Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.8 for Japan (Release Version 17.8)

First Published: 2022-05-02

Last Modified: 2022-05-05

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

CONTENTS

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 17.8
- 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 Catalyst 9800-CL Wireless Controller for Cloud
- Cisco Embedded Wireless Controller on Catalyst Access Points
- Cisco DNA Spaces
- Cisco DNA Connector
- ISE(VM)
- Cisco ISR 1100
- Cisco AP c9115
- Cisco AP c9120
- Cisco AP c9130
- Cisco AP c9105
- Access Point 4800
- Access Point 1810

Acronyms

Acronym	Description
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server
AKM	Authentication Key Management

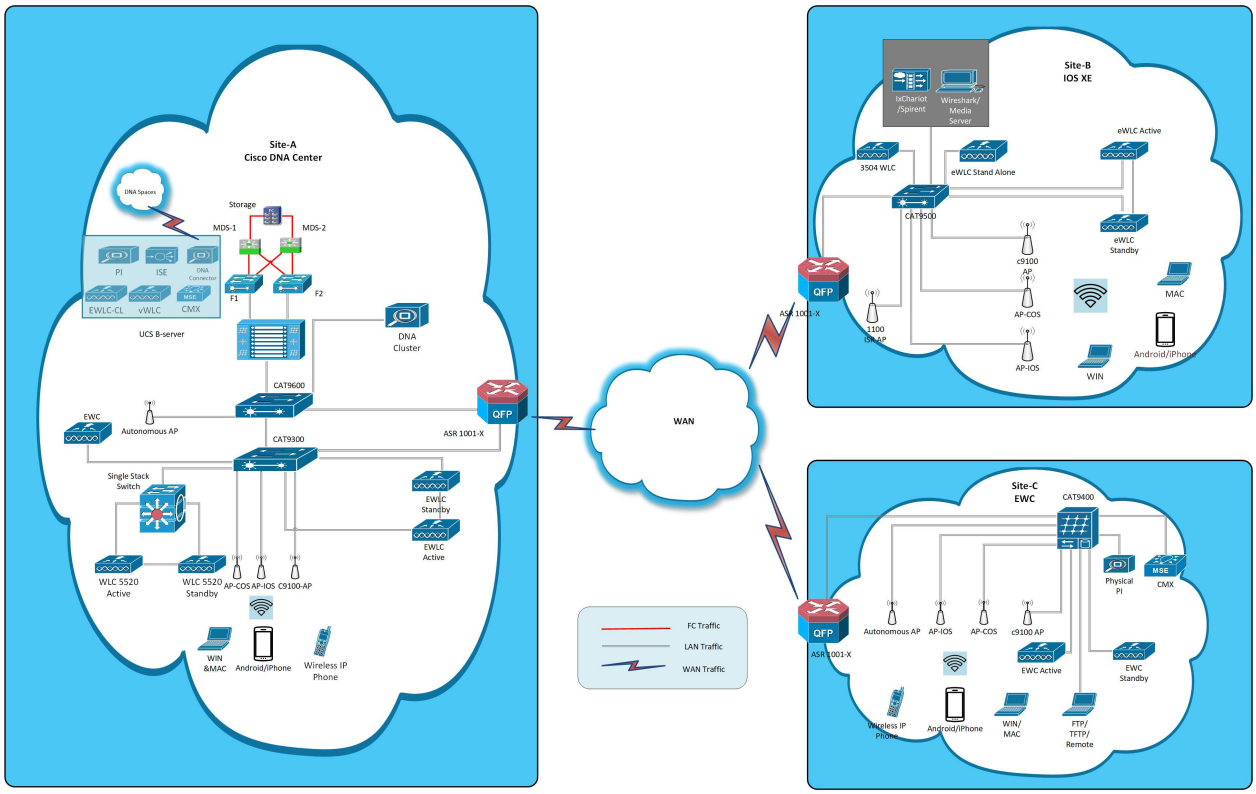
Acronym	Description
AP	Access Point
API	Application Programming Interface
APIC-EM	Application Policy Infrastructure Controller - Enterprise Module
ATF	Air-Time Fairness
AVC	Application Visibility and Control.
BGN	Bridge Group Network
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CA	Central Authentication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

Acronym	Description
FTP	File Transfer Protocol
FW	Firm Ware
HA	High Availability
H-REAP	Hybrid Remote Edge Access Point
IOS	Internetwork Operating System
ISE	Identity Service Engine
ISR	Integrated Services Router
LAG	Link Aggregation
LEAP	Lightweight Extensible Authentication Protocol
LSS	Location Specific Services
LWAPP	Lightweight Access Point Protocol
MAP	Mesh Access Point
MCS	Modulation Coding Scheme
MFP	Management Frame Protection
mDNS	multicast Domain Name System
MIC	Message Integrity Check
MSE	Mobility Service Engine
MTU	Maximum Transmission Unit
NAC	Network Admission Control
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCS	Network Control System
NGWC	Next Generation Wiring closet
NMSP	Network Mobility Services Protocol
OEAP	Office Extended Access Point
PEAP	Protected Extensible Authentication Protocol
PEM	Policy Enforcement Module
PI	Prime Infrastructure
PMF	Protected Management Frame
POI	Point of Interest
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Pre-shared Key

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

Test topology and Environment Matrix

Test Topology



Component Matrix

Category	Component	Version
Controller	Cisco Catalyst 9800-40 Wireless Controller	17.8
	Cisco Catalyst 9800-80 Wireless Controller	17.8
	Cisco Catalyst 9800-CL Wireless Controller for Cloud	17.8
	Cisco Catalyst 9800-L Wireless Controller	17.8
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.8
	Virtual Controller	8.10.121.0
Applications	Cisco DNA Center	2.3.3
	Cisco DNA Spaces	Cloud (Mar 2022)
	Cisco DNA Spaces Connector	2.3.2
	Prime Infrastructure (Virtual Appliance, UCS based)	3.9
	ISE(VM)	3.1
	Cisco Jabber for Windows, iPhone	14.1
	Cisco Air Provisioning App	1.7.4
	Cisco Wireless App	1.1.113
Access Point	Cisco AP 9115	17.8
	Cisco AP 9120	17.8
	Cisco AP 9130	17.8
	Cisco AP 9105	17.8
	Cisco 1100 ISR	17.8
	Cisco AP 4800	15.3
	Cisco AP 1810	15.3

Category	Component	Version
Switch	Cisco Cat 9300	17.8
	Cisco Cat 9200L	17.8
	Cisco Cat 9800	17.8
	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
Chipset	5300, 6300 AGN	15.18.0.1
	7265 AC	21.40.2
	Airport Extreme	7.9.1
Client	Operating System(JOS)	Windows 8 & 8.1 Enterprise
		Windows XP Professional
		Windows 10 & 11
	Apple Mac Book Pro, Apple Mac Book Air (JP Locale)	Mac OS 11.5
	iPad Pro	iOS 15.1
	iPhone 6, 6S ,7 & 11 (JP Locale)	iOS 14.2
	Samsung Galaxy S7,S10, Nexus 6P, Sony Xperia XZ	Android 11
	Wireless IP Phone 8821	11.0.4-14
	End points	Windows 7 Enterprise
		Apple Mac 11.2.1
		Windows 8 & 8.1
		iPhone 6,6S ,7 & 11
		Windows 10
		Windows 11
		Samsung Galaxy S4, S7,S10, Nexus 6P, Sony Xperia
	Cisco AnyConnect VPN Client	4.9.01095
	MS surface GO & GO2	Windows 10
Module	Hyper location Module	NA
Active Directory	AD	Windows server 2022
Call Control	Cisco Unified Communications Manager	12.5.0.99832-3/12.5.0.99832-3-1(JP)

Category	Component	Version
Browsers	IE	11.0
	Mozilla Firefox	99
	Safari	15.3
	Chrome	101.0.4951.41

What's New ?

Cisco Catalyst 9800 Series Wireless Controller

- Ability to configure XOR radio for APs in Sniffer mode
- CLI boot system statement needs clarification
- COS AP packet tracer phase 2
- Need support for TrustSec SGT inline tagging over port channel uplink
- OEAP URL based ACLs for split tunnel
- Per client Bidirectional rate limiting, flex local switching.
- SFP support with C9800
- SSID Scheduler
- WPA3 Supporting 'Transition Disable

EWC

- Anchored SSID support on EWC
- WPA3 Supporting 'Transition Disable'
- Windows 11 Support and MAC 12 Support
- Support Scheduling of SSID broadcast
- Per client Bidirectional rate limiting, flex local switching.

Open Caveats

Defect ID	Title
CSCwb52050	eWC UI : help link contents are not available for AAA configuration
CSCwb19471	Joined APs count not updated in Location dashboard and joined AP is also shown in Available APs
CSCwb22034	eWLC Wireless AP option shows "Unrecognized command' in CLI Mode
CSCwb26624	Incorrect data is showing for uptime and power derate capable
CSCwb51536	UI Alignment Misplaced - ACL page
CSCwb56577	eWC Japanese UI : help link contents are not available for DNS & shows broken link page
CSCwb65684	AP join profile dialog box - power management tab issue
CSCwb56783	Able to create user account by using the username as " "
CSCwa83779	Static WEP security parameters are changing every time
CSCwa83915	JP Locale: Link Aggregation (LAG) Status fields are missed
CSCwa96072	Sniffer channel XOR radio range is showing as 0-255 in CLI
CSCwa93072	Calendar profile spelling correction needs to be modified in CLI
CSCwb56984	Unable to create Wireless Setup ->Basic Profile
CSCwb57089	Define New option is not available to define ACL for Wireless Setup ->Basic
CSCwb31009	Unable to save the configuration if Enter Key is pressed in WLANs Text Boxes
CSCwb56923	Transition Mode WLAN Id error validation is not fully visible
CSCwb32331	EWC - Blank space gets appended on checking wlan details
CSCwb57945	WLANs page is not loading after removing CCKM Timestamp Tolerance
CSCwb49851	eWlC Cli : showing % Ambiguous command

CSCwb57095	eWLC UI: button is overlapping on APs , clearly not visible
CSCwa84592	JP Locale: Unable to configure None OWE security
CSCwb57110	Unable to choose Wireless Setup dropdown list
CSCwb57380	WLAN ID valid input is showing as 1 to 4096 and error validation is not showing
CSCwa83403	Lobby Admin Access is disabled automatically
CSCwb37258	Profile Name and SSID ASCII characters length is showing as wrong for Help guide
CSCwa80672	English Locale: Some fields are missed in All Access Points page
CSCwb17887	JA Locale: Need help and Wireless Debug Analyzer links are not available
CSCwb59234	Max client connection allowed range is showing as (0-10000)
CSCwb59244	WLAN - Local EAP Authentication enable and saved issue
CSCwb59252	Local Policy Page - Add & Delete key Disable issue
CSCwb65650	JA Locale : wlan dropdown textbox popup issue

Resolved Caveats

Defect ID	Title
CSCwb37066	eWLC JA Locale: Need help link is not available

New Features

Ability to configure XOR radio for APs in Sniffer mode

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Xor_1	Configure Sniffer for Dual band radios	To configure Sniffer for Dual band radios	Passed	
EWLCJ178S_Xor_2	Change the XOR radio assignment mode to client-serving/ monitor/Sniffer	To verify XOR radio assignment mode changed or not	Passed	
EWLCJ178S_Xor_3	Verify AP mode is Sniffer after AP reload	To verify ap mode after reload	Passed	
EWLCJ178S_Xor_4	Configure Sniffer for Dual band radios through CLI	To configure Sniffer for Dual band radios through CLI	Failed	CSCwa96072
EWLCJ178S_Xor_5	Validate unable to set sniffer details error message	To validate unable to set sniffer details error message	Passed	
EWLCJ178S_Xor_6	XOR radio band switching from 2.4 Ghz to 5 Ghz	To capture Sniffer from 2.4 Ghz to 5 Ghz	Passed	
EWLCJ178S_Xor_7	XOR radio band switching from 5 Ghz to 2.4 Ghz	To capture Sniffer from 5 Ghz to 2.4 Ghz	Passed	
EWLCJ178S_Xor_8	Perform band switching multiple times and capture packets	Tp perform band switching multiple times and to capture packets	Passed	
EWLCJ178S_Xor_9	Perform band switching every one minute for 10 times	To perform band switching every one minute for 10 times	Passed	
EWLCJ178S_Xor_10	Change mode from local to flex and capture network activity	To capture network activity when AP mode changed from local to flex	Passed	
EWLCJ178S_Xor_11	Change mode from flex to local and capture network activity	To capture network activity when AP mode changed from flex to local	Passed	

EWLCJ178S_Xor_12	Check whether alert is triggered or not when AP mode changed to Sniffer	To check whether alert is triggered or not when AP mode changed to Sniffer	Passed	
EWLCJ178S_Xor_13	Check whether alert is triggered or not when Sniffer details modified	To check whether alert is triggered or not when Sniffer details modified	Passed	
EWLCJ178S_Xor_14	Verify Sniffer Channel range	To verify Sniffer Channel range	Passed	

CLI boot system statement needs clarification

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_CLIboot_1	Verify WORD option in boot config is removed or not	To verify WORD option in boot config is removed or not	Passed	
EWLCJ178S_CLIboot_2	Verify local file system is specified or not after selecting flash option	To verify local file system is specified or not after selecting flash option	Passed	
EWLCJ178S_CLIboot_3	Verify Local file system display files	To verify Local file system display files	Passed	
EWLCJ178S_CLIboot_4	Verify autocomplete filenames or filesystems in config	To verify autocomplete filenames or filesystems in config	Passed	
EWLCJ178S_CLIboot_5	Verify file system for remote file systems	To verify file system for remote file systems	Passed	
EWLCJ178S_CLIboot_6	Verify Boot system config command if file is not present in boot flash at the time of bulk sync in switchover case	To verify Boot system config command if file is not present in boot flash at the time of bulk sync in switchover case	Passed	
EWLCJ178S_CLIboot_7	Verify words given after the “boot system"	Verification for the Word given after the “boot system"	Passed	
EWLCJ178S_CLIboot_8	Verify appropriate error is triggered or not if file not present in local file systems	To verify appropriate error is triggered if file not present in local file systems	Passed	

COS AP packet tracer phase 2

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_PTrace_1	Configure AP Packet Capture on 9800-40 Wireless Controller	To configure AP Packet Capture on 9800-40 Wireless Controller	Passed	
EWLCJ178S_PTrace_2	Configure AP Packet Capture on 9800-80 Wireless Controller	To configure AP Packet Capture on 9800-80 Wireless Controller	Passed	
EWLCJ178S_PTrace_3	Configure AP Packet Capture on 9800-CL Wireless Controller	To configure AP Packet Capture on 9800-CL Wireless Controller	Passed	
EWLCJ178S_PTrace_4	Configure AP Packet Capture on 9800 HA setup Wireless Controller	To configure AP Packet Capture on 9800 HA setup Wireless Controller	Passed	
EWLCJ178S_PTrace_5	Verify packet capture when client moves between SSIDs	To verify packet capture when client moves between SSIDs	Passed	
EWLCJ178S_PTrace_6	Verify packet capture when client roams between APs	To verify packet capture when client roams between APs	Passed	
EWLCJ178S_PTrace_7	Capture ICMP and DHCP packets in AP -Windows	By applying IPv4/IPv6 post authentication ACL list to AP, can drop the packet inside AP for ICMP, DHCP and DHCPv6 packet inside AP	Passed	
EWLCJ178S_PTrace_8	Capture ICMP and DHCP packets in AP - Android	By applying IPv4/IPv6 post authentication ACL list to AP, can drop the packet inside AP for ICMP, DHCP and DHCPv6 packet inside AP	Passed	

EWLCJ178S_PTrace_9	Capture ICMP and DHCP packets in AP - MAC	By applying IPv4/IPv6 post authentication ACL list to AP, can drop the packet inside AP for ICMP, DHCP and DHCPv6 packet inside AP	Passed	
EWLCJ178S_PTrace_10	Capture ICMP and DHCP packets in AP - IOS	By applying IPv4/IPv6 post authentication ACL list to AP, can drop the packet inside AP for ICMP, DHCP and DHCPv6 packet inside AP	Passed	
EWLCJ178S_PTrace_11	Capture ICMP and DHCP packets in AP - Surface Go	By applying IPv4/IPv6 post authentication ACL list to AP, can drop the packet inside AP for ICMP, DHCP and DHCPv6 packet inside AP	Passed	
EWLCJ178S_PTrace_12	Capture ARP and ICMP packets in AP - Windows	Track ARP and ICMP packets by applying the pre authentication ACL lists to AP with web auth	Passed	
EWLCJ178S_PTrace_13	Capture ARP and ICMP packets in AP - Android	Track ARP and ICMP packets by applying the pre authentication ACL lists to AP with web auth	Passed	
EWLCJ178S_PTrace_14	Capture ARP and ICMP packets in AP - MAC	Track ARP and ICMP packets by applying the pre authentication ACL lists to AP with web auth	Passed	

EWLCJ178S_PTrace_15	Capture ARP and ICMP packets in AP - IOS	Track ARP and ICMP packets by applying the pre authentication ACL lists to AP with web auth	Passed	
EWLCJ178S_PTrace_16	Capture ARP and ICMP packets in AP - Surface Go	Track ARP and ICMP packets by applying the pre authentication ACL lists to AP with web auth	Passed	
EWLCJ178S_PTrace_17	Capture EAP packets in AP - Windows	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ178S_PTrace_18	Capture EAP packets in AP - Android	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ178S_PTrace_19	Capture EAP packets in AP - IOS	Capturing the EAP packets during client initial connection with AP	Failed	CSCwb17887
EWLCJ178S_PTrace_20	Capture EAP packets in AP - MAC	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ178S_PTrace_21	Capture EAP packets in AP - Surface Go	Capturing the EAP packets during client initial connection with AP	Passed	

Need support for TrustSec SGT inline tagging over port channel uplink

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_SGT_1	Check if inline tagging is configured in Trustsec	To check if inline tagging is configured in Trustsec	Passed	
EWLCJ178S_SGT_2	Enforce trustsec tagging using 9800-40 controller	To enforce trustsec tagging using 9800-40 controller	Passed	
EWLCJ178S_SGT_3	Enforce trustsec tagging using 9800L controller	To enforce trustsec tagging using 9800L controller	Passed	
EWLCJ178S_SGT_4	Enforce trustsec tagging using 9800CL controller	To enforce trustsec tagging using 9800CL controller	Passed	
EWLCJ178S_SGT_5	Enforce trustsec tagging using 9800 HA controller	To enforce trustsec tagging using 9800 HA controller	Passed	
EWLCJ178S_SGT_6	Enforce trustsec tagging using EWC controller	To enforce trustsec tagging using EWC controller	Passed	
EWLCJ178S_SGT_7	Check trustsec enforcement using WLAN with WPA3 security	To check trustsec enforcement using WLAN with WPA3 security	Passed	
EWLCJ178S_SGT_8	Check trustsec enforcement using WLAN with WPA2 security	To check trustsec enforcement using WLAN with WPA2 security	Passed	
EWLCJ178S_SGT_9	Check trustsec enforcement with Windows client	To check trustsec enforcement with Windows client	Passed	
EWLCJ178S_SGT_10	Check trustsec enforcement with Mac client	To check trustsec enforcement with MAC client	Passed	
EWLCJ178S_SGT_11	Check trustsec enforcement with Android client	To check trustsec enforcement with Android client	Passed	

EWLCJ178S_SGT_12	Check trustsec enforcement with roaming client	To check trustsec enforcement with roaming client	Passed	
EWLCJ178S_SGT_13	Check trustsec enforcement with multiple client scenario	To check trustsec enforcement with multiple client scenario	Passed	

OEAP URL based ACLs for split tunnel

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_OEAP_1	Configure an Access Control List for Split Tunnelling	To configure an Access Control List for Split Tunnelling	Passed	
EWLCJ178S_OEAP_2	Link ACL Policy to the Defined ACL	To link ACL Policy to the Defined ACL	Passed	
EWLCJ178S_OEAP_3	Configure a Wireless Profile Policy and a Split MAC ACL Name	To configure a Wireless Profile Policy and a Split MAC ACL Name	Passed	
EWLCJ178S_OEAP_4	Configure Office Extend AP through GUI	To configure Office Extend AP through GUI	Failed	CSCwa83915
EWLCJ178S_OEAP_5	Configure Office Extend AP through CLI	To configure Office Extend AP through CLI	Passed	
EWLCJ178S_OEAP_6	Verify whether your able to access the Access Point Office Extend through GUI or not	To verify whether your able to access the Access Point Office Extend through GUI or not	Passed	
EWLCJ178S_OEAP_7	Connect Windows Client for Office Extend AP	To connect Windows Client for Office Extend AP	Passed	
EWLCJ178S_OEAP_8	Connect Android Client for Office Extend AP	To connect Android Client for Office Extend AP	Passed	
EWLCJ178S_OEAP_9	Connect Go Plus Client for Office Extend AP	To connect Go Plus Client for Office Extend AP	Passed	
EWLCJ178S_OEAP_10	Connect MAC Client for Office Extend AP	To connect MAC Client for Office Extend AP	Passed	
EWLCJ178S_OEAP_11	Connect IOS Client for Office Extend AP	To connect IOS Client for Office Extend AP	Passed	
EWLCJ178S_OEAP_12	Verify Locally switched traffic using Packet Capture	To verify Locally switched traffic using Packet Capture	Passed	

EWLCJ178S_OEAP_13	Connect any client through centralized SSID	To connect any client through centralized SSID	Passed	
EWLCJ178S_OEAP_14	Verify Office Extend AP details	To verify Office Extend AP details	Passed	
EWLCJ178S_OEAP_15	Verify whether your able to access Office Extend Access Point through a browser or not for 9105 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 9105 AP	Passed	
EWLCJ178S_OEAP_16	Verify whether your able to access Office Extend Access Point through a browser or not for 9120 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 9120 AP	Passed	
EWLCJ178S_OEAP_17	Verify whether your able to access Office Extend Access Point through a browser or not for 9130 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 9130 AP	Passed	
EWLCJ178S_OEAP_18	Verify whether your able to access Office Extend Access Point through a browser or not for 4800 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 4800 AP	Passed	
EWLCJ178S_OEAP_19	Verify MAC Filtering for Office Extend Access Point	To verify MAC Filtering for Office Extend Access Point	Passed	
EWLCJ178S_Reg_370	Configure an Access Control List for Split Tunnelling	To configure an Access Control List for Split Tunnelling	Failed	CSCwb51536
EWLCJ178S_Reg_371	Link ACL Policy to the Defined ACL	To link ACL Policy to the Defined ACL	Passed	
EWLCJ178S_Reg_372	Configure a Wireless Profile Policy and a Split MAC ACL Name	To configure a Wireless Profile Policy and a Split MAC ACL Name	Passed	
EWLCJ178S_Reg_373	Configure Office Extend AP through GUI	To configure Office Extend AP through GUI	Passed	

