Test Results Summary for Catalyst 9800 Series Wireless Controller and EWC 17.9 for Japan (Release Version 17.9)

First Published: 2022-07-27

Last Modified: 2022-07-29

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 17.9
- 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

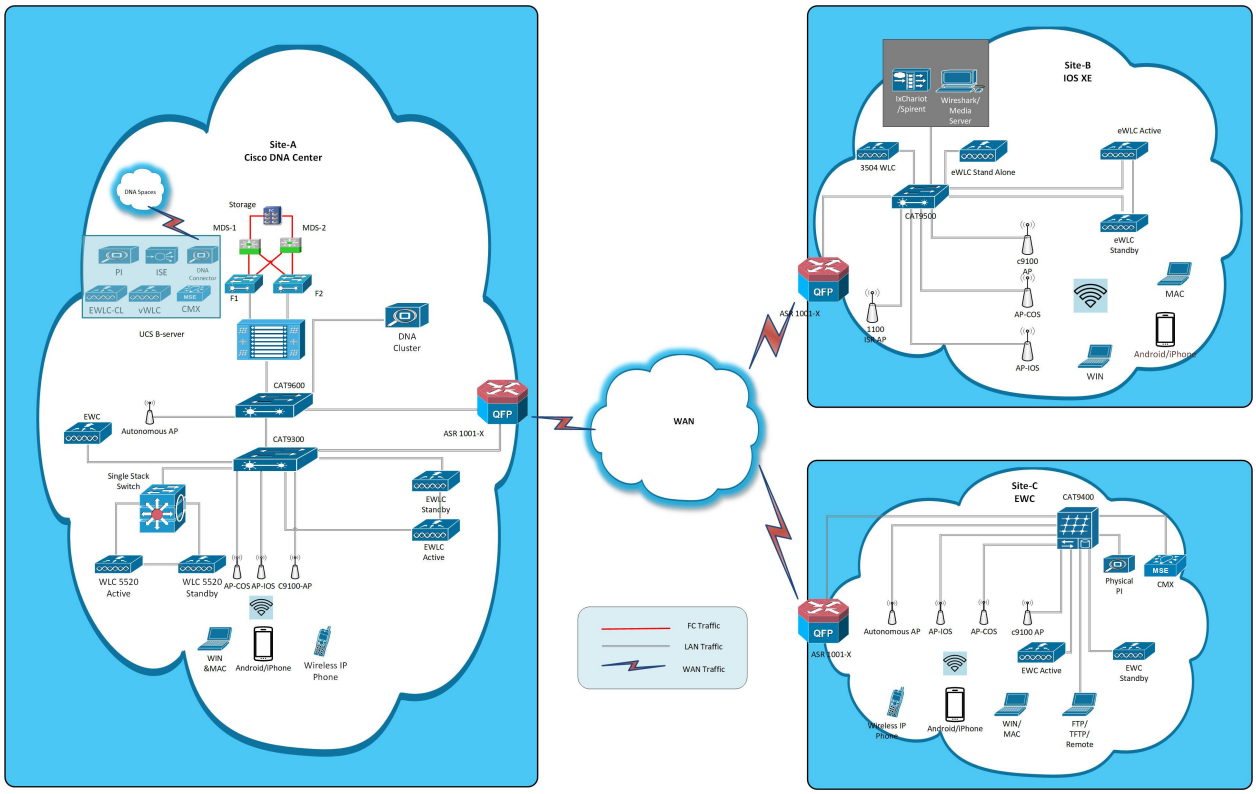
Acronym	Description
AP	Access Point
API	Application Programming Interface
APIC-EM	Application Policy Infrastructure Controller - Enterprise Module
ATF	Air-Time Fairness
AVC	Application Visibility and Control.
BGN	Bridge Group Network
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CA	Central Authentication
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	17.9
	Cisco Catalyst 9800-80 Wireless Controller	17.9
	Cisco Catalyst 9800-CL Wireless Controller for Cloud	17.9
	Cisco Catalyst 9800-L Wireless Controller	17.9
	Cisco Embedded Wireless Controller on Catalyst Access Points	17.9
	Virtual Controller	8.10.121.0
Applications	Cisco DNA Center	2.3.3
	Cisco DNA Spaces	Cloud (Jun 2022)
	Cisco DNA Spaces Connector	2.3.3
	Prime Infrastructure (Virtual Appliance, UCS based)	3.9.0.0
	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	17.9
	Cisco AP 9120	17.9
	Cisco AP 9130	17.9
	Cisco AP 9105	17.9
	Cisco 1100 ISR	17.9
	Cisco AP 4800	15.3
	Cisco AP 1810	15.3

Category	Component	Version
Switch	Cisco Cat 9300	17.9
	Cisco Cat 9200L	17.9
	Cisco Cat 9800	17.9
	Cisco 3750V2 switch	15.0(2)SE2
	Cisco Cat 6509-E	15.1(1)SY1
Chipset	5300, 6300 AGN	15.40.41.5058
	7265 AC	21.40.2
	Airport Extreme	7.9.1
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	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	106.0.5
	Safari	16.1
	Chrome	107.0.5304.107

What's New ?

Cisco Catalyst 9800 Series Wireless Controller

- Web GUI Client 360 View should display additional client information
- Critical KPIs on AP 360: Rogue AP view with channel width
- Walkme for Usage and Troubleshooting
- N+1 Hitless Upgrade - Site based Upgrade
- eWLC C9800 TACACS Accounting Logs for GREEN operations
- Rolling AP Upgrade.
- WPA3 enhancements - FT SAE support
- C9800 QOS Gaps and Fixes
- Scheduling of SSID broadcast
- eWLC Standby Monitoring: LLDP

EWC

- FIPS/CC support for EWC
- Regulatory Domain Reduction - Phase 2
- WPA3 enhancements - FT SAE support
- WebGui Client 360 View should display additional client information
- QOS Gaps and Fixes.
- Walkme for Usage and Troubleshooting
- Local EAP Authentication
- Support Scheduling of SSID broadcast

Open Caveats

Defect ID	Title
CSCwb99428	Walkme - Security-AAA configuration flow issue
CSCwc44450	Site tag configuration flow is overlapping to other controller.
CSCwc04211	Walkme - configure 802.1x auth - Configure policy profile and policy tag issues
CSCwb99351	Able to Enable a Policy profile without central authentication in CLI
CSCwc01838	Configure 802.1x auth - Radius server and add radius server to server issues
CSCwc33730	While configuring flex profile the flow has stopped at VLAN
CSCwc21470	Web Auth Parameter map Name creating with spaces is accepting without any warning.
CSCwc06773	Policy profile -VLAN/VLAN Group Info icon navigating to not existing pages
CSCwc09144	CLI - User-cred password - showing same UNENCRYPTED user password twice
CSCwc06573	Wlan Security -AKM is not updating correctly after changing the WPA2 Encryption type
CSCwc14069	WLAN - Clicking on Empty Space near Status and Broadcast SSID changes enable/disable status
CSCwc47842	Unable to connect to client with WPA3 FT+SAE Security
CSCwb99676	Walkme - policy profile creation flow is not fully complete
CSCwc04120	Walkme - configure 802.1x auth - Configure Authentication Methods and Configure a WLAN issues
CSCwc24111	Top Applications pie chart in Client 360 view getting misplaced
CSCwc01661	JA Locale : Walkme - Security-AAA configuration flow
CSCwc05304	Configure 802.1x auth - Assign the policy tag issue
CSCwc09122	Walkme - Local web auth - create and assign policy tag issues

CSCwc17843	Configuring Flex Connect - configure a site tag flow also seen in Policy and RF tabs
CSCwc33909	JA Locale: Flow issue in Flex Profile page in Japanese UI
CSCwb99585	Walkme - Navigation for policy profile, policy tag & site tag issue
CSCwc18806	Able to configure MPSK Priority 2 without configuring Priority 0
CSCwc33726	Monitor command is duplicated in CLI
CSCwc13144	Configuring AAA server with "show me how" the button is repeating with the flow
CSCwc09113	Local web auth - Web Auth and Authentication method issues
CSCwc09114	Local web auth - wlan and policy profile issues
CSCwc11508	Policy Tag: Able to delete wlan-policy maps without enabling checkbox after cancelling

Resolved Caveats

Defect ID	Title
CSCwc04023	Walkme - Language dropdown needs to be hidden from walkme popup
CSCwc14047	Policy Profile - QoS and AVC Tab is not showing properly
CSCwc09309	Unable to save configuration of WPA+WPA2 after configuring WPA3- OWE Configuration
CSCwc13748	Monitoring - AAA Page Show me how is not navigating
CSCwc05284	Wlan operation successful even after warning / AKM not updating after Encryption type changed
CSCwc05335	Dashboard - Overview dashlets issue
CSCwc12049	eWC UI: Rogue config buttons is overlapping on failures & timer , clearly not visible
CSCwc13796	WLAn- Add to Policy Tags Page loading occurs after give delete to unselecting Policy tags
CSCwb92214	AP join profile dialog box - navigate to issue
CSCwc09126	Local web auth - create user credentials issue
CSCwb92879	Different Data is showing for Image Type in AP Statistics
CSCwb98330	OWE- transition mode wlan id is showing range as (1-4096)
CSCwb99803	Cursor is showing like Clickable in AP Operational Configuration Viewer- Access Points
CSCwc06838	Wlan WPA2 Encryption is aligned improperly in Japanese UI
CSCwc10345	Configuration Mesh- Issue with new site tag configuration
CSCwc13690	Policy Type is not showing for Without AKM Security Type in Client Page
CSCwc24120	All Access Points refresh notification is overlapped on Current Active
CSCwc24129	Walkme: Wireless Debug Analyzer is overlapped on Last Run Result
CSCwc31572	AKM options and Password eye were misaligned in WLAN LAyer 2 Security

CSCwc33187	Manage Syslog Servers - Buffer size is not getting configured properly
CSCwc46686	Wlan Security : WPA-TKIP type warning message is showing in WPA3 Encryption Type
CSCwc51240	AP Statistics : Overlapping of Radio Role with Admin Status in 360 View

New Features

WebGui Client 360 View should display additional client information

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_360view_01	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	CSCwc13690
EWLCJ179S_360view_02	Connect Android Client and check all the Information in Client 360	To connect Android Client and to check all the Information in Client 360	Failed	CSCwc24111
EWLCJ179S_360view_03	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	
EWLCJ179S_360view_04	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	
EWLCJ179S_360view_05	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	
EWLCJ179S_360view_06	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	
EWLCJ179S_360view_07	Connect Wired Client and check all the information in Client 360	To connect Wired Client and check all the information in Client 360	Passed	
EWLCJ179S_360view_08	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	

EWLCJ179S_360view_09	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	CSCwc31572
EWLCJ179S_360view_10	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	
EWLCJ179S_360view_11	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	
EWLCJ179S_360view_12	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	
EWLCJ179S_360view_13	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	
EWLCJ179S_360view_14	Verify client deletion status in Client 360 page	To verify client deletion status in Client 360 page	Passed	
EWLCJ179S_360view_15	Verify Hostname in client 360 page	To validate hostname information	Passed	
EWLCJ179S_360view_16	Verify Connection Speed in client 360 page	To validate Connection Speed information	Passed	
EWLCJ179S_360view_17	Verify Signal Quality (SNR) in client 360 page	To validate SNR information	Passed	
EWLCJ179S_360view_18	Verify Signal Strength in client 360 page	To validate Signal Strength information	Passed	
EWLCJ179S_360view_19	Verify Usage (Volume) in client 360 page	To validate Usage (Volume) information	Passed	
EWLCJ179S_360view_20	Verify Uptime in client 360 page	To validate Uptime information	Passed	

EWLCJ179S_360view_21	Verify DUID information in client 360 page	To validate DUID information	Passed	
EWLCJ179S_360view_22	Verify Frequency Band in client 360 page	To validate Frequency Band information	Passed	
EWLCJ179S_360view_23	Verify WLAN Profile in client 360 page	To validate WLAN Profile information	Passed	CSCwc51240
EWLCJ179S_360view_24	Verify AP MAC in client 360 page	To validate AP MAC information	Passed	
EWLCJ179S_360view_25	Verify Tags - Site, Policy, RF in client 360 page	To validate Tags - Site, Policy, RF information	Passed	
EWLCJ179S_360view_26	Verify Channel Width in client 360 page	To validate Channel Width information	Passed	
EWCJ179S_C360_1	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	
EWCJ179S_C360_2	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	
EWCJ179S_C360_3	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	
EWCJ179S_C360_4	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	
EWCJ179S_C360_5	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	
EWCJ179S_C360_6	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	

EWCJ179S_C360_7	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	
EWCJ179S_C360_8	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	
EWCJ179S_C360_9	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	
EWCJ179S_C360_10	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	
EWCJ179S_C360_11	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	
EWCJ179S_C360_12	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	
EWCJ179S_C360_13	Verify client deletion status in Client 360 page	To verify client deletion status in Client 360 page	Passed	
EWCJ179S_C360_14	Verify Hostname in client 360 page	To validate hostname information	Passed	
EWCJ179S_C360_15	Verify Connection Speed in client 360 page	To validate Connection Speed information	Passed	
EWCJ179S_C360_16	Verify Signal Quality (SNR) in client 360 page	To validate SNR information	Passed	
EWCJ179S_C360_17	Verify Signal Strength in client 360 page	To validate Signal Strength information	Passed	

EWCJ179S_C360_18	Verify Usage (Volume) in client 360 page	To validate Usage (Volume) information	Passed	
EWCJ179S_C360_19	Verify Uptime in client 360 page	To validate Uptime information	Passed	
EWCJ179S_C360_20	Verify DUID information in client 360 page	To validate DUID information	Passed	
EWCJ179S_C360_21	Verify Frequency Band in client 360 page	To validate Frequency Band information	Passed	
EWCJ179S_C360_22	Verify WLAN Profile in client 360 page	To validate WLAN Profile information	Passed	
EWCJ179S_C360_23	Verify AP MAC in client 360 page	To validate AP MAC information	Passed	
EWCJ179S_C360_24	Verify Tags - Site, Policy, RF in client 360 page	To validate Tags - Site, Policy, RF information	Failed	CSCwc06773
EWCJ179S_C360_25	Verify Channel Width in client 360 page	To validate Channel Width information	Passed	

Critical KPIs on AP 360: Rogue AP view with channel width

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_KPIs_01	Check if the Rogue AP is detected in eWLC 9800-80	To verify if the Rogue AP is detected in eWLC 9800-80 and also verify if different rogue AP are detected	Passed	
EWLCJ179S_KPIs_02	Check if the Rogue AP is detected in eWLC 9800-L	To verify if the Rogue AP is detected in eWLC 9800-L and also verify if different rogue AP are detected	Passed	
EWLCJ179S_KPIs_03	Check if the Rogue AP is detected in eWLC 9800-CL	To verify if the Rogue AP is detected in eWLC 9800-CL and also verify if different rogue AP are detected	Passed	
EWLCJ179S_KPIs_04	Check if the Rogue AP is detected in eWLC 9800-80 which has a HA pair	To verify if the Rogue AP is detected in eWLC 9800-80 and also verify if different rogue AP are detected	Passed	
EWLCJ179S_KPIs_05	Configuring the rogue policy and rogue rule in eWLC 9800-80	To configuring the rogue policy and rogue rule in eWLC 9800-80 and verify if the rules are created and rogue is detected	Passed	
EWLCJ179S_KPIs_06	Configuring the rogue policy and rogue rule in eWLC 9800-CL	To configuring the rogue policy and rogue rule in eWLC 9800-CL and verify if the rules are created and rogue is detected	Passed	

EWLCJ179S_KPIs_07	Configuring the rogue policy and rogue rule in eWLC 9800-L	To configuring the rogue policy and rogue rule in eWLC 9800-L and verify if the rules are created and rogue is detected	Passed	
EWLCJ179S_KPIs_08	Checking the channel width of the AP that detected the rogue in eWLC 9800-80	To check the channel width of the AP that detected the rogue and verify the details of the rogue in 9800-80 eWLC	Passed	
EWLCJ179S_KPIs_09	Checking the channel width of the AP that detected the rogue in eWLC 9800-CL	To check the channel width of the AP that detected the rogue and verify the details of the rogue in 9800-CL eWLC	Passed	
EWLCJ179S_KPIs_10	Checking the channel width of the AP that detected the rogue in eWLC 9800-L	To check the channel width of the AP that detected the rogue and verify the details of the rogue in 9800-L eWLC	Passed	

Walkme for Usage and Troubleshooting

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Walkme_1	Check Security-AAA configuration in walkme	To check Security-AAA configuration in walkme	Passed	CSCwc13748
EWLCJ179S_Walkme_2	Check Create SSIDs configuration in walkme	To check Create SSIDs configuration in walkme	Passed	CSCwc04023
EWLCJ179S_Walkme_3	Check Create Policy Profile configuration in walkme	To check Create Policy Profile configuration in walkme	Passed	
EWLCJ179S_Walkme_4	Check Create a Policy Tag configuration in walkme	To check Create a Policy Tag configuration in walkme	Passed	
EWLCJ179S_Walkme_5	Check Create a Flex Profile configuration in walkme	To check Create a Flex Profile configuration in walkme	Failed	CSCwc33730 , CSCwc33909
EWLCJ179S_Walkme_6	Check Create a Site tag configuration in walkme	To check Create a Site tag configuration in walkme	Passed	CSCwc10345
EWLCJ179S_Walkme_7	Check configure a Radius server configuration in walkme	To check configure a Radius server configuration in walkme	Passed	
EWLCJ179S_Walkme_8	Check Add the Radius server to server configuration in walkme	To check Add the Radius server to server configuration in walkme	Failed	CSCwc13144
EWLCJ179S_Walkme_9	Check Configure Authentication Methods configuration in walkme	To check Configure Authentication Methods configuration in walkme	Passed	
EWLCJ179S_Walkme_10	Check Configure a WLAN profile configuration in walkme	To check Configure a WLAN profile configuration in walkme	Passed	CSCwc06838

EWLCJ179S_Walkme_11	Check Configure policy profiles configuration in walkme	To check Configure policy profiles configuration in walkme	Passed	
EWLCJ179S_Walkme_12	Check Configure SSIDs configuration in walkme	To check Configure SSIDs configuration in walkme	Passed	
EWLCJ179S_Walkme_13	Check Configure a Flex profile configuration in walkme	To check Configure a Flex profile configuration in walkme	Passed	
EWLCJ179S_Walkme_14	Check Verify Authentication configuration in walkme	To check Verify Authentication configuration in walkme	Passed	
EWLCJ179S_Walkme_15	Check Let's troubleshoot by a single AP configuration in walkme	To check Let's troubleshoot by a single AP configuration in walkme	Passed	
EWLCJ179S_Walkme_16	Check Radioactive trace with GUI configuration in walkme	To check Radioactive trace with GUI configuration in walkme	Passed	CSCwc24129
EWCJ179S_Walkme_1	Check Security-AAA configuration in walkme	To check Security-AAA configuration in walkme	Failed	CSCwb99428
EWCJ179S_Walkme_2	Check Create SSIDs configuration in walkme	To check Create SSIDs configuration in walkme	Passed	
EWCJ179S_Walkme_3	Check Create Policy Profile configuration in walkme	To check Create Policy Profile configuration in walkme	Failed	CSCwb99676
EWCJ179S_Walkme_4	Check Create a Policy Tag configuration in walkme	To check Create a Policy Tag configuration in walkme	Failed	CSCwb99585
EWCJ179S_Walkme_5	Check Create a Flex Profile configuration in walkme	To check Create a Flex Profile configuration in walkme	Failed	CSCwc17843

