Wireless

CHAPTER **3**

New Features

Image Upgrade Data Models for Controller

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_IU_01	Verify whether AP image gets predownloaded or not	Netconf programmable support for ap image predownload	Passed	
EWCJ175S_IU_02	Verify whether AP image predownload completed or not	Netconf programmable support for ap image predownload with SSO Switchover	Passed	

EWCJ175S_IU_03	Verify whether AP image predownload abort or not	Netconf programmable support for ap image predownload abort	Passed	
EWCJ175S_IU_04	Verify AP image predownload statistics	Netconf programmable support for ap image predownload statistics	Passed	
EWCJ175S_IU_05	Verify whether rollback, rollback id details correct or not	Netconf programmable support for show install rollback, rollback id	Passed	
EWCJ175S_IU_06	Verify rollback profile information correct or not	Netconf programmable support for show install profile, profile <profile name>	Passed	
EWCJ175S_IU_07	Verify AP image and AP image file summary correct or not	Netconf programmable support for show ap image, show ap image file summary	Passed	
EWCJ175S_IU_08	Verify whether AP upgrade image details showing correctly or not	Netconf programmable support for show ap upgrade, show ap upgrade summary, show ap upgrade name <report-name>	Passed	
EWCJ175S_IU_09	Verify whether async notification from netconf server generating or not when ap predownload is initiated	Predownload async notification - INSTALL_AP_IMAGE	Passed	
EWCJ175S_IU_10	Verify whether async notification from netconf server generating or not when ap predownload is inprogress	Predownload async notification - INSTALL_AP_IMAGE	Passed	

EWCJ175S_IU_11	Verify whether AP image gets predownloaded or not	Netconf programmable support for ap image predownload	Passed	
EWCJ175S_IU_12	Verify whether AP image predownload completed or not	Netconf programmable support for ap image predownload with SSO Switchover	Passed	
EWCJ175S_IU_13	Verify whether AP image predownload abort or not	Netconf programmable support for ap image predownload abort	Passed	
EWCJ175S_IU_14	Verify AP image predownload statistics	Netconf programmable support for ap image predownload statistics	Passed	
EWCJ175S_IU_15	Verify whether rollback, rollback id details correct or not	Netconf programmable support for show install rollback, rollback id	Passed	
EWCJ175S_IU_16	Verify rollback profile information correct or not	Netconf programmable support for show install profile, profile <profile name>	Passed	
EWCJ175S_IU_17	Verify AP image and AP image file summary correct or not	Netconf programmable support for show ap image, show ap image file summary	Passed	
EWCJ175S_IU_18	Verify whether AP upgrade image details showing correctly or not	Netconf programmable support for show ap upgrade, show ap upgrade summary, show ap upgrade name <report-name>	Passed	
EWCJ175S_IU_19	Verify whether async notification from netconf server generating or not when ap predownload is initiated	Predownload async notification - INSTALL_AP_IMAGE	Passed	

| EWCJ175S_IU_20 | Verify whether async notification from netconf server generating or not when ap predownload is inprogress | Predownload async notification - INSTALL_AP_IMAGE_ | Passed | |

11ax Advanced traffic based scheduler for scheduling SU OFDMA and MU traffic on 9105/9115/9120

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_11ax_ATBS_01	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configue 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ175S_11ax_ATBS_02	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	
EWCJ175S_11ax_ATBS_03	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Failed	CSCvx06924
EWCJ175S_11ax_ATBS_04	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ175S_11ax_ATBS_05	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ175S_11ax_ATBS_06	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	

EWCJl75S_1lax_ATBS_07	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWCJl75S_1lax_ATBS_08	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Failed	CSCvw87776
EWCJl75S_1lax_ATBS_09	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJl75S_1lax_ATBS_10	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJl75S_1lax_ATBS_11	Modify spatial stream config to 1 stream and monitor OFDMA statistics.	To modify spatial stream config to 1 stream and monitor OFDMA statistics.	Passed	
EWCJl75S_1lax_ATBS_12	Modify spatial stream config to 2 streams and monitor OFDMA statistics.	To modify spatial stream config to 2 streams and monitor OFDMA statistics.	Passed	
EWCJl75S_1lax_ATBS_13	Modify spatial stream config to 3 streams and monitor OFDMA statistics.	To modify spatial stream config to 3 streams and monitor OFDMA statistics.	Passed	
EWCJl75S_1lax_ATBS_14	Modify spatial stream config to 4 streams and monitor OFDMA statistics.	To modify spatial stream config to 4 streams and monitor OFDMA statistics.	Passed	
EWCJl75S_1lax_ATBS_15	Enable videostream and monitor DL/UL OFDMA statistics	To enable videostream and monitor DL/UL OFDMA statistics	Passed	
EWCJl75S_1lax_ATBS_16	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	

EWCJ175S_11ax_ATBS_17	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configue 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	
EWCJ175S_11ax_ATBS_18	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 2.4Ghz band.	Passed	
EWCJ175S_11ax_ATBS_19	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWCJ175S_11ax_ATBS_20	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWCJ175S_11ax_ATBS_21	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWCJ175S_11ax_ATBS_22	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWCJ175S_11ax_ATBS_23	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWCJ175S_11ax_ATBS_24	Verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ175S_11ax_ATBS_25	Verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ175S_11ax_ATBS_26	Connect upto 8 clients and monitor DL/UL 11ax MU statistics	To connect upto 8 clients and monitor DL/UL 11ax MU statistics	Passed	

EWCJl75S_11ax_ATBS_27	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	
EWCJl75S_11ax_ATBS_28	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic	Passed	
EWCJl75S_11ax_ATBS_29	Monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic for AP models - 9105, 9115, 9120	To monitor 11ax traffic over mixed mode with both OFDMA and SU, MU traffic - 9105, 9115, 9120	Passed	

11ax OFDMA Support 8 Users UL 16 Users DL

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_OFDMA_01	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configue 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ175S_OFDMA_02	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	
EWCJ175S_OFDMA_03	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ175S_OFDMA_04	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ175S_OFDMA_05	Verifying the details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	

EWCJ175S_OFDMA_06	Verifying the details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWCJ175S_OFDMA_07	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWCJ175S_OFDMA_08	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	
EWCJ175S_OFDMA_09	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	
EWCJ175S_OFDMA_10	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWCJ175S_OFDMA_11	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWCJ175S_OFDMA_12	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ175S_OFDMA_13	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ175S_OFDMA_14	Connect upto 16 clients and monitor DL/UL OFDMA statistics	To connect upto 16 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ175S_OFDMA_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	
EWCJ175S_OFDMA_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	

EWCJ175S_OFDMA_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	
EWCJ175S_OFDMA_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	
EWCJ175S_OFDMA_19	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	
EWCJ175S_OFDMA_20	Check OFDMA stats with roaming client scenario in different eWC with different 11 ax Aps	To check OFDMA stats with roaming client scenario	Passed	
EWLCJ175S_OFDMA_01	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configue 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ175S_OFDMA_02	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	
EWLCJ175S_OFDMA_03	Verifying details with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ175S_OFDMA_04	Verifying details with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ175S_OFDMA_05	Verifying the details with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ175S_OFDMA_06	Verifying the details with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	

EWLCJ175S_OFDMA_07	Verify details by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ175S_OFDMA_08	Check OFDMA support for AP configured in Local mode.	To check OFDMA support for AP configured in Local mode.	Passed	
EWLCJ175S_OFDMA_09	Check OFDMA support for AP configured in Flex-connect mode.	To check OFDMA support for AP configured in Flex-connect mode.	Passed	
EWLCJ175S_OFDMA_10	Check OFDMA support for AP configured in Bridge mode.	To check OFDMA support for AP configured in Bridge mode.	Passed	
EWLCJ175S_OFDMA_11	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ175S_OFDMA_12	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ175S_OFDMA_13	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ175S_OFDMA_14	Connect upto 16 clients and monitor DL/UL OFDMA statistics	To connect upto 16 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ175S_OFDMA_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	
EWLCJ175S_OFDMA_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	
EWLCJ175S_OFDMA_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	

EWLCJl75S_OFDMA_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	
EWLCJl75S_OFDMA_19	Enable videostream and monitor DL/UL OFDMA statistics	To enable videostream and monitor DL/UL OFDMA statistics	Passed	
EWLCJl75S_OFDMA_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	
EWLCJl75S_OFDMA_21	Check OFDMA stats with roaming client scenario in different eWLC with different 11 ax Aps	To check OFDMA stats with roaming client scenario	Passed	

Called Station ID with AP Ethernet MAC

Logical ID	Title	Description	Status	Defect ID
EWCJl75S_CSIAEM_01	Configure radius-server wireless attribute call station id for authentication and accounting with "policy-tag-name"	To Configure radius-server wireless attribute call station id for authentication and accounting with "policy-tag-name"	Failed	CSCvw55858
EWCJl75S_CSIAEM_02	Configure radius-server wireless attribute call station id for authentication and accounting with "flex-profile-name	To Configure radius-server wireless attribute call station id for authentication and accounting with "flex-profile-name	Passed	
EWCJl75S_CSIAEM_03	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	

EWCJ175S_CSIAEM_04	Configure radius-server wireless attribute call station id for authentication and accounting	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWCJ175S_CSIAEM_05	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWCJ175S_CSIAEM_06	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWCJ175S_CSIAEM_07	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWCJ175S_CSIAEM_08	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWCJ175S_CSIAEM_09	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWCJ175S_CSIAEM_10	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWCJ175S_CSIAEM_11	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWCJ175S_CSIAEM_12	HA active to stanby config impact	To verify config impact HA active to stanby	Passed	
EWCJ175S_CSIAEM_13	active to stanby to active config impact	To verify config impact when active to stanby to active	Passed	

EWCJ175S_CSIAEM_14	Change mac address format in atrribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in atrribute and check config	Passed	
EWCJ175S_CSIAEM_15	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWCJ175S_CSIAEM_16	Change station id case and verify config impact"radius-server attribute wireless authentication callstationIdCase upper/lower"	To Change station id case and verify config impact	Passed	
EWLCJ175S_CSIAEM_01	Configure radius-server wireless attribute call station id for authentication and accounting with "policy-tag-name"	To Configure radius-server wireless attribute call station id for authentication and accounting with "policy-tag-name"	Passed	
EWLCJ175S_CSIAEM_02	Configure radius-server wireless attribute call station id for authentication and accounting with "flex-profile-name	To Configure radius-server wireless attribute call station id for authentication and accounting with "flex-profile-name	Passed	
EWLCJ175S_CSIAEM_03	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWLCJ175S_CSIAEM_04	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWLCJ175S_CSIAEM_05	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	

EWLCJ175S_CSIAEM_06	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWLCJ175S_CSIAEM_07	Configure radius-server wireless attribute call station id for authentication and accounting	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWLCJ175S_CSIAEM_08	Configure radius-server wireless attribute call station id for authentication	To Configure radius-server wireless attribute call station id for authentication	Passed	
EWLCJ175S_CSIAEM_09	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWLCJ175S_CSIAEM_10	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWLCJ175S_CSIAEM_11	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWLCJ175S_CSIAEM_12	HA active to stanby config impact	To verify config impact HA active to stanby	Passed	
EWLCJ175S_CSIAEM_13	active to stanby to active config impact	To verify config impact when active to stanby to active	Passed	
EWLCJ175S_CSIAEM_14	Change mac address format in atrribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in atrribute and check config	Passed	
EWLCJ175S_CSIAEM_15	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	

| EWLCJl75S_CSIAEM_16 | Change station id case and verify config impact"radius-server attribute wireless authentication callstationIdCase upper/lower" | To Change station id case and verify config impact | Passed | |

RRM assurance for granular reasons for power and channel change

Logical ID	Title	Description	Status	Defect ID
EWCJl75S_RRM_Assurance_01	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWCJl75S_RRM_Assurance_02	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	
EWCJl75S_RRM_Assurance_03	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	
EWCJl75S_RRM_Assurance_04	Configure channel parameters for 5ghz band slot 2 and monitor in DNAC	To configure channel parameters for 5ghz band slot 2 and monitor in DNAC	Passed	
EWCJl75S_RRM_Assurance_05	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	
EWCJl75S_RRM_Assurance_06	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	

EWCJ175S_RRM_Assurance_07	Channel updation and monitor assurance in DNAC	To perform channel updation and monitor assurance in DNAC	Passed	
EWCJ175S_RRM_Assurance_08	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	
EWCJ175S_RRM_Assurance_09	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	
EWCJ175S_RRM_Assurance_10	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWCJ175S_RRM_Assurance_11	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWCJ175S_RRM_Assurance_12	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWCJ175S_RRM_Assurance_13	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWCJ175S_RRM_Assurance_14	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	
EWCJ175S_RRM_Assurance_15	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWCJ175S_RRM_Assurance_16	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWCJ175S_RRM_Assurance_17	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	

EWCJ175S_RRM_Assurance_18	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	
EWLCJ175S_RRM_ASSURANCE_01	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWLCJ175S_RRM_ASSURANCE_02	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	
EWLCJ175S_RRM_ASSURANCE_03	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	
EWLCJ175S_RRM_ASSURANCE_04	Configure channel parameters for 5ghz band slot 2 and monitor in DNAC	To configure channel parameters for 5ghz band slot 2 and monitor in DNAC	Passed	
EWLCJ175S_RRM_ASSURANCE_05	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	
EWLCJ175S_RRM_ASSURANCE_06	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	
EWLCJ175S_RRM_ASSURANCE_07	Channel updation and monitor assurance in DNAC	To perform channel updation and monitor assurance in DNAC	Passed	
EWLCJ175S_RRM_ASSURANCE_08	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	

EWLCJ17S_RRM_ASSURANCE_09	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	
EWLCJ17S_RRM_ASSURANCE_10	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWLCJ17S_RRM_ASSURANCE_11	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWLCJ17S_RRM_ASSURANCE_12	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWLCJ17S_RRM_ASSURANCE_13	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWLCJ17S_RRM_ASSURANCE_14	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	
EWLCJ17S_RRM_ASSURANCE_15	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWLCJ17S_RRM_ASSURANCE_16	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWLCJ17S_RRM_ASSURANCE_17	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	
EWLCJ17S_RRM_ASSURANCE_18	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	

Adapative Load EDCA Parameter Giga School

Logical ID	Title	Description	Status	Defect ID
EWLCJ174S_ALB_01	Validate the EDCA parameter with wmm-default profile	To associate the client and verifying EDCA parameter in wmm-default profile	Passed	
EWLCJ174S_ALB_02	Validate the EDCA parameter with custom-voice profile	To associate the client and verifying EDCA parameter in custom-voice profile	Passed	
EWLCJ174S_ALB_03	Validate the EDCA parameter with optimized-video-voice profile	To associate the client and verifying EDCA parameter in optimized-video-voice profile	Passed	
EWLCJ174S_ALB_04	Validate the EDCA parameter with optimized-voice profile	To associate the client and verifying EDCA parameter in optimized-voice profile	Passed	
EWLCJ174S_ALB_05	Validate the EDCA parameter with svp-voice profile	To associate the client and verifying EDCA parameter in svp-voice profile	Passed	
EWLCJ174S_ALB_06	Validate the EDCA parameter with fastlane profile	To associate the client and verifying EDCA parameter in fastlane profile	Passed	
EWLCJ174S_ALB_07	Associate the windows client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ174S_ALB_08	Associate the Android client and verify the EDCA parameter in 9130 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ174S_ALB_09	Associate the MAC client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	

EWLCJ174S_ALB_10	Validate the EDCA parameter with different profile in 2.4GHz frequency	To associate the client and verifying EDCA parameter for 2.4GHZ frequency	Passed	
EWLCJ174S_ALB_11	Validate the EDCA parameter with different profile in 5GHz frequency	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ174S_ALB_12	Validate the EDCA parameter with single client	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ174S_ALB_13	Perform Inter roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ174S_ALB_14	Perform Intra roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ174S_ALB_15	Perform controller reload and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	

Umbrella Enhancements

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_UE_01	Verifying ewlc registered with Umbrella Dashboard	To verify ewlc registered with Umbrella Dashboard	Passed	
EWLCJ175S_UE_02	Verifying syslogs/error messages related to splitdns after changing AP from Local mode to Flex mode	To verify syslogs/error messages related to splitdns when AP is in Flex mode	Passed	
EWLCJ175S_UE_03	Configure Umbrella Parameter Map through CLI and verify details in GUI	To configure Umbrella Parameter Map through CLI and verifing the same in GUI	Passed	

EWLCJ175S_UE_04	Enabling or disabling DNScrypt in GUI and CLI and verify the details	To veify DNScrypt enabling or disabling through GUI and CLI	Passed	
EWLCJ175S_UE_05	Configure whitelist wth patterns, set up AP in flex and connect end devices (like Windows, Android etc) to Umbrella enabled WLAN profile	To configure whitelist with patterns, set up AP in flex and to connect any client to Umbrella enabled WLAN profile	Passed	
EWLCJ175S_UE_06	Configure whitelist wth patterns, set up AP in flex and connect end devices to Umbrella enabled WLAN profile and verify packets sent to clients and verify there are no errors/syslogs	To configure whitelist with patterns, set up AP in flex and to connect any client to Umbrella enabled WLAN profile and verify packets sent to clients and verify there are no errors/syslogs	Passed	
EWLCJ175S_UE_07	Configure custom parameter maps, set up ap in flex, configure whitelist with patterns, check multi-profile splitdns works or not and check no error/syslog messages	To configure custom parameter maps, set up ap in flex, configure whitelist with patterns, check multi-profile splitdns works or not and verify no syslogs/no error messages	Passed	
EWLCJ175S_UE_08	Verify show commands on controller: Configure controller in flex mode, multiple pmaps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	To verify show commands on controller: Configure controller in flex mode, multiple pmaps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	Passed	