EWLCJ178S_Reg_374	Configure Office Extend AP through CLI	To configure Office Extend AP through CLI	Passed	
EWLCJ178S_Reg_375	Verify whether your able to access the Access Point Office Extend through GUI or not	To verify whether your able to access the Access Point Office Extend through GUI or not	Passed	
EWLCJ178S_Reg_376	Connect Windows Client for Office Extend AP	To connect Windows Client for Office Extend AP	Passed	
EWLCJ178S_Reg_377	Connect Android Client for Office Extend AP	To connect Android Client for Office Extend AP	Passed	
EWLCJ178S_Reg_378	Connect Go Plus Client for Office Extend AP	To connect Go Plus Client for Office Extend AP	Passed	
EWLCJ178S_Reg_379	Connect MAC Client for Office Extend AP	To connect MAC Client for Office Extend AP	Passed	
EWLCJ178S_Reg_380	Connect IOS Client for Office Extend AP	To connect IOS Client for Office Extend AP	Passed	
EWLCJ178S_Reg_381	Verify Locally switched traffic using Packet Capture	To verify Locally switched traffic using Packet Capture	Passed	
EWLCJ178S_Reg_382	Connect any client through centralized SSID	To connect any client through centralized SSID	Passed	
EWLCJ178S_Reg_383	Verify Office Extend AP details	To verify Office Extend AP details	Passed	
EWLCJ178S_Reg_384	Verify whether your able to access Office Extend Access Point through a browser or not for 9105 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 9105 AP	Passed	
EWLCJ178S_Reg_385	Verify whether your able to access Office Extend Access Point through a browser or not for 9120 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 9120 AP	Passed	

EWLCJ178S_Reg_386	Verify whether your able to access Office Extend Access Point through a browser or not for 9130 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 9130 AP	Passed	
EWLCJ178S_Reg_387	Verify whether your able to access Office Extend Access Point through a browser or not for 4800 AP	To verify whether your able to access Office Extend Access Point through a browser or not for 4800 AP	Passed	
EWLCJ178S_Reg_388	Verify MAC Filtering for Office Extend Access Point	To verify MAC Filtering for Office Extend Access Point	Passed	

Per client Bidirectional rate limiting, flex local switching

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_RateLimit_1	Configuring rate limit for per client for Android client with WPA 2 Personal security with QOS as Silver	To configure rate limit for client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ178S_RateLimit_2	Configuring rate limit for per client for S10 client with WPA 2 Personal security with QOS as Silver	To configure rate limit for S10 client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ178S_RateLimit_3	Configuring rate limit for per client for Mac OS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Mac OS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ178S_RateLimit_4	Configuring rate limit for per client for IOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for IOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWLCJ178S_RateLimit_5	Configuring rate limit for per client with QOS as Gold for S10 client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a S10 client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	

EWLCJ178S_RateLimit_6	Configuring rate limit for per client with QOS as Gold for Android client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Android client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWLCJ178S_RateLimit_7	Configuring rate limit for per client with QOS as Gold for IOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a IOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWLCJ178S_RateLimit_8	Configuring rate limit for per client with QOS as Gold for Mac OS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Mac OS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWLCJ178S_RateLimit_9	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behaviour of the client is same or not	Passed	
EWLCJ178S_RateLimit_10	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Passed	

EWLCJ178S_RateLimit_11	Creating a AVC rule for the WLAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	
EWLCJ178S_RateLimit_12	Check if windows client works for bidirectional rate limit	To check if windows client works for bidirectional rate limit	Passed	
EWLCJ178S_RateLimit_13	Check if rate limit varies post roaming scenario	To check if rate limit varies post roaming scenario	Passed	
EWLCJ178S_RateLimit_14	Verify rate limit for different models of AP	Verify rate limit for different models of AP	Passed	
EWCJ178S_RateLimit_1	Configuring rate limit for per client for Android client with WPA 2 Personal security with QOS as Silver	To configure rate limit for client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWCJ178S_RateLimit_2	Configuring rate limit for per client for S10 client with WPA 2 Personal security with QOS as Silver	To configure rate limit for S10 client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWCJ178S_RateLimit_3	Configuring rate limit for per client for Mac OS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for Mac OS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	

EWCJ178S_RateLimit_4	Configuring rate limit for per client for IOS client with WPA 2 Personal security with QOS as Silver	To configure rate limit for IOS client with open security and QOS as silver and check if the client gets the rate that is been configured or not.	Passed	
EWCJ178S_RateLimit_5	Configuring rate limit for per client with QOS as Gold for S10 client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a S10 client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWCJ178S_RateLimit_6	Configuring rate limit for per client with QOS as Gold for Android client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Android client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWCJ178S_RateLimit_7	Configuring rate limit for per client with QOS as Gold for IOS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a IOS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	
EWCJ178S_RateLimit_8	Configuring rate limit for per client with QOS as Gold for Mac OS client with WPA 2 Enterprise security	To configure rate limit per client with QOS as Gold and connecting a Mac OS client with WPA 2 Enterprise security and check if the rate limit is applied or not.	Passed	

EWCJ178S_RateLimit_9	Connecting a client to a WLAN configured with rate limit using two different AP	To configure rate limit for client and connecting a client to one AP and check the rate limit and making that AP down and connecting the client to other AP and check if the behaviour of the client is same or not	Passed	
EWCJ178S_RateLimit_10	Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	To Connecting a client to a WLAN configured with rate limit using one ME capable AP and Non Me capable AP in AP group	Failed	CSCwb59234
EWCJ178S_RateLimit_11	Creating a AVC rule for the WLAN for which rate limit is configured .	To configure lesser rate limit in WLAN and configuring higher rate limit in AVC and check if the rate limit for the client	Passed	

SFP support with C9800

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_SFP_1	Connecting a SFP in 9800-80 eWLC	To connect a SFP in eWLC 9800-80 and check if the SFP is detected or not.	Passed	
EWLCJ178S_SFP_2	Connecting different SFP in 9800-80 eWLC	To connect a SFP in eWLC 9800-80 and check if the SFP is detected or not.	Passed	
EWLCJ178S_SFP_3	Connecting multiple same type SFP at one instance in 9800-80 eWLC	To connect multiple same SFP at the same time in 9800-80 eWLC and check if all the SFP are detected and check the behaviour	Passed	
EWLCJ178S_SFP_4	Connecting multiple different type SFP at same time in 9800-80 eWLC	To connect multiple same SFP at the same time in 9800-80 eWLC and check if all the SFP are detected and check the behaviour	Passed	
EWLCJ178S_SFP_5	Checking the SFP details in the HA pair of eWLC 9800-80	To check the SFP details in the HA pair of eWLC 9800-80 .	Passed	
EWLCJ178S_SFP_6	Checking multiple SFP details in the HA pair of eWLC 9800-80	To check multiple SFP details in the HA pair of eWLC 9800-80 .	Passed	
EWLCJ178S_SFP_7	Connecting multiple different type SFP at same time in 9800-80 eWLC having a HA Pair	To connect multiple same SFP at the same time in 9800-80 eWLC having a HA Pair and check if all the SFP are detected and check the behaviour	Passed	

EWLCJ178S_SFP_8	Connecting different SFP in9800-L eWLC	To connect a SFP in eWLC9800-L and check if the SFP is detected or not.	Passed	
EWLCJ178S_SFP_9	Connecting multiple same type SFP at one instance in9800-L eWLC	To connect multiple same SFP at the same time in9800-L eWLC and check if all the SFP are detected and check the behaviour	Passed	
EWLCJ178S_SFP_10	Connecting multiple different type SFP at same time in 9800-L eWLC	To connect multiple same SFP at the same time in9800-L eWLC and check if all the SFP are detected and check the behaviour	Passed	
EWLCJ178S_SFP_11	Checking the SFP details in the HA pair of eWLC 9800-L	To check the SFP details in the HA pair of eWLC9800-L .	Passed	
EWLCJ178S_SFP_12	Checking multiple SFP details in the HA pair of eWLC 9800-L	To check multiple SFP details in the HA pair of eWLC9800-L .	Passed	
EWLCJ178S_SFP_13	Connecting multiple different type SFP at same time in 9800-L eWLC having a HA Pair	To connect multiple same SFP at the same time in9800-L eWLC having a HA Pair and check if all the SFP are detected and check the behaviour	Passed	

Support Scheduling of SSID broadcast

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_S_SSID_1	Configure Daily Calendar Profile	To configure Daily Calendar Profile	Passed	
EWLCJ178S_S_SSID_2	Configure Weekly Calendar Profile	To configure Weekly Calendar Profile	Passed	
EWLCJ178S_S_SSID_3	Configure Monthly Calendar Profile	To configure Monthly Calendar Profile	Passed	
EWLCJ178S_S_SSID_4	Configure Daily, Weekly and Monthly Calendar Profile through CLI	To configure Daily, Weekly and Monthly Calendar Profile through CLI	Passed	
EWLCJ178S_S_SSID_5	Map Calendar Profile to a Policy Profile	To Map Calendar Profile to a Policy Profile	Passed	
EWLCJ178S_S_SSID_6	Try deleting the calendar profile when it is already attached to the policy profile	To try deleting the calendar profile when it is already attached to the policy profile	Passed	
EWLCJ178S_S_SSID_7	While the calendar profile is attached to policy profile, update the timer range for calendar profile	To update the timer range for calendar profile	Passed	
EWLCJ178S_S_SSID_8	Delete the calendar profile from the policy profile	To delete the calendar profile from the policy profile	Passed	
EWLCJ178S_S_SSID_9	Map multiple calendar profiles to a Policy Profile	To Map multiple calendar profiles to a Policy Profile	Passed	
EWLCJ178S_S_SSID_10	Verify Windows client is able to connect to the WLAN only during the configured times	To verify Windows client is able to connect to the WLAN only during the configured times	Passed	

EWLCJ178S_S_SSID_11	Verify Android client is able to connect to the WLAN only during the configured times	To verify Android client is able to connect to the WLAN only during the configured times	Failed	CSCwa80672
EWLCJ178S_S_SSID_12	Verify IOS client is able to connect to the WLAN only during the configured times	To verify IOS client is able to connect to the WLAN only during the configured times	Passed	
EWLCJ178S_S_SSID_13	Verify MAC client is able to connect to the WLAN only during the configured times	To verify MAC client is able to connect to the WLAN only during the configured times	Passed	
EWLCJ178S_S_SSID_14	Verify Surface client is able to connect to the WLAN only during the configured times	To verify Surface client is able to connect to the WLAN only during the configured times	Passed	
EWLCJ178S_S_SSID_15	Verify client is able to connect to the WLAN in Flex mode only during the configured times	To verify client is able to connect to the WLAN in Flex mode only during the configured times	Passed	
EWCJ178S_Schedule_1	verify whether calendar profile can be created in webUI	To verify whether calendar profile can be created in webUI	Passed	
EWCJ178S_Schedule_2	verify whether calendar profile can be created in CLI	To verify whether calendar profile can be created in CLI	Failed	CSCwa93072
EWCJ178S_Schedule_3	Check whether the calendar-profile is merge in with policy profile in cli changes in webui	To check whether the calendar-profile is merge in with policy profile in cli changes in webui	Passed	

EWCJ178S_Schedule_4	Verify whether user able to delete calendar-profile after merging with policy profile	To verify whether user able to delete calendar-profile after merging with policy profile	Passed	
EWCJ178S_Schedule_5	Create a calendar-profile with daily reassurance and merge with a policy profile with wlan_enable	To create a calendar-profile with daily reassurance and merge with a policy profile with wlan_enable	Passed	
EWCJ178S_Schedule_6	create a calendar-profile with weekly reassurance and merge with a policy profile with wlan_enable	To create a calendar-profile with weekly reassurance and merge with a policy profile with wlan_enable	Passed	
EWCJ178S_Schedule_7	create a calendar-profile with monthly reassurance and merge with a policy profile with wlan_enable	To create a calendar-profile with monthly reassurance and merge with a policy profile with wlan_enable	Passed	
EWCJ178S_Schedule_8	create a calendar-profile with daily reassurance and merge with a policy profile with deny-client	To create a calendar-profile with daily reassurance and merge with a policy profile with deny-client	Passed	
EWCJ178S_Schedule_9	create a calendar-profile with weekly reassurance and merge with a policy profile with deny-client	create a calendar-profile with weekly reassurance and merge with a policy profile with deny-client	Passed	
EWCJ178S_Schedule_10	create a calendar-profile with monthly reassurance and merge with a policy profile with deny-client	create a calendar-profile with monthly reassurance and merge with a policy profile with deny-client	Passed	

EWCJ178S_Schedule_11	create calendar-profiles daily, weekly, monthly reassurance and merge with a single policy profile with wlan_enable	To create calendar-profiles daily, weekly, monthly reassurance and merge with a single policy profile with wlan_enable	Passed	
EWCJ178S_Schedule_12	create calendar-profiles daily, weekly, monthly reassurance and merge with a single policy profile with deny client	To create calendar-profiles daily, weekly, monthly reassurance and merge with a single policy profile with deny client	Passed	
EWCJ178S_Schedule_13	create calendar-profiles daily, weekly, monthly reassurance and merge with a single policy profile with wlan_enable and deny client	To create calendar-profiles daily, weekly, monthly reassurance and merge with a single policy profile with wlan_enable and deny client	Passed	
EWCJ178S_Schedule_14	Verify whether Windows client can able to join during assigned calendar-profile in open security	To verify whether Windows client can able to join during assigned calendar-profile in open security	Passed	
EWCJ178S_Schedule_15	Verify whether Android client can able to join during assigned calendar-profile in WPA3 security	To verify whether Android client can able to join during assigned calendar-profile in WPA3 security	Passed	
EWCJ178S_Schedule_16	Verify whether Windows client can able to join during assigned calendar-profile in WPA+WPA2 security	To verify whether Windows client can able to join during assigned calendar-profile in WPA+WPA2 security	Passed	

EWCJ178S_Schedule_17	Verify whether Windows client can able to join during assigned calendar-profile in WPA2+WPA3 security	To verify whether Windows client can able to join during assigned calendar-profile in WPA2+WPA3 security	Passed	
EWCJ178S_Schedule_18	Verify whether MAC client can able to join during assigned calendar-profile	To verify whether MAC client can able to join during assigned calendar-profile	Passed	
EWCJ178S_Schedule_19	Verify whether Android client can able to join during assigned calendar-profile	To verify whether Android client can able to join during assigned calendar-profile	Passed	
EWCJ178S_Schedule_20	Verify whether IOS client can able to join during assigned calendar-profile	To verify whether IOS client can able to join during assigned calendar-profile	Passed	
EWCJ178S_Schedule_21	Verify whether Surface client can able to join during assigned calendar-profile	To verify whether Surface client can able to join during assigned calendar-profile	Passed	

WPA3 Supporting 'Transition Disable'

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_TDisabe_1	Configuring Access Points & radio parameters for 5Ghz band with WPA3 & transition disable option enabled.	To configure Access Points & radio parameters for 5Ghz band with WPA3 & transition disable option enabled.	Passed	
EWLCJ178S_TDisabe_2	Configuring Access Points & radio parameters for 2.4Ghz band with WPA3 & transition disable option enabled.	To configure Access Points & radio parameters for 2.4Ghz band with WPA3 & transition disable option enabled.	Passed	
EWLCJ178S_TDisabe_3	Verifying WPA3/Transition Disable details with 11ax Android client connected.	To verify WPA3/Transition Disable details with 11ax Android client connected.	Passed	
EWLCJ178S_TDisabe_4	Verifying WPA3/Transition Disable details with 11ax iPhone client connected.	To verify WPA3/Transition Disable details with 11ax iPhone client connected.	Passed	
EWLCJ178S_TDisabe_5	Verifying the WPA3/Transition Disable details with Windows client connected.	To verify the WPA3/Transition Disable details with non 11ax Windows client connected.	Passed	
EWLCJ178S_TDisabe_6	Verifying the WPA3/Transition Disable details with Mac client connected.	To verify the WPA3/Transition Disable details with non 11ax Mac client connected.	Failed	CSCwb56984
EWLCJ178S_TDisabe_7	Verify WPA3/Transition Disable details by connecting client to 2.4Ghz radio.	To verify WPA3/Transition Disable details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ178S_TDisabe_8	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE Auth key.	Passed	

EWLCJ178S_TDisabe_9	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the WPA3 support with SAE security key by connecting the windows client.	Passed	
EWLCJ178S_TDisabe_10	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the WPA3 support with SAE security key by connecting the Android client.	Passed	
EWLCJ178S_TDisabe_11	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the WPA3 support with SAE security key by connecting the Mac os client.	Passed	
EWLCJ178S_TDisabe_12	Verifying the WPA3 support with SAE and PSK security key.	To verify the WPA3 support with SAE and PSK security key.	Passed	
EWLCJ178S_TDisabe_13	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 support with SAE and 802.1x security key.	Passed	
EWLCJ178S_TDisabe_14	Validating the WPA3 support with SAE and Layer 3 Splash page web redirect	To validate the WPA3 support with SAE and Layer 3 Splash page web redirect	Passed	
EWLCJ178S_TDisabe_15	Validating the WPA3 support with SAE and Layer 3 On Mac filter failure.	To validate the WPA3 support with SAE and Layer 3 On Mac filter failure.	Passed	
EWLCJ178S_TDisabe_16	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ178S_TDisabe_17	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security.	Passed	
EWLCJ178S_TDisabe_18	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security.	Passed	

EWLCJ178S_TDisabe_19	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with Ft+802.1x security.	Passed	
EWLCJ178S_TDisabe_20	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the WPA3 support with Intra client roaming by using 9115AP	Passed	
EWLCJ178S_TDisabe_21	Verifying the WPA3 support and SAE security with Inter WLC Roaming	To verify the WPA3 support and SAE security with Inter WLC Roaming	Passed	
EWLCJ178S_TDisabe_22	Verifying the WPA3 support Roaming between Controllers	To verify the WPA3 support Roaming between Controllers with same Radio types	Passed	
EWLCJ178S_TDisabe_23	Verifying the WPA3 support with SAE Auth key in local auth and local switching.	To verify the WPA3 support with SAE Auth key in local auth and local switching.	Failed	CSCwb65650
EWLCJ178S_TDisabe_24	Ensure transition disable compatibility with other WPA security modes	To verify transition disable compatibility with other WPA security modes	Passed	
EWLCJ178S_TDisabe_25	Verifying WPA3/Transition Disable details with Surface client connected.	To verify WPA3/Transition Disable details with Surface client connected.	Passed	
EWCJ178S_WPA3_1	Configuring Access Points & radio parameters for 5Ghz band with WPA3 & transition disable option enabled.	To configure Access Points & radio parameters for 5Ghz band with WPA3 & transition disable option enabled.	Passed	
EWCJ178S_WPA3_2	Configuring Access Points & radio parameters for 2.4Ghz band with WPA3 & transition disable option enabled.	To configure Access Points & radio parameters for 2.4Ghz band with WPA3 & transition disable option enabled.	Failed	CSCwb32331

EWCJ178S_WPA3_3	Verifying WPA3/Transition Disable details with 11ax Android client connected.	To verify WPA3/Transition Disable details with 11ax Android client connected.	Passed	
EWCJ178S_WPA3_4	Verifying WPA3/Transition Disable details with 11ax iPhone client connected.	To verify WPA3/Transition Disable details with 11ax iPhone client connected.	Passed	
EWCJ178S_WPA3_5	Verifying the WPA3/Transition Disable details with Windows client connected.	To verify the WPA3/Transition Disable details with non 11ax Windows client connected.	Passed	
EWCJ178S_WPA3_6	Verifying the WPA3/Transition Disable details with Mac client connected.	To verify the WPA3/Transition Disable details with non 11ax Mac client connected.	Passed	
EWCJ178S_WPA3_7	Verify WPA3/Transition Disable details by connecting client to 2.4Ghz radio.	To verify WPA3/Transition Disable details by connecting client to 2.4Ghz radio.	Passed	
EWCJ178S_WPA3_8	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE Auth key.	Passed	
EWCJ178S_WPA3_9	Verifying the WPA3 support with SAE security key by connecting the windows client.	To verify the WPA3 support with SAE security key by connecting the windows client.	Passed	
EWCJ178S_WPA3_10	Verifying the WPA3 support with SAE security key by connecting the Android client.	To verify the WPA3 support with SAE security key by connecting the Android client.	Passed	
EWCJ178S_WPA3_11	Verifying the WPA3 support with SAE security key by connecting the Mac os client.	To verify the WPA3 support with SAE security key by connecting the Mac os client.	Passed	

EWCJ178S_WPA3_12	Verifying the WPA3 support with SAE and PSK security key.	To verify the WPA3 support with SAE and PSK security key.	Passed	
EWCJ178S_WPA3_13	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 support with SAE and 802.1x security key.	Passed	
EWCJ178S_WPA3_14	Validating the WPA3 support with SAE and Layer 3 Splash page web redirect	To validate the WPA3 support with SAE and Layer 3 Splash page web redirect	Passed	
EWCJ178S_WPA3_15	Validating the WPA3 support with SAE and Layer 3 On Mac filter failure.	To validate the WPA3 support with SAE and Layer 3 On Mac filter failure.	Passed	
EWCJ178S_WPA3_16	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWCJ178S_WPA3_17	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security.	Passed	
EWCJ178S_WPA3_18	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security.	Passed	
EWCJ178S_WPA3_19	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with Ft+802.1x security.	Passed	
EWCJ178S_WPA3_20	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the WPA3 support with Intra client roaming by using 9115AP	Passed	

Anchored SSID support on EWC

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_SSID_1	Verify whether tunnel Profile can be configured or not	To Verify whether tunnel Profile can be configured or not	Passed	
EWCJ178S_SSID_2	Verify whether WLAN to the Wireless policy profile can be configured or not	To Verify whether WLAN to the Wireless policy profile can be configured or not	Passed	
EWCJ178S_SSID_3	Configure wlan and connect the windows client by using radio type	To Configure wlan and connect the windows client by using radio type	Passed	
EWCJ178S_SSID_4	Configure wlan and connect the Mac client by using radio type	To Configure wlan and connect the Mac client by using radio type	Passed	
EWCJ178S_SSID_5	Configure wlan and connect the Android client by using radio type	To Configure wlan and connect the Android client by using radio type	Passed	
EWCJ178S_SSID_6	Verify whether tunnel Profile can be configured in GUI	To Verify whether tunnel Profile can be configured in GUI	Passed	
EWCJ178S_SSID_7	Configure wlan and Verify client connection by enabling central forwarding in tunnel profile or not	To Configure wlan and Verify client connection by enabling central forwarding in tunnel profile or not	Passed	
EWCJ178S_SSID_8	Configure wlan and Verify Android client connection by enabling central forwarding in tunnel profile	To Configure wlan and Verify Android client connection by enabling central forwarding in tunnel profile	Passed	
EWCJ178S_SSID_9	Configure wlan and Verify Mac client connection by enabling central forwarding in tunnel profile	To Configure wlan and Verify Mac client connection by enabling central forwarding in tunnel profile	Passed	

EWCJ178S_SSID_10	Verify different client connection by enabling central forwarding in tunnel profile using different radio types	To Verify different client connection by enabling central forwarding in tunnel profile using different radio types	Passed	
EWCJ178S_SSID_11	Verify client connection via AP 9120	To Verify client connection via AP 9120	Passed	
EWCJ178S_SSID_12	Configuring an Access Control List for Tunnelling	To Configure an Access Control List for Tunnelling	Failed	CSCwb57089
EWCJ178S_SSID_13	Configure wlan and Verify IOS client connection by enabling central forwarding in tunnel profile	To Configure wlan and Verify IOS client connection by enabling central forwarding in tunnel profile	Passed	
EWCJ178S_SSID_14	Configure wlan and connect the Surface client by using different security modes.	To Configure wlan and connect the Surface client by using different security modes.	Passed	
EWCJ178S_SSID_15	Configure wlan and connect the client via 9130 AP	To Configure wlan and connect the client via 9130 AP	Passed	
EWCJ178S_SSID_16	Configure wlan and connect the client via 9115 AP	To Configure wlan and connect the client via 9115 AP	Passed	
EWCJ178S_SSID_17	Configure wlan and connect the client via 9105 AP	To Configure wlan and connect the client via 9105 AP	Passed	
EWCJ178S_SSID_18	Configure wlan and connect the client by using 2.4GHz network	To Configure wlan and connect the client by using 2.4GHz network	Passed	
EWCJ178S_SSID_19	Configure wlan and connect the client by using 5GHz network	To Configure wlan and connect the client by using 5GHz network	Passed	
EWCJ178S_SSID_20	Verify by Connecting any client through centralized SSID	To Verify by Connecting any client through centralized SSID	Passed	