EWCJ179S_Walkme_6	Check Create a Site tag configuration in walkme	To check Create a Site tag configuration in walkme	Passed	
EWCJ179S_Walkme_7	Check Policy tag assignment per AP configuration in walkme	To check Policy tag assignment per AP configuration in walkme	Passed	
EWCJ179S_Walkme_8	Check Policy tag assignment for multiple AP configuration in walkme	To check Policy tag assignment for multiple AP configuration in walkme	Passed	
EWCJ179S_Walkme_9	Check configure a Radius server configuration in walkme	To check configure a Radius server configuration in walkme	Failed	CSCwc01661
EWCJ179S_Walkme_10	Check Add the Radius server to server configuration in walkme	To check Add the Radius server to server configuration in walkme	Failed	CSCwc01838
EWCJ179S_Walkme_11	Check Configure Authentication Methods configuration in walkme	To check Configure Authentication Methods configuration in walkme	Failed	CSCwc04120
EWCJ179S_Walkme_12	Check Configure a WLAN profile configuration in walkme	To check Configure a WLAN profile configuration in walkme	Passed	
EWCJ179S_Walkme_13	Check Configure policy profiles configuration in walkme	To check Configure policy profiles configuration in walkme	Passed	
EWCJ179S_Walkme_14	Check Configure a policy tag configuration in walkme	To check Configure a policy tag configuration in walkme	Failed	CSCwc04211
EWCJ179S_Walkme_15	Check Assign the policy tag configuration in walkme	To check Assign the policy tag configuration in walkme	Failed	CSCwc05304
EWCJ179S_Walkme_16	Check Define a Web Auth configuration in walkme	To check Define a Web Auth configuration in walkme	Failed	CSCwc09113

EWCJ179S_Walkme_17	Check Configure an Authentication Method configuration in walkme	To check Configure an Authentication Method configuration in walkme	Passed	
EWCJ179S_Walkme_18	Check Configure SSIDs configuration in walkme	To check Configure SSIDs configuration in walkme	Failed	CSCwc09114
EWCJ179S_Walkme_19	Check Configure policy profile configuration in walkme	To check Configure policy profile configuration in walkme	Passed	
EWCJ179S_Walkme_20	Check Configure policy tag configuration in walkme	To check Configure policy tag configuration in walkme	Passed	
EWCJ179S_Walkme_21	Check Assign policy tag to Aps configuration in walkme	To check Assign policy tag to Aps configuration in walkme	Failed	CSCwc09122
EWCJ179S_Walkme_22	Check Create User Credentials configuration in walkme	To check Create User Credentials configuration in walkme	Passed	CSCwc09126
EWCJ179S_Walkme_23	Check Configuring your Custom QoS profiles configuration in walkme	To check Configuring your Custom QoS profiles configuration in walkme	Passed	
EWCJ179S_Walkme_24	Check Assigning QoS profile to a Policy Profile configuration in walkme	To check Assigning QoS profile to a Policy Profile configuration in walkme	Passed	
EWCJ179S_Walkme_25	Check Assign the Policy profile to a WLAN's Policy Tag configuration in walkme	To check Assign the Policy profile to a WLAN's Policy Tag configuration in walkme	Passed	
EWCJ179S_Walkme_26	Check Assign a WLAN's Policy Tag to a AP configuration in walkme	To check Assign a WLAN's Policy Tag to a AP configuration in walkme	Passed	CSCwc24120

EWCJ179S_Walkme_27	Check Configuring Open Roaming Profile configuration in walkme	To check Configuring Open Roaming Profile configuration in walkme	Passed	
EWCJ179S_Walkme_28	Check Configuring NAI Realms configuration in walkme	To check Configuring NAI Realms configuration in walkme	Passed	
EWCJ179S_Walkme_29	Check Configuring Organisational Identifier Alias configuration in walkme	To check Configuring Organisational Identifier Alias configuration in walkme	Passed	
EWCJ179S_Walkme_30	Check Configuring WAN Metrics configuration in walkme	To check Configuring WAN Metrics configuration in walkme	Passed	
EWCJ179S_Walkme_31	Check Configuring Beacon Parameters configuration in walkme	To check Configuring Beacon Parameters configuration in walkme	Passed	
EWCJ179S_Walkme_32	Check Configuring Authentication and Venue configuration in walkme	To check Configuring Authentication and Venue configuration in walkme	Passed	
EWCJ179S_Walkme_33	Check Configuring 3GPP/Operator configuration in walkme	To check Configuring 3GPP/Operator configuration in walkme	Passed	
EWCJ179S_Walkme_34	Check Configuring calling-station-id configuration in walkme	To check Configuring calling-station-id configuration in walkme	Passed	
EWCJ179S_Walkme_35	Check Configure a RADIUS Server for OR configuration in walkme	To check Configure a RADIUS Server for OR configuration in walkme	Passed	

EWCJ179S_Walkme_36	Check Add the RADIUS Server to the Server for OR configuration in walkme	To check Add the RADIUS Server to the Server for OR configuration in walkme	Passed	
EWCJ179S_Walkme_37	Check Configure Authentication Method for OR configuration in walkme	To check Configure Authentication Method for OR configuration in walkme	Passed	
EWCJ179S_Walkme_38	Check Configure a WLAN profile for OR configuration in walkme	To check Configure a WLAN profile for OR configuration in walkme	Passed	
EWCJ179S_Walkme_39	Check Configure Policy profile for Open Roaming configuration in walkme	To check Configure Policy profile for Open Roaming configuration in walkme	Passed	
EWCJ179S_Walkme_40	Check Configuring a Policy Tag for OR configuration in walkme	To check Configuring a Policy Tag for OR configuration in walkme	Passed	
EWCJ179S_Walkme_41	Check Assign the Policy Tag for OR configuration in walkme	To check Assign the Policy Tag for OR configuration in walkme	Passed	
EWCJ179S_Walkme_42	Check Configure a WLAN configuration in walkme	To check Configure a WLAN configuration in walkme	Passed	
EWCJ179S_Walkme_43	Check Configure a Policy Profile configuration in walkme	To check Configure a Policy Profile configuration in walkme	Passed	
EWCJ179S_Walkme_44	Check Configuring a Policy Tag configuration in walkme	To check Configuring a Policy Tag configuration in walkme	Passed	
EWCJ179S_Walkme_45	Check Configure a Flex profile configuration in walkme	To check Configure a Flex profile configuration in walkme	Passed	

EWCJ179S_Walkme_46	Check Configure a Site tag configuration in walkme	To check Configure a Site tag configuration in walkme	Passed	
EWCJ179S_Walkme_47	Check Verify Authentication configuration in walkme	To check Verify Authentication configuration in walkme	Passed	
EWCJ179S_Walkme_48	Check Are the expected number of Aps Connected? configuration in walkme	To check Are the expected number of Aps Connected? configuration in walkme	Passed	
EWCJ179S_Walkme_49	Check Are there any patterns in AP failure ? configuration in walkme	To check Are there any patterns in AP failure? configuration in walkme	Passed	
EWCJ179S_Walkme_50	Check for disconnection and discovery failures? configuration in walkme	To check for disconnection and discovery failures? configuration in walkme	Passed	
EWCJ179S_Walkme_51	Check Let's troubleshoot by a single AP configuration in walkme	To check Let's troubleshoot by a single AP configuration in walkme	Passed	
EWCJ179S_Walkme_52	Check for wncd issues configuration in walkme	To check for wncd issues configuration in walkme	Passed	
EWCJ179S_Walkme_53	Check for DTLS Errors configuration in walkme	To check for DTLS Errors configuration in walkme	Passed	
EWCJ179S_Walkme_54	Check Radioactive trace with GUI configuration in walkme	To check Radioactive trace with GUI configuration in walkme	Passed	
EWCJ179S_Walkme_55	Check Radioactive trace with CLI configuration in walkme	To check Radioactive trace with CLI configuration in walkme	Passed	

N+1 Hitless Upgrade - Site based Upgrade

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_N1_01	Create mobility group between WLCs (9800-40)	WLC 1 will be in v1, WLC 2 will be in v2 and All AP's are joined to WLC 1 (all WLC will be in same mobility group and in install mode)	Passed	
EWLCJ179S_N1_02	Create mobility group between WLCs (9800-80)	WLC 1 will be in v1, WLC 2 will be in v2 and All AP's are joined to WLC 1 (all WLC will be in same mobility group and in install mode)	Passed	
EWLCJ179S_N1_03	Create mobility group between WLCs (9800-CL)	WLC 1 will be in v1, WLC 2 will be in v2 and All AP's are joined to WLC 1 (all WLC will be in same mobility group and in install mode)	Passed	
EWLCJ179S_N1_04	Create mobility group between WLCs (9800 HA setup)	WLC 1 will be in v1, WLC 2 will be in v2 and All AP's are joined to WLC 1 (all WLC will be in same mobility group and in install mode)	Passed	
EWLCJ179S_N1_05	Verify All AP's are predownloaded the version2 image and after reloading automatically join to WLC 2	Download version 2 image to WLC 1, execute ap preimage download manually, Once all AP's are predownloaded the image, execute command ap image upgrade destination <WLC 2 Name> <WLC 2 IP>	Passed	
EWLCJ179S_N1_06	Verify N+1 Rolling Image Upgrade using WebUI	To verify N+1 Rolling Image Upgrade using WebUI	Passed	

EWLCJ179S_N1_07	Verify N+1 Rolling Image Upgrade using CLI	To verify N+1 Rolling Image Upgrade using CLI	Passed	
EWLCJ179S_N1_08	Repeat the test case 2 then once all AP joined to wlc 2, then reload the wlc 1 with version 2 image and once wlc 1 is up move all AP's to wlc1 using command ap image move destination <WLC 1 Name> <WLC 1IP> [<Upgrade report Name>]	To repeat the test case 2 then once all AP joined to wlc 2, then reload the wlc 1 with version 2 image and once wlc 1 is up move all AP's to wlc1 using command ap image move destination <WLC 1 Name> <WLC 1IP> [<Upgrade report Name>]	Passed	
EWLCJ179S_N1_09	Connect Windows Client after test case 2	To connect Windows Client after test case 2	Passed	
EWLCJ179S_N1_10	Connect Android Client after test case 2	To connect Android Client after test case 2	Passed	
EWLCJ179S_N1_11	Connect MAC Client after test case 2	To connect MAC Client after test case 2	Passed	
EWLCJ179S_N1_12	Connect IOS Client after test case 2	To connect IOS Client after test case 2	Passed	
EWLCJ179S_N1_13	After issue CLI break mobility down and verify still all the AP's can join to wlc 2 , Verify ap upgrade report , Once all AP's are joined to wlc 2 make mobility tunnel up then verify the report	To verify still all the AP's can join to wlc 2 when mobility down and to verify ap upgrade report , Once all AP's are joined to wlc 2 make mobility tunnel up then verify the report	Passed	

EWLCJ179S_N1_14	Create mobility group between WLCs with mixed mode of AP's Local, Sniffer and Flex	WLC 1 will be in v1, WLC 2 will be in v2 and All AP's (Mixed mode of AP's)are joined to WLC 1 (all WLC will be in same mobility group and in install mode)	Passed	
EWLCJ179S_N1_15	Test case 1 after issue CLI shutdown few AP so that it will not be joining to wlc 3 verify the report shows missing AP	After issuing CLI shutdown few AP so that it will not be joining to wlc 3 verify the report shows missing AP	Passed	
EWLCJ179S_N1_16	Verify packet drop and latency between mobility tunnel	To verify packet drop and latency between mobility tunnel	Passed	
EWLCJ179S_N1_17	Verify trap syslog message,ap reset ,preimage download success etc	To verify trap syslog message,ap reset ,preimage download success etc	Passed	

eWLC C9800 TACACS Accounting Logs for GREEN operations

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Tacacs_01	Verify green validation for allowing the user for complete access to ME EWLC network via TACACS	To verify green validation for allowing the user for complete access to ME EWLC network via TACACS	Passed	
EWLCJ179S_Tacacs_02	Verify green validation for providing the user for lobby admin access to the ME EWLC via TACACS	To verify green validation for providing the user for lobby admin access to the ME EWLC via TACACS	Passed	
EWLCJ179S_Tacacs_03	Verify green validation for providing the user for monitoring access to the ME EWLC via TACACS	To verify green validation for providing the user for monitoring access to the ME EWLC via TACACS	Passed	
EWLCJ179S_Tacacs_04	Verify green validation for trying to login ME EWLC via TACACS with invalid credentials	Trying to login ME EWLC via TACACS with invalid credentials	Passed	
EWLCJ179S_Tacacs_05	Verify green validation for 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	
EWLCJ179S_Tacacs_06	Verify green validation for 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	

EWLCJ179S_Tacacs_07	Verify green validation for 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	
EWLCJ179S_Tacacs_08	Verify green validation for providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN, Controller, Wireless, Security, Commands Line Interfaces and "Management" checkboxes.	Passed	
EWLCJ179S_Tacacs_09	Verify green validation for 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	

Rolling AP Upgrade

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Roll_AP_01	Providing the same controller name and ip address for primary controller and N+1 controller	To check whether the same controller name is accepted or not for primary controller and N+1 controller	Passed	
EWLCJ179S_Roll_AP_02	Upgrading the software image in a controller	To check whether the software image is upgraded in controller	Passed	
EWLCJ179S_Roll_AP_03	Scheduling the time to upgrade the software image into a controller.	To check whether the software image is upgraded into a controller in scheduling time	Passed	
EWLCJ179S_Roll_AP_04	Scheduling the time "Now" to upgrade the software image into a controller.	To check whether the software image is upgraded into a controller in scheduling time "Now"	Passed	
EWLCJ179S_Roll_AP_05	Resync trigger to Controller from DNAC after upgrade the software image in controller.	To check whether Controller is reloaded when triggering from DNAC after upgrade the software image in controller.	Passed	
EWLCJ179S_Roll_AP_06	Upgrade the wrong software image into the Controller from DNAC	To verify whether the error message will display when trying to upgrade wrong software image into the Controller from DNAC	Passed	
EWLCJ179S_Roll_AP_07	AP joining status to Controller after upgrade the software image	To check whether the joined Aps upgraded with controller image	Passed	CSCwb99803

EWLCJ179S_Roll_AP_08	Verify the client connectivity status to Controller after upgrade the software image	To check whether the Client associate with controller	Passed	
EWLCJ179S_Roll_AP_09	Upgrading the software image into existing group of AP	To check whether the software image is upgraded into existing group of AP	Passed	
EWLCJ179S_Roll_AP_10	Import the image to image repository using HTTP	To check whether the WLC is upgraded using TFTP from PI	Passed	
EWLCJ179S_Roll_AP_11	Import the image to image repository using FTP	To check whether the WLC is upgraded using FTP from PI	Passed	

WPA3 enhancements - FT SAE support

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_WPA3_01	Configure FT-SAE using CLI	To configure FT-SAE using CLI	Passed	
EWLCJ179S_WPA3_02	Configure FT-SAE using CLI while WLAN Is in use/client is connected to WLAN and active traffic is running	To configure FT-SAE using CLI while WLAN Is in use/client is connected to WLAN and active traffic is running	Passed	
EWLCJ179S_WPA3_03	Unconfiguring/removing FT-SAE using CLI from WLAN config	To unconfigure/remove FT-SAE using CLI from WLAN config	Passed	
EWLCJ179S_WPA3_04	Configure/enable FT-SAE in WPA3 UI page	To configure/enable FT-SAE in WPA3 UI page	Passed	
EWLCJ179S_WPA3_05	Verify enabling FT-802.1x and FT-SAE together	To verify enabling FT-802.1x and FT-SAE together	Passed	CSCwc46686
EWLCJ179S_WPA3_06	Verify configuring WPA2 [FT-PSK] and WPA3 [FT-SAE] in 2 WLANS	To verify configuring WPA2 [FT-PSK] and WPA3 [FT-SAE] in 2 WLANS	Passed	CSCwc09309
EWLCJ179S_WPA3_07	Verify show cli's shall have FT-SAE enable or disable information	To verify show cli's shall have FT-SAE enable or disable information	Failed	CSCwc47842
EWLCJ179S_WPA3_08	Verify statistics for FT-SAE related events during client association/roam	To verify statistics for FT-SAE related events during client association/roam	Passed	
EWLCJ179S_WPA3_09	Verify Client Mobility history/stats has 11r roaming stats	To verify Client Mobility history/stats has 11r roaming stats	Passed	

EWLCJ179S_WPA3_10	Verify Client roam from AP1 to AP2 and vice versa using 6G transmit BSSID. [Over the Air Mode] using H2E	To verify Client roam from AP1 to AP2 and vice versa using 6G transmit BSSID. [Over the Air Mode] using H2E	Passed	
EWLCJ179S_WPA3_11	Verify Client roam from AP1 to AP2 and vice versa using 6G transmit Non-transmit BSSID. [Over the Air Mode] using H2E	To verify Client roam from AP1 to AP2 and vice versa using 6G transmit Non-transmit BSSID. [Over the Air Mode] using H2E	Passed	
EWLCJ179S_WPA3_12	Verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 5G WLAN [over the air Mode]	To verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 5G WLAN [over the air Mode]	Passed	
EWLCJ179S_WPA3_13	Verify Client roam from AP1 to AP2 and vice versa while session timeout to expire using 5G WLAN [over DS Mode]	To verify Client roam from AP1 to AP2 and vice versa while session timeout to expire using 5G WLAN [over DS Mode]	Passed	
EWLCJ179S_WPA3_14	Verify Client roam from AP1 to AP2 and vice versa using 2.4G WLAN. [Over the Air Mode] using HnP	To verify Client roam from AP1 to AP2 and vice versa using 2.4G WLAN. [Over the Air Mode] using HnP	Passed	
EWLCJ179S_WPA3_15	Verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 2.4G WLAN [over the air Mode]	To verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 2.4G WLAN [over the air Mode]	Passed	

EWLCJ179S_WPA3_16	Verification of WPA2 and WPA3 UE connecting	To verify WPA2 and WPA3 UE connection	Passed	
EWLCJ179S_WPA3_17	Verify changing/adding special characters in psk config	To verify changing/adding special characters in psk config	Passed	
EWCJ179S_WPA3_1	Configure FT-SAE using CLI	To configure FT-SAE using CLI	Passed	
EWCJ179S_WPA3_2	Configure FT-SAE using CLI while WLAN Is in use/client is connected to WLAN and active traffic is running	To configure FT-SAE using CLI while WLAN Is in use/client is connected to WLAN and active traffic is running	Passed	
EWCJ179S_WPA3_3	Unconfiguring/removing FT-SAE using CLI from WLAN config	To unconfigure/remove FT-SAE using CLI from WLAN config	Passed	
EWCJ179S_WPA3_4	Configure/enable FT-SAE in WPA3 UI page	To configure/enable FT-SAE in WPA3 UI page	Passed	
EWCJ179S_WPA3_5	Verify enabling FT-802.1x and FT-SAE together	To verify enabling FT-802.1x and FT-SAE together	Passed	
EWCJ179S_WPA3_6	Verify configuring WPA2 [FT-PSK] and WPA3 [FT-SAE] in 2 WLANS	To verify configuring WPA2 [FT-PSK] and WPA3 [FT-SAE] in 2 WLANS	Passed	
EWCJ179S_WPA3_7	Verify show cli's shall have FT-SAE enable or disable information	To verify show cli's shall have FT-SAE enable or disable information	Passed	
EWCJ179S_WPA3_8	Verify statistics for FT-SAE related events during client association/roam	To verify statistics for FT-SAE related events during client association/roam	Passed	
EWCJ179S_WPA3_9	Verify Client Mobility history/stats has 11r roaming stats	To verify Client Mobility history/stats has 11r roaming stats	Passed	