EWLCJ175S_UE_09	Verify client connected or not when global parameter enabled in Local Mode	To verify whether client connected or not when global parameter enabled in Local Mode	Passed	
EWLCJ175S_UE_10	Verify multiple clients connected or not when global parameter and multiple whitelists configured in Local mode	To verify whether multiple clients connected or not when global parameter and multiple whitelists configured in Local mode	Passed	
EWLCJ175S_UE_11	Verify multiple clients connected or not when custom global parameter and multiple whitelists configured in Local mode	To verify whether multiple clients connected or not when custom global parameter and multiple whitelists configured in Local mode	Passed	
EWLCJ175S_UE_12	Verify show commands on controller: Configure controller in local mode, multiple pmaps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	To verify show commands on controller: Configure controller in local mode, multiple pmaps, multiple whitelists, IPv4 server list, IPv6 server list, join clients. Check output is correct. Same check on AP.	Passed	
EWLCJ175S_UE_13	Configure regex param-map with various patterns. Check that the whitelist cannot be associated to an Umbrella profile if it contains unsupported patterns for wireless (config validation)	To configure regex param-map with various patterns. Check that the whitelist cannot be associated to an Umbrella profile if it contains unsupported patterns for wireless (config validation)	Passed	

EWLCJ175S_UE_14	Reload: Configure multiple pmps and multiple local domains, reload the controller and verify configured data exists or not	Reload: To configure multiple pmps and multiple local domains, reload the controller and to verify configured data exists or not	Passed	
EWLCJ175S_UE_15	Reload: Configure multiple pmps and multiple local domains, reload the controller with 17.5 build and verify configured data exists or not in 17.4 build	Reload: To configure multiple pmps and multiple local domains, reload the controller with 17.5 build and to verify configured data exists or not in 17.4 build	Passed	
EWLCJ175S_UE_16	Reload: configure resolver ipv4 address, reload the controller, verify there are no erros	Reload: To configure resolver ipv4 address, reload the controller, to verify there are no erros	Passed	

11ax BSS Coloring OBSS PD on 9105/9115/9120 APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_BSS_01	Enable Global OBSS PD for 5ghz band	To verify wheather the OBBSS PD enable or not for 5 GHz band	Passed	
EWLCJ175S_BSS_02	Disable Global OBSS PD for 5ghz band	To Check wheather the OBBSS PD disable or not for 5 GHz	Passed	
EWLCJ175S_BSS_03	Enable Global OBSS PD for 2.4 ghz band	To verify wheather the OBBSS PD enable or not for 2.4 Ghz GHz band	Passed	
EWLCJ175S_BSS_04	Disable Global OBSS PD for 2.4 ghz band	To Check wheather the OBBSS PD disable or not for 2.4 GHz	Passed	

EWLCJ175S_BSS_05	Set OBSS PD value for 5 GHZ band	To verify wheather the values set for 5 Ghz band or not	Passed	
EWLCJ175S_BSS_06	Set OBSS PD value for 2.4 GHZ band	To verify wheather the values set for 2.4 ghz band or not	Passed	
EWLCJ175S_BSS_07	Creating RF Profile with OBSS PD enabled for 5/2.4 GHz band	To Validate wheather RF Profile cretaed with OBSS PD enable for 5/2.4 GHz band	Passed	
EWLCJ175S_BSS_08	Disabling OBSS PD in RF Profile	To Validate wheather RF Profile is created with OBSS PD enable for 5/2.4 GHz band	Passed	
EWLCJ175S_BSS_09	Viewing OBSS PD supports in different AP models	To checking the OBSS PD supports in different AP models	Passed	
EWLCJ175S_BSS_10	Configuring BSS color details in AP & controller CLIs	To Verify Configured color details is reflected in AP and Controller CLIs	Passed	
EWLCJ175S_BSS_11	Checking the BSS color details are retained after AP and Controller reload	To Check whether the BSS color retained after AP & Controller reload	Passed	
EWLCJ175S_BSS_12	Verify enable/disable of BSS coloring on radio is reflected in management packets	To verify wheather the BSS color is reflected in Management packets or not	Passed	
EWLCJ175S_BSS_13	Verifying OBSS PD with inter roming client using different radio	To check whether OBSS PD is enable or not , when different radio clients are roaming between controllers	Passed	

EWLCJ175S_BSS_14	Verifying OBSS PD enabled with inter roming client using same radio	To check whether OBSS PD enable or not , when same radio clients are roaming between controllers	Passed	
EWLCJ175S_BSS_15	Verifying OBSS PD enabled with Intra client roaming by using 9115AP	To verify whether OBSS PD enabled with client roaming between AP's or not	Passed	
EWLCJ175S_BSS_16	Changing 9115 AP mode from local to Flex connect & check the BSS coloring Configuration	To change the mode of AP from local mode to Flexconnect mode and check the BSS coloring configuration in 9115 Ap	Passed	
EWLCJ175S_BSS_17	Changing 9115 AP mode from flex to local & check the BSS coloring Configuration	To change the mode of AP from flex mode to local mode and check the BSS coloring configuration in 9115 Ap	Passed	

Easy PSK:WLAN Client Onboarding w/o registration

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_EPSK_01	Verify you can configure a wlan with easy psk feature on it when aaa override is set on the associated policy profile. Verify no syslog is thrown.	To Verify whether you can configure a wlan with easy psk feature on it when aaa override is set on the associated policy profile. Verify no syslog is thrown.	Passed	
EWLCJ175S_EPSK_02	Verify that if you configure a wlan with easy psk feature and its associated policy profile does not have the aaa override set, a syslog is thrown.	To Verify that whether you configure a wlan with easy psk feature and its associated policy profile does not have the aaa override set, a syslog is thrown.	Passed	

EWLCJ175S_EPSK_03	Verify that it is not possible to configure Easy PSK if one of the following option is set on the same wlan: mPSK PSK key WPA3 CCKM dot1x	To Verify that it is not possible to configure Easy PSK if one of the following option is set on the same wlan: mPSK PSK key WPA3 CCKM dot1x	Passed	
EWLCJ175S_EPSK_04	Verify that it is not possible to configure any of the following option on a wlan where Easy PSK is enabled mPSK PSK key WPA3 CCKM dot1x	To Verify that it is not possible to configure any of the following option on a wlan where Easy PSK is enabled mPSK PSK key WPA3 CCKM dot1x	Passed	
EWLCJ175S_EPSK_05	Verify that when configuring the feature on a wlan that is pushed on an AP configured in flex mode, a syslog is thrown.	To Verify that when configuring the feature on a wlan that is pushed on an AP configured in flex mode, a syslog is thrown.	Passed	
EWLCJ175S_EPSK_06	Verify that the feature can't be configured on a EWC device	To Verify that the feature can't be configured on a EWC device	Passed	
EWLCJ175S_EPSK_07	Verify that if the feature is configured together with local authentication, a syslog is thrown.	To Verify that if the feature is configured together with local authentication, a syslog is thrown.	Passed	
EWLCJ175S_EPSK_08	Verify that if the feature is configured together with local switching, a syslog is thrown.	To Verify that if the feature is configured together with local switching, a syslog is thrown.	Passed	
EWLCJ175S_EPSK_09	With a valid configuration, save the configuration and perform a reboot. Verify that the configuration is kept and valid, and no syslog is thrown.	To veify with a valid configuration, save the configuration and perform a reboot. Verify that the configuration is kept and valid, and no syslog is thrown.	Passed	

EWLCJ175S_EPSK_10	Remove the Easy PSK feature from the configured wlan in the previous test through yang. Verify that the same config can be observed in the CLI.	To Remove the Easy PSK feature from the configured wlan in the previous test throug yang. Verify that the same config can be observed in the CLI.	Passed	
EWLCJ175S_EPSK_11	Configure a new wlan with easy PSK through SNMP. Verify that the configuration is effective through CLI. Remove the easy PSK from the wlan and verify in the CLI that the same config is no longer applied.	To Configure a new wlan with easy PSK through SNMP. Verify that the configuration is effective through CLI. Remove the easy PSK from the wlan and verify in the CLI that the same config is no longer applied.	Passed	
EWLCJ175S_EPSK_12	Configure a wlan with easy PSK through CLI. Verify that the configuration is effective through SNMP.	To Configure a wlan with easy PSK through CLI. Verify that the configuration is effective through SNMP.	Passed	
EWLCJ175S_EPSK_13	Configure a wlan with Easy PSK feature through the CLI. Verify that you can get the same configuration through yang.	To Configure a wlan with Easy PSK feature through the CLI. Verify that you can get the same configuration through yang.	Passed	

EWLCJ175S_EPSK_14	Configure a WLAN with easy PSK, the Radius with two valid PSKs. Connect one client with the first PSK. Verify the exchange between the controller and the Radius with a capture (verify new AAA attributes are filled correctly). Verify that the client can ping the gateway	To Configure a WLAN with easy PSK, the Radius with two valid PSKs. Connect one client with the first PSK. Verify the exchange between the controller and the Radius with a capture (verify new AAA attributes are filled correctly). Verify that the client can ping the gateway	Passed	
EWLCJ175S_EPSK_15	Following the previous test, disconnect the client and connect it again using the second PSK. Verify again the Radius exchange and the client can reach Run state and can ping the gateway.	Following the previous test, disconnect the client and connect it again using the second PSK. Verify again the Radius exchange and the client can reach Run state and can ping the gateway.	Passed	
EWLCJ175S_EPSK_16	Configure 16 wlans with easy PSK enabled. Connect one client to each WLAN. Verify each client reaches Run state and can ping the gateway.	To Configure 16 wlans with easy PSK enabled. Connect one client to each WLAN. Verify each client reaches Run state and can ping the gateway.	Passed	
EWLCJ175S_EPSK_17	Configure an easy psk wlan using a aaa server that is not reacheable. Verify that the client can't reach Run state and is deleted.	To Configure an easy psk wlan using a aaa server that is not reacheable. Verify that the client can't reach Run state and is deleted.	Passed	

| EWLCJ175S_EPSK_18 | Configure a wlan with easy psk and webauth on mab failure. Make sure that the webauth on mab failure is not applied in case the client is connecting with a non supported passphrase. | To Configure a wlan with easy psk and webauth on mab failure. Make sure that the webauth on mab failure is not applied in case the client is connecting with a non supported passphrase. | Passed | |

Application Experience Support on IOS-XE Wireless Platforms

Logical ID	Title	Description	Status	Defect ID
EWLCJ174S_AES_01	Creating a policy profile in eWLC 9800-40 and check if the profile is shown in Application visibility page	To create a policy profile in 9800-40 eWLC and check if the policy profile is shown in the application viibility page or not	Passed	
EWLCJ174S_AES_02	Creating a policy profile in eWLC 9800-80 and check if the profile is shown in Application visibility page	To create a policy profile in 9800-80 eWLC and check if the policy profile is shown in the application viibility page or not	Passed	
EWLCJ174S_AES_03	Creating a policy profile in eWLC 9800-CL and check if the profile is shown in Application visibility page	To create a policy profile in 9800-CL eWLC and check if the policy profile is shown in the application viibility page or not	Passed	
EWLCJ174S_AES_04	Mapping the created policy profile under Application visibility in eWLC 9800-40 and check the behaviour	To map the created policy profile under Application visibilityin eWLC 9800-40 and check the behaviour .	Passed	

EWLCJ174S_AES_05	Mapping the created policy profile under Application visibility in eWLC 9800-80 and check the behaviour	To map the created policy profile under Application visibilityin eWLC 9800-80 and check the behaviour .	Passed	
EWLCJ174S_AES_06	Mapping the created policy profile under Application visibility in eWLC 9800-CL and check the behaviour	To map the created policy profile under Application visibilityin eWLC 9800-CL and check the behaviour .	Passed	
EWLCJ174S_AES_07	Enabling External Collector address for the policy profile mapped in Application visibility and checking the behaviour	To enabling External Collector address for the policy profile mapped in Application visibility and checking the behaviour	Passed	
EWLCJ174S_AES_08	Checking if the local Collector in the Application visbility works for the eWLC which works in Standalone mode	To check if the local collecctor for the application visibility works or not for the eWLC which works on standalone mode	Passed	
EWLCJ174S_AES_09	Checking if the local Collector in the Application visbility works for the eWLC which works in Active mode	To check if the local collecctor for the application visibility works or not for the eWLC which works on Active mode	Passed	
EWLCJ174S_AES_10	Checking if the local Collector in the Application visbility works for the eWLC which is in HA mode	To check if the local collecctor for the application visibility works or not for the eWLC which is in HA mode	Passed	

Enabling Packet trace and conditional debug in eWLC 9800-CL

Logical ID	Title	Description	Status	Defect ID

EWLCJ175S_PT_01	Enabling Packet trace and conditional debug in eWLC 9800-40	To check if the packet trace and conditional debug is enabled on 9800-40 or not	Passed	
EWLCJ175S_PT_02	Enabling Packet trace and conditional debug in eWLC 9800-80	To check if the packet trace and conditional debug is enabled on 9800-80 or not	Passed	
EWLCJ175S_PT_03	Enabling Packet trace and conditional debug in eWLC 9800-CL	To check if the packet trace and conditional debug is enabled on 9800-CL or not	Passed	
EWLCJ175S_PT_04	Enabling Packet trace and conditional debug in eWLC 9800 with HA setup	To check if the packet trace and conditional debug is enabled or not	Passed	
EWLCJ175S_PT_05	Verifying if the packet trace for 9800-40 are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800-40 or not	Passed	
EWLCJ175S_PT_06	Verifying if the packet trace for 9800-80 are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800-80 or not	Passed	
EWLCJ175S_PT_07	Verifying if the packet trace for 9800-CL are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800-CL or not	Passed	
EWLCJ175S_PT_08	Verifying if the packet trace for 9800 HA are captured and the details shown correctly	To check if the packet trace is enabled and the configured command output are shown for the eWLC 9800 HA or not	Passed	

| EWLCJ175S_PT_09 | Upgrading the eWLC after configuring the Packet trace and conditional debug command and check | To check if the configured packet trace and conditional debug are same even after the upgrade of the eWLC | Passed | |
| EWLCJ175S_PT_10 | Downgrading the eWLC after configuring the Packet trace and conditional debug command and check | To check if the configured packet trace and conditional debug are same even after the downgrade of the eWLC | Passed | |

Client Debug Bundle

Logical ID	Title	Description	Status	Defect ID
EWCJ174S_CDB_01	Verify the tech wireless command	To Verify the tech wireless command	Passed	
EWCJ174S_CDB_02	Verify the debugs error , events, info , payload , client details , keep alive in 9115	To Verify the debugs error , events, info , payload , client details , keep alive in 9115	Passed	
EWCJ174S_CDB_03	Verify the debugs error , events, info , payload , client details , keep alive in 9117	To Verify the debugs error , events, info , payload , client details , keep alive in 9117	Passed	
EWCJ174S_CDB_04	Verify the debugs error , events, info , payload , client details , keep alive in 9120	To Verify the debugs error , events, info , payload , client details , keep alive in 9120	Passed	
EWCJ174S_CDB_05	Verify the debugs error , events, info , payload , client details , keep alive in 9130	To Verify the debugs error , events, info , payload , client details , keep alive in 9130	Passed	

EWCJ174S_CDB_06	Verify mobility stats on Controller with different MAC clients	To Verify mobility stats on Controller with different MAC clients	Passed	
EWCJ174S_CDB_07	Verify mobility stats on Controller with different Android clients	To Verify mobility stats on Controller with different Android clients	Passed	
EWCJ174S_CDB_08	Verify mobility stats on Controller with different Windows clients	To Verify mobility stats on Controller with different Windows clients	Passed	
EWCJ175S_Reg_268	Verify the tech wireless command	To Verify the tech wireless command	Passed	
EWCJ175S_Reg_269	Verify the debugs error , events, info , payload , client details , keep alive in 9115	To Verify the debugs error , events, info , payload , client details , keep alive in 9115	Passed	
EWCJ175S_Reg_270	Verify the debugs error , events, info , payload , client details , keep alive in 9117	To Verify the debugs error , events, info , payload , client details , keep alive in 9117	Passed	
EWCJ175S_Reg_271	Verify the debugs error , events, info , payload , client details , keep alive in 9120	To Verify the debugs error , events, info , payload , client details , keep alive in 9120	Passed	
EWCJ175S_Reg_272	Verify the debugs error , events, info , payload , client details , keep alive in 9130	To Verify the debugs error , events, info , payload , client details , keep alive in 9130	Passed	
EWCJ175S_Reg_273	Verify mobility stats on Controller with different MAC clients	To Verify mobility stats on Controller with different MAC clients	Passed	

EWCJ175S_Reg_274	Verify mobility stats on Controller with different Android clients	To Verify mobility stats on Controller with different Android clients	Passed	
EWCJ175S_Reg_275	Verify mobility stats on Controller with different Windows clients	To Verify mobility stats on Controller with different Windows clients	Passed	

ICAP Support for C9130 fo 8 users

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_ICAP_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 EWLC	Passed	
EWLCJ175S_ICAP_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 EWLC	Passed	
EWLCJ175S_ICAP_03	Packet capture for Android client using Intellingent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWLCJ175S_ICAP_04	Packet capture for Windows JOS client using Intellingent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWLCJ175S_ICAP_05	Packet capture for IOS client using Intellingent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	

EWLCJ175S_ICAP_06	Packet capture for Mac OS client using Intellingent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	
EWLCJ175S_ICAP_07	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in EWLC	Passed	
EWLCJ175S_ICAP_08	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in EWLC	Passed	
EWLCJ175S_ICAP_09	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in EWLC	Passed	
EWLCJ175S_ICAP_10	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-webconsent	Passed	
EWLCJ175S_ICAP_11	Packet capture for Anyconnect client using Intellingent Capture option in APgroup page	To verify the packet capture for Anyconnect client using Intelligent capture in APgroup page	Passed	
EWLCJ175S_ICAP_12	Packet capture for Windows JOS client using Intellingent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWLCJ175S_ICAP_13	Packet capture for Android client using Intellingent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	