Windows 11 Support and MAC 12 Support

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_WM_1	Connecting a latest version Windows client with WPA 3 PSK security	To connect a latest version windows client to 9120 AP with the WLAN security as WPA PSK	Passed	
EWCJ178S_WM_2	Connecting a latest version windows client with WPA 3 802.1x security	To connect a latest version windows client to 9120 AP with the WLAN security as WPA 3	Failed	CSCwb57945
EWCJ178S_WM_3	Performing Intra controller roaming of latest version of MAC OS client	To check whether intra controller roaming of latest version of MAC OS works properly or not	Passed	
EWCJ178S_WM_4	Performing Intra controller roaming of latest version of Windows client	To check whether intra controller roaming of latest version of windows client works properly or not	Passed	
EWCJ178S_WM_5	Performing Inter controller roaming of latest version of Windows client	To check whether inter controller roaming of latest version of window client works properly or not	Passed	
EWCJ178S_WM_6	Performing Inter controller roaming of latest version of MAC client	To check whether inter controller roaming of latest version of MAC client works properly or not	Passed	
EWCJ178S_WM_7	Check commination between 11ax-os updated window/mac client and wired client	To check commination between 11ax-os updated window/mac client and wired client	Passed	

EWCJ178S_WM_8	Connecting a latest version of Window client to the 9105 AP	To connect a latest version of client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_WM_9	Connecting latest version of Android client to the 9105 AP	To connect a latest version of Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_WM_10	Connecting a latest version of IOS client to the 9105 AP	To connect a latest version of IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_WM_11	Connecting a latest version of MAC client to the 9105 AP	To connect a latest version of client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_WM_12	Reassociation of latest version of window/mac client to the AP after reboot	To verify if the latest version of window/mac client gets reassociated to the to the AP .	Passed	
EWCJ178S_WM_13	Roam 11ax-latest version of windows client between 9105 Aps	To check roaming happening or not for 11ax-latest version of windows client between 9105 Aps	Passed	
EWCJ178S_WM_14	Roam 11ax-latest version of mac client between 9130 Aps	To check roaming happening or not for 11ax-os updated mac client between 9130 Aps	Passed	
EWCJ178S_WM_15	Verify details by connecting latest version of window/mac client to 2.4Ghz radio of 9105 AP.	To verify OFDMA details by connecting latest version of window/mac client to 2.4 Ghz radio.	Passed	

EWCJ178S_WM_16	Verify details by connecting updated window/mac client to 5 Ghz radio of 9105 AP	To verify OFDMA details by connecting updated window/mac client to 5 Ghz radio.	Passed	
EWCJ178S_WM_17	Verify 9105AP MU-MIMO details with latest version of window/mac client connecting to WPA2 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with latest version of window/mac client connecting to WPA2 configured WLAN	Passed	
EWCJ178S_WM_18	Verify 9105AP MU-MIMO details with latest version of window/mac client connecting to WPA 3 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with updated window/mac client connecting to WPA 3 configured WLAN	Passed	
EWCJ178S_WM_19	Connect the latest version of MAC OS Clients with all the 5 key combinations	To Connect the latest version of MAC OS Clients with all the 5 key combinations	Passed	
EWCJ178S_WM_20	Connect the latest version of window OS Clients with all the 5 key combinations	To Connect the latest version of window OS Clients with all the 5 key combinations	Passed	

Regression Features

11ax Advanced traffic based scheduler for scheduling SU, OFDMA and MU traffic on 9105/9115/9120/9130

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_1	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWLCJ178S_Reg_2	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWLCJ178S_Reg_3	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ178S_Reg_4	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ178S_Reg_5	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ178S_Reg_6	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ178S_Reg_7	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ178S_Reg_8	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	

EWLCJ178S_Reg_9	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ178S_Reg_10	Connect up to 8 clients and monitor DL/UL OFDMA statistics	To connect up to 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_15	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_17	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	
EWLCJ178S_Reg_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	

EWLCJ178S_Reg_19	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWLCJ178S_Reg_20	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWLCJ178S_Reg_21	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWLCJ178S_Reg_22	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWLCJ178S_Reg_23	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_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	
EWLCJ178S_Reg_26	Connect up to 8 clients and monitor DL/UL 11ax MU statistics	To connect up to 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWLCJ178S_Reg_27	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	
EWLCJ178S_Reg_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	

EWLCJ178S_Reg_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	
EWCJ178S_Reg_1	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 5Ghz band.	Passed	
EWCJ178S_Reg_2	Configuring 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	To configure 11ax Access Points, Channel width, OFDMA & radio parameters for 2.4Ghz band.	Passed	
EWCJ178S_Reg_3	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ178S_Reg_4	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ178S_Reg_5	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ178S_Reg_6	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWCJ178S_Reg_7	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWCJ178S_Reg_8	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	

EWCJ178S_Reg_9	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWCJ178S_Reg_10	Connect up to 8 clients and monitor DL/UL OFDMA statistics	To connect up to 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ178S_Reg_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	
EWCJ178S_Reg_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	
EWCJ178S_Reg_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	
EWCJ178S_Reg_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	
EWCJ178S_Reg_15	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWCJ178S_Reg_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	
EWCJ178S_Reg_17	Configuring 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	To configure 11ax Access Points, Channel width, 11ax MU & radio parameters for 5Ghz band.	Passed	
EWCJ178S_Reg_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	

EWCJ178S_Reg_19	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWCJ178S_Reg_20	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWCJ178S_Reg_21	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWCJ178S_Reg_22	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWCJ178S_Reg_23	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWCJ178S_Reg_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	
EWCJ178S_Reg_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	
EWCJ178S_Reg_26	Connect up to 8 clients and monitor DL/UL 11ax MU statistics	To connect up to 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWCJ178S_Reg_27	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	
EWCJ178S_Reg_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	

EWCJ178S_Reg_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 BSS Coloring(OBSS PD) on 9105/9115/9120/9130 APs

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_30	Enable Global OBSS PD for 5ghz band	To verify whether the OBBSS PD enable or not for 5 GHz band	Passed	
EWLCJ178S_Reg_31	Disable Global OBSS PD for 5ghz band	To Check whether the OBBSS PD disable or not for 5 GHz	Passed	
EWLCJ178S_Reg_32	Enable Global OBSS PD for 2.4 ghz band	To verify whether the OBBSS PD enable or not for 2.4 Ghz band	Passed	
EWLCJ178S_Reg_33	Disable Global OBSS PD for 2.4 ghz band	To Check whether the OBBSS PD disable or not for 2.4 GHz	Passed	
EWLCJ178S_Reg_34	Set OBSS PD value for 5 GHZ band	To verify whether the values set for 5 Ghz band or not	Passed	
EWLCJ178S_Reg_35	Set OBSS PD value for 2.4 GHZ band	To verify whether the values set for 2.4 ghz band or not	Passed	
EWLCJ178S_Reg_36	Creating RF Profile with OBSS PD enabled for 5/2.4 GHz band	To Validate whether RF Profile created with OBSS PD enable for 5/2.4 GHz band	Passed	
EWLCJ178S_Reg_37	Disabling OBSS PD in RF Profile	To Validate whether RF Profile is created with OBSS PD enable for 5/2.4 GHz band	Passed	
EWLCJ178S_Reg_38	Viewing OBSS PD supports in different AP models	To checking the OBSS PD supports in different AP models	Passed	
EWLCJ178S_Reg_39	Configuring BSS colour details in AP & controller CLIs	To Verify Configured colour details is reflected in AP and Controller CLIs	Passed	

EWLCJ178S_Reg_40	Checking the BSS colour details are retained after AP and Controller reload	To Check whether the BSS colour retained after AP & Controller reload	Passed	
EWLCJ178S_Reg_41	Verify enable/disable of BSS colouring on radio is reflected in management packets	To verify whether the BSS colour is reflected in Management packets or not	Passed	
EWLCJ178S_Reg_42	Verifying OBSS PD with inter roaming client using different radio	To check whether OBSS PD is enable or not , when different radio clients are roaming between controllers	Passed	
EWLCJ178S_Reg_43	Verifying OBSS PD enabled with inter roaming client using same radio	To check whether OBSS PD enable or not , when same radio clients are roaming between controllers	Passed	
EWLCJ178S_Reg_44	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	
EWLCJ178S_Reg_45	Changing 9115 AP mode from local to Flex connect & check the BSS colouring Configuration	To change the mode of AP from local mode to Flex connect mode and check the BSS colouring configuration in 9115 Ap	Passed	
EWLCJ178S_Reg_46	Changing 9115 AP mode from flex to local & check the BSS colouring Configuration	To change the mode of AP from flex mode to local mode and check the BSS colouring configuration in 9115 Ap	Passed	

4800: 3rd Radio in Monitor Mode (IOS-XE)

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_47	Check if AP profile configuration is done and pushed to AP from controller	To check if AP profile configuration is done and pushed to AP from controller	Passed	
EWLCJ178S_Reg_48	Verify operation with AP mode as local and sub mode as AWIPS	To verify operation with AP mode as local and sub mode as AWIPS	Passed	
EWLCJ178S_Reg_49	Verify operation with AP mode as flex and sub mode as AWIPS	To verify operation with AP mode as flex and sub mode as AWIPS	Passed	
EWLCJ178S_Reg_50	Verify operation with AP mode as local/flex and sub mode as none	To verify operation with AP mode as local/flex and sub mode as none	Passed	
EWLCJ178S_Reg_51	Verify operation with AP mode as local and different combinations of slot sub modes	To verify operation with AP mode as local and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_52	Verify operation with AP mode as local and different combinations of slot sub modes	To verify operation with AP mode as local and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_53	Verify operation with AP mode as monitor and different combinations of slot sub modes	To verify operation with AP mode as monitor and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_54	Connect client with each combination of AP mode/sub mode and monitor the status	To connect client with each combination of AP mode/sub mode and monitor the status	Passed	

EWLCJ178S_Reg_55	Connect android client with each combination of AP mode/sub mode and monitor the status	To connect android client with each combination of AP mode/sub mode and monitor the status	Passed	
EWLCJ178S_Reg_56	Connect MAC client with each combination of AP mode/sub mode and monitor the status	To connect MAC client with each combination of AP mode/sub mode and monitor the status	Passed	
EWLCJ178S_Reg_57	Connect Surface client with each combination of AP mode/sub mode and monitor the status	To connect Surface client with each combination of AP mode/sub mode and monitor the status	Passed	
EWLCJ178S_Reg_58	Verify catalyst 9120 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify catalyst 9120 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_59	Verify catalyst 9130 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify catalyst 9130 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_60	Verify catalyst 9105 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify catalyst 9105 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_61	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	

EWLCJ178S_Reg_62	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	
EWLCJ178S_Reg_63	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot sub modes	Passed	

9800-CL licensing enhancements for better tracking of 9800-CL in production deployments

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_663	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ178S_Reg_664	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWLCJ178S_Reg_665	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWLCJ178S_Reg_666	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWLCJ178S_Reg_667	Validate license info in 9800-CL	To validate license info in 9800-CL	Passed	
EWLCJ178S_Reg_668	Validate license info after upgrade	To validate license info after upgrade	Passed	
EWLCJ178S_Reg_669	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWLCJ178S_Reg_670	Verify alert is generated or not for smart license report is not acknowledged	To verify alert is generated or not for smart license report is not acknowledged	Passed	
EWLCJ178S_Reg_671	Verify Smart Licensing status	To verify Smart Licensing status	Passed	
EWLCJ178S_Reg_672	Verify Smart Licensing Events	To verify Smart Licensing Events	Passed	
EWLCJ178S_Reg_673	Enable/disable Smart Licensing and Save & Reload	To enable/disable Smart Licensing and Save & Reload	Passed	
EWLCJ178S_Reg_674	Enable/disable Smart Licensing and Save & Without Reload	To enable/disable Smart Licensing and Save & Without Reload	Passed	

9800 feature requests to select cipher-suite to be used for localauth PEAP

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_641	Configuring Local EAP profile through UI and enabling Peap	To configure Local eap profile through UI and enabling PEAP on that profile and verifying the same	Passed	
EWLCJ178S_Reg_642	Configuring Local EAP profile through CLI and enabling Peap to check the behaviour	To configure Local eap profile through CLI and enabling PEAP on that profile and verifying the same	Passed	
EWLCJ178S_Reg_643	Configuring single cipher suit for PEAP in eWLC 9800-80 through eap profile	To configure local eap profile for PEAP and enabling cipher suit	Passed	
EWLCJ178S_Reg_644	Configuring multiple cipher suit for PEAP in eWLC 9800-80 through eap profile	To configure local eap profile for PEAP and enabling multiple cipher suit	Passed	
EWLCJ178S_Reg_645	Connecting a client to 9105 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	To connecting a client to 9105 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_646	Connecting a client to 9115 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	To connecting a client to 9115 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_647	Connecting a client to 9120 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	To connecting a client to 9120 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	Passed	

EWLCJ178S_Reg_648	Connecting a client to 9130 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	To connecting a client to 9130 AP in eWLC 9800-80 having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_649	Connecting a client to 9105 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	To connecting a client to 9105 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_650	Connecting a client to 9115 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	To connecting a client to 9115 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_651	Connecting a client to 9120 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	To connecting a client to 9120 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_652	Connecting a client to 9130 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	To connecting a client to 9130 AP in eWLC 9800-L having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_653	Connecting a client to 9105 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	To connecting a client to 9105 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_654	Connecting a client to 9115 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	To connecting a client to 9115 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	Passed	

EWLCJ178S_Reg_655	Connecting a client to 9120 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	To connecting a client to 9120 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_656	Connecting a client to 9130 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	To connecting a client to 9130 AP in eWLC 9800-CL having a ciphersuit configured on local eap profile	Passed	
EWLCJ178S_Reg_657	Check if the PEAP config with ciphersuit is retained after the Master failover scenario	To check if the PEAP config with ciphersuit is retained after the master failover scenario	Passed	
EWLCJ178S_Reg_658	Check if the PEAP config with ciphersuit is retained after the eWLC reload	To check if the PEAP config with ciphersuit is retained after the eWLC reload	Passed	
EWLCJ178S_Reg_659	Check inter controller roaming scenario when client connected to Local eap PEAP with single ciphersuit	To check if inter controller roaming happens when client connected to Local eap profile with single cipher suit enabled	Passed	
EWLCJ178S_Reg_660	Check inter controller roaming scenario when client connected to Local eap PEAP with Multiple ciphersuit	To check if inter controller roaming happens when client connected to Local eap profile with multiple cipher suit enabled	Passed	
EWLCJ178S_Reg_661	Check intra controller roaming scenario when client connected to Local eap PEAP with single ciphersuit	To check if intra controller roaming happens when client connected to Local eap profile with single cipher suit enabled	Passed	

EWLCJ178S_Reg_662	Check intra controller roaming scenario when client connected to Local eap PEAP with Multiple ciphersuit	To check if intra controller roaming happens when client connected to Local eap profile with multiple cipher suit enabled	Passed	

Adapative Load EDCA Parameter

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_64	Validate the EDCA parameter with wmm-default profile	To associate the client and verifying EDCA parameter in wmm-default profile	Passed	
EWLCJ178S_Reg_65	Validate the EDCA parameter with custom-voice profile	To associate the client and verifying EDCA parameter in custom-voice profile	Passed	
EWLCJ178S_Reg_66	Validate the EDCA parameter with optimized-video-voice profile	To associate the client and verifying EDCA parameter in optimized-video-voice profile	Passed	
EWLCJ178S_Reg_67	Validate the EDCA parameter with optimized-voice profile	To associate the client and verifying EDCA parameter in optimized-voice profile	Passed	
EWLCJ178S_Reg_68	Validate the EDCA parameter with svp-voice profile	To associate the client and verifying EDCA parameter in svp-voice profile	Passed	
EWLCJ178S_Reg_69	Validate the EDCA parameter with Fastlane profile	To associate the client and verifying EDCA parameter in Fastlane profile	Passed	
EWLCJ178S_Reg_70	Associate the windows client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ178S_Reg_71	Associate the Android client and verify the EDCA parameter in 9130 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ178S_Reg_72	Associate the MAC client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	

EWLCJ178S_Reg_73	Validate the EDCA parameter with different profile in 2.4GHz frequency	To associate the client and verifying EDCA parameter for 2.4GHZ frequency	Passed	
EWLCJ178S_Reg_74	Validate the EDCA parameter with different profile in 6GHz frequency	To associate the client and verifying EDCA parameter for 6GHZ frequency	Passed	
EWLCJ178S_Reg_75	Validate the EDCA parameter with different profile in 5GHz frequency	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ178S_Reg_76	Validate the EDCA parameter with single client	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ178S_Reg_77	Perform Inter roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ178S_Reg_78	Perform Intra roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ178S_Reg_79	Perform controller reload and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ178S_Reg_80	Associate the MS-GO client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ178S_Reg_81	Associate the MS-GO2 client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	

AP Tags needs to be perserved

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_82	Verify whether your able to execute tag persistency command or not	To verify whether your able to execute tag persistency command or not	Passed	
EWLCJ178S_Reg_83	Verify whether your able to configure AP Join Profile, Policy tag, Site tag, RF tag	To verify whether your able to configure AP Join Profile, Policy tag, Site tag, RF tag	Passed	
EWLCJ178S_Reg_84	Map tagX profile to Access Point	To map tagX profile to Access Point	Passed	
EWLCJ178S_Reg_85	Test tag source priority is followed by AP tags persistency	To test tag source priority is followed by AP tags persistency	Passed	
EWLCJ178S_Reg_86	Upload multiple AP MAC addresses, tagX through CSV file	To upload multiple AP MAC addresses, tagX through CSV file	Passed	
EWLCJ178S_Reg_87	Verify Tag Source Priority	To verify Tag Source Priority	Passed	
EWLCJ178S_Reg_88	Move Access Point from eWLC1 to eWLC2 with Preserved tags	To move Access Point from eWLC1 to eWLC2 with Preserved tags	Passed	
EWLCJ178S_Reg_89	Move Access Point from eWLC1 to eWLC2 without Preserved tags and verify automatic default tagX parameters	To move Access Point from eWLC1 to eWLC2 without Preserved tags and to verify automatic default tagX parameters	Passed	
EWLCJ178S_Reg_90	Move Access Point to other controller on Priority base	To move Access Point to other controller on Priority base	Passed	
EWLCJ178S_Reg_91	Verify Syslogs after moving AP from eWLC1 to eWLC2	To verify Syslogs after moving AP from eWLC1 to eWLC2	Passed	

EWLCJ178S_Reg_92	Move AP from eWLC1 to eWLC2 using Basic Profile with Preserved tags	To move AP from eWLC1 to eWLC2 using Basic Profile with Preserved tags	Passed	
EWLCJ178S_Reg_93	Connect Windows client when AP tags are Preserved and verify client status	To connect Windows client when AP tags are Preserved and to verify client status	Passed	
EWLCJ178S_Reg_94	Connect Android client when AP tags are Preserved and verify client status	To connect Android client when AP tags are Preserved and verify client status	Passed	
EWLCJ178S_Reg_95	Connect IOS client when AP tags are Preserved and verify client status	To connect IOS client when AP tags are Preserved and verify client status	Passed	
EWLCJ178S_Reg_96	Connect MAC client when AP tags are Preserved and verify client status	To connect MAC client when AP tags are Preserved and verify client status	Passed	
EWLCJ178S_Reg_97	Connect Surface client when AP tags are Preserved and verify client status	To connect Surface client when AP tags are Preserved and verify client status	Passed	
EWLCJ178S_Reg_98	Create AP tags needs to be Preserved using Basic Profile and check Joined APs and Clients count	To create AP tags needs to be Preserved using Basic Profile and check Joined APs and Clients count	Passed	
EWLCJ178S_Reg_99	Verify AP disjoined alert is triggered or not in Prime Infrastructure	To verify AP disjoined alert is triggered or not in Prime Infrastructure	Passed	
EWLCJ178S_Reg_100	Verify AP moved alert is triggered or not in Prime Infrastructure	To verify AP moved alert is triggered or not in Prime Infrastructure	Passed	
EWLCJ178S_Reg_101	Create Location and upload empty csv file	To create Location and upload empty csv file	Passed	
EWLCJ178S_Reg_102	Create Location, upload bulk csv file and check AP Joined status	To create Location, upload bulk csv file and check AP Joined status	Passed	

Called Station ID with AP Ethernet MAC

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_103	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	
EWLCJ178S_Reg_104	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	
EWLCJ178S_Reg_105	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flexprofilename”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flexprofilename”	Passed	
EWLCJ178S_Reg_106	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-macaddress-ssid-flexprofilename	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-macaddress-ssid flexprofilename	Passed	
EWLCJ178S_Reg_107	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac -ssid-policytagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac -ssid-policytagname”	Passed	

EWLCJ178S_Reg_108	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-policy tagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-policy tagname”	Passed	
EWLCJ178S_Reg_109	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-site tagname”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-sitetag name”	Passed	
EWLCJ178S_Reg_110	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-sitetag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-sitetag name”	Passed	
EWLCJ178S_Reg_111	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWLCJ178S_Reg_112	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWLCJ178S_Reg_113	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWLCJ178S_Reg_114	HA active to standby config impact	To verify config impact HA active to standby	Passed	
EWLCJ178S_Reg_115	active to standby to active config impact	To verify config impact when active to standby to active	Passed	

EWLCJ178S_Reg_116	Change mac address format in attribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in attribute and check config	Passed	
EWLCJ178S_Reg_117	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWLCJ178S_Reg_118	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	
EWCJ178S_Reg_61	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	
EWCJ178S_Reg_62	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	
EWCJ178S_Reg_63	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flex profile name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-flex profile name”	Passed	

EWCJ178S_Reg_64	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-flex profile name	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-flex profile name	Passed	
EWCJ178S_Reg_65	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-policy tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-policytag name”	Passed	
EWCJ178S_Reg_66	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-policy tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-policy tag name”	Passed	
EWCJ178S_Reg_67	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-ethmac-ssid-site tag name”	Passed	
EWCJ178S_Reg_68	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-sitetag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-sitetag name”	Passed	
EWCJ178S_Reg_69	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	

EWCJ178S_Reg_70	configuring both AAA and local authentication	To configuring both AAA and local authentication	Failed	CSCwb52050
EWCJ178S_Reg_71	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWCJ178S_Reg_72	HA active to standby config impact	To verify config impact HA active to standby	Passed	
EWCJ178S_Reg_73	active to standby to active config impact	To verify config impact when active to standby to active	Passed	
EWCJ178S_Reg_74	Change mac address format in attribute and check config impact "radius-server attribute 31 mac format ? "	To Change mac address format in attribute and check config	Passed	
EWCJ178S_Reg_75	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWCJ178S_Reg_76	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	Failed	CSCwa84592