EWCJ179S_WPA3_10	Verify Client roam from AP1 to AP2 and vice versa using 6G transmit BSSID. [Over the Air Mode] using H2E	To verify Client roam from AP1 to AP2 and vice versa using 6G transmit BSSID. [Over the Air Mode] using H2E	Passed	
EWCJ179S_WPA3_11	Verify Client roam from AP1 to AP2 and vice versa using 6G transmit Non-transmit BSSID. [Over the Air Mode] using H2E	To verify Client roam from AP1 to AP2 and vice versa using 6G transmit Non-transmit BSSID. [Over the Air Mode] using H2E	Passed	
EWCJ179S_WPA3_12	Verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 5G WLAN [over the air Mode]	To verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 5G WLAN [over the air Mode]	Passed	
EWCJ179S_WPA3_13	Verify Client roam from AP1 to AP2 and vice versa while session timeout to expire using 5G WLAN [over DS Mode]	To verify Client roam from AP1 to AP2 and vice versa while session timeout to expire using 5G WLAN [over DS Mode]	Passed	
EWCJ179S_WPA3_14	Verify Client roam from AP1 to AP2 and vice versa using 2.4G WLAN. [Over the Air Mode] using HnP	To verify Client roam from AP1 to AP2 and vice versa using 2.4G WLAN. [Over the Air Mode] using HnP	Passed	
EWCJ179S_WPA3_15	Verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 2.4G WLAN [over the air Mode]	To verify Client roam from AP1 to AP2 and vice versa while session timeout and roaming trigger in same time using 2.4G WLAN [over the air Mode]	Passed	

EWCJ179S_WPA3_16	Verification of WPA2 and WPA3 UE connecting	To verify WPA2 and WPA3 UE connection	Passed	
EWCJ179S_WPA3_17	Verify changing/adding special characters in psk config	To verify changing/adding special characters in psk config	Passed	

C9800 QOS Gaps and Fixes

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Qos_1	configure policy profile egress - platinum for upstream traffic	To verify QOS details during upstream traffic for platinum	Passed	
EWLCJ179S_Qos_2	configure policy profile egress - platinum for downstream traffic	To verify QOS details during downstream traffic for platinum	Passed	
EWLCJ179S_Qos_3	configure policy profile egress - gold for upstream traffic	To verify QOS details during upstream traffic for gold	Passed	
EWLCJ179S_Qos_4	configure policy profile egress - gold for downstream traffic	To verify QOS details during downstream traffic for gold	Passed	
EWLCJ179S_Qos_5	configure policy profile egress - silver for upstream traffic	To verify QOS details during upstream traffic for silver	Passed	
EWLCJ179S_Qos_6	configure policy profile egress - silver for downstream traffic	To verify QOS details during downstream traffic for silver	Passed	
EWLCJ179S_Qos_7	configure policy profile egress - bronze for upstream traffic	To verify QOS details during upstream traffic for bronze	Passed	
EWLCJ179S_Qos_8	configure policy profile egress - bronze for downstream traffic	To verify QOS details during downstream traffic for bronze	Passed	
EWLCJ179S_Qos_9	configure policy profile egress - gold with invalid dscp value	To verify QOS details during upstream traffic for gold with dscp value 22(AF23)	Passed	

EWLCJ179S_Qos_10	configure policy profile egress - platinum with non-standard value	To verify QOS details during upstream traffic for gold with dscp value 21(non-standard)	Passed	
EWCJ179S_Qos_1	configure policy profile egress - platinum for upstream traffic	To verify QOS details during upstream traffic for platinum	Passed	
EWCJ179S_Qos_2	configure policy profile egress - platinum for downstream traffic	To verify QOS details during downstream traffic for platinum	Passed	
EWCJ179S_Qos_3	configure policy profile egress - gold for upstream traffic	To verify QOS details during upstream traffic for gold	Passed	
EWCJ179S_Qos_4	configure policy profile egress - gold for downstream traffic	To verify QOS details during downstream traffic for gold	Passed	
EWCJ179S_Qos_5	configure policy profile egress - silver for upstream traffic	To verify QOS details during upstream traffic for silver	Passed	
EWCJ179S_Qos_6	configure policy profile egress - silver for downstream traffic	To verify QOS details during downstream traffic for silver	Passed	
EWCJ179S_Qos_7	configure policy profile egress - bronze for upstream traffic	To verify QOS details during upstream traffic for bronze	Passed	
EWCJ179S_Qos_8	configure policy profile egress - bronze for downstream traffic	To verify QOS details during downstream traffic for bronze	Passed	
EWCJ179S_Qos_9	configure policy profile egress - gold with invalid dscp value	To verify QOS details during upstream traffic for gold with dscp value 22(AF23)	Passed	

EWCJ179S_Qos_10	configure policy profile egress - platinum with non-standard value	To verify QOS details during upstream traffic for gold with dscp value 21(non-standard)	Passed	

Support Scheduling of SSID broadcast

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_SSID_1	Configure Daily Calendar Profile	To configure Daily Calendar Profile	Passed	
EWLCJ179S_SSID_2	Configure Weekly Calendar Profile	To configure Weekly Calendar Profile	Passed	
EWLCJ179S_SSID_3	Configure Monthly Calendar Profile	To configure Monthly Calendar Profile	Failed	CSCwb99351
EWLCJ179S_SSID_4	Configure Daily, Weekly and Monthly Calendar Profile through CLI	To configure Daily, Weekly and Monthly Calendar Profile through CLI	Passed	
EWLCJ179S_SSID_5	Map Calendar Profile to a Policy Profile	To Map Calendar Profile to a Policy Profile	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_SSID_8	Delete the calendar profile from the policy profile	To delete the calendar profile from the policy profile	Passed	
EWLCJ179S_SSID_9	Map multiple calendar profiles to a Policy Profile	To Map multiple calendar profiles to a Policy Profile	Passed	
EWLCJ179S_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	

EWLCJ179S_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	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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_SSID_1	verify whether calendar profile can be created in webUI	To verify whether calendar profile can be created in webUI	Passed	
EWCJ178S_SSID_2	verify whether calendar profile can be created in CLI	To verify whether calendar profile can be created in CLI	Passed	
EWCJ178S_SSID_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_SSID_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_SSID_5	Create a calendar-profile with daily reoccurrence and merge with a policy profile with wlan_enable	To create a calendar-profile with daily reoccurrence and merge with a policy profile with wlan_enable	Passed	
EWCJ178S_SSID_6	create a calendar-profile with weekly reoccurrence and merge with a policy profile with wlan_enable	To create a calendar-profile with weekly reoccurrence and merge with a policy profile with wlan_enable	Passed	
EWCJ178S_SSID_7	create a calendar-profile with monthly reoccurrence and merge with a policy profile with wlan_enable	To create a calendar-profile with monthly reoccurrence and merge with a policy profile with wlan_enable	Passed	
EWCJ178S_SSID_8	create a calendar-profile with daily reoccurrence and merge with a policy profile with deny-client	To create a calendar-profile with daily reoccurrence and merge with a policy profile with deny-client	Passed	
EWCJ178S_SSID_9	create a calendar-profile with weekly reoccurrence and merge with a policy profile with deny-client	create a calendar-profile with weekly reoccurrence and merge with a policy profile with deny-client	Passed	
EWCJ178S_SSID_10	create a calendar-profile with monthly reoccurrence and merge with a policy profile with deny-client	create a calendar-profile with monthly reoccurrence and merge with a policy profile with deny-client	Passed	

EWCJ178S_SSID_11	create calendar-profiles daily, weekly, monthly reoccurrence and merge with a single policy profile with wlan_enable	To create calendar-profiles daily, weekly, monthly reoccurrence and merge with a single policy profile with wlan_enable	Passed	
EWCJ178S_SSID_12	create calendar-profiles daily, weekly, monthly reoccurrence and merge with a single policy profile with deny_client	To create calendar-profiles daily, weekly, monthly reoccurrence and merge with a single policy profile with deny_client	Passed	
EWCJ178S_SSID_13	create calendar-profiles daily, weekly, monthly reoccurrence and merge with a single policy profile with wlan_enable and deny_client	To create calendar-profiles daily, weekly, monthly reoccurrence and merge with a single policy profile with wlan_enable and deny_client	Passed	
EWCJ178S_SSID_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_SSID_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_SSID_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_SSID_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_SSID_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_SSID_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_SSID_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_SSID_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	

eWLC Standby Monitoring: LLDP

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_LLDP_01	Configure HA SSO RMI & validate HA RMI parameters.	To Configure HA SSO RMI	Passed	
EWLCJ179S_LLDP_02	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ179S_LLDP_03	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ179S_LLDP_04	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ179S_LLDP_05	Check process usage details in standby console	To check process usage details in standby console	Passed	
EWLCJ179S_LLDP_06	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ179S_LLDP_07	SSH to standby console directly and check connectivity	To SSH to standby console directly and check connectivity	Passed	
EWLCJ179S_LLDP_08	Monitor health of the system	To monitor health of the system	Passed	
EWLCJ179S_LLDP_09	Preventing write access in standby console	To prevent write access in standby console	Passed	
EWLCJ179S_LLDP_10	Validating inventory information on standby	To validate inventory information on standby	Passed	
EWLCJ179S_LLDP_11	Check logging information of standby chassis	To check logging information of standby chassis	Passed	
EWLCJ179S_LLDP_12	Monitor failure fan state via SNMP	To monitor failure fan state via SNMP	Passed	
EWLCJ179S_LLDP_13	Check lldp entry in standby console	To check lldp entry in standby console	Passed	

EWLCJ179S_LLDP_14	Check lldp errors/overflows in standby console	To check lldp errors/overflows in standby console	Passed	
EWLCJ179S_LLDP_15	Check lldp interface in standby console	To check lldp interface in standby console	Passed	
EWLCJ179S_LLDP_16	Check lldp neighbours in standby console	To check lldp neighbours in standby console	Passed	
EWLCJ179S_LLDP_17	Check lldp neighbour details in standby console	To check lldp neighbour details in standby console	Passed	
EWLCJ179S_LLDP_18	Check lldp traffic in standby console	To check lldp traffic in standby console	Passed	
EWLCJ179S_LLDP_19	Check lldp debug commands in standby console	To check lldp debug commands in standby console	Passed	
EWLCJ179S_LLDP_20	Clear lldp counters to clear the statistics	To clear lldp counters to clear the statistics	Passed	

FIPS/CC support for EWC

Logical ID	Feature	Description	Status	Defect ID
EWCJ179S_FIPS_1	FIPS/CC Support for EWC	To check whether the FIPS is already configured or not	Passed	
EWCJ179S_FIPS_2	FIPS/CC Support for EWC	To enable FIPS mode	Passed	
EWCJ179S_FIPS_3	FIPS/CC Support for EWC	To disable FIPS mode	Passed	
EWCJ179S_FIPS_4	FIPS/CC Support for EWC	To check whether the CC is already configured or not	Passed	
EWCJ179S_FIPS_5	FIPS/CC Support for EWC	To enable CC mode	Passed	
EWCJ179S_FIPS_6	FIPS/CC Support for EWC	To disable CC mode	Passed	
EWCJ179S_FIPS_7	FIPS/CC Support for EWC	To check whether both FIPS and CC are enabled at same time	Passed	
EWCJ179S_FIPS_8	FIPS/CC Support for EWC	To check the Configuration after several Reboots	Passed	
EWCJ179S_FIPS_9	FIPS/CC Support for EWC	To check the Configuration after Upgrade and downgrade	Passed	
EWCJ179S_FIPS_10	FIPS/CC Support for EWC	To Check whether Windows client able to join in wlan after FIPS&CC configuration	Passed	
EWCJ179S_FIPS_11	FIPS/CC Support for EWC	To check whether Mac client able to join in wlan after FIPS&CC configuration	Passed	
EWCJ179S_FIPS_12	FIPS/CC Support for EWC	To check whether Android client able to join in wlan after FIPS&CC configuration	Passed	

EWCJ179S_FIPS_13	FIPS/CC Support for EWC	To check whether Surface client able to join in wlan after FIPS&CC configuration	Passed	
EWCJ179S_FIPS_14	FIPS/CC Support for EWC	To check whether IOS client able to join in wlan after FIPS&CC configuration	Passed	

Regulatory Domain Reduction - Phase 2

Logical ID	Title	Description	Status	Defect Id
EWCJ179S_RegDomain_1	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWCJ179S_RegDomain_2	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWCJ179S_RegDomain_3	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWCJ179S_RegDomain_4	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWCJ179S_RegDomain_5	Verify country code is changed for access point	To verify country code is changed for access point	Passed	
EWCJ179S_RegDomain_6	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	
EWCJ179S_RegDomain_7	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	
EWCJ179S_RegDomain_8	Verify AP joins to other eWLC with another country code supported	To verify AP joins to other eWLC with another country code supported	Passed	
EWCJ179S_RegDomain_9	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	

EWCJ179S_RegDomain_10	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	
EWCJ179S_RegDomain_11	Verify at least one Regulatory Domain is configured or not	To verify at least one Regulatory Domain is configured or not	Passed	
EWCJ179S_RegDomain_12	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Passed	
EWCJ179S_RegDomain_13	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWCJ179S_RegDomain_14	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	
EWCJ179S_RegDomain_15	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWCJ179S_RegDomain_16	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWCJ179S_RegDomain_17	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWCJ179S_RegDomain_18	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	
EWCJ179S_RegDomain_19	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	

EWCJ179S_RegDomain_20	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	
EWCJ179S_RegDomain_21	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	
EWCJ179S_RegDomain_22	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	

Local EAP Authentication

Logical ID	Title	Description	Status	Defect ID
EWCJ179S_LEAP_1	Check for Local EAP Authentication available in wlan	To Check for Local EAP Authentication available in wlan	Passed	
EWCJ179S_LEAP_2	Create a Local EAP Profile with leap alone	To Create a Local EAP Profile with leap alone	Passed	
EWCJ179S_LEAP_3	Create a Local EAP Profile with leap alone and create a wlan	To Create a Local EAP Profile with leap alone and create a wlan	Passed	
EWCJ179S_LEAP_4	Connect Windows client with created LEAP mode wlan	To Connect Windows client with created LEAP mode wlan	Passed	
EWCJ179S_LEAP_5	Connect Mac client with created LEAP mode wlan	To Connect Windows client with created LEAP mode wlan	Passed	
EWCJ179S_LEAP_6	Connect Android client with created LEAP mode wlan	To Connect Windows client with created LEAP mode wlan	Passed	
EWCJ179S_LEAP_7	Connect Surface client with created LEAP mode wlan	To Connect Windows client with created LEAP mode wlan	Passed	
EWCJ179S_LEAP_8	Create a Local EAP Profile with eap-fast alone	To Create a Local EAP Profile with eap-fast alone	Passed	
EWCJ179S_LEAP_9	Create a Local EAP Profile with eap-fast alone and create a wlan	To Create a Local EAP Profile with eap-fast alone and create a wlan	Passed	
EWCJ179S_LEAP_10	Connect Windows client with created EAP-FAST mode wlan	To Connect Windows client with created EAP-FAST mode wlan	Passed	

EWCJ179S_LEAP_11	Connect Mac client with created EAP-FAST mode wlan	To Connect Windows client with created EAP-FAST mode wlan	Passed	
EWCJ179S_LEAP_12	Connect Android client with created EAP-FAST mode wlan	To Connect Windows client with created EAP-FAST mode wlan	Passed	
EWCJ179S_LEAP_13	Connect Surface client with created EAP-FAST mode wlan	To Connect Windows client with created EAP-FAST mode wlan	Passed	
EWCJ179S_LEAP_14	Create a Local EAP Profile with eap-tls alone	To Create a Local EAP Profile with eap-tls alone	Passed	
EWCJ179S_LEAP_15	Create a Local EAP Profile with eap-tls alone and create a wlan	To Create a Local EAP Profile with eap-tls alone and create a wlan	Passed	
EWCJ179S_LEAP_16	Connect Windows client with created EAP-TLS mode wlan	To Connect Windows client with created EAP-TLS mode wlan	Passed	
EWCJ179S_LEAP_17	Connect Mac client with created EAP-TLS mode wlan	To Connect Windows client with created EAP-TLS mode wlan	Passed	
EWCJ179S_LEAP_18	Connect Android client with created EAP-TLS mode wlan	To Connect Windows client with created EAP-TLS mode wlan	Passed	
EWCJ179S_LEAP_19	Connect Surface client with created EAP-TLS mode wlan	To Connect Windows client with created EAP-TLS mode wlan	Passed	
EWCJ179S_LEAP_20	Create a Local EAP Profile with peap alone	To Create a Local EAP Profile with peap alone	Passed	
EWCJ179S_LEAP_21	Create a Local EAP Profile with peap alone and create a wlan	To Create a Local EAP Profile with peap alone and create a wlan	Passed	

EWCJ179S_LEAP_22	Connect Windows client with created PEAP mode wlan	To Connect Windows client with created PEAP mode wlan	Passed	
EWCJ179S_LEAP_23	Connect Mac client with created PEAP mode wlan	To Connect Windows client with created PEAP mode wlan	Passed	
EWCJ179S_LEAP_24	Connect Android client with created PEAP mode wlan	To Connect Windows client with created PEAP mode wlan	Failed	CSCwc09144
EWCJ179S_LEAP_25	Connect Surface client with created PEAP mode wlan	To Connect Windows client with created PEAP mode wlan	Passed	
EWCJ179S_LEAP_26	Create a Local EAP Profile with all available modes	To Create a Local EAP Profile with all available modes	Passed	
EWCJ179S_LEAP_27	Create a Local EAP Profile with all available mode and create a wlan	To Create a Local EAP Profile with all available mode and create a wlan	Passed	
EWCJ179S_LEAP_28	Connect Windows client with created all modes enabled wlan	To Connect Windows client with created all modes enabled wlan	Passed	
EWCJ179S_LEAP_29	Connect Mac client with created all modes enabled wlan	To Connect Windows client with created all modes enabled wlan	Passed	
EWCJ179S_LEAP_30	Connect Android client with created all modes enabled wlan	To Connect Windows client with created all modes enabled wlan	Passed	
EWCJ179S_LEAP_31	Connect Surface client with created all modes enabled wlan	To Connect Windows client with created all modes enabled wlan	Passed	
EWCJ179S_LEAP_32	Check with MAC filtering in Local EAP enabled wlan and check for client connection	To check with MAC filtering in Local EAP enabled wlan and check for client connection	Passed	