EWLCJ175S_ICAP_14	Packet capture for iOS client using Intellingent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	
EWLCJ175S_ICAP_15	Packet capture for MacOS client using Intellingent Capture option in AP page	To verify the packet capture for MacOS client using Intelligent capture in AP page	Passed	
EWLCJ175S_ICAP_16	Packet capture for Anyconnect client using Intellingent Capture option in AP page	To verify the packet capture for Anyconnect client using Intelligent capture in AP page	Passed	

Capability to enable/disable 11ax features per SSID

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_CE_01	Check the 11 ax enabling or not via GUI	To verify whether the 11 ax parameters enable or not via GUI	Passed	
EWLCJ175S_CE_02	Check the 11 ax disabling or not via GUI	To verify whether the 11 ax parameters disable or not via GUI	Passed	
EWLCJ175S_CE_03	Check the 11 ax enabling or not via CLI	To verify whether the 11 ax parameters enable or not via CLI	Passed	
EWLCJ175S_CE_04	Check the 11 ax disabling or not via CLI	To verify whether the 11 ax parameters disable or not via CLI	Passed	
EWLCJ175S_CE_05	Disabling 11 ax radio and checking the client connectivity	To check the client connectivity after disabling 11 ax	Passed	
EWLCJ175S_CE_06	Checking the 11 ax parameters after AP reboot	To verify the 11 ax for after AP reboot	Passed	

EWLCJ175S_CE_07	Checking the 11 ax parameters after AP radio change	To check whether the 11 ax parameters showing or not after changing the AP radio	Passed	
EWLCJ175S_CE_08	Verifying 11 ax parameters for different AP models	To Verify the 11 ax parameters for different AP models	Passed	
EWLCJ175S_CE_09	Validating the 11ax parameters after disjoin the AP	To validate the 11 ax parameters for after Ap disjoin	Passed	
EWLCJ175S_CE_10	Verifying the 11 ax parametrs after deleting the client	To verify the 11 ax parameters for deleted client	Passed	
EWLCJ175S_CE_11	monitoring the 11 ax parameters after AP provisioning from DNAC	To check the 11 ax parameters after AP provisioning from DNAC	Passed	
EWLCJ175S_CE_12	Verifying the 11 ax parameters by deleting the SSID	To Verify the 11 ax parameters after Deleting SSID	Passed	
EWLCJ175S_CE_13	Verifying the 11 ax parameters for intra roaming client	To Verify the 11 ax parameters after client roaming between AP's	Passed	
EWLCJ175S_CE_14	Checking the 11 ax parameters for inter roaming client	To Verify the 11 ax parameters status after client roaming between controllers	Passed	
EWLCJ175S_CE_15	Verifying the 11 ax status by changing the security type	To check the11 ax parameters after changing the security type	Passed	
EWLCJ175S_CE_16	Validating the 11ax status for Virtual EWLC	To validate the 11 ax parameters for vEWLC	Passed	

HA Management Enhancements

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_HA_01	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	

EWLCJ175S_HA_02	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ175S_HA_03	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ175S_HA_04	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ175S_HA_05	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ175S_HA_06	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	
EWLCJ175S_HA_07	Enable gatway failover, verify output details and monitor devices for switchover.	To enable gatway failover, verify output details & monitor devices for switchover.	Passed	
EWLCJ175S_HA_08	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	
EWLCJ175S_HA_09	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ175S_HA_10	ISSU upgrade with HA SSO RMI	To peform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ175S_HA_11	Check ISSU downgrade with HA SSO RMI	To peform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ175S_HA_12	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ175S_HA_13	Force multiple switchover after upgrade to check if RMI link is up or not	To force multiple switchover after upgrade to check if RMI link is up or not	Passed	

EWLCJ175S_HA_14	Validate licensing information after ISSU upgrade/downgrade	To validate licensing information after ISSU upgrade/downgrade	Passed	
EWLCJ175S_HA_15	Validate licensing information after multiple switchover and reload	To validate licensing information after multiple switchover and reload	Passed	
EWLCJ175S_HA_16	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ175S_HA_17	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	
EWLCJ175S_HA_18	Configure HA SSO RMI after RP-clear & validate HA RMI parameters.	To configure HA SSO RMI after RP-clear & validate HA RMI parameters.	Passed	
EWLCJ175S_HA_19	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ175S_HA_20	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ175S_HA_21	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ175S_HA_22	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ175S_HA_23	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ175S_HA_24	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	
EWLCJ175S_HA_25	Force multiple switchover and verify AP & client association	To force multiple switchover and verify AP & client association	Passed	

Standby Monitoring Enhancements

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_SME_01	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	
EWLCJ175S_SME_02	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ175S_SME_03	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ175S_SME_04	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ175S_SME_05	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ175S_SME_06	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ175S_SME_07	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	
EWLCJ175S_SME_08	SSH to standby console via AAA authentication	To SSH to standby console via AAA authentication	Passed	
EWLCJ175S_SME_09	SSH to standby console via Tacacs authentication	To SSH to standby console via Tacacs authentication	Passed	
EWLCJ175S_SME_10	Monitor health of the system	To monitor health of the system	Passed	
EWLCJ175S_SME_11	Preventing write access in standby console	To prevent write access in standby console	Passed	
EWLCJ175S_SME_12	Validating inventory information on standby	To validate inventory information on standby	Passed	

EWLCJ175S_SME_13	Check logging information of standby chassis	To check logging information of standby chassis	Passed	
EWLCJ175S_SME_14	Monitor failure fan state via SNMP	To monitor failure fan state via SNMP	Passed	
EWLCJ175S_SME_15	Validation of Auto upgrade scenario	To validate auto upgrade scenario from standby chassis	Passed	

ISSU Data Model Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_ISSU__01	Configure HA setup using RP/RMI option.	To configure HA setup using RP/RMI option.	Passed	
EWLCJ175S_ISSU__02	ISSU upgrade with HA SSO RMI	To peform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ175S_ISSU__03	Check ISSU downgrade with HA SSO RMI	To peform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ175S_ISSU__04	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ175S_ISSU__05	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ175S_ISSU__06	Disabling the Rollback timer druing upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ175S_ISSU__07	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ175S_ISSU__08	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	

EWLCJ175S_ISSU_09	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ175S_ISSU_10	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Passed	
EWLCJ175S_ISSU_11	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	
EWLCJ175S_ISSU_12	Profile addition during ISSU	To add profile during ISSU operation	Passed	
EWLCJ175S_ISSU_13	Verify AP upgrade related during ISSU	To verify AP upgrade related during ISSU	Passed	
EWLCJ175S_ISSU_14	Verfiy that config-sync related commands are not supported	To verfiy that config-sync related commands are not supported	Passed	
EWLCJ175S_ISSU_15	ISSU support on yang enabled scenario	To check ISSU support on yang enabled scenario	Passed	
EWLCJ175S_ISSU_16	APDP/APSP support on yang model enabled	To check APDP/APSP support on yang enabled scenario	Passed	
EWLCJ175S_ISSU_17	SMU support on yang model	To check SMU support on yang enabled scenario	Passed	
EWLCJ175S_ISSU_18	Validation of Auto upgrade scenario	To validate auto upgrade scenario	Passed	
EWLCJ175S_ISSU_19	Rolling AP upgrade/AP predownload support on yang model	To check rolling AP upgrade/AP predownload support on yang model	Passed	

Rejection of Wrong WLAN ID

Logical ID	Title	Description	Status	Defect ID

EWLCJ175S_RW_01	Connecting a client to a dot 1x security without wlan id being set	To connect a client to a dot1 x security without wlan id being set and check if the clients gets connected	Passed	
EWLCJ175S_RW_02	Connecting a window client to a dot 1x security with wlan id being set in ISE	To connect a client to a dot1 x security with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_03	Connecting a Android client to a dot 1x security with wlan id being set in ISE	To connect a Android client to a dot1 x security with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_04	Connecting a IOS client to a dot 1x security with wlan id being set in ISE	To connect a IOS client to a dot1 x security with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_05	Connecting a Mac os client to a dot 1x security with wlan id being set in ISE	To connect a Mac os client to a dot1 x security with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_06	Connecting a client to a dot 1x security with wlan id being set in ISE using 9115 AP	To connect a client to a dot1 x security to 9115 AP with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_07	Connecting a client to a dot 1x security with wlan id being set in ISE using 9120 AP	To connect a client to a dot1 x security to 9120 AP with wlan id being set and check if the clients gets connected or not	Passed	

EWLCJ175S_RW_08	Connecting a client to a dot 1x security with wlan id being set in ISE using 9130 AP	To connect a client to a dot1 x security to 9130 AP with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_09	Connecting a client to a dot 1x security with wlan id being set in ISE using 4800 AP	To connect a client to a dot1 x security to 4800 AP with wlan id being set and check if the clients gets connected or not	Passed	
EWLCJ175S_RW_10	Configuring WLAN id attribute to one and making the Window clients to join the other WLAN for which attribute is not set and check the behaviour	To configure WLAN attribute to one ID and connecting a window client to join other wlan to check the behaviour	Passed	
EWLCJ175S_RW_11	Configuring WLAN id attribute to one and making the Android clients to join the other WLAN for which attribute is not set and check the behaviour	To configure WLAN attribute to one ID and connecting a Android client to join other wlan to check the behaviour	Passed	
EWLCJ175S_RW_12	Configuring WLAN id attribute to one and making the IOS clients to join the other WLAN for which attribute is not set and check the behaviour	To configure WLAN attribute to one ID and connecting a IOS client to join other wlan to check the behaviour	Passed	
EWLCJ175S_RW_13	Configuring WLAN id attribute to one and making the Mac OS clients to join the other WLAN for which attribute is not set and check the behaviour	To configure WLAN attribute to one ID and connecting a Mac OS client to join other wlan to check the behaviour	Passed	

EWLCJ175S_RW_14	Configuring Multiple Wlan id attributes set in ISE and Window Clients join different wlan	To create multiple WLAN Id attributes in ISE and connecting a Window client to the WLAN whose attribute is not configured in ISE to check the behaviour of the client	Passed	
EWLCJ175S_RW_15	Configuring Multiple Wlan id attributes set in ISE and Android Clients join different wlan	To create multiple WLAN Id attributes in ISE and connecting a Android client to the WLAN whose attribute is not configured in ISE to check the behaviour of the client	Passed	
EWLCJ175S_RW_16	Configuring Multiple Wlan id attributes set in ISE and IOS Clients join different wlan	To create multiple WLAN Id attributes in ISE and connecting a IOS client to the WLAN whose attribute is not configured in ISE to check the behaviour of the client	Passed	
EWLCJ175S_RW_17	Configuring Multiple Wlan id attributes set in ISE and Mac OS Clients join different wlan	To create multiple WLAN Id attributes in ISE and connecting a Mac OS client to the WLAN whose attribute is not configured in ISE to check the behaviour of the client	Passed	

EWLCJ175S_RW_18	Connecting a Window Clients to one of the wlan defined in ISE among the Multiple Wlan id attributes set in ISE	To Configure multiple WLAN Id attributes in ISE and connecting a Window client to the WLAN among the configured WLAN Id's check the behaviour of the client	Passed	
EWLCJ175S_RW_19	Connecting a Android Clients to one of the wlan defined in ISE among the Multiple Wlan id attributes set in ISE	To Configure multiple WLAN Id attributes in ISE and connecting a Android client to the WLAN among the configured WLAN Id's check the behaviour of the client	Passed	
EWLCJ175S_RW_20	Connecting a IOS Clients to one of the wlan defined in ISE among the Multiple Wlan id attributes set in ISE	To Configure multiple WLAN Id attributes in ISE and connecting a IOS client to the WLAN among the configured WLAN Id's check the behaviour of the client	Passed	
EWLCJ175S_RW_21	Connecting a Mac OS Clients to one of the wlan defined in ISE among the Multiple Wlan id attributes set in ISE	To Configure multiple WLAN Id attributes in ISE and connecting a Mac OS client to the WLAN among the configured WLAN Id's check the behaviour of the client	Passed	

Error Propagation for Exec Commands

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Error_01	Validate the command for clear_personal_ssid	To Validate the command to clear the SSID	Passed	

EWLCJ175S_Error_02	Validate the command for ap config to controller	To Execute the command for ap config	Passed	
EWLCJ175S_Error_03	Validate the command for ap country	To Execute the command for ap country	Passed	
EWLCJ175S_Error_04	Execute the command to get crash data	To Validate the command to get crash detail or not	Passed	
EWLCJ175S_Error_05	Validate the command for flash opertaion	To Validate the command for flash operation	Passed	
EWLCJ175S_Error_06	Execute the command port config details	To Execute the command and validate port config shown or not	Passed	
EWLCJ175S_Error_07	Execute the command for ap slot	To Execute the command for ap slot	Passed	
EWLCJ175S_Error_08	Validate the command to sniffing	To Execute the command for ap sniffing	Passed	
EWLCJ175S_Error_09	Validate the command for bss_color	To Execute the command for bss color	Passed	
EWLCJ175S_Error_10	Validate the commmand for dual band role	To Execute the command for dual band role	Passed	

CHAPTER 4

Regression Features

APSP/APDP support in WebUI for EWLC-ME

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_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	
EWCJ175S_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	
EWCJ175S_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	
EWCJ175S_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	

EWCJ175S_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	
EWCJ175S_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	
EWCJ175S_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	
EWCJ175S_Reg_08	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ175S_Reg_09	Verifying whether APSP/APDP is accepting a invalid credentials.	To check whether APSP/APDP is accepting invalid credentials or not	Passed	
EWCJ175S_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
EWCJ175S_Reg_11	To Deploy Fabric configuration from webUI on 9300	To Verify Fabric UI on 9300	Passed	
EWCJ175S_Reg_12	To Deploy Fabric configuration from webUI on 9300 and Windows Client	To Verify Fabric UI on 9300 with Window Client	Passed	
EWCJ175S_Reg_13	To Deploy Fabric configuration from webUI on 9300 and Android Client	To Verify Fabric UI on 9300 with Android Client	Passed	

EWCJ175S_Reg_14	To Deploy Fabric configuration from webUI on 9300 and MAC Client	To Verify Fabric UI on 9300 with MAC Client	Passed	
EWCJ175S_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	
EWCJ175S_Reg_16	To Deploy Fabric configuration from webUI on 9400	To Verify Fabric UI on 9400	Passed	
EWCJ175S_Reg_17	To Deploy Fabric configuration from webUI on 9400 and Windows Client	To Verify Fabric UI on 9400 with Window Client	Passed	
EWCJ175S_Reg_18	To Deploy Fabric configuration from webUI on 9400 and Android Client	To Verify Fabric UI on 9400 with Android Client	Passed	
EWCJ175S_Reg_19	To Deploy Fabric configuration from webUI on 9400 and MAC Client	To Verify Fabric UI on 9400 with MAC Client	Passed	
EWCJ175S_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	
EWCJ175S_Reg_21	To Deploy Fabric configuration from webUI on 9500	To Verify Fabric UI on 9500	Passed	
EWCJ175S_Reg_22	To Deploy Fabric configuration from webUI on 9500 and Windows Client	To Verify Fabric UI on 9500 with Window Client	Passed	
EWCJ175S_Reg_23	To Deploy Fabric configuration from webUI on 9500 and Android Client	To Verify Fabric UI on 9500 with Android Client	Passed	
EWCJ175S_Reg_24	To Deploy Fabric configuration from webUI on 9500 and MAC Client	To Verify Fabric UI on 9500 with MAC Client	Passed	

EWCJ175S_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	

WGB client support on ME

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_26	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWCJ175S_Reg_27	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWCJ175S_Reg_28	Configuring WGB in eWC	To verify WGB configuration is successful or not in eWC	Passed	
EWCJ175S_Reg_29	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	
EWCJ175S_Reg_30	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	
EWCJ175S_Reg_31	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	

EWCJ175S_Reg_32	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	
EWCJ175S_Reg_33	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	
EWCJ175S_Reg_34	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	
EWCJ175S_Reg_35	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	
EWCJ175S_Reg_36	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	
EWCJ175S_Reg_37	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWCJ175S_Reg_38	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients afte session timeout	Passed	
EWCJ175S_Reg_39	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

EWCJ175S_Reg_291	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWCJ175S_Reg_292	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWCJ175S_Reg_293	Configuring WGB in EWC	To verify WGB configuration is successful or not in EWC	Passed	
EWCJ175S_Reg_294	Validating the client connected to WGB	To validate the List of all clients connected to WGB	Passed	
EWCJ175S_Reg_295	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	
EWCJ175S_Reg_296	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	
EWCJ175S_Reg_297	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	
EWCJ175S_Reg_298	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	

EWCJ175S_Reg_299	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	
EWCJ175S_Reg_300	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	
EWCJ175S_Reg_301	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	
EWCJ175S_Reg_302	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	
EWCJ175S_Reg_303	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	
EWCJ175S_Reg_304	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	
EWCJ175S_Reg_305	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	

EWCJ175S_Reg_306	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	
EWCJ175S_Reg_307	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	
EWCJ175S_Reg_308	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	
EWCJ175S_Reg_309	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWCJ175S_Reg_310	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients afte session timeout	Passed	
EWCJ175S_Reg_311	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

PSK Multi-auth Support

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_40	Creating Wlan with WPA2 Secutiry with MPSK	Verify Wlan Creating with WPA2 Secutiry with MPSK	Passed	
EWCJ175S_Reg_41	Edit WPA2 Secutiry PSK Keys on MPSK	Verify Wlan Edit with WPA2 Secutiry with MPSK	Passed	
EWCJ175S_Reg_42	Delete WPA2 Secutiry PSK Keys on MPSK	Verify Wlan Delete with WPA2 Secutiry with MPSK	Passed	