Capability to enable/disable 11ax features per SSID

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_119	Check the 11 ax enabling or not via GUI	To verify whether the 11 ax parameters enable or not via GUI	Passed	
EWLCJ178S_Reg_120	Check the 11 ax disabling or not via GUI	To verify whether the 11 ax parameters disable or not via GUI	Passed	
EWLCJ178S_Reg_121	Check the 11 ax enabling or not via CLI	To verify whether the 11 ax parameters enable or not via CLI	Passed	
EWLCJ178S_Reg_122	Check the 11 ax disabling or not via CLI	To verify whether the 11 ax parameters disable or not via CLI	Passed	
EWLCJ178S_Reg_123	Disabling 11 ax radio and checking the client connectivity	To check the client connectivity after disabling 11 ax	Passed	
EWLCJ178S_Reg_124	Checking the 11 ax parameters after AP reboot	To verify the 11 ax for after AP reboot	Passed	
EWLCJ178S_Reg_125	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	
EWLCJ178S_Reg_126	Verifying 11 ax parameters for different AP models	To Verify the 11 ax parameters for different AP models	Passed	
EWLCJ178S_Reg_127	Validating the 11ax parameters after disjoin the AP	To validate the 11 ax parameters for after Ap disjoin	Passed	
EWLCJ178S_Reg_128	Verifying the 11 ax parameters after deleting the client	To verify the 11 ax parameters for deleted client	Passed	

EWLCJ178S_Reg_129	monitoring the 11 ax parameters after AP provisioning from DNAC	To check the 11 ax parameters after AP provisioning from DNAC	Passed	
EWLCJ178S_Reg_130	Verifying the 11 ax parameters by deleting the SSID	To Verify the 11 ax parameters after Deleting SSID	Passed	
EWLCJ178S_Reg_131	Verifying the 11 ax parameters for intra roaming client	To Verify the 11 ax parameters after client roaming between AP's	Passed	
EWLCJ178S_Reg_132	Checking the 11 ax parameters for inter roaming client	To Verify the 11 ax parameters status after client roaming between controllers	Passed	
EWLCJ178S_Reg_133	Verifying the 11 ax status by changing the security type	To check the11 ax parameters after changing the security type	Passed	
EWLCJ178S_Reg_134	Validating the 11ax status for Virtual EWLC	To validate the 11 ax parameters for vEWLC	Passed	

Dot1x+EWA on mac Failure

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_135	Verifying the Dot1x+EWA support with mac failure.	To verify the Dot1x+EWA support with mac filter Configuration.	Passed	
EWLCJ178S_Reg_136	Verifying the Dot1x+EWA support with mac filter by connecting the windows client.	To verify the Client packets by connecting the windows client to dot1x and EWA supported SSID	Passed	
EWLCJ178S_Reg_137	Verifying the Dot1x+EWA support with mac filter by connecting the Android client.	To verify the Client packets by connecting the Android client to Dot1x+EWA supported SSID	Passed	
EWLCJ178S_Reg_138	Verifying the Dot1x+EWA support with mac filter by connecting the Mac os client.	To verify the Client packets by connecting the Mac os client to Dot1x+EWA supported SSID	Passed	
EWLCJ178S_Reg_139	Verifying the Dot1x+EWA support with mac filter by connecting the samsung10 client.	To verify the Client packets by connecting the S10 os client to Dot1x+EWA supported SSID	Passed	
EWLCJ178S_Reg_140	Verifying the Dot1x+EWA support with Wpa2 security mac failure	To verify the Dot1x+EWA Configuration with wpa2 supported SSID	Passed	
EWLCJ178S_Reg_141	Verifying the Dot1x+EWA support with Wpa3 security .	To verify the Dot1x+EWA Configuration with wpa3 supported SSID	Passed	
EWLCJ178S_Reg_142	Validating the Dot1x+EWA support and Layer 2 On Mac filter	To verify the Dot1x+EWA support and Layer3 On Mac filter failure	Passed	

EWLCJ178S_Reg_143	verifying the Dot1x+EWA support with Layer3 Splash page web redirect.	To verify the Dot1x+EWA support with Layer3 Splash page web redirect.	Passed	
EWLCJ178S_Reg_144	Verifying the EWA support with 802.1x-SHA256 security.	To verify the EWA support with 802.1x-SHA256 security for the different clients.	Passed	
EWLCJ178S_Reg_145	Verifying the Dot1x+EWA support with Ft	To verify the Dot1x+EWA support with +Ft for the different clients.	Passed	
EWLCJ178S_Reg_146	Verifying the Dot1x+EWA support with Intra client roaming by using 9115AP	To verify the Intra client roaming by using Dot1x+EWA support with 9115AP	Passed	
EWLCJ178S_Reg_147	Verifying the Dot1x+EWA security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with Dot1x+EWA support	Passed	
EWLCJ178S_Reg_148	Verifying the Dot1x+EWA support with Roaming between Controllers with Different Radio types	To verify whether Client is Moving between Controllers with Different Radio type or not with dot1x+EWA WLAN.	Passed	
EWLCJ178S_Reg_149	Verifying the Dot1x+EWA support Roaming between Controllers with same Radio types	To verify whether Client is Moving between Controllers with same Radio type or not with dot1x+EWA WLAN.	Passed	
EWLCJ178S_Reg_150	Verifying the Dot1x+EWA support with local auth and local switching.	To verify the Dot1x+EWA security in local auth and local switching.	Passed	

EWLCJ178S_Reg_151	Verifying the Dot1x+EWA support with mac filter by connecting the MS GO2 client.	To verify the Client packets by connecting the MS GO2 client to dot1x and EWA supported SSID	Passed	
EWLCJ178S_Reg_152	Verifying the Dot1x+EWA support with mac filter by connecting the Sleeping client	To verify the Client packets by connecting the sleeping client to dot1x and EWA supported SSID	Passed	
EWLCJ178S_Reg_153	Validate client association in DNAC	To verify client details showing or not in DANC	Passed	
EWLCJ178S_Reg_154	Validate client association in PI	To verify client details showing or not in PI	Passed	
EWLCJ178S_Reg_155	Configure wlan with EWA in DNAC & check client details in DNA space	To verify wlan created or not in DANC	Passed	
EWCJ178S_Reg_103	Create WLAN using WLAN wizard	To check whether Wlan able to create or not using WLAN Wizard option	Passed	
EWCJ178S_Reg_104	Check the client connectivity for created WLAN using WLAN Wizard	To Check the client connectivity using created WLAN in WLAN Wizard	Passed	
EWCJ178S_Reg_105	Checking the Client connectivity for Dot1x security	To verify whether the client connected with Dot1x security or not	Passed	
EWCJ178S_Reg_106	Create flex connect EWA and check the client connectivity	To check the client connectivity for flex connect EWA	Failed	CSCwb57110
EWCJ178S_Reg_107	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Passed	
EWCJ178S_Reg_108	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Passed	

EWCJ178S_Reg_109	Verifying the Dot1x+EWA support with Wpa2 security mac failure	To verify the Dot1x+EWA Configuration with wpa2 supported SSID	Passed	
EWCJ178S_Reg_110	Verifying the Dot1x+EWA support with Wpa3 security .	To verify the Dot1x+EWA Configuration with wpa3 supported SSID	Passed	
EWCJ178S_Reg_111	Validating the Dot1x+EWA support and Layer 2 On Mac filter	To verify the Dot1x+EWA support and Layer3 On Mac filter failure	Passed	
EWCJ178S_Reg_112	Verifying the Dot1x+EWA support with Layer3 Splash page web redirect.	To verify the Dot1x+EWA support with Layer3 Splash page web redirect.	Passed	
EWCJ178S_Reg_113	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWCJ178S_Reg_114	Connecting Windows client to 9115 AP with Local mode Dot1x+EWA	To verify whether the windows client connect to 9115 AP with local mode Dot1x or not	Passed	
EWCJ178S_Reg_115	Configure Webauth on MAC failure with PSK	To verify the Webauth on MAC failure with PSK configuration	Passed	
EWCJ178S_Reg_116	Configure Webauth on MAC failure with dot1x	To verify the Webauth on MAC failure with Dot1x configuration	Passed	
EWCJ178S_Reg_117	Configure Webauth on MAC failure with FT dot1x	To verify the Webauth on MAC failure with FT Dot1x configuration	Passed	
EWCJ178S_Reg_118	Create wlan with dot1x +EWA security and check the inter roaming	To verify the Intra roaming by using dot1x+EWA security	Passed	

EWCJ178S_Reg_119	Create wlan with dot1x+ EWA security and check the intra roaming	To verify the Inter roaming by using dot1x+ EWA security	Passed	
EWCJ178S_Reg_120	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Passed	
EWCJ178S_Reg_121	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Passed	
EWCJ178S_Reg_122	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWCJ178S_Reg_123	Verifying the EWA support with 802.1x-SHA256 security.	To verify the EWA support with 802.1x-SHA256 security for the different clients.	Passed	

Easy PSK:WLAN Client Onboarding w/o registration

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_156	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	
EWLCJ178S_Reg_157	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	
EWLCJ178S_Reg_158	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	
EWLCJ178S_Reg_159	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	
EWLCJ178S_Reg_160	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	

EWLCJ178S_Reg_161	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	
EWLCJ178S_Reg_162	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	
EWLCJ178S_Reg_163	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	
EWLCJ178S_Reg_164	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 verify 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	
EWLCJ178S_Reg_165	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 through yang. Verify that the same config can be observed in the CLI.	Passed	
EWLCJ178S_Reg_166	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	

EWLCJ178S_Reg_167	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	
EWLCJ178S_Reg_168	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	
EWLCJ178S_Reg_169	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	
EWLCJ178S_Reg_170	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	

EWLCJ178S_Reg_171	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	
EWLCJ178S_Reg_172	Configure an easy psk wlan using a aaa server that is not reachable. 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 reachable. Verify that the client can't reach Run state and is deleted.	Passed	
EWLCJ178S_Reg_173	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	

Efficient AP Image Upgrade for eWLC

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_174	Verify if https AP image download is disabled by default on eWLC	To verify if the https AP download is disabled by default and check the same for all eWLC	Passed	
EWLCJ178S_Reg_175	Enabling the https AP image download from CLI for 9800-40 eWLC	To enabling the https AP image download from CLI for 9800-40 eWLC	Passed	
EWLCJ178S_Reg_176	Enabling the https AP image download from CLI for 9800-80 eWLC	To enabling the https AP image download from CLI for 9800-80 eWLC	Passed	
EWLCJ178S_Reg_177	Enabling the https AP image download from CLI for 9800-L eWLC	To enabling the https AP image download from CLI for 9800-L eWLC	Passed	
EWLCJ178S_Reg_178	Enabling the https AP image download from CLI for 9800-CL eWLC	To enabling the https AP image download from CLI for 9800-CL eWLC	Passed	
EWLCJ178S_Reg_179	Verify 9105 AP is able to download image using https	To verify if 9105 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_180	Verify 9115 AP is able to download image using https	To verify if 9115 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_181	Verify 9120 AP is able to download image using https	To verify if 9120 AP is able to download image using https and check the AP details after the image download	Passed	

EWLCJ178S_Reg_182	Verify 9130 AP is able to download image using https	To verify if 9130 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_183	Verify 4800 AP is able to download image using https	To verify if 4800 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_184	Verify if 9105 AP is able to download image using ftp	To verify if 9105 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_185	Verify if 9115 AP is able to download image using ftp	To verify if 9115 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_186	Verify if 9120 AP is able to download image using ftp	To verify if 9120 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_187	Verify if 9130 AP is able to download image using ftp	To verify if 9130 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_188	Verify if 4800 AP is able to download image using ftp	To verify if 4800 AP is able to download image using https and check the AP details after the image download	Passed	
EWLCJ178S_Reg_189	Verify AP is able to download image via capwap after disabling https or ftp	To verify AP is able to download image via capwap after disabling https or ftp	Passed	

EWLCJ178S_Reg_190	Verify AP join image download over https and HA switchover is triggered	To verify the behaviour when HA switchover is triggered during AP join image download over https	Passed	
EWLCJ178S_Reg_191	Verify AP join image download over ftp and HA switchover is triggered	To verify the behaviour when HA switchover is triggered during AP join image download over FTP	Passed	
EWLCJ178S_Reg_192	Verify flex mode AP is able to download image using https in AP join state	To verify flex mode AP is able to download image using https in AP join state	Passed	
EWLCJ178S_Reg_193	Verify if the Https image download happens when window clients connected	To verify if the Https AP image download is happening when the Window client is connected to the AP and check the client behaviour	Passed	
EWLCJ178S_Reg_194	Verify if the Https image download happens when Android clients connected	To verify if the Https AP image download is happening when the Android client is connected to the AP and check the client behaviour	Passed	
EWLCJ178S_Reg_195	Verify if the Https image download happens when iPhone clients connected	To verify if the Https AP image download is happening when the iPhone client is connected to the AP and check the client behaviour	Passed	

EWLCJ178S_Reg_196	Verify if the Https image download happens when Mac clients connected	To verify if the Https AP image download is happening when the Mac client is connected to the AP and check the client behaviour	Passed	

Enhanced PnP for workflow support (AP dependency)

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_197	Configure AP via PNP workflow using EAP-TLS authentication	To configure AP via PNP workflow using EAP-TLS authentication	Passed	
EWLCJ178S_Reg_198	Configure AP via PNP workflow using EAP-PEAP authentication	To configure AP via PNP workflow using EAP-PEAP authentication	Passed	
EWLCJ178S_Reg_199	Configure AP via PNP workflow using EAP-FAST authentication	To configure AP via PNP workflow using EAP-FAST authentication	Passed	
EWLCJ178S_Reg_200	Configure 4800 AP via PNP workflow using EAP authentication	To configure 4800 AP via PNP workflow using EAP authentication	Passed	
EWLCJ178S_Reg_201	Configure 9120 AP via PNP workflow using EAP authentication	To configure 9120 AP via PNP workflow using EAP authentication	Passed	
EWLCJ178S_Reg_202	Configure 9115 AP via PNP workflow using EAP authentication	To configure 9115 AP via PNP workflow using EAP authentication	Passed	
EWLCJ178S_Reg_203	Configure 9105 AP via PNP workflow using EAP authentication	To configure 9105 AP via PNP workflow using EAP authentication	Passed	
EWLCJ178S_Reg_204	Configure 9130 AP via PNP workflow using EAP authentication	To configure 9130 AP via PNP workflow using EAP authentication	Passed	
EWLCJ178S_Reg_205	Configure 9105 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9105 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	

EWLCJ178S_Reg_206	Configure 9115 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9115 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ178S_Reg_207	Configure 9120 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9120 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ178S_Reg_208	Configure 9130 as EWC & onboard an AP via PnP workflow with EAP authentication	To configure 9130 as EWC & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ178S_Reg_209	Configure EWC redundancy & onboard an AP via PnP workflow with EAP authentication	To configure EWC redundancy & onboard an AP via PnP workflow with EAP authentication	Passed	
EWLCJ178S_Reg_210	Configure AP via PnP workflow and claim multiple AP's at the same time	To configure AP via PnP workflow and claim multiple AP's at the same time	Passed	

HA Management - Interface Status of the Stndby through the Active using SNMP

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_211	Check if standby interface status details are shown on bootup in active	To check if standby interface status details are shown on bootup in active	Passed	
EWLCJ178S_Reg_212	Check if standby interface status details are shown on moving to SSO mode in active	To check if standby interface status details are shown on moving to SSO mode in active	Passed	
EWLCJ178S_Reg_213	Check if standby interface status details are updated on adding interface in active	To check if standby interface status details are updated on adding interface in active	Passed	
EWLCJ178S_Reg_214	Check if standby interface status details are updated on adding VLAN interface in active	To check if standby interface status details are updated on adding VLAN interface in active	Passed	
EWLCJ178S_Reg_215	Check if standby interface status details are updated on removing rmi cable/breaking the HA connectivity	To check if standby interface status details are updated on removing rmi cable/breaking the HA connectivity	Passed	
EWLCJ178S_Reg_216	Check if standby interface status details changes upon AP addition	To check if standby interface status details changes upon AP addition	Passed	
EWLCJ178S_Reg_217	Check if standby interface status details are updated on removing VLAN interface in active	To check if standby interface status details are updated on removing VLAN interface in active	Passed	
EWLCJ178S_Reg_218	Check if standby interface status details are updated on shutting VLAN interface in active	To check if standby interface status details are updated on shutting VLAN interface in active	Passed	

EWLCJ178S_Reg_219	Check if standby interface status details are shown in active chassis on standby reload	To check if standby interface status details are shown in active chassis on standby reload	Passed	
EWLCJ178S_Reg_220	Check if standby interface status details are shown on active chassis for different SNMP protocols/privileges	To check if standby interface status details are shown on active chassis for different SNMP protocols/privileges	Passed	
EWLCJ178S_Reg_221	Check if standby interface status details are shown without loopback/null address	To check if standby interface status details are shown without loopback/null address	Passed	

HA SSO RMI

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_222	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	
EWLCJ178S_Reg_223	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ178S_Reg_224	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ178S_Reg_225	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ178S_Reg_226	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ178S_Reg_227	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	
EWLCJ178S_Reg_228	Enable gateway failover, verify output details and monitor devices for switchover.	To enable gateway failover, verify output details & monitor devices for switchover.	Passed	
EWLCJ178S_Reg_229	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	
EWLCJ178S_Reg_230	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ178S_Reg_231	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ178S_Reg_232	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ178S_Reg_233	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	

EWLCJ178S_Reg_234	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	
EWLCJ178S_Reg_235	Force multiple switchover and verify AP & client association	To force multiple switchover and verify AP & client association	Passed	
EWLCJ178S_Reg_236	Validate licensing information after ISSU upgrade/downgrade	To validate licensing information after ISSU upgrade/downgrade	Passed	
EWLCJ178S_Reg_237	Validate licensing information after multiple switchover and reload	To validate licensing information after multiple switchover and reload	Passed	
EWLCJ178S_Reg_238	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ178S_Reg_239	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	
EWLCJ178S_Reg_240	Configure HA SSO RMI after RP-clear & validate HA RMI parameters.	To configure HA SSO RMI after RP-clear & validate HA RMI parameters.	Passed	
EWLCJ178S_Reg_241	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ178S_Reg_242	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ178S_Reg_243	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ178S_Reg_244	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ178S_Reg_245	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	

EWLCJ178S_Reg_246	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	

Intelligent AP auditing on WLC

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_247	Configure Radio monitoring	Verify the radio monitoring parameter configured or not	Passed	
EWLCJ178S_Reg_248	Configure AP monitoring	Verify the Ap monitoring parameter configured or not	Passed	
EWLCJ178S_Reg_249	Configure high CPU utilization	To Verify reload happen or not for high CPU utilization	Passed	
EWLCJ178S_Reg_250	Configure high memory utilization	To Verify reload happen or not for high memory utilization	Passed	
EWLCJ178S_Reg_251	Validate the AP disconnect reason code for high memory	Check the AP disconnect reason code if AP is showing high memory.	Passed	
EWLCJ178S_Reg_252	Validate the AP disconnect reason code for high CPU.	Check the AP disconnect reason code if AP is showing high CPU.	Passed	
EWLCJ178S_Reg_253	show commands stats for AP action	Verify if AP show stats commands of AP high CPU/memory and radio stuck are incrementing on each action	Passed	
EWLCJ178S_Reg_254	Configure different sampling periods.	Configure different sampling periods for AP CPU and high memory and verify if computation works fine.	Passed	

EWLCJ178S_Reg_255	Configure different threshold time	Configure different threshold values for AP CPU and high memory and verify if computation works fine.	Passed	
EWLCJ178S_Reg_256	NETCONF config data	Configure all AP system and radio monitoring via NETCONF	Passed	
EWLCJ178S_Reg_257	NETCONF notification	Verify that NETCONF notification is getting generated for AP high CPU, high memory disconnect reason and radio reset due to radio stuck.	Passed	
EWLCJ178S_Reg_258	Pre-download/upgrade case	No AP reload action should be taken when AP is doing pre-download or upgrade of the image	Passed	
EWLCJ178S_Reg_259	Validate AP action for max value configure in sampling period	Configure Max Sampling values for AP CPU and high memory and verify if computation works fine	Passed	
EWLCJ178S_Reg_260	Validate AP action for max value configure in threshold time	Configure Max threshold time for AP CPU and high memory and verify if computation works fine	Passed	
EWLCJ178S_Reg_261	Validate the CPU and memory details in DNAC	Verify the radio , AP monitoring parameter details showing or not in DANC	Passed	
EWLCJ178S_Reg_262	Verify the client association during ap reload	Verify client connected or not after ap reload	Passed	

EWLCJ178S_Reg_263	Configure high CPU & memory for continuous ap reload action	Verify any crash happen or not during continuous reload ap action	Passed	

iPSK Peer to Peer Blocking

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_264	Verifying the iPSK tag generation for the Connected Window JOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Window JOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ178S_Reg_265	Verifying the iPSK tag generation for the Connected MAC OS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When MAC OS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ178S_Reg_266	Verifying the iPSK tag generation for the Connected iOS Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When iOS connected to iPSK enabled WLAN Profile	Passed	
EWLCJ178S_Reg_267	Verifying the iPSK tag generation for the Connected Android Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Android connected to iPSK enabled WLAN Profile	Passed	
EWLCJ178S_Reg_268	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	
EWLCJ178S_Reg_269	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	
EWLCJ178S_Reg_270	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	

EWLCJ178S_Reg_271	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	
EWLCJ178S_Reg_272	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	
EWLCJ178S_Reg_273	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	
EWLCJ178S_Reg_274	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	
EWLCJ178S_Reg_275	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	
EWLCJ178S_Reg_276	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	
EWLCJ178S_Reg_277	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	

EWLCJ178S_Reg_278	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	
EWLCJ178S_Reg_279	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	
EWLCJ178S_Reg_280	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	
EWLCJ178S_Reg_281	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	
EWLCJ178S_Reg_282	Verifying connected clients with the particular iPSK tag in CLI	To verify whether all the clients sharing iPSK tag are shown or not in eWLC CLI	Passed	
EWLCJ178S_Reg_283	Verifying the wlan configuration with iPSK tag Configuration through eWLC Web	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC Web	Passed	

EWLCJ178S_Reg_284	Verifying the wlan generation with iPSK tag Configuration through eWLC CLI	To verify whether wlan profile can be created or not with the iPSK configuration through the eWLC CLI	Passed	
EWLCJ178S_Reg_285	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	
EWLCJ178S_Reg_286	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	
EWLCJ178S_Reg_287	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	
EWLCJ178S_Reg_288	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	
EWLCJ178S_Reg_289	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWLCJ178S_Reg_290	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	
EWLCJ178S_Reg_291	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	

EWLCJ178S_Reg_292	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	
EWLCJ178S_Reg_293	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	
EWLCJ178S_Reg_294	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	
EWLCJ178S_Reg_295	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	
EWLCJ178S_Reg_296	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	
EWLCJ178S_Reg_297	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	

EWLCJ178S_Reg_298	Verifying the iPSK tag generation for the Connected anyconnect Client in eWLC UI/CLI	To verify whether iPSK tag generated or not When Anyconnect client connected to iPSK enabled WLAN Profile	Passed	
EWLCJ178S_Reg_299	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	
EWLCJ178S_Reg_300	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	
EWLCJ178S_Reg_301	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	
EWLCJ178S_Reg_302	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	
EWLCJ178S_Reg_303	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	

EWLCJ178S_Reg_304	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	
EWLCJ178S_Reg_305	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	
EWLCJ178S_Reg_306	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	
EWLCJ178S_Reg_307	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	
EWLCJ178S_Reg_308	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	