EWCJ179S_LEAP_33	Do a AP to AP Roaming in same Controller and check for Client Connection	To do a AP to AP Roaming in same Controller and check for Client Connection	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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_3	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWLCJ179S_Reg_4	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWLCJ179S_Reg_5	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWLCJ179S_Reg_6	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWLCJ179S_Reg_7	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_15	Enable video stream and monitor DL/UL OFDMA statistics	To enable video stream and monitor DL/UL OFDMA statistics	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_Reg_19	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWLCJ179S_Reg_20	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWLCJ179S_Reg_21	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWLCJ179S_Reg_22	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWLCJ179S_Reg_23	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_27	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_Reg_3	Monitor traffic with 11ax Android client connected.	To verify OFDMA details with 11ax Android client connected.	Passed	
EWCJ179S_Reg_4	Monitor traffic with 11ax iPhone client connected.	To verify OFDMA details with 11ax iPhone client connected.	Passed	
EWCJ179S_Reg_5	Monitor traffic with non 11ax Windows client connected.	To verify OFDMA details with non 11ax Windows client connected.	Passed	
EWCJ179S_Reg_6	Monitor traffic with non 11ax Mac client connected.	To verify OFDMA details with non 11ax Mac client connected.	Passed	
EWCJ179S_Reg_7	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWCJ179S_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	

EWCJ179S_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	
EWCJ179S_Reg_10	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_Reg_15	Enable videostream and monitor DL/UL OFDMA statistics	To enable videostream and monitor DL/UL OFDMA statistics	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	

EWCJ179S_Reg_19	Monitor traffic with 11ax Android client connected.	To verify 11ax MU details with 11ax Android client connected.	Passed	
EWCJ179S_Reg_20	Monitor traffic with 11ax iPhone client connected.	To verify 11ax MU details with 11ax iPhone client connected.	Passed	
EWCJ179S_Reg_21	Monitor traffic with non 11ax Windows client connected.	To verify 11ax MU details with non 11ax Windows client connected.	Passed	
EWCJ179S_Reg_22	Monitor traffic with non 11ax Mac client connected.	To verify 11ax MU details with non 11ax Mac client connected.	Passed	
EWCJ179S_Reg_23	Monitor traffic by connecting client to 2.4Ghz radio.	To verify 11ax MU details by connecting client to 2.4Ghz radio.	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_Reg_26	Connect upto 8 clients and monitor DL/UL 11ax MU statistics	To connect upto 8 clients and monitor DL/UL 11ax MU statistics	Passed	
EWCJ179S_Reg_27	Check 11ax MU stats with roaming client scenario	Check 11ax MU stats with roaming client scenario	Passed	
EWCJ179S_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	

EWCJ179S_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
EWLCJ179S_Reg_30	Enable Global OBSS PD for 5ghz band	To verify whether the OBBSS PD enable or not for 5 GHz band	Passed	
EWLCJ179S_Reg_31	Disable Global OBSS PD for 5ghz band	To Check whether the OBBSS PD disable or not for 5 GHz	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_34	Set OBSS PD value for 5 GHZ band	To verify whether the values set for 5 Ghz band or not	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_38	Viewing OBSS PD supports in different AP models	To checking the OBSS PD supports in different AP models	Passed	
EWLCJ179S_Reg_39	Configuring BSS colour details in AP & controller CLIs	To Verify Configured colour details is reflected in AP and Controller CLIs	Passed	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_Reg_663	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ179S_Reg_664	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWLCJ179S_Reg_665	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWLCJ179S_Reg_666	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWLCJ179S_Reg_667	Validate license info in 9800-CL	To validate license info in 9800-CL	Passed	
EWLCJ179S_Reg_668	Validate license info after upgrade	To validate license info after upgrade	Passed	
EWLCJ179S_Reg_669	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_671	Verify Smart Licensing status	To verify Smart Licensing status	Passed	
EWLCJ179S_Reg_672	Verify Smart Licensing Events	To verify Smart Licensing Events	Passed	
EWLCJ179S_Reg_673	Enable/disable Smart Licensing and Save & Reload	To enable/disable Smart Licensing and Save & Reload	Passed	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	

Ability to configure XOR radio for APs in Sniffer mode

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_675	Configure Sniffer for Dual band radios	To configure Sniffer for Dual band radios	Passed	
EWLCJ179S_Reg_676	Change the XOR radio assignment mode to client-serving/ monitor/ Sniffer	To verify XOR radio assignment mode changed or not	Passed	
EWLCJ179S_Reg_677	Verify AP mode is Sniffer after AP reload	To verify ap mode after reload	Passed	
EWLCJ179S_Reg_678	Configure Sniffer for Dual band radios through CLI	To configure Sniffer for Dual band radios through CLI	Passed	
EWLCJ179S_Reg_679	Validate unable to set sniffer details error message	To validate unable to set sniffer details error message	Passed	
EWLCJ179S_Reg_680	XOR radio band switching from 2.4 Ghz to 5 Ghz	To capture Sniffer from 2.4 Ghz to 5 Ghz	Passed	
EWLCJ179S_Reg_681	XOR radio band switching from 5 Ghz to 2.4 Ghz	To capture Sniffer from 5 Ghz to 2.4 Ghz	Passed	
EWLCJ179S_Reg_682	Perform band switching multiple times and capture packets	Tp perform band switching multiple times and to capture packets	Passed	
EWLCJ179S_Reg_683	Perform band switching every one minute for 10 times	To perform band switching every one minute for 10 times	Passed	
EWLCJ179S_Reg_684	Change mode from local to flex and capture network activity	To capture network activity when AP mode changed from local to flex	Passed	
EWLCJ179S_Reg_685	Change mode from flex to local and capture network activity	To capture network activity when AP mode changed from flex to local	Passed	

EWLCJ179S_Reg_686	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	
EWLCJ179S_Reg_687	Check whether alert is triggered or not when Sniffer details modified	To check whether alert is triggered or not when Sniffer details modified	Passed	
EWLCJ179S_Reg_688	Verify Sniffer Channel range	To verify Sniffer Channel range	Passed	

Adapative Load EDCA Parameter

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_64	Validate the EDCA parameter with wmm-default profile	To associate the client and verifying EDCA parameter in wmm-default profile	Passed	
EWLCJ179S_Reg_65	Validate the EDCA parameter with custom-voice profile	To associate the client and verifying EDCA parameter in custom-voice profile	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_67	Validate the EDCA parameter with optimized-voice profile	To associate the client and verifying EDCA parameter in optimized-voice profile	Passed	
EWLCJ179S_Reg_68	Validate the EDCA parameter with svp-voice profile	To associate the client and verifying EDCA parameter in svp-voice profile	Passed	
EWLCJ179S_Reg_69	Validate the EDCA parameter with Fastlane profile	To associate the client and verifying EDCA parameter in Fastlane profile	Passed	
EWLCJ179S_Reg_70	Associate the windows client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ179S_Reg_71	Associate the Android client and verify the EDCA parameter in 9130 AP	To associate the client and verifying EDCA parameter	Passed	
EWLCJ179S_Reg_72	Associate the MAC client and verify the EDCA parameter in 9120 AP	To associate the client and verifying EDCA parameter	Passed	

EWLCJ179S_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	
EWLCJ179S_Reg_74	Validate the EDCA parameter with different profile in 6GHz frequency	To associate the client and verifying EDCA parameter for 6GHZ frequency	Passed	
EWLCJ179S_Reg_75	Validate the EDCA parameter with different profile in 5GHz frequency	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ179S_Reg_76	Validate the EDCA parameter with single client	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ179S_Reg_77	Perform Inter roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ179S_Reg_78	Perform Intra roaming and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ179S_Reg_79	Perform controller reload and validate the load balancing	To associate the client and verifying EDCA parameter for 5GHZ frequency	Passed	
EWLCJ179S_Reg_80	Associate the MS-GO client with SSID and validate the EDCA parameter	To associate the client and verifying EDCA parameter.	Passed	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	CSCwc13796
EWLCJ179S_Reg_84	Map tagX profile to Access Point	To map tagX profile to Access Point	Passed	
EWLCJ179S_Reg_85	Test tag source priority is followed by AP tags persistency	To test tag source priority is followed by AP tags persistency	Passed	
EWLCJ179S_Reg_86	Upload multiple AP MAC addresses, tagX through CSV file	To upload multiple AP MAC addresses, tagX through CSV file	Passed	
EWLCJ179S_Reg_87	Verify Tag Source Priority	To verify Tag Source Priority	Passed	
EWLCJ179S_Reg_88	Move Access Point from eWLC1 to eWLC2 with Preserved tags	To move Access Point from eWLC1 to eWLC2 with Preserved tags	Failed	CSCwc44450
EWLCJ179S_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	
EWLCJ179S_Reg_90	Move Access Point to other controller on Priority base	To move Access Point to other controller on Priority base	Passed	
EWLCJ179S_Reg_91	Verify Syslog's after moving AP from eWLC1 to eWLC2	To verify Syslog's after moving AP from eWLC1 to eWLC2	Passed	

EWLCJ179S_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	
EWLCJ179S_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	Failed	CSCwc05284
EWLCJ179S_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	Failed	CSCwc06573
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	Failed	CSCwc11508
EWLCJ179S_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	
EWLCJ179S_Reg_101	Create Location and upload empty csv file	To create Location and upload empty csv file	Passed	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_105	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	
EWLCJ179S_Reg_106	Configure radius-server wireless attribute call station id for authentication and accounting with “ap- macaddress - ssid-flex profile name	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap- macaddress - ssid-flex profile name	Passed	
EWLCJ179S_Reg_107	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-policy tag name”	Passed	

EWLCJ179S_Reg_108	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	
EWLCJ179S_Reg_109	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	
EWLCJ179S_Reg_110	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-site tag name”	Passed	
EWLCJ179S_Reg_111	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWLCJ179S_Reg_112	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWLCJ179S_Reg_113	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	
EWLCJ179S_Reg_114	HA active to standby config impact	To verify config impact HA active to standby	Passed	
EWLCJ179S_Reg_115	active to standby to active config impact	To verify config impact when active to standby to active	Passed	

EWLCJ179S_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	
EWLCJ179S_Reg_117	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWLCJ179S_Reg_118	Change station id case and verify config impact "radius-server attribute wireless authentication call station Id Case upper/ lower"	To Change station id case and verify config impact	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	

EWCJ179S_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-policy tag name”	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_Reg_68	Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-site tag name”	To Configure radius-server wireless attribute call station id for authentication and accounting with “ap-mac address-ssid-site tag name”	Passed	
EWCJ179S_Reg_69	configure different servers for authentication and accounting	To configure different servers for authentication and accounting	Passed	
EWCJ179S_Reg_70	configuring both AAA and local authentication	To configuring both AAA and local authentication	Passed	
EWCJ179S_Reg_71	downgrade and upgrade impact	To verify config impact after downgrade and upgrade	Passed	

EWCJ179S_Reg_72	HA active to standby config impact	To verify config impact HA active to standby	Passed	
EWCJ179S_Reg_73	active to standby to active config impact	To verify config impact when active to standby to active	Passed	
EWCJ179S_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	
EWCJ179S_Reg_75	with mac filtering configured in AAA	To Configure mac filtering and verify client connectivity	Passed	
EWCJ179S_Reg_76	Change station id case and verify config impact "radius-server attribute wireless authentication call station Id Case upper/lower"	To Change station id case and verify config impact	Passed	

Capability to enable/disable 11ax features per SSID

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_119	Check the 11 ax enabling or not via GUI	To verify whether the 11 ax parameters enable or not via GUI	Passed	
EWLCJ179S_Reg_120	Check the 11 ax disabling or not via GUI	To verify whether the 11 ax parameters disable or not via GUI	Passed	
EWLCJ179S_Reg_121	Check the 11 ax enabling or not via CLI	To verify whether the 11 ax parameters enable or not via CLI	Passed	
EWLCJ179S_Reg_122	Check the 11 ax disabling or not via CLI	To verify whether the 11 ax parameters disable or not via CLI	Passed	
EWLCJ179S_Reg_123	Disabling 11 ax radio and checking the client connectivity	To check the client connectivity after disabling 11 ax	Passed	
EWLCJ179S_Reg_124	Checking the 11 ax parameters after AP reboot	To verify the 11 ax for after AP reboot	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_126	Verifying 11 ax parameters for different AP models	To Verify the 11 ax parameters for different AP models	Passed	
EWLCJ179S_Reg_127	Validating the 11ax parameters after disjoin the AP	To validate the 11 ax parameters for after Ap disjoin	Passed	
EWLCJ179S_Reg_128	Verifying the 11 ax parameters after deleting the client	To verify the 11 ax parameters for deleted client	Passed	

EWLCJ179S_Reg_129	monitoring the 11 ax parameters after AP provisioning from DNAC	To check the 11 ax parameters after AP provisioning from DNAC	Passed	
EWLCJ179S_Reg_130	Verifying the 11 ax parameters by deleting the SSID	To Verify the 11 ax parameters after Deleting SSID	Passed	
EWLCJ179S_Reg_131	Verifying the 11 ax parameters for intra roaming client	To Verify the 11 ax parameters after client roaming between AP's	Passed	
EWLCJ179S_Reg_132	Checking the 11 ax parameters for inter roaming client	To Verify the 11 ax parameters status after client roaming between controllers	Passed	
EWLCJ179S_Reg_133	Verifying the 11 ax status by changing the security type	To check the11 ax parameters after changing the security type	Passed	
EWLCJ179S_Reg_134	Validating the 11ax status for Virtual EWLC	To validate the 11 ax parameters for vEWLC	Passed	

CLI boot system statement needs clarification

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_736	Verify WORD option in boot config is removed or not	To verify WORD option in boot config is removed or not	Passed	
EWLCJ179S_Reg_737	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	
EWLCJ179S_Reg_738	Verify Local file system display files	To verify Local file system display files	Passed	
EWLCJ179S_Reg_739	Verify autocomplete filenames or filesystems in config	To verify autocomplete filenames or filesystems in config	Passed	
EWLCJ179S_Reg_740	Verify file system for remote file systems	To verify file system for remote file systems	Passed	
EWLCJ179S_Reg_741	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	
EWLCJ179S_Reg_742	Verify words given after the “boot system"	Verification for the Word given after the “boot system"	Passed	
EWLCJ179S_Reg_743	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
EWLCJ179S_Reg_702	Configure AP Packet Capture on 9800-40 Wireless Controller	To configure AP Packet Capture on 9800-40 Wireless Controller	Passed	
EWLCJ179S_Reg_703	Configure AP Packet Capture on 9800-80 Wireless Controller	To configure AP Packet Capture on 9800-80 Wireless Controller	Failed	CSCwc14069
EWLCJ179S_Reg_704	Configure AP Packet Capture on 9800-CL Wireless Controller	To configure AP Packet Capture on 9800-CL Wireless Controller	Passed	
EWLCJ179S_Reg_705	Configure AP Packet Capture on 9800 HA setup Wireless Controller	To configure AP Packet Capture on 9800 HA setup Wireless Controller	Passed	
EWLCJ179S_Reg_706	Verify packet capture when client moves between SSIDs	To verify packet capture when client moves between SSIDs	Passed	
EWLCJ179S_Reg_707	Verify packet capture when client roams between APs	To verify packet capture when client roams between APs	Passed	
EWLCJ179S_Reg_708	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	
EWLCJ179S_Reg_709	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	

EWLCJ179S_Reg_710	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	
EWLCJ179S_Reg_711	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	
EWLCJ179S_Reg_712	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	
EWLCJ179S_Reg_713	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	
EWLCJ179S_Reg_714	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	
EWLCJ179S_Reg_715	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	
EWLCJ179S_Reg_716	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	

EWLCJ179S_Reg_717	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	
EWLCJ179S_Reg_718	Capture EAP packets in AP - Windows	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ179S_Reg_719	Capture EAP packets in AP - Android	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ179S_Reg_720	Capture EAP packets in AP - IOS	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ179S_Reg_721	Capture EAP packets in AP - MAC	Capturing the EAP packets during client initial connection with AP	Passed	
EWLCJ179S_Reg_722	Capture EAP packets in AP - Surface Go	Capturing the EAP packets during client initial connection with AP	Passed	

Dot1x+EWA on mac Failure

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_135	Verifying the Dot1x+EWA support with mac failure.	To verify the Dot1x+EWA support with mac filter Configuration.	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_140	Verifying the Dot1x+EWA support with Wpa2 security mac failure	To verify the Dot1x+EWA Configuration with wpa2 supported SSID	Passed	
EWLCJ179S_Reg_141	Verifying the Dot1x+EWA support with Wpa3 security .	To verify the Dot1x+EWA Configuration with wpa3 supported SSID	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_145	Verifying the Dot1x+EWA support with Ft	To verify the Dot1x+EWA support with +Ft for the different clients.	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_147	Verifying the Dot1x+EWA security with Inter WLC Roaming	To verify inter WLC Roaming between WLANs with Dot1x+EWA support	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_153	Validate client association in DNAC	To verify client details showing or not in DANC	Passed	
EWLCJ179S_Reg_154	Validate client association in PI	To verify client details showing or not in PI	Passed	
EWLCJ179S_Reg_155	Configure wlan with EWA in DNAC & check client details in DNA space	To verify wlan created or not in DANC	Passed	
EWCJ179S_Reg_77	Create WLAN using WLAN wizard	To check whether Wlan able to create or not using WLAN Wizard option	Passed	
EWCJ179S_Reg_78	Check the client connectivity for created WLAN using WLAN Wizard	To Check the client connectivity using created WLAN in WLAN Wizard	Passed	
EWCJ179S_Reg_79	Checking the Client connectivity for Dot1x security	To verify whether the client connected with Dot1x security or not	Passed	
EWCJ179S_Reg_80	Create flex connect EWA and check the client connectivity	To check the client connectivity for flex connect EWA	Passed	
EWCJ179S_Reg_81	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Passed	
EWCJ179S_Reg_82	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Passed	

EWCJ179S_Reg_83	Verifying the Dot1x+EWA support with Wpa2 security mac failure	To verify the Dot1x+EWA Configuration with wpa2 supported SSID	Passed	
EWCJ179S_Reg_84	Verifying the Dot1x+EWA support with Wpa3 security .	To verify the Dot1x+EWA Configuration with wpa3 supported SSID	Passed	
EWCJ179S_Reg_85	Validating the Dot1x+EWA support and Layer 2 On Mac filter	To verify the Dot1x+EWA support and Layer3 On Mac filter failure	Passed	
EWCJ179S_Reg_86	Verifying the Dot1x+EWA support with Layer3 Splash page web redirect.	To verify the Dot1x+EWA support with Layer3 Splash page web redirect.	Passed	
EWCJ179S_Reg_87	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWCJ179S_Reg_88	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	
EWCJ179S_Reg_89	Configure Webauth on MAC failure with PSK	To verify the Webauth on MAC failure with PSK configuration	Passed	
EWCJ179S_Reg_90	Configure Webauth on MAC failure with dot1x	To verify the Webauth on MAC failure with Dot1x configuration	Passed	
EWCJ179S_Reg_91	Configure Webauth on MAC failure with FT dot1x	To verify the Webauth on MAC failure with FT Dot1x configuration	Passed	
EWCJ179S_Reg_92	Create wlan with dot1x +EWA security and check the inter roming	To verify the Intra roaming by using dot1x+EWA security	Passed	