EWCJ175S_Reg_43	Creating Wlan with WPA2 Secutiry with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Secutiry with MPSK - Format with Hexa:	Passed	
EWCJ175S_Reg_44	Creating Wlan with WPA2 Secutiry with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ175S_Reg_45	Verify WPA2 Secutiry with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Secutiry with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWCJ175S_Reg_46	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ175S_Reg_47	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ175S_Reg_48	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ175S_Reg_49	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ175S_Reg_50	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ175S_Reg_51	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ175S_Reg_52	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWCJ175S_Reg_53	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	

EWCJ175S_Reg_54	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ175S_Reg_55	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

EoGRE Support for ME

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_56	Creating EoGRE Tunnel Gateway.	To check whether the tunnel gateway is created or not.	Passed	
EWCJ175S_Reg_57	Creating EoGRE Tunnel Domain	To check whether the tunnel Domain is created or not.	Passed	
EWCJ175S_Reg_58	Configuring the Global Parameter for the EoGRE.	To check whether the global parameters are configured or not.	Passed	
EWCJ175S_Reg_59	Configuring the tunnel Profile.	To check whether the tunnel profile is created or not.	Passed	
EWCJ175S_Reg_60	Associate the WLAN to the Wireless policy profile.	To check whether the wlan is associated with the policy profile.	Passed	
EWCJ175S_Reg_61	Adding a policy tag and site tag to AP	To check whether the policy and site tag is added to an AP.	Passed	
EWCJ175S_Reg_62	Checking the client connectivity.	To check whether the client is connected or not	Passed	
EWCJ175S_Reg_63	Getting the EoGRE tunnel from PI	To check whether the tunnel is exported from PI or not	Passed	
EWCJ175S_Reg_64	Connect the ios clients and check the connectivity.	To check whether the ios clients get connected successfully.	Passed	

	EWCJ175S_Reg_65	Connect the mac os clients and check the connectivity.	To check whether the mac os clients get connected successfully.	Passed	
	EWCJ175S_Reg_66	Checking the traffic in the tunnel.	To check whether the traffic in the tunnel is managed or not.	Passed	

iPSK Peer-2-Peer Blocking

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_67	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	
EWCJ175S_Reg_68	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	
EWCJ175S_Reg_69	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	
EWCJ175S_Reg_70	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	
EWCJ175S_Reg_71	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	

EWCJ175S_Reg_72	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	
EWCJ175S_Reg_73	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	
EWCJ175S_Reg_74	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	
EWCJ175S_Reg_75	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	
EWCJ175S_Reg_76	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	
EWCJ175S_Reg_77	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	
EWCJ175S_Reg_78	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	

EWCJ175S_Reg_79	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	
EWCJ175S_Reg_80	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	
EWCJ175S_Reg_81	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	
EWCJ175S_Reg_82	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	
EWCJ175S_Reg_83	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	
EWCJ175S_Reg_84	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	

EWCJ175S_Reg_85	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	
EWCJ175S_Reg_86	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	
EWCJ175S_Reg_87	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	
EWCJ175S_Reg_88	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	
EWCJ175S_Reg_89	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	
EWCJ175S_Reg_90	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	
EWCJ175S_Reg_91	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	
EWCJ175S_Reg_92	Verifying iPSK WLAN configuration after importing and exporting thhe same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	

EWCJ175S_Reg_93	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	
EWCJ175S_Reg_94	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	
EWCJ175S_Reg_95	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	
EWCJ175S_Reg_96	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	
EWCJ175S_Reg_97	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	
EWCJ175S_Reg_98	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 forsame OS Clients.	Passed	
EWCJ175S_Reg_99	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	

EWCJ175S_Reg_100	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	
EWCJ175S_Reg_101	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	
EWCJ175S_Reg_102	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	
EWCJ175S_Reg_103	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	Failed	CSCvw84280
EWCJ175S_Reg_104	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	
EWCJ175S_Reg_105	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	

EWCJ175S_Reg_106	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	
EWCJ175S_Reg_107	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	
EWCJ175S_Reg_108	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	
EWCJ175S_Reg_109	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	
EWCJ175S_Reg_110	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	

EWCJ175S_Reg_111	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	
EWCJ175S_Reg_112	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ175S_Reg_113	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

BSS Coloring on AX APs

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_114	Configuring Automatic BSS coloring for 2.4 ghz AP radios	To Check whether automatic BSS coloring is applied or not in 2.4 ghz ap radio	Passed	
EWCJ175S_Reg_115	Configuring automatic BSS color for 5ghz radio	To Check whether automatic BSS coloring is applied or not in 5 ghz ap radio	Passed	
EWCJ175S_Reg_116	Configuring auto BSS color appering 2.4 to 5 Ghz radio or vice versa	To verify whether different BSS coloring is occur while Changing the AP radios 2.4 to 5 viseversa	Passed	
EWCJ175S_Reg_117	Configuring Manual BSS color configuration for 2.4/5 ghz radio	To Check whether Manual BSS coloring is applied or not in 2.4 ghz ap radio	Passed	

EWCJ175S_Reg_118	Verifying the static BSS color assignment for the 5 ghz radio in Flex-connect mode	To Check whether Static BSS coloring is applied or not in 5 ghz ap radio	Passed	
EWCJ175S_Reg_119	Checking the manual BSS coloring while changing the AP radio from 2.4 ghz to 5 ghz	To verify whether different BSS coloring is occur while Changing the AP radios	Passed	
EWCJ175S_Reg_120	Checking the BSS color details are retained after AP and Controller reload	To Check whether the BSS color retained after AP & Controller reload	Passed	
EWCJ175S_Reg_121	Verifying BSS coloring with Intra client roaming by using 9115AP	To verify whether BSS coloring with client roaming between AP's or not	Passed	
EWCJ175S_Reg_122	Verifying BSS coloring with inter roming client using different radio	To check whether BSS coloring is appearing or not , when different radio clients are roaming between controllers	Passed	
EWCJ175S_Reg_123	Verifying BSS coloring with inter roming client using same radio	To check whether BSS coloring is appearing or not , when same radio clients are roaming between controllers	Passed	
EWCJ175S_Reg_124	Capturing the Windows client connectivity & BSS coloring using Wireshark	To check the window client connectivity & BSS coloring using Wireshark	Passed	
EWCJ175S_Reg_125	Capturing the Android client connectivity & BSS coloring using Wireshark	To check the Android client connectivity & BSS coloring using Wireshark	Passed	
EWCJ175S_Reg_126	Capturing the Mac OS client connectivity & BSS coloring using Wireshark	To check the Mac OS client connectivity & BSS coloring using Wireshark	Passed	

| EWCJ175S_Reg_127 | Changing 9115 AP mode from local to Flex connect & check the BSS coloring Configuration | To change the mode of AP from local mode to Flexconnect mode and check the BSS coloring configuration in 9115 Ap | Passed | |
| EWCJ175S_Reg_128 | Changing 9115 AP mode from flex to local & check the BSS coloring Configuration | To change the mode of AP from flex mode to local mode and check the BSS coloring configuration in 9115 Ap | Passed | |

CMX Parity for eWLC ME

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_129	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	
EWCJ175S_Reg_130	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	
EWCJ175S_Reg_131	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	

EWCJ175S_Reg_132	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	
EWCJ175S_Reg_133	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	
EWCJ175S_Reg_134	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	
EWCJ175S_Reg_135	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	
EWCJ175S_Reg_136	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	
EWCJ175S_Reg_137	Verify the Disconnected client details in CMX	To check whether the client is disconnected or not in CMX	Passed	
EWCJ175S_Reg_138	Verifying the Intra client roaming in CMX	To verify whether the client is roaming between AP's or not	Passed	
EWCJ175S_Reg_139	Verifying the Inter client roaming in CMX	To verify whether the clients are roaming between controllers	Passed	

EWCJ175S_Reg_140	Verifying the Wired client details in CMX	To Check whether the Wired client details are showing or not in CMX	Passed	
EWCJ175S_Reg_141	Verifying the guest LAN client details in CMX	To Check whether the Guest LAN client details are showing or not in CMX	Passed	
EWCJ175S_Reg_142	Verifying MIMO client details using Wireshark	To check Whether all the clients getting same BW & data rate or not	Passed	

EWC Day0 Elimination

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_143	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	
EWCJ175S_Reg_144	Manualy 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 manualy	Passed	
EWCJ175S_Reg_145	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	
EWCJ175S_Reg_146	Checking the image version after Provisioning Ewlc_ME with PnP	Verifying the image version after Provisioning Ewlc_ME with PnP	Passed	
EWCJ175S_Reg_147	Checking the AP details after Provisioning Ewlc_ME with PnP	Verifying the AP details after Provisioning Ewlc_ME with PnP	Passed	

EWCJ175S_Reg_148	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Passed	
EWCJ175S_Reg_149	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	
EWCJ175S_Reg_150	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	
EWCJ175S_Reg_151	Configuring wrong details for PnP while claming the device	To verify whether user is able to Provisioned the eWLC_ME with providing wrong PnP configuration in DNAC	Passed	
EWCJ175S_Reg_152	Checking the eWLC_ME after configuring factory reset with save config	Verifying whether user able to bring device to day0 or notwith save config as yes	Passed	

TACACS

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_153	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	
EWCJ175S_Reg_154	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	

EWCJ175S_Reg_155	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	
EWCJ175S_Reg_156	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	
EWCJ175S_Reg_157	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	
EWCJ175S_Reg_158	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	
EWCJ175S_Reg_159	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	
EWCJ175S_Reg_160	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, Wireless, Command Line Interfaces and "Management" checkboxes.	Passed	
EWCJ175S_Reg_161	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
EWCJ175S_Reg_162	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 successfullyin	Passed	
EWCJ175S_Reg_163	Uploading the empty CSV file in eWC UI	To check whether an blank CSV file could be uploaded in eWC UI	Passed	
EWCJ175S_Reg_164	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	
EWCJ175S_Reg_165	Connecting the Client with wlan security mac filtering + WPA personal	To Connect the Client with wlan security mac filtering + WPA personal	Passed	
EWCJ175S_Reg_166	Connecting the Client with wlan security mac filtering + WPA enterprise	To Connect the Client with wlan security mac filtering + WPA enterprise	Passed	
EWCJ175S_Reg_167	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	

| EWCJ175S_Reg_168 | Connecting the client after client identity account expired in ISE | To Connect the Client after client identity account expired in ISE | Passed | |
| EWCJ175S_Reg_169 | 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 | |

Internal DHCP Server

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_170	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	
EWCJ175S_Reg_171	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	
EWCJ175S_Reg_172	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	
EWCJ175S_Reg_173	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	
EWCJ175S_Reg_174	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	

802 1x support with EAP-TLS and EAP-PEAP

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_175	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	
EWCJ175S_Reg_176	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	
EWCJ175S_Reg_177	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	
EWCJ175S_Reg_178	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	
EWCJ175S_Reg_179	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	
EWCJ175S_Reg_180	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	
EWCJ175S_Reg_181	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	

EWCJ175S_Reg_182	Enabling dot1x auth for AP in 3850 Switch	Configuring the 3850 Switch for Dot1x authentication by mapping the identity profiles to a port.	Passed	
EWCJ175S_Reg_183	Checking the configuration of 802.1x authentication paramaters 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	
EWCJ175S_Reg_184	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	
EWCJ175S_Reg_185	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	
EWCJ175S_Reg_186	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	
EWCJ175S_Reg_187	Trying to configure of 802.1x authentication paramaters 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	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID

EWCJ175S_Reg_188	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	
EWCJ175S_Reg_189	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	
EWCJ175S_Reg_190	Configuring optimized roaming with 5 GHz band and roamt Android client	To verify that optimized roaming with 5 GHz band and check association of Android client	Passed	
EWCJ175S_Reg_191	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	
EWCJ175S_Reg_192	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	
EWCJ175S_Reg_193	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 Threashold configured and check association of iOS client	Passed	

EWCJ175S_Reg_194	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 succesfully and check association of iOS client	Passed	
EWCJ175S_Reg_195	Configuring optimized roaming with 5 GHz band , 12 MBPS Threshold and roam iOS client	To verfiy that optimized roaming with 5 GHz band , 12 MBPS Threshold configured succesfully and check association of iOS client	Passed	
EWCJ175S_Reg_196	Moving the Andoroid client from AP after enable optimized roaming	To verify that client got disassocited when signal is poor while moving from AP	Passed	
EWCJ175S_Reg_197	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassocited when signal is poor while moving from AP	Passed	
EWCJ175S_Reg_198	Moving the Android client from AP after enable optimized roaming in ME with interference availability	To verify that client got disassocited when signal is poor while moving from 2700 AP with interference availability	Passed	
EWCJ175S_Reg_199	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	
EWCJ175S_Reg_200	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	

| EWCJ175S_Reg_201 | Importing/exporting configuration file after optimized roaming configuring | To verify that optimization roaming configuration remain same after import and export configuration file | Passed | |

ICAP Support for C9130

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_202	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	Passed	
EWCJ175S_Reg_203	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	Passed	
EWCJ175S_Reg_204	Packet capture for Android client using Intellingent Capture option in Apgroup	To verify the packet capture for Android client using Intelligent capture in APgroup	Passed	
EWCJ175S_Reg_205	Packet capture for Windows JOS client using Intellingent Capture option in APgroup	To verify the packet capture for Windows client using Intelligent capture in APgroup	Passed	
EWCJ175S_Reg_206	Packet capture for IOS client using Intellingent Capture option in APgroup	To verify the packet capture for IOS client using Intelligent capture in APgroup	Passed	
EWCJ175S_Reg_207	Packet capture for Mac OS client using Intellingent Capture option in APgroup	To verify the packet capture for MAC OS client using Intelligent capture in APgroup	Passed	

EWCJ175S_Reg_208	Capturing of Packet of the client when the client is connected with open security	To capture packet when the client is connected to the iOS AP with security as OPEN in EWC	Passed	
EWCJ175S_Reg_209	Capturing of Packet of the client when the client is connected with WPA 2 PSK security	To capture packet when the client is connected to the iOS AP with security as WPA 2 PSK in EWC	Passed	
EWCJ175S_Reg_210	Capturing of Packet of the client when the client is connected with WPA 2 Enterprise security	To capture packet when the client is connected to the iOS AP with security as WPA 2 Enterprise in EWC	Passed	
EWCJ175S_Reg_211	Capturing of Packet of the client when the client is connected with captive portal-web consent	To capture packet when the client is connected to the AP with security as Captive portal-webconsent	Passed	
EWCJ175S_Reg_212	Packet capture for Anyconnect client using Intellingent Capture option in APgroup page	To verify the packet capture for Anyconnect client using Intelligent capture in APgroup page	Passed	
EWCJ175S_Reg_213	Packet capture for Windows JOS client using Intellingent Capture option in AP page	To verify the packet capture for Windows JOS client using Intelligent capture in AP page	Passed	
EWCJ175S_Reg_214	Packet capture for Android client using Intellingent Capture option in AP page	To verify the packet capture for Android client using Intelligent capture in AP page	Passed	
EWCJ175S_Reg_215	Packet capture for iOS client using Intellingent Capture option in AP page	To verify the packet capture for iOS client using Intelligent capture in AP page	Passed	

| EWCJ175S_Reg_216 | Packet capture for MacOS client using Intellingent Capture option in AP page | To verify the packet capture for MacOS client using Intelligent capture in AP page | Passed | |
| EWCJ175S_Reg_217 | Packet capture for Anyconnect client using Intellingent Capture option in AP page | To verify the packet capture for Anyconnect client using Intelligent capture in AP page | Passed | |

mDNS gateway support for flex/Mobility Express

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_218	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	
EWCJ175S_Reg_219	Creating mDNS profile by adding required services	To verify whether mDNS profile is created with required services	Passed	
EWCJ175S_Reg_220	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	
EWCJ175S_Reg_221	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	
EWCJ175S_Reg_222	Checking mDNS gateway are applied to Apple TV and authentication server as radius in ME	To verify mDNS gateway are applied to AppleTV and authentication server as radius in ME.	Passed	
EWCJ175S_Reg_223	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	

EWCJ175S_Reg_224	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	
EWCJ175S_Reg_225	Checking mDNS gateway are applying to Apple iPad and Apple chromecast clients with Static WEP security after enabling the mdns AP to 9130/9115/4800/9120/3700APs	To check whether the mdns gateway are applying to Apple iPad and Apple chromecast clients with Static WEP security or not after enabling the mDNS-ap to9130/9115/4800/9120/3700APs.	Passed	
EWCJ175S_Reg_226	Checking mDNS gateway are applied to MAC OS with wlan open security	Verifying mDNS gateway are applied to Mac OS with open ssid	Passed	
EWCJ175S_Reg_227	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	
EWCJ175S_Reg_228	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	
EWCJ175S_Reg_229	Checking mDNS gateway are applied to Apple Devices with Fast transition enabled	To Check mDNS gateway are applied to Apple Devices with fasttransition enabled	Passed	
EWCJ175S_Reg_230	Performing client communication between two clients connected two different vlan	To Check whether client communicate between two clients connected to different vlan	Passed	
EWCJ175S_Reg_231	Performing roaming operation when mDNS is applied	To Check the roaming operation when mDNS is applied	Passed	
EWCJ175S_Reg_232	Checking mDNS config after exporting config file	To check whether the mDNS config is same after exporting config file	Passed	

EWCJ175S_Reg_233	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	
EWCJ175S_Reg_234	Verifying the mDNS configuration in DNAC	To Verify the mDNS gateway configuration in DNAC	Passed	
EWCJ175S_Reg_235	Verifying mDNS configuration Via EWC CLI	To verify the mDNS configuration through EWC CLI	Passed	