EWLCJ178S_Reg_309	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ178S_Reg_310	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ178S_Reg_155	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	
EWCJ178S_Reg_156	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	
EWCJ178S_Reg_157	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	
EWCJ178S_Reg_158	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	
EWCJ178S_Reg_159	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	
EWCJ178S_Reg_160	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	

EWCJ178S_Reg_161	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	
EWCJ178S_Reg_162	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	
EWCJ178S_Reg_163	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	
EWCJ178S_Reg_164	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	
EWCJ178S_Reg_165	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	
EWCJ178S_Reg_166	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	
EWCJ178S_Reg_167	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	

EWCJ178S_Reg_168	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	
EWCJ178S_Reg_169	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	
EWCJ178S_Reg_170	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	
EWCJ178S_Reg_171	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	
EWCJ178S_Reg_172	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	
EWCJ178S_Reg_173	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	

EWCJ178S_Reg_174	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	
EWCJ178S_Reg_175	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	
EWCJ178S_Reg_176	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	
EWCJ178S_Reg_177	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	
EWCJ178S_Reg_178	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	
EWCJ178S_Reg_179	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	
EWCJ178S_Reg_180	Verifying iPSK WLAN configuration after importing and exporting the same configuration file	To verify whether the wlan configuration retains same or not after exporting the same configuration file	Passed	
EWCJ178S_Reg_181	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	

EWCJ178S_Reg_182	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	
EWCJ178S_Reg_183	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	
EWCJ178S_Reg_184	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	
EWCJ178S_Reg_185	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	
EWCJ178S_Reg_186	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	
EWCJ178S_Reg_187	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	

EWCJ178S_Reg_188	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	
EWCJ178S_Reg_189	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	
EWCJ178S_Reg_190	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	
EWCJ178S_Reg_191	Verifying the generation of ipsk tag with WPA-TKIP-PSk for same/different os clients.	To verify whether iPSK generated or not when WLAN is enabled with WPA-TkIP-PSK	Passed	
EWCJ178S_Reg_192	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	
EWCJ178S_Reg_193	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	

EWCJ178S_Reg_194	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	
EWCJ178S_Reg_195	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	
EWCJ178S_Reg_196	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	
EWCJ178S_Reg_197	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	
EWCJ178S_Reg_198	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	

EWCJ178S_Reg_199	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	
EWCJ178S_Reg_200	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ178S_Reg_201	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	

Knob to disable Random MAC Clients

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_311	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWLCJ178S_Reg_312	Enable Deny LAA in WLAN and connect iPhone with burned in mac	To verify connectivity after enabling LAA in WLAN and connect iPhone with burned in mac	Passed	
EWLCJ178S_Reg_313	Enable Deny LAA in WLAN and connect Windows with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Windows with burned in mac / WIFI adapter mac	Passed	
EWLCJ178S_Reg_314	Enable Deny LAA in WLAN and connect Android with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Android with burned in mac	Passed	
EWLCJ178S_Reg_315	Enable Deny LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWLCJ178S_Reg_316	Enable Deny LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Passed	
EWLCJ178S_Reg_317	Enable Deny LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	

EWLCJ178S_Reg_318	Connect iPhone without deny LAA in WLAN and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ178S_Reg_319	Connect windows without deny LAA in WLAN and after joining enable deny LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ178S_Reg_320	Connect android without deny LAA in WLAN and after joining enable deny LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWLCJ178S_Reg_321	Connect iPhone without deny LAA in WLAN and after joining enable deny LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWLCJ178S_Reg_322	Connect windows without deny LAA in WLAN and after joining enable deny LAA in WLAN device disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect windows without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	

EWLCJ178S_Reg_323	Connect android without deny LAA in WLAN and after joining enable deny LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect android without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWLCJ178S_Reg_324	Connect one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	To verify connectivity after connecting one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	Passed	
EWLCJ178S_Reg_325	Add LAA address of in iPhone client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of iPhone client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWLCJ178S_Reg_326	Add LAA address of in windows client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of Windows client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	

EWLCJ178S_Reg_327	functionality of Non random mac Client with default config and verify client details in DNAC	To verify functionality of Non random mac Client with default config and verify client details in DNAC	Passed	
EWLCJ178S_Reg_328	client connectivity to WLAN enabled with LAA deny after ewlc reload	To verify client connectivity to WLAN enabled with LAA deny after ewlc reload	Passed	
EWCJ178S_Reg_202	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWCJ178S_Reg_203	Enable LAA in WLAN and connect iPhone with burned in mac	To verify connectivity after enabling LAA in WLAN and connect iPhone with burned in mac	Passed	
EWCJ178S_Reg_204	Enable LAA in WLAN and connect Windows with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Windows with burned in mac / WIFI adapter mac	Passed	
EWCJ178S_Reg_205	Enable LAA in WLAN and connect Android with burned in mac	To verify connectivity after enabling LAA in WLAN and connect Android with burned in mac	Passed	
EWCJ178S_Reg_206	Enable LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWCJ178S_Reg_207	Enable LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Passed	

EWCJ178S_Reg_208	Enable LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	
EWCJ178S_Reg_209	Connect iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ178S_Reg_210	Connect windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting windows without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ178S_Reg_211	Connect android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	To verify connectivity after connecting android without LAA and after joining enable LAA device in WLAN and verify client connectivity.	Passed	
EWCJ178S_Reg_212	Connect iPhone without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting iPhone without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	

EWCJ178S_Reg_213	Connect windows without LAA and after joining enable LAA in WLAN device disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect windows without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWCJ178S_Reg_214	Connect android without LAA and after joining enable LAA in WLAN, disconnect and reconnect the device to different SSID without LAA	To verify connectivity after connecting connect android without LAA and after joining enable LAA device disconnect and reconnect the device to different SSID without LAA	Passed	
EWCJ178S_Reg_215	Connect one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	To verify connectivity after connecting one device in random mac and other with burned-in mac to WLAN profile with LAA enabled	Passed	
EWCJ178S_Reg_216	Add LAA address of in iPhone client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of iPhone client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	

EWCJ178S_Reg_217	Add LAA address of in windows client and Create a DHCP pool in ewlc and give LAA of windows as client identifier and use LAA deny profile, connect client then check client gets denied or not	To verify connectivity after adding LAA mac address of Windows client and Create a DHCP pool in ewlc and give private mac address as client identifier and use LAA deny profile, connect client then check client gets denied or not	Passed	
EWCJ178S_Reg_218	functionality of Non random mac Client with default config and verify client details in DNAC	To verify functionality of Non random mac Client with default config and verify client details in DNAC	Passed	
EWCJ178S_Reg_219	functionality of Non random mac Client with default config and verify client details in DNA Spaces Behaviour metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS Behaviour metrics	Passed	
EWCJ178S_Reg_220	functionality of Non random mac Client with default config and verify client details in DNA Spaces location metrics	To verify functionality of Non random mac Client with default config and verify client details in DNAS location metrics	Passed	
EWCJ178S_Reg_221	client connectivity to WLAN enabled with LAA deny after ewlc reload	To verify client connectivity to WLAN enabled with LAA deny after ewlc reload	Passed	

Link local bridging support

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_329	Configure Link Local Bridging policy profile configuration via CLI	To configure Link Local Bridging policy profile configuration via CLI	Passed	
EWLCJ178S_Reg_330	Checking the status of the LL bridging after creating the policy profile	To check the status of the LL bridging in policy profile	Passed	
EWLCJ178S_Reg_331	Enabling Link Local Bridging policy profile configuration via UI	To enabling Link Local Bridging policy profile configuration via UI	Passed	
EWLCJ178S_Reg_332	Configuring LL bridging policy profile with different VLAN id and connecting a client	To configure Link Local Bridging policy profile with different VLAN id and check if the clients gets connected or not	Passed	
EWLCJ178S_Reg_333	Connecting a Window client to the LL bridging policy profile configured with VLAN	To connect a Window client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ178S_Reg_334	Connecting a Android client to the LL bridging policy profile configured with VLAN	To connect a Android client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	

EWLCJ178S_Reg_335	Connecting a IOS client to the LL bridging policy profile configured with VLAN	To connect a IOS client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ178S_Reg_336	Connecting a Mac OS client to the LL bridging policy profile configured with VLAN	To connect a Mac OS client to the LL bridging policy profile configured with VLAN and check if the client connected and the VLAN given in policy profile is used by the client for traffic	Passed	
EWLCJ178S_Reg_337	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Window client from first to second controller.	To roam the Window client frone one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ178S_Reg_338	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Android client from first to second controller.	To roam the Android client frone one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	

EWLCJ178S_Reg_339	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the IOS client from first to second controller.	To roam the IOS client frone one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ178S_Reg_340	Enable link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC. Roam the Window client from first to second controller.	To roam the Mac OS client frone one eWLC to another eWLC enabling link local bridging in an inter controller scenario, with a different VLAN set on first eWLC than on second eWLC.	Passed	
EWLCJ178S_Reg_341	Enabling link local bridging in policy profile in a HA setup and verifying the same after switchover	To verify the link local bridging in policy profile in a HA setup and check the configuration after the switchover	Passed	
EWLCJ178S_Reg_342	Enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	Passed	
EWLCJ178S_Reg_343	Enable link local bridging in policy profile in a HA setup and Join a Android client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window client to try Switch over.	Passed	
EWLCJ178S_Reg_344	Enable link local bridging in policy profile in a HA setup and Join a IOS client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a IOS client to try Switch over.	Passed	

EWLCJ178S_Reg_345	Enable link local bridging in policy profile in a HA setup and Join a Mac OS client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a Mac OS client to try Switch over.	Passed	
EWLCJ178S_Reg_346	Enable link local bridging in policy profile in a HA setup and Join a window Surface client to try Switch over.	To enable link local bridging in policy profile in a HA setup and Join a window Surface client to try Switch over.	Passed	

MAC Address Consistency

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_347	Configuring the Mobility Peer Mac Address with different formats to verify the consistency	To configure the Mobility Peer Mac Address with different formats to verify the consistency	Passed	
EWLCJ178S_Reg_348	Configure AP Provisioning to check MAC Address consistency	To Configure Ap Provisioning to check MAC Address consistency	Failed	CSCwb19471
EWLCJ178S_Reg_349	Configure Ap tag to check MAC Address consistency	To Configure Ap tag to check MAC Address consistency	Failed	CSCwb57095
EWLCJ178S_Reg_350	Configure Policy Map to check MAC Address consistency	To Configure Policy Map to check MAC Address consistency	Passed	
EWLCJ178S_Reg_351	Configure Device authentication to check MAC Address consistency	To Configure Device authentication to check MAC Address consistency	Passed	
EWLCJ178S_Reg_352	Configure Device authentication through CSV file to check MAC Address consistency	To Configure Device authentication through CSV file to check MAC Address consistency	Passed	
EWLCJ178S_Reg_353	Configure Excluded clients to check MAC Address consistency	To configure Excluded clients to check MAC Address consistency	Passed	
EWLCJ178S_Reg_354	Configure Radioactive trace to check MAC Address consistency	To configure Radioactive trace to check MAC Address consistency	Passed	
EWLCJ178S_Reg_355	Configure packet tracer to check MAC Address consistency	To configure Packet tracer to check MAC Address consistency	Passed	

EWLCJ178S_Reg_356	Configure Ap Join to check MAC Address consistency	To Configure Ap Join to check MAC Address consistency	Passed	
EWLCJ178S_Reg_357	Configure Mac filtering windows client connection to check MAC Address consistency	To Configure Mac filtering windows client connection to check MAC Address consistency	Passed	
EWLCJ178S_Reg_358	Configure Mac filtering MAC/Android client connection to check MAC Address consistency	To Configure Mac filtering MAC/Android client connection to check MAC Address consistency	Passed	
EWLCJ178S_Reg_359	Configure client whitelisting to check MAC Address consistency	To Configure client whitelisting to check MAC Address consistency	Passed	
EWLCJ178S_Reg_360	Deleting a Whitelisted User & client MAC Address in UI	To check whether a guest user & MAC Address consistency can be deleted or not in EWLC UI	Passed	
EWLCJ178S_Reg_361	Associating Window client with Mac filter enabled L3-Web auth SSID & Web login with guest user	To check that Window 10 client got associated with Mac filter enabled L3-Web auth SSID & Login with guest user credentials	Passed	
EWLCJ178S_Reg_362	Configure when eWC1 is down AP should join to eWC2	To Configure when eWC1 is down AP should join to eWC2	Passed	
EWLCJ178S_Reg_363	Verify client delete reason (mac-address) code is generated or not to check MAC Address consistency	To Verify client delete reason (mac-address) code is generated or not to check MAC Address consistency	Passed	
EWLCJ178S_Reg_364	Verify whether your able to add APs MAC Address to LSC Provision List	To Verify whether your able to add APs MAC Address to LSC Provision List	Passed	

EWLCJ178S_Reg_365	Verify whether you are able to add APs MAC Address through CSV file to LSC Provision List	To Verify whether you are able to add APs MAC Address through CSV file to LSC Provision List	Passed	
EWLCJ178S_Reg_366	Verify whether you are able to add MAC Address in Ap certificate policy	To Verify whether you are able to add MAC Address in Ap certificate policy	Passed	
EWLCJ178S_Reg_367	Verify whether you are able to add MAC Address through CSC file in Ap certificate policy	To Verify whether you are able to add MAC Address through CSC file in Ap certificate policy	Passed	
EWLCJ178S_Reg_368	Verifying whether you are able to get RA logs to check MAC Address consistency	To Verify whether you are able to get RA logs to check MAC Address consistency	Passed	
EWLCJ178S_Reg_369	Verify mac filtering client connection in WLC to check MAC Address consistency	To Verify mac filtering client connection in WLC to check MAC Address consistency	Passed	
EWCJ178S_Reg_222	Configure Excluded clients by using mac_address consistency	To Configure Excluded clients by using mac_address consistency	Passed	
EWCJ178S_Reg_223	Configure Radioactive trace by using mac_address consistency	To Configure Radioactive trace by using mac_address consistency	Passed	
EWCJ178S_Reg_224	Configure packet tracer by using mac_address consistency	To Configure Packet tracer by using mac_address consistency	Passed	
EWCJ178S_Reg_225	Configure Ap Provisioning by using mac_address consistency	To Configure Ap Provisioning by using mac_address consistency	Passed	
EWCJ178S_Reg_226	Configure Ap tag by using mac_address consistency	To Configure Ap tag by using mac_address consistency	Passed	

EWCJ178S_Reg_227	Configure Policy Map by using mac_address consistency	To Configure Policy Map by using mac_address consistency	Passed	
EWCJ178S_Reg_228	Configure Device authentication by using mac_address consistency	To Configure Device authentication by using mac_address consistency	Passed	
EWCJ178S_Reg_229	Configure Device authentication through CSV file by using mac_address consistency	To Configure Device authentication through CSV file by using mac_address consistency	Passed	
EWCJ178S_Reg_230	Configure Ap Join by using mac_address consistency	To Configure Ap Join by using mac_address consistency	Failed	CSCwb65684
EWCJ178S_Reg_231	Configure Mac filtering windows client connection by using mac_address consistency	To Configure Mac filtering windows client connection by using mac_address consistency	Failed	CSCwb31009
EWCJ178S_Reg_232	Configure Mac filtering MAC/Android client connection by using mac_address consistency	To Configure Mac filtering MAC/Android client connection by using mac_address consistency	Failed	CSCwb59244
EWCJ178S_Reg_233	Configure client whitelisting by using mac_address consistency	To Configure client whitelisting by using mac_address consistency	Passed	
EWCJ178S_Reg_234	Deleting a Whitelisted User & client mac address in UI	To check whether a guest user & mac address consistency can be deleted or not in EWLC UI	Passed	
EWCJ178S_Reg_235	Associating Window client with Mac filter enabled L3-Web auth SSID & Web login with guest user	To check that Window 10 client got associated with Mac filter enabled L3-Web auth SSID & Login with guest user credentials	Passed	

EWCJ178S_Reg_236	Configure when eWC1 is down AP should join to eWC2	To Configure when eWC1 is down AP should join to eWC2	Passed	
EWCJ178S_Reg_237	Verify client delete reason (mac-address) code is generated or not by using mac_address consistency	To Verify client delete reason (mac-address) code is generated or not by using mac_address consistency	Passed	
EWCJ178S_Reg_238	Verify whether your able to add APs MAC address to LSC Provision List	To Verify whether your able to add APs MAC address to LSC Provision List	Passed	
EWCJ178S_Reg_239	Verify whether you are able to add APs MAC address through CSV file to LSC Provision List	To Verify whether you are able to add APs MAC address through CSV file to LSC Provision List	Passed	
EWCJ178S_Reg_240	Verify whether you are able to add MAC address in Ap certificate policy	To Verify whether you are able to add MAC address in Ap certificate policy	Passed	
EWCJ178S_Reg_241	Verify whether you are able to add MAC address through CSC file in Ap certificate policy	To Verify whether you are able to add MAC address through CSC file in Ap certificate policy	Passed	
EWCJ178S_Reg_242	Verify whether you are able to get RA logs by using Mac_address consistency	To Verify whether you are able to get RA logs by using Mac_address consistency	Passed	
EWCJ178S_Reg_243	Verify mac filtering client connection in WLC by using mac_address consistency	To Verify mac filtering client connection in WLC by using mac_address consistency	Passed	

Mesh faster forced client roaming

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_594	Enable/disable fast-teardown through CLI and verify output of show commands	To enable/disable fast-teardown through CLI and to verify output of show commands	Passed	
EWLCJ178S_Reg_595	Configure all feature parameters to non-default values and check with show commands	To configure all feature parameters to non-default values and check with show commands	Passed	
EWLCJ178S_Reg_596	Roam Windows machine b/w APs when fast-teardown set to default and verify latency	To roam Windows machine b/w APs when fast-teardown set to default and verify latency	Passed	
EWLCJ178S_Reg_597	Roam Windows machine b/w APs when fast-teardown set to non-default and verify latency	To roam Windows machine b/w APs when fast-teardown set to non-default and verify latency	Passed	
EWLCJ178S_Reg_598	Roam Android client b/w APs when fast-teardown set to default and verify latency	To roam Android client b/w APs when fast-teardown set to default and verify latency	Passed	
EWLCJ178S_Reg_599	Roam Android client b/w APs when fast-teardown set to non-default and verify latency	To roam Android client b/w APs when fast-teardown set to non-default and verify latency	Passed	
EWLCJ178S_Reg_600	Roam MAC client b/w APs when fast-teardown set to default and verify latency	To roam MAC client b/w APs when fast-teardown set to default and verify latency	Passed	
EWLCJ178S_Reg_601	Roam MAC client b/w APs when fast-teardown set to non-default and verify latency	To roam MAC client b/w APs when fast-teardown set to non-default and verify latency	Passed	

EWLCJ178S_Reg_602	Roam IOS client b/w APs when fast-teardown set to default and verify latency	To roam IOS client b/w APs when fast-teardown set to default and verify latency	Passed	
EWLCJ178S_Reg_603	Roam IOS client b/w APs when fast-teardown set to non-default and verify latency	To roam IOS client b/w APs when fast-teardown set to non-default and verify latency	Passed	
EWLCJ178S_Reg_604	Roam Surface Go Plus client b/w APs when fast-teardown set to default and verify latency	To roam Surface Go Plus client b/w APs when fast-teardown set to default and verify latency	Passed	
EWLCJ178S_Reg_605	Roam Surface Go Plus client b/w APs when fast-teardown set to non-default and verify latency	To roam Surface Go Plus client b/w APs when fast-teardown set to non-default and verify latency	Passed	

Per AP Group NTP Server Config

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_389	Configure AP Group NTP Server in CMX and verify NTP status in Console	To configure AP Group NTP Server in CMX and verify NTP status in Console	Passed	
EWLCJ178S_Reg_390	Remove NTP Server from CMX and verify NTP status in Console	To remove NTP Server from CMX and verify NTP status in Console	Passed	
EWLCJ178S_Reg_391	Add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	
EWLCJ178S_Reg_392	Remove NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To remove NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	
EWLCJ178S_Reg_393	Verify whether AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address through GUI	To verify whether AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address through GUI	Passed	
EWLCJ178S_Reg_394	Verify whether AP is getting ntpd is not running or not after removing NTP IPV4/IPV6 address through GUI	To verify whether AP is getting ntpd is not running or not after removing NTP IPV4/IPV6 address through GUI	Failed	CSCwb22034
EWLCJ178S_Reg_395	Modify AP Timezone using Controller	To modify AP Timezone using Controller	Passed	
EWLCJ178S_Reg_396	Check warning message when Hyper location enabled, but NTP server is not configured	To check warning message when Hyper location enabled, but NTP server is not configured	Passed	

EWLCJ178S_Reg_397	Check memory leaks after configuring NTP Server and Authentication Key through CLI	To check memory leaks after configuring NTP Server and Authentication Key	Passed	
EWLCJ178S_Reg_398	Check memory leaks after configuring NTP Server and Authentication Key through GUI	To check memory leaks after configuring NTP Server and Authentication Key	Passed	
EWLCJ178S_Reg_399	Configure Authentication key in CLI and remove configured key through GUI	To configure Authentication key in CLI and to remove configured key through GUI	Passed	
EWLCJ178S_Reg_400	Verify whether 9105 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9105 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ178S_Reg_401	Verify whether 9115 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9115 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ178S_Reg_402	Verify whether 9120 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	To verify whether 9120 AP is getting ntpd is up and running or not after configuring NTP IPV4/IPV6 address	Passed	
EWLCJ178S_Reg_403	Connect multiple Aps and check ntpd is up and running or not after configuring NTP IPV4/IPV6 address in AP Join page	To connect multiple Aps and check ntpd is up and running or not after configuring NTP IPV4/IPV6 address in AP Join page	Passed	

EWLCJ178S_Reg_404	Configure Authentication key through Best Practices and check whether AP is getting ntpd is up and running or not	To configure Authentication key through Best Practices and check whether AP is getting ntpd is up and running or not	Passed	
EWLCJ178S_Reg_405	Check UI is getting error message or not if trusted-key is invalid	To check UI is getting error message or not if trusted-key is invalid	Passed	
EWLCJ178S_Reg_406	Check any errors messages triggered or not after configuring trusted key	To check any errors messages triggered or not after configuring trusted key	Passed	

Provide alert mechanism on web-ui for critical events on controller

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_407	Verify alerts are displayed for critical events	To Verify alerts are displayed for critical events	Passed	
EWLCJ178S_Reg_408	Verify alerts are displayed for alert events	To Verify alerts are displayed for alert events	Passed	
EWLCJ178S_Reg_409	Verify alerts are displayed for emergency events	To Verify alerts are displayed for emergency events	Passed	
EWLCJ178S_Reg_410	Export syslog events	To Export syslog events from webui	Passed	
EWLCJ178S_Reg_411	Verify user able to filter options	To Verify user able to filter syslog messages	Passed	
EWLCJ178S_Reg_412	Disable Event banner	To Disable Event banner using preference	Passed	
EWLCJ178S_Reg_413	Enable Event banner	To Enable Event banner using preference	Passed	
EWLCJ178S_Reg_414	Delete an Event Notification	To Delete an Event Notification	Passed	CSCwb37066
EWLCJ178S_Reg_415	Delete multiple/all Event Notification	To Delete multiple/all Event Notification	Passed	
EWLCJ178S_Reg_416	Verify Event count in Pie chart	To Verify Event count are properly shown in Pie chart	Passed	
EWLCJ178S_Reg_417	Force Switchover in HA and verify alerts are shown	To Force Switchover in HA and verify alerts are shown	Passed	
EWLCJ178S_Reg_418	Verify Banner preferences after switchover in HA	To Verify Banner preferences after switchover in HA	Passed	