EWCJ179S_Reg_93	Create wlan with dot1x+ EWA security and check the intra roming	To verify the Inter roaming by using dot1x+ EWA security	Passed	
EWCJ179S_Reg_94	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Passed	
EWCJ179S_Reg_95	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Passed	
EWCJ179S_Reg_96	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWCJ179S_Reg_97	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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_Reg_197	Configure AP via PNP workflow using EAP-TLS authentication	To configure AP via PNP workflow using EAP-TLS authentication	Passed	
EWLCJ179S_Reg_198	Configure AP via PNP workflow using EAP-PEAP authentication	To configure AP via PNP workflow using EAP-PEAP authentication	Passed	
EWLCJ179S_Reg_199	Configure AP via PNP workflow using EAP-FAST authentication	To configure AP via PNP workflow using EAP-FAST authentication	Passed	
EWLCJ179S_Reg_200	Configure 4800 AP via PNP workflow using EAP authentication	To configure 4800 AP via PNP workflow using EAP authentication	Passed	
EWLCJ179S_Reg_201	Configure 9120 AP via PNP workflow using EAP authentication	To configure 9120 AP via PNP workflow using EAP authentication	Passed	
EWLCJ179S_Reg_202	Configure 9115 AP via PNP workflow using EAP authentication	To configure 9115 AP via PNP workflow using EAP authentication	Passed	
EWLCJ179S_Reg_203	Configure 9105 AP via PNP workflow using EAP authentication	To configure 9105 AP via PNP workflow using EAP authentication	Passed	
EWLCJ179S_Reg_204	Configure 9130 AP via PNP workflow using EAP authentication	To configure 9130 AP via PNP workflow using EAP authentication	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_216	Check if standby interface status details changes upon AP addition	To check if standby interface status details changes upon AP addition	Passed	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_Reg_222	Configure HA setup using RP option.	To configure HA setup using RP option.	Passed	
EWLCJ179S_Reg_223	Validate the HA setup parameters.	To validate the HA setup parameters.	Passed	
EWLCJ179S_Reg_224	Unpairing HA setup using no RP-Method	To unpair the HA setup using no RP-Method	Passed	
EWLCJ179S_Reg_225	Configure HA SSO RMI	To Configure HA SSO RMI	Passed	
EWLCJ179S_Reg_226	Validate the HA RMI parameters.	To validate the HA RMI parameters.	Passed	
EWLCJ179S_Reg_227	Update RMI configuration in eWLC UI and check the output	To update RMI configuration in eWLC UI and check the output	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_229	Force-switchover to verify HA SSO RMI behaviour.	To verify HA SSO RMI behaviour on force-switchover.	Passed	
EWLCJ179S_Reg_230	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ179S_Reg_231	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ179S_Reg_232	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ179S_Reg_233	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	

EWLCJ179S_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	
EWLCJ179S_Reg_235	Force multiple switchover and verify AP & client association	To force multiple switchover and verify AP & client association	Passed	
EWLCJ179S_Reg_236	Validate licensing information after ISSU upgrade/downgrade	To validate licensing information after ISSU upgrade/downgrade	Passed	
EWLCJ179S_Reg_237	Validate licensing information after multiple switchover and reload	To validate licensing information after multiple switchover and reload	Passed	
EWLCJ179S_Reg_238	Clear RMI based configuration from UI	To clear RMI based configuration from UI	Passed	
EWLCJ179S_Reg_239	Clear RMI based configuration from CLI	To clear RMI based configuration from CLI	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_241	Verify HA setup details from Standby console	To verify HA setup details in Standby console	Passed	
EWLCJ179S_Reg_242	Check interfaces state from standby console	To check interfaces state from standby console	Passed	
EWLCJ179S_Reg_243	Check environment details from standby console	To monitor environment details from standby console	Passed	
EWLCJ179S_Reg_244	Check process usage details in standby console	To check process usage details in standby console	Passed	

EWLCJ179S_Reg_245	Monitor running process in Standby unit from Active unit console	To monitor running process in Standby unit from Active unit console	Passed	
EWLCJ179S_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
EWLCJ179S_Reg_247	Configure Radio monitoring	Verify the radio monitoring parameter configured or not	Passed	
EWLCJ179S_Reg_248	Configure AP monitoring	Verify the Ap monitoring parameter configured or not	Passed	
EWLCJ179S_Reg_249	Configure high CPU utilization	To Verify reload happen or not for high CPU utilization	Passed	
EWLCJ179S_Reg_250	Configure high memory utilization	To Verify reload happen or not for high memory utilization	Passed	
EWLCJ179S_Reg_251	Validate the AP disconnect reason code for high memory	Check the AP disconnect reason code if AP is showing high memory.	Passed	
EWLCJ179S_Reg_252	Validate the AP disconnect reason code for high CPU.	Check the AP disconnect reason code if AP is showing high CPU.	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_254	Configure different sampling periods.	Configure different sampling periods for AP CPU and high memory and verify if computation works fine.	Passed	

EWLCJ179S_Reg_255	Configure different threshold time	Configure different threshold values for AP CPU and high memory and verify if computation works fine.	Passed	
EWLCJ179S_Reg_256	NETCONF config data	Configure all AP system and radio monitoring via NETCONF	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_261	Validate the CPU and memory details in DNAC	Verify the radio , AP monitoring parameter details showing or not in DANC	Passed	
EWLCJ179S_Reg_262	Verify the client association during ap reload	Verify client connected or not after ap reload	Passed	

EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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 forsake OS Clients.	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_Reg_309	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWLCJ179S_Reg_310	Verifying clients roaming with different iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ179S_Reg_129	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	
EWCJ179S_Reg_130	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	
EWCJ179S_Reg_131	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	
EWCJ179S_Reg_132	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	

EWCJ179S_Reg_133	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	CSCwc14047
EWCJ179S_Reg_134	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	
EWCJ179S_Reg_135	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	
EWCJ179S_Reg_136	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	
EWCJ179S_Reg_137	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	
EWCJ179S_Reg_138	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	
EWCJ179S_Reg_139	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	

EWCJ179S_Reg_140	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	
EWCJ179S_Reg_141	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	
EWCJ179S_Reg_142	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	
EWCJ179S_Reg_143	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	
EWCJ179S_Reg_144	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	
EWCJ179S_Reg_145	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	

EWCJ179S_Reg_146	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	
EWCJ179S_Reg_147	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	
EWCJ179S_Reg_148	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	
EWCJ179S_Reg_149	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	
EWCJ179S_Reg_150	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	
EWCJ179S_Reg_151	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	
EWCJ179S_Reg_152	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	

EWCJ179S_Reg_153	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	
EWCJ179S_Reg_154	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	
EWCJ179S_Reg_155	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	
EWCJ179S_Reg_156	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	
EWCJ179S_Reg_157	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	
EWCJ179S_Reg_158	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	
EWCJ179S_Reg_159	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	

EWCJ179S_Reg_160	Verifying generation of iPSK tag with FT-PSK for same OS clients.	To verify whether iPSK generated or not when WLAN is enabled with FT-PSK for same OS Clients.	Passed	
EWCJ179S_Reg_161	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	
EWCJ179S_Reg_162	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	
EWCJ179S_Reg_163	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	
EWCJ179S_Reg_164	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	
EWCJ179S_Reg_165	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	

EWCJ179S_Reg_166	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	
EWCJ179S_Reg_167	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	
EWCJ179S_Reg_168	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	
EWCJ179S_Reg_169	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	
EWCJ179S_Reg_170	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	

EWCJ179S_Reg_171	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	
EWCJ179S_Reg_172	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	
EWCJ179S_Reg_173	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	
EWCJ179S_Reg_174	Verifying clients roaming with same iPSK tag	To verify whether the client is roaming from one Ap to another Ap.	Passed	
EWCJ179S_Reg_175	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
EWLCJ179S_Reg_311	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWCJ179S_Reg_176	Configure a WLAN and verify LAA default setting	To Configure a WLAN and verify LAA default setting	Passed	
EWCJ179S_Reg_177	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	
EWCJ179S_Reg_178	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	
EWCJ179S_Reg_179	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	
EWCJ179S_Reg_180	Enable LAA in WLAN and connect iPhone with LAA	To verify connectivity after enabling LAA in WLAN and connect iPhone with LAA	Passed	
EWCJ179S_Reg_181	Enable LAA in WLAN and connect Windows with LAA	To verify connectivity after enabling LAA in WLAN and connect Windows with LAA	Passed	

EWCJ179S_Reg_182	Enable LAA in WLAN and connect Android with LAA	To verify connectivity after enabling LAA in WLAN and connect Android with LAA	Passed	
EWCJ179S_Reg_183	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	
EWCJ179S_Reg_184	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	
EWCJ179S_Reg_185	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	
EWCJ179S_Reg_186	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	

EWCJ179S_Reg_187	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	
EWCJ179S_Reg_188	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	
EWCJ179S_Reg_189	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	
EWCJ179S_Reg_190	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	

EWCJ179S_Reg_191	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	
EWCJ179S_Reg_192	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	
EWCJ179S_Reg_193	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	
EWCJ179S_Reg_194	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	
EWCJ179S_Reg_195	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
EWLCJ179S_Reg_329	Configure Link Local Bridging policy profile configuration via CLI	To configure Link Local Bridging policy profile configuration via CLI	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_331	Enabling Link Local Bridging policy profile configuration via UI	To enabling Link Local Bridging policy profile configuration via UI	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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 from 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	
EWLCJ179S_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 from 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	

EWLCJ179S_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 from 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	
EWLCJ179S_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 from 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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_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	
EWLCJ179S_Reg_348	Configure AP Provisioning to check MAC Address consistency	To Configure Ap Provisioning to check MAC Address consistency	Passed	
EWLCJ179S_Reg_349	Configure Ap tag to check MAC Address consistency	To Configure Ap tag to check MAC Address consistency	Passed	
EWLCJ179S_Reg_350	Configure Policy Map to check MAC Address consistency	To Configure Policy Map to check MAC Address consistency	Passed	
EWLCJ179S_Reg_351	Configure Device authentication to check MAC Address consistency	To Configure Device authentication to check MAC Address consistency	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_353	Configure Excluded clients to check MAC Address consistency	To configure Excluded clients to check MAC Address consistency	Passed	
EWLCJ179S_Reg_354	Configure Radioactive trace to check MAC Address consistency	To configure Radioactive trace to check MAC Address consistency	Passed	
EWLCJ179S_Reg_355	Configure packet tracer to check MAC Address consistency	To configure Packet tracer to check MAC Address consistency	Passed	

EWLCJ179S_Reg_356	Configure Ap Join to check MAC Address consistency	To Configure Ap Join to check MAC Address consistency	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_359	Configure client whitelisting to check MAC Address consistency	To Configure client whitelisting to check MAC Address consistency	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_362	Configure when eWC1 is down AP should join to eWC2	To Configure when eWC1 is down AP should join to eWC2	Passed	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWCJ179S_Reg_196	Configure Excluded clients by using mac_address consistency	To Configure Excluded clients by using mac_address consistency	Passed	
EWCJ179S_Reg_197	Configure Radioactive trace by using mac_address consistency	To Configure Radioactive trace by using mac_address consistency	Passed	
EWCJ179S_Reg_198	Configure packet tracer by using mac_address consistency	To Configure Packet tracer by using mac_address consistency	Passed	
EWCJ179S_Reg_199	Configure Ap Provisioning by using mac_address consistency	To Configure Ap Provisioning by using mac_address consistency	Passed	
EWCJ179S_Reg_200	Configure Ap tag by using mac_address consistency	To Configure Ap tag by using mac_address consistency	Passed	

EWCJ179S_Reg_201	Configure Policy Map by using mac_address consistency	To Configure Policy Map by using mac_address consistency	Passed	
EWCJ179S_Reg_202	Configure Device authentication by using mac_address consistency	To Configure Device authentication by using mac_address consistency	Passed	
EWCJ179S_Reg_203	Configure Device authentication through CSV file by using mac_address consistency	To Configure Device authentication through CSV file by using mac_address consistency	Passed	
EWCJ179S_Reg_204	Configure Ap Join by using mac_address consistency	To Configure Ap Join by using mac_address consistency	Passed	CSCwb92214
EWCJ179S_Reg_205	Configure Mac filtering windows client connection by using mac_address consistency	To Configure Mac filtering windows client connection by using mac_address consistency	Passed	
EWCJ179S_Reg_206	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	Passed	
EWCJ179S_Reg_207	Configure client whitelisting by using mac_address consistency	To Configure client whitelisting by using mac_address consistency	Passed	
EWCJ179S_Reg_208	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	
EWCJ179S_Reg_209	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	

EWCJ179S_Reg_210	Configure when eWC1 is down AP should join to eWC2	To Configure when eWC1 is down AP should join to eWC2	Passed	
EWCJ179S_Reg_211	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	
EWCJ179S_Reg_212	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	
EWCJ179S_Reg_213	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	
EWCJ179S_Reg_214	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	
EWCJ179S_Reg_215	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	
EWCJ179S_Reg_216	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	
EWCJ179S_Reg_217	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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

Need support for TrustSec SGT inline tagging over port channel uplink

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_723	Check if inline tagging is configured in Trustsec	To check if inline tagging is configured in Trustsec	Passed	
EWLCJ179S_Reg_724	Enforce trustsec tagging using 9800-40 controller	To enforce trustsec tagging using 9800-40 controller	Passed	
EWLCJ179S_Reg_725	Enforce trustsec tagging using 9800L controller	To enforce trustsec tagging using 9800L controller	Passed	
EWLCJ179S_Reg_726	Enforce trustsec tagging using 9800CL controller	To enforce trustsec tagging using 9800CL controller	Passed	
EWLCJ179S_Reg_727	Enforce trustsec tagging using 9800 HA controller	To enforce trustsec tagging using 9800 HA controller	Passed	
EWLCJ179S_Reg_728	Enforce trustsec tagging using EWC controller	To enforce trustsec tagging using EWC controller	Passed	
EWLCJ179S_Reg_729	Check trustsec enforcement using WLAN with WPA3 security	To check trustsec enforcement using WLAN with WPA3 security	Passed	
EWLCJ179S_Reg_730	Check trustsec enforcement using WLAN with WPA2 security	To check trustsec enforcement using WLAN with WPA2 security	Passed	
EWLCJ179S_Reg_731	Check trustsec enforcement with Windows client	To check trustsec enforcement with Windows client	Passed	
EWLCJ179S_Reg_732	Check trustsec enforcement with Mac client	To check trustsec enforcement with MAC client	Passed	
EWLCJ179S_Reg_733	Check trustsec enforcement with Android client	To check trustsec enforcement with Android client	Passed	

EWLCJ179S_Reg_734	Check trustsec enforcement with roaming client	To check trustsec enforcement with roaming client	Passed	
EWLCJ179S_Reg_735	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
EWLCJ179S_Reg_370	Configure an Access Control List for Split Tunnelling	To configure an Access Control List for Split Tunnelling	Passed	
EWLCJ179S_Reg_371	Link ACL Policy to the Defined ACL	To link ACL Policy to the Defined ACL	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_373	Configure Office Extend AP through GUI	To configure Office Extend AP through GUI	Passed	
EWLCJ179S_Reg_374	Configure Office Extend AP through CLI	To configure Office Extend AP through CLI	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_376	Connect Windows Client for Office Extend AP	To connect Windows Client for Office Extend AP	Passed	
EWLCJ179S_Reg_377	Connect Android Client for Office Extend AP	To connect Android Client for Office Extend AP	Passed	
EWLCJ179S_Reg_378	Connect Go Plus Client for Office Extend AP	To connect Go Plus Client for Office Extend AP	Passed	
EWLCJ179S_Reg_379	Connect MAC Client for Office Extend AP	To connect MAC Client for Office Extend AP	Passed	
EWLCJ179S_Reg_380	Connect IOS Client for Office Extend AP	To connect IOS Client for Office Extend AP	Passed	
EWLCJ179S_Reg_381	Verify Locally switched traffic using Packet Capture	To verify Locally switched traffic using Packet Capture	Passed	

EWLCJ179S_Reg_382	Connect any client through centralized SSID	To connect any client through centralized SSID	Passed	
EWLCJ179S_Reg_383	Verify Office Extend AP details	To verify Office Extend AP details	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_388	Verify MAC Filtering for Office Extend Access Point	To verify MAC Filtering for Office Extend Access Point	Passed	

Per AP Group NTP Server Config

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	Passed	
EWLCJ179S_Reg_395	Modify AP Time zone using Controller	To modify AP Time zone using Controller	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_Reg_407	Verify alerts are displayed for critical events	To Verify alerts are displayed for critical events	Passed	
EWLCJ179S_Reg_408	Verify alerts are displayed for alert events	To Verify alerts are displayed for alert events	Passed	
EWLCJ179S_Reg_409	Verify alerts are displayed for emergency events	To Verify alerts are displayed for emergency events	Passed	
EWLCJ179S_Reg_410	Export syslog events	To Export syslog events from webui	Passed	
EWLCJ179S_Reg_411	Verify user able to filter options	To Verify user able to filter syslog messages	Passed	
EWLCJ179S_Reg_412	Disable Event banner	To Disable Event banner using preference	Passed	
EWLCJ179S_Reg_413	Enable Event banner	To Enable Event banner using preference	Passed	
EWLCJ179S_Reg_414	Delete an Event Notification	To Delete an Event Notification	Passed	
EWLCJ179S_Reg_415	Delete multiple/all Event Notification	To Delete multiple/all Event Notification	Passed	
EWLCJ179S_Reg_416	Verify Event count in Pie chart	To Verify Event count are properly shown in Pie chart	Passed	
EWLCJ179S_Reg_417	Force Switchover in HA and verify alerts are shown	To Force Switchover in HA and verify alerts are shown	Passed	
EWLCJ179S_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
EWLCJ179S_Reg_419	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Passed	
EWLCJ179S_Reg_420	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWLCJ179S_Reg_421	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWLCJ179S_Reg_422	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	
EWLCJ179S_Reg_423	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_425	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWLCJ179S_Reg_426	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWLCJ179S_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	

EWLCJ179S_Reg_428	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWLCJ179S_Reg_429	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWLCJ179S_Reg_430	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWLCJ179S_Reg_431	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWLCJ179S_Reg_432	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	
EWLCJ179S_Reg_433	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWLCJ179S_Reg_434	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	
EWCJ179S_Reg_247	Creating Wlan with WPA2 Security with MPSK	Verify Wlan Creating with WPA2 Security with MPSK	Failed	CSCwc18806
EWCJ179S_Reg_248	Edit WPA2 Security PSK Keys on MPSK	Verify Wlan Edit with WPA2 Security with MPSK	Passed	
EWCJ179S_Reg_249	Delete WPA2 Security PSK Keys on MPSK	Verify Wlan Delete with WPA2 Security with MPSK	Passed	
EWCJ179S_Reg_250	Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Verify Creating Wlan with WPA2 Security with MPSK - Format with Hexa:	Passed	

EWCJ179S_Reg_251	Creating Wlan with WPA2 Security with MPSK - Password Type : AES :	Verify the Security Type with Advance Security	Passed	
EWCJ179S_Reg_252	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	
EWCJ179S_Reg_253	Connect the MAC Clients	Verify Connect the MAC Clients with all the 5 Key Combinations	Passed	
EWCJ179S_Reg_254	Connect the Android Clients	Verify Connect the Android Clients with all the 5 Key Combinations:	Passed	
EWCJ179S_Reg_255	Connect the Apple Mobile Clients with all the 5 Key Combinations:	Verify Connect the Apple Clients with all the 5 Key Combinations:	Passed	
EWCJ179S_Reg_256	Connect the Windows Clients with all the 5 Key Combinations:	Verify Connect the Windows Clients with all the 5 Key Combinations:	Passed	
EWCJ179S_Reg_257	MPSK with Ap Model 9115	Verify the Configurations with Ap Different Ap Model 9115	Passed	
EWCJ179S_Reg_258	Connect Ap Model 9120	Verify the Configurations with Ap Different Ap Model 9120:	Passed	
EWCJ179S_Reg_259	Connect Ap Model 4800	Verify the Configurations with Ap Different Ap Model 4800:	Passed	
EWCJ179S_Reg_260	Connect Ap Model 3800	Verify the Configurations with Ap Different Ap Model 3800	Passed	