200 Country Code Support

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_237	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	
EWCJ175S_Reg_240	Verifying the Configuration of the country code during day 0 Configuration.	To Check whether the country code is configured during day 0 Configuration.	Passed	
EWCJ175S_Reg_241	Verifying the country code by connecting Android clients.	To Check whether android clients are connected successfully after a change in the country code.	Passed	
EWCJ175S_Reg_243	Verifying the country code by connecting Windows clients.	To Check whether Windows clients are connected successfully after a change in the country code.	Passed	

Explicit warning for configuration-triggered downtime

Logical ID	Title	Description	Status	Defect ID

EWCJ175S_Reg_244	Verifying the warning message after changing AP/RF/Site tags	To verify the warning message after changing AP/RF / site Tag	Passed	
EWCJ175S_Reg_245	Checking the warning message for after changing the AP tag in Flex mode AP	To check the warning message for changing Ap tag in flex mode AP	Passed	
EWCJ175S_Reg_246	Validating the warning message for after changing the RF tag in flex mode AP	To Validate the warning message for changing RF tag in flex mode AP	Passed	
EWCJ175S_Reg_247	Verifying the warning message for after changing the Site tag in Flex mode AP	To Verify the warning message for changing Site tag in flex mode AP	Passed	
EWCJ175S_Reg_248	Verifying the warning message for after changing the AP tag in Local mode AP	To Verify the warning message for changing Ap tag in Local mode AP	Passed	
EWCJ175S_Reg_249	Verifying the warning message for after changing the RF tag in Local mode AP	To Verify the warning message for changing RF tag in Local mode AP	Passed	
EWCJ175S_Reg_250	Verifying the warning message for after changing the Site tag in Local mode AP	To Verify the warning message for changing Site tag in local mode AP	Passed	
EWCJ175S_Reg_251	Verifying the warning message by editing the policy Tag in WLAN	To verify whether the warning message showing or not after editing Policy Tag in WLAN	Passed	
EWCJ175S_Reg_252	Checking the Warning message for editing the policy profile	To check the warning message for editing the Policy profile	Passed	
EWCJ175S_Reg_253	Checking the Warning message after AP reboot	To verify the warning message for after AP reboot	Passed	

EWCJ175S_Reg_254	Checking warning message after AP radio change	To check whether the warning message showing or not after changing the AP radio	Passed	
EWCJ175S_Reg_255	Verifying the warning message for different AP models	To Verify the warning message for different AP models	Passed	
EWCJ175S_Reg_256	Validating the warning message after disjoin the AP	To validate the warning message for after Ap disjoin	Passed	
EWCJ175S_Reg_257	Verifying the warning message after deleting the client	To verify the warning message for deleted client	Passed	
EWCJ175S_Reg_258	Verifying the warning message after 2.4/5 ghz radio down	To verify the warning message after 2.4/5 ghz radio down	Passed	
EWCJ175S_Reg_259	Verifying the warning message by changing the AP ip Address	To validate the warning message by changing the AP ip Address	Passed	
EWCJ175S_Reg_260	Validating the warning message for Virtual EWLC	To validate the warning message for vEWLC	Passed	
EWCJ175S_Reg_261	Checking the warning message after deleting the AP tag	To validate the warning message after deleting the AP tag	Passed	
EWCJ175S_Reg_262	Checking the warning message after deleting the RF tag	To validate the warning message after deleting the RF tag	Passed	
EWCJ175S_Reg_263	Checking the warning message after deleting the Site tag	To validate the warning message after deleting the Site tag	Passed	
EWCJ175S_Reg_264	monitoring the warning message after chaging AP tag Via CLI	To check the warning message for changing Ap tag via CLI	Passed	

EWCJ175S_Reg_265	monitoring the warning message after chaging RF tag Via CLI	To check the warning message for changing RF tag via CLI	Passed	
EWCJ175S_Reg_266	monitoring the warning message after chaging site tag Via CLI	To check the warning message for changing Site tag via CLI	Passed	
EWCJ175S_Reg_267	monitoring the warning message after AP provisioning from DNAC	To check the warning message after AP provisioning from DNAC	Passed	

Active Config Visualization

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_276	verify the virtual config in EWC 9115	To verify the virtual config in EWC 9115	Passed	
EWCJ175S_Reg_277	verify the virtual config in EWC 9117	To verify the virtual config in EWC 9117	Passed	
EWCJ175S_Reg_278	verify the virtual config in EWC 9120	To verify the virtual config in EWC 9120	Passed	
EWCJ175S_Reg_279	verify the virtual config in EWC 9130	To verify the virtual config in EWC 9130	Passed	

Copy of webauth tar bundle in EWC HA setup

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_280	Download WebAuth Bundle with TFTP option	To Download WebAuth Bundle with TFTP option	Passed	
EWCJ175S_Reg_281	Download WebAuth Bundle with FTP option	To Download WebAuth Bundle with FTP option	Passed	
EWCJ175S_Reg_282	Download WebAuth Bundle with SFTP option	To Download WebAuth Bundle with SFTP option	Passed	
EWCJ175S_Reg_283	Download WebAuth Bundle with HTTP option	To Download WebAuth Bundle with HTTP option	Passed	

EWCJ175S_Reg_284	Verify Pop-up/Alert when space is low FTP	To Verify Pop-up/Alert when space is low FTP	Passed	
EWCJ175S_Reg_285	VerifyPop-up/Alert when space is low SFTP	To VerifyPop-up/Alert when space is low SFTP	Passed	
EWCJ175S_Reg_286	VerifyPop-up/Alert when space is low TFTP	To VerifyPop-up/Alert when space is low TFTP	Passed	
EWCJ175S_Reg_287	Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9115	To Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9115	Passed	
EWCJ175S_Reg_288	Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9117	To Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9117	Passed	
EWCJ175S_Reg_289	Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9120	To Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9120	Passed	
EWCJ175S_Reg_290	Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9130	To Verify tar file should have been copied to both bootflash and stby-bootflash in EWC 9130	Passed	

WGB Support

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_26	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	

EWCJ175S_Reg_27	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWCJ175S_Reg_28	Configuring WGB in eWC	To verify WGB configuration is successful or not in eWC	Passed	
EWCJ175S_Reg_29	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	
EWCJ175S_Reg_30	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	
EWCJ175S_Reg_31	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	
EWCJ175S_Reg_32	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	
EWCJ175S_Reg_33	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	

EWCJ175S_Reg_34	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	
EWCJ175S_Reg_35	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	
EWCJ175S_Reg_36	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	
EWCJ175S_Reg_37	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWCJ175S_Reg_38	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients afte session timeout	Passed	
EWCJ175S_Reg_39	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	
EWCJ175S_Reg_291	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWCJ175S_Reg_292	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWCJ175S_Reg_293	Configuring WGB in EWC	To verify WGB configuration is successful or not in EWC	Passed	

EWCJ175S_Reg_294	Validating the client connected to WGB	To validate the List of all clients connected to WGB	Passed	
EWCJ175S_Reg_295	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	
EWCJ175S_Reg_296	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	
EWCJ175S_Reg_297	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	
EWCJ175S_Reg_298	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	
EWCJ175S_Reg_299	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	
EWCJ175S_Reg_300	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	

EWCJ175S_Reg_301	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	
EWCJ175S_Reg_302	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	
EWCJ175S_Reg_303	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	
EWCJ175S_Reg_304	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	
EWCJ175S_Reg_305	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	
EWCJ175S_Reg_306	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	
EWCJ175S_Reg_307	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	
EWCJ175S_Reg_308	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	

EWCJ175S_Reg_309	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWCJ175S_Reg_310	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients afte session timeout	Passed	
EWCJ175S_Reg_311	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	
EWLCJ175S_Reg_334	Configuring the Capwap ap to autonomous AP	To change the capwap ap to autonomous ap and check if the AP is converted	Passed	
EWLCJ175S_Reg_335	Configuring the Autonomous AP as the WGB	To configure the autonomous AP as WGB and check if the AP changes as WGB.	Passed	
EWLCJ175S_Reg_336	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	
EWLCJ175S_Reg_337	Associating the WGB on WPA 2 with PSK with 9115 AP	To associate the WGB on WPA 2 PSK security with 9115 AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ175S_Reg_338	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	

EWLCJ175S_Reg_339	Associating the WGB on WPA 2 with PSK	To associate the WGB on WPA 2 PSK security with 9115 AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ175S_Reg_340	Associating the WGB on WPA 3 with PSK	To associate the WGB on WPA 3 PSK security with 9115 AP and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ175S_Reg_341	Associating the WGB on WPA 2 with 802.1x	To associate the WGB on WPA 2 802.1x security with 9115 and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ175S_Reg_342	Associating the WGB on WPA 3 with 802.1x	To associate the WGB on WPA 3 802.1x security with 9115 and check if the WGB associates with the WLAN or not.	Passed	
EWLCJ175S_Reg_343	Checking of WGB roaming from one AP to another AP	To check the roaming of WGB from one AP to another AP and check if the roaming happens succesfully	Passed	
EWLCJ175S_Reg_344	Performing Inter controller roaming for WGB clients with OPEN security	To check inter controller roaming for WGB clients with OPEN security	Passed	
EWLCJ175S_Reg_345	Performing Inter controller roaming for WGB clients with WPA2 PSK security	To check inter controller roaming for WGB clients with WPA2 PSK security	Passed	

EWLCJ175S_Reg_346	Performing Inter controller roaming for WGB clients with WPA2 Dot1x security	To check inter controller roaming for WGB clients with WPA2 Dot1x security	Passed	
EWLCJ175S_Reg_347	Performing Inter controller roaming for WGB clients with WPA3 PSK security in	To check inter controller roaming for WGB clients with WPA3 PSK security in AP bridge mode	Passed	
EWLCJ175S_Reg_348	Performing Inter controller roaming for WGB clients with WPA3 Dot1x security in AP bridge mode	To check inter controller roaming for WGB clients with WPA3 Dot1x security in AP bridge mode	Passed	
EWLCJ175S_Reg_349	Associating the WGB on open security with local authentication	To check WGB client association with OPEN security and local authentication	Passed	
EWLCJ175S_Reg_350	Checking Reassociation happens for WGB clients after session timeout	To verify reassociation for WGB clients afte session timeout	Passed	
EWLCJ175S_Reg_351	Performing local switching for WGB clients with 9115 AP	To verify local switching traffic for client with 9115 AP	Passed	

Ethernet VLAN tag on AP

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_312	Providing the VLAN tag to the 9115 AP from eWC CLI.	To Verify the VLAN tag status of the 9115 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_313	Unassign the VLAN tag to the 9115 AP from EWC CLI.	To Verify the VLAN tag status of the 9115 AP after reboot and join back to the EWC.	Passed	

EWCJ175S_Reg_314	Providing the VLAN tag to the 9120 AP from EWC CLI.	To Verify the VLAN tag status of the 9120 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_315	Unassign the VLAN tag to the 9120 AP from EWC CLI.	To Verify the VLAN tag status of the 9120 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_316	Providing the VLAN tag to the 9130 AP from EWC CLI.	To Verify the VLAN tag status of the 9130 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_317	Unassign the VLAN tag to the 9130 AP from EWC CLI.	To Verify the VLAN tag status of the 9130 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_318	Providing the VLAN tag to the 4800 AP from EWC CLI.	To Verify the VLAN tag status of the 4800 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_319	Unassign the VLAN tag to the 4800 AP from EWC CLI.	To Verify the VLAN tag status of the 4800 AP after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_320	Check the VLAN tag is overriding or not via CLI	To verify whether the VLAN tag is overriding or not after assigning VLAN Tag to the particular Ap	Passed	
EWCJ175S_Reg_321	Check the VLAN tag is overriding or not via GUI	To verify whether the VLAN tag is overriding or not after assigning to new VLAN tag to particular Ap	Passed	
EWCJ175S_Reg_322	Checking the VLAN Tag after DCA Mode change	To check the VLAN tag after changing DCA mode	Passed	

EWCJ175S_Reg_323	Checking the VLAN Tag after changing Radio band	To check the VLAN tag after changing radio band	Passed	
EWCJ175S_Reg_324	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the Android Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the Android client connectivity.	Passed	
EWCJ175S_Reg_325	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the Windows Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the Windows client connectivity.	Passed	
EWCJ175S_Reg_326	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the IOS Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the IOS client connectivity.	Failed	CSCvx02719
EWCJ175S_Reg_327	Providing the VLAN tag to the 9115/9120/9130 AP's from EWC CLI and connect the anyconnect Client.	To Verify the VLAN tag status of the 9115/9120/9130 AP's after reboot and join back to the EWC and Verify the anyconnect client connectivity.	Failed	CSCvx02724
EWCJ175S_Reg_328	Providing the VLAN tag to the Group of AP's from EWC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the EWC.	Passed	
EWCJ175S_Reg_329	Unassign the VLAN tag to the Group of AP's from EWC CLI.	To Verify the VLAN tag status of the Group of AP's after reboot and join back to the EWC.	Passed	

EWCJ175S_Reg_330	Providing the VLAN tag to the Catalyst AP's from EWC CLI and change the mode of the AP to Monitor from local.	To Verify the VLAN tag status of the Catalyst AP's after changing the mode of the AP to monitor from local.	Passed	
EWCJ175S_Reg_331	Providing the VLAN tag to the Catalyst AP from EWC CLI and change the mode of the AP to flex from Local.	To Verify the VLAN tag status of the Catalyst AP's after changing the mode of the AP to flex from local.	Passed	
EWCJ175S_Reg_332	Providing the VLAN tag to the 4800 AP from EWC CLI and change the mode of the AP to sniffer from Local.	To Verify the VLAN tag status of the 4800 AP after changing the mode of the AP to sniffer from local.	Passed	

Smart Licensing

Logical ID	Title	Description	Status	Defect ID
EWCJ175S_Reg_333	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWCJ175S_Reg_334	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWCJ175S_Reg_335	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWCJ175S_Reg_336	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWCJ175S_Reg_337	Smart Licensing HA Support in eWC	To verify Smart Licensing for HA Support in eWC	Passed	
EWCJ175S_Reg_338	Change a SLR on a C9800 SSO HA pair	To change a SLR on a C9800 SSO HA pair	Passed	

EWCJ175S_Reg_339	Removing SLR from a C9800 SSO HA pair	To verify by removing SLR from a C9800 SSO HA pair	Passed	
EWCJ175S_Reg_340	Validate license info on Standby AP	To validate license info on standby AP	Passed	
EWCJ175S_Reg_341	Validate license info after EWC upgrade	To validate license info after EWC upgrade	Passed	
EWCJ175S_Reg_342	Validate license info after switchover in AP	To validate license info after switchover in AP	Passed	
EWCJ175S_Reg_343	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	

Multi LAG and Load Balancing based on VLAN and SSO

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_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	
EWLCJ175S_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	
EWLCJ175S_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.	Failed	CSCvw63135
EWLCJ175S_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	
EWLCJ175S_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	

EWLCJ175S_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	

AdvAP_QBSS_MCAST

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_07	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	
EWLCJ175S_Reg_08	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	
EWLCJ175S_Reg_09	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	
EWLCJ175S_Reg_10	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	

EWLCJ175S_Reg_11	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	
EWLCJ175S_Reg_12	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	
EWLCJ175S_Reg_13	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	
EWLCJ175S_Reg_14	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	
EWLCJ175S_Reg_15	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	
EWLCJ175S_Reg_16	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	

EWLCJ175S_Reg_17	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	
EWLCJ175S_Reg_18	Verify the AP name in Beacon and Probes fames by configuring Aironet IE and rejoin the AP's to eWLC-2 from eWLC-1.	To check whether AP name in Beacon and Probes fames by configuring Aironet IE and rejoin the AP's to eWLC-2 from eWLC-1.	Passed	
EWLCJ175S_Reg_19	Verify the Multicast filter and MC2UC traffic to local-switching client	To verify the Multicasat filter and local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
EWLCJ175S_Reg_20	Verify the Multicast filter and MC2UC traffic to Central-switching client	To verify the Multicasat filter and central-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
EWLCJ175S_Reg_21	Verify the Multicast filter and Flex AP reboot in connected mode when Flex LS client receiving MC2UC traffic	To verify whether client reassociates and receives MC2UC traffic when flex AP is rebooted in connected mode with multicast filter.	Passed	
EWLCJ175S_Reg_22	Verify the Multicast filter and MC2UC traffic to Central-switching client after Download/upload the configuration file to controller	To verify the Multicasat filter client subscribed to videostreaming receives MC2UC traffic after download/upload the configuration file from controller	Passed	

OKC

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_23	Configure and verify the OKC to the WLAN configuration.	To check whether OKC configured to WLAN or not.	Passed	
EWLCJ175S_Reg_24	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	
EWLCJ175S_Reg_25	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	
EWLCJ175S_Reg_26	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	
EWLCJ175S_Reg_27	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	
EWLCJ175S_Reg_28	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	
EWLCJ175S_Reg_29	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	

EWLCJ175S_Reg_30	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	
EWLCJ175S_Reg_31	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	
EWLCJ175S_Reg_32	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	
EWLCJ175S_Reg_33	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	
EWLCJ175S_Reg_34	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	
EWLCJ175S_Reg_35	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	

EWLCJ175S_Reg_36	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	
EWLCJ175S_Reg_37	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	
EWLCJ175S_Reg_38	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	
EWLCJ175S_Reg_39	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
EWLCJ175S_Reg_40	Configuring TWT in 9115 Ap	To check Whether 9115 Ap get TWT parameter details properly	Passed	
EWLCJ175S_Reg_41	Configuring TWT in 9120 Ap	To check Whether 9120 Ap get TWT parameter details properly	Passed	