PSK + Mulit Auth Support for Guest

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_419	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ178S_Reg_420	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ178S_Reg_421	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ178S_Reg_422	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ178S_Reg_423	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ178S_Reg_424	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWLCJ178S_Reg_425	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ178S_Reg_426	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWLCJ178S_Reg_427	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWLCJ178S_Reg_428	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	

EWLCJ178S_Reg_429	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ178S_Reg_430	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ178S_Reg_431	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ178S_Reg_432	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ178S_Reg_433	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ178S_Reg_434	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ178S_Reg_273	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWCJ178S_Reg_274	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ178S_Reg_275	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWCJ178S_Reg_276	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWCJ178S_Reg_277	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	

EWCJ178S_Reg_278	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Verify WPA2 Security with MPSK Applied in Wlan's with Window's Clients with all the 5 Key Combinations	Passed	
EWCJ178S_Reg_279	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ178S_Reg_280	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ178S_Reg_281	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ178S_Reg_282	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ178S_Reg_283	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ178S_Reg_284	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ178S_Reg_285	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWCJ178S_Reg_286	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWCJ178S_Reg_287	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ178S_Reg_288	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

Regulatory Domain Reduction

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_435	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWLCJ178S_Reg_436	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWLCJ178S_Reg_437	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWLCJ178S_Reg_438	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWLCJ178S_Reg_439	Verify country code is changed for access point	To verify country code is changed for access point	Passed	
EWLCJ178S_Reg_440	Verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	To verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	Passed	
EWLCJ178S_Reg_441	Configure multiple countries through UI dashboard and disable same countries through CLI	To configure multiple countries through UI dashboard and disable same countries through CLI	Passed	
EWLCJ178S_Reg_442	Verify AP joins to other eWLC with another country code supported	To verify AP joins to other eWLC with another country code supported	Passed	
EWLCJ178S_Reg_443	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	
EWLCJ178S_Reg_444	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	

EWLCJ178S_Reg_445	Verify at least one Regulatory Domain is configured or not	To verify at least one Regulatory Domain is configured or not	Passed	
EWLCJ178S_Reg_446	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Passed	
EWLCJ178S_Reg_447	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWLCJ178S_Reg_448	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	
EWLCJ178S_Reg_449	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWLCJ178S_Reg_450	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWLCJ178S_Reg_451	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWLCJ178S_Reg_452	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	
EWLCJ178S_Reg_453	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	
EWLCJ178S_Reg_454	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	
EWLCJ178S_Reg_455	Verify list of access point models and protocols are supported per country and regulatory domain	To verify list of access point models and protocols are supported per country and regulatory domain	Passed	

EWLCJ178S_Reg_456	Verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	To verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	Passed	
EWCJ178S_Reg_289	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWCJ178S_Reg_290	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWCJ178S_Reg_291	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWCJ178S_Reg_292	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWCJ178S_Reg_293	Verify country code is changed for access point	To verify country code is changed for access point	Passed	
EWCJ178S_Reg_294	Verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	To verify Syslog is generated or not after configuring non-regulatory country code to the Access Point	Passed	
EWCJ178S_Reg_295	Configure multiple countries through UI dashboard and disable same countries through CLI	To configure multiple countries through UI dashboard and disable same countries through CLI	Passed	
EWCJ178S_Reg_296	Verify AP joins to other eWLC with another country code supported	To verify AP joins to other eWLC with another country code supported	Passed	
EWCJ178S_Reg_297	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	

EWCJ178S_Reg_298	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	
EWCJ178S_Reg_299	Verify at least one Regulatory Domain is configured or not	To verify at least one Regulatory Domain is configured or not	Passed	
EWCJ178S_Reg_300	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Passed	
EWCJ178S_Reg_301	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWCJ178S_Reg_302	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	
EWCJ178S_Reg_303	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWCJ178S_Reg_304	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWCJ178S_Reg_305	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWCJ178S_Reg_306	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	
EWCJ178S_Reg_307	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	
EWCJ178S_Reg_308	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	

EWCJ178S_Reg_309	Verify list of access point models and protocols are supported per country and regulatory domain	To verify list of access point models and protocols are supported per country and regulatory domain	Passed	
EWCJ178S_Reg_310	Verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	To verify Prime Infrastructure Syslog alert is generated or not for non-regulatory domain	Passed	

SmartLicensing

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_457	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ178S_Reg_458	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWLCJ178S_Reg_459	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWLCJ178S_Reg_460	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWLCJ178S_Reg_461	Smart Licensing HA Support	To verify Smart Licensing for HA Support	Passed	
EWLCJ178S_Reg_462	Change a SLR on a C9800 SSO HA pair	To change a SLR on a C9800 SSO HA pair	Passed	
EWLCJ178S_Reg_463	Removing SLR from a C9800 SSO HA pair	To verify by removing SLR from a C9800 SSO HA pair	Passed	
EWLCJ178S_Reg_464	Validate license info in HA SSO RMI pair	To validate license info in HA SSO RMI pair	Passed	
EWLCJ178S_Reg_465	Validate license info on Standby unit directly	To validate license info on standby unit directly	Passed	
EWLCJ178S_Reg_466	Validate license info after ISSU upgrade	To validate license info after ISSU upgrade	Passed	
EWLCJ178S_Reg_467	Validate license info after multiple switchover	To validate license info after multiple switchover	Passed	
EWLCJ178S_Reg_468	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	

EWCJ178S_Reg_329	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWCJ178S_Reg_330	Generate token from CSSM	To Generate token from CSSM	Passed	
EWCJ178S_Reg_331	Product instance direct-connect using trust token	To verify Product instance direct-connect using trust token	Passed	
EWCJ178S_Reg_332	verify device status in CSSM	To verify device status in CSSM	Passed	
EWCJ178S_Reg_333	verify Smart Licensing Support in eWC HA	To verify Smart Licensing Support in eWC HA	Passed	
EWCJ178S_Reg_334	verify device details and license count changes in CSSM	To verify device details and license count changes in CSSM	Passed	
EWCJ178S_Reg_335	Add More AP's to device and Install trust token validate count on CSSM	To Add More AP's to device after Installing trust token to validate license count on CSSM	Passed	
EWCJ178S_Reg_336	Validate license info after switchover in AP	To validate license info after switchover in AP	Passed	
EWCJ178S_Reg_337	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWCJ178S_Reg_338	Install CSLU and add device and check status	Install CSLU and add device and check status	Passed	
EWCJ178S_Reg_339	Verify product details in CSSM after successfully shared product details from CSLU	Verify product details in CSSM after successfully shared product details from CSLU	Passed	

SSID per radio on Dual 5G

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_469	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWLCJ178S_Reg_470	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWLCJ178S_Reg_471	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	
EWLCJ178S_Reg_472	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWLCJ178S_Reg_473	Associating windows client to 9115 Ap with WPA2 security type for 2.4GHz radio policy	To Verify Windows client associate to 2.4 GHz radio with WPA2 security type or not	Passed	
EWLCJ178S_Reg_474	Associating Android client to 9120 Ap with WPA2 security type for 5GHz radio policy	To Verify android client associate to 5 GHz radio with WPA2 security type or not	Passed	
EWLCJ178S_Reg_475	Associating iOS client to 9130 Ap with WPA2 security type for 6GHz radio policy	To Verify iOS client associate to 6 GHz radio with WPA2 security type or not	Passed	
EWLCJ178S_Reg_476	Associating Mac client to 9105 Ap with WPA3 security type for 2.4GHz radio policy	To Verify mac client associate to 2.4 GHz radio with WPA3 security type or not	Passed	
EWLCJ178S_Reg_477	Associating Ms-go client to 9115 Ap with WPA3 security type for 5GHz radio policy	To associate the client and verifying EDCA parameter	Passed	

EWLCJ178S_Reg_478	Associating MS-GO2 client to 9120 Ap with WPA3 + AES cipher + OWE AKM security type for 6GHz radio policy	To Verify MS-GO2 client associate to 6 GHz radio with WPA3 + AES cipher + OWE AKM security type or not	Passed	
EWLCJ178S_Reg_479	Associating client with WPA3 + AES cipher + 802.1x-SHA256 AKM security type for 6GHz radio policy	To Verify Windows client associate to 6 GHz radio with WPA3 security type or not	Passed	
EWLCJ178S_Reg_480	Associating client with WPA3 + AES cipher + SAE AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + AES cipher + SAE AKM security type or not	Passed	
EWLCJ178S_Reg_481	Associating client with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type or not	Passed	
EWLCJ178S_Reg_482	Associating client with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type or not	Passed	
EWLCJ178S_Reg_483	Associating client with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type or not	Passed	
EWLCJ178S_Reg_484	Associating client with WPA3 + adaptive WPA2 security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + adaptive WPA2 security type or not	Passed	

EWLCJ178S_Reg_485	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWLCJ178S_Reg_486	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWLCJ178S_Reg_487	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWLCJ178S_Reg_488	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	
EWLCJ178S_Reg_489	Validate 2.4 GHz radio policy details in DNAC	To verify 2.4 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ178S_Reg_490	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ178S_Reg_491	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ178S_Reg_492	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWLCJ178S_Reg_493	Limit the client by radio policy	To verify the no of client associate with particular radio policy	Passed	
EWCJ178S_Reg_340	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWCJ178S_Reg_341	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWCJ178S_Reg_342	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	

EWCJ178S_Reg_343	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWCJ178S_Reg_344	Associating windows client to 9115 Ap with WPA2 security type for 2.4GHz radio policy	To Verify Windows client associate to 2.4 GHz radio with WPA2 security type or not	Passed	
EWCJ178S_Reg_345	Associating Android client to 9120 Ap with WPA2 security type for 5GHz radio policy	To Verify android client associate to 5 GHz radio with WPA2 security type or not	Passed	
EWCJ178S_Reg_346	Associating iOS client to 9130 Ap with WPA2 security type for 6GHz radio policy	To Verify iOS client associate to 6 GHz radio with WPA2 security type or not	Passed	
EWCJ178S_Reg_347	Associating Mac client to 9105 Ap with WPA3 security type for 2.4GHz radio policy	To Verify mac client associate to 2.4 GHz radio with WPA3 security type or not	Passed	
EWCJ178S_Reg_348	Associating Ms-go client to 9115 Ap with WPA3 security type for 5GHz radio policy	To associate the client and verifying EDCA parameter	Passed	
EWCJ178S_Reg_349	Associating MS-GO2 client to 9120 Ap with WPA3 + AES cipher + OWE AKM security type for 6GHz radio policy	To Verify MS-GO2 client associate to 6 GHz radio with WPA3 + AES cipher + OWE AKM security type or not	Passed	
EWCJ178S_Reg_350	Associating client with WPA3 + AES cipher + 802.1x-SHA256 AKM security type for 6GHz radio policy	To Verify Windows client associate to 6 GHz radio with WPA3 security type or not	Passed	

EWCJ178S_Reg_351	Associating client with WPA3 + AES cipher + SAE AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + AES cipher + SAE AKM security type or not	Passed	
EWCJ178S_Reg_352	Associating client with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + CCMP256 cipher + SUITEB192-1X AKM security type or not	Passed	
EWCJ178S_Reg_353	Associating client with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP256 cipher + SUITEB-1X AKM security type or not	Passed	
EWCJ178S_Reg_354	Associating client with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + GCMP128 cipher + SUITEB192-1X AKM security type or not	Passed	
EWCJ178S_Reg_355	Associating client with WPA3 + adaptive WPA2 security type for 6GHz radio policy	To Verify client associate to 6 GHz radio with WPA3 + adaptive WPA2 security type or not	Passed	
EWCJ178S_Reg_356	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWCJ178S_Reg_357	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWCJ178S_Reg_358	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWCJ178S_Reg_359	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	

EWCJ178S_Reg_360	Validate 2.4 GHz radio policy details in DNAC	To verify 2.4 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ178S_Reg_361	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ178S_Reg_362	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ178S_Reg_363	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWCJ178S_Reg_364	Limit the client by radio policy	To verify the no of client associate with particular radio policy	Passed	

SUDI 2099 certificate support on 9800

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_494	Enabling SUDI99 CA III Certificate of eWLC 9800-40 using CLI	To enable SUDI99 CA III certificate in eWLC 9800-40 and check if the SUDI certificate	Passed	
EWLCJ178S_Reg_495	Enabling SUDI99 CA III Certificate of eWLC 9800-80 using CLI	To enable SUDI99 CA III certificate in eWLC 9800-80 and check if the SUDI certificate	Passed	
EWLCJ178S_Reg_496	Enabling SUDI99 CA III Certificate of eWLC 9800-L using CLI	To enable SUDI99 CA III certificate in eWLC 9800-L and check if the SUDI certificate	Passed	
EWLCJ178S_Reg_497	Enabling SUDI99 CA III Certificate of eWLC 9800-CL using CLI	To enable SUDI99 CA III certificate in eWLC 9800-CL and check if the SUDI certificate	Passed	
EWLCJ178S_Reg_498	Enabling SUDI99 CA III Certificate of eWLC 9800-40 using UI	To validate if SUDI99 CA III certificate in eWLC 9800-40 is enabled through UI	Passed	
EWLCJ178S_Reg_499	Enabling SUDI99 CA III Certificate of eWLC 9800-80 using UI	To validate if SUDI99 CA III certificate in eWLC 9800-80 is enabled through UI	Passed	
EWLCJ178S_Reg_500	Enabling SUDI99 CA III Certificate of eWLC 9800-L using UI	To validate if SUDI99 CA III certificate in eWLC 9800-L is enabled through UI	Passed	
EWLCJ178S_Reg_501	Enabling SUDI99 CA III Certificate of eWLC 9800-CL using UI	To validate if SUDI99 CA III certificate in eWLC 9800-CL is enabled through UI	Passed	

EWLCJ178S_Reg_502	Disabling the SUDI 99 CA III certificate and checking the same in UI and CLI	To disable the SUDI 99 certificate in eWLC and check if the SUDI 99 CA III is disabled or not	Passed	
EWLCJ178S_Reg_503	Configuring SUDI99 CA III Certificate of eWLC with HA configured	To enable SUDI 99 CA III for the certificate for eWLC which is configured with HA	Passed	
EWLCJ178S_Reg_504	Validating if the eWLC 9800-40 has the CMCA3 certificate in SNI packet of TLS	To check if the eWLC 9800-40 has the CMCA3 certificate in SNI packet of TLS	Passed	
EWLCJ178S_Reg_505	Validating if the eWLC 9800-80 has the CMCA3 certificate in SNI packet of TLS	To check if the eWLC 9800-80 has the CMCA3 certificate in SNI packet of TLS	Passed	
EWLCJ178S_Reg_506	Validating if the eWLC 9800-L has the CMCA3 certificate in SNI packet of TLS	To check if the eWLC 9800-L has the CMCA3 certificate in SNI packet of TLS	Passed	
EWLCJ178S_Reg_507	Validating if the eWLC 9800-CL has the CMCA3 certificate in SNI packet of TLS	To check if the eWLC 9800-CL has the CMCA3 certificate in SNI packet of TLS	Passed	
EWLCJ178S_Reg_508	Check the SNI packet for the 9115 AP to validate RSA SUDI	To check the SNI packet for the 9115 AP to validate RSA SUDI by validating the client hello certificate Request .	Passed	
EWLCJ178S_Reg_509	Check the SNI packet for the 9105 AP to validate RSA SUDI	To check the SNI packet for the 9105 AP to validate RSA SUDI by validating the client hello certificate Request .	Passed	

EWLCJ178S_Reg_510	Check the SNI packet for the 9120 AP to validate RSA SUDI	To check the SNI packet for the 9120 AP to validate RSA SUDI by validating the client hello certificate Request .	Passed	
EWLCJ178S_Reg_511	Check the SNI packet for the 9130 AP to validate RSA SUDI	To check the SNI packet for the 9130 AP to validate RSA SUDI by validating the client hello certificate Request .	Passed	
EWLCJ178S_Reg_512	Disabling the SUDI 99 CA III certificate and checking the same in AP	To disable the SUDI 99 CA III certificate and checking the same in AP certificate Request	Passed	

Open RRM

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_606	Configure rrm and enable connectivity to kairos cloud	To configure rrm and enable connectivity to kairos cloud	Passed	
EWLCJ178S_Reg_607	Configure rrm and test for 5ghz band	To configure rrm and for 5ghz band	Passed	
EWLCJ178S_Reg_608	Configure rrm and test for 2.4ghz band	To configure rrm and test for 2.4ghz band	Passed	
EWLCJ178S_Reg_609	Configure rrm with WPA3 security	To configure rrm with WPA3 security	Passed	
EWLCJ178S_Reg_610	Configure rrm with WPA2 security	To configure rrm with WPA2 security	Passed	
EWLCJ178S_Reg_611	Configure rrm and test with android client	To configure rrm and test with android client	Passed	
EWLCJ178S_Reg_612	Configure rrm and test with iPhone client	To configure rrm and test with iPhone client	Passed	
EWLCJ178S_Reg_613	Configure rrm and test with Mac client	To configure rrm and test with Mac client	Passed	
EWLCJ178S_Reg_614	Configure rrm and test with Surface client	To configure rrm and test with Surface client	Passed	
EWLCJ178S_Reg_615	Configure rrm and test with Windows client	To configure rrm and test with Windows client	Passed	
EWLCJ178S_Reg_616	Configure rrm and test with only FRA enabled	To configure rrm and test with only FRA enabled	Passed	
EWLCJ178S_Reg_617	Configure rrm and test with only DCA enabled	To configure rrm and test with only DCA enabled	Passed	
EWLCJ178S_Reg_618	Configure rrm and test with only TPC enabled	To configure rrm and test with only TPC enabled	Passed	

EWLCJ178S_Reg_619	Configure rrm and test with only DBS enabled	To configure rrm and test with only DBS enabled	Passed	
EWLCJ178S_Reg_620	Configure rrm and test with different RF algorithm combinations	To configure rrm and test with different RF algorithm combinations	Passed	
EWLCJ178S_Reg_621	Configure rrm and test with manually assigned channel bandwidth and channel nos	To configure rrm and test with manually assigned channel bandwidth and channel nos	Passed	
EWLCJ178S_Reg_622	Configure rrm and test with 9115, 9120, 9130 AP	To configure rrm and test with 9115, 9120, 9130 AP	Passed	
EWLCJ178S_Reg_623	Configure rrm and test with 4800 AP	To configure rrm and test with 4800 AP	Passed	
EWLCJ178S_Reg_624	Configure rrm and test with eWLC HA	To configure rrm and test with eWLC HA	Passed	
EWLCJ178S_Reg_625	Configure rrm and test with EWC	To configure rrm and test with EWC	Passed	
EWCJ178S_Reg_365	Configure rrm and enable connectivity to kairos cloud	To configure rrm and enable connectivity to kairos cloud	Passed	
EWCJ178S_Reg_366	Configure rrm and test for 5ghz band	To configure rrm and for 5ghz band	Passed	
EWCJ178S_Reg_367	Configure rrm and test for 2.4ghz band	To configure rrm and test for 2.4ghz band	Passed	
EWCJ178S_Reg_368	Configure rrm with WPA3 security	To configure rrm with WPA3 security	Passed	
EWCJ178S_Reg_369	Configure rrm with WPA2 security	To configure rrm with WPA2 security	Passed	
EWCJ178S_Reg_370	Configure rrm and test with android client	To configure rrm and test with android client	Passed	
EWCJ178S_Reg_371	Configure rrm and test with iPhone client	To configure rrm and test with iPhone client	Passed	

EWCJ178S_Reg_372	Configure rrm and test with Mac client	To configure rrm and test with Mac client	Passed	
EWCJ178S_Reg_373	Configure rrm and test with Surface client	To configure rrm and test with Surface client	Passed	
EWCJ178S_Reg_374	Configure rrm and test with Windows client	To configure rrm and test with Windows client	Passed	
EWCJ178S_Reg_375	Configure rrm and test with only FRA enabled	To configure rrm and test with only FRA enabled	Passed	
EWCJ178S_Reg_376	Configure rrm and test with only DCA enabled	To configure rrm and test with only DCA enabled	Passed	
EWCJ178S_Reg_377	Configure rrm and test with only TPC enabled	To configure rrm and test with only TPC enabled	Passed	
EWCJ178S_Reg_378	Configure rrm and test with only DBS enabled	To configure rrm and test with only DBS enabled	Passed	
EWCJ178S_Reg_379	Configure rrm and test with different RF algorithm combinations	To configure rrm and test with different RF algorithm combinations	Passed	
EWCJ178S_Reg_380	Configure rrm and test with manually assigned channel bandwidth and channel nos	To configure rrm and test with manually assigned channel bandwidth and channel nos	Passed	
EWCJ178S_Reg_381	Configure rrm and test with 9115, 9120, 9130 AP	To configure rrm and test with 9115, 9120, 9130 AP	Passed	
EWCJ178S_Reg_382	Configure rrm and test with 4800 AP	To configure rrm and test with 4800 AP	Passed	
EWCJ178S_Reg_383	Configure rrm and test with eWLC HA	To configure rrm and test with eWLC HA	Passed	
EWCJ178S_Reg_384	Configure rrm and test with EWC	To configure rrm and test with EWC	Failed	CSCwb56923

Support 11k/v across wncd instances

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_513	Configure and verify 11v BSS Transition Management	To configure and verify 11v BSS Transition Management	Passed	
EWLCJ178S_Reg_514	Configure and verify 11v BSS Transition Management through CLI	To configure and verify 11v BSS Transition Management through CLI	Passed	
EWLCJ178S_Reg_515	Configure and verify 11k Beacon Radio Measurement	To configure and verify 11k Beacon Radio Measurement	Passed	
EWLCJ178S_Reg_516	Configure and verify 11k Beacon Radio Measurement through CLI	To configure and verify 11k Beacon Radio Measurement through CLI	Passed	
EWLCJ178S_Reg_517	Verify 802.11k Information Elements in Wireshark	To verify 802.11k Information Elements in Wireshark	Passed	
EWLCJ178S_Reg_518	Validate access points in ap upgrading stage are not included in the neighbour list	To validate access points in ap upgrading stage are not included in the neighbour list	Passed	
EWLCJ178S_Reg_519	Validate rf-profile admin state and rf-parameters is correctly showing or not after connecting 11kv client	To validate rf-profile admin state and rf-parameters is correctly showing or not after connecting 11kv client	Passed	
EWLCJ178S_Reg_520	Connect Windows Client and verify 11kv parameters in Wireshark	To connect Windows Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ178S_Reg_521	Connect Android Client and verify 11kv parameters in Wireshark	To connect Android Client and to verify 11kv parameters in Wireshark	Passed	

EWLCJ178S_Reg_522	Connect MAC Client and verify 11kv parameters in Wireshark	To connect MAC Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ178S_Reg_523	Connect IOS Client and verify 11kv parameters in Wireshark	To connect IOS Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ178S_Reg_524	Connect Go Plus Client and verify 11kv parameters in Wireshark	To connect Go Plus Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ178S_Reg_525	Validate BSSID neighbour enabled when other controller APs with having same ssid	To validate BSSID neighbour enabled when other controller APs with having same ssid	Passed	
EWLCJ178S_Reg_526	Validate 11kv neighbour list not included when AP admin state is brought down	To validate 11kv neighbour list not included when AP admin state is brought down	Passed	
EWLCJ178S_Reg_527	Validate 11kv neighbour list not included when radio admin state is brought down	To validate 11kv neighbour list not included when radio admin state is brought down	Passed	
EWLCJ178S_Reg_528	Verify 11kv neighbour list when one radio is disabled	To verify 11kv neighbour list when one radio is disabled	Passed	
EWLCJ178S_Reg_529	Verify 11kv elements in omni peek and check the frames	To verify 11kv elements in omni peek and check the frames	Passed	
EWLCJ178S_Reg_530	Verify 11kv frames in packet analyser when client is in sleeping status	To verify 11kv frames in packet analyser when client is in sleeping status	Passed	
EWCJ178S_Reg_385	Configuring 802.11v BSS Transition Management in GUI	To Verify Configured 802.11v BSS Transition Management in GUI	Passed	