EWCJ179S_Reg_261	Connect Ap Model 3700	Verify the Configurations with Ap Different Ap Model 3700	Passed	
EWCJ179S_Reg_262	Connect Ap Model 1532	Verify the Configurations with Ap Different Ap Model 1532:	Passed	

Regulatory Domain Reduction

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_435	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWLCJ179S_Reg_436	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWLCJ179S_Reg_437	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWLCJ179S_Reg_438	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWLCJ179S_Reg_439	Verify country code is changed for access point	To verify country code is changed for access point	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_443	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	
EWLCJ179S_Reg_444	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	

EWLCJ179S_Reg_445	Verify at least one Regulatory Domain is configured or not	To verify at least one Regulatory Domain is configured or not	Passed	
EWLCJ179S_Reg_446	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Passed	
EWLCJ179S_Reg_447	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWLCJ179S_Reg_448	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	
EWLCJ179S_Reg_449	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWLCJ179S_Reg_450	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWLCJ179S_Reg_451	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWLCJ179S_Reg_452	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	
EWLCJ179S_Reg_453	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	
EWLCJ179S_Reg_454	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	
EWLCJ179S_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	

EWLCJ179S_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	
EWCJ179S_Reg_263	Verify whether supported countries are showing properly or not	To verify whether supported countries are showing properly or not	Passed	
EWCJ179S_Reg_264	Verify whether configured countries are showing properly or not	To verify whether configured countries are showing properly or not	Passed	
EWCJ179S_Reg_265	Configure Regulatory Domain Country code	To configure Regulatory Domain Country code	Passed	
EWCJ179S_Reg_266	Configure multiple Countries and assign country code to access point	To configure multiple Countries and assign country code to access point	Passed	
EWCJ179S_Reg_267	Verify country code is changed for access point	To verify country code is changed for access point	Passed	
EWCJ179S_Reg_268	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	
EWCJ179S_Reg_269	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	
EWCJ179S_Reg_270	Verify AP joins to other eWLC with another country code supported	To verify AP joins to other eWLC with another country code supported	Passed	
EWCJ179S_Reg_271	Verify eWLC reboot to retain the country code	To verify eWLC reboot to retain the country code	Passed	

EWCJ179S_Reg_272	Verify non-regulatory country code change	To verify non-regulatory country code change	Passed	
EWCJ179S_Reg_273	Verify at least one Regulatory Domain is configured or not	To verify at least one Regulatory Domain is configured or not	Passed	
EWCJ179S_Reg_274	Associate Windows client to AP with Regulatory country code	To associate Windows client to AP with Regulatory country code	Passed	
EWCJ179S_Reg_275	Associate Android client to AP with Regulatory country code	To associate Android client to AP with Regulatory country code	Passed	
EWCJ179S_Reg_276	Associate MAC client to AP with Regulatory country code	To associate MAC client to AP with Regulatory country code	Passed	
EWCJ179S_Reg_277	Associate IOS client to AP with Regulatory country code	To associate IOS client to AP with Regulatory country code	Passed	
EWCJ179S_Reg_278	Associate Surface client to AP with Regulatory country code	To associate Surface client to AP with Regulatory country code	Passed	
EWCJ179S_Reg_279	Verify PID values once configured Regulatory Domain	To verify PID values once configured Regulatory Domain	Passed	
EWCJ179S_Reg_280	Verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	To verify Packet Capture, Ping and Traffic after configuring Regulatory Domain	Passed	
EWCJ179S_Reg_281	Verify Radio Operation status of AP	To verify Radio Operation status of AP	Passed	
EWCJ179S_Reg_282	Day 0 configuration when no country code configured	To do Day 0 configuration when no country code configured	Passed	

EWCJ179S_Reg_283	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	
EWCJ179S_Reg_284	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	

SFP support with C9800

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_689	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	
EWLCJ179S_Reg_690	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	
EWLCJ179S_Reg_691	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	
EWLCJ179S_Reg_692	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	
EWLCJ179S_Reg_693	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	
EWLCJ179S_Reg_694	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	
EWLCJ179S_Reg_695	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	

EWLCJ179S_Reg_696	Connecting different SFP in9800-L eWLC	To connect a SFP in eWLC9800-L and check if the SFP is detected or not.	Passed	
EWLCJ179S_Reg_697	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	
EWLCJ179S_Reg_698	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	
EWLCJ179S_Reg_699	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	
EWLCJ179S_Reg_700	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	
EWLCJ179S_Reg_701	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	

SmartLicensing

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_457	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ179S_Reg_458	Enable Smart Licensing and Register Device	To enable Smart Licensing and Register Device	Passed	
EWLCJ179S_Reg_459	Smart License Reservation	To perform Smart License Reservation and verify details	Passed	
EWLCJ179S_Reg_460	Deleting SLR Licenses	To verify by deleting SLR Licenses	Passed	
EWLCJ179S_Reg_461	Smart Licensing HA Support	To verify Smart Licensing for HA Support	Passed	
EWLCJ179S_Reg_462	Change a SLR on a C9800 SSO HA pair	To change a SLR on a C9800 SSO HA pair	Passed	
EWLCJ179S_Reg_463	Removing SLR from a C9800 SSO HA pair	To verify by removing SLR from a C9800 SSO HA pair	Passed	
EWLCJ179S_Reg_464	Validate license info in HA SSO RMI pair	To validate license info in HA SSO RMI pair	Passed	
EWLCJ179S_Reg_465	Validate license info on Standby unit directly	To validate license info on standby unit directly	Passed	
EWLCJ179S_Reg_466	Validate license info after ISSU upgrade	To validate license info after ISSU upgrade	Passed	
EWLCJ179S_Reg_467	Validate license info after multiple switchover	To validate license info after multiple switchover	Passed	
EWLCJ179S_Reg_468	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	

EWCJ179S_Reg_303	Smart Account Creation, registration and activation.	To verify smart Account Creation, registration and activation.	Passed	
EWCJ179S_Reg_304	Generate token from CSSM	To Generate token from CSSM	Passed	
EWCJ179S_Reg_305	Product instance direct-connect using trust token	To verify Product instance direct-connect using trust token	Passed	
EWCJ179S_Reg_306	verify device status in CSSM	To verify device status in CSSM	Passed	
EWCJ179S_Reg_307	verify Smart Licensing Support in eWC HA	To verify Smart Licensing Support in eWC HA	Passed	
EWCJ179S_Reg_308	verify device details and license count changes in CSSM	To verify device details and license count changes in CSSM	Passed	
EWCJ179S_Reg_309	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	
EWCJ179S_Reg_310	Validate license info after switchover in AP	To validate license info after switchover in AP	Passed	
EWCJ179S_Reg_311	Validate license info on multiple reload	To validate license info on multiple reboot	Passed	
EWCJ179S_Reg_312	Install CSLU and add device and check status	Install CSLU and add device and check status	Passed	
EWCJ179S_Reg_313	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
EWLCJ179S_Reg_469	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWLCJ179S_Reg_470	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWLCJ179S_Reg_471	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	
EWLCJ179S_Reg_472	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_Reg_485	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWLCJ179S_Reg_486	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWLCJ179S_Reg_487	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWLCJ179S_Reg_488	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_490	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ179S_Reg_491	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	
EWLCJ179S_Reg_492	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWLCJ179S_Reg_493	Limit the client by radio policy	To verify the no of client associate with particular radio policy	Passed	
EWCJ179S_Reg_314	Associate client to 5 GHz radio policy with slot 0	To verify slot details shown or not	Passed	
EWCJ179S_Reg_315	Associate client to 5 GHz radio policy with slot 1	To verify slot details shown or not	Passed	
EWCJ179S_Reg_316	Associate client to 5 GHz radio policy with slot 2	To verify slot details shown or not	Passed	

EWCJ179S_Reg_317	Creating WLAN with 6 GHz radio policy	To Validate client details with 6 GHz radio	Passed	
EWCJ179S_Reg_318	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	
EWCJ179S_Reg_319	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	
EWCJ179S_Reg_320	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	
EWCJ179S_Reg_321	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	
EWCJ179S_Reg_322	Associating Ms-go client to 9115 Ap with WPA3 security type for 5GHz radio policy	To associate the client and verifying EDCA parameter	Passed	
EWCJ179S_Reg_323	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	
EWCJ179S_Reg_324	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	

EWCJ179S_Reg_325	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	
EWCJ179S_Reg_326	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	
EWCJ179S_Reg_327	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	
EWCJ179S_Reg_328	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	
EWCJ179S_Reg_329	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	
EWCJ179S_Reg_330	Perform inter roaming across different radio policy	To verify radio policy details after inter roaming	Passed	
EWCJ179S_Reg_331	Perform intra roaming across different radio policy	To verify radio policy details after intra roaming	Passed	
EWCJ179S_Reg_332	Perform IRCM across different radio policy	To verify radio policy details after IRCM	Passed	
EWCJ179S_Reg_333	Validate radio policy details in PI	To verify radio policy details after config pushed to PI	Passed	

EWCJ179S_Reg_334	Validate 2.4 GHz radio policy details in DNAC	To verify 2.4 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ179S_Reg_335	Validate 5 GHz radio policy details in DNAC	To verify 5 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ179S_Reg_336	Validate 6 GHz radio policy details in DNAC	To verify 6 GHz radio policy details after config pushed to DNAC	Passed	
EWCJ179S_Reg_337	Validate stots of radio policy in CMX	To verify 5 GHz radio slots difference in CMX	Passed	
EWCJ179S_Reg_338	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
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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
EWLCJ179S_Reg_606	Configure Open rrm and enable connectivity to kairos cloud	To configure Open rrm and enable connectivity to kairos cloud	Passed	
EWLCJ179S_Reg_607	Configure Open rrm and test for 5ghz band	To configure Open rrm and for 5ghz band	Passed	
EWLCJ179S_Reg_608	Configure Open rrm and test for 2.4ghz band	To configure Open rrm and test for 2.4ghz band	Passed	
EWLCJ179S_Reg_609	Configure Open rrm with WPA3 security	To configure Open rrm with WPA3 security	Passed	
EWLCJ179S_Reg_610	Configure Open rrm with WPA2 security	To configure Open rrm with WPA2 security	Passed	
EWLCJ179S_Reg_611	Configure Open rrm and test with android client	To configure Open rrm and test with android client	Passed	
EWLCJ179S_Reg_612	Configure Open rrm and test with iphone client	To configure Open rrm and test with iphone client	Passed	
EWLCJ179S_Reg_613	Configure Open rrm and test with Mac client	To configure Open rrm and test with Mac client	Passed	
EWLCJ179S_Reg_614	Configure Open rrm and test with Surface client	To configure Open rrm and test with Surface client	Passed	
EWLCJ179S_Reg_615	Configure Open rrm and test with Windows client	To configure Open rrm and test with Windows client	Passed	
EWLCJ179S_Reg_616	Configure Open rrm and test with only FRA enabled	To configure Open rrm and test with only FRA enabled	Passed	
EWLCJ179S_Reg_617	Configure Open rrm and test with only DCA enabled	To configure Open rrm and test with only DCA enabled	Passed	

EWLCJ179S_Reg_618	Configure Open rrm and test with only TPC enabled	To configure Open rrm and test with only TPC enabled	Passed	
EWLCJ179S_Reg_619	Configure Open rrm and test with only DBS enabled	To configure Open rrm and test with only DBS enabled	Passed	
EWLCJ179S_Reg_620	Configure Open rrm and test with different RF algorithm combinations	To configure Open rrm and test with different RF algorithm combinations	Passed	
EWLCJ179S_Reg_621	Configure Open rrm and test with manually assigned channel bandwidth and channel nos	To configure Open rrm and test with manually assigned channel bandwidth and channel nos	Passed	
EWLCJ179S_Reg_622	Configure Open rrm and test with 9115, 9120, 9130 AP	To configure Open rrm and test with 9115, 9120, 9130 AP	Passed	
EWLCJ179S_Reg_623	Configure Open rrm and test with 4800 AP	To configure Open rrm and test with 4800 AP	Passed	
EWLCJ179S_Reg_624	Configure Open rrm and test with eWLC HA	To configure Open rrm and test with eWLC HA	Passed	
EWLCJ179S_Reg_625	Configure Open rrm and test with EWC	To configure Open rrm and test with EWC	Passed	

Support 11k/v across wncd instances

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_513	Configure and verify 11v BSS Transition Management	To configure and verify 11v BSS Transition Management	Passed	
EWLCJ179S_Reg_514	Configure and verify 11v BSS Transition Management through CLI	To configure and verify 11v BSS Transition Management through CLI	Passed	
EWLCJ179S_Reg_515	Configure and verify 11k Beacon Radio Measurement	To configure and verify 11k Beacon Radio Measurement	Passed	
EWLCJ179S_Reg_516	Configure and verify 11k Beacon Radio Measurement through CLI	To configure and verify 11k Beacon Radio Measurement through CLI	Passed	
EWLCJ179S_Reg_517	Verify 802.11k Information Elements in Wireshark	To verify 802.11k Information Elements in Wireshark	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_520	Connect Windows Client and verify 11kv parameters in Wireshark	To connect Windows Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ179S_Reg_521	Connect Android Client and verify 11kv parameters in Wireshark	To connect Android Client and to verify 11kv parameters in Wireshark	Passed	

EWLCJ179S_Reg_522	Connect MAC Client and verify 11kv parameters in Wireshark	To connect MAC Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ179S_Reg_523	Connect IOS Client and verify 11kv parameters in Wireshark	To connect IOS Client and to verify 11kv parameters in Wireshark	Passed	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_528	Verify 11kv neighbour list when one radio is disabled	To verify 11kv neighbour list when one radio is disabled	Passed	
EWLCJ179S_Reg_529	Verify 11kv elements in omni peek and check the frames	To verify 11kv elements in omni peek and check the frames	Passed	
EWLCJ179S_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	
EWCJ179S_Reg_339	Configuring 802.11v BSS Transition Management in GUI	To Verify Configured 802.11v BSS Transition Management in GUI	Passed	

EWCJ179S_Reg_340	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	
EWCJ179S_Reg_341	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	
EWCJ179S_Reg_342	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	
EWCJ179S_Reg_343	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	
EWCJ179S_Reg_344	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	
EWCJ179S_Reg_345	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	
EWCJ179S_Reg_346	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	
EWCJ179S_Reg_347	Connect Android Client and verify 11kv parameters in Wireshark	To connect Android Client and to verify 11kv parameters in Wireshark	Passed	

EWCJ179S_Reg_348	Connect MAC Client and verify 11kv parameters in Wireshark	To connect MAC Client and to verify 11kv parameters in Wireshark	Passed	
EWCJ179S_Reg_349	Connect IOS Client and verify 11kv parameters in Wireshark	To connect IOS Client and to verify 11kv parameters in Wireshark	Passed	
EWCJ179S_Reg_350	Connect Windows Client and verify 11kv parameters in Wireshark	To connect Windows Client and verify 11kv parameters in Wireshark	Passed	
EWCJ179S_Reg_351	Verify 11k/11v, with one wncd, the candidate list is proper.	To verify 11k/11v, with one wncd, the candidate list is proper.	Passed	
EWCJ179S_Reg_352	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	
EWCJ179S_Reg_353	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
EWLCJ179S_Reg_531	Verify Client delete reason code for Webauth timer expiry when AP is in Local mode	LWA webauth timer expire	Passed	
EWLCJ179S_Reg_532	Verify Client delete reason code for Webauth timer expiry when AP is in Flex mode	LWA webauth timer expire	Passed	
EWLCJ179S_Reg_533	Verify Client delete reason code for Mac filtering	MAB authentication failed for Wireless client	Passed	
EWLCJ179S_Reg_534	Verify Client delete reason code for Mac filtering when AP is in Flex mode	MAB authentication failed for Wireless client	Passed	
EWLCJ179S_Reg_535	Verify Client delete reason code for Wrong PSK	To verify Client delete reason code for Wrong PSK	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_537	Verify Client delete reason code for dot1x timer expired	Deleting the client due to the expiry dot1x timer	Passed	
EWLCJ179S_Reg_538	Verify Client Manually Excluded with reason code	To verify Client Manually Excluded with reason code	Passed	
EWLCJ179S_Reg_539	Verify Client delete reason code for VLAN mismatch	To verify Client delete reason code for VLAN mismatch	Passed	

EWLCJ179S_Reg_540	Verify Android client delete reason code for dot1x authentication failure	Deleting the Android client due to the dot1x authentication failure	Passed	
EWLCJ179S_Reg_541	Verify Windows client delete reason code for dot1x authentication failure	Deleting the Windows client due to dot1x authentication failure	Passed	
EWLCJ179S_Reg_542	Verify IOS client delete reason code for dot1x authentication failure	Deleting the IOS client due to dot1x authentication failure	Passed	
EWLCJ179S_Reg_543	Verify Surface client delete reason code for dot1x authentication failure	Deleting the Surface client due to dot1x authentication failure	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_545	Verify syslog when client connected with run state	To verify syslog when client connected with run state	Passed	
EWLCJ179S_Reg_546	Verify Client delete reason code for IP learn state	To verify Client delete reason code for IP learn state	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_548	Configure Roaming between controllers and verify client delete reason	To configure Roaming between controllers and verify client delete reason	Passed	

EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_551	Verify Client delete reason CO_ CLIENT_ DELETE_ REASON_ MN_AP_ IPLEARN_ TIMEOUT	Client failed to get IP within this period	Passed	
EWLCJ179S_Reg_552	Verify Client delete reason code for Wired LAN	Deleting the clients connected to a port	Passed	
EWCJ179S_Reg_363	Validate the client delete reason after changing AP mode	To validate the client delete reason after changing AP mode	Passed	
EWCJ179S_Reg_364	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	
EWCJ179S_Reg_365	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	

EWCJ179S_Reg_366	Checking the client delete reason after expire the webauth timer	To validate the client delete reason after expire the webauth timer	Passed	
EWCJ179S_Reg_367	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	
EWCJ179S_Reg_368	Validate the client delete reason after MAB authentication failed	To validate the client delete reason after MAB authentication failed	Passed	
EWCJ179S_Reg_369	Checking the client delete reason after expire dot1x timer	To check the client delete reason after expire dot1x timer	Passed	
EWCJ179S_Reg_370	Validate the client delete reason after client failed to get IP	To validate the client delete reason after client failed to get IP	Passed	
EWCJ179S_Reg_371	Verifying the Android client delete reason after eap timer expires	To validate the Android client delete reason after eap timer expires	Passed	
EWCJ179S_Reg_372	Verifying the Windows client delete reason after eap timer expires	To validate the windows client delete reason after eap timer expires	Passed	
EWCJ179S_Reg_373	Validating the client delete reason when Authentication response rejected	To verify the client delete reason when Authentication response rejected	Passed	
EWCJ179S_Reg_374	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	