EWLCJ175S_Reg_42	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	
EWLCJ175S_Reg_43	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	
EWLCJ175S_Reg_44	Configuring TWT in 11ax Ap with flexconnect mode	To verify the 11ax ap get TWT parameter in flexconnect mode	Passed	
EWLCJ175S_Reg_45	Configuring TWT in 11ax Ap with Local mode	To verify the 11ax ap get TWT parameter in Local mode	Passed	
EWLCJ175S_Reg_46	Associate the sleeping client with 11ax Ap	To Verify sleeping client associate with 11ax Ap properly or not	Passed	
EWLCJ175S_Reg_47	Clear the TWT configuration Check the Client behaviour	To verify the client behaviour after clear the TWT configuration	Passed	

WPA3 Support

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_48	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE security Configuration.	Passed	
EWLCJ175S_Reg_49	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the the Client packets by connecting the windows client to WPA3 and SAE supported SSID	Passed	

EWLCJ175S_Reg_50	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the the Client packets by connecting the Android client to WPA3 and SAE supported SSID	Passed	
EWLCJ175S_Reg_51	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the the Client packets by connecting the Mac os client to WPA3 and SAE supported SSID	Passed	
EWLCJ175S_Reg_52	Verifying the WPA3 support with SAE and PSK security key.	To verify the the Client packets by connecting the client to WPA3 and SAE and PSK supported SSID	Passed	
EWLCJ175S_Reg_53	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 Configuration with SAE and 802.1x supported SSID	Passed	
EWLCJ175S_Reg_54	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	
EWLCJ175S_Reg_55	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	
EWLCJ175S_Reg_56	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ175S_Reg_57	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	
EWLCJ175S_Reg_58	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security for the different clients.	Passed	

EWLCJ175S_Reg_59	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	
EWLCJ175S_Reg_60	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with +Ft_802.1x security for the different clients.	Passed	
EWLCJ175S_Reg_61	Verifying the WPA3 support with Intra clinet roaming by using 9115AP	To verify the Intra clinet roaming by using WPA3 support with 9115AP	Passed	
EWLCJ175S_Reg_62	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	
EWLCJ175S_Reg_63	Verifying the WPA3 support with Roaming between Controllers with Differenet Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with WPA3 WLAN.	Passed	
EWLCJ175S_Reg_64	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	
EWLCJ175S_Reg_65	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 support on all 11ac Wave 2 Indoor APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_66	Verifying the Mesh configuration.	To check whether the Mesh configurations are configuring correct or not.	Passed	

EWLCJ175S_Reg_67	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	
EWLCJ175S_Reg_68	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	
EWLCJ175S_Reg_69	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	
EWLCJ175S_Reg_70	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	
EWLCJ175S_Reg_71	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	
EWLCJ175S_Reg_72	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	
EWLCJ175S_Reg_73	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	
EWLCJ175S_Reg_74	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	
EWLCJ175S_Reg_75	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	

EWLCJ175S_Reg_76	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	
EWLCJ175S_Reg_77	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	
EWLCJ175S_Reg_78	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	
EWLCJ175S_Reg_79	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	
EWLCJ175S_Reg_80	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	
EWLCJ175S_Reg_81	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	
EWLCJ175S_Reg_82	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	
EWLCJ175S_Reg_83	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	

EWLCJ175S_Reg_84	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	
EWLCJ175S_Reg_85	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	
EWLCJ175S_Reg_86	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	
EWLCJ175S_Reg_87	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	
EWLCJ175S_Reg_88	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	
EWLCJ175S_Reg_89	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 loacl	Passed	
EWLCJ175S_Reg_90	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	
EWLCJ175S_Reg_91	Check and verify the intra roaming with bridge mode AP	To check whether intra roaming happening or not with bridge mode Ap's	Passed	

| EWLCJ175S_Reg_92 | 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 | |

iRCM

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_164	Setting UP the secure mobility tunnel between 9800 Controller & 5520 WLC	To check whether both Control & Data path gets UP or not between 9800 Controller & 5520 Controller	Passed	
EWLCJ175S_Reg_165	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	
EWLCJ175S_Reg_166	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	
EWLCJ175S_Reg_167	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	
EWLCJ175S_Reg_168	Configuring the Anchor controller option in 9800 WLC UI	To check whether Anchor option can be configured or not in a 9800 Controller.	Passed	

EWLCJ175S_Reg_169	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	
EWLCJ175S_Reg_170	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	
EWLCJ175S_Reg_171	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	
EWLCJ175S_Reg_172	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	
EWLCJ175S_Reg_173	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	

EWLCJ175S_Reg_174	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	
EWLCJ175S_Reg_175	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	
EWLCJ175S_Reg_176	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	
EWLCJ175S_Reg_177	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	
EWLCJ175S_Reg_178	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	
EWLCJ175S_Reg_179	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	

EWLCJ175S_Reg_180	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	
EWLCJ175S_Reg_181	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	
EWLCJ175S_Reg_182	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	
EWLCJ175S_Reg_183	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	
EWLCJ175S_Reg_184	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	

| EWLCJ175S_Reg_185 | 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 | |
| EWLCJ175S_Reg_186 | 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

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_187	Performing Upgradation using ISSU	To check whether the upgradation is performed or not via ftp	Passed	
EWLCJ175S_Reg_188	Performing Rollback for controller using ISSU.	To check whether the rollback happening for Controller image or not.	Passed	
EWLCJ175S_Reg_189	Disabling the Rollback timer druing upgrading controller using ISSU.	To check that the rollback doesn't happen for Controller image or not.	Passed	
EWLCJ175S_Reg_190	Aborting the upgradation of Controller using ISSU.	To check whether the upgradation for Controller image is aborted or not.	Passed	
EWLCJ175S_Reg_191	Performing Upgradation for controller using ISSU via tftp server.	To check whether the Controller Upgradation via tftp is happening or not.	Passed	

EWLCJ175S_Reg_192	Performing Upgradation for Controller using ISSU via sftp server.	To check whether the Controller Upgradation via sftp is happening or not.	Passed	
EWLCJ175S_Reg_193	Performing Upgradation for controller using ISSU via http server.	To check whether the Controller Upgradation via http is happening or not.	Passed	
EWLCJ175S_Reg_194	Checking the client connectivity	To check whether the client continuously connecting during the upgrade of AP	Passed	

syslog

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_204	Adding syslog server in eWLC and checking the syslog messages in syslog server	To check whether syslogs are generating in syslog server after adding in Ewlc	Passed	
EWLCJ175S_Reg_205	Configuring multiple syslog servers in eWLC and checking the syslog messages in syslog server	To verify whether syslogs are generating in syslog server after adding multiple servers in Ewlc	Passed	
EWLCJ175S_Reg_206	Downloading the syslogs after generated in Ewlc	To check whether able to dowload the syslogs from Ewlc	Passed	
EWLCJ175S_Reg_207	Clearing the logs in controller after generated successfully	To verify whether user able to clear the all generated logs in Ewlc	Passed	
EWLCJ175S_Reg_208	Checking the alert messages after configured syslog server level as "alert"	To check the alert syslogs in syslog server after configured severity level as alert	Passed	
EWLCJ175S_Reg_209	Configuring syslog servers in eWLC with log level setting as critical	To verify the critical logs in syslog server after configuration in device	Passed	

| EWLCJ175S_Reg_210 | Checking the information messages after configured syslog server level as "information" | To check the information syslogs in syslog server after configured severity level as information | Passed | |
| EWLCJ175S_Reg_211 | Checking the debugging messages after configured syslog server level as "debugging" | To check the debugging syslogs in syslog server after configured severity level as debugging | Passed | |

CWA Central Web Authentication

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_212	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	
EWLCJ175S_Reg_213	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	
EWLCJ175S_Reg_214	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	
EWLCJ175S_Reg_215	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	
EWLCJ175S_Reg_216	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	

EWLCJ175S_Reg_217	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	
EWLCJ175S_Reg_218	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 droped or not	Passed	
EWLCJ175S_Reg_219	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	
EWLCJ175S_Reg_220	Associating a different Clients to a SSID which is mapped with ISE by permiting the action in ACL using TCP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permiting the action in ACL using TCP protocol	Passed	
EWLCJ175S_Reg_221	Associating a different Clients to a SSID which is mapped with ISE by permiting the action in ACL using UDP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permiting the action in ACL using UDP protocol	Passed	
EWLCJ175S_Reg_222	Associating a different Clients to a SSID which is mapped with ISE by permiting the action in ACL using ICMP protocol	To verify whether Clients gets connected to SSID which is mapped with ISE by permiting the action in ACL using ICMP protocol	Passed	

EWLCJ175S_Reg_223	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	
EWLCJ175S_Reg_224	Validate whether eWLC is switch between configured Radius servers	To verify whether AAA authentication is occuring when one radius server goes down	Passed	
EWLCJ175S_Reg_225	Reboot the Controller after CWA enabling	To verify whether Configurations are showing same or different after controller reboot	Passed	
EWLCJ175S_Reg_226	Creating a CWA along with ACL Configuration through CLI	To verify whether ACL rule is created or not through CLI	Passed	
EWLCJ175S_Reg_227	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	
EWLCJ175S_Reg_228	Exporting/Importing configuration of CWA	To verify whether export and import is done succesfully	Passed	

MC2UC Video streaming

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_239	MC2UC traffic to local-switching client	To verify that the local-switching client subscribed to videostreaming receives MC2UC traffic	Passed	
EWLCJ175S_Reg_240	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	

Reg_241 MC2UC traffic

EWLCJ175S_Reg_241	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	
EWLCJ175S_Reg_242	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 videostream	Passed	
EWLCJ175S_Reg_243	Client disassociates when receiving MC2UC traffic	To verify whether AP stops sending traffic when client disassociates	Passed	
EWLCJ175S_Reg_244	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	
EWLCJ175S_Reg_245	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	
EWLCJ175S_Reg_246	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	
EWLCJ175S_Reg_247	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	

| EWLCJ175S_Reg_248 | Videstream config sync for LS WLAN in HA setup | To verify whether the videostreaming config for LS WLAN has been synced between the Active and Standby in HA setup | Passed | |
| EWLCJ175S_Reg_249 | 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 | |

UL/DL OFDMA Support for 9130

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_250	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configue 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ175S_Reg_251	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	

Out of band access to standby WLC in a SSO pair

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_252	Configure HA SSO RMI & validate Standby Enviromental Comments	To validate Standby Enviromental Comments	Passed	
EWLCJ175S_Reg_253	Configure HA SSO RMI & validate Standby process Comments	To validate Standby process Comments	Passed	

EWLCJ175S_Reg_254	Configure HA SSO RMI & validate Standby debugging Comments	To validate Standby debugging Comments	Passed	
EWLCJ175S_Reg_255	Configure HA SSO RMI & validate Standby memory Comments	To validate Standby memory Comments	Passed	
EWLCJ175S_Reg_256	Configure HA SSO RMI & validate Standby File System Comments	To validate Standby File System Comments	Passed	
EWLCJ175S_Reg_257	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	
EWLCJ175S_Reg_258	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ175S_Reg_259	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ175S_Reg_260	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ175S_Reg_261	Check process usage details in standby console	To check process usage details in standby console	Passed	

RLAN Support for Fabric and across all modes in IOS-XE

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_262	Configuring RLAN in eWLC via UI	To Configure RLAN in eWLC through UI and check if the RLAN is created or not	Passed	
EWLCJ175S_Reg_263	Checking the client connectivity to RLAN configured with Open security and macfiltering	To verify whether client is connecting to RLAN with open security and macfiltering	Passed	

EWLCJ175S_Reg_264	Enabling the 802.1x security and MAC filtering to RLAN	To create a RLAN with 802.1x security and MAC filtering connecting a windows client to the RLAN and check if the client gets connected to the RLAN port in the AP or not	Passed	
EWLCJ175S_Reg_265	Configuring RLAN with open security and connect two wired clients (windows,MAC)	To verify whether two wired clients gets connected with open security	Passed	
EWLCJ175S_Reg_266	Configuring RLAN with open+macfilter security and connect 2 wired clients (windows,MAC)	To verify whether two wired clients gets connected with open+macfilter security	Passed	
EWLCJ175S_Reg_267	Connecting the client to the RLAN configuring with 802.1x security and host mode as single Host	To verify whether a windows client connecting to the RLAN with 802.1x security and host mode as single Host	Passed	
EWLCJ175S_Reg_268	Configuring RLAN with 802.1x security and host mode as multi host and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi host	Passed	
EWLCJ175S_Reg_269	Configuring RLAN with 802.1x security and host mode as multi domain and connect the client	To verify whether a client connecting to RLAN with 802.1x security and host mode as multi domain	Passed	
EWLCJ175S_Reg_270	Checking the client connectivity to a RLAN with 802.1x security and mapping a AVC profile	To create a RLAN with 802.1x security and applying AVC profile, connecting a windows client to the RLAN and check if the AVC profile gets applied to the client connecting to it or not.	Passed	

EWLCJ175S_Reg_271	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Replace	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Replace	Passed	
EWLCJ175S_Reg_272	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as Shutdown	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Shutdown	Passed	
EWLCJ175S_Reg_273	Checking the client connectivity with 802.1x security and host mode as single Host and violation mode as protect	To verify whether client connecting to a RLAN with 802.1x security and host mode as single host along with violation mode as Protect	Passed	
EWLCJ175S_Reg_274	Rebooting the eWLC after connecting the client to RLAN	Checking whether RLAN configurations showing same or different after rebooting	Passed	
EWLCJ175S_Reg_275	Downgrading the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after downgradingeWLC and also verifying client connectivity	Passed	
EWLCJ175S_Reg_276	Upgrade the eWLC after configuring RLAN and connect the client	Checking whether RLAN configurations showing same or different after upgrading theeWLC and also verifying client connectivity	Passed	

| EWLCJ175S_Reg_277 | Uploading and downloading the config file and checking the RLAN configuration | To verify whether RLAN configurations showing same or different after uploading and downloading file to eWLC and also verifying client connectivity | Passed | |

COS AP Packet Tracer Phase 2

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_278	Enabling client trace dump in 3800 COS AP	To check if the client trace dump is enabled on the 3800 AP and check the behaviour of the AP	Passed	
EWLCJ175S_Reg_279	Enabling client trace dump in 2800 COS AP	To check if the client trace dump is enabled on the 2800 AP and check the behaviour of the AP	Passed	
EWLCJ175S_Reg_280	Enabling client trace dump in 4800 COS AP	To check if the client trace dump is enabled on the 4800 AP and check the behaviour of the AP	Passed	
EWLCJ175S_Reg_281	Capturing client trace dump for the client connected with Open security with 2800 AP	To capture the client trace dump using 2800 AP for the client connected with OPEN security	Passed	
EWLCJ175S_Reg_282	Capturing client trace dump for the client connected with WPA 2 security with 2800 AP	To capture the client trace dump using 2800 AP for the client connected with WPA 2 security	Passed	
EWLCJ175S_Reg_283	Capturing client trace dump for the client connected with WPA 3 security with 2800 AP	To capture the client trace dump using 2800 AP for the client connected with WPA 3 security	Passed	

EWLCJ175S_Reg_284	Capturing client trace dump for the client connected with Open security with 3800 AP	To capture the client trace dump using 3800 AP for the client connected with OPEN security	Passed	
EWLCJ175S_Reg_285	Capturing client trace dump for the client connected with WPA 2 security with 3800 AP	To capture the client trace dump using 3800 AP for the client connected with WPA 2 security	Passed	
EWLCJ175S_Reg_286	Capturing client trace dump for the client connected with WPA 3 security with 3800 AP	To capture the client trace dump using 3800 AP for the client connected with WPA 3 security	Passed	
EWLCJ175S_Reg_287	Capturing client trace dump for the client connected with Open security with 4800 AP	To capture the client trace dump using 4800 AP for the client connected with OPEN security	Passed	
EWLCJ175S_Reg_288	Capturing client trace dump for the client connected with WPA 2 security with 4800 AP	To capture the client trace dump using 4800 AP for the client connected with WPA 2 security	Passed	
EWLCJ175S_Reg_289	Capturing client trace dump for the client connected with WPA 3 security with 4800 AP	To capture the client trace dump using 4800 AP for the client connected with WPA 3 security	Passed	
EWLCJ175S_Reg_290	Analyzing the client trace for windows client conneted to COS AP	To analyze the client trace dump for the windows client connected to COS AP	Passed	
EWLCJ175S_Reg_291	Analyzing the client trace for Android client conneted to COS AP	To analyze the client trace dump for the Android client connected to COS AP	Passed	
EWLCJ175S_Reg_292	Analyzing the client trace for IOS client conneted to COS AP	To analyze the client trace dump for the IOS client connected to COS AP	Passed	

EWLCJ175S_Reg_293	Analyzing the client trace for MAC os client conneted to COS AP	To analyze the client trace dump for the MAC os client connected to COS AP	Passed	
EWLCJ175S_Reg_294	Connecting 4 clients to the COS AP and analyzing the client trace dump in AP	To analyze the client trace dump for the MAC os client connected to COS AP	Passed	
EWLCJ175S_Reg_295	Check if the client trace dump is trigereed when the AP operating in 2.4 GHz	To check if the client trace dump is generated when the AP is operating in 2.4GHz and client connected to it	Passed	
EWLCJ175S_Reg_296	Check if the client trace dump is trigereed when the AP operating in 5 GHz GHz	To check if the client trace dump is generated when the AP is operating in 5 GHz and client connected to it	Passed	

DL 11ax Mu-MIMO for VC/SS APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_297	Configuring 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 5Ghz band.	To configue 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 5Ghz band.	Passed	
EWLCJ175S_Reg_298	Configuring 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU-MIMO & radio parameters for 2.4Ghz band.	Passed	
EWLCJ175S_Reg_299	Verifying details with 11ax Android client connected.	To verify 11ax MU-MIMO details with 11ax Android client connected.	Passed	