EWCJ178S_Reg_386	Validate that ap_radio_data is properly updated with entries from AP's spread across WNCD instances.	To Validate that ap_radio_data is properly updated with entries from AP's spread across WNCD instances.	Passed	
EWCJ178S_Reg_387	Validate that ap_radio_data is properly updated with entries from AP's spread across WNCD instances.	To Validate that ap_radio_data is properly updated with entries from AP's spread across WNCD instances.	Passed	
EWCJ178S_Reg_388	Validate access points in ap upgrading stage are not included in the neighbour list.	To Validate access points in ap upgrading stage are not included in the neighbour list.	Passed	
EWCJ178S_Reg_389	Validate derivation of rf-profile admin state is correctly derived from rf-tag or not	To Validate derivation of rf-profile admin state is correctly derived from rf-tag or not	Passed	
EWCJ178S_Reg_390	Validate that when AP admin state is brought down it will not be included in 11k/v neighbour list.	To Validate that when AP admin state is brought down it will not be included in 11k/v neighbour list.	Passed	
EWCJ178S_Reg_391	Validate that when radio admin state is brought down it will not be included in 11k/v neighbour list	Validate that when radio admin state is brought down it will not be included in 11k/v neighbour list	Passed	
EWCJ178S_Reg_392	Validate that when particular rf-profile is brought down, Radio's on it will not be included in 11k/v neighbour list.	To Validate that when particular rf-profile is brought down, Radio's on it will not be included in 11k/v neighbour list.	Passed	
EWCJ178S_Reg_393	Connect Android Client and verify 11kv parameters in Wireshark	To connect Android Client and to verify 11kv parameters in Wireshark	Passed	

EWCJ178S_Reg_394	Connect MAC Client and verify 11kv parameters in Wireshark	To connect MAC Client and to verify 11kv parameters in Wireshark	Passed	
EWCJ178S_Reg_395	Connect IOS Client and verify 11kv parameters in Wireshark	To connect IOS Client and to verify 11kv parameters in Wireshark	Passed	
EWCJ178S_Reg_396	Connect Windows Client and verify 11kv parameters in Wireshark	To connect Windows Client and verify 11kv parameters in Wireshark	Passed	
EWCJ178S_Reg_397	Verify 11k/11v, with one wncd, the candidate list is proper.	To verify 11k/11v, with one wncd, the candidate list is proper.	Passed	
EWCJ178S_Reg_398	Verify 11k/11v, with multiple wncd, with neighbours across wncd' s. the candidate list is proper.	To Verify 11k/11v, with multiple wncd, with neighbours across wncd' s. the candidate list is proper.	Passed	
EWCJ178S_Reg_399	Validate that with BSSID neighbour enabled, Other controller access points with having same ssid enabled should be included in neighbour list.	To Validate that with BSSID neighbour enabled, Other controller access points with having same ssid enabled should be included in neighbour list.	Passed	

To share Client Delete reason code at AP to controller

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_531	Verify Client delete reason code for Webauth timer expiry when AP is in Local mode	LWA webauth timer expire	Passed	
EWLCJ178S_Reg_532	Verify Client delete reason code for Webauth timer expiry when AP is in Flex mode	LWA webauth timer expire	Passed	
EWLCJ178S_Reg_533	Verify Client delete reason code for Mac filtering	MAB authentication failed for Wireless client	Passed	
EWLCJ178S_Reg_534	Verify Client delete reason code for Mac filtering when AP is in Flex mode	MAB authentication failed for Wireless client	Passed	
EWLCJ178S_Reg_535	Verify Client delete reason code for Wrong PSK	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ178S_Reg_536	Verify Client delete reason code for Wrong PSK when AP is in Flex mode	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ178S_Reg_537	Verify Client delete reason code for dot1x timer expired	Deleting the client due to the expiry dot1x timer	Passed	
EWLCJ178S_Reg_538	Verify Client Manually Excluded with reason code	To verify Client Manually Excluded with reason code	Passed	
EWLCJ178S_Reg_539	Verify Client delete reason code for VLAN mismatch	To verify Client delete reason code for VLAN mismatch	Passed	
EWLCJ178S_Reg_540	Verify Android client delete reason code for dot1x authentication failure	Deleting the Android client due to the dot1x authentication failure	Passed	

EWLCJ178S_Reg_541	Verify Windows client delete reason code for dot1x authentication failure	Deleting the Windows client due to dot1x authentication failure	Passed	
EWLCJ178S_Reg_542	Verify IOS client delete reason code for dot1x authentication failure	Deleting the IOS client due to dot1x authentication failure	Passed	
EWLCJ178S_Reg_543	Verify Surface client delete reason code for dot1x authentication failure	Deleting the Surface client due to dot1x authentication failure	Failed	CSCwb49851
EWLCJ178S_Reg_544	Verify client delete reason code for dot1x authentication failure when AP is in Flex mode	Deleting the client due to dot1x authentication failure	Passed	
EWLCJ178S_Reg_545	Verify syslog when client connected with run state	To verify syslog when client connected with run state	Passed	
EWLCJ178S_Reg_546	Verify Client delete reason code for IP learn state	To verify Client delete reason code for IP learn state	Passed	
EWLCJ178S_Reg_547	Checking the client delete reason when Client using wrong bssid while associating	To check the client delete reason when client using wrong BSSID while associating	Passed	
EWLCJ178S_Reg_548	Configure Roaming between controllers and verify client delete reason	To configure Roaming between controllers and verify client delete reason	Passed	
EWLCJ178S_Reg_549	Verify Client delete reason CO_CLIENT_ DELETE_ REASON_MN_AP_FLEX_ FT_FAILURE due to FT roaming failure	To verify Client delete reason due to FT roaming failure	Passed	

EWLCJ178S_Reg_550	Using DNAC verify Client delete reason CO_CLIENT_DELETE_REASON_MN_AP_CLSM_WEBAUTH_TIMER_EXPIRED	Using DNAC, to verify Client delete reason CO_CLIENT_DELETE_REASON_MN_AP_CLSM_WEBAUTH_TIMER_EXPIRED	Passed	
EWLCJ178S_Reg_551	Verify Client delete reason CO_CLIENT_DELETE_REASON_MN_AP_IPLEARN_TIMEOUT	Client failed to get IP within this period	Passed	
EWLCJ178S_Reg_552	Verify Client delete reason code for Wired LAN	Deleting the clients connected to a port	Passed	
EWCJ178S_Reg_409	Validate the client delete reason after changing AP mode	To validate the client delete reason after changing AP mode	Passed	
EWCJ178S_Reg_410	Checking the client delete reason when Client is disconnected in run State	To verify the client delete reason when client is disconnected in run state	Passed	
EWCJ178S_Reg_411	Checking the client delete reason when Client using wrong bssid while associating	To check the client delete reason when client using wrong BSSID while associating	Passed	
EWCJ178S_Reg_412	Checking the client delete reason after expire the webauth timer	To validate the client delete reason after expire the webauth timer	Passed	
EWCJ178S_Reg_413	Checking the client delete reason when AP moves from standalone mode to connected mode	To validate the client delete reason when AP moves from standalone mode to connected mode	Passed	
EWCJ178S_Reg_414	Validate the client delete reason after MAB authentication failed	To validate the client delete reason after MAB authentication failed	Passed	

EWCJ178S_Reg_415	Checking the client delete reason after expire dot1x timer	To check the client delete reason after expire dot1x timer	Passed	
EWCJ178S_Reg_416	Validate the client delete reason after client failed to get IP	To validate the client delete reason after client failed to get IP	Passed	
EWCJ178S_Reg_417	Verifying the Android client delete reason after eap timer expires	To validate the Android client delete reason after eap timer expires	Passed	
EWCJ178S_Reg_418	Verifying the Windows client delete reason after eap timer expires	To validate the windows client delete reason after eap timer expires	Passed	
EWCJ178S_Reg_419	Validating the client delete reason when Authentication response rejected	To verify the client delete reason when Authentication response rejected	Passed	
EWCJ178S_Reg_420	Validating the client delete reason when Failing to send the Association response message to the wireless client	To validate the client delete reason when Failing to send the Association response message to the wireless client	Passed	
EWCJ178S_Reg_421	Checking the client delete reason when Deleting client due to de-authentication	To Check the client delete reason when Deleting client due to de-authentication	Passed	
EWCJ178S_Reg_422	Verifying the Samsung S10 client delete reason after eap timer expires	To validate the Samsung S10 client delete reason after eap timer expires	Passed	
EWCJ178S_Reg_423	Verifying the iPhone client delete reason after eap timer expires	To validate the iPhone client delete reason after eap timer expires	Passed	
EWCJ178S_Reg_424	Verifying the Surface Go client delete reason after eap timer expires	To validate the Surface Go client delete reason after eap timer expires	Passed	

EWCJ178S_Reg_425	Verifying the IOS client delete reason after eap timer expires	To validate the IOS client delete reason after eap timer expires	Passed	
EWCJ178S_Reg_426	Verifying the Client delete reason due to FT roaming failure	To verify the Client delete reason due to FT roaming failure	Passed	
EWCJ178S_Reg_427	Verify alert triggered in Alarms & Events in PI	To verify alert triggered in Alarms & Events in PI	Passed	
EWCJ178S_Reg_428	Verify alert triggered for Webauth failure in Alarms & Events Prime Infra	To verify alert triggered for Webauth failure in Alarms & Events Prime Infra	Passed	

Usability CLI Enhancement request

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_626	Configure eWLC with AP and verify CLI output	To configure eWLC with AP and verify CLI output	Passed	
EWLCJ178S_Reg_627	Configure eWLC with AP and verify CLI output for 2.4Ghz	To configure eWLC with AP and verify CLI output for 2.4Ghz	Passed	
EWLCJ178S_Reg_628	Configure eWLC with AP and verify CLI output for 5Ghz	To configure eWLC with AP and verify CLI output for 5Ghz	Passed	
EWLCJ178S_Reg_629	Configure eWLC with AP and verify CLI output for 6Ghz	To configure eWLC with AP and verify CLI output for 6Ghz	Passed	
EWLCJ178S_Reg_630	Verify if neighbour summary details are shown in descending order of RSSI value	To verify if neighbour summary details are shown in descending order of RSSI value	Passed	
EWLCJ178S_Reg_631	Verify CLI command output details in 9800L	To verify CLI command output details in 9800L	Passed	
EWLCJ178S_Reg_632	Verify CLI command output details in 9800CL	To verify CLI command output details in 9800CL	Passed	
EWLCJ178S_Reg_633	Verify CLI command output details in 9800-40/80	To verify CLI command output details in 9800-40/80	Passed	
EWLCJ178S_Reg_634	Verify CLI command output details in 9800 HA platform	To verify CLI command output details in 9800 HA platform	Passed	
EWLCJ178S_Reg_635	Verify CLI command output details in EWC device	To verify CLI command output details in EWC device	Passed	
EWLCJ178S_Reg_636	Verify CLI command output details in EWC HA device	To verify CLI command output details in EWC HA device	Passed	

EWLCJ178S_Reg_637	Verify CLI command output with more than 5 AP's joined	To verify CLI command output with more than 5 AP's joined	Passed	
EWLCJ178S_Reg_638	Disable 5Ghz network and check the CLI output	To disable 5Ghz network and check the CLI output	Passed	
EWLCJ178S_Reg_639	Disable 6Ghz network and check the CLI output	To disable 6Ghz network and check the CLI output	Passed	
EWLCJ178S_Reg_640	Disable 2.4Ghz network and check the CLI output	To disable 2.4Ghz network and check the CLI output	Passed	

WebGui Client 360 View should display additional client information

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_675	Connect Windows Client and check all the Information in Client 360	To connect Windows Client and to check all the Information in Client 360	Passed	
EWLCJ178S_Reg_676	Connect Android Client and check all the Information in Client 360	To connect Android Client and to check all the Information in Client 360	Passed	
EWLCJ178S_Reg_677	Connect IOS Client and check all the Information in Client 360	To connect IOS Client and to check all the Information in Client 360	Passed	
EWLCJ178S_Reg_678	Connect Surface Client and check all the Information in Client 360	To connect Surface Client and to check all the Information in Client 360	Passed	
EWLCJ178S_Reg_679	Connect MAC Client and check all the Information in Client 360	To connect MAC Client and to check all the Information in Client 360	Passed	
EWLCJ178S_Reg_680	Disconnect the Client intermittently and verify the status in Onboarding and Issues tab	To disconnect the Client intermittently and verify the status in Onboarding and Issues tab	Passed	
EWLCJ178S_Reg_681	Connect Wired Client and check all the information in Client 360	To connect Wired Client and check all the information in Client 360	Passed	
EWLCJ178S_Reg_682	Verify client status in Client 360 page when clients gets connected to 9105 AP	To verify client status in Client 360 page when clients gets connected to 9105 AP	Passed	

EWLCJ178S_Reg_683	Verify client status in Client 360 page when clients gets connected to 9115 AP	To verify client status in Client 360 page when clients gets connected to 9115 AP	Passed	
EWLCJ178S_Reg_684	Verify client status in Client 360 page when clients gets connected to 9120 AP	To verify client status in Client 360 page when clients gets connected to 9120 AP	Passed	
EWLCJ178S_Reg_685	Verify client status in Client 360 page when clients gets connected to 9130 AP	To verify client status in Client 360 page when clients gets connected to 9130 AP	Passed	
EWLCJ178S_Reg_686	Roam the client between controllers and check the status in Client 360 page	to roam the client between controllers and check the status in Client 360 page	Passed	
EWLCJ178S_Reg_687	Roam the client between APs and check the status in Client 360 page	To roam the client between APs and check the status in Client 360 page	Passed	
EWLCJ178S_Reg_688	Verify client deletion status in Client 360 page	To verify client deletion status in Client 360 page	Passed	
EWLCJ178S_Reg_689	Verify Hostname in client 360 page	To validate hostname information	Passed	
EWLCJ178S_Reg_690	Verify Connection Speed in client 360 page	To validate Connection Speed information	Passed	
EWLCJ178S_Reg_691	Verify Signal Quality (SNR) in client 360 page	To validate SNR information	Passed	
EWLCJ178S_Reg_692	Verify Signal Strength in client 360 page	To validate Signal Strength information	Passed	
EWLCJ178S_Reg_693	Verify Usage (Volume) in client 360 page	To validate Usage (Volume) information	Passed	
EWLCJ178S_Reg_694	Verify Uptime in client 360 page	To validate Uptime information	Passed	

EWLCJ178S_Reg_695	Verify DUID information in client 360 page	To validate DUID information	Passed	
EWLCJ178S_Reg_696	Verify Frequency Band in client 360 page	To validate Frequency Band information	Passed	
EWLCJ178S_Reg_697	Verify WLAN Profile in client 360 page	To validate WLAN Profile information	Passed	
EWLCJ178S_Reg_698	Verify AP MAC in client 360 page	To validate AP MAC information	Passed	
EWLCJ178S_Reg_699	Verify Tags - Site, Policy, RF in client 360 page	To validate Tags - Site, Policy, RF information	Passed	
EWLCJ178S_Reg_700	Verify Channel Width in client 360 page	To validate Channel Width information	Passed	
EWCJ178S_Reg_77	Connect Windows Client and check all the Information in Client 360	To connect Windows Client and to check all the Information in Client 360	Passed	
EWCJ178S_Reg_78	Connect Android Client and check all the Information in Client 360	To connect Android Client and to check all the Information in Client 360	Passed	
EWCJ178S_Reg_79	Connect IOS Client and check all the Information in Client 360	To connect IOS Client and to check all the Information in Client 360	Passed	
EWCJ178S_Reg_80	Connect Surface Client and check all the Information in Client 360	To connect Surface Client and to check all the Information in Client 360	Passed	
EWCJ178S_Reg_81	Connect MAC Client and check all the Information in Client 360	To connect MAC Client and to check all the Information in Client 360	Passed	
EWCJ178S_Reg_82	Disconnect the Client intermittently and verify the status in Onboarding and Issues tab	To disconnect the Client intermittently and verify the status in Onboarding and Issues tab	Passed	

EWCJ178S_Reg_83	Connect Wired Client and check all the information in Client 360	To connect Wired Client and check all the information in Client 360	Passed	
EWCJ178S_Reg_84	Verify client status in Client 360 page when clients gets connected to 9105 AP	To verify client status in Client 360 page when clients gets connected to 9105 AP	Passed	
EWCJ178S_Reg_85	Verify client status in Client 360 page when clients gets connected to 9115 AP	To verify client status in Client 360 page when clients gets connected to 9115 AP	Passed	
EWCJ178S_Reg_86	Verify client status in Client 360 page when clients gets connected to 9120 AP	To verify client status in Client 360 page when clients gets connected to 9120 AP	Passed	
EWCJ178S_Reg_87	Verify client status in Client 360 page when clients gets connected to 9130 AP	To verify client status in Client 360 page when clients gets connected to 9130 AP	Passed	
EWCJ178S_Reg_88	Roam the client between controllers and check the status in Client 360 page	to roam the client between controllers and check the status in Client 360 page	Passed	
EWCJ178S_Reg_89	Roam the client between APs and check the status in Client 360 page	To roam the client between APs and check the status in Client 360 page	Passed	
EWCJ178S_Reg_90	Verify client deletion status in Client 360 page	To verify client deletion status in Client 360 page	Passed	
EWCJ178S_Reg_91	Verify Hostname in client 360 page	To validate hostaname information	Passed	
EWCJ178S_Reg_92	Verify Connection Speed in client 360 page	To validate Connection Speed information	Passed	
EWCJ178S_Reg_93	Verify Signal Quality (SNR) in client 360 page	To validate SNR information	Passed	

EWCJ178S_Reg_94	Verify Signal Strength in client 360 page	To validate Signal Strength information	Passed	
EWCJ178S_Reg_95	Verify Usage (Volume) in client 360 page	To validate Usage (Volume) information	Passed	
EWCJ178S_Reg_96	Verify Uptime in client 360 page	To validate Uptime information	Passed	
EWCJ178S_Reg_97	Verify DUID information in client 360 page	To validate DUID information	Passed	
EWCJ178S_Reg_98	Verify Frequency Band in client 360 page	To validate Frequency Band information	Passed	
EWCJ178S_Reg_99	Verify WLAN Profile in client 360 page	To validate WLAN Profile information	Passed	
EWCJ178S_Reg_100	Verify AP MAC in client 360 page	To validate AP MAC information	Passed	
EWCJ178S_Reg_101	Verify Tags - Site, Policy, RF in client 360 page	To validate Tags - Site, Policy, RF information	Passed	
EWCJ178S_Reg_102	Verify Channel Width in client 360 page	To validate Channel Width information	Passed	

WebUI: WLAN/AAA/ACL Simplication

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_Reg_553	Connecting Android client to 9105 AP with Local mode PSK.	To verify whether the android client connect to 9105 AP with local mode PSK or not	Passed	
EWLCJ178S_Reg_554	Connecting Windows client to 9115 AP with Local mode Dot1x	To verify whether the windows client connect to 9115 AP with local mode Dot1x or not	Passed	
EWLCJ178S_Reg_555	Configuring Dot1x Security & checking the Authentication list via CLI	To configure Dot1x Security & validate the Authentication list via CLI	Failed	CSCwa83403
EWLCJ178S_Reg_556	Connecting mac client to 9130 AP with Local mode LWA	To verify Whether the MAC client to 9130 Ap with local mode LWA	Passed	
EWLCJ178S_Reg_557	Validating AAA parameters in Local mode LWA	To Validate the AAA parameters in Local mode LWA	Passed	
EWLCJ178S_Reg_558	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Passed	
EWLCJ178S_Reg_559	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWLCJ178S_Reg_560	Connect the windows client with local mode CWA	To check the windows client connectivity for local mode CWA	Failed	CSCwa83779
EWLCJ178S_Reg_561	Creating user group for Local mode CWA	To create User group for Local mode CWA	Passed	
EWLCJ178S_Reg_562	Checking the client connectivity for flex connect LWA	To check whether the client connected with flex connect LWA or not	Passed	

EWLCJ178S_Reg_563	Validate the client connectivity for flex connect EWA	To validate whether the client connected with flex connect EWA or not	Passed	
EWLCJ178S_Reg_564	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Failed	CSCwb37258
EWLCJ178S_Reg_565	Monitor the client connectivity for flex connect CWA	To monitor whether the client connect with flex connect CWA or not	Passed	
EWLCJ178S_Reg_566	Checking the client connectivity for Guest Foreign CWA	To check the client connectivity for Guest foreign CWA	Passed	
EWLCJ178S_Reg_567	validating radius server details in Guest foreign CWA	To validate the radius server details	Passed	
EWLCJ178S_Reg_568	Monitor the client connectivity for Guest CWA Anchor	To monitor whether the client connect with Guest CWA anchor or not	Passed	

C9105 EWC AP Support

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_30	Association of 9105 AP with different eWLC model	To associate 9105 AP to eWLC with latest image and check if the AP gets associated or not	Failed	CSCwb56577
EWCJ178S_Reg_31	Associating 9105 AP with different country code as with eWLC	To associate 9105 AP with different country code and check if the AP does not get joined to eWLC	Passed	
EWCJ178S_Reg_32	Configuring AP with duplicate IP	To configure AP with a duplicate IP address and check if the AP shows error message and AP does not join the eWLC	Passed	
EWCJ178S_Reg_33	Rebooting the 9105 AP	To check if the AP gets Rebooted or not and check if the AP joins the controller again.	Passed	
EWCJ178S_Reg_34	Rebooting the AP with primary controller given in High Availability	To reboot the AP by giving the primary controller IP using high availability and check if the AP joins the primary controller	Passed	
EWCJ178S_Reg_35	Checking the details of the AP through the CLI	To check the details of the AP using CLI and check if the details are correctly shown or not	Passed	
EWCJ178S_Reg_36	Connecting a Window client to the 9105 AP	To connect a window client to the AP and check if the client gets connected to the AP without any errors.	Passed	

EWCJ178S_Reg_37	Connecting a Android client to the 9105 AP	To connect a Android client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_Reg_38	Connecting a IOS client to the 9105 AP	To connect a IOS client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_Reg_39	Connecting a MAC client to the 9105 AP	To connect a MAC client to the AP and check if the client gets connected to the AP without any errors.	Passed	
EWCJ178S_Reg_40	AP failover priority with critical	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWCJ178S_Reg_41	AP failover priority with High priority	To check AP failover priority with critical and check if the AP gets connected to the next controller .	Passed	
EWCJ178S_Reg_42	Moving AP from 9800-40 eWLC to 9800-80 through High availability	To check if the AP moves from 9800-40 eWLC to 9800-80 eWLC through high availability.	Passed	
EWCJ178S_Reg_43	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	
EWCJ178S_Reg_44	Checking if the client do not connect to the AP after rebooting and joining the primary controller	To check if the client gets connected to the AP after rebooting the AP and AP joining the primary controller .where there is no same WLAN	Passed	