EWCJ179S_Reg_375	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	
EWCJ179S_Reg_376	Verifying the Samsung S10 client delete reason after eap timer expires	To validate the Samsung S10 client delete reason after eap timer expires	Passed	
EWCJ179S_Reg_377	Verifying the iPhone client delete reason after eap timer expires	To validate the iPhone client delete reason after eap timer expires	Passed	
EWCJ179S_Reg_378	Verifying the Surface Go client delete reason after eap timer expires	To validate the Surface Go client delete reason after eap timer expires	Passed	
EWCJ179S_Reg_379	Verifying the IOS client delete reason after eap timer expires	To validate the IOS client delete reason after eap timer expires	Passed	
EWCJ179S_Reg_380	Verifying the Client delete reason due to FT roaming failure	To verify the Client delete reason due to FT roaming failure	Passed	
EWCJ179S_Reg_381	Verify alert triggered in Alarms & Events in PI	To verify alert triggered in Alarms & Events in PI	Passed	
EWCJ179S_Reg_382	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
EWLCJ179S_Reg_626	Configure eWLC with AP and verify CLI output	To configure eWLC with AP and verify CLI output	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_628	Configure eWLC with AP and verify CLI output for 5Ghz	To configure eWLC with AP and verify CLI output for 5Ghz	Passed	
EWLCJ179S_Reg_629	Configure eWLC with AP and verify CLI output for 6Ghz	To configure eWLC with AP and verify CLI output for 6Ghz	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_631	Verify CLI command output details in 9800L	To verify CLI command output details in 9800L	Passed	
EWLCJ179S_Reg_632	Verify CLI command output details in 9800CL	To verify CLI command output details in 9800CL	Passed	
EWLCJ179S_Reg_633	Verify CLI command output details in 9800-40/80	To verify CLI command output details in 9800-40/80	Passed	
EWLCJ179S_Reg_634	Verify CLI command output details in 9800 HA platform	To verify CLI command output details in 9800 HA platform	Passed	
EWLCJ179S_Reg_635	Verify CLI command output details in EWC device	To verify CLI command output details in EWC device	Passed	
EWLCJ179S_Reg_636	Verify CLI command output details in EWC HA device	To verify CLI command output details in EWC HA device	Passed	

EWLCJ179S_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	
EWLCJ179S_Reg_638	Disable 5Ghz network and check the CLI output	To disable 5Ghz network and check the CLI output	Passed	
EWLCJ179S_Reg_639	Disable 6Ghz network and check the CLI output	To disable 6Ghz network and check the CLI output	Passed	
EWLCJ179S_Reg_640	Disable 2.4Ghz network and check the CLI output	To disable 2.4Ghz network and check the CLI output	Passed	

WebUI: WLAN/AAA/ACL Simplication

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_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	
EWLCJ179S_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	
EWLCJ179S_Reg_555	Configuring Dot1x Security & checking the Authentication list via CLI	To configure Dot1x Security & validate the Authentication list via CLI	Passed	
EWLCJ179S_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	
EWLCJ179S_Reg_557	Validating AAA parameters in Local mode LWA	To Validate the AAA parameters in Local mode LWA	Passed	
EWLCJ179S_Reg_558	Checking the client connectivity for Local mode EWA	To check the client connectivity for local mode EWA	Passed	
EWLCJ179S_Reg_559	Checking the parameter Map for Local mode EWA	To check the parameter map for local mode EWA	Passed	
EWLCJ179S_Reg_560	Connect the windows client with local mode CWA	To check the windows client connectivity for local mode CWA	Passed	
EWLCJ179S_Reg_561	Creating user group for Local mode CWA	To create User group for Local mode CWA	Passed	
EWLCJ179S_Reg_562	Checking the client connectivity for flex connect LWA	To check whether the client connected with flex connect LWA or not	Passed	

EWLCJ179S_Reg_563	Validate the client connectivity for flex connect EWA	To validate whether the client connected with flex connect EWA or not	Passed	
EWLCJ179S_Reg_564	Mapping ACL policy in Flex connect EWA	To map the ACL policy in flex connect EWA	Passed	
EWLCJ179S_Reg_565	Monitor the client connectivity for flex connect CWA	To monitor whether the client connect with flex connect CWA or not	Passed	
EWLCJ179S_Reg_566	Checking the client connectivity for Guest Foreign CWA	To check the client connectivity for Guest foreign CWA	Passed	
EWLCJ179S_Reg_567	validating radius server details in Guest foreign CWA	To validate the radius server details	Passed	
EWLCJ179S_Reg_568	Monitor the client connectivity for Guest CWA Anchor	To monitor whether the client connect with Guest CWA anchor or not	Passed	

WPA3 Supporting 'Transition Disable'

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_Reg_569	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	
EWLCJ179S_Reg_570	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	
EWLCJ179S_Reg_571	Verifying WPA3/Transition Disable details with 11ax Android client connected.	To verify WPA3/Transition Disable details with 11ax Android client connected.	Passed	
EWLCJ179S_Reg_572	Verifying WPA3/Transition Disable details with 11ax iPhone client connected.	To verify WPA3/Transition Disable details with 11ax iPhone client connected.	Passed	
EWLCJ179S_Reg_573	Verifying the WPA3/Transition Disable details with Windows client connected.	To verify the WPA3/Transition Disable details with non 11ax Windows client connected.	Passed	CSCwb98330
EWLCJ179S_Reg_574	Verifying the WPA3/Transition Disable details with Mac client connected.	To verify the WPA3/Transition Disable details with non 11ax Mac client connected.	Passed	
EWLCJ179S_Reg_575	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	
EWLCJ179S_Reg_576	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE Auth key.	Passed	

EWLCJ179S_Reg_577	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	
EWLCJ179S_Reg_578	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	
EWLCJ179S_Reg_579	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	
EWLCJ179S_Reg_580	Verifying the WPA3 support with SAE and PSK security key.	To verify the WPA3 support with SAE and PSK security key.	Passed	
EWLCJ179S_Reg_581	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 support with SAE and 802.1x security key.	Passed	
EWLCJ179S_Reg_582	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	
EWLCJ179S_Reg_583	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	
EWLCJ179S_Reg_584	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWLCJ179S_Reg_585	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security.	Passed	
EWLCJ179S_Reg_586	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security.	Passed	

EWLCJ179S_Reg_587	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with Ft+802.1x security.	Passed	
EWLCJ179S_Reg_588	Verifying the WPA3 support with Intra clinet roaming by using 9115AP	To verify the WPA3 support with Intra clinet roaming by using 9115AP	Passed	
EWLCJ179S_Reg_589	Verifying the WPA3 support and SAE security with Inter WLC Roaming	To verify the WPA3 support and SAE security with Inter WLC Roaming	Passed	
EWLCJ179S_Reg_590	Verifying the WPA3 support Roaming between Controllers	To verify the WPA3 support Roaming between Controllers with same Radio types	Passed	
EWLCJ179S_Reg_591	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.	Passed	
EWLCJ179S_Reg_592	Ensure transition disable compatibility with other WPA security modes	To verify transition disable compatibility with other WPA security modes	Passed	
EWLCJ179S_Reg_593	Verifying WPA3/Transition Disable details with Surface client connected.	To verify WPA3/Transition Disable details with Surface client connected.	Passed	
EWCJ179S_Reg_383	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	
EWCJ179S_Reg_384	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	

EWCJ179S_Reg_385	Verifying WPA3/Transition Disable details with 11ax Android client connected.	To verify WPA3/Transition Disable details with 11ax Android client connected.	Passed	
EWCJ179S_Reg_386	Verifying WPA3/Transition Disable details with 11ax iPhone client connected.	To verify WPA3/Transition Disable details with 11ax iPhone client connected.	Passed	
EWCJ179S_Reg_387	Verifying the WPA3/Transition Disable details with Windows client connected.	To verify the WPA3/Transition Disable details with non 11ax Windows client connected.	Passed	
EWCJ179S_Reg_388	Verifying the WPA3/Transition Disable details with Mac client connected.	To verify the WPA3/Transition Disable details with non 11ax Mac client connected.	Passed	
EWCJ179S_Reg_389	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	
EWCJ179S_Reg_390	Verifying the WPA3 support with SAE Auth key.	To verify the WPA3 support with SAE Auth key.	Passed	
EWCJ179S_Reg_391	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	
EWCJ179S_Reg_392	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	
EWCJ179S_Reg_393	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	

EWCJ179S_Reg_394	Verifying the WPA3 support with SAE and PSK security key.	To verify the WPA3 support with SAE and PSK security key.	Passed	
EWCJ179S_Reg_395	Verifying the WPA3 support with SAE and 802.1x security key.	To verify the WPA3 support with SAE and 802.1x security key.	Passed	
EWCJ179S_Reg_396	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	
EWCJ179S_Reg_397	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	
EWCJ179S_Reg_398	verifying the WPA3 support with SAE and PMF PSK Auth key.	To verify the WPA3 support with SAE and PMF PSK Auth key.	Passed	
EWCJ179S_Reg_399	Verifying the WPA3 support with 802.1x security.	To verify the WPA3 support with 802.1x security.	Passed	
EWCJ179S_Reg_400	Verifying the WPA3 support with 802.1x and CCKM security.	To verify the WPA3 support with 802.1x and CCKM security.	Passed	
EWCJ179S_Reg_401	Verifying the WPA3 support with Ft+802.1x security.	To verify the WPA3 support with Ft+802.1x security.	Passed	
EWCJ179S_Reg_402	Verifying the WPA3 support with Intra client roaming by using 9115AP	To verify the WPA3 support with Intra client roaming by using 9115AP	Passed	

C9105 EWC AP Support

Logical ID	Title	Description	Status	Defect ID
EWCJ179S_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	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	

EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	CSCwc12049
EWCJ179S_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	
EWCJ179S_Reg_43	Reassociation of client to the AP after reboot	To verify if the client gets reassociated to the to the AP .	Passed	
EWCJ179S_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	

EWCJ179S_Reg_45	Performing Intra controller roaming of Android client	To check whether intra controller roaming of Android clients works properly or not	Passed	
EWCJ179S_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	
EWCJ179S_Reg_47	Performing Intra controller roaming of Mac OS client	To check whether intra controller roaming of MacOS clients works properly or not	Passed	
EWCJ179S_Reg_48	Performing Inter controller roaming of Windows OS client	To check whether inter controller roaming of windows clients works properly or not	Passed	
EWCJ179S_Reg_49	Performing Inter controller roaming of Android client	To check whether inter controller roaming of Android clients works properly or not	Passed	
EWCJ179S_Reg_50	Performing Inter controller roaming of IOS client	To check whether inter controller roaming of IOS clients works properly or not	Passed	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	

EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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	
EWCJ179S_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
EWCJ179S_Reg_98	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	
EWCJ179S_Reg_99	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	
EWCJ179S_Reg_100	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	
EWCJ179S_Reg_101	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	
EWCJ179S_Reg_102	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	
EWCJ179S_Reg_103	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	
EWCJ179S_Reg_104	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	
EWCJ179S_Reg_105	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	

EWCJ179S_Reg_106	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	
EWCJ179S_Reg_107	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	
EWCJ179S_Reg_108	Checking the VLAN Tag after DCA Mode change	To check the VLAN tag after changing DCA mode	Passed	
EWCJ179S_Reg_109	Checking the VLAN Tag after changing Radio band	To check the VLAN tag after changing radio band	Passed	
EWCJ179S_Reg_110	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	
EWCJ179S_Reg_111	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	
EWCJ179S_Reg_112	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	

EWCJ179S_Reg_113	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	
EWCJ179S_Reg_114	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	
EWCJ179S_Reg_115	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	
EWCJ179S_Reg_116	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	
EWCJ179S_Reg_117	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	
EWCJ179S_Reg_118	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
EWCJ179S_Reg_119	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	
EWCJ179S_Reg_120	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	
EWCJ179S_Reg_121	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	
EWCJ179S_Reg_122	Checking the image version after Provisioning Ewlc_ME with PnP	Verifying the image version after Provisioning Ewlc_ME with PnP	Passed	
EWCJ179S_Reg_123	Checking the AP details after Provisioning Ewlc_ME with PnP	Verifying the AP details after Provisioning Ewlc_ME with PnP	Passed	
EWCJ179S_Reg_124	Checking WLANs broadcasting or not after provisioning	To verify whether WLANs are broadcasting or not after provisioning	Passed	
EWCJ179S_Reg_125	Connecting client to created WLAN and checking the client details	Verifying the client details after connecting WLAN	Passed	
EWCJ179S_Reg_126	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	

EWCJ179S_Reg_127	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	
EWCJ179S_Reg_128	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
EWCJ179S_Reg_218	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	
EWCJ179S_Reg_219	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	
EWCJ179S_Reg_220	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	
EWCJ179S_Reg_221	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	
EWCJ179S_Reg_222	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	

EWCJ179S_Reg_223	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	
EWCJ179S_Reg_224	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	
EWCJ179S_Reg_225	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	
EWCJ179S_Reg_226	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	
EWCJ179S_Reg_227	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	
EWCJ179S_Reg_228	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	
EWCJ179S_Reg_229	Connect iOS client from where SSID signal is week	To verify that iOS client connecting or not from where SSID signal is week	Passed	

EWCJ179S_Reg_230	Restarting the ME eWC after optimized roaming configuration	To verify that optimization roaming configuration remain same after reboot	Passed	
EWCJ179S_Reg_231	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
EWCJ179S_Reg_232	Verify parallel mode image download using TFTP in EWC 9130	To Verify parallel mode image download using TFTP in EWC 9130	Passed	
EWCJ179S_Reg_233	Verify parallel mode image download using SFTP in EWC 9130	To Verify parallel mode image download using SFTP in EWC 9130	Passed	
EWCJ179S_Reg_234	Verify parallel mode image download using TFTP in EWC HA setup	To Verify parallel mode image download using TFTP in EWC HA setup	Passed	
EWCJ179S_Reg_235	Verify parallel mode image download using SFTP in EWC HA setup	To Verify parallel mode image download using SFTP in EWC HA setup	Passed	
EWCJ179S_Reg_236	Verify parallel mode image download using TFTP in EWC 9120	To Verify parallel mode image download using TFTP in EWC 9120	Passed	
EWCJ179S_Reg_237	Verify parallel mode image download using SFTP in EWC 9120	To Verify parallel mode image download using SFTP in EWC 9120	Passed	
EWCJ179S_Reg_238	Verify parallel mode image download using TFTP in EWC 9115	To Verify parallel mode image download using TFTP in EWC 9115	Passed	
EWCJ179S_Reg_239	Verify parallel mode image download using SFTP in EWC 9115	To Verify parallel mode image download using SFTP in EWC 9115	Passed	
EWCJ179S_Reg_240	Verify parallel mode image download using TFTP in EWC 9105	To Verify parallel mode image download using TFTP in EWC 9105	Passed	

EWCJ179S_Reg_241	Verify parallel mode image download using SFTP in EWC 9105	To Verify parallel mode image download using SFTP in EWC 9105	Passed	
EWCJ179S_Reg_242	Cancel Image TFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWCJ179S_Reg_243	Cancel Image SFTP download process after predownloaded completion and upgrade with another version	To verify Image downloaded based on latest version	Passed	
EWCJ179S_Reg_244	Upgrade using TFTP without parallel image support	To verify Upgrade using TFTP without parallel image support	Passed	
EWCJ179S_Reg_245	Upgrade using SFTP without parallel image support	To verify Upgrade using SFTP without parallel image support	Passed	
EWCJ179S_Reg_246	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
EWCJ179S_Reg_285	Configuring Access Points, Channel width radio parameters for 5Ghz band.	To configure Access Points, Channel width radio parameters for 5Ghz band.	Passed	
EWCJ179S_Reg_286	Configuring Access Points, Channel width radio parameters for 2.4Ghz band.	To configure Access Points, Channel width radio parameters for 2.4Ghz band.	Passed	
EWCJ179S_Reg_287	Configure channel parameters for 5ghz band and monitor in DNAC	To configure channel parameters for 5ghz band and monitor in DNAC	Passed	
EWCJ179S_Reg_288	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	
EWCJ179S_Reg_289	Configure channel parameters for 24ghz band and monitor in DNAC	To configure channel parameters for 24ghz band and monitor in DNAC	Passed	
EWCJ179S_Reg_290	Configure channel parameters for dual band and monitor in DNAC	To configure channel parameters for dual band and monitor in DNAC	Passed	
EWCJ179S_Reg_291	Channel updating and monitor assurance in DNAC	To perform channel updating and monitor assurance in DNAC	Passed	
EWCJ179S_Reg_292	Configure tx power for 5ghz band and monitor in DNAC	To configure tx power for 5ghz band and monitor in DNAC	Passed	
EWCJ179S_Reg_293	Configure tx power for 24ghz band and monitor in DNAC	To configure tx power for 24ghz band and monitor in DNAC	Passed	

EWCJ179S_Reg_294	Configure tx power for dual band and monitor in DNAC	To configure tx power for dual band and monitor in DNAC	Passed	
EWCJ179S_Reg_295	Configure tx power for 5ghz rrm band and monitor in DNAC	To configure tx power for 5ghz rrm band and monitor in DNAC	Passed	
EWCJ179S_Reg_296	Configure tx power for 24ghz rrm band and monitor in DNAC	To configure tx power for 24ghz rrm band and monitor in DNAC	Passed	
EWCJ179S_Reg_297	Validate assurance via RRM using Android client	To validate assurance via RRM using Android client	Passed	
EWCJ179S_Reg_298	Validate assurance via RRM using Surface client	To validate assurance via RRM using Surface client	Passed	
EWCJ179S_Reg_299	Validate assurance via RRM using mac client	To validate assurance via RRM using mac client	Passed	
EWCJ179S_Reg_300	Validate assurance via RRM using different models of AP	To validate assurance via RRM using different models of AP	Passed	
EWCJ179S_Reg_301	Validate assurance via RRM using EWC-AP	To validate assurance via RRM using EWC-AP	Passed	
EWCJ179S_Reg_302	Validate assurance via RRM using HA pair	To validate assurance via RRM using HA pair	Passed	

TACACS

Logical ID	Title	Description	Status	Defect ID
EWCJ179S_Reg_354	Allowing the user for complete access to ME EWLC network via TACACS	To check whether user can able to read-write access the complete ME EWLC network or not via TACACS	Passed	
EWCJ179S_Reg_355	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	
EWCJ179S_Reg_356	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	
EWCJ179S_Reg_357	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	
EWCJ179S_Reg_358	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	
EWCJ179S_Reg_359	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	

EWCJ179S_Reg_360	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	
EWCJ179S_Reg_361	Providing the user for selected access to the ME EWLC via TACACS	To check whether user can able to have access with the selected checkbox's like "WLAN, Controller, Wireless, Security, Commands Line Interfaces and "Management" checkboxes.	Passed	
EWCJ179S_Reg_362	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	

Config Wireless

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_config_1	Web Auth Parameter map Name creating with spaces is accepting without any warning.	To verify the Web auth parameter	Failed	CSCwc21470
EWCJ179S_config_1	Dashboard - Overview dashlets issue	To verify the dashboard	Passed	CSCwc05335
EWCJ179S_config_2	Monitor command is duplicated in CLI	To verify Monitor command is duplicated in CLIor not	Failed	CSCwc33726
EWCJ179S_config_3	Different Data is showing for Image Type in AP Statistics	To verify the AP image type statistics	Passed	CSCwb92879