EWLCJ175S_Reg_300	Verifying details with 11ax iPhone client connected.	To verify 11ax MU-MIMO details with 11ax iPhone client connected.	Passed	
EWLCJ175S_Reg_301	Verifying details with non 11ax Windows client connected.	To verify 11ax MU-MIMO details with non 11ax Windows client connected.	Passed	
EWLCJ175S_Reg_302	Verifying details with non 11ax Mac client connected.	To verify 11ax MU-MIMO details with non 11ax Mac client connected.	Passed	
EWLCJ175S_Reg_303	Verify details by connecting client to 2.4Ghz radio.	To verify 11ax MU-MIMO details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ175S_Reg_304	Verify MU-MIMO using different models of AP - 9115, 9120, 9130.	To verify MU-MIMO using different models of AP - 9115, 9120, 9130.	Passed	
EWLCJ175S_Reg_305	Check 11ax MU-MIMO support for AP configured in Local mode.	To check 11ax MU-MIMO support for AP configured in Local mode.	Passed	
EWLCJ175S_Reg_306	Check 11ax MU-MIMO support for AP configured in Flex-connect mode.	To check 11ax MU-MIMO support for AP configured in Flex-connect mode.	Passed	
EWLCJ175S_Reg_307	Check 11ax MU-MIMO support for AP configured in Bridge mode.	To check 11ax MU-MIMO support for AP configured in Bridge mode.	Passed	
EWLCJ175S_Reg_308	Check 11ax MU-MIMO support for AP configured in Flex+Mesh mode.	To check 11ax MU-MIMO support for AP configured in Flex+Mesh mode.	Passed	
EWLCJ175S_Reg_309	Verify 11ax MU-MIMO details with client connecting to WPA2 - PSK configured WLAN	To verify 11ax MU-MIMO details with client connecting to WPA2 - PSK configured WLAN	Passed	

EWLCJ175S_Reg_310	Verify 11ax MU-MIMO details with client connecting to WPA3 - Dot1x configured WLAN	To verify 11ax MU-MIMO details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ175S_Reg_311	Connect upto 8 clients and monitor DL/UL 11ax MU-MIMO statistics	To connect upto 8 clients and monitor DL/UL 11ax MU-MIMO statistics	Passed	
EWLCJ175S_Reg_312	Modify spatial stream config to 1 stream and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 1 stream and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ175S_Reg_313	Modify spatial stream config to 2 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 2 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ175S_Reg_314	Modify spatial stream config to 3 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 3 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ175S_Reg_315	Modify spatial stream config to 4 streams and monitor 11ax MU-MIMO statistics.	To modify spatial stream config to 4 streams and monitor 11ax MU-MIMO statistics.	Passed	
EWLCJ175S_Reg_316	Enable videostream and monitor DL/UL 11ax MU-MIMO statistics	To enable videostream and monitor DL/UL 11ax MU-MIMO statistics	Passed	
EWLCJ175S_Reg_317	Modify MCS data rates & monitor 11ax MU-MIMO stats with 11ax Android client connected.	To modify MCS data rates & monitor 11ax MU-MIMO stats with 11ax Android client connected.	Passed	
EWLCJ175S_Reg_318	Check 11ax MU-MIMO stats with roaming client scenario	Check 11ax MU-MIMO stats with roaming client scenario	Passed	

Web UI for Golden Monitor for Packet Drops

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_320	Verify that display of Datapath utlization information for 9800-CL .	To Verify that display of Datapath utlization information for Virtual EWLC in UI is same as CLI.	Passed	
EWLCJ175S_Reg_321	Verify that display of Datapath utlization information for 9800-80	To Verify that display of Datapath utlization information for 9800-80 is same as CLI	Passed	
EWLCJ175S_Reg_322	Verify that display of Datapath utlization information for 9800-L	To Verify that display of Datapath utlization information for 9800-L is same as CLI	Passed	
EWLCJ175S_Reg_323	Verify that display of Datapath utlization information for 9800-40	To Verify that display of Datapath utlization information for Gladius is same as CLI	Passed	
EWLCJ175S_Reg_324	Verify that display of CPU allocation dashlet is not available for appliance based controllers	To Verify that display of CPU allocation dashlet is not available for appliance based controllers same as CLI	Passed	
EWLCJ175S_Reg_325	Verify that display of right unit for tx and rx of packets per port for all controller types	To Verify that display of right unit for tx and rx of packets per port for all controller types same as CLI	Passed	
EWLCJ175S_Reg_326	Verify that display of CPU vs Time graph is shown properly in Appliance based ewlc	To Verify that display of CPU vs Time graph is shown properly as per CLI in Appliance based ewlc	Passed	

EWLCJ175S_Reg_327	Verify that display of CPU allocation during export/import of config files for ewlc 9800-CL	To Verify that display of CPU allocation during export/import of config files for ewlc 9800-CL	Passed	
EWLCJ175S_Reg_328	Verify that display of CPU utilization during backup/restore of config files for appliance based ewlc	To Verify that display of CPU utilization during backup/restore of config files for appliance based ewlc	Passed	
EWLCJ175S_Reg_329	Verify that display of CPU allocation after performing upgrade/downgrade of ewlc 9800-CL	To Verify that display of CPU allocation after performing upgrade/downgrade of ewlc 9800-CL	Passed	
EWLCJ175S_Reg_330	Verify that display of CPU allocation after performing AP upgrade/downgrade for ewlc 9800-CL	To Verify that display of CPU allocation after performing AP upgrade/downgrade for ewlc 9800-CL	Passed	
EWLCJ175S_Reg_331	Verify that display of CPU allocation after Performing Rolling AP upgrade from PI or DNAC then check the CPU Allocation	To Verify that display of CPU allocation after Performing Rolling AP upgrade from PI or DNAC then check the CPU Allocation	Passed	
EWLCJ175S_Reg_332	Verify that display of CPU Utilization after Enabling all the debug commands together	To Verify that display of CPU Utilization after Enabling all the debug commands together	Passed	
EWLCJ175S_Reg_333	Verify that display of Datapath utlization information for eWLC after connecting more than one clients in different AP's .	To Verify that display of Datapath utlization information for eWLC after connecting more than one clients in different AP's .	Passed	

Dynamic Protocol Pack Upgrade - WLC and AP

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_352	Checking the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not	To check if the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not and check if the page is loaded properly	Passed	
EWLCJ175S_Reg_353	Checking the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not with dark mode enabled	To check if the Dynamic Protocol Pack Upgrade tab in AVC page is opening or not with dark mode enabled and check if the page is loaded properly	Passed	
EWLCJ175S_Reg_354	Check the active protocol pack in the controller using the CLI command	To check the active protocol pack in the controller using the CLI command and verify the same using UI	Passed	
EWLCJ175S_Reg_355	Adding the protocol pack for eWLC 9800-40	To upgrade the protocol pack for eWLC for 9800-40	Passed	
EWLCJ175S_Reg_356	Adding the protocol pack for eWLC 9800-80	To upgrade the protocol pack for eWLC for 9800-80	Passed	
EWLCJ175S_Reg_357	Adding the protocol pack for eWLC 9800-L	To upgrade the protocol pack for eWLC for 9800-L	Passed	
EWLCJ175S_Reg_358	Adding the protocol pack for eWLC 9800-CL	To upgrade the protocol pack for eWLC for 9800-CL	Passed	
EWLCJ175S_Reg_359	Deleting the protocol pack upgraded to eWLC 9800-40 to check	To delete the upgraded protocol pack from eWLC 9800-40 and check if the pack is deleted .	Passed	

EWLCJ175S_Reg_360	Deleting the protocol pack upgraded to eWLC 9800-80 to check	To delete the upgraded protocol pack from eWLC 9800-80 and check if the pack is deleted .	Passed	
EWLCJ175S_Reg_361	Deleting the protocol pack upgraded to eWLC 9800-L to check	To delete the upgraded protocol pack from eWLC 9800-CL and check if the pack is deleted .	Passed	
EWLCJ175S_Reg_362	Deleting the protocol pack upgraded to eWLC 9800-CL to check	To delete the upgraded protocol pack from eWLC 9800-CL and check if the pack is deleted .	Passed	
EWLCJ175S_Reg_363	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of bootflash is very less	To check if the upgrade of the protocol pack happens if the space is less in the bootflash of the eWLC 9800-40 device	Passed	
EWLCJ175S_Reg_364	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of bootflash is very less	To check if the upgrade of the protocol pack happens if the space is less in the bootflash of the eWLC 9800-40 device	Passed	
EWLCJ175S_Reg_365	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of bootflash is very less	To check if the upgrade of the protocol pack happens if the space is less in the bootflash of the eWLC 9800-40 device	Passed	

EWLCJ175S_Reg_366	Check if the upgrade of protocol pack happens in eWLC 9800-40 when the memory of bootflash is very less	To check if the upgrade of the protocol pack happens if the space is less in the bootflash of the eWLC 9800-40 device	Passed	
EWLCJ175S_Reg_367	Upgrading the protocol pack and also upgrading the eWLC 9800-40 to watch the protocol pack	To upgarde the protocol pack and eWLC 9800-40 and check ifthe protocol pack if same befor and after upgrading	Passed	
EWLCJ175S_Reg_368	Downgrading the eWLC 9800-40 after upgrading the protocol pack	To downgrade the eWLC 9800-40 after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	
EWLCJ175S_Reg_369	Upgrading the protocol pack and also upgrading the eWLC 9800-80 to watch the protocol pack	To upgarde the protocol pack and eWLC 9800-80 and check ifthe protocol pack if same befor and after upgrading	Passed	
EWLCJ175S_Reg_370	Downgrading the eWLC 9800-80 after upgrading the protocol pack	To downgrade the eWLC 9800-80 after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	
EWLCJ175S_Reg_371	Upgrading the protocol pack and also upgrading the eWLC 9800-CL to watch the protocol pack	To upgarde the protocol pack and eWLC 9800-CL and check ifthe protocol pack if same befor and after upgrading	Passed	
EWLCJ175S_Reg_372	Downgrading the eWLC 9800-CL after upgrading the protocol pack	To downgrade the eWLC 9800-CL after upgrading the protocol pack and check the version of the protocol pack after downgrade	Passed	

| EWLCJ175S_Reg_373 | Upgrading the protocol pack and also upgrading the eWLC 9800-L to watch the protocol pack | To upgarde the protocol pack and eWLC 9800-L and check ifthe protocol pack if same befor and after upgrading | Passed | |
| EWLCJ175S_Reg_374 | Downgrading the eWLC 9800-L after upgrading the protocol pack | To downgrade the eWLC 9800-L after upgrading the protocol pack and check the version of the protocol pack after downgrade | Passed | |

HA SSO RMI

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_375	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	
EWLCJ175S_Reg_376	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ175S_Reg_377	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ175S_Reg_378	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ175S_Reg_379	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ175S_Reg_380	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	
EWLCJ175S_Reg_381	Enable gatway failover, verify output details and monitor devices for switchover.	To enable gatway failover, verify output details & monitor devices for switchover.	Passed	
EWLCJ175S_Reg_382	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	

EWLCJ175S_Reg_383	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ175S_Reg_384	ISSU upgrade with HA SSO RMI	To peform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ175S_Reg_385	Check ISSU downgrade with HA SSO RMI	To peform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ175S_Reg_386	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ175S_Reg_387	Force multiple switchover after upgrade to check if RMI link is up or not	To force multiple switchover after upgrade to check if RMI link is up or not	Passed	
EWLCJ175S_Reg_388	Force multiple switchover and verify AP & client association	To force multiple switchover and verify AP & client association	Passed	
EWLCJ175S_Reg_389	Validate licensing information after ISSU upgrade/downgrade	To validate licensing information after ISSU upgrade/downgrade	Passed	
EWLCJ175S_Reg_390	Validate licensing information after multiple switchover and reload	To validate licensing information after multiple switchover and reload	Passed	
EWLCJ175S_Reg_391	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ175S_Reg_392	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	
EWLCJ175S_Reg_393	Configure HA SSO RMI after RP-clear & validate HA RMI parameters.	To configure HA SSO RMI after RP-clear & validate HA RMI parameters.	Passed	

EWLCJ175S_Reg_394	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ175S_Reg_395	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ175S_Reg_396	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ175S_Reg_397	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ175S_Reg_398	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ175S_Reg_399	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	

Best Practices WebUI

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_412	Enable/Disable the http/https for management	Verify the web UI is able to open or not through http/https after modification	Passed	
EWLCJ175S_Reg_413	Configure the NTP server	To check whether NTP server is able to configure or not for WEB UI	Failed	CSCvw49202
EWLCJ175S_Reg_414	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	
EWLCJ175S_Reg_415	Create the WLAN with WPA2	Verify the WLAN with WPA2 after configuring via best practice	Passed	
EWLCJ175S_Reg_416	Enable the User Login Policies	Checking the User Login Policies is enabled or not	Passed	

EWLCJ175S_Reg_417	Enable the Local Profiling on one or more active WLANs	Verify the enabled Local Profile on Active WLAN	Passed	
EWLCJ175S_Reg_418	Configure the client band for all Active WLANs	To check whether client Band is applied or not for Active WLANs	Passed	
EWLCJ175S_Reg_419	Enable the 5ghz band for Active WLAN	Verify the 5ghz client band on active WLANs	Passed	
EWLCJ175S_Reg_420	Enable the 2.4ghz band for Active WLAN	Checking the 2.4ghz client band on active WLANs	Passed	
EWLCJ175S_Reg_421	Configure the Best channel width	To check whether Best channel width is configured or not on both radios	Passed	
EWLCJ175S_Reg_422	Enable the Flexible Radio Assignment	To check whether Flexible Radio Assignment is enabled or not	Passed	
EWLCJ175S_Reg_423	Configure the Load balance for one or more active WLAN	Verify the Load balance enabled or not on Active WLAN	Passed	
EWLCJ175S_Reg_424	Enable the Auto Dynamic Channel Assignment	To check whether global channel is enabled or not	Passed	

Opn DNS

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_Reg_425	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	
EWLCJ175S_Reg_426	Verifying the created profile mapped with ewc GUI and CLI	To Verify whether the profile mapped with ewc and refleted in ewc GUI & CLI or not	Passed	

EWLCJ175S_Reg_427	Verifying the WLAN created with open DNS configuration	To verify whether the WLAN created with open DNS configuration or not	Passed	
EWLCJ175S_Reg_428	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	
EWLCJ175S_Reg_429	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	
EWLCJ175S_Reg_430	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	
EWLCJ175S_Reg_431	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	
EWLCJ175S_Reg_432	clear the data plane stats in open DNS configuration	To verify whether the data plate stats is cleared or not	Passed	
EWLCJ175S_Reg_433	Perform the roaming between 9115 & 9120 Aps	To verify the open DNs configuration after client roaming between 9115 & 9120 Aps	Passed	
EWLCJ175S_Reg_434	Perform the roaming between two ewc	To verify the open dns after Inter roaming	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_config_1	Username is predefined in eWLC after upgrading to 17.5	To verify the username is predefined or not after upgrading 17.5	Failed	CSCvw29392
EWLCJ175S_config_2	IOSD & Init Memory Leak observed in c9800-40 eWLC	To check the memory leak in c9800-40 eWLC	Failed	CSCvw76287
EWCJ175S_config_3	Password is visible for user accounts in Edge Browser	To check whether the Password is visible or not in edge browser	Failed	CSCvw39897
EWCJ175S_config_7	9800 Ap: debug al crashed multiple crash files with crash loop eg, nginx_pman	To verify al the crash files	Failed	CSCvw60007

SR cases

Logical ID	Title	Description	Status	Defect ID
EWLCJ175S_SR_01	Check smart licensing in 9800 setup.	To check smart licensing in HA setup.	Passed	
EWLCJ175S_SR_02	Check smart licensing in HA setup.	To check smart licensing in HA setup.	Passed	
EWLCJ175S_SR_03	Check license info after multiple reload in HA setup.	To check license info after multiple reload in HA setup.	Passed	
EWLCJ175S_SR_04	Check license info after multiple switchover in HA setup.	To check license info after multiple switchover in HA setup.	Passed	
EWLCJ175S_SR_05	Check license info after upgrading to latest build in HA setup.	To check license info after upgrading to latest build in HA setup.	Passed	

EWLCJ175S_SR_06	Check license info after downgrading to older build in HA setup.	To check license info after downgrading to older build in HA setup.	Passed	
EWLCJ175S_SR_07	Check interface status on multiple switchover in HA setup	To check interface status on multiple switchover in HA setup	Passed	
EWLCJ175S_SR_08	Check interface status on multiple reload in HA setup	To check interface status on multiple reload in HA setup	Passed	
EWLCJ175S_SR_09	Verify client connectivity on channel addition/deletion for 11ax protocol	To verify client connectivity on channel addition/deletion for 11ax protocol	Passed	
EWLCJ175S_SR_10	Verify client connectivity on channel addition/deletion for 5Ghz 11ac protocol	To verify client connectivity on channel addition/deletion for 11ac protocol	Passed	
EWLCJ175S_SR_11	Verify client connectivity on channel addition/deletion for 11n protocol	To verify client connectivity on channel addition/deletion for 11n protocol	Passed	
EWLCJ175S_SR_12	Enable & configure SNMP server on eWLC	To enable & configure SNMP server on eWLC	Passed	
EWLCJ175S_SR_13	Enable & configure SNMP server on eWC	To enable & configure SNMP server on eWC	Passed	
EWLCJ175S_SR_14	Enable & configure SNMP server on Japanese locale	To enable & configure SNMP server on Japanese locale	Passed	
EWLCJ175S_SR_15	Configure non-broadcasted SSID	Configure non-broadcasted SSID and check beacon frames are sent properly	Passed	