EWCJ178S_Reg_45	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
EWCJ178S_Reg_46	Performing Intra controller roaming of IOS client	To check whether intra controller roaming of IOS clients works properly or not in eWLC	Passed	
EWCJ178S_Reg_47	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
EWCJ178S_Reg_48	Performing Inter controller roaming of Windows OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
EWCJ178S_Reg_49	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWCJ178S_Reg_50	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
EWCJ178S_Reg_51	Performing Inter controller roaming of Mac OS client	To check whether inter controller roaming of Mac OS clients works properly or not	Passed	
EWCJ178S_Reg_52	Change AP mode from local to Flex connect in 9105 AP.	To change the mode of AP from local mode to Flex connect mode and check if the AP does not reboot.	Passed	
EWCJ178S_Reg_53	Changing the AP from Flex connect to Local mode and check if the AP reboot	To check if the AP reboots when AP mode is changed from flex connect to Local mode .	Passed	

EWCJ178S_Reg_54	Adding two 9105 AP in the AP group and connecting a client to the AP with specific WLAN	To add two 9105 AP in AP group and map a WLAN to group and connect a client to the WLAN and check the client connectivity	Passed	
EWCJ178S_Reg_55	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	
EWCJ178S_Reg_56	Packet capture of client when the client is connected to 9115/9120 AP with 2.4 GHz	To capture the Packet of the client when the client is connected to AP with radio as 2.4GHz	Passed	
EWCJ178S_Reg_57	Verify details by connecting client to 2.4Ghz radio of 9105 AP.	To verify OFDMA details by connecting client to 2.4 Ghz radio.	Passed	
EWCJ178S_Reg_58	Verify details by connecting client to 5 Ghz radio of 9105 AP	To verify OFDMA details by connecting client to 5 Ghz radio.	Passed	
EWCJ178S_Reg_59	Verify 9105AP MU-MIMO details with client connecting to WPA2 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA2 configured WLAN	Passed	
EWCJ178S_Reg_60	Verify 9105AP MU-MIMO details with client connecting to WPA 3 configured WLAN	To verify 11ax MU-MIMO details of 9105 AP with client connecting to WPA 3 configured WLAN	Passed	

Ethernet VLAN tag on AP

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_124	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	
EWCJ178S_Reg_125	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	
EWCJ178S_Reg_126	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	
EWCJ178S_Reg_127	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	
EWCJ178S_Reg_128	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	
EWCJ178S_Reg_129	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	
EWCJ178S_Reg_130	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	
EWCJ178S_Reg_131	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	

EWCJ178S_Reg_132	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	
EWCJ178S_Reg_133	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	
EWCJ178S_Reg_134	Checking the VLAN Tag after DCA Mode change	To check the VLAN tag after changing DCA mode	Passed	
EWCJ178S_Reg_135	Checking the VLAN Tag after changing Radio band	To check the VLAN tag after changing radio band	Passed	
EWCJ178S_Reg_136	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	
EWCJ178S_Reg_137	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	
EWCJ178S_Reg_138	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.	Passed	

EWCJ178S_Reg_139	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.	Passed	
EWCJ178S_Reg_140	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	
EWCJ178S_Reg_141	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	
EWCJ178S_Reg_142	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	
EWCJ178S_Reg_143	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	
EWCJ178S_Reg_144	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	

EWC Day0 Elimination

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_145	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	
EWCJ178S_Reg_146	Manually adding single device Pnp details and Provisioning the 9115AX eWLC_ME in day0	Verify that user is able to Provisioned the eWLC_ME in day0 after adding Pnp Details manually	Passed	
EWCJ178S_Reg_147	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	
EWCJ178S_Reg_148	Checking the image version after Provisioning Ewlc_ME with PnP	Verifying the image version after Provisioning Ewlc_ME with PnP	Passed	
EWCJ178S_Reg_149	Checking the AP details after Provisioning Ewlc_ME with PnP	Verifying the AP details after Provisioning Ewlc_ME with PnP	Passed	
EWCJ178S_Reg_150	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Passed	
EWCJ178S_Reg_151	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	
EWCJ178S_Reg_152	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	

EWCJ178S_Reg_153	Configuring wrong details for PnP while claiming the device	To verify whether user is able to Provisioned the eWLC_ME with providing wrong PnP configuration in DNAC	Passed	
EWCJ178S_Reg_154	Checking the eWLC_ME after configuring factory reset with save config	Verifying whether user able to bring device to day0 or not with save config as yes	Passed	

Optimized Roaming

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_244	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	
EWCJ178S_Reg_245	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	
EWCJ178S_Reg_246	Configuring optimized roaming with 5 GHz band and roam Android client	To verify that optimized roaming with 5 GHz band and check association of Android client	Passed	
EWCJ178S_Reg_247	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	
EWCJ178S_Reg_248	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	

EWCJ178S_Reg_249	Configuring optimized roaming with 2.4 GHz band ,9 MBPS Threshold and roam iOS client	To verify that optimized roaming with 2.4 GHz band ,9 MBPS Threshold configured and check association of iOS client	Passed	
EWCJ178S_Reg_250	Configuring optimized roaming with 5 GHz band and roam iOS client	To verify that optimized roaming with 5 GHz band &customized interval(40 Sec) configured successfully and check association of iOS client	Passed	
EWCJ178S_Reg_251	Configuring optimized roaming with 5 GHz band , 12 MBPS Threshold and roam iOS client	To verify that optimized roaming with 5 GHz band , 12 MBPS Threshold configured successfully and check association of iOS client	Passed	
EWCJ178S_Reg_252	Moving the Android client from AP after enable optimized roaming	To verify that client got disassociated when signal is poor while moving from AP	Passed	
EWCJ178S_Reg_253	Moving the iOS client from AP after disabling the optimized roaming	To verify that client wouldn't disassociated when signal is poor while moving from AP	Passed	
EWCJ178S_Reg_254	Moving the Android client from AP after enable optimized roaming in ME with interference availability	To verify that client got disassociated when signal is poor while moving from 2700 AP with interference availability	Passed	
EWCJ178S_Reg_255	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	

EWCJ178S_Reg_256	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWCJ178S_Reg_257	Importing/exporting configuration file after optimized roaming configuring	To verify that optimization roaming configuration remain same after import and export configuration file	Passed	

Parallel Download

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_258	Verify parallel mode image download using TFTP in EWC 9130	To Verify parallel mode image download using TFTP in EWC 9130	Passed	
EWCJ178S_Reg_259	Verify parallel mode image download using SFTP in EWC 9130	To Verify parallel mode image download using SFTP in EWC 9130	Passed	
EWCJ178S_Reg_260	Verify parallel mode image download using TFTP in EWC HA setup	To Verify parallel mode image download using TFTP in EWC HA setup	Passed	
EWCJ178S_Reg_261	Verify parallel mode image download using SFTP in EWC HA setup	To Verify parallel mode image download using SFTP in EWC HA setup	Passed	
EWCJ178S_Reg_262	Verify parallel mode image download using TFTP in EWC 9120	To Verify parallel mode image download using TFTP in EWC 9120	Passed	
EWCJ178S_Reg_263	Verify parallel mode image download using SFTP in EWC 9120	To Verify parallel mode image download using SFTP in EWC 9120	Passed	
EWCJ178S_Reg_264	Verify parallel mode image download using TFTP in EWC 9115	To Verify parallel mode image download using TFTP in EWC 9115	Passed	
EWCJ178S_Reg_265	Verify parallel mode image download using SFTP in EWC 9115	To Verify parallel mode image download using SFTP in EWC 9115	Passed	
EWCJ178S_Reg_266	Verify parallel mode image download using TFTP in EWC 9105	To Verify parallel mode image download using TFTP in EWC 9105	Passed	

EWCJ178S_Reg_267	Verify parallel mode image download using SFTP in EWC 9105	To Verify parallel mode image download using SFTP in EWC 9105	Passed	
EWCJ178S_Reg_268	Cancel Image TFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWCJ178S_Reg_269	Cancel Image SFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWCJ178S_Reg_270	Upgrade using TFTP without parallel image support	To verify Upgrade using TFTP without parallel image support	Passed	
EWCJ178S_Reg_271	Upgrade using SFTP without parallel image support	To verify Upgrade using SFTP without parallel image support	Passed	
EWCJ178S_Reg_272	Verify Image upgrade using http method	To Verify Image upgrade using http method	Passed	

RRM assurance for granular reasons for power and channel change

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_311	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWCJ178S_Reg_312	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	
EWCJ178S_Reg_313	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	
EWCJ178S_Reg_314	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	
EWCJ178S_Reg_315	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	
EWCJ178S_Reg_316	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	
EWCJ178S_Reg_317	Channel updating and monitor assurance in DNAC	To perform channel updating and monitor assurance in DNAC	Passed	
EWCJ178S_Reg_318	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	
EWCJ178S_Reg_319	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	

EWCJ178S_Reg_320	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWCJ178S_Reg_321	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWCJ178S_Reg_322	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWCJ178S_Reg_323	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWCJ178S_Reg_324	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	
EWCJ178S_Reg_325	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWCJ178S_Reg_326	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWCJ178S_Reg_327	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	
EWCJ178S_Reg_328	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	

TACACS

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_Reg_400	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	Failed	CSCwb57380
EWCJ178S_Reg_401	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	
EWCJ178S_Reg_402	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	
EWCJ178S_Reg_403	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	
EWCJ178S_Reg_404	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	
EWCJ178S_Reg_405	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	

EWCJ178S_Reg_406	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	
EWCJ178S_Reg_407	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 "Command Line Interfaces and "Management" checkboxes.	Passed	
EWCJ178S_Reg_408	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	

SRCFD

Logical ID	Title	Description	Status	Defect ID
EWLCJ178S_SR_01	Configuring SNMP trap link Status on the eWLC 9800-80 Platform	To configure SNMP trap link status on eWLC 9800-80 Platform	Passed	
EWLCJ178S_SR_02	Configuring SNMP trap link Status on the eWLC 9800-L Platform	To configure SNMP trap link status on eWLC 9800-80 Platform	Passed	
EWLCJ178S_SR_03	Configuring SNMP trap link Status on the eWLC 9800-80 Platform with HA pair	To configure SNMP trap link status on eWLC 9800-80 Platform with HA pair and check the behaviour after the HA failover	Passed	
EWLCJ178S_SR_04	Configuring SNMP trap link Status on the eWLC 9800-L Platform with HA pair	To configure SNMP trap link status on eWLC 9800-L Platform with HA pair and check the behaviour after the HA failover	Passed	
EWLCJ178S_SR_05	Passing traffic to client through Catalyst 9105 AP continuously and check for any errors	To verify if the client traffic passes through catalyst 9105 AP and check if there is error or lag in the traffic	Passed	
EWLCJ178S_SR_06	Passing traffic to client through Catalyst 9120 AP continuously and check for any errors	To verify if the client traffic passes through catalyst 9120 AP and check if there is error or lag in the traffic	Passed	
EWLCJ178S_SR_07	Passing traffic to client through Catalyst 9130 AP continuously and check for any errors	To verify if the client traffic passes through catalyst 9130 AP and check if there is error or lag in the traffic	Passed	

EWLCJ178S_SR_08	Passing traffic to client through Catalyst 9115 AP continuously and check for any errors	To verify if the client traffic passes through catalyst 9115 AP and check if there is error or lag in the traffic	Passed	
EWLCJ178S_SR_09	Passing traffic to client through Catalyst 4800 AP continuously and check for any errors	To verify if the client traffic passes through catalyst 4800 AP and check if there is error or lag in the traffic	Passed	
EWLCJ178S_SR_10	Resetting The 9130 AXI APs	To resetting the 9130 AXI AP	Passed	
EWLCJ178S_SR_11	Change the Country Code in Ap	To change the country code available in AP	Passed	
EWLCJ178S_SR_12	mapping the policy tag and rf tags in AP	to map the policy tag and rf tags in AP configuration	Passed	
EWLCJ178S_SR_13	verify different chassis number in 9800-CL Controller	to verify different chassis number in 9800-CL Controller	Passed	
EWLCJ178S_SR_14	verify different chassis number in 9800 -L Controller	to verify different chassis number in 9800-L Controller	Passed	
EWLCJ178S_SR_15	verify different chassis number in 9800 -80 Controller	to verify different chassis number in 9800-80 Controller	Passed	
EWLCJ178S_SR_16	Check config stats in HA SSO RP on multiple power cycles	To check config stats in HA SSO RP on multiple power cycles	Passed	
EWLCJ178S_SR_17	Check config stats in HA SSO RMI on multiple power cycles	To check config stats in HA SSO RMI on multiple power cycles	Passed	
EWLCJ178S_SR_18	Check config stats in HA SSO on multiple switchover	To check config stats in HA SSO on multiple switchover	Passed	
EWLCJ178S_SR_19	Check the client connectivity with AP in flex local mode	To check the client connectivity with AP in flex local mode	Passed	

EWLCJ178S_SR_20	Check the android client connectivity with AP in flex local mode	To check the client connectivity with AP in flex local mode	Passed	
EWLCJ178S_SR_21	Check the MAC client connectivity with AP in flex local mode	To check the client connectivity with AP in flex local mode	Passed	
EWLCJ178S_SR_22	Check the client connectivity with AP in flex local mode and AP roaming to secondary controller	To check the client connectivity with AP in flex local mode and AP roaming to secondary controller	Passed	
EWLCJ178S_SR_23	Check AP info upon AP unplug & connect to switch	To check if AP joins eWLC automatically upon after initial connect & unplug with switch	Passed	
EWLCJ178S_SR_24	Check AP info upon AP unplug & connect to switch	To check if different models of AP join eWLC automatically upon after initial connect & unplug with switch	Passed	
EWLCJ178S_SR_25	Check AP info upon AP factory reset, unplug & connect to switch	To check if AP joins eWLC automatically upon after initial connect, factory reset & unplug with switch	Passed	
EWLCJ178S_SR_26	Check AP info upon AP unplug & connect to switch for catalyst 9100 AP's	To check if different models of AP join eWLC automatically upon after initial connect & unplug with switch	Passed	
EWLCJ178S_SR_27	Verify if hostapd process comes up during AP bootup	To verify if hostapd process comes up during AP bootup	Passed	
EWLCJ178S_SR_28	Check if the new user gets added via UI	To check if the new user gets added via UI	Passed	
EWLCJ178S_SR_29	Check if the new user gets added via CLI	To check if the new user gets added via CLI	Passed	

EWLCJ178S_SR_30	Verify enable/disable of BSS colouring on radio is reflected in management packets	To verify whether the BSS colour is reflected in Management packets or not	Passed	
EWLCJ178S_SR_31	Verifying OBSS PD with inter roaming client using different radio	To check whether OBSS PD is enable or not , when different radio clients are roaming between controllers	Passed	
EWLCJ178S_SR_32	Verifying OBSS PD enabled with inter roaming client using same radio	To check whether OBSS PD enable or not , when same radio clients are roaming between controllers	Passed	
EWLCJ178S_SR_33	Verify if client moves to run state using different models of AP	To verify if client moves to run state using different models of AP	Passed	
EWLCJ178S_SR_34	Configure FRA radio	To configure FRA radio	Passed	
EWLCJ178S_SR_35	Configuring the Dual Radio Mode and Enabling Slots	To configure the Dual Radio Mode and Enabling Slots	Passed	
EWLCJ178S_SR_36	Configure Default XOR Radio Support 9120 APs	To configure Default XOR Radio Support 9120 APs	Passed	
EWLCJ178S_SR_37	Configure XOR Radio Support for the Specified Slot Number	To configure XOR Radio Support for the Specified Slot Number	Failed	CSCwb26624
EWLCJ178S_SR_38	Join 9130 AP in 9800-L controller	To join 9130 AP in 9800-L controller	Passed	
EWLCJ178S_SR_39	Configure the 802.11 Performance Profile	To configure the 802.11 Performance Profile	Passed	
EWLCJ178S_SR_40	Configure Rogue Access Point Detection in RF Groups	To configure Rogue Access Point Detection in RF Groups	Passed	
EWLCJ178S_SR_41	Configure Time zone	To configure Time zone	Passed	

EWLCJ178S_SR_42	Modify AP Time zone using Controller	To modify AP Time zone using Controller	Passed	
EWLCJ178S_SR_43	Configure AP Group NTP Server in CMX and verify NTP status in Console	To configure AP Group NTP Server in CMX and verify NTP status in Console	Passed	
EWLCJ178S_SR_44	Add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	To add NTP IPv4/IPV6 address for AP profile through CLI and verify TLV logs	Passed	
EWLCJ178S_SR_45	Monitor any crashes generated or not after configuring real time statistics	To monitor crashes	Passed	
EWLCJ178S_SR_46	Monitor any crashes generated after configuring Static IP for an AP	To monitor any crashes generated after configuring Static IP for an AP	Passed	
EWLCJ178S_SR_47	Monitor any crashes generated after configuring Static IP for an 9100 Series AP	To monitor any crashes generated after configuring Static IP for an 9100 Series AP	Passed	
EWLCJ178S_SR_48	Upgrade the 9120 ap with latest image	Verify core file generated or not while ap reload	Passed	
EWLCJ178S_SR_49	Upgrade the 9130 ap with latest image	Verify core file generated or not while ap reload	Passed	
EWLCJ178S_SR_50	Upgrade the 9115 ap with latest image	Verify core file generated or not while ap reload	Passed	
EWLCJ178S_SR_51	Upgrade the 9105 ap with latest image	Verify core file generated or not while ap reload	Passed	
EWLCJ178S_SR_52	Reload the ap after Changing the radio 2.4 ghz	Verify 2.4 Ghz radio retained or not after reload	Passed	
EWLCJ178S_SR_53	Reload the ap after Changing the radio 5 ghz	Verify 5 Ghz radio retained or not after reload	Passed	

EWLCJ178S_SR_54	Reload the ap after Changing the radio 6 ghz	Verify 6 Ghz radio retained or not after reload	Passed	
EWLCJ178S_SR_55	Associate S10 mobile with 9120 AP and perform roaming	Verify client connected or not with 9120 ap	Passed	
EWLCJ178S_SR_56	Associate Sony mobile with 9130 AP and perform roaming	Verify client connected or not with 9130 ap	Passed	
EWLCJ178S_SR_57	Associate iOS client with 9115 AP and perform roaming	Verify client connected or not with 9115 ap	Passed	
EWLCJ178S_SR_58	Associate windows client with 9105 AP and perform roaming	Verify client connected or not with 9105 ap	Passed	
EWLCJ178S_SR_59	Perform HA switchover and observe memory leak	Verify checking channel utilization during client connectivity	Passed	
EWLCJ178S_SR_60	reload the ewlc for n times and check memory leak	Verify crash happened or not during continue reload	Passed	
EWLCJ178S_SR_61	connect Android client with dot1x security	Verify crash happened or not during client connectivity	Passed	
EWLCJ178S_SR_62	Perform roaming for n times and verify memory leak	Verify crash happened or not during roaming	Passed	
EWLCJ178S_SR_63	Perform channel change and verify client details	Verify client details shown or not	Passed	
EWLCJ178S_SR_64	Perform ap radio change and verify client details	Verify client details shown or not	Passed	

EWLCJ178S_SR_65	PSRT: DNA: Heatmaps not displayed for Some APs in the network hierarchy miss radio/assurance info while it is present on Device 360	To add network devices & check Heatmaps not displayed for APs	Passed	
EWLCJ178S_SR_66	checking Heatmaps of Some APs in the network hierarchy	To add network devices & check Heatmaps not displayed for APs	Passed	
EWLCJ178S_SR_67	checking detailed information Some APs in network hierarchy & on Device 360	To add network devices & check Heatmaps not displayed for APs	Passed	
EWLCJ178S_SR_68	Upgrading DNA-C To Latest BUILD to see APs in the network hierarchy for radio/assurance info & on Device 360	To add network devices & check Heatmaps not displayed for APs	Passed	
EWLCJ178S_SR_69	Verify if AP details is updated in the network hierarchy radio/assurance info & on Device 360	To add network devices & check Heatmaps not displayed for APs	Passed	
EWLCJ178S_SR_70	Some APs in the network hierarchy miss radio/assurance info while it is present on Device 360	To add network devices & check Heatmaps not displayed for APs	Passed	
EWLCJ178S_SR_71	C9800 WLC random crashes with no system report but generates DP ucode crash	To check boot loop of catalyst 9800 & hardware issue	Passed	
EWLCJ178S_SR_72	Upgrading C9800 WLC random crashes with no system report but generates DP ucode crash	To check boot loop of catalyst 9800 & hardware issue	Passed	

EWLCJ178S_SR_73	checking hardware issue of C9800 WLC for random crash	To check boot loop of catalyst 9800 & hardware issue	Passed	
EWLCJ178S_SR_74	C9800 WLC generates DP ucode after random crashes	To check boot loop of catalyst 9800 & hardware issue	Passed	
EWLCJ178S_SR_75	Cisco Catalyst 9130 AP flashes insufficient power LED when USB is enabled on PoE+ Switch	C9130 LED is blinking as blue, green and red	Passed	
EWLCJ178S_SR_76	Cisco Catalyst 9124 AP flashes insufficient power LED when USB is enabled on PoE+ Switch	C9130 LED is blinking as blue, green and red	Passed	
EWLCJ178S_SR_77	Upgrading & checking Cisco Catalyst AP, if it flashes insufficient power LED when USB is enabled on PoE+ Switch	C9130 LED is blinking as blue, green and red	Passed	
EWLCJ178S_SR_78	Cisco Catalyst 9136 AP flashes insufficient power LED when USB is enabled on PoE+ Switch	C9130 LED is blinking as blue, green and red	Passed	
EWLCJ178S_SR_79	Disabling USB & checking Cisco Catalyst AP if it, flashes insufficient power LED	C9130 LED is blinking as blue, green and red	Passed	
EWLCJ178S_SR_80	C9800 -L : Guest users are not getting expired in Prime Infrastructure after they expire in 9800 controller	to create guest user & Access permission over web authentication is still valid after delete a guest us	Passed	

EWLCJ178S_SR_81	9800-CL : Upgrade Prime Infrastructure after they expire in 9800- CL controller	to create guest user & Access permission over web authentication is still valid after delete a guest us	Passed	
EWLCJ178S_SR_82	Guest users are not getting expired in Prime Infrastructure after they expire in 9800-80 controller	to create guest user & Access permission over web authentication is still valid after delete a guest us	Passed	
EWLCJ178S_SR_83	checking Guest users in Prime Infrastructure after they expire in 9800 controller	to create guest user & Access permission over web authentication is still valid after delete a guest us	Passed	
EWLCJ178S_SR_84	Guest users are not getting expired in Prime Infrastructure after they expire in 9800 controller	to create guest user & Access permission over web authentication is still valid after delete a guest us	Passed	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
EWCJ178S_config_1	Able to create user account by using the username as " "	To verify the user account by using the username as special character	Failed	CSCwb56783
EWCJ178S_config_2	Local Policy Page - Add & Delete key Disable issue	To verify Local Policy Page - Add & Delete key Disable issue	Failed	CSCwb59252

Related Documents

Related Documentation

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.8 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.8 Release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/release-notes/rn-17-8-9800.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-march22.html

Cisco Catalyst 9600 Series Switches 17.7 Release Notes

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-7/release_notes/ol-17-7-9600.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/2-3-3/release_notes/b_cisco_dna_center_rn_2_3_3.html

PI 3.9 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-9/user/guide/bk_CiscoPrimeInfrastructure_3_9_0_UserGuide.html

ISE 3.1 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/release_notes/b_ise_31_RN.html