SRCFD

Logical ID	Title	Description	Status	Defect ID
EWLCJ179S_SR_01	Upgrade the 9120 ap with latest image	Verify core file generated or not while image upgrade	Passed	
EWLCJ179S_SR_02	Upgrade the 9130 ap with latest image	Verify core file generated or not while image upgrade	Passed	
EWLCJ179S_SR_03	Upgrade the 9115 ap with latest image	Verify core file generated or not while image upgrade	Passed	
EWLCJ179S_SR_04	Upgrade the 9105 ap with latest image	Verify core file generated or not while image upgrade	Passed	
EWLCJ179S_SR_05	Reload the ap after Changing the radio 2.4 ghz	Verify 2.4 Ghz radio retained or not after reload	Passed	
EWLCJ179S_SR_06	Reload the ap after Changing the radio 5 ghz	Verify 5 Ghz radio retained or not after reload	Passed	
EWLCJ179S_SR_07	Reload the ap after Changing the radio 6 ghz	Verify 6 Ghz radio retained or not after reload	Passed	
EWLCJ179S_SR_08	Associate S10 mobile with 9120 AP and perform roaming	Verify client connected or not with 9120 ap	Passed	
EWLCJ179S_SR_09	Associate sony mobile with 9130 AP and perform roaming	Verify client connected or not with 9130 ap	Passed	
EWLCJ179S_SR_10	Associate iOS client with 9115 AP and perform roaming	Verify client connected or not with 9115 ap	Passed	
EWLCJ179S_SR_11	Associate windows client with 9105 AP and perform roaming	Verify client connected or not with 9105 ap	Passed	
EWLCJ179S_SR_12	connect Android client with local security	Verify checking channel utilization during client connectivity	Passed	

EWLCJ179S_SR_13	connect windows client with flex mode	Verify crash happened or not during continue reload	Passed	
EWLCJ179S_SR_14	connect mac client with dot1x security	Verify crash happened or not during client connectivity	Passed	
EWLCJ179S_SR_15	Cisco 1852 AP: Kernel panic - not syncing: soft lockup: hung tasks	to check AP 1830 series in C9115 controller	Passed	
EWLCJ179S_SR_16	configure AP 1830 series in C9115 controller by ap console	to check AP 1830 series in C9115 controller by ap console	Passed	
EWLCJ179S_SR_17	configuring AP 1850 series in 9800 controller	to check AP 1850 series in 9800 controller	Passed	
EWLCJ179S_SR_18	check the kernel panic status in C9800-ap eWC	to check the kernel panic status in C9800-ap eWC	Passed	
EWLCJ179S_SR_19	configuring AP 4800 series in C1115 controller	to check kernel panic of AP 4800 series in C1115 controller	Passed	
EWLCJ179S_SR_20	ARP Broadcast for some VLANs shown as DISABLED in GUI even though it's enabled at vlan configuration	to configure vlan for ARP broad cast	Passed	
EWLCJ179S_SR_21	configuring Vlan & enable ARP Broadcast	to configure Vlan & enable ARP Broadcast	Passed	
EWLCJ179S_SR_22	configuring Vlan & enable ARP Broadcast in eWC	to configure Vlan & enable ARP Broadcast in eWC	Passed	
EWLCJ179S_SR_23	Stuck of show tech-support wireless - SSH session struck	to check logs of tech-support wireless	Passed	

EWLCJ179S_SR_24	configure keepalive to check ssh session	configure keepalive to check ssh session to check logs of tech-support wireless	Passed	
EWLCJ179S_SR_25	Set Up Cisco Smart Licensing on Prime Infrastructure	Cisco Smart Licensing on Prime Infrastructure	Passed	
EWLCJ179S_SR_26	Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager	To configure Transport Mode Between PI and Cisco Smart Software Manager	Passed	
EWLCJ179S_SR_27	Enable Smart License on Prime Infrastructure	to Enable Smart License on Prime Infrastructure	Passed	
EWLCJ179S_SR_28	Smart License registration not working in direct or gateway or proxy mode in all Prime Infra version	To verify smart Account Creation, registration and activation.	Passed	
EWLCJ179S_SR_29	Generate token from CSSM	To Generate token from CSSM	Passed	
EWLCJ179S_SR_30	Product instance direct-connect using trust token	To verify Product instance direct-connect using trust token	Passed	
EWLCJ179S_SR_31	verify device status in CSSM	To verify device status in CSSM	Passed	
EWLCJ179S_SR_32	verify Smart Licensing Support in eWC HA	To verify Smart Licensing Support in eWC HA	Passed	
EWLCJ179S_SR_33	verify device details and license count changes in CSSM	To verify device details and license count changes in CSSM	Passed	
EWLCJ179S_SR_34	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	

EWLCJ179S_SR_35	Check AP info upon AP unplug & connect to switch	To check if AP joins eWLC automatically upon after initial connect & unplug with switch	Passed	
EWLCJ179S_SR_36	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	
EWLCJ179S_SR_37	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	
EWLCJ179S_SR_38	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	
EWLCJ179S_SR_39	Verify if hostapd process comes up during AP bootup	To verify if hostapd process comes up during AP bootup	Passed	
EWLCJ179S_SR_40	Check AP connectivity with client upon association via 5Ghz radio	To check AP connectivity with client upon association via 5Ghz radio	Passed	
EWLCJ179S_SR_41	Check AP connectivity with client upon association via 2.4 Ghz	To check AP connectivity with client upon association via 2.4 Ghz	Passed	
EWLCJ179S_SR_42	Check AP connectivity with client upon association for different AP models	To check AP connectivity with client upon association for different AP models	Passed	

EWLCJ179S_SR_43	Check AP connectivity with client upon association for different AP models during roaming scenario	To check AP connectivity with client upon association for different AP models during roaming scenario	Passed	
EWLCJ179S_SR_44	Monitor traffic by connecting client to 2.4Ghz radio.	To verify OFDMA details by connecting client to 2.4Ghz radio.	Passed	
EWLCJ179S_SR_45	Verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	To verify OFDMA details with client connecting to WPA2 - PSK configured WLAN	Passed	
EWLCJ179S_SR_46	Verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	To verify OFDMA details with client connecting to WPA3 - Dot1x configured WLAN	Passed	
EWLCJ179S_SR_47	Connect upto 8 clients and monitor DL/UL OFDMA statistics	To connect upto 8 clients and monitor DL/UL OFDMA statistics	Passed	
EWLCJ179S_SR_48	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify EWC Internal AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ179S_SR_49	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify EWC & 4800 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	
EWLCJ179S_SR_50	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Verify EWC & 9100 AP operation with AP mode as local/flex/monitor and different combinations of slot submodes	Passed	

EWLCJ179S_SR_51	Validate the EDCA parameter with wmm-default profile	To associate the client and verifying EDCA parameter in wmm-default profile	Passed	
EWLCJ179S_SR_52	Enabling the RP method with RMI enabled already.	To enable the RP method with RMI option enabled already.	Passed	
EWLCJ179S_SR_53	ISSU upgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ179S_SR_54	Check ISSU downgrade with HA SSO RMI	To perform ISSU upgrade in HA SSO RMI setup and monitor behaviour	Passed	
EWLCJ179S_SR_55	Client retention during ISSU upgrade/downgrade	To verify client retention after ISSU upgrade/downgrade.	Passed	
EWLCJ179S_SR_56	Resetting the 9120 AP	To resetting the 9120 AP	Passed	
EWLCJ179S_SR_57	Change the Country Code in Ap	To change the country code available in AP	Passed	
EWLCJ179S_SR_58	mapping the policy tag and rf tags in AP	to map the policy tag and rf tags in AP configuration	Passed	
EWLCJ179S_SR_59	Change the Ap to 9130	To change the Ap to 9130 in console	Passed	
EWLCJ179S_SR_60	Connect 9130 AP with more than 3 devices	To Connect the 9130 AP with more than 3 devices	Passed	
EWLCJ179S_SR_61	Connect different models-AP 9120 with 2 devices	To Connect the 9120 AP with 2 devices	Passed	
EWLCJ179S_SR_62	Connect 9115 AP model with 2 devices	To Connect the 9115 AP with 2 devices	Passed	
EWLCJ179S_SR_63	Connect 9130 AP with only one device	To Connect 9130 AP with only one device	Passed	

EWLCJ179S_SR_64	Check if the memory leak is present in windows client	To check if the memory leak is present in windows client or not	Passed	
EWLCJ179S_SR_65	Check if the memory leak is present in different android version	To check if the memory leak is present in different version of android client or not	Passed	
EWLCJ179S_SR_66	Check if the memory leak is present in mac client	To check if the memory leak is present in mac client or not	Passed	
EWLCJ179S_SR_67	Change the AP mode into Monitor mode	To change the AP mode into Monitor mode and verify Crash occurs	Passed	
EWLCJ179S_SR_68	Change the AP mode into Sniffer mode	To change the AP mode into Sniffer mode and verify Crash occurs	Passed	
EWLCJ179S_SR_69	Connect with different model-9120 AP in local mode	To Connect the 9120 AP in local mode and Check any crash occurs	Passed	
EWLCJ179S_SR_70	Connect with different model-9105 AP in local mode	To Connect the 9105 AP in local mode and Check any crash occurs	Passed	
EWLCJ179S_SR_71	Enable native vlan for Swtichport in CLI	To enable native vlan for Swtichport in CLI	Passed	
EWLCJ179S_SR_72	Allow VLAN 0 ARP as priority tagging	To allow VLAN 0 ARPas priority tagging	Passed	
EWLCJ179S_SR_73	Disabling the ARP Broadcast in controller	To Disabling the ARP Broadcast in controller	Passed	
EWLCJ179S_SR_74	Check Radio Band Changes after refresh key pressed in 2.4GHz changing or not in 9800-L controller	To check Radio Band Changes after refresh key pressed in 2.4GHz changing or not in 9800-L controller	Passed	

EWLCJ179S_SR_75	Check Radio Band Changes after refresh key pressed in 2.4GHz changing or not in 9800-CL controller	To check Radio Band Changes after refresh key pressed in 2.4GHz changing or not in 9800-CL controller	Passed	
EWLCJ179S_SR_76	Check Radio Band Changes after refresh key pressed in 2.4GHz changing or not in 9800-80 controller	To check Radio Band Changes after refresh key pressed in 2.4GHz changing or not in 9800-80 controller	Passed	
EWLCJ179S_SR_77	Check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9105 AP	To check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9105 AP	Passed	
EWLCJ179S_SR_78	Check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9115 AP	To check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9115 AP	Passed	
EWLCJ179S_SR_79	Check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9120 AP	To check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9120 AP	Passed	
EWLCJ179S_SR_80	Check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9130 AP	To check Radio Band Changes without pressing refresh key in 2.4GHz changing or not in 9130 AP	Passed	
EWLCJ179S_SR_81	Check whether the Controller 9800-L is working fine while executing RA trace on AP	To check whether the Controller 9800-L is working fine while executing RA trace on AP	Passed	
EWLCJ179S_SR_82	Check whether the Controller 9800-CL is working fine while executing RA trace on AP	To check whether the Controller 9800-CL is working fine while executing RA trace on AP	Passed	

EWLCJ179S_SR_83	Check whether the Controller 9800-80 is working fine while executing RA trace on AP	To check whether the Controller 9800-80 is working fine while executing RA trace on AP	Passed	
EWLCJ179S_SR_84	Check whether the Controller 9800-80 is working fine after executing RA trace logs and after switchover	To check whether the Controller 9800-80 is working fine after executing RA trace logs and after switchover	Passed	
EWLCJ179S_SR_85	Check whether the client connections to the Ap are shown in RA	To check whether the client connections to the Ap are shown in RA	Passed	
EWLCJ179S_SR_86	Check whether the client connections to the Ap are shown in RA in CLI	To check whether the client connections to the Ap are shown in RA in CLI	Passed	
EWLCJ179S_SR_87	Disconnect the client while generating the RA and look whether the logs are generated without any crash	To disconnect the client while generating the RA and look whether the logs are generated without any crash	Passed	
EWLCJ179S_SR_88	Check Whether the syslog's are generating for AP in 9800-L Controller	To check Whether the syslog's are generating for AP in 9800-L Controller	Passed	CSCwc33187
EWLCJ179S_SR_89	Check Whether the syslog's are generating for AP in 9800-CL Controller	To check Whether the syslog's are generating for AP in 9800-CL Controller	Passed	
EWLCJ179S_SR_90	Check Whether the syslog's are generating for APs in 9800-80 Controller	To Check Whether the syslog's are generating for APs in 9800-80 Controller	Passed	
EWLCJ179S_SR_91	Connect a new ap to a controller and check the tag assignment to the AP in syslog's	To connect a new ap to a controller and check the tag assignment to the AP in syslog's	Passed	

EWLCJ179S_SR_92	Perform Reset in AP and check the behaviour of the AP after Reset in syslog	To perform Reset in AP and check the behaviour of the AP after Reset in syslog	Passed	
EWLCJ179S_SR_93	Check whether "SIP-5-LICENSING: SIP service is Up. License report acknowledged." log is seen in 9800-L controller	To check whether "SIP-5-LICENSING: SIP service is Up. License report acknowledged." log seen in 9800-L controller	Passed	
EWLCJ179S_SR_94	Check whether "SIP-5-LICENSING: SIP service is Up. License report acknowledged." log seen in 9800-CL controller	To check whether "SIP-5-LICENSING: SIP service is Up. License report acknowledged." log seen in 9800-CL controller	Passed	
EWLCJ179S_SR_95	Check whether "SIP-5-LICENSING: SIP service is Up. License report acknowledged." log seen in 9800-80 controller	To check whether "SIP-5-LICENSING: SIP service is Up. License report acknowledged." log seen in 9800-80 controller	Passed	
EWLCJ179S_SR_96	Check Whether the Smart licensing changes are shown in syslog or not	To check Whether the Smart licensing changes are shown in syslog or not	Passed	
EWLCJ179S_SR_97	Check for the smart licensing changes of HA-setup controller after smart licensing disabled in active and active to standby switchover	To check for the smart licensing changes of HA-setup controller after smart licensing disabled in active and active to standby switchover	Passed	
EWLCJ179S_SR_98	Show ap upgrade report shows when the ap is local mode	verify if ap is in local mode ap upgrade report show 100 % or not	Passed	
EWLCJ179S_SR_99	Show ap upgrade report shows when the ap is flex mode	verify if ap is in flex mode ap upgrade report	Passed	

EWLCJ179S_SR_100	Show ap upgrade report shows when the ap is monitor mode	verify if ap is in monitor ap upgrade report show 100 % or not	Passed	
EWLCJ179S_SR_101	Client ARP entry remains even if the client is disconnected, if the client is android device	verify if the client is a android device	Passed	
EWLCJ179S_SR_102	Client ARP entry remains even if the client is disconnected, if the client is android device	verify if the client is a android device with security 802.1x	Passed	
EWLCJ179S_SR_103	Client ARP entry remains even if the client is disconnected, if the client is a windows system	verify if the client will connect after windows update	Passed	
EWLCJ179S_SR_104	9800 Physical appliance in HA / Show inventory displays same serial number for Chassis 1 and 2	verify show inventory displays same serial number for chassis 1 and 2 when controller upgrade in controller 55	Passed	
EWLCJ179S_SR_105	9800 Physical appliance in HA / Show inventory displays same serial number for Chassis 1 and 2	verify show inventory displays same serial number for chassis 1 and 2 when ap upgrade 55 controller	Passed	
EWLCJ179S_SR_106	9800 Physical appliance in HA / Show inventory displays same serial number for Chassis 1 and 2	verify show inventory displays same serial number for chassis 1 and 2 when controller upgrade 61 controller	Passed	
EWLCJ179S_SR_107	Cisco 3802 FQI/NMI reset at rb_next+0xc when the ap is in 6ghz radio	verify Cisco 3802 FQI/NMI reset at rb_next+0xc in when ap is 6ghz radio	Passed	

EWLCJ179S_SR_108	Cisco 3802 FQI/NMI reset at rb_next+0xc when the ap is in 5 ghz radio	verify Cisco 3802 FQI/NMI reset at rb_next+0xc in when ap is 5 ghz radio	Passed	
EWLCJ179S_SR_109	Cisco 3802 FQI/NMI reset at rb_next+0xc when the ap is in 2.4 ghz radio	verify Cisco 3802 FQI/NMI reset at rb_next+0xc in when ap is 2.4 ghz radio	Passed	
EWLCJ179S_SR_110	check whether the controller 9800-CL is logged in client machine without a capwap crash	To check whether the controller 9800-CL is logged in client machine without a capwap crash	Passed	
EWLCJ179S_SR_111	check whether the controller 9800-L is logged in client machine without a capwap crash	To check whether the controller 9800-L is logged in client machine without a capwap crash	Passed	
EWLCJ179S_SR_112	check whether the controller 9800-80 is logged in client machine without a capwap crash	To check whether the controller 9800-80 is logged in client machine without a capwap crash	Passed	
EWLCJ179S_SR_113	check whether the controller 9800-CL is changing time zone and in CLI showing the same time zone for ap	To check whether the controller 9800-CL is changing time zone and in CLI showing the same time zone for ap	Passed	
EWLCJ179S_SR_114	check whether the controller 9800-L is changing time zone and in CLI showing the same time zone for ap	To check whether the controller 9800-L is changing time zone and in CLI showing the same time zone for ap	Passed	

EWLCJ179S_SR_115	check whether the controller 9800-80 is changing time zone and in CLI showing the same time zone for ap	To check whether the controller 9800-80 is changing time zone and in CLI showing the same time zone for ap	Passed	
EWLCJ179S_SR_116	check whether the controller 9800-CL is showing correct mesh info	To check whether the controller 9800-CL is showing correct mesh info	Passed	
EWLCJ179S_SR_117	check whether the controller 9800-80 is showing correct mesh info	To check whether the controller 9800-80 is showing correct mesh info	Passed	
EWLCJ179S_SR_118	check whether the controller 9800-L is showing correct mesh info	To check whether the controller 9800-L is showing correct mesh info	Passed	
EWLCJ179S_SR_119	Apple client can't associate using SAE to a WPA3-enabled PSK SSID	check whether it is working in WAP+WAP2 configuration	Passed	
EWLCJ179S_SR_120	Apple client can't associate using SAE to a WPA3-enabled PSK SSID	check whether it is working in WAP2+WAP3 configuration	Passed	
EWLCJ179S_SR_121	Apple client can't associate using SAE to a WPA3-enabled PSK SSID	check whether it is working in WAP3 configuration	Passed	

Related Documents

Related Documentation

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.9 Configuration Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg.html

Cisco Catalyst 9800 Series Wireless Controller 17.9 Release Notes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/release-notes/rn-17-9-9800.html

Release Notes for Cisco Digital Network Architecture Spaces

https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/release-notes/b-cisco-dnas-rn.html

Cisco Catalyst 9600 Series Switches 17.9 Release Notes

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-9/release_notes/ol-17-9-9600.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/2-3-4/release_notes/b_cisco_dna_center_rn_2_3_4.html

PI 3.10 User Guide

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-10/user/guide/ciscoprimeinfrastructure_3_10_userguide.html

ISE 3.2 Release Notes

https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/release_notes/b_ise_32_RN.html