EWLCJ175S_SR_16	Configure non-broadcasted SSID	Configure non-broadcasted SSID and check beacon frames are sent properly	Passed	
EWLCJ175S_SR_17	Configure non-broadcasted SSID	Configure non-broadcasted SSID and check beacon frames are sent properly	Passed	
EWLCJ175S_SR_18	Configure non-broadcasted SSID	Configure non-broadcasted SSID and check beacon frames are sent properly	Passed	
EWLCJ175S_SR_19	Verify the nvram configuration after reload	To verify the nvram configuration after reload	Passed	
EWLCJ175S_SR_20	Verify the version of the Boot loader image	To check the boot loader version is displayed correctly or not	Passed	
EWLCJ175S_SR_21	Verify the contents of the Address Resolution Protocol (ARP) table	To verify the contents of the Address Resolution Protocol (ARP) table in CAT9K switch or not	Passed	
EWLCJ175S_SR_22	Verify upgradation of Controller using FTP	To verify if the Controller device's software is upgraded with the latest build	Passed	
EWLCJ175S_SR_23	Verify Upgradation of Controller using TFTP	To verify if the Controller device's software is upgraded with the latest build	Passed	
EWLCJ175S_SR_24	Downgrading Controller Software using FTP	To verify if the Controller device's software is downgraded with the chosen build	Passed	
EWLCJ175S_SR_25	Downgrading Controller Software using TFTP	To verify if the Controller device's software is downgraded with the chosen build	Passed	

EWLCJ175S_SR_26	Upgrade Software by providing a wrong file format in Controller device.	To verify the upgradation of the software update by provide wrong file format.	Passed	
EWLCJ175S_SR_27	Verify the Upgradation of Controller Software without cleaning up the disks	To verify if the Controller device's software is upgraded with the latest build	Passed	
EWLCJ175S_SR_28	Verify the Upgradation of Controller software by interrupting the installation and reinitiating the process	To verify the upgradation of Controller Software by interrupting the installation and reinitiating the process	Passed	
EWLCJ175S_SR_29	Verify Hundred Gig bit interface status in Orthrus device	To verify Hundred Gig bit interface status in Orthrus device	Passed	
EWLCJ175S_SR_30	Verify Hundred Gig bit interface status by giving shutdown/no shutdown commands	to verify Hundred Gig bit interface status by giving shutdown/no shutdown commands	Passed	
EWLCJ175S_SR_31	Verify Hundred Gig bit Mac-link status in Orthrus device	To verify Hundred Gig bit Mac-link status in Orthrus device	Passed	
EWLCJ175S_SR_32	Verify interface swap status in Orthrus device	To verify interface swap status in Orthrus device	Passed	
EWLCJ175S_SR_33	Verify interface status by giving shutdown/no shutdown commands after swapping in Orthrus device	To verify interface status by giving shutdown/no shutdown commands after swapping interface in Orthrus device	Passed	
EWLCJ175S_SR_34	Verify the temperature status of Controller device in CLI	To verify the temperature status of Controller device in CLI	Passed	

EWLCJ175S_SR_35	Verify the temperature summary of a Controller	To verify whether the temperature summary of Controller is displayed correctly or not	Passed	
EWLCJ175S_SR_36	Verify the temperature status of AP through Controller CLI	To verify the temperature status of AP through Controller CLI	Passed	
EWLCJ175S_SR_37	Verify the temperature status of AP through Console and compare with controller CLI	To verify the temperature status of AP through Console and compare with controller CLI	Passed	
EWLCJ175S_SR_38	Verify the temperature status of different Aps through Console and Controller CLI	To verify the temperature status of different Aps through Console and Controller CLI	Passed	
EWLCJ175S_SR_39	Verify the power outage and recovery of a Controller device	To verify the power outage and recovery of a Controller device	Passed	
EWLCJ175S_SR_40	Verify the CPU Usage of Controller device	To verify if the CPU Usage of the Controller device is displayed correctly	Passed	
EWLCJ175S_SR_41	Check the Digital Optical Monitoring in the optical interfaces	To verify whether DOM can show the Optical Rx and Tx levels is:	Passed	
EWLCJ175S_SR_42	Verify whether able to enable Radar channels from 1 to 14 for 2.4 Ghz and 5Ghz for new RF Profile	To verify whether able to enable Radar channels from 1 to 14 for 2.4 Ghz and 5Ghz for new RF Profile	Passed	
EWLCJ175S_SR_43	Verify whether able to enable different Radar Channels for Pre configured client density 5Ghz	To verify whether able to enable different Radar Channels for Pre configured client density 5Ghz	Passed	

EWLCJ175S_SR_44	Verify whether able to enable different Radar Channels for Pre configured client density 2.4Ghz	To verify whether able to enable different Radar Channels for Pre configured client density 2.4Ghz	Passed	
EWLCJ175S_SR_45	Verify whether able to configure Radar Channels for the following 120,124,128 and 144	To verify whether able to configure Radar Channels for the following 120,124,128 and 144	Passed	
EWLCJ175S_SR_46	Verify client connectivity using different Radar Channels with Band 5GHZ band	To verify client connectivity using different Radar Channels with Band 5GHZ band	Passed	
EWLCJ175S_SR_47	Verify client connectivity using different Radar Channels with Band 2.4GHZ band	To verify client connectivity using different Radar Channels with Band 2.4GHZ band	Passed	
EWLCJ175S_SR_48	Configure DHCP and verify ip address assigned to clients	To Configure DHCP and verify ip address assigned to clients	Passed	
EWLCJ175S_SR_49	Configure DHCP with reduced lease time	To Configure DHCP with reduced lease time	Passed	
EWLCJ175S_SR_50	Configure DHCP for specific client mac address	To Configure DHCP for specific client mac address	Passed	
EWLCJ175S_SR_51	Configure with a ip server and hostname server with domain name lookup enabled	To Configure with a ip server and hostname server with domain name lookup enabled	Passed	
EWLCJ175S_SR_52	Configure with a ip server and two hostname server	To Configure with a ip server and two hostname server	Passed	
EWLCJ175S_SR_53	Configure with a ip server and NTP address	To Configure with a ip server and with NTP IP address	Passed	
EWLCJ175S_SR_54	Configure with two NTP servers with stratum lebvel set	To Configure with two dns one hostname and one ip	Passed	

EWLCJ175S_SR_55	Bootup AP and capture logs	To bootup and verify any umwanted messages are displayed in logs	Passed	
EWLCJ175S_SR_56	send wrong config using netconf	To verify device status after sending wrong config using netconf	Passed	
EWLCJ175S_SR_57	Verify no Frequent channel change on XOR radio operating on 5GHz band	To Verify no Frequent channel change on XOR radio operating on 5GHz band	Passed	
EWLCJ175S_SR_58	Verify no Frequent channel change on Slot 1 radio when XOR Radio is also operating on 5GHz band	To Verify no Frequent channel change on Slot 1 radio when XOR Radio is also operating on 5GHz band	Passed	
EWLCJ175S_SR_59	Verify no Frequent channel change on XOR radio operating on 5GHz band when AP mapped to custom-rf-profile	Verify no Frequent channel change on XOR radio operating on 5GHz band when AP mapped to custom-rf-profile	Passed	
EWLCJ175S_SR_60	[EWC-SIT] GUI: Neighbors's page is blank	On the EWC GUI, the Neighbor's page is blank. This page is not applicable to EWC and needs to be removed.	Passed	
EWLCJ175S_SR_61	[EWC-SIT] GUI: Neighbors's page is blank	On the EWLC GUI, the Neighbor's page is blank. This page is not applicable to EWC and needs to be removed.	Passed	
EWLCJ175S_SR_62	[EWC-SIT] GUI: Neighbors's page is blank	On the EWLC GUI, the Neighbor's page is blank. This page is not applicable to EWC and needs to be removed.	Passed	

EWLCJ175S_SR_63	C9800 GUI: Unable to load All Access Point entry while AP image download	When an AP is downloading AP image from C9800 and then we change entry size by searching from AP name (trigger1.png) or selecting items per page (trigger2.png), Even if reload the page again from web browser, the issue is not resolved.	Passed	
EWLCJ175S_SR_64	C9800 GUI: Unable to load All Access Point entry while AP image download	When an AP is downloading AP image from C9800 and then we change entry size by searching from AP name (trigger1.png) or selecting items per page (trigger2.png), Even if reload the page again from web browser, the issue is not resolved.	Passed	
EWLCJ175S_SR_65	C9800 GUI: Unable to load All Access Point entry while AP image download	When an AP is downloading AP image from C9800 and then we change entry size by searching from AP name (trigger1.png) or selecting items per page (trigger2.png), Even if reload the page again from web browser, the issue is not resolved.	Passed	

EWLCJ175S_SR_66	Client goes into 'Exclusionlist' even if the "Client Exclusion is Disabled"	With WPS "client Exclusion Policy" Disabled & WLAN Policy - Client Exclusion Disabled, if the client fails authentication multiple times, it gets moved to "Client Exclusionlist" for the "client exclusion" period available on WLAN policy profile.	Passed	
EWLCJ175S_SR_67	Client goes into 'Exclusionlist' even if the "Client Exclusion is Disabled"	With "Enabliing client exclusion in best practices in EWLC"	Passed	
EWLCJ175S_SR_68	Client goes into 'Exclusionlist' even if the "Client Exclusion is Disabled"	With WPS "client Exclusion Policy" Disabled & WLAN Policy - Client Exclusion Disabled, if the client fails authentication multiple times, it gets moved to "Client Exclusionlist" for the "client exclusion" period available on WLAN policy profile.	Passed	
EWLCJ175S_SR_69	Connecting a 11ax AP with domain as IN to eWLC and check the beacon frames	To connect a 11ax AP with IN domain and check the beacon frames to validate the details in the beacon frames using wireshark	Passed	
EWLCJ175S_SR_70	Connecting a 11ax AP with domain as US to eWLC and check the beacon frames	To connect a 11ax AP with US domain and check the beacon frames to validate the details in the beacon frames using wireshark	Passed	

EWLCJ175S_SR_71	Connecting a 4800 AP with domain as US to eWLC and check the beacon frames	To connect a 4800 AP with US domain and check the beacon frames to validate the details in the beacon frames using wireshark	Passed	
EWLCJ175S_SR_72	Connecting a 3800 AP with domain as IN to eWLC and check the beacon frames	To connect a 3800 AP with IN domain and check the beacon frames to validate the details in the beacon frames using wireshark	Passed	
EWLCJ175S_SR_73	Try disabling 11n radio when the 11ax radio is enabled .	To try disabling 11n radio when 11ax radio is enabled and check the behaviour of the radio after reloading	Passed	
EWLCJ175S_SR_74	Try disabling 11ac radio when the 11ax radio is enabled .	To try disabling 11ac radio when 11ax radio is enabled and check the behaviour of the radio after reloading	Passed	
EWLCJ175S_SR_75	check if the configuration is persistent across reload disabling 11ac and 11n	To check if the configuration is persistent across reload disabling 11ac and 11n	Passed	
EWLCJ175S_SR_76	Connecting a latest version Android client with WPA 3 PSK security	To connect a latest version android client to 9120 AP with the WLAN security as WPA PSK	Passed	
EWLCJ175S_SR_77	Connecting a latest version Android client with WPA 3 802.1x security	To connect a latest version android client to 9120 AP with the WLAN security as WPA 3	Passed	

EWLCJ175S_SR_78	Connecting a latest version Android client with WPA 3 PSK security	To connect a latest version android client to 3800 AP with the WLAN security as WPA PSK	Passed	
EWLCJ175S_SR_79	Connecting a latest version Android client with WPA 3 802.1x security	To connect a latest version android client to 3800 AP with the WLAN security as WPA 3	Passed	
EWLCJ175S_SR_80	Configuring different Syslog facility for 9115 11ax AP in eWLC and checking the same in the APs	To configure different syslog facility for 9115 AP in eWLC AP join profile and validating the same in the AP	Passed	
EWLCJ175S_SR_81	Configuring different Syslog facility for 9120 11ax AP in eWLC and checking the same in the APs	To configure different syslog facility for 9120 AP in eWLC AP join profile and validating the same in the AP	Passed	
EWLCJ175S_SR_82	Configuring different Syslog facility for 1810 AP in eWLC and checking the same in the APs	To configure different syslog facility for 1810 AP in eWLC AP join profile and validating the same in the AP	Passed	
EWLCJ175S_SR_83	Checking the Time zones name for the COS AP in eWLC	To check whether time zones can be modified for the COS AP's	Passed	
EWLCJ175S_SR_84	Checking the Time zones name for the COS AP in eWLC after reload	To check whether time zones can be modified for the COS AP's after reload	Failed	CSCvw67337
EWLCJ175S_SR_85	Checking the ARP issue with Windows 10 client	To check ARP entry issue with Win 10 client	Passed	
EWLCJ175S_SR_86	Checking the ARP issue with mobile client	To check ARP entry issue with mobile client	Passed	

EWLCJ175S_SR_87	Checking the ARP issue with different AP models	To check ARP entry issue with different AP models	Passed	
EWLCJ175S_SR_88	Checking the ARP issue with different security method configured	To check ARP entry issue with different security method configured	Passed	
EWLCJ175S_SR_89	RF-Profile Max Client test in local mode with custom-rf-profile	To check the RF-profile max client test in local mode	Passed	
EWLCJ175S_SR_90	RF-Profile Max Client test in Flex mode with custom-rf-profile	To check the RF-profile max client test in flex mode	Passed	
EWLCJ175S_SR_91	Reduce max-clients count when more clients are connected to AP	To check the client connectivity after reducing max client count	Passed	
EWLCJ175S_SR_92	Checking the payload values after changing the RF profiles	To check the payload values after changing the RF profiles	Passed	
EWLCJ175S_SR_93	Checking the payload values after changing AP Radio(2.4/5 Ghz)	To check the payload values after changing the AP radio(2.4/5 Ghz)	Passed	
EWLCJ175S_SR_94	Verifying the client deletion status	To verify the client deletion status	Passed	
EWLCJ175S_SR_95	Enable the channel for IN regulatory doamin	To verify the Channels able to enable or not foe the IN regulatry domain	Passed	
EWLCJ175S_SR_96	Enable the channel for J4 regulatory doamin	To verify the Channels able to enable or not foe the J4 regulatry domain	Passed	
EWLCJ175S_SR_97	Enable the channel for J4 regulatory doamin via CLI	To verify the Channels able to enable or not foe the IN regulatry domain	Passed	
EWLCJ175S_SR_98	Joining the 4800 ap to the controller latest image	To verify the ap join to the contorller or not	Passed	

EWLCJ175S_SR_99	Joining the 3800 /2800 ap to the controller latest image	To verify the ap join to the contorller or not	Passed	
EWLCJ175S_SR_100	Joining the 9130 ap to the controller latest image	To verify the ap join to the contorller or not	Passed	
EWLCJ175S_SR_101	Joining the 9115 ap to the controller latest image	To verify the ap join to the contorller or not	Passed	
EWLCJ175S_SR_102	Joining the 9120 ap to the controller latest image	To verify the ap join to the contorller or not	Passed	
EWLCJ175S_SR_103	Associate the client to open security type form dot1x	To check whether the client associated or not	Passed	
EWLCJ175S_SR_104	Associate the client to PSK+Mac filter security type form dot1x	To check whether the client associated or not	Passed	
EWLCJ175S_SR_105	Associate the client to PSK security type form dot1x	To check whether the client associated or not	Passed	
EWLCJ175S_SR_106	Configuring TWT 9130 ap with altest image	To verify the TWT configuration suppoeted or not	Passed	
EWLCJ175S_SR_107	Configuring TWT 9115 ap with altest image	To verify the TWT configuration suppoeted or not	Passed	
EWLCJ175S_SR_108	Configuring TWT 9120 ap with altest image	To verify the TWT configuration suppoeted or not	Passed	
EWLCJ175S_SR_109	Verify the Crash in ewc	To Verify the Crash in ewc	Passed	
EWLCJ175S_SR_110	Verify the Crash in ewlc	To Verify the Crash in ewlc	Passed	
EWLCJ175S_SR_111	Verifying the Android client Connection statusbased in 2.4 and 5 G radio.	To verify the client connection status based in 2.4 and 5 G radio.	Passed	

EWLCJ175S_SR_112	Verifying the MAC client Connection statusbased in 2.4 and 5 G radio.	To verify the client connection status based in 2.4 and 5 G radio.	Passed	
EWLCJ175S_SR_113	Verifying the Windows client Connection statusbased in 2.4 and 5 G radio.	To verify the client connection status based in 2.4 and 5 G radio.	Passed	
EWLCJ175S_SR_114	Verify the Ap upgrade in 9115	To Verify the Ap upgrade in 9115	Passed	
EWLCJ175S_SR_115	Verify the Ap upgrade in 9120	To Verify the Ap upgrade in 9120	Passed	
EWLCJ175S_SR_116	Verify the Ap upgrade in 9130	To Verify the Ap upgrade in 9130	Passed	
EWLCJ175S_SR_117	verify the channels in 2.4 and 5 G in 9115	To verify the channels in 2.4 and 5 G in 9115	Passed	
EWLCJ175S_SR_118	verify the channels in 2.4 and 5 G in 9120	To verify the channels in 2.4 and 5 G in 9120	Passed	
EWLCJ175S_SR_119	verify the channels in 2.4 and 5 G in 9130	To verify the channels in 2.4 and 5 G in 9130	Passed	

Related Documents

-

Related Documentation

CME 8.10 release 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 3.9 User Guide

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

ISE 3.0 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-4/config-guide/b_wl_17_4_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.4 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-4/config-guide/b_wl_17_4_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.4 Release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-4/release-notes/rn-17-4-9800.html

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-dec20.html

Cisco Catalyst 9600 Series Switches 17.4 Release Notes

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-4/release_notes/ol-17-4-9600.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/2-1-2/release_notes/b_cisco_dna_center_rn_2_1_2.html